Irreducibility and Galois Groups of Random Polynomials

Hanson Hao, Eli Navarro, Henri Stern

Abstract

Let $f(x)$ be a random integral polynomial of degree $d \geq 2$ with coefficients uniformly and independently drawn from $[-N, N]$. It is well known that the probability that $f(x)$ is irreducible over the integers with Galois group S_d tends to 1 as $N \to \infty$. However, finding more precise estimations for these probabilities is still an active area of research. In this paper, we survey the classic work on this problem as well as a recent method introduced by Rivin. Additionally, we discuss the precision of Rivin's argument for special classes of polynomials and end by investigating a toy case of cubic trinomials.

Contents

1 Introduction

Suppose $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1x + a_0$ is a random integral polynomial. If we further suppose that the integral coefficients a_i are chosen uniformly and independently at random from $[-N, N]$, some questions arise: What is the probability that $f(x)$ is reducible over the integers? What is the Galois group of $f(x)$ over the rational numbers?

Questions of this sort date back to at least the 1930's [17]. In this paper we provide a survey of known results and methods in the study of random integral polynomials, specifically in the Large Box Model where $N \to \infty$ and the degree d is fixed. The two properties of random integral polynomials that we are concerned with are reducibility over the integers and their Galois groups over the rationals.

1.1 Large Box Model

The Large Box Model is the primary model we investigate.

Definition 1.1. *In the **Large Box Model**, the degree d of the random polynomials is fixed, and the integral coefficients a_i are chosen independently and uniformly at random from the **support** $[-N, N]$ as $N \to \infty$.*

The model was introduced by B.L. van der Waerden in the 1930's. In a 1936 paper [17], van der Waerden proved that the probability that a random integral polynomial in the Large Box Model is irreducible over $\mathbb{Z}$ tends to 1 as $N \to \infty$. This also proved a formulation of Hilbert's Irreducibility Theorem [4]. A proof of van der Waerden's result on irreducibility is the subject of Section 2. van der Waerden also proved the following:

Theorem 1.2. *(van der Waerden, 1936) For a random polynomial $f(x)$ in the Large Box Model:*

$$\Pr(\mathrm{Gal}(f(x)) = S_d) \geq 1 - O(N^{-1/6}).$$

In that same paper, van der Waerden conjectured that the error term could be generalized to $O(N^{-1+\epsilon})$ for any $\epsilon > 0$. S. Chow and R. Dietmann [7] proved van der Waerden's conjecture for random polynomials of degrees 3 and 4 in a 2018 paper.

In a 1963 paper, R. Chela [6] built upon van der Waerden's results on irreducibility to show that the probability of irreducibility has tight bound $(1 + o(1))c_d/N$ as $N \to \infty$, where c_d is some constant depending on d only. This paper's results and proofs are the subject of Section 3. Chela's proof is built on the observation that random polynomials with linear factors make up a plurality of reducible polynomials; this is shown by van der Waerden's theorem in Section 2. Chela utilizes elementary counting and geometric methods to prove a series of lemmas leading to the final result.

In 2015, I. Rivin [13] uploaded a paper that provided a new method for calculating the probability of reducibility for random polynomials. This method

and its applications are one of the main topics of this survey, and it is discussed in sections 4, 5, and 6. Central to this method is the use of a Schwartz-Zippel type bound which bounds the size of an algebraic variety over a finite field by some power of the size of the field. The resulting probability is actually less precise than that given by Chela, but Rivin's method is more streamlined and more broadly applicable. More importantly, using some results from the classification of finite simple groups, Rivin applies his method to give a necessary and sufficient condition for a random polynomial to have Galois group S_d or A_d over the rationals.

1.2 Bounded Height Model

The Bounded Height Model is an alternative to the Large Box Model for researching properties of random integral polynomials. While we do not focus on the Bounded Height Model in this paper, we include some interesting results from the model in this subsection.

Definition 1.3. *In the **Bounded Height Model**, the degree d of the random polynomials goes to infinity, and the integral coefficients a_i are chosen independently and uniformly at random from a support of fixed size.*

The dominant paradigm in the Large Box Model, as depicted in Chela and Rivin's papers, treats polynomials of degree d as elements of $\mathbb{R}^d$. In the Bounded Height Model however, $d \to \infty$. Consequently, this paradigm is generally not applicable to the Bounded Height Model. Proofs in the Bounded Height Model generally rely on group theory, the theory of random walks, and analytic number theory.

In 1993, A.M. Odlyzko and B. Poonen [11] conjectured that in certain versions of the Bounded Height Model, irreducibility of polynomials becomes certain as the degree goes to infinity.

Conjecture 1.4. *(Odlyzko and Poonen, 1993) Let d be a positive integer. For random monic polynomials $g_{0,1,d}(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$, where the a_i are 0 or 1 independently with probability 1/2, the probability that $g_{0,1,d}(x)$ is reducible goes to 0 as the degree d goes to infinity.*

The following result, due to E. Breuillard and P. Varjú [5], confirms Odlyzko and Poonen's conjecture, conditional on the Riemann Hypothesis holding for certain number fields.

Theorem 1.5. *(Breuillard and Varjú, 2019) Let $f(x)$ be a random monic polynomial of degree d with coefficients 0,1. Suppose the Riemann hypothesis holds for the Dedekind zeta function ζ_K for all number fields $K = \mathbb{Q}(a)$, where a is the root of a polynomial with 0,1 coefficients. Then:*

$$\Pr(f(x) \text{ irreducible in } \mathbb{Z}[x]) \to 1 \quad \text{as } d \to \infty.$$

In a 1999 paper, S.V. Konyagin [9] conjectured that in the case that a random polynomial in this model is reducible, it almost certainly has a linear factor $(x+1)$.

Conjecture 1.6. *(Konyagin, 1999) Let d be a positive integer. For random monic polynomials $g_{0,1,d}(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$, where the a_i are 0 or 1 independently with probability 1/2, the probability that $g_{0,1,d}(x)$ has a linear factor $x+1$ conditioned on $g_{0,1,d}(x)$ being reducible, goes to 1 as d goes to infinity.*

Another result given by L. Bary-Soroker, D. Koukoulopoulos, and G. Kozma [1], is weaker than Theorem 1.5, but not conditional on any form of the Riemann Hypothesis.

Theorem 1.7. *(Bary-Soroker, et al., 2020) Let $\Upsilon_H(n)$ denote the set of monic polynomials of degree n, all of whose coefficients lie in $[1, H]$. Then there are absolute constants $c > 0$ and $n_0 \geq 1$ such that if $H \geq 35$, $n \geq n_0$, and we choose a polynomial from $\Upsilon_H(n)$ uniformly at random, then it is irreducible with probability $\geq 1 - n^{-c}$.*

1.3 Outline

In Section 2, we present van der Waerden's result on irreducibility and its proof. In Section 3, we provide Chela's 1963 results and the necessary proofs by building upon van der Waerden's results. In Section 4, we introduce Rivin's method for finding the probability of reducibility for random polynomials, which makes use of some results from algebraic geometry. In Section 5, we show how Rivin utilizes his method in order to give a necessary and sufficient condition for a random polynomial to have Galois group S_d or A_d. Section 6 discusses the applicability and limitations of Rivin's method on reducibility for the special case of random monic trinomials, and Section 7 investigates the distribution of Galois groups in the restricted case of cubic trinomials.

1.4 Notation

We adopt the Vinogradov asymptotic notation $X \ll_d Y$ which denotes that there exists a constant C_d dependent only on the parameter d such that $|X| \leq C_d Y$.

2 van der Waerden's Results on Irreducibility

In his 1936 paper, van der Waerden [17] showed that the number of random polynomials reducible over the integers with factors of any degree are comparable in size to a power of the bound of the support.

Definition 2.1. *Let $\rho_k(d, N)$ be the number of reducible random polynomials of degree d, support $[-N, N]$, with factor of lowest degree $1 \leq k \leq d/2$. Let $\rho(d, N)$ be the number of all such reducible polynomials with factors of any degree.*

Theorem 2.2. *(van der Waerden, 1936)*

$$\rho_k(d,N) \ll_d N^{d-k} \quad \text{if } d > 2k,$$
$$\rho_k(d,N) \ll_d N^{d-k}\log N \quad \text{if } d = 2k.$$

Proving this result requires two distinct notions of the size of a polynomial: the height and the Mahler measure.

