On the Irreducibles of $\mathbb{N}_0[x]$ and $\mathbb{N}_0[\![x]\!]$

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

Summer Workshop for Intrepid Mathematicians (SWIM)

August 29, 2025

Outline

Motivation

- In the 1890s, Hilbert showed that "most" monic polynomials in $\mathbb{Z}[x]$ are irreducible with their Galois group isomorphic to the symmetric group S_d.
- Later, Kuba refined this result by proving that the number of (not necessarily monic) polynomials in $\mathbb{Z}[x]$ of fixed degree d and height at most N that are reducible over $\mathbb{Q}[x]$ is $\mathcal{O}(N^d)$.
- Borst et al. proposed a heuristic suggesting that the density of reducible polynomials f with "well-behaved" coefficients that are divisible by a factor of the form $a + bx^k$, where $k = \min(\operatorname{supp}(f) \setminus \{0\})$, is equal to 1.
- 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, meaning that, asymptotically, almost all elements of fixed degree are reducible.

General Notation

- $\mathbb{Z}$ is the set of integers.
- $\mathbb{N}$ is the set of positive integers.
- $\mathbb{N}_0$ is the set of nonnegative integers.
- $\mathbb{P}$ is the set of prime numbers.
- $\mathbb{Q}$ is the set of rational numbers.
- $\mathbb{Q}_{\geq 0}$ is the set of nonnegative rational numbers.

Background

- A monoid is a pair $(M, +)$ consisting of a set M and an associative binary operation $+$ such that M is closed under $+$ and has an identity $0 \in M$. In our work, we assume that $+$ is commutative and cancellative.
- A unit is an element $u \in M$ such that there exists some $v \in M$ satisfying $u + v = 0$. The set of units of M is denoted as $\mathcal{U}(M)$.

Examples

1. The nonnegative integers $\mathbb{N}_0$ form an additive monoid with identity 0.
2. The set of rationals with absolute value at most 1 is a multiplicative monoid whose units are ± 1.

Background

Let M be a monoid.

- An atom, or irreducible, is an element $a \in M$ such that if $a = x + y$ for some $x, y \in M$, then $x \in \mathcal{U}(M)$ or $y \in \mathcal{U}(M)$. The set of atoms of M is denoted as $\mathcal{A}(M)$.
- M is called atomic if every element of $M \setminus \mathcal{U}(M)$ can be expressed as a finite sum of atoms.

Examples

1. The positive integers $(\mathbb{N}, \cdot)$ form an atomic monoid with $\mathcal{A}(\mathbb{N}) = \mathbb{P}$.
2. $(\mathbb{Q}_{\geq 0}, +)$ is an example of a non-atomic monoid.

Background

- A commutative semiring is a triple $(R, +, \cdot)$ satisfying the following properties:
  - $(R, +)$ is a monoid with identity 0.
  - $(R, \cdot)$ is a (not necessarily cancellative) monoid with identity 1.
  - $a(b + c) = ab + ac$ for all $a, b, c \in R$.
- A commutative ring is a commutative semiring such that $(R, +)$ is an abelian group.
- An integral domain is a commutative ring such that the monoid $(R \setminus \{0\}, \cdot)$ is cancellative.

Example

The integers $(\mathbb{Z}, +, \cdot)$ form an integral domain.

Note: Moving forward, we will assume that semirings and rings are commutative.

Background

Let $(S, +, \cdot)$ be a (commutative) semiring with additive identity 0 and multiplicative identity 1.

- A subset $S' \subseteq S$ is a subsemiring if $(S', +, \cdot)$ is a semiring with the same identities as S.
- A semidomain is a subsemiring of an integral domain.
- $\mathcal{U}(S)$ and $S^\times$ denote the additive and multiplicative units of S.
- A semidomain is additively reduced provided that $\mathcal{U}(S) = \{0\}$.
  Ex. $\mathbb{N}_0$
- $\mathcal{A}_+(S)$ and $\mathcal{A}_\times(S)$ denote the additive and multiplicative atoms of S.

