

IRREDUCIBILITY OF RANDOM POLYNOMIALS

CHRISTIAN BORST, EVAN BOYD, CLAIRE BREKKEN, SAMANTHA SOLBERG,
MELANIE MATCHETT WOOD, AND PHILIP MATCHETT WOOD

ABSTRACT. We study the probability that a random polynomial with integer coefficients is reducible when factored over the rational numbers. Using computer-generated data, we investigate a number of different models, including both monic and non-monic polynomials. Our data supports conjectures made by Odlyzko and Poonen and by Konyagin, and we formulate a universality heuristic and new conjectures that connect their work with Hilbert’s Irreducibility Theorem and work of van der Waerden. The data indicates that the probability that a random polynomial is reducible divided by the probability that there is a linear factor appears to approach a constant and, in the large-degree limit, this constant appears to approach one. In cases where the model makes it impossible for the random polynomial to have a linear factor, the probability of reducibility appears to be close to the probability of having a non-linear, low-degree factor. We also study characteristic polynomials of random matrices with $+1$ and -1 entries.

1. INTRODUCTION

Hilbert’s Irreducibility Theorem states that a monic polynomial of degree d , where each coefficient is chosen uniformly and independently from integers in the interval $[-K, K]$, is irreducible over the integers with probability tending to one as K goes to infinity. This statement of the theorem was proved by van der Waerden [25] in 1934. In 1963, Chela [4] proved that the number of reducible (over the integers) polynomials of this form divided by K^{d-1} approaches a constant as K goes to infinity. Chela’s result [4] can be interpreted as proving that the probability of reducibility divided by the probability that the constant coefficient equals zero approaches a constant as K goes to infinity (see Theorem 3.1 and Figure 1), and we believe that this interpretation is an example of a universal phenomenon.

Heuristic 1.1 (Universality). *Let $f(x)$ be a random polynomial with sufficiently well-behaved integer coefficients. Then the probability that $f(x)$ is reducible over the rationals divided by the probability that f has a linear (or lowest possible degree) factor approaches a constant C in the limit as the degree goes to infinity, or in the limit as the support of the random coefficients goes to infinity, or both. Furthermore, in the limit as the degree goes to infinity, whether or not the support goes to infinity, the constant C should equal 1.*

We study many polynomial models that appear to satisfy Heuristic 1.1 (primarily with independent coefficients, though some with dependence, see Section 4), and the “well-behaved” condition is meant to exclude models with specific features that cause high-degree factors, for example, a random polynomial of degree d formed as the product of two random polynomials with degree around $d/2$. Throughout, “reducible” will be used as shorthand for “reducible over the rationals.” Note that for monic polynomials, reducibility over the rationals is equivalent to reducibility over the integers by Gauss’s Lemma. For non-monic polynomials, we are interested in cases where all

Key words and phrases. random integer polynomials, irreducible, low-degree factors.

Christian Borst, Evan Boyd, Claire Brekken, and Samantha Solberg were supported by NSF grant DMS-1301690.

Melanie Matchett Wood was supported by an American Institute of Mathematics Five-Year Fellowship, a Packard Fellowship for Science and Engineering, a Sloan Research Fellowship, and National Science Foundation grant DMS-1301690. Philip Matchett Wood was supported by NSA grant H98230-16-1-0301.

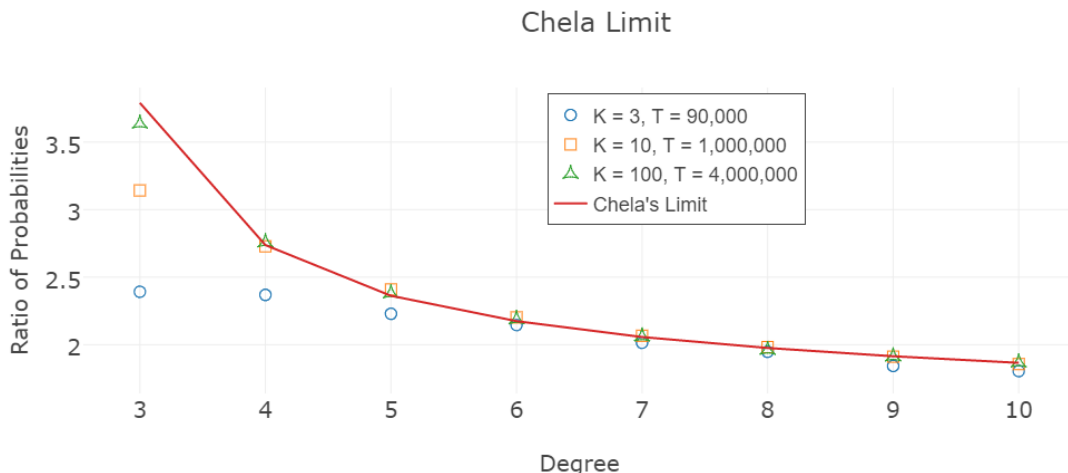


FIGURE 1. Let $h(x)$ be a degree d monic polynomial with all other coefficients chosen independently and randomly from integers in the interval $[-K, K]$. A result proven by Chela [4] (see Theorem 3.1) implies that the probability that $h(x)$ is reducible divided by the probability that the constant coefficient is zero goes to a limit as K goes to infinity. Above is a plot of data supporting this result when $K = 3, 10$ and 100 , where T is the number of random trials to compute the respective data points. The data points are a ratio of the probability of reducibility divided by $\frac{1}{2K+1}$, which is the probability that the constant coefficient is zero. The figure indicates that convergence to the limit proven by Chela is relatively fast, especially for degree 6 and larger. The 99.9999% confidence intervals are ± 0.058 , ± 0.053 , and ± 0.251 for $K = 3, 10$, and 100 , respectively.

factors have positive degree, so we factor over the rationals; for example, $2x^2 + 4 = 2(x^2 + 2)$ is irreducible over the rationals, because 2 has a multiplicative inverse in the rationals.

O'Rourke and Wood [17] study a variety of models, proving that pointwise delocalization of the roots of a random polynomial implies that low-degree factors are very unlikely. Konyagin [12] studied random monic polynomials with 0 or 1 for coefficients and proved a bound on the probability of low-degree factors which he then used to prove a bound on the probability of reducibility. Heuristic 1.1 compliments these results on low-degree factors by suggesting that high-degree factors are even less likely than low-degree factors, and proving results in this direction is an interesting open problem.

Kuba [13] studied non-monic polynomials with integer coefficients chosen independently in the interval $[-K, K]$ (conditioned on the lead coefficient being nonzero), and proved a result implying that the probability of reducibility divided by the probability that the constant term is zero is bounded by a constant. This can be viewed as a step towards proving a version of Chela's [4] result (and a case of Heuristic 1.1) for non-monic polynomials. In Section 3, we will test generalizations of Hilbert's Irreducibility Theorem, studying polynomials with fixed degree in the limit as the support for the coefficients grows, and we will state special cases of Heuristic 1.1 as conjectures.

