ON IRREDUCIBLE POLYNOMIALS WITH POSITIVE INTEGER COEFFICIENTS

NEIL KOLEKAR, MAIYA QIU, AND RICHARD WANG

Abstract. We investigate the distribution of irreducible polynomials within the semidomain of polynomials with non-negative integer coefficients. Our main result establishes that the atomic density of this structure is 1; that is, asymptotically almost all polynomials with non-negative integer coefficients are irreducible. We contrast this with the set of polynomials having coefficients restricted to zero and one, proving that their atomic density is exactly 1/2. Furthermore, we derive improved asymptotic bounds for the number of reducible polynomials with bounded degree and height. Finally, we apply these global density results to the local setting, providing a new proof of a Goldbach-type theorem for Laurent polynomials.

1. Introduction

The study of the distribution of irreducible polynomials over $\mathbb{Z}[x]$ traces back to the work of Hilbert in the 1890s. A central question in this area is understanding how often a randomly chosen integer polynomial is irreducible, particularly in the context of the *bounded height model*, where one fixes the degree and bounds the absolute values of the coefficients. Let $E_d(N)$ denote the number of monic polynomials in $\mathbb{Z}[x]$ of degree d and height at most N whose Galois group G_f is not the full symmetric group S_d. Hilbert's Irreducibility Theorem implies that $E_d(N) = o(N^d)$, establishing that most monic polynomials of fixed degree and bounded height are irreducible and have Galois group S_d.

In 1936, van der Waerden [**waerden**] refined this result by proving that

$$E_d(N) = \mathcal{O}\left(N^{d-\frac{1}{6(d-2)\log\log N}}\right).$$

Subsequent work in the 1960s further sharpened this picture. Chela [**chela**] determined an explicit constant c_d such that the number of reducible monic polynomials is given by $c_d N^{d-1} + o(N^{d-1})$. Chela observed that reducibility is often detected via divisibility by linear factors, and that counting such polynomials yields a precise asymptotic. Later, Kuba [**kuba**] showed that the total number of (not necessarily monic) polynomials in $\mathbb{Z}[x]$ of fixed degree d and height at most N that are reducible in $\mathbb{Q}[x]$ is $\mathcal{O}(N^d)$. Dubickas [**dubickas**] built upon these ideas to derive sharper asymptotics for the number of reducible polynomials with fixed degree and bounded height, again focusing on those divisible by linear factors. A key ingredient in his argument is a result of Kuba [**kuba**], which gives an upper bound on the number of reducible polynomials that are not divisible by any linear factor, a crucial case for obtaining accurate estimates.

Abstracting from their probabilistic framework, Borst et al. [**Borst**] proposed a heuristic suggesting that the density of reducible polynomials f with "well-behaved" coefficients that

Date: December 1, 2025.

are divisible by a factor of the form $a + bx^k$, where $a, b \neq 0$ and $k = \min(\text{supp}(f) \setminus \{0\})$, is equal to 1. In other words, under mild assumptions on the distribution of coefficients, almost every such polynomial is divisible by a sparse linear factor anchored at the lowest nonzero degree term.

We investigate the distribution of irreducible polynomials over the *semidomain* $\mathbb{N}_0[x]$, the semidomain of polynomials with nonnegative integer coefficients. Informally, a semidomain resembles an integral domain, except that elements are not required to have additive inverses. Semidomains have recently emerged as a rich framework for studying algebraic and arithmetic properties beyond the classical ring-theoretic setting [**chapmanmonoidsemidom**, **pologottipolysemidom**, **subatomicity**].

In the study of numerical semigroup algebras, an asymptotic invariant for understanding the distribution of irreducible elements is *atomic density* introduced by Antoniou et al. [**antoniou**]. This notion measures the limiting proportion of irreducible elements within each graded component of the algebra. In their work, Antoniou et al. showed that the atomic density of $\mathbb{F}_q[S]$, where S is a numerical semigroup and q a prime power, is zero, which means that asymptotically almost all elements of fixed degree are reducible. Following [**antoniou**], we define an analogous notion of atomic density for the semidomain $\mathbb{N}_0[x]$. In Section 3, we show that the atomic density of $\mathbb{N}_0[x]$ is equal to 1. In other words, most polynomials in $\mathbb{N}_0[x]$ are irreducible.

We then turn our attention, in Section 4, to the subset of polynomials in $\mathbb{N}_0[x]$ with coefficients in $\{0, 1\}$, hereafter referred to as *0-1 polynomials*. In the context of $\mathbb{Z}[x]$, these polynomials have been studied extensively. While Konyagin [**Konyagin**] established an upper bound of $c \cdot 2^d / \log d$ for the number of irreducible 0-1 polynomials of degree d, Borst et al. [**Borst**] provided a lower bound of $\sqrt{2/\pi d}$ for the probability that a random degree-d 0-1 polynomial is reducible. We show that, in this restricted setting, the atomic density is equal to $\frac{1}{2}$.

Section 5 is devoted to finding asymptotic bounds on the number of reducible polynomials with fixed coefficient and degree bounds, paralleling the results of Kuba in [**kuba**]. In particular, we verify that the heuristic of Borst et al. in [**Borst**] persists in $\mathbb{N}_0[x]$.

We conclude, in Section 6, by studying the existence of irreducible polynomials subject to prescribed coefficient constraints. From a probabilistic perspective, this corresponds to conditioning the ambient distribution on finitely many coordinates and asking whether irreducibility persists under such local restrictions. While atomic density captures the overall distribution of irreducible polynomials, this study offers a finer-grained local perspective that refines that picture.

2. Background

We now review some of the standard notation and terminology that we will use later. For a comprehensive background on semiring theory, we recommend the monograph [**JG1999**].

We adopt standard mathematical symbols, using $\mathbb{Z}, \mathbb{Q}$, and $\mathbb{R}$ to represent the sets of integers, rational numbers, and real numbers, respectively. The notation $\mathbb{N}$ designates the set of positive integers, whereas $\mathbb{N}_0$ refers to the set of nonnegative integers. Given a real number r and a subset $S \subseteq \mathbb{R}$, we define $S_{<r}$ as the subset of elements in S that are strictly less than r; analogous definitions apply to $S_{>r}$ and $S_{\geq r}$. For nonnegative integers m and n, we use $[\![m, n]\!]$ to denote the discrete interval $\{k \in \mathbb{Z} \mid m \leq k \leq n\}$; observe that if $m > n$

then $[\![m, n]\!] = \emptyset$. Lastly, given a positive rational number q, we write $\mathsf{n}(q)$ and $\mathsf{d}(q)$ for the numerator and denominator of q when expressed in lowest terms. For a positive integer n and prime p, we define $\nu_p(n)$ to be the largest integer k for which $p^k \mid n$ over integers.

2.1. **Commutative Monoids.** Throughout this paper, a *monoid* is defined to be a semigroup with identity that is cancellative and commutative. Unless we specify otherwise, we will use multiplicative notation for monoids. For the rest of the section, let M be a monoid. We use the notation $M^\times$ to denote the group of units (i.e., invertible elements) of M. We say that M is *reduced* provided that the group of units of M is trivial. Given a subset S of M, we let $\langle S \rangle$ denote the smallest submonoid of M containing S.

For elements $b, c \in M$, we say that b *divides* c *in* M and write $b \mid_M c$ if there exists $b' \in M$ such that $c = bb'$. A submonoid N of M is *divisor-closed* if for every $c \in N$ and $b \in M$ the relation $b \mid_M c$ implies that $b \in N$. Let S be a nonempty subset of M. We use the term *common divisor* of S to refer to an element $d \in M$ that divides all elements of S. We call a common divisor d of S a *greatest common divisor* if it is divisible by all other common divisors of S. We denote by $\gcd_M(S)$ the set consisting of all greatest common divisors of S and drop the subscript when there is no risk of confusion.

An element $a \in M \setminus M^\times$ is called an *atom* (or *irreducible*) if for every $b, c \in M$ the equality $a = bc$ implies that either $b \in M^\times$ or $c \in M^\times$. We denote by the set of atoms of M by $\mathcal{A}(M)$. We say that M is *atomic* if every element in $M \setminus M^\times$ can be written as a finite product of atoms. On the other hand, we say that M is *antimatter* if $\mathcal{A}(M) = \emptyset$. It is not hard to show that if M is an atomic monoid that is antimatter then M is an abelian group.

2.2. **Semirings and Semidomains.** A *semiring* S is a (nonempty) set endowed with two binary operations denoted by '$\cdot$' and '$+$' and called *multiplication* and *addition*, respectively, such that the following conditions hold:

(1) $(S \setminus \{0\}, \cdot)$ is a commutative semigroup with an identity element denoted by 1;
(2) $(S, +)$ is a monoid with its identity element denoted by 0;
(3) $b \cdot (c + d) = b \cdot c + b \cdot d$ for all $b, c, d \in S$.

We usually write bc instead of $b \cdot c$ for elements b, c in a semiring S. We would like to emphasize that a more general notion of a 'semiring' does not usually assume the commutativity of the underlying multiplicative semigroup, but throughout this article we will assume that the multiplication operation is commutative. A subset S' of a semiring S is a *subsemiring* of S if $(S', +)$ is a submonoid of $(S, +)$ that contains 1 and is closed under multiplication. Clearly, every subsemiring of S is a semiring.