Definition 2.3. *The **height** of a polynomial $f(x) = a_d x^d + a_{d-1}x^{d-1} + \dots a_1 x + a_0$, denoted by $H(f)$, is defined as:*

$$H(f) := \max_i |a_i|.$$

Definition 2.4. *If $f(x)$ is a polynomial that factors over $\mathbb{C}$ as*

$$f(x) = a(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_d),$$

*then the **Mahler measure** of $f(x)$, denoted by $M(f)$, is defined as:*

$$M(f) := |a| \prod_{|\alpha_i|\geq 1} |\alpha_i|.$$

Example 2.5. *The polynomial $f(x) = x^3 + 2x^2 - 9x - 18 = (x+3)(x-3)(x+2)$ has Mahler measure*

$$M(f) = |a| \prod_{|\alpha_i|\geq 1} |\alpha_i| = 3 \cdot 3 \cdot 2 = 18.$$

It is immediate from the definition of the Mahler measure that it is multiplicative [3], i.e. for a polynomial $f(x) = g(x)h(x)$, the equality $M(f) = M(g)M(h)$ holds. This property, along with the following lemma relating the Mahler measure of a polynomial to its height, form the foundation of van der Waerden's results.

Lemma 2.6. *Let $f(x)$ be a polynomial of degree d. Then:*

$$\binom{d}{\lfloor d/2 \rfloor}^{-1} H(f) \leq M(f) \leq H(f)\sqrt{d+1}.$$

Proof. See [10]. □

We now have the tools and background to prove Theorem 2.2. The proof consists of calculating all possible factorizations of a random polynomial with a degree k factor, and then using the height and Mahler measure to bound this number above by N.

Proof of Theorem 2.2. Let $f(x)$ be a monic polynomial of degree d with support $[-N, N]$. Suppose that:

$$f(x) = g(x)h(x),$$

where $g(x)$ and $h(x)$ are monic integer polynomials. Suppose further that $\deg(g) = k$, where $1 \leq k \leq d/2$. Let b, c denote the heights of $g(x)$ and $h(x)$ respectively. The following inequality results from the multiplicativity of the Mahler measure and Lemma 2.6:

$$bc := H(g)H(h) \ll_d M(g)M(h) = M(f) \ll_d H(f) \leq N. \tag{2.1}$$

We now need to calculate all the possible arrangements of coefficients for the polynomials $g(x)$ and $h(x)$. Fix b. The height b of $g(x) = x^k + b_{k-1}x^{k-1} + \cdots + b_1x + b_0$ can occur at k possible terms, and the corresponding coefficient can either be b or $-b$. The other $k-1$ terms each have one of $2b+1$ possible values. The $d-k$ non-leading terms of $h(x)$ each have one of $2c+1$ possible values. Multiplying all these factors together gives all the possible factorizations of $f(x)$ for a fixed b and c. The number of such possible factorizations is thus $2k(2b+1)^{k-1}(2c+1)^{d-k}$. This quantity can be related to N by the following series of inequalities:

$$2k(2b+1)^{k-1}(2c+1)^{d-k} \ll_{k,d} b^{k-1}c^{d-k} \ll_d b^{k-1}c^{d-k} \ll_d b^{k-1}\left(\frac{N}{b}\right)^{d-k},$$

where the first inequality comes from expanding out $(2b+1)$ and $(2c+1)$, the second inequality comes from the observation that k is bounded above by d and accordingly omitting the dependence on k, and the final inequality is a result of (2.1). Summing across all possible values of b yields:

$$\rho_k(d,N) \ll_d 2\sum_{b=1}^{N} b^{k-1}(\frac{N}{b})^{d-k} = 2N^{d-k}\sum_{b=1}^{N}\frac{1}{b^{d-2k+1}} \ll_d N^{d-k}.$$

Note the case $b = 0$ is not included since we are considering only monic polynomials, and the factor of 2 is to account for both positive and negative values of b. In the case that $d = 2k$, the approximation $\sum_{b=1}^{N}\frac{1}{b^{d-2k+1}} = \sum_{b=1}^{N}\frac{1}{b} \approx \log N$ holds. The result is that:

$$\rho_k(d,N) \ll_d 2N^{d-k}\sum_{b=1}^{N}\frac{1}{b} \ll_d N^{d-k}\log N,$$

completing the proof. □

3 Chela's Results

In 1963, R. Chela released a paper building upon van der Waerden's results [6]. Where van der Waerden's work gave only an upper and lower bound for the number of reducible random polynomials, Chela's paper explicitly lays out a limit that gives the probability that a random polynomial is reducible as its support grows to infinity. To do this, Chela utilizes a corollary of van der Waerden's inequality which roughly states that the plurality of reducible polynomials

have linear factors. Chela's argument flows by illustrating a counting method for polynomials with linear factors and then proving that this count suffices to arrive at a limit for the probability that a polynomial is reducible.

Although Chela's results can easily be thought of as a probability, they are in fact given as a limit as follows:

Theorem 3.1. *For degree $d > 2$,*

$$\lim_{N\to\infty} \frac{\rho(d,N)}{N^{d-1}} = 2^d \left(\zeta(d-1) - \frac{1}{2} + \frac{k_d}{2^{d-1}}\right),$$

where ζ is the Riemann zeta function.

Here, k_d is defined as an hypervolume in $d-1$ dimensional Euclidean space. We let

$$k_d = \int_{(R)} \cdots \int dx_1 \dots dx_{d-1},$$

where $\{x_1, \dots, x_{d-1}\}$ are the coordinates of $\mathbb{R}^{d-1}$ and (R) is the region defined by

$$|x_1| \leq 1,\ i = 1, \dots, d-1,\ \left|\sum_{i=1}^{d-1} x_i\right| \leq 1.$$

We note that as n tends to infinity, $\zeta(n)$ tends to 1. However, $\zeta(1)$ is undefined, which is why Theorem 3.1 applies only when $d > 2$. A discussion of the limit when $d = 2$ will be presented at the end of this section.

To arrive at a proof of Theorem 3.1, several lemmas are required. Essentially we will illustrate a method to count (up to some error) the number of polynomials which are reducible with a linear factor, then, we will prove that this count suffices to give a robust approximation of the total number of reducible polynomials. Then, because we are dealing with independently and uniformly chosen random variables where each outcome is equally likely, we will have enough information to render a probability that a given polynomial is reducible as the support goes to infinity.

Before outlining the necessary lemmas, we need to define two related, but distinct, counting architectures.

We define $T_{d,N}(v)$ as the number of random polynomials with support N and $(x + v)$ as a factor, where v is an integer.

We define $\bar{\rho}_1(d, N)$ as the number of such polynomials with at least two, not necessarily distinct, linear factors.

Note that $\sum_v T_{d,N}(v)$ is similar to $\rho_1(d, N)$, but the sum is not equal because it allows for double counting of polynomials with multiple distinct linear factors. However, the two quantities are related as follows:

Lemma 3.2. *Summing over all $v \in [-N, N]$, we have:*

$$\rho_1(d,N) = \sum_v T_{d,N}(v) + o(N^{d-1})$$

Proof. As mentioned above, we have $\sum_v T_{d,N}(v) \geq \rho_1(d,N)$ due to possible double counting. Let R_i for $i = 1, \ldots, d$ be the number of polynomials with i distinct linear factors. We then have that $\sum_v T_{d,N}(v) = R_1 + \sum_{i=2}^{d} iR_i$. Additionally, for $i > 1$, we have

$$R_i \leq \bar{\rho}_1(d,N) < \rho_2(d,N) = o(N^{d-1}).$$

Since i is at least 2, every polynomial counted in R_i is also counted in $\bar{\rho}_1(n,N)$, which gives the first inequality. The second inequality comes from the fact that $\rho_2(d,N)$ counts polynomials with irreducible quadratic factors which $\bar{\rho}_1(d,N)$ does not. The final equality comes directly from van der Waerden's results. Note that $R_1 \leq \rho_1(d,N)$, and when we combine this we have

$$\begin{aligned}\sum_v T_{d,N}(v) - \rho_1(d,N) &= R_1 + \sum_{i=2}^{d} iR_i - \rho_1(d,N) \\ &\leq \sum_{i=2}^{d} iR_i \\ &= o(N^{d-1}).\end{aligned}$$

□

We have now related $\sum_v T_{d,N}(v)$ and $\rho_1(d,N)$. Next, we must quantify $\sum_v T_{d,N}(v)$.