In Hilbert's Irreducibility Theorem, the degree is fixed and the support of the coefficients is growing, and we believe that Heuristic 1.1 also holds for cases where the range of support of the coefficients is fixed and the degree goes to infinity. For example, let $g_{\{0,1\},d}(x)$ be a monic degree d polynomial with constant coefficient equal to 1 and with every other coefficient equal to 0 or 1 independently with probability $\frac{1}{2}$. In 1993, Odlyzko and Poonen [16] conjectured that the

Probability of Reducibility of 0,1 Polynomials

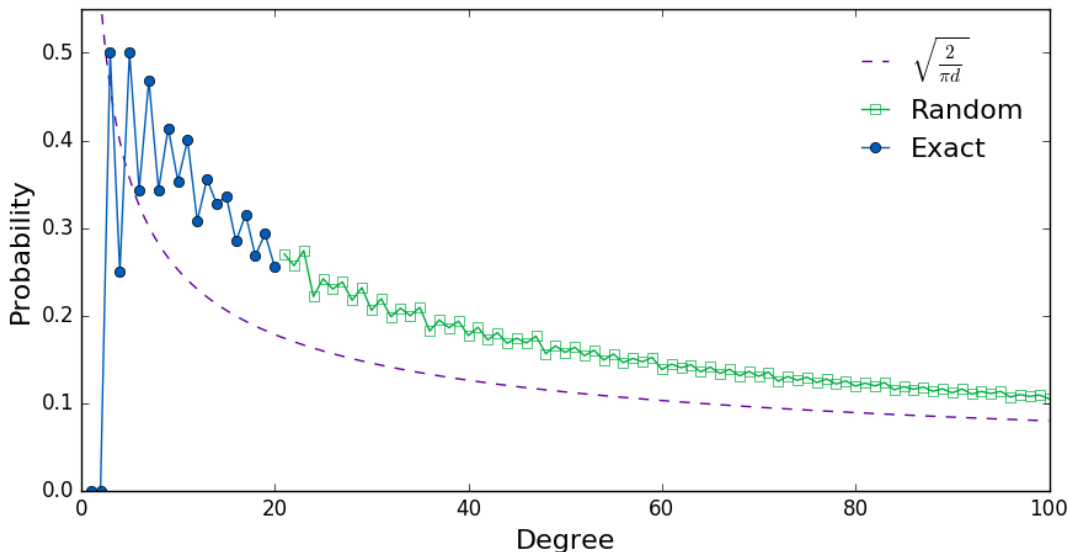


FIGURE 2. The plot above shows the probability of reducibility for monic 0,1 polynomials, where the lead and constant coefficients are 1 and all other coefficients are 0 or 1 independently with probability $1/2$ (note this figure also appears in [17, Figure 1]). The exact points (circles) were computed by exhaustive generation of all 0,1 polynomials of degree up to 20. The random points (squares) were generated with 1,000,000 random trials, giving a 99.9999% confidence interval of ± 0.0025 . The curve (dashed) is an asymptotic lower bound for the probability of reducibility derived from the probability that $x - 1$ is a factor of the polynomial (see Proposition 5.1). The data shows that the probability of reducibility approaches the probability that $x - 1$ is a factor, supporting Konyagin’s conjecture [12] and Heuristic 1.1 (see also Figure 4).

probability of irreducibility for these polynomials approaches 1 as the degree d approaches infinity. Konyagin [12] then conjectured in 1999 that the probability that $x + 1$ is a factor of $g_{\{0,1\},d}(x)$, given that it is reducible, approaches 1 as d approaches infinity, which can be viewed as a case of Heuristic 1.1 (see Figure 2).

We consider the following related model: Let $g_{\pm 1,d}(x)$ be a monic polynomial with degree d with all other coefficients $+1$ or -1 independently with probability $\frac{1}{2}$. In Conjecture 2.2, we extend Odlyzko and Poonen’s conjecture to these polynomials as well. A version of Konyagin’s conjecture appears to apply to odd-degree polynomials $g_{\pm 1,d}(x)$, where having a linear factor appears to be the most common way for such a polynomial to factor—see Figure 3 and Conjecture 2.1. Even-degree polynomials $g_{\pm 1,d}(x)$ cannot have a linear factor, but these polynomials may still support a variant of Konyagin’s conjecture where having a quadratic or other low-degree factor appears to be the most common way for such a polynomial to factor—see Lemma 5.2. Also, O’Rourke and Wood [17] prove that all polynomials of this form have a vanishingly small probability of having a factor with any fixed degree, including linear factors, as d goes to infinity. Data for both polynomials $g_{\{0,1\},d}(x)$ and $g_{\pm 1,d}(x)$ supports these conjectures and our Heuristic 1.1 (see Section 2).

Random polynomials with coefficients 1 or -1 have also been studied by Peled, Sen, and Zeitouni [18], and they prove that the probability of a double root is asymptotically equal to the probability

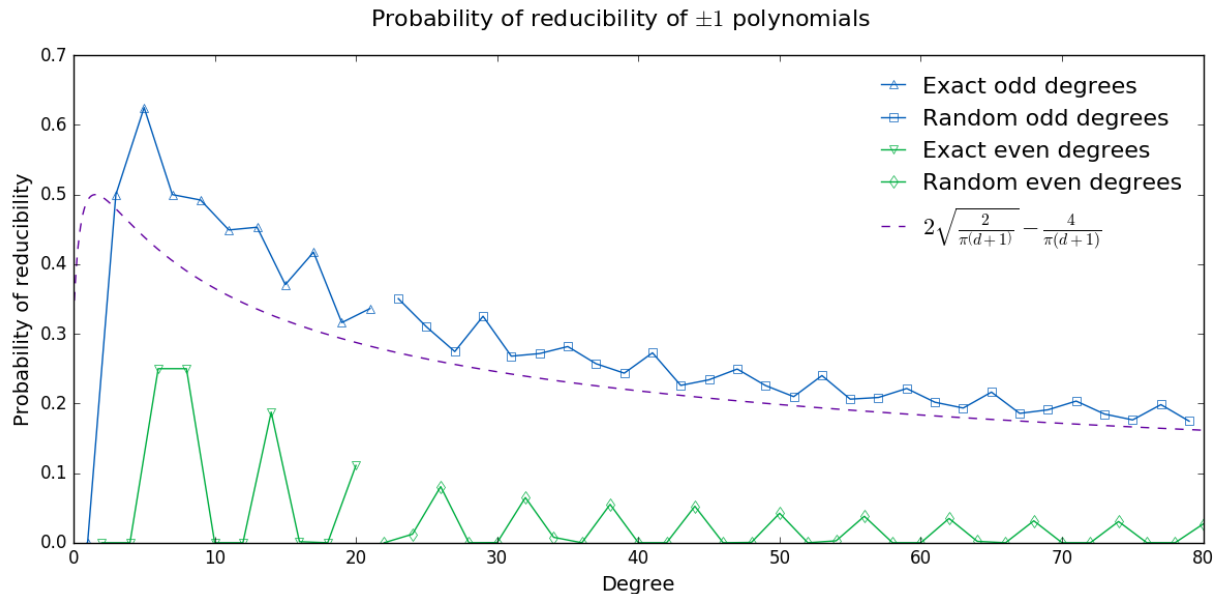


FIGURE 3. The plot above shows probability of reducibility for monic polynomials where each coefficient is $+1$ or -1 independently with probability $1/2$ (note that this figure also appears in [17, Figure 2]). The random data was calculated using 150,000,000 trials, giving a 99.9999% confidence interval of 0.0002 for every value. The lower bound on the probability of reducibility for odd degrees (dashed) is the asymptotic probability that a degree d polynomial has a linear factor (see Proposition 5.3). If the degree is even, the polynomials cannot have a linear factor, and the reducibility probability appears to be distinctly lower. For even degrees, a Galois theory argument ([17, Subsection 2.2]) proves that the reducibility probability is exactly zero whenever $d + 1$ is prime and 2 generates the multiplicative group of $(\mathbb{Z}/(d + 1))^{\times}$, which should happen for infinitely many d by Artin’s Conjecture (see, for example, [15]).

that either -1 or 1 is a double root (and they further extend this result to polynomials with coefficients 1 , 0 , or -1 ; see Bary-Soroker and Kozma [2] for the bivariate case). This result is related to Section 2 where we conjecture for random polynomials with 1 or -1 coefficients that, among reducible polynomials, the probability that $x + 1$ or $x - 1$ is a factor tends to 1 (see Conjecture 2.1). Very roughly, both Peled, Sen, and Zeitouni’s result [18] and Conjecture 2.1 suggest that the coincidence of having a double root or the coincidence of factoring are most likely to happen in the simplest way, and that is when 1 or -1 is a root.