Definition 2.1. A *semidomain* is a subsemiring of an integral domain. [1]

Let S be a semidomain. We say that $(S \setminus \{0\}, \cdot)$ is the *multiplicative monoid* of S, and we denote it by S^*. Following standard notation from ring theory, we denote the group of units of the multiplicative monoid S^* as $S^\times$, and they are referred to simply as the *units* of S. For $b, c \in S$ such that b divides c in S^*, we write $b \mid_S c$ (instead of $b \mid_{S^*} c$). Also, for a nonempty subset B of S, we use $\gcd(B)$ to denote the set of greatest common divisors of B in the monoid S^*. On the other hand, we denote the set of atoms of the multiplicative monoid S^* by $\mathcal{A}(S)$ instead of $\mathcal{A}(S^*)$, while we denote the set of atoms of the additive monoid $(S, +)$ by $\mathcal{A}_+(S)$. A semidomain S is *additively reduced* if 0 is the only invertible element of the monoid $(S, +)$.

[1] Zero divisors are implicitly excluded.

We now define polynomial semidomains. Let R be an integral domain containing the semidomain S as a subsemiring. Then the *semiring of polynomials* $S[x]$ *over* S, also referred to as the *polynomial semidomain of* S is a subsemiring of $R[x]$, and so $S[x]$ is also a semidomain. The elements of $S[x]$ are also polynomials in $R[x]$, and thus all standard terminology for polynomials, such as degree and leading coefficient, applies to elements of $S[x]$. Similarly, the *semiring of Laurent polynomials* $S[x^{\pm 1}]$ *over* S is also a semidomain.

3. Atomic Density of $\mathbb{N}_0[x]$

In this section, we investigate the asymptotic density of irreducible elements in the semidomain $\mathbb{N}_0[x]$. Specifically, we show that, in a precise asymptotic sense, almost every polynomial in $\mathbb{N}_0[x]$ is irreducible, but before formalizing this idea, let us establish some notation.

Definition 3.1. For given nonnegative integers d and N, we define $\mathcal{T}(d, N)$ to be the number of polynomials in $\mathbb{N}_0[x]$ of degree at most d and height at most N. Similarly, $I(d, N)$ (resp., $R(d, N)$) denote the number of such polynomials which are irreducible (resp., reducible).

Observe that the identity $\mathcal{T}(d, N) = \mathcal{I}(d, N) + \mathcal{R}(d, N) = (N+1)^{d+1}$ holds. Moreover, we define $\mathcal{T}_d(N)$ and $\mathcal{T}_N(d)$ as the number of polynomials of *exact degree* d and height at most N, and of *exact height* N and degree at most d, respectively. The corresponding counts of irreducible and reducible polynomials are denoted $\mathcal{I}_d(N), \mathcal{R}_d(N)$ and $\mathcal{I}_N(d), \mathcal{R}_N(d)$.

We can now define atomic density.

Definition 3.2. The *atomic density* of $\mathbb{N}_0[x]$ is defined as the common value of

$$\lim_{d\to\infty}\lim_{N\to\infty}\frac{\mathcal{I}(d,N)}{\mathcal{T}(d,N)} \quad \text{and} \quad \lim_{N\to\infty}\lim_{d\to\infty}\frac{\mathcal{I}(d,N)}{\mathcal{T}(d,N)},$$

provided that both limits exist and agree.

Note that the fact that the two iterated limits in the above definition coincide is nontrivial and is part of the proof of the subsequent theorem. We are now in a position to show that the atomic density of $\mathbb{N}_0[x]$ is 1.

Theorem 3.3. *The atomic density of* $\mathbb{N}_0[x]$ *is equal to* 1.

Proof. Take nonnegative integers $d, N \in \mathbb{N}_0$. To estimate the cardinality of the set $\mathcal{R}(d, N)$, we partition it into two subsets according to whether a given reducible polynomial is divisible by a monomial. Let A represent the set of elements of $\mathcal{R}(d, N)$ that are not divisible by any monomial, and let B represent the set of elements of $\mathcal{R}(d, N)$ that are divisible by a monomial.

It is straightforward to verify that the set B contains exactly $(N+1)^d$ polynomials with zero constant term, and at most

$$\sum_{\substack{p\in\mathbb{P}\\ p\le N}}\left(\left\lfloor\frac{N}{p}\right\rfloor+1\right)^{d+1}$$

polynomials divisible by a constant greater than one. Additionally, observe that the following inequality holds:

$$\begin{aligned}\sum_{\substack{p\in\mathbb{P}\\ p\le N}}\left(\left\lfloor\frac{N}{p}\right\rfloor+1\right)^{d+1} &\le \sum_{\substack{p\in\mathbb{P}\\ p\le N}}\sum_{k=0}^{d+1}\binom{d+1}{k}\left(\frac{N}{p}\right)^k \\ &= \sum_{k=0}^{d+1}\left(N^k\binom{d+1}{k}\sum_{\substack{p\in\mathbb{P}\\ p\le N}}\left(\frac{1}{p}\right)^k\right).\end{aligned} \tag{3.1}$$

We now estimate the cardinality of the set A. To this end, we introduce the following notation. Set

$$R_d(N) \coloneqq \{f \in \mathcal{R}_d(N) : f(0) > 0 \text{ and } k \nmid f \text{ for any } k \in \mathbb{N}_{>1}\}.$$

Note that $R_d(N)$ counts all reducible polynomials of exact degree d that are not divisible by any monomial. We claim that

$$|R_d(N)| \le (N+1)^d \left(\ln N + \gamma + \mathcal{O}(1/N)\right)^2 \left(\frac{2N+2}{N}\right), \tag{3.2}$$

where γ is the Euler-Mascheroni constant, and the implied constant of $\mathcal{O}(1/N)$ is absolute. Without loss of generality, we can assume that $d \ge 3$. Consider the set

$$C = \left\{(f,g) \in (\mathbb{N}_0[x] \setminus x\mathbb{N}_0[x])^2 : 2 \le 2\deg f \le \deg f + \deg g = d \text{ and } H(fg) \le N\right\}.$$

For an arbitrary element $(f,g) \in C$, we can write

$$f = n_k x^k + n_{k-1}x^{k-1} + \cdots + n_0 \quad \text{and} \quad g = m_{d-k}x^{d-k} + m_{d-k-1}x^{d-k-1} + \cdots + m_0,$$

where the coefficients $n_k, n_{k-1}, \ldots, n_0, m_{d-k}, m_{d-k-1}, \ldots, m_0$ are nonnegative integers. Since $H(fg) \le N$, we obtain $n_k m_{d-k} \le N$ and $n_0 m_0 \le N$. Moreover, note that the inequalities $n_0 > 0$ and $m_0 > 0$ hold, which leads to $n_i + m_i \le N$ for each index $i \in [\![1, k-1]\!]$. Consequently, if we set

$$C_k \coloneqq \left\{ \begin{array}{l} (n_k, n_{k-1}, \ldots, n_0,\, m_{d-k}, m_{d-k-1}, \ldots, m_0) \in (\mathbb{N}_0)^d : \\ \quad 0 < n_0 m_0 \le N, \\ \quad 0 < n_k m_{d-k} \le N, \\ \quad n_i + m_i \le N \quad \text{for each } i \in [\![1, k-1]\!] \end{array} \right\}$$

for each $k \in [\![1, \lfloor \frac{d}{2} \rfloor]\!]$ then there exists an injective function

$$\varphi\colon C \hookrightarrow \bigcup_{k=1}^{\lfloor d/2 \rfloor} C_k, \quad (f,g) \mapsto (n_k, n_{k-1}, \ldots, n_0,\, m_{d-k}, m_{d-k-1}, \ldots, m_0).$$

Now for every $k \in [\![1, \lfloor \frac{d}{2} \rfloor]\!]$, we have

$$\begin{aligned}
|C_k| &\leq (N+1)^{d-2k} \binom{N+2}{2}^{k-1} \left(\sum_{j=1}^{N} \left\lfloor \frac{N}{j} \right\rfloor \right)^2 \\
&\leq N^2 \left(\ln N + \gamma + \mathcal{O}(1/N) \right)^2 (N+1)^{d-2k} \binom{N+2}{2}^{k-1} \\
&\leq (N+1)^d \left(\ln N + \gamma + \mathcal{O}(1/N) \right)^2 \left(\frac{N+2}{2N+2} \right)^{k-1}
\end{aligned}$$

given that $\sum_{j=1}^{N} 1/j = \ln N + \gamma + \mathcal{O}(1/n)$ (see, for instance, [**GKP94**]), where γ is the Euler-Mascheroni constant. Thus,

$$\begin{aligned}
|R_d(N)| \leq |C| \leq \sum_{k=1}^{\lfloor d/2 \rfloor} |C_k| &\leq \sum_{k=1}^{\lfloor d/2 \rfloor} \left[(N+1)^d \left(\ln N + \gamma + \mathcal{O}(1/N) \right)^2 \left(\frac{N+2}{2N+2} \right)^{k-1} \right] \\
&\leq (N+1)^d \left(\ln N + \gamma + \mathcal{O}(1/N) \right)^2 \sum_{k=1}^{\infty} \left(\frac{N+2}{2N+2} \right)^{k-1} \\
&= (N+1)^d \left(\ln N + \gamma + \mathcal{O}(1/N) \right)^2 \left(\frac{2N+2}{N} \right),
\end{aligned}$$

which proves Claim (3.2). This, in turn, allows us to estimate the cardinality of the set A of reducible polynomials of degree at most d and height at most N that are not divisible by any monomial. In fact,

$$\begin{aligned}
|A| \leq \sum_{i=0}^{d} |R_i(N)| &\leq 2 \left(\ln N + \gamma + \mathcal{O}(1/N) \right)^2 \left(\frac{N+1}{N} \right) \sum_{i=0}^{d} (N+1)^i \\
&\leq \frac{2 \left(\ln N + \gamma + \mathcal{O}(1/N) \right)^2 (N+1)^{d+2}}{N^2}.
\end{aligned}$$