Lemma 3.3. *For $d > 2$ and $1 < |v| \leq N$,*

$$\lim_{N\to\infty} \frac{\sum_{|v|>1} T_{d,N}(v)}{N^{d-1}} = 2^d(\zeta(d-1) - 1).$$

Proof. We see that if v is a root of $f(x)$, then $-v$ must be a root of $f(-x)$. As such, $T_{d,N}(v) = T_{d,N}(-v)$ and we can assume that $2 \leq v \leq N$. To arrive at this count for the number of polynomials that are reducible with a given linear factor $(x+v)$, we will appeal to constraints on the coefficients of the degree $d-1$ factor of the polynomial. To this end, we have

$$\begin{aligned}f(x) &= x^d + a_{d-1}x^{d-1} + \cdots + a_0 \\ &= (x+v)(x^{d-1} + b_{d-2}x^{d-2} + \cdots + b_0).\end{aligned}$$

Seen this way, we can define $T_{d,N}(v)$ as the number of valid $(d-1)$-tuples $(b_{d-2}, \ldots, b_0)$ (with "valid" meaning that the $(d-1)$-tuples produce polynomials $f(x)$ whose coefficients remains within the constraint of the support $[-N, N]$). From here, we have a set of relationships between the a_i coefficients and the b_i coefficients. In particular, $a_{d-1} = b_{d-2} + v$, $vb_0 = a_0$, and

$$b_i = \frac{a_i - b_{i-1}}{v},\ 0 \leq i \leq d-2,\ (b_{d-1} = 0).$$

To count the possible $(d-1)$-tuples, we note that for a fixed b_{i-1}, we have $a_i \in [-N, N]$ and can therefore conclude that b_i must lie within the range

$$\left[\frac{-N - b_{i-1}}{v}, \frac{N - b_{i-1}}{v}\right].$$

Note that the amplitude of this range is $\frac{2N}{v}$ which is independent of b_{i-1}. This implies that, for a given b_{i-1}, there are either $\frac{2N}{v}$ or $\frac{2N}{v}+1$ integer values of b_i. Thus, the number of solutions the set of relations on a_i and b_i given above is

$$\prod_{i=1}^{d-1}\left(\frac{2N}{v} + r_{vi}\right), \ (|r_{vi}| \leq 1).$$

We take this product from $i = 1$ to $i = d-1$ because we have $d-1$ coefficients b_i with which we are concerned. Before continuing, it is important to note that $b_i \in [\frac{-N-b_{i-1}}{v}, \frac{N-b_{i-1}}{v}]$ is not *a priori* enough to satisfy $a_{d-1} = b_{d-2} + v$. However, we have the following inequality:

$$|b_{d-2}| \leq N\left(\frac{1}{v} + \frac{1}{v^2} + \cdots + \frac{1}{v^{d-1}}\right).$$

This follows from the fact that $|b_0| = |\frac{a_0}{v}| \leq \frac{N}{v}$ and

$$|b_1| = \left|\frac{a_1 - b_0}{v}\right| = \frac{|a_1 - b_0|}{v} = \frac{|a_1| + |b_0|}{v} \leq \frac{N + \frac{N}{v}}{v} = \frac{N}{v} + \frac{N}{v^2}.$$

Then, the inequality stated above follows by induction. From here, we have that if $v < N$,

$$\begin{aligned} |b_{d-2} + v| &\leq |b_{d-2}| + v \\ &\leq N\left(\frac{1}{v} + \cdots + \frac{1}{v^{d-2}}\right) + v \\ &< N\left(\frac{1}{v-1}\right) + v. \end{aligned}$$

If v is not 2 or $N-1$, this holds if N is large enough. If $v = 2$, note that because $(\frac{1}{v} + \ldots + \frac{1}{v^{n-1}}) < 1$, for large enough N we have that $N(\frac{1}{v} + \ldots + \frac{1}{v^{n-1}}) < N-2$. If $v = N-1$, then we see that $|b_{d-2} + v| < \frac{N}{N-2} + N - 1 = N + \frac{2}{N-2}$. But this value must be an integer, so $|b_{d-2} + v| \leq N$. This guarantees that, for large enough N, we have that $|b_{d-2} + v| \leq N$ which is necessary for $a_{d-1} = b_{d-2} + v$ to be satisfied. With all this information, we can then sum over all possible values of v and arrive at

$$\sum_{2 \leq v \leq N} T_{d,N}(v) = \sum_{v=2}^{N-1}\prod_{i=1}^{d-1}\left(\frac{2N}{v} + r_{vi}\right) + T_{d,N}(N).$$

Then, as we remarked above, we have $T_{d,N}(v) = T_{d,N}(-v)$, so

$$\sum_{|v|\geq 1} T_{d,N}(v) = 2\sum_{v=2}^{N-1}\prod_{i=1}^{d-1}\left(\frac{2N}{v} + r_{vi}\right) + 2T_{d,N}(N).$$

In order to simplify this equation into the desired form, we note that r_{vi} is either 0 or 1. This way, the product can be expressed as $(\frac{2N}{v})^{d-1} + O(N^{d-2})$. We also have that $T_{d,N}(N)$ is $o(N^{d-1})$ since this is the number of ways of choosing the $d-1$ values of b_i even without the restrictions discussed above. With all of this information together, we have

$$\begin{aligned}
\sum_{|v|\geq 1} T_{d,N}(v) &= 2\sum_{v=2}^{N-1}\left(\frac{2N}{v}\right)^{d-1} + o(N^{d-1}) \\
\Rightarrow \frac{\sum_{|v|\geq 1} T_{d,N}(v)}{N^{d-1}} &= 2^d \sum_{v=2}^{N-1}\left(\frac{1}{v^{d-1}}\right) + \frac{o(N^{d-1})}{N^{d-1}} \\
\Rightarrow \lim_{N\to\infty} \frac{\sum_{|v|\geq 1} T_{d,N}(v)}{N^{d-1}} &= 2^d \sum_{v=2}^{\infty}\frac{1}{v^{d-1}} \\
&= 2^d\left(\sum_{v=1}^{\infty}\frac{1}{v^{d-1}} - 1\right) \\
&= 2^d\left(\zeta(d-1) - 1\right),
\end{aligned}$$

thus completing the proof of the lemma. □

Before continuing to the third and final lemma, we need to define two more tools. First, we let

$$t(f(x)) = a_{d-1} + \cdots + a_0.$$

In other words, $t(f(x))$ represents the sum of all the coefficients of $f(x)$ except the coefficient of the leading term. Second, $L_d(N,h)$ is the number of polynomials $f(x)$ such that $t(f(x)) = h$. Note that $L_d(N,h) = L_d(N,-h)$ because we have that $t(f(x)) = -t(f(-x))$. Additionally, we have that $T_{d,N}(-1) = L_d(N,-1)$. This follows from the fact that a polynomial with root 1 must have all its coefficients sum to 0, and since $L_d(N,h)$ ignores the leading coefficient (which is 1 since all polynomials we are considering are monic), we arrive at $T_{d,N}(-1) = L_d(N,-1)$. Lemma 3.3 counted polynomials with linear factors $(x-v)$ where $|v|$ was greater than 1. We can now use the relationship $T_{d,N}(-1) = L_d(N,-1)$ and the following lemma to count polynomials with linear factors $(x-v)$ where $|v| = 1$.

Lemma 3.4.

$$\lim_{N\to\infty}\frac{L_d(N,h)}{N^{d-1}} = k_d.$$

Proof. First, we can assume h to be positive since $L_d(N,h) = L_d(N,-h)$. To prove this lemma, we will start by showing that for all h,

$$\lim_{N\to\infty} \frac{L_d(N,h)}{L_d(N,0)} = 1.$$

To prove this, we will require the assumption that $\lim_{N\to\infty} \frac{L_d(N,0)}{N^{d-1}} = k_n$. The assumption will be proved later.

Let $\mathcal{L}_d(N,h)$ be the *set* of polynomials such that $t(f(x)) = h$. Take some $f(x) \in \mathcal{L}_d(N,0)$ and then let $f'(x) = x^d + a'_{d-1}x^{d-1} + \cdots + a'_1 x + a'_0$ where $a'_{d-1} = a_{d-1}, \ldots, a'_1 = a_1$, and $a'_0 = a_0 + h$. This implies that $f'(x) \in \mathcal{L}_d(N+h,h)$. From the natural mapping $f(x) \to f'(x)$, we have an injective map

$$\mathcal{L}_d(N,0) \to \mathcal{L}_d(N+h,h).$$

Since this map is injective, we can comment on the relative sizes of the sets in question. Specifically, we have

$$L_d(N,0) \le L_d(N+h,h).$$

We can make a nearly identical argument with $f(x) \in L_d(N,h)$ and $f'(x)$ defined as $a'_{d-1} = a_{d-1}, \ldots, a'_1 = a_1, a'_0 = a_0 - h$, and we can conclude that

$$L_d(N,h) \le L_d(N+h,0).$$

Then, if we replace N with $N-h$ in $L_d(N,0) \le L_d(N+h,h)$ we are left with $L_d(N-h,0) \le L_d(N,h)$. Now we have two relations for $L_d(N,h)$, and we can express them as follows

$$\frac{L_d(N-h,0)}{L_d(N,0)} \le \frac{L_d(N,h)}{L_d(N,0)} \le \frac{L_d(N+h,0)}{L_d(N,0)}.$$