Random polynomials of the sort considered in Hilbert’s Irreducibility Theorem have been studied in probabilistic Galois theory. For example, van der Waerden [25] proved that if $h_{[-K,K],d}(x)$ is monic with degree d and all of its coefficients are chosen independently and uniformly from integers in the interval $[-K, K]$, then the probability that the Galois group for $h_{[-K,K],d}(x)$ is S_d , the symmetric group of d elements, tends to 1 as K tends to infinity. Work proving successively better upper bounds on the probability that $h_{[-K,K],d}(x)$ does not have Galois group S_d has continued with the work of Knobloch in 1955 [10] and 1956 [11], Gallagher in 1973 [6], Zywinia in 2010 [26], Dietmann in 2013 [5], and finally Rivin [19] in 2015, who proved the upper bound $\frac{\log^c K}{K}$, where $c = c_d$ is a constant depending on d , which is the first upper bound demonstrating that the probability decreases linearly in K , up to a polylog factor.

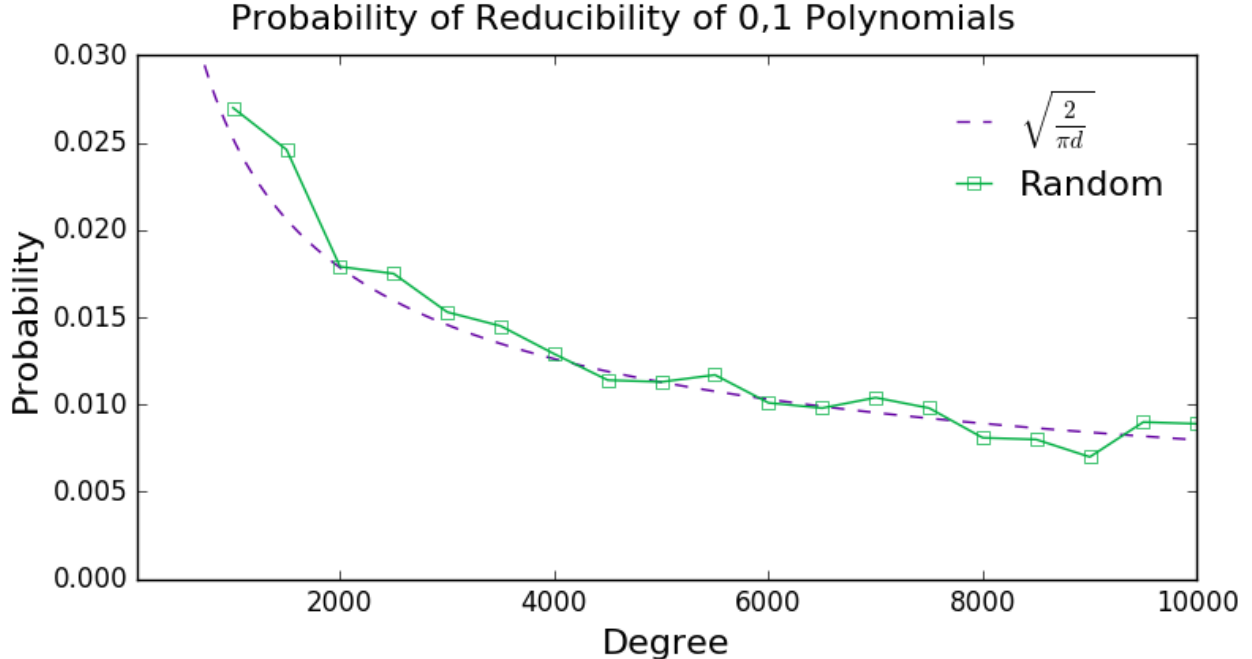


FIGURE 4. The probability of reducibility for 0,1 polynomials of high degree. The random data (squares) was generated with 10,000 trials, a relatively small number necessitated by the high degree, giving a 95% (2 standard deviations) confidence interval of ± 0.010 , which is relatively large for this figure. The asymptotic lower bound (dashed) is the same bound as in Figure 2, and we believe some points fall below this asymptotic lower bound due to measurement error, which would be corrected if substantially more trials were conducted.

For this paper, computer simulations were used to randomly measure data points in the real numbers whose exact values are unknown, and we quantify the likely difference between our measured data points and the actual values using confidence intervals. For example, we say a randomly measured data value of x has a 99.9999% (five standard deviations) confidence interval of $\pm \epsilon$ to mean that, at the start of the random experiment, there is at most a one-in-a-million chance (i.e., probability 0.000001) that the measured value will differ from the actual value by more than ϵ . The data for this paper was collected using HTCondor [14, 21, 24], a high-throughput computing software system developed and maintained at the University of Wisconsin-Madison, and programming was done primarily in Magma.

The paper is organized as follows. Section 2 studies examples of monic polynomials where the support of coefficients is fixed and the degree is increasing, including coefficients either 0 or 1 and coefficients either 1 or -1 , where each coefficient is independently chosen with probability $\frac{1}{2}$. Section 3 gives examples of random monic and non-monic polynomials where the degree is fixed and the range of support of the coefficients is growing. This includes coefficients chosen uniformly from integers in the interval $[-K, K]$ and other distributions on integers in the interval $[-K, K]$. Section 4 studies characteristic polynomials of random d by d matrices where each entry is $+1$ or -1 independently with probability $1/2$, a case where both the degree of the polynomial and the support of the coefficients tend to infinity as d increases. Propositions, lemmas, and proofs appear in Section 5.