We are now in a position to establish that the atomic density of $\mathbb{N}_0[x]$ is equal to 1. By Inequality (3.1), we have

$$\begin{aligned}
&\lim_{d\to\infty} \lim_{N\to\infty} \frac{\mathcal{R}(d,N)}{\mathcal{T}(d,N)} \\
&\quad \leq \lim_{d\to\infty} \lim_{N\to\infty} \frac{1}{N+1} + \sum_{k=0}^{d+1} \left(\frac{N^k \binom{d+1}{k}}{(N+1)^{d+1}} \cdot \sum_{\substack{p \in \mathbb{P} \\ p \leq N}} \left(\frac{1}{p} \right)^k \right) + \frac{2(N+1) \left(\ln N + \gamma + \mathcal{O}(1/N) \right)^2}{N^2} \\
&\quad = \lim_{d\to\infty} \lim_{N\to\infty} \sum_{k=0}^{d+1} \left(\frac{N^k \binom{d+1}{k}}{(N+1)^{d+1}} \cdot \sum_{\substack{p \in \mathbb{P} \\ p \leq N}} \left(\frac{1}{p} \right)^k \right),
\end{aligned}$$

with the first and third term of the sum vanishing as $N \to \infty$. Moving the outermost summation out of the coefficient limit,

$$\begin{aligned}
&\lim_{d\to\infty} \sum_{k=0}^{d+1} \left(\lim_{N\to\infty} \frac{N^k \binom{d+1}{k}}{(N+1)^{d+1}} \cdot \sum_{\substack{p\in\mathbb{P} \\ p\le N}} \left(\frac{1}{p}\right)^k \right) \\
&\le \lim_{d\to\infty} \left(\lim_{N\to\infty} \sum_{\substack{p\in\mathbb{P} \\ p\le N}} \left(\frac{1}{p}\right)^{d+1} \right) \\
&= \lim_{d\to\infty} \sum_{p\in\mathbb{P}} \left(\frac{1}{p}\right)^{d+1} = 0.
\end{aligned}$$

It remains to show that

$$\lim_{N\to\infty} \lim_{d\to\infty} \frac{\mathcal{R}(d,N)}{\mathcal{T}(d,N)} = 0.$$

As before, for each fixed N, we have

$$\lim_{d\to\infty} \frac{\mathcal{R}(d,N)}{\mathcal{T}(d,N)} \le \frac{1}{N+1} + \sum_{\substack{p\in\mathbb{P} \\ p\le N}} \left(\frac{\frac{N}{p}+1}{N+1}\right)^{d+1} + \frac{2(N+1)\left(\ln N + \gamma + \mathcal{O}(1/N)\right)^2}{N^2}.$$

For every prime $p \le N$,

$$0 < \frac{\frac{N}{p}+1}{N+1} = \frac{N+p}{p(N+1)} < 1,$$

so each term $\left(\frac{\frac{N}{p}+1}{N+1}\right)^{d+1}$ tends to 0 as $d \to \infty$. Therefore

$$\lim_{d\to\infty} \frac{\mathcal{R}(d,N)}{\mathcal{T}(d,N)} \le \frac{1}{N+1} + \frac{2(N+1)\left(\ln N + \gamma + \mathcal{O}(1/N)\right)^2}{N^2}.$$

Taking the limit as $N \to \infty$ on the right-hand side gives 0, and hence

$$\lim_{N\to\infty} \lim_{d\to\infty} \frac{\mathcal{R}(d,N)}{\mathcal{T}(d,N)} = 0.$$

Consequently,

$$\lim_{N\to\infty} \lim_{d\to\infty} \frac{\mathcal{I}(d,N)}{\mathcal{T}(d,N)} = 1.$$

We can then conclude that the atomic density of $\mathbb{N}_0[x]$ is equal to 1. □

The following two graphs illustrate the growth of density for low values of degree and coefficient bounds.

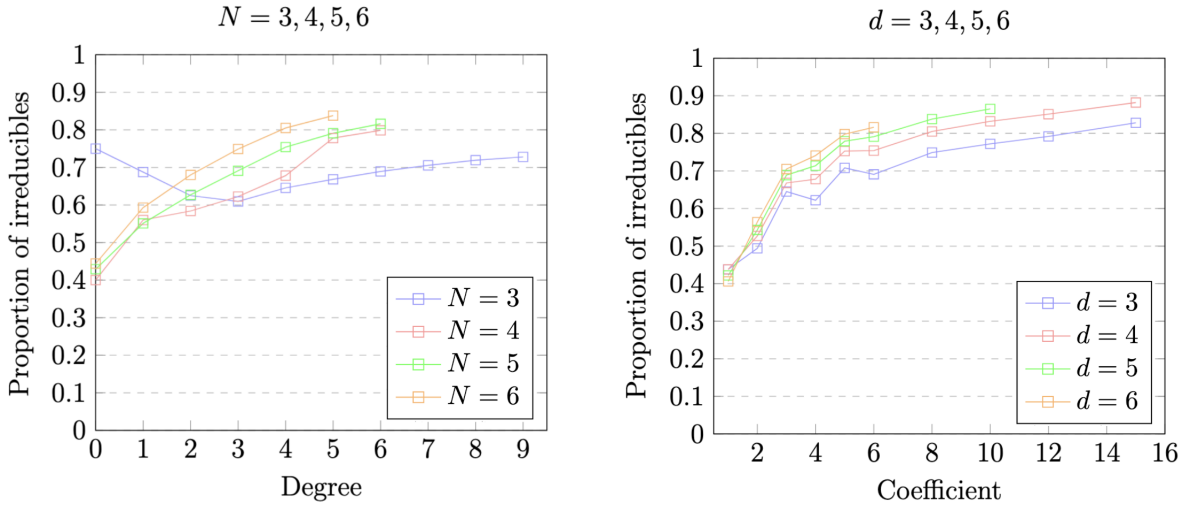

Figure 1. Degree bound ≤ 9 (left) and coefficient bound ≤ 16 (right) v.s. proportion of irreducibles in $\mathbb{N}_0[x]$

3.1. **Atomic Density of $\mathbb{Q}[x]$ and $\mathbb{Q}_0[x]$.** Having established that most polynomials in $\mathbb{N}_0[x]$ are irreducible—paralleling the classical case of $\mathbb{Z}[x]$, where irreducibility is closely connected to that in $\mathbb{Q}[x]$ via Gauss' lemma—we now turn to subsemidomains of $\mathbb{Q}[x]$. While the behavior of $\mathbb{N}_0[x]$ and $\mathbb{Z}[x]$ suggests that atomic density 1 might be typical, this phenomenon does not, in general, extend to all subsemidomains of $\mathbb{Q}[x]$. In what follows, we first extend the notion of atomic density to arbitrary subsemidomains of $\mathbb{Q}[x]$ and then provide explicit examples showing that the atomic density can take any prescribed value in the interval $[0, 1]$. In particular, we begin by exhibiting a subdomain of $\mathbb{Q}[x]$ whose atomic density equals 0.

Given a polynomial $f = q_n x^n + \cdots + q_0 \in \mathbb{Q}[x]$ (written in canonical form), we let $\mathsf{d}(f)$ denote the smallest positive integer such that $\mathsf{d}(f)f \in \mathbb{Z}[x]$.

Definition 3.4. Let $S \subseteq \mathbb{Q}[x]$ be a subsemidomain. For $c, d, N \in \mathbb{N}$, let $\mathcal{T}_S(c, d, N)$ be the number of polynomials $f \in S$ of degree at most d with $\mathsf{d}(f) \leq c$ and whose integral multiple $\mathsf{d}(f)f$ has height in $[-N, N]$. Among these, let $\mathcal{I}_S(c, d, N)$ denote the irreducible ones.

The *atomic density* of S is the real number, when it exists,

$$\psi(S) := \lim_{c\to\infty} \lim_{d\to\infty} \lim_{N\to\infty} \frac{\mathcal{I}_S(c, d, N)}{\mathcal{T}_S(c, d, N)}.$$

Observe that when the semidomain S is $\mathbb{N}_0[x]$, Definition 3.4 coincides with Definition 3.2.