Observe that

$$\begin{aligned}
\lim_{N\to\infty} \frac{L_d(N-h,0)}{L_d(N,0)} &= \lim_{N\to\infty} \left(\frac{L_d(N-h,0)}{L_d(N,0)} \cdot \frac{N^{d-1}}{(N-h)^{d-1}} \right) \\
&= \lim_{N\to\infty} \frac{\frac{L_d(N-h,0)}{(N-h)^{d-1}}}{\frac{L_d(N,0)}{N^{d-1}}} \\
&= \frac{k_d}{k_d} = 1.
\end{aligned}$$

Here, we used the assumption $\lim_{N\to\infty} \frac{L_d(N,0)}{N^{d-1}} = k_n$ outlined at the beginning of the proof. We can then use an identical process as above, simply replacing $N-h$ with $N+h$, and we will arrive at the same result. By the squeeze theorem, we can conclude that for all h,

$$\lim_{N\to\infty} \frac{L_d(N,h)}{L_d(N,0)} = 1.$$

We must now prove our assumption. While all of our methodology thus far has been algebraic and combinatoric in nature, we will need a geometric appeal in order to prove that $\lim_{N\to\infty} \frac{L_d(N,0)}{N^{d-1}} = k_n$. We must define several geometric objects. Let E_d be $d-$dimensional Euclidean space with coordinates $x_1, \ldots, x_d$, and let Λ_d be the lattice of integer points of E_d. Given a region $S \subset E_d$, we take $||S||$ to denote the number of points in $S \cap \Lambda_d$, and $V(S)$ to denote the volume of S.

We can now create a geometric object such that the number of lattice points contained in that object is equal to $L_d(N, 0)$. We take C_d to be the hypercube defined by $\{(x_1, \ldots, x_d) \in E_d : |x_i| \leq N\}$ and H to be the plane given by $x_1 + \cdots + x_d = 0$. In other words, C_d represents all possible $d-$tuples of coefficients lying within the support $[-N, N]$ and H represents those $d-$tuples of coefficients such that $t(f(x)) = 0$. So, together we have

$$L_d(N, 0) = ||C_d \cap H||.$$

To make this problem easier to solve, we will reduce complexity by one degree. Note that H is already a $(d-1)-$dimensional space, so $C_d \cap H$ is also $(d-1)-$dimensional. Take $C_d \cap H$ to be given by $|x_i| \leq N$, $i \in (1, \ldots, d-1)$, and $|\sum_{i=1}^{d-1} x_i| \leq N$. This expression of $C_d \cap H$ is given by a collection of $(d-1)$-tuples, such that the height of the tuple is less than or equal to N so is the sum. This $(d-1)-$dimensional definition is equivalent to the previously given $d-$dimensional definition, because given $d-1$ points whose sum is less than or equal to N, there exists a unique point in C_d such that the inclusion of this as the d^{th} point of the sum would make the sum 0.

Finally, we use the fact, which can be found in Chapter 3 of *Computing the continuous discretely* by Beck and Robins [2], that

$$\lim_{N\to\infty} \frac{||C_d \cap H||}{N^{d-1}} = V(R_1),$$

where R_1 is the scaling of $C_d \cap H$ by a factor of $1/N$ as follows:

$$R_1 := |y_i| \leq 1,\ i \in (1, \ldots, d-1),\ \left|\sum_{i=1}^{d-1} x_i\right| \leq 1.$$

Here, $V(R_1)$ is identical to the definition of k_d given at the beginning of this section. So we may conclude that

$$\lim_{N\to\infty} \frac{L_d(N,h)}{N^{d-1}} = \lim_{N\to\infty} \frac{L_d(N,0)}{N^{d-1}} = \lim_{N\to\infty} \frac{||C_d \cap H||}{N^{d-1}} = V(R_1) = k_d.$$

□

Then, as we stated before, because we have $T_{d,N}(1) = L_d(N, -1)$, a corollary of Lemma 3.4 is

$$\lim_{N\to\infty} \frac{T_{d,N}(1)}{N^{d-1}} = k_d.$$

We may now combine the results of our three lemmas to arrive at a proof of Theorem 3.1. Observe that

$$\sum_v T_{d,N}(v) = \sum_{|v|>1} T_{d,N}(v) + 2T_{d,N}(1) + T_{d,N}(0).$$

We see that $T_{d,N}(0)$ is just the number of polynomials where the constant coefficient is 0. This number is approximately $2^{d-1}N^{d-1}$. Using this fact, Lemma 3.3, and the above corollary of Lemma 3.4, we have

$$\begin{aligned}\lim_{N\to\infty} \frac{\sum_v T_{d,N}(v)}{N^{d-1}} &= \lim_{N\to\infty} \frac{\sum_{|v|>1} T_{d,N}(v)}{N^{d-1}} + 2\lim_{N\to\infty} \frac{T_{d,N}(1)}{N^{d-1}} + \lim_{N\to\infty} \frac{T_{d,N}(0)}{N^{d-1}} \\ &= 2^d(\zeta(d-1)-1) + 2k_d + 2^{d-1} \\ &= 2^d\left(\zeta(d-1) - \frac{1}{2} + \frac{k_d}{2^{d-1}}\right).\end{aligned}$$

The final step follows from van der Waerden's results, which give us that $\rho(d,N) = \rho_1(d,N) + o(N^{d-1})$, and Lemma 3.2, which states that $\rho_1(d,N) = \sum_v T_{d,N}(v) + o(N^{d-1})$. So, we have that, for $d > 2$,

$$\begin{aligned}\lim_{N\to\infty} \frac{\rho(d,N)}{N^{d-1}} &= \lim_{N\to\infty} \frac{\sum_v T_{d,N}(v) + o(N^{d-1}) + o(N^{d-1})}{N^{d-1}} \\ &= \lim_{N\to\infty} \frac{\sum_v T_{d,N}(v)}{N^{d-1}} + 2\lim_{N\to\infty} \frac{o(N^{d-1})}{N^{d-1}} \\ &= \lim_{N\to\infty} \frac{\sum_v T_{d,N}(v)}{N^{d-1}} + 0 \\ &= 2^d\left(\zeta(d-1) - \frac{1}{2} + \frac{k_d}{2^{d-1}}\right).\end{aligned}$$

This completes the proof of Theorem 3.1. This conclusion can be restated as a probability that a given polynomial is reducible. We know that the number of possible random polynomials is approximately $(2N)^d$, so the probability that a polynomial is reducible (with large enough N) is given by the approximation

$$\Pr(f(x)\ reducible) = \frac{(2^d(\zeta(d-1) - \frac{1}{2} + \frac{k_d}{2^{d-1}})N^{d-1}}{(2N)^d}.$$

Evidently, this probability goes to 0 as N goes to infinity.

To complete this discussion of the reducibility of random polynomials, we must consider the case where $d = 2$. Theorem 3.1 only covers the case when $d > 2$. To do this, we have

Theorem 3.5.

$$\lim_{N\to\infty} \frac{\rho(2,N)}{2N\ln(N)} = 1.$$

Proof. This is the result as it appears in Chela's paper, but we can in fact provide a more precise result. We will show that $\rho(2,N) = 2N\ln(N) + 2\gamma N + o(N)$ where γ is the Euler-Mascheroni constant.

We begin by noting that

$$\sum_{n=1}^{k} \frac{1}{n} = \ln(k) + \gamma + o(k).$$

Suppose $f(x)$, a degree 2 polynomial with support $[-N, N]$, can be factorized as $f(x) = (x+a)(x+b)$. Then, to find the number of reducible polynomials is the same as counting viable pairs (a, b). So, begin with the case that $0 \leq a \leq b \leq N$. Then we must have that $a \leq \sqrt{N}$. Thus the number of $f(x)$ satisfying this condition is

$$r_1 = \sum_{a=1}^{\lfloor\sqrt{N}\rfloor} \lfloor \frac{N}{a} \rfloor = \frac{N \ln(N) + \gamma N + o(N)}{2}.$$

Then, consider the case where $-N \leq b \leq a \leq 0$. Similarly, we will have that the number of $f(x)$ satisfying this condition is

$$r_2 = \sum_{-a=1}^{\lfloor\sqrt{N}\rfloor} \lfloor \frac{N}{-a} \rfloor = \frac{N \ln(N) + \gamma N + o(N)}{2}.$$

Finally, we have the case where $-N \leq a \leq 0 \leq b \leq N$. The number of $f(x)$ in this case is

$$r_3 = \sum_{a=1}^{N} \lfloor \frac{N}{a} \rfloor = N \ln(N) + \gamma N + o(N).$$

Then, the total number of reducible polynomials is given by

$$\rho(2, N) = r_1 + r_2 + r_3 = 2N \ln(N) + 2\gamma N + o(N).$$

This leaves us with a slightly more precise version of Chela's result. □

We can again restate this an approximated probability as follows

$$\Pr(f(x)\ reducible) = \frac{\rho(2, N)}{(2N)^2} = \frac{2N \ln(N) + 2\gamma N + o(N)}{4N^2}.$$

And, as before, this probability goes to 0 as N goes to infinity.