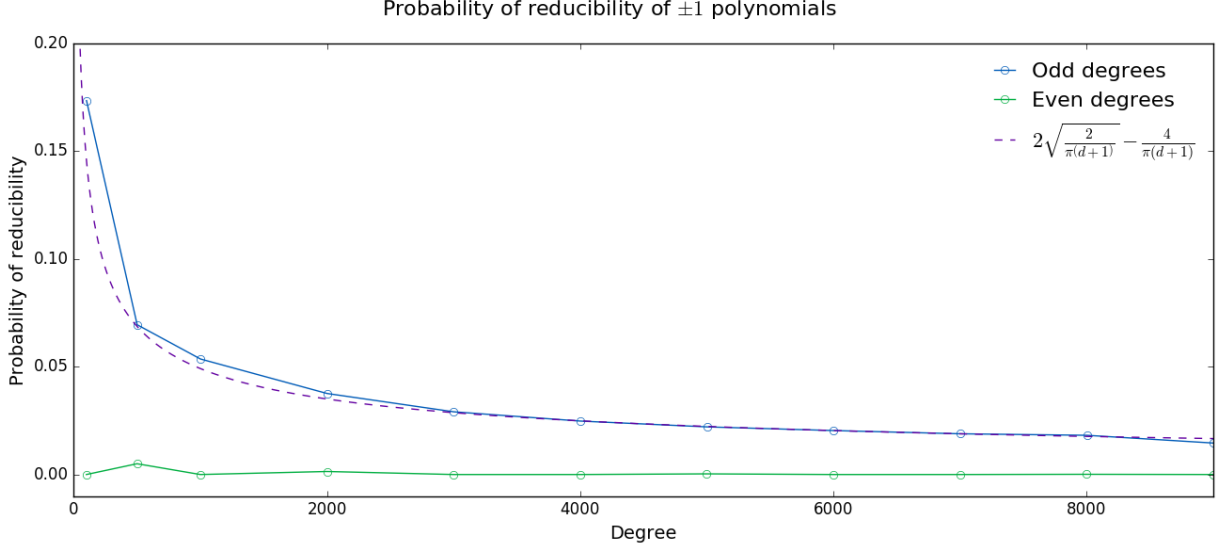


FIGURE 5. The probability of reducibility for ± 1 polynomials with high degree. The data was calculated randomly using 10,000 trials, giving 95% (2 standard deviations) confidence interval of ± 0.01 . The lower bound for odd-degrees is the same as the lower bound in Figure 3.

2. FIXED SUPPORT WITH GROWING DEGREE

Zero-One Polynomials. Let $g_{\{0,1\},d}(x) = x^d + a_{d-1}x^{d-1} + \dots + a_1x + 1$ be a random monic polynomial with degree d and constant coefficient 1, where every other coefficient a_1, \dots, a_{d-1} is 0 or 1 independently with probability $1/2$. As shown in Proposition 5.1, the probability that $g_{\{0,1\},d}(x)$ has $x+1$ as a factor is asymptotically $\sqrt{\frac{2}{\pi d}}$, which is a lower bound for the probability of reducibility. Our data suggests that as the degree increases, the probability of reducibility converges to this lower bound (see Figures 2 and 4).

Consider a random monic polynomial $h_{\{0,1\},d}(x)$ with the same form as $g_{\{0,1\},d}(x)$ above, but with the constant term also allowed to be 0 or 1 independently with probability $1/2$. One could ask: For polynomials $h_{\{0,1\},d}(x)$, does the probability of reducibility divided by the probability that the constant term is 0 go to 1 as the degree d increases? The answer to this question is yes if and only if the probability that the polynomials $g_{\{0,1\},d}(x)$ are irreducible goes to 1 as the degree d goes to infinity. The equivalence is true because the probability of reducibility for polynomials $h_{\{0,1\},d}(x)$ is equal to $1/2$ (the probability that the constant coefficient is zero) plus the probability of reducibility for polynomials $g_{\{0,1\},d}(x)$. Thus, Heuristic 1.1 for $h_{\{0,1\},d}(x)$ is equivalent to Odlyzko-Poonen's conjecture [16] that $g_{\{0,1\},d}(x)$ becomes irreducible with probability tending to 1 as d goes to infinity.

Rademacher ± 1 Polynomials. Let $g_{\pm 1,d}(x) = x^d + a_{d-1}x^{d-1} + \dots + a_0$ be a monic, degree d polynomial where each coefficient a_0, a_1, \dots, a_{d-1} is either 1 or -1 independently with probability $\frac{1}{2}$. In Figure 3 and Figure 5, we see that the probability of reducibility of $g_{\pm 1,d}(x)$ polynomials decreases as the degree d goes to infinity. For odd-degree d , we prove that $2\sqrt{\frac{2}{\pi(d+1)}} - \frac{4}{\pi(d+1)}$ is an asymptotic lower bound, based on the probability that $x+1$ or $x-1$ is a factor (see Lemma 5.2 and Proposition 5.3). For even-degree d , a linear factor over the integers is impossible (see Lemma 5.2). Figure 3 and Figure 5 suggest that, when the degree is odd, the probability that $g_{\pm 1,d}(x)$ is reducible

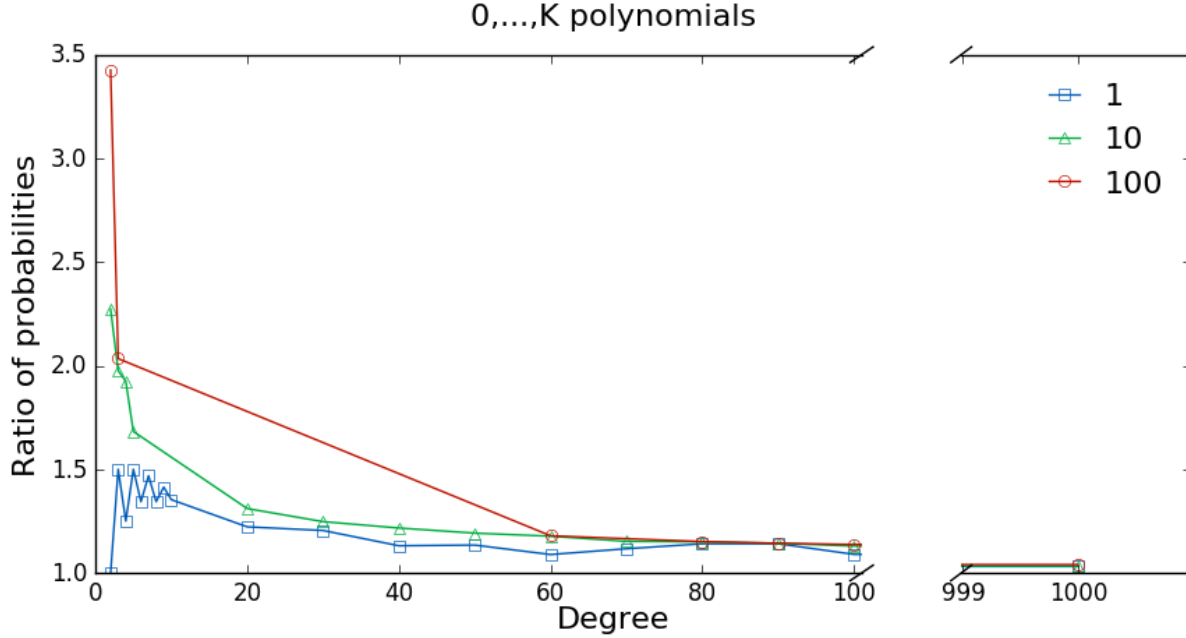


FIGURE 6. Consider a random monic polynomial where each coefficient is sampled uniformly from integers in the interval $[0, K]$. Above is a plot of data measuring the probability that such a polynomial is reducible divided by the probability that the constant term is 0, which is $\frac{1}{K+1}$. The ratio appears to tend to 1 as the degree increases, supporting Heuristic 1.1. Each data point was generated with $2500K^2$ trials, giving 99.9999% confidence intervals of ± 0.1 , ± 0.055 and ± 0.0505 , respectively, for $K = 1, 10$, and 100 .

approaches the probability that $g_{\pm 1, d}(x)$ has a linear factor, supporting Heuristic 1.1 and suggesting the following conjecture, which is analogous to Konyagin's conjecture in [12].