Lemma 3.5. *There exists a bijection $\varphi\colon \mathbb{Q}[x]^* \xrightarrow{\sim} \mathbb{Q}^* \times P$, where P denotes the set of primitive polynomials in $\mathbb{N}_0[x]$. (Note that a polynomial is primitive if its the greatest common divisor of its coefficients is 1).*

Proof. Given a nonzero polynomial $f = q_0 + q_1 x + \cdots + q_m x^m \in \mathbb{Q}[x]^*$, where each coefficient $q_i = \frac{n_i}{d_i}$ is written in lowest terms with $\gcd(n_i, d_i) = 1$, set

$$q^f := \frac{\operatorname{lcm}(d_0, \ldots, d_m)}{\gcd(n_0, \ldots, n_m)}.$$

The map $\varphi\colon \mathbb{Q}[x]^* \to \mathbb{Q}^* \times P$ is given by the assignment $f \mapsto (q^f, q^f f)$. Verifying that φ is a well-defined bijection (i.e. φ satisfies both injectivity and surjectivity) is straightforward, so we leave this task to the reader. □

Before formally defining atomic density in $\mathbb{Q}[x]$, we prove the following lemma.

Lemma 3.6. *There exists a bijection $f : \mathbb{Q}[x] \longmapsto (\mathbb{Q}, P_{\mathbb{Z}}[x])$ where $P_{\mathbb{Z}[x]}$ denotes the set of primitive polynomials of $\mathbb{Z}[x]$.*

Proof. Take a polynomial $g(x)$ in $\mathbb{Q}[x]$, and let it be expressed as $a_n x^n + a_{n-1} + x^{n-1} + \cdots + a_0$ where each coefficient is in its reduced form. Let us express each $a_i = d_i/n_i$. Then let $L = \operatorname{lcm}(d_i)$ and $N = \gcd(n_i)$. It is quite clear that g is surjective as we can take $\frac{N}{L} g'(x) \in (\mathbb{Q}, P_{\mathbb{Z}}[x])$ where

$$g'(x) = \sum_{i=0}^{n} \left(\frac{La_i}{N} \right) x^i.$$

Note that the coefficient is an integer by definition. Also, note that $\gcd(\{La_i\}) = \gcd(\{n_i\}) = N$ (if otherwise, we would be able to divide away a constant from L and reach a smaller LCM). Hence after each coefficient La_i is divided by N, the resulting polynomial $g'(x)$ is primitive.

It is easy to show that this mapping f is also injective. For the sake of contradiction suppose we have $\frac{a}{b} g(x) = \frac{a'}{b'} g'(x)$ for some $a/b, a'/b' \in \mathbb{Q}[x]$ and $g(x), g'(x) \in P_{\mathbb{Z}}[x]$. Hence we have $ab' g(x) = a'b g'(x)$. Clearly $\gcd(ab' g(x)) = ab' \neq \gcd(a'b g'(x)) = a'b$ unless $ab' = a'b$, in which case $a/b = a'/b'$. Hence we have that f is both surjective and injective and we are done. □

We can now define atomic density as

$$\lim_{s \to \infty} \lim_{d,n \to \infty} \frac{\mathcal{I}_s(d, N)}{\mathcal{T}_p(d, N)}$$

if the limit converges. Note that it would not make sense to also consider the double limit with $d, n \to \infty$ and $s \to \infty$ switched as this would lead to a non-converging sequence of 0's and 1's. For the density of $\mathbb{Q}[x]$ (resp. $\mathbb{Q}_0[x]$) $\mathcal{T}_p(d, N)$ denotes the cardinality of

$$\left\{ \frac{a'}{b'} \cdot f(x) \mid f(x) \in \mathcal{A}(T'(d, N)); (a', b') \in \mathbb{N}_0 \times \mathbb{N}_0 \right\}$$

where $T'(d, N)$ is the number of primitive polynomials in $\mathbb{Z}[x]$ (resp. $\mathbb{N}_0[x]$) with height bounded by n and degree by d. We use $\mathcal{I}_s(d, N)$ to denote the number of polynomials in the above set that are irreducible in $\mathbb{Z}[x]$ (resp. $\mathbb{N}_0[x]$).

Theorem 3.7. *Under the definition above, the atomic density of $\mathbb{Q}[x]$ and $\mathbb{Q}_0[x]$ are both 1.*

Proof. Following our definition, note that we have $\mathcal{T}_p(d, N) = k \cdot T'(d, N)$ and $\mathcal{I}_s(d, N) = k \cdot \mathcal{I}(d, N)$ where $\mathcal{I}(d, N)$ is the number of irreducibles in $\mathbb{Z}[x]$ (resp. $\mathbb{N}_0[x]$) with degree bounded by d and height by n for some constant $k \leq s + 1$ (we use k instead of simply $s + 1$ as we do not want to count equivalent fractions multiple times). Since $T'(d, N) \subseteq \mathcal{T}(d, N)$ we have $\mathcal{T}_p(d, N) = k \cdot T'(d, N) \leq k \cdot \mathcal{T}(d, N)$ whereas $\mathcal{I}_s(d, N) = k \cdot \mathcal{I}(d, N)$. Hence we have that

$$\lim_{s \to \infty} \lim_{d,n \to \infty} \frac{\mathcal{I}_s(d, N)}{\mathcal{T}_p(d, N)} \leq \lim_{s \to \infty} \lim_{d,n \to \infty} \frac{k \cdot \mathcal{I}(d, N)}{k \cdot \mathcal{T}(d, N)} = \lim_{s \to \infty} 1 = 1.$$

And so we have proven that the density of $\mathbb{Q}[x]$ and $\mathbb{Q}_0[x]$ are both 1. □

We are now in a position to prove that the atomic density of subsemidomains of $\mathbb{Q}[x]$ can take any prescribed real value in the interval $[0, 1]$.

Lemma 3.8. *Let $r \in \mathbb{R}$ such that $0 \leq r \leq 1$. Then there exists a subset $P_r \subseteq \mathbb{P}$ such that*

$$\prod_{p \in P_r} \left(1 - \frac{1}{p}\right) = r.$$

Proof. Recall that the Euler product tells us that

$$\prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p}\right) = \lim_{s \to 1^+} \prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p^s}\right) = \lim_{s \to 1^+} \frac{1}{\zeta(s)} = 0,$$

so we can take $P_0 = \mathbb{P}$. Since the empty product is defined as 1, we also have $P_1 = \varnothing$. Let $r \in (0, 1)$. We construct two sequences $(r_n)_{n \in \mathbb{N}}$ and $(p_n)_{n \in \mathbb{N}}$ satisfying that $r_0 = 1$, $p_0 = 1$, and if $r_{n-1} > r$ for some $n \in \mathbb{N}$ then set $r_n \coloneqq r_{n-1}(1 - \frac{1}{p_n})$, where p_n is the smallest prime such that $p_n > p_{n-1}$ and $r_n \geq r$.

Now, we observe that the sequence of r_n terminates if $r_k = r$ for some k, and otherwise converges to r. To show this, define $A \subseteq \mathbb{N}$ as the set of indices i for which p_i is defined. We let $P_r = \{p_i \mid i \in A\}$, and note that P_r is not empty, since p_1 exists because $r < 1 = r_0$. If A is finite, it is necessarily of the form $\{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$. This is only possible if $r_n = r$, so if A is finite then

$$\prod_{p \in P_r} \left(1 - \frac{1}{p}\right) = \prod_{i \in A} \left(1 - \frac{1}{p_i}\right) = r_n = r.$$

Otherwise, $A = \mathbb{N}$. In this case, note that $\mathbb{P} \setminus P_r$ is an infinite set; otherwise, we would have $r = c \cdot \prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p}\right) = 0$ for some finite c, contradicting our assumption that $r > 0$. We have

$$\prod_{p \in P_r} \left(1 - \frac{1}{p}\right) = \prod_{i \in A} \left(1 - \frac{1}{p_i}\right) = \lim_{n \to \infty} \prod_{i=1}^{n} \left(1 - \frac{1}{p_i}\right) = \lim_{n \to \infty} r_n.$$

It remains to verify that this limit exists and converges to r. Clearly, by definition, $r_i > r_j > r$ for any positive integers $i < j$. Thus, it suffices to show that for any $\varepsilon > 0$, there exists some $k \in \mathbb{N}$ such that $r_k < r + \varepsilon$.

For the sake of contradiction, suppose $r_k \geq r + \varepsilon$ for all $k \in \mathbb{N}$. Since we proved $\mathbb{P} \setminus P_r$ is an infinite set, it follows that there exists some $q \in \mathbb{P} \setminus P_r$ such that $\left(1 - \frac{1}{q}\right) \geq \frac{r}{r+\varepsilon}$, so that $r_k \left(1 - \frac{1}{q}\right) \geq r$ for all k. Now, since q is fixed and A is infinite, let m be the least integer such that $p_m > q$. Letting $k = m - 1$, we have $r_{m-1} \left(1 - \frac{1}{q}\right) \geq r$. Since $q < p_m$, this contradicts the definition of p_m, which states that it is the least prime p satisfying $r_{m-1} \left(1 - \frac{1}{p}\right) \geq r$. Therefore, we conclude that $\lim_{n \to \infty} r_n = r$. □

Now for every real number $r \in (0, 1)$, we set $D_r \coloneqq \mathbb{Z} + x\mathbb{Z}[\frac{1}{p} \mid p \in P_r][x]$ to be a subsemidomain of $\mathbb{Q}[x]$. Next we show that $\psi(D_r) = r$.