4 Rivin's Irreducibility Results

This section introduces Rivin's Method for calculating reducibility in the Large Box Model. In 2015, Igor Rivin proposed a variation on Chela's proof and results [13]. Rivin's version of the reducibility question gives a more streamlined understanding of the basic principle that the probability that a random polynomial is reducible goes to 0 as the support grows to infinity. Although less precise, his results show the same conclusion with far less work. Where Chela counts the number of reducible polynomials, or at least the number of polynomials which

have a linear factor, Rivin instead counts the number of possible configurations of random coefficients which lead to a reducible polynomial. In this way, Rivin is able to execute his entire counting argument in one step, rather than in the three that were necessary to fully justify Chela's results.

Definition 4.1. *An algebraic variety is a set of solutions to a system of polynomial equations over an affine space F^d, where F is a field. We can express a variety V as follows*

$$V = \{x \in F^d : P_1(x) = a_1, P_2(x) = a_2, \ldots, P_n(x) = a_n\}.$$

Rivin's argument will hinge on the creation of a variety out of the coefficients of the random polynomial $f(x)$. In this variety, x will represent ordered $d-$tuples of coefficients, each a possible polynomial. From there, he is able to put a bound on the size of the variety. In other words, he bounds the number of possible solutions and thus bounds the number of possible polynomials. To do this, we require the Schwartz-Zippel bound. Note that while algebraic varieties may include many more that one polynomial equation in their definition, we will actually only require one polynomial equation for this proof. As such, all algebraic varieties and the lemmas regarding them that are mentioned moving forward will only note the existence of one polynomial equation.

Lemma 4.2. *Let F be a finite field and $\bar{F}$ be its algebraic closure. If we have a variety $V = \{x \in \bar{F}^d : P(x) = a\}$, where P is a polynomial function $\bar{F}^d \to \bar{F}$, then $|V(F)|$, the number of F-points of V, is bounded by*

$$|V(F)| \ll_M |F|^{dim(V)},$$

where M is the complexity of V given by some integer larger than both d and the degree of P.

Note that an F point of V is a solution to the variety where all values of x lie in the field F. We will not prove the Schwartz-Zippel bound here, but a detailed discussion of it can be found at [18].

This lemma is slightly too broad for our purposes, so we will make use of a helpful precision as follows:

Lemma 4.3. *Let V be a variety as before, but now defined over $\mathbb{Z}$. Then, the number $|V(N)|$ of $\mathbb{Z}$-points of V of height bounded above by $N > 1$ is bounded by*

$$|V(N)| \ll_M N^{dim(V)}.$$

Proof. By Bertrand's Postulate [14], there exists a prime p such that $N \leq p \leq 2N$. So, by Lemma 4.2 we have that $|V(\mathbb{F}_p)| \ll_M |\mathbb{F}_p|^{dim(V)}$. But because $N \leq p$, every $\mathbb{Z}$ point of V of height bounded above by N corresponds to a unique point in $\mathbb{F}_p$. From here, Lemma 4.3 follows directly. □

We have

$$f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0.$$

Now, we let $f(x) = g(x)h(x)$ where

$$g(x) = x^k + b_{k-1}x^{k-1} + \cdots + b_0.$$

We begin by fixing a_0, but we continue to allow $\{a_1, \ldots, a_{d-1}\}$ to vary in $[-N, N]$. This action has interesting parallels to Chela's work. Like in the geometric portion of the proof of Lemma 3.4, we are reducing by one degree of complexity in order to make the problem easier to solve.

Next, we take $\{\alpha_1, \ldots, \alpha_d\}$ to be the set of roots of $f(x)$. There are a few relationships that are important to lay out. First, it is evident that $a_0 = \prod_{i=1}^{d} \alpha_i$. We also have that $b_0 | a_0$. Most importantly, we have that the roots of $g(x)$ are some $k-$subset of the roots of $f(x)$ and therefore b_0 equals the product of some $k-$subset of the roots of $f(x)$. Expressed another way, we have that

$$\prod_{1 \leq i_1 \leq \cdots \leq i_k \leq d} (\alpha_{i_1}\alpha_{i_2}...\alpha_{i_k} - b_0) = 0.$$

This states that in the product of every possible $k-$tuple of the roots of $f(x)$ minus b_0, one term must be 0 and therefore the whole product must be 0.

Importantly, this equation is true up to automorphism on the roots of $f(x)$. No matter how the roots are rearranged, it is always true that the product of one $k-$tuple equals b_0. This fact allows us to create a variety in the coefficients of $f(x)$. Because the product is fixed under all automorphisms, it is therefore a symmetric polynomial in b_0. By the Fundamental Theorem of Symmetric Polynomials, we know that a symmetric polynomial in the roots of f can be expressed as a polynomial in the elementary symmetric polynomials of the roots of f, which are precisely the coefficients of f. As such, there exists some polynomial g_k in the coefficients of $f(x)$ such that

$$g_k(a_1, \ldots, a_{d-1}) = \prod_{1 \leq i_1 \leq \cdots \leq i_k \leq d} (\alpha_{i_1}\alpha_{i_2}...\alpha_{i_k} - b_0) = 0.$$

Note that g_k is in terms of $\{a_1, \ldots, a_{d-1}\}$, since at the beginning of this process, we fixed a_0 as some integer in $[-N, N]$. With g_k, we have a variety in the coefficients of $f(x)$, so we may now use the Schwartz-Zippel bound. Before doing so, it is important to note that this variety in non-trivial. In other words, it does not reduce to $0 = 0$ and the statement $g_k = 0$ actually carries significance. A proof of this fact can be found in [12].

Using the variation of the Schwartz-Zippel bound laid out in Lemma 4.3, we have that

$$|g_k(N)| = O(N^{d-2}),$$

where $|g_k(N)|$ is the number of $\mathbb{Z}$-points of the variety $\{g_k = 0\}$. Here we have switched from $\ll$ notation to Big O notation because it will make the rendering of the final result simpler, but the two notations are effectively the same in this case. Note that the dimension of the variety is $d - 2$ because we have one equation and $d - 1$ unknowns. This tells us that, given a fixed a_0, there are at most $O(N^{d-2})$ reducible polynomials. Thus, the probability that such

a polynomial is reducible at most is $O(1/N)$. We must then account for the variability in a_0. To do this, we use a well-known fact which states that the average number of divisors of $n \in [1, N]$ is approximately $\log N$. This means that are approximately $\log N$ choices for b_0, and because b_0 uniquely determines a_0, we have that there are approximately $\log N$ choices for a_0. Putting this together, we have that the probability that a random polynomial is reducible is given by $O\left(\frac{\log N}{N}\right)$. Although this is slightly less precise than Chela's result, it is a far simpler proof, and it preserves the all-important fact that as N goes to infinity, to probability that a random polynomial is reducible goes to 0.

5 Rivin's Method on Galois Groups

In this section we briefly mention some applications of Rivin's counting method to the problem of determining the Galois group of a randomly chosen polynomial. We first introduce some group-theoretic facts.

Definition 5.1. *A permutation group $G_n \leq S_n$ acting on $\{1, \ldots, n\}$ in the natural way is k-transitive if it acts transitively on* ordered *k-tuples of elements in $\{1, \ldots, n\}$.*

Definition 5.2. *A permutation group $G_n \leq S_n$ acting on $\{1, \ldots, n\}$ in the natural way is k-homogeneous if it acts transitively on* unordered *k-tuples of elements in $\{1, \ldots, n\}$.*

The following theorems follow from the classification of finite simple groups.

Theorem 5.3. *For $n \geq 8$, the only 6-transitive groups are S_n and A_n.*

Theorem 5.4 (Livingstone-Wagner)**.** *If G_n is k-homogeneous, with $k \geq 5$ and $k \leq \frac{n}{2}$, then G_n is also k-transitive.*

Notice that k-transitivity implies k-homogeneity, and the preceding theorem gives a partial converse.