Examples of semidomains

1. The nonnegative integers $(\mathbb{N}_0, +, \cdot)$
2. The nonnegative rationals $(\mathbb{Q}_{\geq 0}, +, \cdot)$

Extensions

- The polynomial extension of a semidomain S is the semidomain

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

Ex. $\mathbb{N}_0[x]$: polynomials with nonnegative integer coefficients

- The formal power series extension of S is the semidomain

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

Ex. $\mathbb{N}_0[\![x]\!]$: power series with nonnegative integer coefficients

Remark: The Laurent polynomial (resp. series) extension of S is obtained by allowing for negative exponents in $S[x]$ (resp. $S[\![x]\!]$) and is denoted as $S[x^{\pm 1}]$ (resp. $S[\![x^{\pm 1}]\!]$).

Background

Let $S[x]$ be a polynomial semidomain. (Definitions extend to $S[x^{\pm 1}]$, $S[\![x]\!]$, $S[\![x^{\pm 1}]\!]$.)

- The elements of $S[x]$ are polynomials, and thus all standard terminology for polynomials, such as degree, applies to elements of $S[x]$.
- The support of a polynomial or series $f = \sum_{k \in \mathbb{Z}} c_k x^k \in S[x]$ is defined as $\mathsf{supp}(f) := \{k \in \mathbb{Z} \mid c_k \neq 0\}$.
- An element $f \in S[x]$ is monolithic if, whenever $f = gh$ with $g, h \in S[x]$, at least one of g or h is a monomial.

  Ex. $2x^2 + 10x + 2$: monolithic in $\mathbb{N}_0[x]$, but not irreducible

$$\textit{monolithic} + \gcd(\textit{coefficients}) = 1 \iff \textit{irreducible}$$

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

While all irreducibles in $\mathbb{Z}[x]$ remain irreducible in $\mathbb{N}_0[x]$, the structure of $\mathbb{N}_0[x]$ also introduces significant departures from the familiar behavior of irreducibles in $\mathbb{Z}[x]$.

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

Corollary

If $f \in \mathbb{N}_0[x^{\pm 1}]$ with setwise coprime coefficients satisfies $f(n) \in \mathbb{P}$ for some $n \in \mathbb{N}$, then f is irreducible.

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

The converse is false; there exist irreducible polynomials $f \in \mathbb{N}_0[x]$ such that $f(n) \notin \mathbb{P}$ for any $n \in \mathbb{N}$.

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.

Irreducibility in $\mathbb{N}_0[x]$

A useful tool for proving irreducibility in $\mathbb{N}_0[x]$ is the use of coefficient bounding.

Proposition (Kolekar-Qiu-Wang, 202?)

For any $k \in \mathbb{N}$, the polynomial $f(x) \in \mathbb{N}_0[x]$ is irreducible if and only if $f(x^k)$ is irreducible.

Proof: This proof uses basic coefficient bounding. The essence of the proof lies in the observation that if $f(x^k) = gh$, then $\mathsf{supp}(g) \cup \mathsf{supp}(h) \subseteq \mathsf{supp}(f(x^k))$, forcing $g(x^{1/k}), h(x^{1/k}) \in \mathbb{N}_0[x]$.

In general, the fact that $\mathbb{N}_0$ is additively reduced allows us to easily obtain lower bounds on the coefficients of reducible polynomials.

Irreducibility in $\mathbb{N}_0[\![x]\!]$

So far, we have discussed criteria for irreducibility in $\mathbb{N}_0[x]$. In fact, these carry over more or less unchanged to the context of $\mathbb{N}_0[\![x]\!]$.

Proposition (Kolekar-Qiu-Wang, 202?)

For any $k \in \mathbb{N}$, the series $f(x) \in \mathbb{N}_0[\![x]\!]$ is irreducible if and only if $f(x^k)$ is irreducible.

Corollary

When evaluating the irreducibility of a polynomial or series f, one may assume that the elements of $\mathsf{supp}(f)$ are setwise coprime.

Remark: It is easy to see that these criteria trivially generalize to the Laurent counterparts of these semidomains.