Proposition 3.9. *The atomic density of D_r is equal to r.*

Proof. For $c, d, N \in \mathbb{N}$, let $\mathcal{T}_{D_r}(c, d, N)$ be the number of polynomials $f \in D_r$ of degree at most d with $\mathsf{d}(f) \leq c$ and whose integral multiple $\mathsf{d}(f)f$ has height in $[-N, N]$. Among these, let $\mathcal{I}_{D_r}(c, d, N)$ denote the irreducible ones.

For a fixed $N \in \mathbb{N}$, let $\psi(D_r, N)$ denote the density of irreducibles in D_r with all coefficients bounded in absolute value by N. Let us also define $\psi_k(D_r, N)$ to be the density of irreducibles among all $f \in D_r$ with constant term $k \in \mathbb{Z}$ and coefficients bounded by N. We then define

$$\psi(D_r) = \lim_{N\to\infty} \psi(D_r, N) = \lim_{N\to\infty} \frac{1}{2N+1} \sum_{k=-N}^{N} \psi_k(D_r, N).$$

We will now evaluate $\psi_k(D_r, N)$. In the case that there exists some $p \in P_r$ such that $p \mid k$, it is clear that all f with constant term k are divisible by the irreducible element $p \in P_r$. Thus, if k is divisible by some $p \in P_r$ then $\psi_k(D_r, N) = 0$. Otherwise, if such a p does not exist then all reducible f with constant term k are expressible as gh, for nonconstant g and h. This occurs precisely when f is irreducible over $\mathbb{Q}[x]$, which has atomic density 1. Thus, $\psi_k(D_r, N) = 1$ in these cases.

By the Chinese remainder theorem, the number of integers in the interval $[\![-N, N]\!]$ coprime to all elements of P_r must be between $\lfloor (2N+1)r \rfloor$ and $\lceil (2N+1)r \rceil$. Hence,

$$r = \lim_{N\to\infty} \frac{\lfloor (2N+1)r \rfloor}{2N+1} \leq \lim_{N\to\infty} \frac{1}{2N+1} \sum_{k=-N}^{N} \psi_k(D_r, N) \leq \lim_{N\to\infty} \frac{\lceil (2N+1)r \rceil}{2N+1} = r.$$

Therefore, we conclude that $\psi(D_r) = r$, completing the proof. □

The approach used to define atomic density for polynomials in $\mathbb{N}_0[x]$ cannot be directly extended to the setting of power series with coefficients in $\mathbb{N}_0$, even though every irreducible polynomial remains irreducible when regarded as a power series. The main obstacle lies in the fact that $\mathbb{N}_0[\![x]\!]$ is uncountable, whereas our previous definition fundamentally relies on approximating the ambient space by an increasing sequence of finite sets. In the polynomial case, this sequence exhausts the countable set of polynomials by bounding both the degree and the height of the coefficients. In contrast, for power series, no such sequence of finite subsets can approximate the entire uncountable space of series with coefficients in $\mathbb{N}_0$. Consequently, the notion of atomic density, as developed for $\mathbb{N}_0[x]$, does not naturally extend to $\mathbb{N}_0[\![x]\!]$.

4. Atomic Density of 0-1 Polynomials

In this section, we turn our attention to the subset of polynomials in $\mathbb{N}_0[x]$ with coefficients in $\{0, 1\}$, hereafter referred to as *0-1 polynomials*. We show that, in this restricted setting, the atomic density is equal to $\frac{1}{2}$. It has been proved that 0-1 polynomials in $\mathbb{Z}_0[x]$ have density $1/2$ (see, for instance, [**Borst**]).

Theorem 4.1. *For the number of reducible polynomials of degree d or less, denoted $\mathcal{R}(d)$, we have $\mathcal{R}(d) \leq 2^d + \mathcal{O}(\varphi^{d-1})$, where $\varphi \approx 1.618$ is the golden ratio.*

Proof. For degree d let us denote the number of such polynomials as $\mathcal{R}(d)$. Then we can write $\mathcal{R}(d) \leq 2^d + \mathcal{R}'(d)$ where 2^d denotes the number of 0-1 polynomials with constant term 0, and $\mathcal{R}'(d)$ denotes the number of tuples $(a_1 \dots a_{j-1}, b_1 \dots b_{d-j-1})$ where each a_i and b_i is

either 0 or 1. Note that we are essentially counting the number of reducible polynomials that can be expressed as

$$f(x) = (1 + a_1x + \cdots + a_{j-1}x^{j-1} + x^j)(1 + b_1x + \cdots b_{d-j-1}x^{d-j-1} + b_{d-j}x^{d-j}),$$

We can partition *all* coefficients of b into the following sequences based on the indices' remainder modulo j:

$$\begin{cases} b_j, b_{2j}, \dots \\ b_1, b_{j+1}, \dots \\ \vdots \\ b_{j-1}, b_{2j-1}, \dots \end{cases}.$$

Then notice that there would not exist consecutive pairs of 1's in each sequence because it would lead to coefficients greater than 1 when multiplied by the leading and constant in $1 + a_1x + \cdots + a_{j-1}x^{j-1} + x^j$. If we count the number of possible such sequences for a given length n using F_n, we have $F_0 = 2$, $F_1 = 3$, and the recurrence relation $F_n = F_{n-1} + F_{n-2}$ (F_{n-1} with the additional term 0, or alternatively the last term is 1 and so the second to last term is 0 with F_{n-2} to count the rest of the sequence. Notice that this is the well-known Fibonacci recurrence relation with the sequence terms shifted by 3, so we have that for each sequence the number of different choices would be $f_k = \frac{\varphi^{k-3} - \phi^{k-3}}{\sqrt{5}}$ where $k = \lceil (d-j)/j \rceil$ and ϕ is the conjugate of φ, equal to $\frac{1-\sqrt{5}}{2}$. Since there are j such sequences the number of reducible polynomials is bounded above by

$$\left(\frac{\varphi^{k-3} - \phi^{k-3}}{\sqrt{5}}\right)^j \leq \mathcal{O}\left(\frac{\varphi^{k-3}}{\sqrt{5}}\right)^j.$$

Finally we sum this over each possible j from 1 to $\lfloor d/2 \rfloor$ to get

$$\frac{\frac{1}{\sqrt{5}} \cdot (\varphi^{d-3} - \phi^{d-3}) \cdot (1 - \frac{1}{\varphi\sqrt{5}}^{d-2/2})}{\frac{1}{1-\varphi\sqrt{5}}} \leq \mathcal{O}(2^d).$$

And so adding the constant term zero polynomials we have that $\mathcal{R}(d) \leq 2^d + \mathcal{O}(\varphi^d)$. □

Corollary 4.2. *The density of irreducibles of all 0-1 polynomials in $\mathbb{N}_0[x]$ is 1/2.*

Proof. Defining density to be $\lim_{d\to\infty} \frac{\mathcal{I}(d)}{\mathcal{T}(d)}$ where $\mathcal{I}(d)$ is the number of irreducible 0-1 polynomials of degree d or less and $\mathcal{T}(d) = 2^{d+1}$, we have that

$$\frac{\mathcal{I}(d)}{\mathcal{T}(d)} = \frac{2^{d+1} - \mathcal{R}(d)}{2^{d+1}} = \frac{2^d - \mathcal{O}(\varphi^d)}{2^{d+1}} = \frac{1}{2}.$$

□

We now provide a lower bound on the number of reducibles by considering the number of polynomials divisible by $x + 1$, ultimately proving that the asymptotic of reducible 0-1 polynomials of degree d or less with constant term 1 is $\mathcal{O}(\varphi^d)$.

For a fixed degree d, consider factors of the form $x^k + 1$ for each $k \in [\![1, d]\!]$. For a polynomial f that can be expressed as $(x^k + 1)g(x)$, we can directly count the number of possible f: Let f_d denote the number of possible 0-1 polynomials of degree d or less divisible by $x + 1$. Then we can write $f_d = f_{d-1} + f_{d-2}$, where f_{d-1} accounts for all such polynomials with degree $< d$, and f_{d-2} accounts for polynomials of the form $x^d + x^{d-1} + f'$: note that

if the coefficient of x^d is 1 we must have the coefficient of x^{d-1} to be 1 then removing these two terms the remaining polynomial f' must be another 0-1 polynomial divisible by $x+1$ of degree $d-2$ or less. Its initial terms are $f_0 = 1$ (accounting for 0), $f_1 = 2$ (0 and $x+1$), and we can verify $f_2 = 3$ (0, $x+1$, x^2+x). This is the well-known recurrence for Fibonacci numbers with the terms shifted by 1 and so we have that the exact number of such polynomials is

$$f_d = \frac{\varphi^{d+1} - \phi^{d+1}}{\sqrt{5}} = \mathcal{O}(\varphi^{d+1})$$

since $|\varphi| = |\frac{1+\sqrt{5}}{2}| > |\phi| = |\frac{1-\sqrt{5}}{2}|$.