As above, let $f(x) = x^d + a_{d-1}x_{d-1} + \ldots + a_0$ be an arbitrary monic polynomial of degree d, and let G be the Galois group of f. Fix $d \geq 12$ (we will see later that this is necessary to apply the Livingstone-Wagner Theorem), and let the roots of f be $r_1, \ldots, r_d$, in an ordering consistent with the permutation action of G. In order to apply Rivin's method, which deals with the irreducibility of a polynomial, not its Galois group, it is necessary to construct a suitable resolvent polynomial. Define

$$f_6(x) = \prod_{1 \leq i_1 < \ldots < i_6 \leq d} \left(x - r_{i_1} \ldots r_{i_6}\right).$$

The coefficients of f are rational algebraic numbers, hence (rational) integers. Let G_6 be the Galois group of f_6. We have the following facts:

Lemma 5.5. *If the G is S_d or A_d with $d \geq 12$, then $G_6 \cong G$. In particular, f_6 is irreducible.*

Proof. Let L be the splitting field of f, and K the splitting field of f_6, so that $L/K/\mathbb{Q}$ is a tower of extensions. We have $G = \mathrm{Gal}(L/\mathbb{Q})$, and let $H = \mathrm{Gal}(L/K)$. Since G is S_d or A_d, it is 6-transitive, so for any two 6-products of roots of f, $P1$ and $P2$, there is some $g \in G$ sending $P1$ to $P2$. Then the coset gH in $G/H = \mathrm{Gal}(K/\mathbb{Q}) \cong G_6$ sends $P1$ to $P2$ since it is the restriction of the action of g on L to K, so G_6 is transitive on the $\binom{d}{6} > 2$ roots of f_6 (here we may conclude irreducibility of f_6). Now, G_6 is the quotient of S_d or A_d by a normal subgroup, so it must be one of $S_d = S_d/1$, $A_d = A_d/1$, $\mathbb{Z}/2\mathbb{Z} = S_d/A_d$, or $1 = S_d/S_d = A_d/A_d$. From the transitivity of G_6, the last two cases cannot be possible, so indeed G_6 is either S_d or A_d. □

Lemma 5.6. *If G_6 is transitive, then G is 6-homogeneous.*

Proof. This is very similar to the previous proof. We prove the contrapositive. Say L is the splitting field of f, K the splitting field of f_6, so tha $L/K/\mathbb{Q}$ is a tower of extensions. Set $G = \mathrm{Gal}(L/\mathbb{Q})$ and $H = \mathrm{Gal}(L/K)$. Then in $G_6 \cong \mathrm{Gal}(K/\mathbb{Q})$, the action of each coset gH on K is exactly the action of g on L, restricted to K. So if $\mathrm{Gal}(L/\mathbb{Q})$ is not 6-homogeneous, there exists no element $g \in G$ mapping some certain 6-product $P1$ to some other certain 6-product $P2$, so there exists no element in G_6 mapping $P1$ to $P2$. Hence G_6 is not transitive. □

Combined, these lemmas tells us that

Theorem 5.7. *The Galois group of f is S_d or A_d if and only if f_6 is irreducible.*

Proof. If p_6 is irreducible, then G_6 is transitive, and by Lemma 5.6, G is 6-homogeneous. Since $d \geq 12$, the conditions of Theorem 5.4 apply, so that G is 6-transitive. But as G is a permutation subgroup of S_d for $d \geq 8$, by Theorem 5.3, G is either S_d or A_d.

The reverse direction follows immediately from Lemma 5.5. □

Now, since the constant term of f_6 is $a_0^{\binom{d}{6}\cdot\frac{6}{d}}$, one would ideally like to apply Rivin's method directly to determine the probability that f_6 is irreducible. From that, we would like to conclude that the probability that a monic polynomial f of degree $d \geq 12$ with coefficients picked uniformly and independently from $[-N, N]$ has Galois group S_d or A_d is at most $O(\frac{\log^C N}{N})$, where the exponent C is at most $\binom{d}{6} \cdot \frac{6}{d}$ (this follows from the fact that the average number of divisors of $a_0^{\binom{d}{6}\cdot\frac{6}{d}}$ is at most $(\log N)^{\binom{d}{6}\cdot\frac{6}{d}}$, which is derived from previous arguments). However, this method relies on the critical condition that the variety generated from eliminating the dependency equations in a possible factorization is never the trivial variety. In [12], an f_6 is constructed such that this variety *is* trivial. So more analysis on the structure of f_6 is necessary before Rivin's method can be applied to general polynomials f.

6 Further Discussion of Rivin's Method

It is natural to apply Rivin's counting method, which gives an upper bound on the probability that a random polynomial (selected from some finite set) is reducible, to similar situations. We may ask the following general question:

Question 6.1. *When does Rivin's method give a tight upper bound on the number of reducible random polynomials?*

Clearly, this is not always the case. Above, we saw that Rivin's method gives the tight upper bound of $O(\frac{\log N}{N})$ (where N is the height) for degree $d = 2$ in the Large Box Model, but it does not give a tight upper bound for any $d > 2$. We now simplify our discussion a bit and consider the strength of Rivin's method when applied to *random monic trinomials*.

For a fixed degree d, consider the set of trinomials of degree d with height bounded by N:

$$P_{d,N} = \{x^d + ax^m + b : 0 < m < d; a, b \in [-N, N]\}.$$

The size of $P_{d,N}$ is $(d-1)(2N-1)^2 = O(N^2)$. We may ask for the probability that a randomly chosen polynomial from $P_{d,N}$ (with all choices equally likely) is reducible. Clearly a lower bound is $\frac{1}{2N+1} = O(\frac{1}{N})$. The same line of argument as in Section 4 gives us the following upper bound:

Theorem 6.2. *The probability that a randomly chosen polynomial from $P_{d,N}$ is reducible is at most $O(\frac{\log N}{N})$.*

When d is even, this upper bound is indeed tight:

Theorem 6.3. *For even d, the probability that a randomly chosen polynomial from $P_{d,N}$ is reducible is at least $\Omega(\frac{\log N}{N})$.*

Proof. Recall that there are $\Omega(N \log N)$ reducible quadratics of height bounded by N. Therefore there are $\Omega(N \log N)$ reducible trinomials of the form $x^d + ax^{\frac{d}{2}} + b$. For any other m strictly between 0 and d, there are at least $\Omega(N)$ reducible trinomials of the form $x^d + ax^m + b$. Hence there are at least $\Omega(N \log N) + (d-2)\Omega(N) = \Omega(N \log N)$ reducible trinomials in $P_{d,N}$, from with the theorem follows. □

However, when d is odd, there are no obvious symmetries to exploit, and the situation becomes much more difficult. We believe that this lack of symmetry implies that Rivin's upper bound is *not* tight:

Conjecture 6.4. *For odd d, the probability that a randomly chosen polynomial from $P_{d,N}$ is reducible is (asymptotically) strictly greater that $\Omega(\frac{\log N}{N})$.*

More generally:

Heuristic 6.5. *Let P be a set of* similarly structured *monic polynomials of height bounded by N, more specifically, a set of monic polynomials of fixed degree d where a certain subset $\{a_{i_1}, a_{i_2}, \ldots\}$ of the coefficients (i.e. $\{i_1, i_2, \ldots\} \subset \{1, \ldots, d-1\}$) of each $p \in P$ are fixed (to 0), and the rest of the nonconstant coefficients are allowed to vary in $[-N, N]$. Assume that the polynomials in P have no "*obvious*" symmetries. Then Rivin's bound is not tight; in other words, the probability that a randomly chosen polynomial from P is reducible is (asymptotically) strictly greater that $\Omega(\frac{\log N}{N})$.*

7 A Toy Case: Cubic Trinomials

The following work shows the difficulty of determining the Galois group of a random polynomial, even in very restricted low-degree cases. The authors were interested in trinomials of low degree so as to investigate simplified variants of Rivin's f_6 resolvent (which does not have an effective explicit description in terms of the coefficients of f), but even this was quite challenging. The following Theorem 7.1, Theorem 7.3 and Theorem 7.8 can be found at [8], but we will give original proofs of the first two results that do not rely on any results concerning elliptic curves.

We investigate integer-coefficient polynomials of the form $p(x) = x^3 + c_1 x + c_0$. The discriminant of p is

$$D = -4c_1^3 - 27c_0^2.$$

Recall that if p is irreducible, its Galois group is completely determined by the value of D. Furthermore, the Galois groups of $x^3 + c_1 x + c_0$ and $x^3 + c_1 x - c_0$ are equal, as the roots of the latter polynomial are negatives of the roots of the former.