Conjecture 2.1. *Let d be an odd positive integer. For random monic polynomials $g_{\pm 1, d}(x) = x^d + a_{d-1}x^{d-1} + \dots + a_0$, where the a_i are $+1$ or -1 independently with probability $1/2$, the probability that $g_{\pm 1, d}(x)$ has a linear factor $x + 1$ or $x - 1$, conditioned on $g_{\pm 1, d}(x)$ being reducible, goes to 1 as the degree d goes to infinity.*

The data also suggests the following analog of Odlyzko and Poonen's [16] conjecture.

Conjecture 2.2. *Let d be a positive integer. For random monic polynomials $g_{\pm 1, d}(x) = x^d + a_{d-1}x^{d-1} + \dots + a_0$, where the a_i are $+1$ or -1 independently with probability $1/2$, the probability that $g_{\pm 1, d}(x)$ is reducible goes to 0 as the degree d goes to infinity.*

3. GROWING SUPPORT WITH FIXED DEGREE

Uniform integers in the interval $[-K, K]$. Chela [4] proved the theorem below, which we have rephrased in terms of a ratio of probabilities to show its connection with Heuristic 1.1.

Theorem 3.1 (Chela [4]). *Let $h = h_{[-K, K], d}(x) = x^d + a_{d-1}x^{d-1} + \dots + a_1x + a_0$ be a polynomial with degree $d > 2$, where the a_i are chosen uniformly and independently from integers in the interval $[-K, K]$. As K goes to infinity, the probability of reducibility divided by the probability that the*

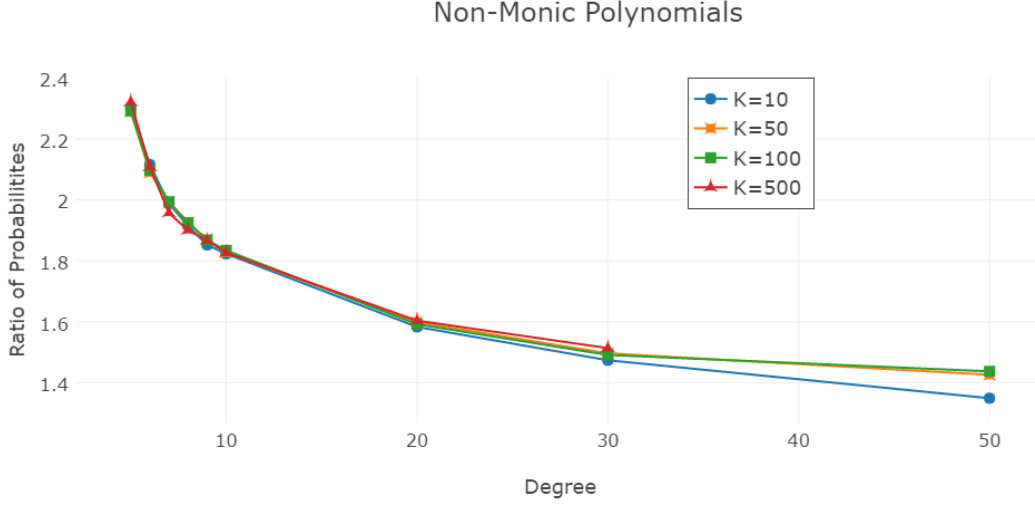


FIGURE 7. Above is a plot of data supporting a result due to Kuba [13] (Theorem 3.2) for $K = 10, 50, 100$, and 500 , with the data generated using 250,000, 6,250,000, 25,000,000, and 625,000,000 trials, respectively. The points are a ratio of the probability of reducibility divided by $\frac{1}{2K+1}$, which is the probability that the constant coefficient is zero. The 99.9999% confidence interval for each data point is at most ± 0.105 .

constant coefficient is zero goes to the limit C_d , i.e.,

$$(1) \quad \lim_{K \rightarrow \infty} \frac{\Pr(h(x) \text{ is reducible})}{\frac{1}{2K+1}} = C_d := 2\zeta(d-1) - 1 + \frac{k_d}{2^{d-2}},$$

where $k_d = \int \int \dots \int dx_1 dx_2 \dots dx_{d-1}$, with the iterated integral running over all x_i satisfying $|x_i| \leq 1$ for $1 \leq i \leq d-1$ and $|x_1 + x_2 + \dots + x_{d-1}| \leq 1$.

We generated data for polynomials $h_{[-K,K],d}(x)$ to find the probability of reducibility for varying K values—see Figure 1. It is interesting to note that our data fits closely with Chela’s limit for small K values, especially when d increases. Also note that the right-hand side of (1) in Theorem 3.1 approaches 1 as d goes to infinity, supporting Heuristic 1.1.

Uniform integers in the interval $[0, K]$. We consider the probability of reducibility for polynomials of the form $f_{[0,K],d}(x) = x^d + a_{d-1}x^{d-1} + \dots + a_1x + a_0$, where the a_i are chosen uniformly and independently from the interval $[0, K]$ and K is a positive integer. To study Heuristic 1.1 in this case, we collected data for the probability of reducibility divided by the probability that the constant coefficient is zero (which is $1/(K+1)$) for various degrees and values of K . Figure 6 indicates that, as predicted by Heuristic 1.1, the ratio of probabilities appears to tend to a constant as K increases and to tend to 1 as the degree increases.

Non-Monic Uniform Coefficients. Kuba [13] considered non-monic polynomials and proved the following theorem, which we have rephrased in terms of a ratio of probabilities to show its connection with Heuristic 1.1.

Theorem 3.2 (Kuba [13]). *Let $h_{K,d}(x) = a_dx^d + a_{d-1}x^{d-1} + \dots + a_0$ be a polynomial with degree $d > 2$, where the a_i are chosen uniformly and independently from integers in the interval $[-K, K]$,*

and a_d is nonzero. Then,

$$\frac{\Pr(h_{K,d}(x) \text{ is reducible})}{\frac{1}{2K+1}} \leq C_d, \quad \text{for every } K \geq 1,$$

where C_d is a constant depending only on d . (Note that the left-hand side of the inequality above is always at least 1.)

Our computer data indicates that the probability that $h_{K,d}(x)$ is reducible divided by $\frac{1}{2K+1}$ decreases to 1 as d goes to infinity; see Figure 7. Data with higher degree (we also tested $d = 80, 90, 100, 200$) further suggests that this ratio goes to 1.

Binomial Coefficients. One natural, non-uniform way to choose coefficients in the interval $[0, K]$ is to use a binomial distribution, $\text{Bin}(K, p)$, where K is a positive integer and $0 \leq p \leq 1$, so that the value ℓ is taken with probability $\binom{K}{\ell} p^\ell (1-p)^{K-\ell}$. Heuristic 1.1 is easiest to understand when the probability of a linear factor is dominated by the probability that the constant coefficient is zero, and thus we let $p = 1/K$, in which case the constant coefficient is zero with probability $(1 - 1/K)^K$, which is close to e^{-1} especially as K increases. Interestingly, this binomial model has features similar to 0,1 polynomials, in that each coefficient takes the value zero with roughly constant probability as K increases, while still having the support of the coefficients tend to infinity as K increases (the binomial distribution approximates a Poisson distribution as K increases). Data in Figure 8 suggests that Heuristic 1.1 still holds, and we make the following conjecture.