Lastly if we were to combine this with polynomials of constant term 0, note that we would have overcounted the number of polynomials divisible by $x(x+1)$. Note that each such polynomial would be equivalent to x multiplied by a polynomial of degree $d-1$ or less, which is counted for by $f_{d-1} = \mathcal{O}(\varphi^d)$. Hence by the inclusion-exclusion principle we still have

$$\mathcal{R}(d) \geq 2^d + \mathcal{O}(\varphi^{d+1}) - \mathcal{O}(\varphi^d) = 2^d + \mathcal{O}(\varphi^{d+1}) = 2^d + \mathcal{O}(\varphi^d).$$

Combining this with the upper bound we reach the following theorem on the number of reducible 0-1 polynomials of degree d or less.

Theorem 4.3. *The asymptotic number of reducible 0-1 polynomials in $\mathbb{N}_0[x]$ with degree d or less is $2^{d-1} + \mathcal{O}(\varphi^d)$, where φ takes the fixed value of $\frac{1+\sqrt{5}}{2}$.*

The following figure demonstrates how the density approaches $\frac{1}{2}$ as the degree increases.

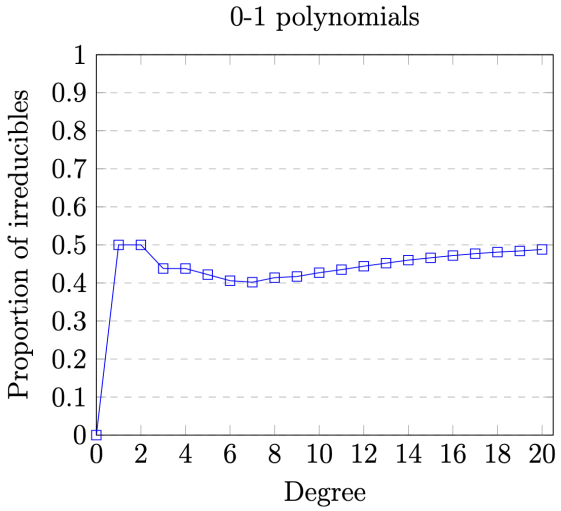

Figure 2. Irreducibles proportion for 0-1 polynomials converging to $\frac{1}{2}$.

5. Counting Reducible Polynomials in $\mathbb{N}_0[x]$

In this section, we will find refined bounds on $\mathcal{R}(d, N)$ for the individual asymptotics $d \to \infty$ and $N \to \infty$. Using a recursive approach, we obtain both upper and lower asymptotic bounds on $\mathcal{R}(d, N)$ as $d \to \infty$. We also obtain an asymptotic upper bound on $\mathcal{R}(d, N)$ as $N \to \infty$, via a lattice point interpretation of divisibility in $\mathbb{N}_0[x]$.

5.1. **Asymptotics for $d \to \infty$.**

Definition 5.1. For every positive integer n, denote ρ_n by the spectral radius of the $n \times n$ matrix T_n defined by

$$(T_n)_{ij} = \begin{cases} 1 & i+j \le n+1 \\ 0 & \text{otherwise.} \end{cases}$$

Furthermore, set

$$C_n := \lim_{k\to\infty} \frac{1}{\rho_n^k} \mathbf{u} \cdot T_n^{k-1} \cdot \mathbf{u}^T,$$

where $\mathbf{u} = [0, 1, \ldots, 1]$.

In order to ensure that C_n is well defined, we must check that the Perron-Frobenius theorem applies to the matrix T_n. A sufficient condition for Perron-Frobenius is that the directed graph G_n on $[n]$ associated with T_n is strongly connected. Note that two, not necessarily distinct vertices i and j of G_n are adjacent if and only if $i + j \le n + 1$. As such, the edges between any two vertices of G_n are bidirectional, so we may delete the self-loops of G_n and regard it as a simple finite graph; it suffices to show that the resulting graph is connected. It is not hard to check that G_n is connected for $n = 1, 2, 3$. Suppose that $n > 3$. For all $3 \le i < j \le n$, we note that i and j are connected because of the path $i \to 2 \to 1 \to j$. Therefore, G_n is connected, so we conclude that C_n is well defined.

Definition 5.2. Let $S(d, N)$ denote the set of polynomials in $\mathbb{N}_0[x]$ with degree at most d, height at most N, and nonzero constant term.

Lemma 5.3. *Let a and b be positive integers with $\gcd(a, b) = 1$. Then, the number of polynomials in $S(d, N)$ that are divisible by the binomial $a + bx$ is at most $\sim \rho_{N+1}^{d+1} \cdot C_{N+1}$ as $d \to \infty$, with equality at $a = b = 1$.*

Proof. For $0 \le k \le N$, let $A(k, d)$ denote the number of polynomials in $S(d, N)$ that are divisible by $a + bx$ and have x^d coefficient equal to bk. Note the recurrence

$$A(k, d) = \sum_{k'=0}^{N} A(k', d-1) \cdot \mathbf{1}_{ak+bk' \le N}$$

for every $d \ge 1$, by casework on the leading coefficient of polynomials in $S(d, N)$. Thus, if we let $\mathbf{v}_d$ denote the vector $[A(0, d), \ldots, A(N, d)]^T$, then we have $\mathbf{v}_d \preceq T_{N+1} \cdot \mathbf{v}_{d-1}$, or equivalently,

$$\mathbf{v}_d \preceq T_{N+1}^d \cdot \mathbf{v}_0 = T_{N+1}^d \cdot \mathbf{u}^T.$$

The desired result follows. □

Proposition 5.4. *Let $f(x) \in \mathbb{N}_0[x]$ be a nonconstant polynomial. Then, the number of polynomials in $S(d, N)$ that are divisible by $f(x)$ is at most $\sim \rho_{N+1}^{d+1} \cdot C_{N+1}^k$, with equality at $f(x) = 1 + x^k$ for every $k \ge 1$.*

Proof. Note that the number of polynomials in $S(d, N)$ that are divisible by $f(x)$ is at most the number of polynomials in $S(d, N)$ that are divisible by $([x^0]f(x)) + x^{\deg(f)}([x^{\deg(f)}]f(x))$. The result follows via application of Lemma 5.3. □

Theorem 5.5. *We have the following asymptotic bounds for $\mathcal{R}(d, N)$ as $d \to \infty$, by casework on the value of C_{N+1}.*

(1) $(N+1)^d + \mathcal{O}(\rho_{N+1}^d) \leq \mathcal{R}(d,N) \leq (N+1)^d + \mathcal{O}((N+1)^{\frac{d}{2}} C_{N+1}^{\frac{d}{2}} \rho_{N+1}^d)$ *provided that* $C_{N+1} > \frac{1}{N+1}$;

(2) $(N+1)^d + \mathcal{O}(\rho_{N+1}^d) \leq \mathcal{R}(d,N) \leq (N+1)^d + \mathcal{O}(d\rho_{N+1}^d)$ *if* $C_{N+1} = \frac{1}{N+1}$;

(3) $\mathcal{R}(d,N) = (N+1)^d + \mathcal{O}(\rho_{N+1}^d)$ *if* $C_{N+1} < \frac{1}{N+1}$.

Proof. Note that $\mathcal{R}(d,N) - (N+1)^d$ is the number of reducible polynomials in $S(d,N)$. Bounding the number of reducible polynomials in $S(d,N)$ below by the number of polynomials in $S(d,N)$ that are divisible by $1+x$, we immediately obtain the desired lower bound in all cases of C_{N+1}.

We will now prove the desired upper bound. Observe that the number of reducible polynomials in $S(d,N)$ is bounded above by the sum

$$\sum_{\substack{f \in S(d,N) \\ \deg(f) \leq \frac{d}{2}}} \Big| \{P \in S(d,N) : f \mid P, f \neq P\} \Big| = \left(\sum_{\substack{f \in S(d,N) \\ \deg(f) \leq \frac{d}{2}}} \Big| \{P \in S(d,N) : f \mid P\} \Big| \right) - (N+1)^{\frac{d}{2}+1}.$$

Note that

$$\sum_{\substack{f \in S(d,N) \\ \deg(f) \leq \frac{d}{2}}} \Big| \{P \in S(d,N) : f \mid P\} \Big| \leq_d \sum_{1 \leq k \leq \frac{d}{2}} N^2 (N+1)^{k-1} \cdot \rho_{N+1}^{d+1} \cdot C_{N+1}^k$$

by Proposition 5.7 and the fact that there are $N^2(N+1)^{k-1}$ polynomials in $S(d,N)$ degree exactly k. We have

$$\sum_{1 \leq k \leq \frac{d}{2}} N^2 (N+1)^{k-1} \cdot C_{N+1}^k = \frac{N^2}{N+1} \sum_{1 \leq k \leq \frac{d}{2}} ((N+1) C_{N+1})^k.$$

Observe that

$$\sum_{1 \leq k \leq \frac{d}{2}} ((N+1) C_{N+1})^k = \begin{cases} \mathcal{O}((N+1)^{\frac{d}{2}} C_{N+1}^{\frac{d}{2}}) & C_{N+1} > \frac{1}{N+1} \\ \mathcal{O}(d) & C_{N+1} = \frac{1}{N+1} \\ \mathcal{O}(1) & C_{N+1} < \frac{1}{N+1} \end{cases}$$

as $d \to \infty$. Therefore, the desired upper bounds follow for all cases of C_{N+1}. □

As a corollary, we have the following precise asymptotic for the number of 0-1 polynomials of degree at most d.