The following theorems are proved using only basic number-theoretic techniques:

Theorem 7.1. *$p(x) = x^3 + c_1 x \pm 1$ has Galois group S_3 unless $c_1 = 0, -2, -3$. In the first two cases, p is reducible; in the third case, p is irreducible with Galois group A_3.*

Corollary 7.2. *The Galois group of $x^3 + c_2 x^2 + 1$ is S_3 unless $c_2 = 0, -2, -3$, and the Galois group of $x^3 - c_2 x^2 - 1$ is S_3 unless $c_2 = 0, -2, -3$.*

Theorem 7.3. *If q is a rational prime, then $p(x) = x^3 + c_1 x \pm q$ does not have Galois group S_3 for only finitely many integers c_1.*

First, the following preliminary lemmas are needed:

Lemma 7.4 (Thue, [15])**.** *Let $f(x, y) \in \mathbb{Z}[x, y]$ be an irreducible homogeneous polynomial in two variables of degree at least 3. Then $f(x, y) = m$ for any fixed $m \in \mathbb{Z} - \{0\}$ has only finitely many solutions.*

Lemma 7.5. *The only integer solutions to*

$$(x+y)^3 - 9x^2y = 1 \tag{7.1}$$

are $(-1,-1),(1,0)$*, and* $(0,1)$*.*

Proof. Notice that (a,b) is a solution to Equation 7.1 if and only if $(a+b,-a)$ is a solution to $x^3 - 9xy^2 - 9y^3 = 1$. From [16], Appendix B, Equation B.3, the only integer solutions to this equation are $(1,0),(-2,1)$, and $(1,-1)$, which gives the result. □

Lemma 7.6. *The only solutions in integers to* $r^2 - 3r + 9 = c^3$ *are* $(r,c) = (-3,3);(6,3)$*. In particular,* $c = 3$*.*

Proof. Let (r,c) be a solution to the given equation. We see that $r^2 - 3r + 9 = (r+3\omega)(r+3\omega^2)$, where $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ is a primitive cube root of unity. First, we rule out the possibility that $(r+3\omega)$ and $(r+3\omega^2)$ are coprime in $\mathbb{Z}[\omega]$. For if this were the case, they would each be cubes in $\mathbb{Z}[\omega]$, hence,

$$\begin{aligned} r + 3\omega &= (a+b\omega)^3 \\ &= a^3 + b^3 - 3ab^2 + (3a^2b - 3ab^2)\omega \end{aligned}$$

for some integers a,b. Comparing coefficients of ω, we see that $(ab)(a-b) = 1$, which has no solutions in integers.

Hence some non-unit $d \in \mathbb{Z}[\omega]$ divides both $r+3\omega$ and $r+3\omega^2$. Then d divides their difference, $3\omega - 3\omega^2 = 6\omega + 3$, which has norm 27. Therefore $3|N(d)$. Since $N(d)|r^2 - 3r + 9$, we must have $3|r$, so that c is also a multiple of 3. Write $r = 3m$ and $c = 3n$, so we are now looking for integer solutions to $m^2 - m + 1 = 3n^3$. From this we immediately see that $3 \nmid m$, $3 \nmid n$, and $9 \nmid m^2 - m + 1$.

Therefore we have $(m+\omega)(m+\omega^2) = 3n^3 = (-1+\omega)(-1+\omega^2)n^3$. Neither factor on the left hand side divides 3 (which has norm 9), so $m+\omega$ divides exactly one of $-1+\omega$ or $-1+\omega^2$ (and $m+\omega^2$ divides the other). Consider the first case, that $m+\omega$ divides $-1+\omega$.

Now, if there was some non-unit d dividing both $(m+\omega)$ and $(m+\omega^2)$, d would divide the difference $\omega - \omega^2 = 2\omega + 1$, which has norm 3, meaning $N(d) = 3$. Therefore $\frac{m+\omega}{-1+\omega}$ and $\frac{m+\omega^2}{-1+\omega^2}$ are coprime in $\mathbb{Z}[\omega]$.

Hence, there exist integers a,b such that

$$\begin{aligned} m + \omega &= (-1+\omega)(a+b\omega)^3 \\ &= (-a^3 - b^3 - 3a^2b + 6ab^2) + (a^3 + b^3 - 6a^2b + 3ab^2)\omega. \end{aligned}$$

Comparing coefficients of ω, we see

$$a^3 + b^3 - 6a^2b + 3ab^2 = (a+b)^3 - 9a^2b = 1. \tag{7.2}$$

From Lemma 7.5, we know all the possible values of a and b; in each case, $m = -a^3 - b^3 - 3a^2b + 6ab^2 = -1$. This means that the only solution for the first case is $m = -1$.

In the second case, $m+\omega$ divides $-1+\omega^2$, so that $\frac{m+\omega}{-1+\omega^2} = \frac{m+\omega}{-2-\omega}$ is a cube in $\mathbb{Z}[\omega]$. Thus, for some integers a and b,

$$\begin{aligned} m+\omega &= (-2-\omega)(a+b\omega)^3 \\ &= (-2a^3-2b^3+3a^2b+3ab^2)+(-a^3-b^3-3a^2b+6ab^2)\omega. \end{aligned}$$

Comparing coefficients of ω, we see

$$-a^3-b^3-3a^2b+6ab^2 = 1. \tag{7.3}$$

Now, (a,b) is a solution to Equation 7.3 if and only if $(-b,-a)$ is a solution to Equation 7.2. Therefore the only solutions to Equation 7.3 are $(1,1);(0,-1);(-1,0)$. In all three cases, $m=-2a^3-2b^3+3a^2b+3ab^2=2$. This means that the only solution for the second case is $m=2$. This exhausts all possibilities.

Recalling that $r=3m$, the only solutions for r are $r=-3$ and $r=6$, and in both cases, $r^2-3r+9=27$, meaning that $c=3$.

□

Lemma 7.7. *The only integral values c_1 for which $x^3+c_1x\pm1$ is reducible are $c_1=0,-2$.*

Proof. If $x^3+c_1x\pm1$ were reducible, it must have an integral root, which must be 1 or -1. Thus the only compatible values of c_1 are 0 and -2. □

We are ready to prove Theorems 7.1 and 7.3.

Proof of Theorem 7.1. Consider the cases where $x^3+c_1x\pm1$ is irreducible, so it has Galois group A_3 if and only if the discriminant $D=-4c_1^3-27$ is a rational square. To find such c_1, it suffices to compute integer solutions (r,c_1) to $c_1^3+r^2-3r+9=0$, since the discriminant of this as a quadratic in r is precisely D. From Lemma 7.6, we see that the only solutions (r,c_1) are $(3,-3)$ and $(6,-3)$, which, along with Lemma 7.7, gives Theorem 1. □

Proof of Theorem 7.3. Fix c_0 to be a (positive) rational prime q. Note that there are only finitely many c_1 such that x^3+c_1x+q is reducible. Therefore we may assume that x^3+c_1x+q is irreducible, so it has Galois group A_3 if and only if the discriminant $D=-4c_1^3-27q^2$ is a rational square. Then there is some integer r such that (r,c_1) is a solution to $c_1^3+r^2-3rq+9q^2=0$, since the discriminant of this as a quadratic in r is precisely D. Hence

$$r^2-3rq+9q^2=(r+3q\omega)(r+3q\omega^2)=c^3 \tag{7.4}$$

for an integer $c=-c_1$. So to prove Theorem 7.3, it suffices to show that there are only finitely many integers r such that the norm of $r+3q\omega$ is an integral cube.

Case 0: Suppose that $r+3q\omega, r+3q\omega^2$ are coprime. Then by the same argument as in Lemma 7.6, there exist integers a,b such that $r+3q\omega=(a+b\omega)^3 \Rightarrow q=(ab)(a-b)$, which is not possible unless $q=2$ (and in this case, there

are only finitely many solutions). Since r is also a polynomial in the a, b, there can only be finitely many (r, c) satisfying Equation 7.4 such that $r+3q\omega, r+3q\omega^2$ are coprime.

For the other cases, suppose that $r + 3q\omega, r + 3q\omega^2$ are not coprime with greatest common divisor $d \in \mathbb{Z}[\omega]$. Then $N(d)|N(3q\omega - 3q\omega^2) \Rightarrow N(d)|27q^2$. Since $N(d) > 1$, it can only have 3 or q as prime factors.

Case 1: $q \equiv 2 \mod 3$. Now, if $q|N(d)$, because $N(d)|r^2 - 3rq + 9q^2$, we must have $q|r$ and $q|c$. Then writing $r = qm$ and $c = qn$, we have $m^2-3m+9 = (m+3\omega)(m+3\omega^2) = qn^3$. But since $q \equiv 2 \mod 3$, it is prime in $\mathbb{Z}[\omega]$, so either $m+3\omega$ or $m+3\omega^2 = (m-3)-3\omega$ is a multiple of the integer q, a contradiction.

Thus $N(d)$ is a power of 3, so we may write $r = 3m$ and $c = 3n$, so that $m^2 - mq + q^2 = 3n^3$. Going through the possibilities, we find that $9 \nmid m^2 - mq + q^2$, so that $\frac{m+q\omega}{-1+\omega}$, $\frac{m+q\omega^2}{-1+\omega^2}$ are coprime, hence both are cubes in $\mathbb{Z}[\omega]$. From the argument in Lemma 7.6, there must exist integers a, b such that $q = a^3 + b^3 - 6a^2b + 3ab^2$, and by Lemma 7.4, there are only finitely many solutions (a, b) (setting $b = 1$ shows that $a^3+b^3-6a^2b+3ab^2$ is irreducible). Since $r = 3m$ is also a polynomial in the a, b, there can only be finitely many (r, c) satisfying Equation 7.4 in this case.