Conjecture 3.3. *For a random monic polynomial $h_{\text{Bin},K,d}(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1x + a_0$ with coefficients a_0, \dots, a_{d-1} chosen from the interval $[0, K]$ using a $\text{Bin}(K, 1/K)$ distribution, the probability that the polynomial is reducible divided by the probability that the constant coefficient is zero goes to 1 as K goes to infinity.*

4. CHARACTERISTIC POLYNOMIAL OF A RANDOM ± 1 MATRIX.

We consider the probability of reducibility for $\chi(x)$, the characteristic polynomial of a d by d matrix with integer entries. This case is different than the previous two sections because both the degree of the characteristic polynomial and the support of the coefficients grow as d increases. We study the case where the d by d matrix has entries that are $+1$ or -1 independently with probability $\frac{1}{2}$. Some results are known for other models of random matrices. In [20], Rivin studies random integer matrices formed as products of random elements in the special linear group $\text{SL}(n, \mathbb{Z})$, where the random elements are chosen in two ways: either uniformly over all matrices in $\text{SL}(n, \mathbb{Z})$ with coefficients uniformly bounded by a constant, or in terms of word length based on a fixed generating set for $\text{SL}(n, \mathbb{Z})$. Rivin [20] shows that the probability that the characteristic polynomial is reducible tends to 0 in both cases as n increases, and also studies $\text{Sp}(n, \mathbb{Z})$ (see further extensions in [7]).

In the case where the d by d matrix has entries that are $+1$ or -1 independently with probability $\frac{1}{2}$, Figure 9 indicates that the probability of reducibility decreases as d increases, and the probability of reducibility appears to become close to a lower bound derived from the probability that the matrix has a pair of rows or columns that are dependent (this implies that the constant coefficient, which is the determinant of the matrix, is zero). It has long been conjectured (see, for example, [9, 8, 22, 23, 3, 1]) that the probability that a uniform random d by d matrix with ± 1 entries has determinant zero is asymptotically

$$(2) \quad 4 \binom{d}{2} \left(\frac{1}{2}\right)^d = \left(\frac{1}{2} + o(1)\right)^d,$$

where $o(1)$ is a small quantity tending to zero as d tends to infinity. The term $4 \binom{d}{2} \left(\frac{1}{2}\right)^d$ is an asymptotic lower bound coming from the probability that there is a pair of rows or columns that

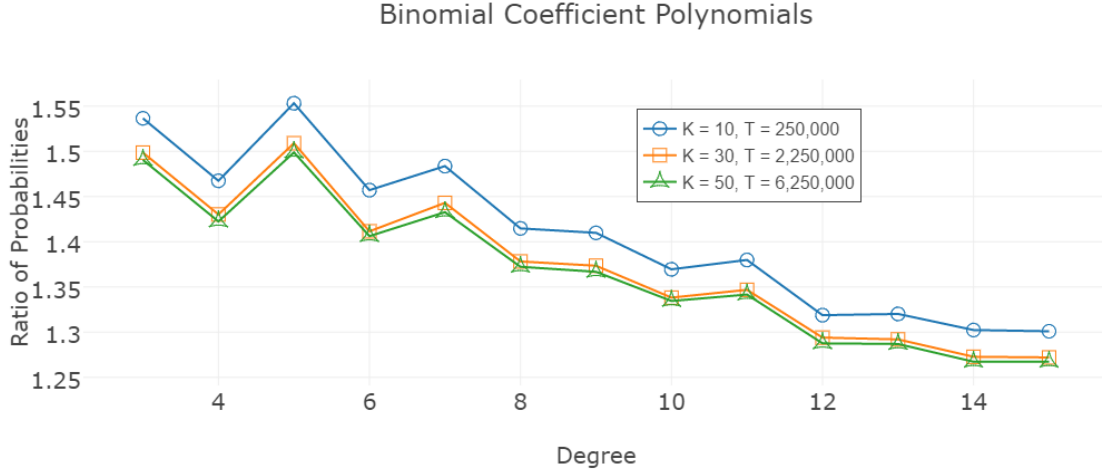


FIGURE 8. Let $h_{\text{Bin},K,d}(x)$ be a monic random polynomial with all other coefficients chosen independently from $\{0, 1, \dots, K\}$ using a $\text{Bin}(K, 1/K)$ distribution. The plot shows the probability that $h_{\text{Bin},K}(x)$ is reducible divided by the probability that the constant coefficient is zero for degrees $d = 3$ to $d = 15$ and K equal to 10, 30, and 50. Note that the ratio appears to tend to 1 as the degree increases, supporting Heuristic 1.1 (see Conjecture 3.3). For the data points for $K = 10, 30$, and 50 , the 99.9999% confidence intervals are ± 0.0017 , ± 0.0006 and ± 0.0004 , respectively.

are dependent. Figure 9 uses a different asymptotic lower bound (see Proposition 5.4) that is similar but more accurate for small d . Based on our data we make the following conjecture, which implies the bound in (2) and also supports Heuristic 1.1.

Conjecture 4.1. *If $\chi(x)$ is the characteristic polynomial of a d by d random matrix, where each entry is $+1$ or -1 independently with probability $1/2$, then*

$$\lim_{d \rightarrow \infty} \frac{\Pr(\chi(x) \text{ is reducible})}{4 \binom{d}{2} \left(\frac{1}{2}\right)^d} = 1.$$

5. PROPOSITIONS AND PROOFS

In this section we collect lower bounds on the probability of a linear factor in given polynomial models using combinatorics. We use the notation $o(1)$ to signify a small function which tends to 0 as d tends to infinity.

Proposition 5.1. *For a random monic polynomial $g_{\{0,1\},d}(x) = x^d + a_{d-1}x^{d-1} + \dots + a_1x + 1$ where a_i is 0 or 1 independently with probability $\frac{1}{2}$, the probability that $g_{\{0,1\},d}(x)$ has a linear factor is $(1 + o(1)) \sqrt{\frac{2}{\pi d}}$.*

Proof. By a geometric series argument similar to [17, Lemma 4.1], $x + 1$ is the only possible linear factor for a polynomial $g_{\{0,1\},d}(x)$, and to have $x + 1$ as a factor, -1 must be a root. We will consider the cases of d odd and d even separately.

If d is odd, then among the random coefficients a_i , there are $\frac{d-1}{2}$ even-degree terms and $\frac{d-1}{2}$ odd-degree terms, and the number of even-degree terms with a non-zero coefficient must equal the number of odd-degree terms with a non-zero coefficient; thus, the number of polynomials with $x + 1$ as a factor is when d is even is