Corollary 5.6. *We have* $\mathcal{R}(d,1) = 2^d + \mathcal{O}(\varphi^d)$ *as* $d \to \infty$.

Proof. By virtue of Theorem 5.5, it suffices to show that $C_2 < \frac{1}{2}$. This follows from the fact that $C_2 = \frac{1}{\varphi\sqrt{5}} < \frac{1}{2}$. □

5.2. Asymptotics for $N \to \infty$.

Proposition 5.7. *Let* a *and* b *be positive integers at most* N. *Then, there exists a constant* C_d *dependent only on* d *such that the number of polynomials in* $S(d,N)$ *that are divisible by the binomial* $a+bx$ *is at most* $N^d/a^d + C_d \cdot N^{d-1}/a^{d-1}$ *as* $N \to \infty$.

Proof. Let $\mathcal{L}$ denote the lattice generated by the set

$$\{(a, b, 0, \ldots, 0),\ (0, a, b, 0, \ldots, 0),\ \ldots, (0, \ldots, 0, a, b),\ (0, \ldots, 0, a)\} \subseteq \mathbb{N}_0^d.$$

The points in $\mathcal{L}$ represent the first d coefficients of polynomials in $S(d, N)$ that are divisible by $a + bx$. As such, the number of polynomials in $S(d, N)$ that are divisible by $a + bx$ is equal to $|[0, N]^d \cap \mathcal{L}|$. Note that the volume of the basis vectors of $\mathcal{L}$ is given by

$$\begin{vmatrix} a & b & 0 & \ldots & 0 \\ 0 & a & b & \ldots & 0 \\ & & & \vdots & \\ 0 & 0 & 0 & \ldots & a \end{vmatrix} = a^d.$$

Thus, by the Davenport's Lemma [**Davenport˙Browning˙2005**], we have $|[0, N]^d \cap \mathcal{L}| \leq \frac{N^d}{a^d} + C_d \cdot \frac{N^{d-1}}{a^{d-1}}$ for some constant C_d dependent only on d as $N \to \infty$ as desired. □

Remark 5.8. We briefly remark that the lattice point interpretation of divisibility over $\mathbb{N}_0[x]$ has been used in the context of factorization algorithms over boolean polynomials; we refer the reader to [**Kim2005**] for more details.

Proposition 5.9. *Let $f(x) \in \mathbb{N}_0[x]$ be a polynomial with constant coefficient $a \in (0, N]$ and leading coefficient $b \in (0, N]$. Then, there exists a constant $C_{d,k}$ dependent only on d and k such that the number of polynomials in $S(d, N)$ that are divisible by $f(x)$ is at most $N^{d-k+1}/a^{d-k+1} + C_{d,k} \cdot N^{d-k}/a^{d-k}$ as $N \to \infty$.*

Proof. Note that the number of polynomials in $S(d, N)$ that are divisible by $f(x)$ is at most the number of polynomials in $S(d, N)$ that are divisible by $a + bx^k$. For $0 \leq i \leq k - 1$, set

$$g_i(x) := \sum_{m \equiv i \bmod k} ([x^m]g(x)) \cdot x^m$$

for all polynomials $g(x) \in \mathbb{N}_0[x]$. Since $\sum_{i=0}^{k-1} \deg(g_i) = \deg(g) + 1 - k$ for all $g(x) \in \mathbb{N}_0[x]$, the desired result follows from Proposition 5.7. □

Theorem 5.10. *For all $d \geq 6$, we have $\mathcal{R}(d, N) = \mathcal{O}(N^d)$ as $N \to \infty$.*

Proof. Note that when $b \geq a$, the number of polynomials in $S(d, N)$ that are divisible by $f(x) = a + \cdots + bx^k$ is at most $N^{d-k+1}/b^{d-k+1} + C_d \cdot N^{d-k}/b^{d-k}$, as the number of polynomials in $S(d, N)$ that are divisible by $f(x)$ is the same as the number of those that are divisible by the polynomial $g(x) = b + \cdots + ax^k$ whose coefficients are the same as that of $f(x)$ but reversed in order. Thus, the number of polynomials in $S(d, N)$ that are divisible by a polynomial $x \nmid f(x)$ of degree k is at most

$$\begin{aligned} 2\sum_{a=1}^{N}\sum_{b=1}^{a}\left(\frac{N^{d-k}}{a^{d-k}} + C_{d,k} \cdot \frac{N^{d-k+1}}{a^{d-k+1}}\right) &= 2\sum_{a=1}^{N}\left(\frac{N^{d-k}}{a^{d-k-1}} + C_{d,k} \cdot \frac{N^{d-k+1}}{a^{d-k}}\right) \\ &\leq 2N^{d-k}(\zeta(d-k-1) + NC_{d,k} \cdot \zeta(d-k)) = \mathcal{O}(N^{d-k+1}), \end{aligned}$$

as long as $d - k - 1 \geq 2$. Summing over $1 \leq k \leq d/2$ returns a final upper bound of $\mathcal{O}(N^d)$. □

Kuba [**kuba**] showed that in the context of $\mathbb{Z}[x]$, one has $\mathcal{R}(d, N) = \mathcal{O}(N^d)$ as the pair (d, N) approaches (∞, ∞). We conjecture that the same holds over $\mathbb{N}_0[x]$.

Conjecture 5.11. *The number of reducible polynomials in $\mathbb{N}_0[x]$ of degree at most d and height at most N is $\mathcal{O}(N^d)$ as (d, N) approaches (∞, ∞).*

Now that we have found asymptotic bounds on $\mathcal{R}(d, N)$ for both $d \to \infty$ and $N \to \infty$, we have the following corollary, which partially resolves Conjecture 5.11.

Corollary 5.12. *The number of reducible polynomials $\mathcal{R}(d, N)$ in $\mathbb{N}_0[x]$ of degree at most d and height at most N satisfies*

$$\mathcal{R}(d, N) = \mathcal{O}(N^d) \qquad N \to \infty, \text{ then } d \to \infty$$

and

$$\mathcal{R}(d, N) = \mathcal{O}(N^d) \qquad d \to \infty, \text{ then } N \to \infty.$$

Proof. The first bound readily follows from Theorem 5.10. Since $\rho_{N+1} \geq \frac{N}{2} + 1 > \sqrt{N+1}$ by the Rayleigh quotient bound [**HornJohnson2013**], the second asymptotic follows from Theorem 5.5. □

We also have the following $\mathbb{N}_0[x]$-analogue of the heuristic proposed by Borst et al. in [**Borst**].

Corollary 5.13. *Let $\mathcal{RL}(d, N)$ denote the number of reducible polynomials in $\mathbb{N}_0[x]$ of degree at most d and height at most N which are divisible by a factor of the form $a + bx$ for positive integers a and b. Then for all $d \geq 6$, we have*

$$\lim_{N \to \infty} \frac{\mathcal{RL}(d, N)}{\mathcal{R}(d, N)} = 1.$$

Proof. By Proposition 5.7, the number of reducible polynomials in $\mathbb{N}_0[x]$ of degree at most d and height at most N which are divisible by is $N^d + \mathcal{O}(N^{d-1})$ as $N \to \infty$. Thus, $\mathcal{RL}(d, N) \geq N^d + \mathcal{O}(N^{d-1})$ as $N \to \infty$, so by Theorem 5.10, the desired result follows. □

6. Irreducible Polynomials with Prescribed Coefficients

We conclude by examining the existence of irreducible polynomials subject to prescribed coefficient constraints. Probabilistically, this corresponds to conditioning the ambient distribution on finitely many coordinates and testing the stability of irreducibility under local restrictions. In particular, we prove in Proposition 6.2 that after prescribing all but one coefficient of a polynomial, irreducibility in $\mathbb{N}_0[x]$ can still be achieved by a suitable choice of the remaining coefficient. As an application, we offer a shorter proof for an analogue of the Goldbach conjecture in the context of $\mathbb{N}_0[x, x^{-1}]$ as formulated in [**kaplanpolo**, **sophialiao**].

Definition 6.1. We say that a nonzero polynomial $f \in \mathbb{N}_0[x]$ is *monolithic* if $f = gh$ implies that either g or h is a monomial of $\mathbb{N}_0[x^{\pm 1}]$.

Observe that since all monomials are units in $\mathbb{N}_0[x^{\pm 1}]$, monolithic polynomials are essentially the subset of irreducible polynomials of $\mathbb{N}_0[x^{\pm 1}]$ which lie in $\mathbb{N}_0[x]$.