Case 2: $q \equiv 1 \mod 3$. If $q|N(d)$, as above, we write $r = qm$ and $c = qn$, so

$$m^2 - 3m + 9 = (m + 3\omega)(m + 3\omega^2) = qn^3 \tag{7.5}$$

Suppose that these two factors are relatively prime. Clearly, neither divides q, but q is not prime in $\mathbb{Z}[\omega]$. Write $q = c^2 - ce + e^2$ for some integers c, e. We note the following facts:

- Because q is prime, c and e are coprime.
- Because $3 \nmid q$, the following combinations $(c, e) \equiv (0, 0); (1, 2); (2, 1) \mod 3$ do not occur. In particular, $2c - e$ does not divide 3.
- q factorizes as $(c + e\omega)((c - e) - e\omega)$. Furthermore, $c+(c-e)\omega = -\omega^2((c-e)-e\omega) = (-\frac{1}{\omega})((c-e)-e\omega)$ is also a factor of q.
- At least one of e or $c - e$ is not a multiple of 3.
- $3 \nmid m$. Therefore none of $A = m + 3\omega$, $B = (-\omega)A = -\omega(m + 3\omega) = 3 + (3 - m)\omega$, $C = m + 3\omega^2 = (m - 3) - 3\omega$, $D = (-\omega)C = -\omega((m - 3) - 3\omega) = -3 - m\omega$ are real.

Now, one of A, B, C, or D equals $(c + e\omega)(a + b\omega)^3$, where $q = c^2 - ce + e^2$ and $3 \nmid e$ (this must happen by the fourth item above). It was necessary to introduce B and D above to possibly correct for the $-\omega^2$ unit. However, it does not matter which of A, B, C, or D it is, since each has nonzero ω component s. Equating ω components, we have

$$s = (e)a^3 + (3c - 3e)a^2b - (3c)ab^2 + (e)b^3. \tag{7.6}$$

To apply Lemma 7.4 and conclude there are only finitely many integral solutions (a, b) (implying that there are only finitely many m that satisfy Equation 7.5), we need to show that the right-hand side of Equation 7.6 is irreducible. To see this, set $b = 1$ and apply the transformation $a \to a - 1$, so that the right-hand side of Equation 7.6 becomes

$$(e)a^3 + (3c - 6e)a^2 + (-9c + 9e)a + 3(2c - e). \tag{7.7}$$

By construction, $3 \nmid e$, and by the second bullet point, $3 \nmid 2c - e$. Hence the above polynomial is Eisenstein at 3, so the right-hand side of Equation 7.6 is indeed irreducible, and there are only finitely many possibilities for $r = qm$ in this case.

Otherwise, $m + 3\omega, m + 3\omega^2$ are not relatively prime. Then the norm of their greatest common divisor is a multiple of 3, so that $3|m, 3|n$. Writing $m = 3m', n = 3n'$, we have

$$(m')^2 - m' + 1 = (m' + \omega)((m' - 1) - \omega) = 3q(n')^3. \tag{7.8}$$

We know that $9 \nmid (m')^2 - m' + 1$, and $3 = (-1+\omega)(-1+\omega^2) = (-1+\omega)(-2-\omega)$, so $m' + \omega$ divides either $-1 + \omega$ or $-2 - \omega$, and $(m' - 1) - \omega$ divides the other. Note that after this division, the two quotients are coprime. Futhermore, $m' \neq 0, \pm 1, \pm 2$ as the left-hand side of Equation 7.8 divides both 3 and the prime $q \equiv 1 \mod 3$, so each of the four possible quotients has nonzero ω component, even after multiplying each by $-\omega$. Then one of the four possible quotients (possibly adjusting by $-\omega$) is equal to $(c+e\omega)(a+b\omega)^3$ with $q = c^2 - ce + e^2, 3 \nmid e$. By the same argument as above, this case only gives finitely many possibilities for $r = 3qm'$.

The final possibility is that $N(d)$ is a power of 3. Then write $r = 3m$ and $c = 3n$, so that $m^2 - mq + q^2 = 3n^3$. Going through the possibilities, we find that $9 \nmid m^2 - mq + q^2$, so we may finish as in Case 1. So this case only gives finitely many possibilities for r.

Case 3: $q = 3$. Then $N(d)|27q^2$ is a power of 3. Thus $r^2 - 3rq + 9q^2 = r^2 - 9r + 81$ is a multiple of 3, whereupon we write $r = 3m$ and $c = 3n$, so that

$$m^2 - 3m + 9 = 3n^3. \tag{7.9}$$

From this we see that $3|m$, which makes the left-hand side of Equation 7.9 a multiple of 9, implying $3|n$. Writing $m = 3m', n = 3n'$, we obtain $(m')^2 - m' + 1 = 9(n')^3$. But this is a contradiction, as the left-hand side never divides 9. So this case does not give any possibilities for r.

Combining the results of cases 0, 1, 2, and 3 (i.e. zero or finitely many possibilities for r in each), we obtain Theorem 7.3.

□

We end with a natural generalization of Theorem 7.3:

Theorem 7.8. *For any nonzero integer c_0, $p(x) = x^3 + c_1x + c_0$ does not have Galois group S_3 for only finitely many integers c_1.*

Proof. This proof relies on more advanced machinery—in particular, results on elliptic curves. See Example 2.5, [8]. □

8 Acknowledgments

We would like to thank our project mentor, Max Xu, for introducing us to this problem and providing us with the necessary background material. We are grateful for his encouragement throughout the project and for his many valuable insights. The first author would like to thank Keith Conrad for his proof of Theorem 7.8 and other assistance on the results of Section 7. Finally, we would like to thank Pawel Grzegrzolka and the rest of the Stanford Undergraduate Research Institute in Mathematics (SURIM) staff for setting up this program, as well as for their flexibility and support during a very unusual summer.

References

[1] Bary-Soroker, L., Koukoulopoulos, D., & Kozma, G. *Irreducibility of Random Polynomials: General Measures*. arxiv.org/abs/2007.14567.

[2] Beck, M. & Robins, S. *Computing the continuous discretely*. Undergraduate Texts in Mathematics. Springer, New York, 2007.

[3] Bombieri, E. & and Gubler, W. *Heights in Diophantine Geometry*. Cambridge: Cambridge University Press, 2006.

[4] Borst, C., Boyd, E., Brekken, C., Solberg, S., Matchett Wood, M., & Matchett Wood, P. *Irreducibility of Random Polynomials*. Experimental Mathematics, 27:4, 498-506

[5] Breuillard, E. & Varjú, P. *Irreducibility of random polynomials of large degree*. https://arxiv.org/abs/1810.13360.

[6] Chela, R. *Reducible polynomials*. J. Lond. Math. Soc. 38 (1963), 183–188.

[7] Chow, S. & Dietmann, R. *Enumerative Galois Theory for Cubics and Quartics*. Advances in Mathematics 372 (2020): 107282. https://arxiv.org/abs/1807.05820

[8] Conrad, K. *Galois groups of cubics and quartics (not in characteristic 2)*. http://www.math.uconn.edu/~kconrad/blurbs/galoistheory/cubicquartic.pdf.

[9] Konyagin, S. V. *On the Number of Irreducible Polynomials with 0,1, Coefficients. Acta Arith.* 88:4 (1999),333–350. https://arxiv.org/abs/2002.10554.

[10] Mahler, K. *An Application of Jensen's Formula to Polynomials*. Mathematika, vol. 7, no. 2, 1960, pp. 98–100., doi:10.1112/S0025579300001637.

[11] Odlyzko, A. M. & Poonen, B. *Zeros of Polynomials with 0,1 Coefficients*. L'Enseignement Mathématique 39 (1993), 317–348.

[12] Pham, H. T. & Xu, M. *Irreducibility of random polynomials of bounded degree*. https://arxiv.org/abs/2002.10554.

[13] Rivin, I. *Galois Groups of Generic Polynomials*. https://arxiv.org/abs/1511.06446.

[14] Tchebychev, P. *Mémoire sur les nombres premiers*. Journal de mathématiques pures et appliquées, Sér. 1(1852), 366-390.

[15] Thue, A. *Über Annäherungswerte algebraischer Zahlen*. J. reine angew. Math. 135, 284-305, 1909.

[16] Tzanakis, N. *The diophantine equation* $x^3 - 3xy^2 - y^3 = 1$ *and related equations*. J.Number Th. 18, No 2 (1984), 192–205.

[17] van der Waerden, B. L. *Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt*. Monatsh. Math. Phys., 43(1):133–147, 1936.

[18] Zippel, R. *Probabilistic algorithms for sparse polynomials*. Symbolic and Algebraic Computation (EUROSAM '79, Internat. Sympos., Marseille, 1979), volume 72 of Lecture Notes in Comput. Sci., pages 216–226. Springer, Berlin-New York, 1979.