On the distribution of irreducible polynomials with positive integer coefficients

Neil Kolekar, Maiya Qiu, and Richard Wang
Mentor: Dr. Harold Polo

MIT PRIMES October Conference
October 18, 2025

Outline

Background

- An integral domain is a commutative ring R which has no zero divisors.
  - Multiplicative cancellativity: $ab = ac$ implies $b = c$ for all $a, b, c \in R$ with $a \neq 0$.
- A semidomain is a subset of an integral domain inheriting the same operations $(+, \cdot)$ and identities (resp. $0, 1$), and all axioms **with the exception of the additive inverse**.

Example

1. The integers $(\mathbb{Z}, +, \cdot)$ form an integral domain.
2. The nonnegative integers $\mathbb{N}_0$ form a semidomain, since they are a subset of $\mathbb{Z}$.

Extensions

- The polynomial extension of $\mathbb{N}_0$ (also called a polynomial semidomain):

$$\mathbb{N}_0[x] = \left\{ \sum_{k=0}^{d} c_k x^k \,\middle|\, d \in \mathbb{N}_0,\ c_k \in \mathbb{N}_0 \right\}.$$

- The formal power series extension of $\mathbb{N}_0$:

$$\mathbb{N}_0[\![x]\!] = \left\{ \sum_{k \in \mathbb{N}_0} c_k x^k \,\middle|\, c_k \in \mathbb{N}_0 \right\}.$$

Background

For an element $f = \sum_{k \in \mathbb{Z}} c_k x^k$ of $\mathbb{N}_0[x]$,
(Definitions extend to $\mathbb{N}_0[\![x]\!]$.)

- All standard terminology for polynomials (e.g. degree) applies. In particular, the height of a polynomial with integer coefficients is the maximum absolute value of its coefficients.
- The support of f is defined as $\operatorname{supp}(f) := \{k \in \mathbb{Z} \mid c_k \neq 0\}$.
- The polynomial f is monolithic if $f = gh$ ($g, h \in \mathbb{N}_0[x]$) implies one of g or h is a monomial.

  Ex. $2x^2 + 10x + 2$: monolithic, but not irreducible

Irreducibles in $\mathbb{N}_0[x] \subseteq \mathbb{Z}[x]$

We primarily study the distribution of irreducible polynomials in $\mathbb{N}_0[x]$, a subset of $\mathbb{Z}[x]$.

- The irreducibles in $\mathbb{Z}[x]$ are well-studied.
- Every irreducible in $\mathbb{Z}[x]$ continues to be irreducible in $\mathbb{N}_0[x]$, but the behavior of irreducibles in $\mathbb{N}_0[x]$ is also rather different.
  Ex. $x^3 + 1 = (x+1)(x^2 - x + 1)$ is irreducible in $\mathbb{N}_0[x]$

Proposition (well-known)

If $f \in \mathbb{N}_0[x]$ satisfies $f(n) \in \mathbb{P}$ for some $n \in \mathbb{N}$, then f is monolithic.

Proof: This is immediate by the fact that $f(n) = 1$ for some $n \in \mathbb{N}$ if and only if $f = x^k$ for some $k \geq 0$.

Irreducibles in $\mathbb{N}_0[x] \subseteq \mathbb{Z}[x]$

The converse of the previous proposition is false.

- There exist irreducible polynomials $f \in \mathbb{N}_0[x]$ such that $f(n) \notin \mathbb{P}$ for any $n \in \mathbb{N}$.
- The irreducible structure of $\mathbb{N}_0[x]$ is nontrivial and interesting to study.

Example

Let $f = x^6 + x^5 + x^3 + 1 \in \mathbb{N}_0[x]$. Observe that

$$f = (x+1)(x^2+1)(x^3 - x + 1),$$

where f is irreducible in $\mathbb{N}_0[x]$. Moreover, since $n+1,\ n^2+1 \geq 2$ for all $n \in \mathbb{N}$, it follows that $f(n)$ is composite for every $n \in \mathbb{N}$.