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

We investigate the asymptotic density of irreducibles in certain polynomial semidomains, taking $\mathbb{N}_0[x]$ as a primary example. But this raises a natural question: *how should one measure asymptotic density?*

Example

Consider the semidomain $\mathbb{N}_0$. 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

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

We note, however, that this is only one possible notion of density, and other definitions may lead to different perspectives.

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

We first need some notation. 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.
- $\mathcal{I}(d, N)$ denotes the number of irreducible polynomials in $\mathbb{N}_0[x]$ of degree at most d with coefficients bounded above by N.
- $\mathcal{R}(d, N)$ denotes the number of reducible polynomials in $\mathbb{N}_0[x]$ of degree at most d with coefficients bounded above by N.

These definitions also make sense in the context of Laurent polynomials with coefficients in $\mathbb{N}_0$.

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

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 can be defined for $\mathbb{Z}[x]$, and it is straightforward to verify that its atomic density equals 1.
- In practice, we will be computing the limit of $\dfrac{\mathcal{R}(d,N)}{\mathcal{T}(d,N)}$.

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

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; this fraction goes to 0.
2. For the remaining polynomials, examine the constant and leading terms, and apply coefficient bounding to the remaining terms to find that the reducibles among these polynomials 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?)

The number of reducibles in $\mathbb{N}_0[x]$ satisfies $\mathcal{R}(d, N) = \mathcal{O}(N^d)$ as $N, d \to \infty$.[a]

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

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

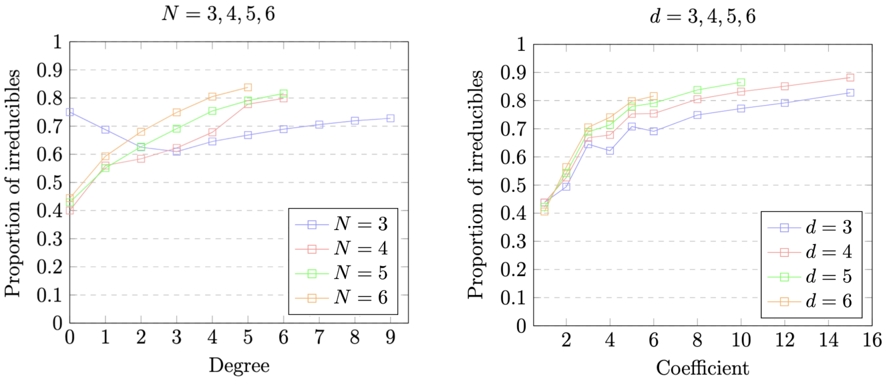


Figure 1: Graph of atomic density in $\mathbb{N}_0[x]$ for low degree and coefficient bounds

Density of Irreducibles in $\mathbb{N}_0[\![x]\!]$

Fix nonnegative integers $d, N \in \mathbb{N}_0$.

- The degree-d truncation of a power series is the polynomial obtained by keeping only the terms of degree $\leq d$.
- Let $\mathcal{I}_\infty(d, N)$ denote the number of polynomials $f \in \mathbb{N}_0[x]$ of degree at most d and height at most N that are *not* the degree-d truncation of some product gh, where g and h are non-units in $\mathbb{N}_0[\![x]\!]$.

Definition

The atomic density of $\mathbb{N}_0[\![x]\!]$ is defined as

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

if this limit exists.

Density of Irreducibles in $\mathbb{N}_0[\![x]\!]$

Theorem (Kolekar-Qiu-Wang, 202?)

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

Remark: While the distributions of irreducibles in $\mathbb{N}_0[x]$ and $\mathbb{Z}[x]$ still share some similarities, irreducibles in $\mathbb{N}_0[\![x]\!]$ and $\mathbb{Z}[\![x]\!]$ behave radically differently.

Example

Observe that $f = (1+x)(2+x)$ is reducible in $\mathbb{N}_0[\![x]\!]$ but irreducible in $\mathbb{Z}[\![x]\!]$ because $1+x$ is a unit. In fact, it can be shown that a series $f \in \mathbb{Z}[\![x]\!]$ with a prime constant term must be irreducible.

Atomic Density of 0-1 Polynomials

Definition

A 0–1 polynomial is a polynomial $f \in \mathbb{N}_0[x]$ with all coefficients in $\{0, 1\}$.