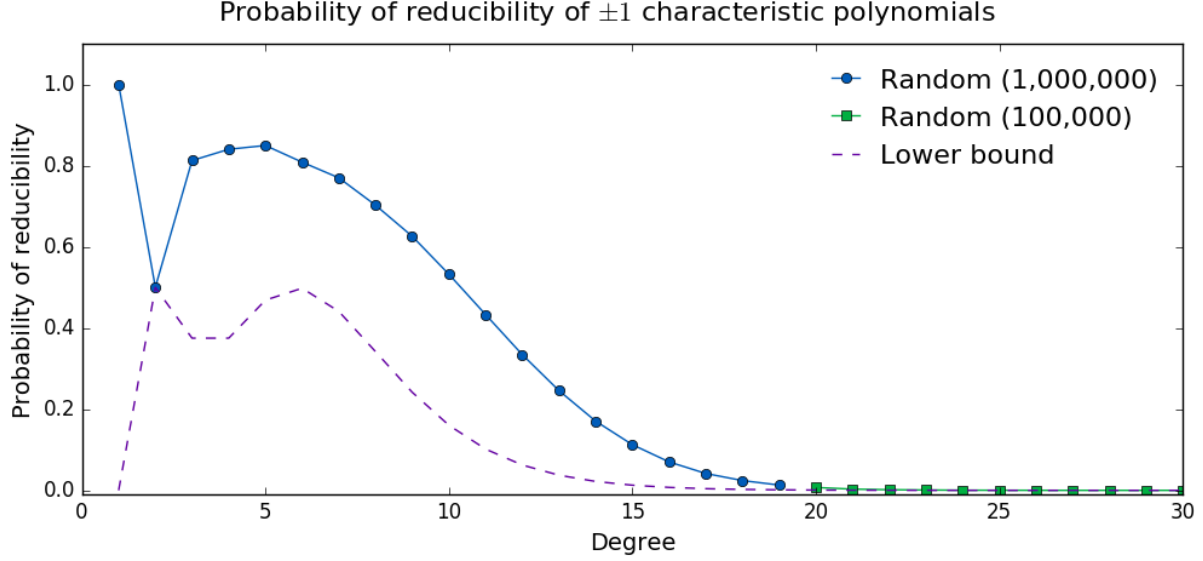


FIGURE 9. Above is a plot of the probability of reducibility for the characteristic polynomial of a random d by d matrix with entries either $+1$ or -1 independently with probability $\frac{1}{2}$. The first 19 points (circles) were calculated randomly using 1,000,000 trials, giving a 99.9999% confidence interval of ± 0.0025 for each value. The remaining points (squares) were calculated randomly using 100,000 trials, giving a 99.9999% confidence interval of ± 0.0079 . The asymptotic lower bound curve (dashed line) is from Proposition 5.4.

$$\sum_{k=0}^{\frac{d-1}{2}} \binom{\frac{d-1}{2}}{k} \binom{\frac{d-1}{2}}{k}.$$

Using Vandermonde's identity and Stirling's approximation $k! = \sqrt{2\pi k} \left(\frac{k}{e}\right)^k (1 + o(1))$, we have

$$\sum_{k=0}^{\frac{d-1}{2}} \binom{\frac{d-1}{2}}{k} \binom{\frac{d-1}{2}}{\frac{d-1}{2} - k} = \binom{d-1}{\frac{d-1}{2}} = 2^{d-1} \sqrt{\frac{2}{\pi d}} (1 + o(1)).$$

Thus, the probability of having $x+1$ as a factor is $\sqrt{\frac{2}{\pi d}} (1 + o(1))$.

When d is even, the x^d term and the constant term are both positive and thus, if k of the $\frac{d}{2} - 1$ random coefficients for even-degree terms are non-zero, then $k+2$ of the $\frac{d}{2}$ random coefficients for odd-degree terms must also be non-zero. Thus the number of polynomials with $x+1$ as a factor when d is odd is

$$\sum_{k=0}^{\frac{d}{2}-2} \binom{\frac{d}{2}}{k+2} \binom{\frac{d}{2}-1}{k} = \binom{d-1}{\frac{d}{2}-2}$$

by Vandermonde's identity. Applying Stirling's approximation we have that the probability of having $x+1$ as a factor

$$\frac{1}{2^{d-1}} \binom{d-1}{\frac{d}{2}-2} = \binom{1}{2^{d-1}} \frac{d-2}{8(d+1)} \binom{d+2}{\frac{d+2}{2}} = \frac{d-2}{d+1} \sqrt{\frac{2}{\pi(d+2)}} (1 + o(1)) = \sqrt{\frac{2}{\pi d}} (1 + o(1)),$$

completing the proof. \square

Lemma 5.2. *Consider monic polynomials of the form $g(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1x + a_0$, where a_i is 1 or -1 . The only possible linear factors over the integers of such a polynomial are $x + 1$ and $x - 1$. If d is even, $g(x)$ cannot have a linear factor. If d is odd, the number of polynomials $g(x)$ having $x - 1$ as a factor is equal to the number of polynomials $g(x)$ having $x + 1$ as a factor, which is equal to $\binom{\frac{d+1}{2}}{2}$.*

Proof. First, we prove that there cannot be a linear factor when d is even, using the fact that having a linear factor implies that there is an integer root. A geometric series argument shows (see [17, Lemma 4.1]) that for a polynomial $g(x)$, all roots must have absolute value strictly between $\frac{1}{2}$ and 2; thus 1 and -1 are the only possible integer roots for a polynomial $g(x)$. In order to have 1 or -1 as a root, the polynomial must have an equal number of positive and negative terms. When d is even, a degree d polynomial has $d + 1$ terms where $d + 1$ is odd, and thus, a linear factor is not possible.

Next, we compute the number of polynomials $g(x)$ with $x - 1$ as a factor when d is odd. Having $x - 1$ as a factor means that $g(1) = 0$. Note that $g(x)$ has $d + 1$ terms and the leading coefficient is 1, and so of the remaining d terms, there must be enough negative coefficients to sum to 0 when $x = 1$. Thus, there must be $\frac{d+1}{2}$ negative coefficients in the remaining d terms. There are $\binom{\frac{d}{2}}{2}$ ways to choose which terms will have a negative sign, so there are $\binom{\frac{d}{2}}{2}$ degree d polynomials $g(x)$ with $x - 1$ as a factor when d is odd.

Finally, we use a bijective proof to show that the number of $g(x)$ with $x - 1$ as a factor is equal to the number of $g(x)$ with $x + 1$ as a factor. Let $\tilde{g}(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1x + a_0$ where a_i is 1 or -1 such that $\tilde{g}(x)$ is a polynomial with $x = 1$ as a root. Then $g(x) = \sum_{i=0}^d (-1)^{i+1} x^i a_i$ has $x = -1$ as a root. The mapping of \tilde{g} to g is bijective, thus completing the proof. \square

Proposition 5.3. *Let d be an odd positive integer. For a random monic polynomial $g_{\pm 1, d}(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$ where each a_i is $+1$ or -1 independently with probability $1/2$, the probability that $g_{\pm 1, d}(x)$ has a linear factor is $\left(2\sqrt{\frac{2}{\pi(d+1)}} - \frac{4}{\pi(d+1)}\right)(1 + o(1))$.*

Proof. Using Lemma 5.2, we see that an upper bound for the number of polynomials with 1 or -1 as roots—double counting polynomials with both 1 and -1 as roots—is $2\binom{\frac{d+1}{2}}{2} = \binom{\frac{d+1}{2}}{2}$. We will use inclusion-exclusion to correct the double counting. If both 1 and -1 are roots, then $1 + \sum_{i=0}^{d-1} a_i = 0$ and $-1 + \sum_{i=0}^{d-1} (-1)^i a_i = 0$. Combining these two equations shows that 1 and -1 are both roots if and only if

$$\sum_{\substack{i=0, \\ i \text{ even}}}^{d-1} a_i = 0 \quad \text{and} \quad 1 + \sum_{\substack{i=0, \\ i \text{ odd}}}^{d-1} a_i = 0.$$