Furthermore, if $f \in \mathbb{N}_0[x]$ is irreducible but admits a factorization $f = gh$ in $\mathbb{Z}[x]$ with $g(n), h(n) \geq 2$ for all $n \in \mathbb{N}$, then $f(n)$ can never be prime.

Motivation

When studying the distribution of irreducibles one often computes the "density" of irreducibles.

- Intuition: measure the overall *proportion* of nonnegative integer polynomials which are irreducible.
- In our work, we use techniques for proving irreducibility to analyze this density in the context of $\mathbb{N}_0[x]$.
- Main result: we prove that almost all polynomials in $\mathbb{N}_0[x]$ are irreducible.

Past Work

Much work has been done on the density of irreducible polynomials in related domains.

Theorem [Hilbert, 1890s]

"Most" monic polynomials in $\mathbb{Z}[x]$ are irreducible, with their Galois group isomorphic to the symmetric group S_d.

Theorem [Kuba, 2009]

The number of polynomials in $\mathbb{Z}[x]$ of fixed degree d and height at most N reducible over $\mathbb{Q}[x]$ is $\mathcal{O}(N^d)$.

Past Results

Theorem [Borst et al., 2018]

The density of reducible polynomials f with "well-behaved" coefficients divisible by a factor of the form $a + bx^k$, where $k = \min(\mathrm{supp}(f) \setminus \{0\})$, is equal to 1.

Theorem [Antoniou et al., 2022]

The density of irreducibles of $\mathbb{F}_q[S]$, where S is a numerical semigroup and q a prime power, is zero.

This Work: Focusing on $\mathbb{N}_0[x]$

Little research has been done regarding the density of irreducibles in $\mathbb{N}_0[x]$.

We aim to characterize the irreducible structure of the less-studied $\mathbb{N}_0[x]$, largely by extending existing results about $\mathbb{Z}[x]$.

- Known: the atomic density of $\mathbb{Z}[x]$ is 1.
- We show that the same holds for $\mathbb{N}_0[x]$.

How to Measure Atomic Density?

We want to extend the idea of a simple proportion to work with infinity:

- *How do we measure the asymptotic density of irreducibles in semidomains such as* $\mathbb{N}_0[x]$*?*
- To get an idea of how to measure atomic density, we may first consider the semidomain $\mathbb{N}_0$ as a motivating example.

Example: Atomic density in $\mathbb{N}_0$.

Note that in $\mathbb{N}_0$, irreducibles equate primes. Then, one way to define the asymptotic density of irreducibles is

$$\lim_{N\to\infty} \frac{\pi(N)}{N+1},$$

where π is the prime-counting function. $\pi(N) \sim \frac{N}{\log N}$, so

$$\frac{\pi(N)}{N+1} \sim \frac{1}{\log N} \to 0 \quad \text{as } N \to \infty.$$

Note that other notions of density may lead to different values for density.

New Notations for $\mathbb{N}_0[x]$

Let us define some new notations for $\mathbb{N}_0[x]$. Take nonnegative integers $d, N \in \mathbb{N}_0$.

- $\mathcal{T}(d, N)$ denotes the number of polynomials in $\mathbb{N}_0[x]$ of degree at most d with coefficients bounded above by N.
- $\mathcal{I}(d, N)$ is defined analogously but for irreducible polynomials.
- $\mathcal{R}(d, N)$ for reducible polynomials.

Observation

$$\mathcal{I}(d, N) + \mathcal{R}(d, N) = \mathcal{T}(d, N) = (N + 1)^{d+1}$$

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

Definition

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 iterated limits exist and agree.

Remarks

- A similar notion applies to $\mathbb{Z}[x]$, hence our adoption of this definition.
- In practice, we will be computing the limit of $1-\dfrac{\mathcal{R}(d,N)}{\mathcal{T}(d,N)}$.

Main Result

Theorem (Kolekar-Qiu-Wang, 202?)

The atomic density of $\mathbb{N}_0[x]$ is 1. Specifically, $\mathcal{R}(d, N) = \mathcal{O}(N^d \log^2 N)$.