Proposition 6.2. *Fix $c_i \in \mathbb{N}_0$ for each $i \in [\![0, d]\!]$ except $i = k$ for some $k \in \mathbb{N}_0$. Then there exists $N \in \mathbb{N}$ such that for all $n \geq N$, the polynomial $f = c_d x^d + c_{d-1} x^{d-1} + \cdots + c_0$ with $c_k = n$ is monolithic.*

Proof. Set $N \coloneqq (n+1)(m+1)^2$ where m is the maximum of the set coefficients. Again suppose for the sake of contradiction that there exists some $n \geq N$ where the polynomial f as expressed above with $c_k = n$ is not monolithic. Then f must be able to be expressed as gh for some non-constant polynomials $g = a_0 + a_1 \dots a_j x^j$ and $h = b_0 + b_1 \dots b_{d-j} x^{d-j}$. Then since

$$c_k = \sum_{i=0}^{k} a_i b_{k-i} \leq (k+1)m^2 < (n+1)(m+1)^2,$$

we have that there must be some coefficient of g or h that is greater than m. However in this case since g and h have at least one other term with non-zero coefficient we would have some other coefficient of f be greater than m, contradiction. Hence f is monolithic and we are done. □

Remark 6.3. In fact, we can prove that there exists a much tighter bound to N. Let $N = \lfloor (d+2)m^2/2 \rfloor + 1$ where m is the maximum number of the set of fixed coefficients $\{c_0, c_1 \dots c_k, c_{k+1} \dots c_d\}$. We prove that the proposition holds for all $n \geq N$. Suppose for the sake of contradiction that f is not monolithic, and it can be expressed as the product of two nonnegative integer coefficient polynomials

$$a(x)b(x) = (a_0 + a_1 x + \cdots + a_j x^j)(b_0 + b_1 x + \cdots b_{n-j} x^{d-j})$$

where j is some nonnegative integer less than d. Then we can write

$$c_k = \sum_{i=0}^{k} a_i b_{k-i}$$

where a_i (resp. b_i) is equal to zero if $i > j$ (resp. $i > d - j$). Without loss of generality let $j < d - j$ then $j \leq \lfloor n/2 \rfloor$ and so we can rewrite

$$c_k = \sum_{i=0}^{j} a_i b_{k-i}.$$

Since $c_k = N$ and we are summing $\lfloor (d+2)/2 \rfloor$ products, by the Pigeonhole Principle we must have $a_l b_{k-l} > m^2$ for some $l \in [\![0, j]\!]$, and so we have $a_l > m$ or $b_{k-l} > m$. If $a_l > m$ (resp. $b_{k-l} > m$) and $b(x)$ (resp. $a(x)$) is not a monomial, there would be some other nonzero coefficient $b_{l'}$ with $l' \neq k - l$ (resp. $a_{l'}$ with $l' \neq l$) resulting in $c_{l+l'}$ (resp. $c_{k-l+l'}$) greater than m, contradiction. Hence f must be monolithic.

Observe that this bound on N is sharp: if we consider quadratics $ax^2 + bx + c$ in $\mathbb{N}_0[x]$ with $a, c = 1$ the bound would give us $N = 2m^2 + 1 = 3$. If we took $n = N - 1$, $x^2 + 2x + 1$ fails for obvious reasons.

Note that this bound is not optimal. In particular, we provide a refined bound for the specific case of fixing all coefficients except the leading coefficient or the constant term in the following proposition.

Proposition 6.4. *Let $c_0, \dots, c_k \in \mathbb{N}$ be fixed. Then there exists $N \in \mathbb{N}$ such that, for all $n \geq N$, the polynomials*

$$f_n = nx^{t_{k+1}} + c_k x^{\mathcal{T}_k} + \cdots + c_0 \quad \text{and} \quad g_n = c_k x^{\mathcal{T}_k} + \cdots + c_0 x^{t_0} + n$$

are monolithic.

Proof. Set $N \coloneqq \max(c_0,\dots,c_k)^2+1$. Suppose towards a contradiction that the polynomial f_n (resp., g_n) is not monolithic for some $n \geq N$. Then we have $f_n = gh$ (resp., $g_n = gh$), where neither g nor h is a monomial. Hence we may assume that the leading coefficient (resp., independent term) of g is bigger than or equal to $\sqrt{n}$. Since h is a not a monomial, one of the coefficients $c_0,\dots,c_k$ is bigger than or equal to $\sqrt{n}$. Thus, for some $i \in [\![0,k]\!]$, we obtain the inequality

$$c_i \geq \sqrt{n} \geq \sqrt{N} > \sqrt{\max(c_0,\dots,c_k)^2} = \max(c_0,\dots,c_k) \geq c_i,$$

which is impossible. Therefore f_n and g_n are both monolithic for all $n \geq N$. □

Corollary 6.5. *Let $c_0,\dots,c_k \in \mathbb{N}$ be fixed. For a prime number $p \in \mathbb{P}$, the polynomials*

$$px^{t_{k+1}} + c_k x^{\mathcal{T}_k} + \cdots + c_0 \quad \text{and} \quad c_k x^{\mathcal{T}_k} + \cdots + c_0 x^{t_0} + p$$

are irreducible in $\mathbb{N}_0[x]$ provided that $p > \max(c_0,\dots,c_k)$.

We can now use Corollary 6.5 to provide a simpler proof of the fact that almost every Laurent polynomial can be written as the sum of at most two irreducibles.

Proposition 6.6. *Every $f \in \mathbb{N}_0[x^{\pm 1}]$ can be written as the sum of at most two irreducible polynomials provided that $|\mathsf{supp}(f)| > 1$ and $f(1) > 3$.*

Proof. Write $f = c_k x^k + \cdots + c_0$ with $c_0, c_k \in \mathbb{N}$ and $c_1,\dots,c_{k-1} \in \mathbb{N}_0$. Observe that, given a polynomial $g \in \mathbb{N}_0[x^{\pm 1}]$, if $g(1)$ is a prime number then g is irreducible. Consequently, we may assume that $f(1)$ is not the sum of at most two prime numbers. In particular, $f(1) > 6$. We have two possible cases.

Case 1: $c_i \leq 1$ for every $i \in [\![0,k]\!]$. Let p be the biggest prime number satisfying $p < f(1)-2$. Since there is a prime number between p and $2p$, the inequality $\frac{f(1)-2}{2} < p$ holds. Now either

$$\sum_{i=1}^{\lceil k/2\rceil-1} c_i \leq \frac{f(1)-2}{2} \quad \text{or} \quad \sum_{i=\lfloor k/2\rfloor+1}^{k} c_i \leq \frac{f(1)-2}{2}.$$

Without loss of generality, suppose that $\sum_{i=1}^{\lceil k/2\rceil-1} c_i \leq \frac{f(1)-2}{2}$. It is not hard to see that, for some index $t \in [\![\lfloor \frac{k}{2}\rfloor + 1, k]\!]$, we can write

$$f = [c_k x^k + \cdots + c_t x^t + c_0] + [c_{t-1}x^{t-1} + \cdots + c_1 x]$$

such that $\sum_{i=1}^{t-1} c_i = p$. Hence, both summands between brackets are irreducible.

Case 2: $c_i > 1$ for some $i \in [\![0,k]\!]$. Let p be the biggest prime number satisfying $p \leq \max(c_0,\dots,c_k)$. Now let u and v in $[\![0,k]\!]$ be the biggest index and the smallest index, respectively, satisfying $c_u \geq p$ and $c_v \geq p$. Note that if $u > v$ then we can write f as

$$\left(px^u + (c_v - p)x^v + \sum_{i=v+1}^{u-1} \left\lfloor \tfrac{c_i}{2} \right\rfloor x^i + \sum_{i=0}^{v-1} c_i x^i\right) + \left((c_u - p)x^u + px^v + \sum_{i=v+1}^{u-1} \left(c_i - \left\lfloor \tfrac{c_i}{2} \right\rfloor\right)x^i + \sum_{i=u+1}^{k} c_i x^i\right).$$

where both summands between brackets are irreducible by Corollary 6.5. For the rest of the proof, we may assume that $0 < v = u < k$. Observe that $c_u \leq 2p-2$. Without loss of

generality, assume that

$$0 < \sum_{i=0}^{u-1} c_i \leq \sum_{i=u+1}^{k} c_i.$$

There exists a prime number q satisfying

$$c_u - p + \sum_{i=0}^{u-1} c_i \leq q \leq 2c_u - 2p + 2\sum_{i=0}^{u-1} c_i \leq f(1) + c_u - 2p \leq f(1) - 2.$$

Now if $q \leq f(1) - p$ then we can write

$$f = \left[px^u + \sum_{i=u+1}^{k} d_i x^i \right] + \left[(c_u - p)x^u + \sum_{i=u+1}^{k} (c_i - d_i)x^i + \sum_{i=0}^{u-1} c_i x^i \right],$$

where $\sum_{i=u+1}^{k} d_i = f(1) - p - q$ and $0 \leq d_i \leq c_i$ for every $i \in [\![u+1, k]\!]$. Since the first summand between brackets is irreducible by Corollary 6.5, we are done. On the other hand, if $f(1) - p < q$ then, for some index $t \in [\![u+1, k]\!]$, we can write

$$f = [(f(1) - q - 1)x^u + x^t] + [f - (f(1) - q - 1)x^u - x^t],$$

where both summands between brackets are irreducible. □

Acknowledgments

The authors would like to thank their mentor, Dr. Harold Polo, for his constant and invaluable guidance and support throughout this research period. The authors extend their gratitude to the MIT PRIMES program for making this opportunity possible. Finally, the authors would like to thank Professor Nathan Kaplan for suggesting literature and interesting questions related to this project.