This implies that $\frac{d+1}{2}$ is even, so $d \equiv 3 \pmod{4}$. The number of ways to choose such $a_i \in \{+1, -1\}$ is $\binom{\frac{d+1}{2}}{\frac{d+1}{4}} \binom{\frac{d-1}{2}}{\frac{d+1}{4}} = \frac{1}{2} \binom{\frac{d+1}{2}}{\frac{d+1}{4}}^2$. By inclusion-exclusion, we thus see that the number of polynomials having $+1$ or -1 as a root (with no double counting) is

$$\binom{\frac{d+1}{2}}{\frac{d+1}{4}} - \frac{1}{2} \binom{\frac{d+1}{2}}{\frac{d+1}{4}}^2 = \left(2\sqrt{\frac{2}{\pi(d+1)}} - \frac{4}{\pi(d+1)}\right) 2^d (1 + o(1)),$$

where the second equality is from Stirling's approximation, which implies that $\binom{k}{\frac{k}{2}} = \sqrt{\frac{2}{\pi k}} 2^k (1 + o(1))$ for positive even integers k . Dividing by 2^d shows that the probability that $g_{\pm 1, d}(x)$ has a linear factor is $\left(2\sqrt{\frac{2}{\pi(d+1)}} - \frac{4}{\pi(d+1)}\right) (1 + o(1))$. \square

We end the section with a proposition and proof giving an asymptotic lower bound on the probability that the characteristic polynomial of a d by d matrix with $+1$ and -1 entries is reducible. Note that one could use [1, Theorem 2.1] to find a similar lower bound that holds for all d ; the bound below highlights the terms that are relevant for small d and is asymptotically accurate for large d .

Proposition 5.4. *For a characteristic polynomial $\chi(x)$ of a d by d matrix whose entries are $+1$ or -1 independently with probability $\frac{1}{2}$, the probability of reducibility is at least*

$$4\binom{d}{2} \left(\frac{1}{2}\right)^d - 2\binom{d}{2}^2 \left(\frac{1}{2}\right)^d \left(\frac{1}{2}\right)^{d-2} - o(1/2^d).$$

Proof. The determinant of a matrix is the constant coefficient of its characteristic polynomial, and, if the determinant is 0, then $\chi(x)$ has 0 for a root. The above asymptotic lower bound on the probability of reducibility comes from an asymptotic lower bound on the probability the matrix has a determinant 0. The first term is the asymptotic probability of 2 rows of the matrix being linearly dependent or 2 columns being dependent, double counting when both events occur (note that an additional factor of two appears because there are two ways for vectors with all entries in $\{+1, -1\}$ to be dependent). The second term is the asymptotic probability of 2 rows and 2 columns being dependent at the same time. Using inclusion-exclusion, we subtract these terms to avoid double counting. The $o(1/2^d)$ accounts for lower-order terms, for example the probability that two or more distinct pairs of rows each have a dependency. Note we have included the a second-order term even though it is smaller than the error because it makes the bound more accurate for small d . \square

6. ACKNOWLEDGEMENTS

We thank Steve Goldstein for his support and guidance in programming and collecting data, and we thank the HTCondor system [14, 21, 24] at the University of Wisconsin-Madison for making our computations possible. We also thank the Simons Foundation for providing licenses for Magma, the primary computer algebra system used for this project.

REFERENCES

1. R. Arratia and S. DeSalvo, On the singularity of random Bernoulli matrices—novel integer partitions and lower bound expansions, *Ann. Comb.* **17** (2013), no. 2, 251–274.
2. L. Bary-Soroker and G. Kozma, Is a bivariate polynomial with ± 1 coefficients irreducible? Very likely!, *Int. J. Number Theory* **13** (2017), no. 4, 933–936.
3. J. Bourgain, V. H. Vu, P. M. Wood, On the singularity probability of discrete random matrices, *Journal of Functional Analysis*, Volume 258, Issue 2 (2010), 559–603.
4. R. Chela, Reducible Polynomials, *J. London Math. Soc.* **38** (1963), 183–188.
5. R. Dietmann, Probabilistic Galois theory, *Bull. Lond. Math. Soc.* **45** (2013), no. 3, 453–462.
6. P. X. Gallagher, The large sieve and probabilistic Galois theory, in *Analytic number theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972)*, 91–101, Amer. Math. Soc., Providence, RI.
7. A. Gorodnik, A. Nevo, Splitting fields of elements in arithmetic groups, *Math. Res. Lett.* **18** (2011), no. 6, 1281–1288.
8. J. Kahn, J. Komlós and E. Szemerédi, On the probability that a random ± 1 -matrix is singular, *J. Amer. Math. Soc.* **8** (1995), no. 1, 223–240.
9. J. Komlós, On the determinant of $(0, 1)$ matrices, *Studia Sci. Math. Hungar* **2** (1967), 7–21.
10. H.-W. Knobloch, Zum Hilbertschen Irreduzibilitätssatz, *Abh. Math. Sem. Univ. Hamburg* **19** (1955), 176–190.
11. H.-W. Knobloch, Die Seltenheit der reduziblen Polynome, *Jber. Deutsch. Math. Verein.* **59** (1956), Abt. 1, 12–19.

12. S. V. Konyagin, On the number of Irreducible Polynomials with 0,1, Coefficients, *Acta Arith.* **88** (1999), no. 4, 333-350.
13. G. Kuba, On the Distribution of Reducible Polynomials, *Mathematica Slovaca*, **59** (2009), No. 3, 349-356
14. M. Litzkow, Remote Unix - Turning Idle Workstations into Cycle Servers, *Proceedings of Usenix Summer Conference*, pages 381-384, 1987.
15. P. Moree, Artin's primitive root conjecture—a survey, *Integers* **12** (2012), no. 6, 1305–1416.
16. A.M. Odlyzko, B. Poonen, Zeros of Polynomials with 0,1 Coefficients, *L'Enseignement Mathématique* **39**, (1993), 317-348.
17. S. O'Rourke, P. M. Wood, Low-degree Factors of Random Polynomials, arXiv preprint arXiv:1608.01938 (2016).
18. Peled, R.; Sen, A.; Zeitouni, O. Double roots of random Littlewood polynomials. *Israel J. Math.* **213** (2016), no. 1, 55–77.
19. I. Rivin, Galois Groups of Generic Polynomials, available at arXiv:1511.06446, 19 Nov 2015.
20. I. Rivin, Walks on groups, counting reducible matrices, polynomials, and surface and free group automorphisms, *Duke Math. J.* **142** (2008), no. 2, 353-379.
21. T. Tannenbaum, D. Wright, K. Miller, M. Livny, Condor - A Distributed Job Scheduler, in Thomas Sterling, editor, *Beowulf Cluster Computing with Linux*, The MIT Press, 2002.
22. T. Tao and V. Vu, On random ± 1 matrices: singularity and determinant, *Random Structures Algorithms* **28** (2006), no. 1, 1–23.
23. T. Tao and V. Vu, On the singularity probability of random Bernoulli matrices, *J. Amer. Math. Soc.* **20** (2007), no. 3, 603–628.
24. D. Thain, T Tannenbaum, M. Livny, Distributed Computing Practice: The Condor Experience, *Concurrency and Computation: Practice and Experience*, **Vol. 17** (2005), No. 2-4, pages 323-356.
25. B. L. van der Waerden, Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt, *Monatsh. Math. Phys.* **43** (1936), no. 1, 133-147.
26. D. Zywin, Hilberts irreducibility theorem and the larger sieve, available at arXiv:1011.6465, 30 Nov 2010.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF WISCONSIN - MADISON, MADISON, WISCONSIN 53706

E-mail address: enboyd@wisc.edu

E-mail address: sgsolberg@wisc.edu

E-mail address: cborst@wisc.edu

E-mail address: cbrekken@wisc.edu

E-mail address: mmwood@math.wisc.edu

E-mail address: pmwood@math.wisc.edu