Sketch of proof:

1. Clearly, $\frac{1}{N+1}$ of polynomials in $\mathbb{N}_0[x]$ are divisible by x, and this fraction goes to 0 as $N \to \infty$.
2. For the remaining polynomials, we use coefficient bounding on the reducibles among them to show that these also have density 0.
3. The factor of $\log^2 N$ comes from the fact that $(\frac{1}{1} + \cdots + \frac{1}{N})^2 = \mathcal{O}(\log^2 N)$.

Conjecture (Kolekar-Qiu-Wang, 202?)

As $N, d \to \infty$, $\mathcal{R}(d, N) = \mathcal{O}(N^d)$ as $N, d \to \infty$ holds in $\mathbb{N}_0[x]$. [a]

[a] Based on the work of Kuba, who proved an analogous result for $\mathbb{Z}[x]$.

Numerical Data of Atomic Density in $\mathbb{N}_0[x]$

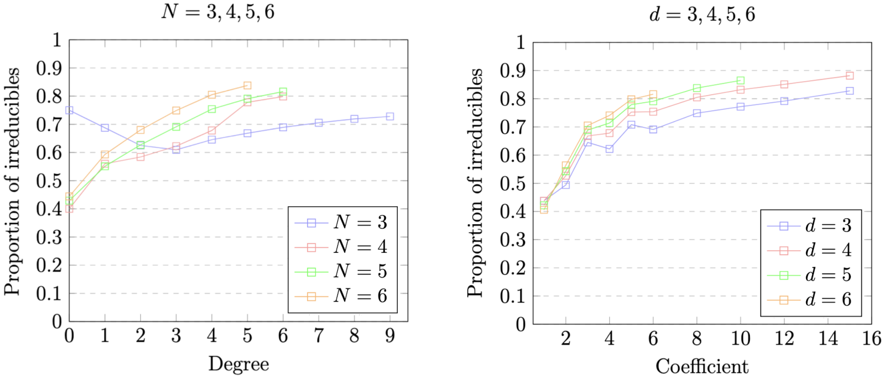

Figure 1: Graph of atomic density in $\mathbb{N}_0[x]$ for low degree and coefficient bounds

Conclusions

Main Result

- We showed that the atomic density of $\mathbb{N}_0[x]$ is 1.

Extensions

- We extended our atomic density results in $\mathbb{N}_0[x]$ to the power series semidomain $\mathbb{N}_0[\![x]\!]$.
- Going beyond considering the overall proportion, we found refined asymptotics for the number of reducibles with bounded coefficient and degree.
- We also considered the atomic density in certain subsets of $\mathbb{N}_0[x]$ as well as related semidomains, producing results analogous to findings in $\mathbb{Z}[x]$ [Konyagin, 1999].

Future Work

- Currently, we are considering an unsolved problem concerning $\mathbb{Z}[x]$ on the distance between irreducibles by Turán and extending it to $\mathbb{N}_0[x]$.
- Atomic density measures the *global* proportion of irreducibles, while Turán's problem focuses on their *local* distribution.
- We hope to ultimately find a direct connection between this problem on irreducibles' distance and overall atomic density.

References

Antoniou, A., Edmonds, R., Kubik, B., O'Neill, C., and Talbott, S. (2022).
On atomic density of numerical semigroup algebras.
Journal of Commutative Algebra, 14(4):455 – 470.

Borst, C., Boyd, E., Brekken, C., Solberg, S., Wood, M. M., and and, P. M. W. (2018).
Irreducibility of random polynomials.
Experimental Mathematics, 27(4):498–506.

Konyagin, S. V. (1999).
On the number of irreducible polynomials with 0,1 coefficients.
Acta Arithmetica, 88(4):333–350.

Kuba, G. (2009).
On the distribution of reducible polynomials.
Mathematica Slovaca, 59(3):349–356.

Acknowledgements

We thank our mentor Dr. Harold Polo for his guidance and support in our research, as well as Nathan Kaplan for recommending recent work relevant to this project and for his comments.

We would also like to thank the MIT PRIMES program for the amazing opportunity to conduct research.

Finally, we are incredibly grateful to the organizers of this conference for making it possible for us to present these results.

Thank you!