- In 1999, Konyagin studied 0–1 polynomials in the context of $\mathbb{Z}[x]$ using low degree factors to find the atomic density.
- More recent studies such as Borst et al. continue to find the asymptote of the proportion of irreducibles, accompanied with computer generated data.

0-1 Polynomials in $\mathbb{N}_0[x]$

Let $\mathcal{T}(d)$, $\mathcal{I}(d)$, and $\mathcal{R}(d)$ denote, respectively, the numbers of all, irreducible, and reducible polynomials in $\mathbb{N}_0[x]$ of degree at most d. Clearly, $\mathcal{T}(d) = 2^{d+1}$.

Definition

The atomic density of 0-1 polynomials is given by

$$\lim_{d\to\infty} \frac{\mathcal{I}(d)}{\mathcal{T}(d)},$$

provided that this limit exists.

Notice that a 0-1 polynomial is reducible over $\mathbb{N}_0[x]$ if and only if it is a product of nonconstant 0-1 polynomials.

Atomic Density of 0-1 Polynomials

Theorem (Kolekar-Qiu-Wang, 202?)

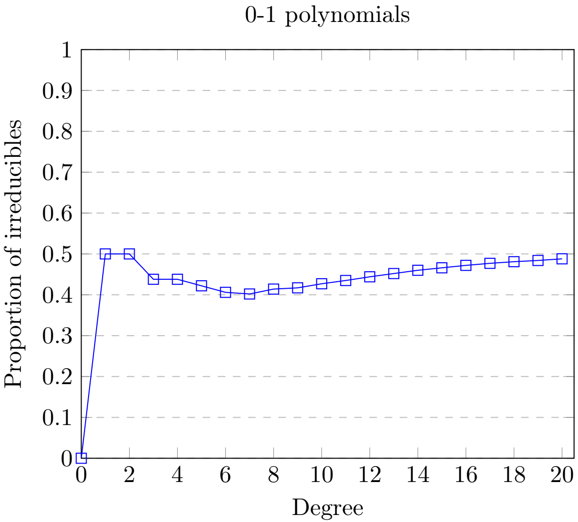
The number of reducible 0-1 polynomials of degree at most d satisfies $\mathcal{R}(d) = 2^d + \mathcal{O}(\varphi^d)$, where $\varphi \approx 1.618$ is the golden ratio.

The 2^d term trivially comes from polynomials of constant term 0. Meanwhile, the contribution of $\mathcal{O}(\varphi^d)$ derives itself from a Fibonacci bound on reducibles divisible by a binomial.

Corollary (Kolekar-Qiu-Wang, 202?)

The atomic density of the subset of 0-1 polynomials in $\mathbb{N}_0[x]$ is $\frac{1}{2}$.

Numerical Data of Atomic Density of 0-1 Polynomials



Atomic Density of 0-1 Power Series

The atomic density of 0-1 power series (power series with coefficients in $\{0, 1\}$) is defined analogously to $\mathbb{N}_0[\![x]\!]$, albeit with the coefficient bound removed.

Theorem (Kolekar-Qiu-Wang, 202?)

The atomic density of the subset of 0-1 power series in $\mathbb{N}_0[\![x]\!]$ is also $\frac{1}{2}$.

Corollary (Kolekar-Qiu-Wang, 202?)

The density of 0-1 power series f for which f has a finite factorization is $\frac{1}{2}$. (Equivalently, most reducible 0-1 power series can be expressed as the finite product of irreducibles).

Distance to an Irreducible

Turán's conjecture

There exists an absolute constant C such that for every polynomial $f \in \mathbb{Z}[x]$, there exists an irreducible polynomial $g \in \mathbb{Z}[x]$ with $\deg g \leq \deg f$ such that $|f - g| \leq C$.

Remarks:

- While the atomic density captures the *global* distribution of irreducibles, Turán's problem concerns their *local* distribution—a question that is considerably more difficult.
- Turán's conjecture holds ($C = 3$) once the irreducible polynomial g is allowed to have arbitrary degree.
- Original problem still of much interest. Numerical computations strongly suggest $C \leq 4$.

Distance to an Irreducible

Proposition (Kolekar-Qiu-Wang 202?)

For every polynomial $f \in \mathbb{N}_0[x]$, there exists an irreducible polynomial $g \in \mathbb{N}_0[x]$ such that $|f - g| \leq 2$.

Proof: For each polynomial f with constant term 0, we can let $g(x) = f(x) + 1 + x^k$ for sufficiently large k to obtain g irreducible.

Turán's conjecture for $\mathbb{N}_0[x]$. There exists an absolute constant C such that for every polynomial $f \in \mathbb{N}_0[x]$, there exists an irreducible polynomial $g \in \mathbb{N}_0[x]$ with $\deg g \leq \deg f$ such that $|f - g| \leq C$.

Remark: If a bound C exists for polynomials in $\mathbb{N}_0[x]$, then $C \geq 2$. Indeed, one may consider the example $f = 2x + x^2$.

Conjecture (Kolekar-Qiu-Wang, 202?)

The bound $C \leq 3$ holds for Turán's problem in $\mathbb{N}_0[x]$.

Turán's Problem in $\mathbb{N}_0[\![x]\!]$

- In light of the difficulty of Turán's problem in $\mathbb{N}_0[x]$, we now consider this same problem in $\mathbb{N}_0[\![x]\!]$.
- It turns out that in the case of power series, Turán's problem is false.

Proposition (Kolekar-Qiu-Wang, 202?)

For any $C \in \mathbb{N}$, there exists some $f \in \mathbb{N}_0[\![x]\!]$ whose distance to any irreducible is greater than C.

- Construction: consider $f = \frac{1}{1-nx} = 1 + nx + n^2x^2 + \cdots \in \mathbb{N}_0[\![x]\!]$ for arbitrarily large values of n.
- The key idea behind the proof is that any power series with increasing coefficients is divisible by $1 + x$.

Turán's Problem for 0-1 Polynomials

- Analogously to before, we consider the distance to irreducibles in the context of 0-1 polynomials.

Turán's problem for 0-1 polynomials

We wonder if, for any 0-1 polynomial f, there exists some irreducible 0-1 polynomial g such that $|f - g|$ is bounded.

- Note that each coefficient can be effectively "toggled" at most once, and we can also think about it as using the Hamming distance.

Turán's Problem for 0-1 Polynomials

- Restricting ourselves to 0-1 polynomials, we can sharpen the bound for C.

Proposition (Kolekar-Qiu-Wang, 202?)

If a bound C exists for 0-1 polynomials, then $C \geq 3$.

- For counterexamples, take $f = x + x^2 + \cdots + x^{n-1}$ for any composite n of the form $2^m - 1$ for $m \in \mathbb{N}$.
- One can prove that $f + 1 - x^k$ is divisible by the binomial $1 + x^{2^{\nu_2(k+1)}}$ for all $k \in [\![0, n-1]\!]$. Here, we use $2^{\nu_2(k+1)}$ to denote the greatest power of 2 dividing $k + 1$.
- The smallest working example occurs when $n = 15$.

Conjecture (Kolekar-Qiu-Wang, 202?)

The bound $C = 3$ holds for all 0-1 polynomials.

Turán's Problem for 0-1 Series

Turán's problem is resolved in the context of 0-1 power series.

Proposition (Kolekar-Qiu-Wang, 202?)

There exists a 0-1 series f (for example, consider the construction $f = 1 + x + x^2 + \cdots$) such that any 0-1 series g of finite distance from f is reducible.

It is in fact not hard to see that, for any finite subset $A \subseteq \mathbb{N}_0$, the 0-1 series $f - \sum_{k \in A} x^k$ is divisible by $1 + x^{\max(A)+1}$ and is thus reducible.

References

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.

Filaseta, M. and Mossinghoff, M. (2012).
The distance to an irreducible polynomial, ii.
Mathematics of Computation, 81:1571–1585.

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.
- We thank the MIT PRIMES Program for this opportunity to conduct research.
- We thank the SWIM organizers for making it possible for us to present in this workshop.

Thank you!