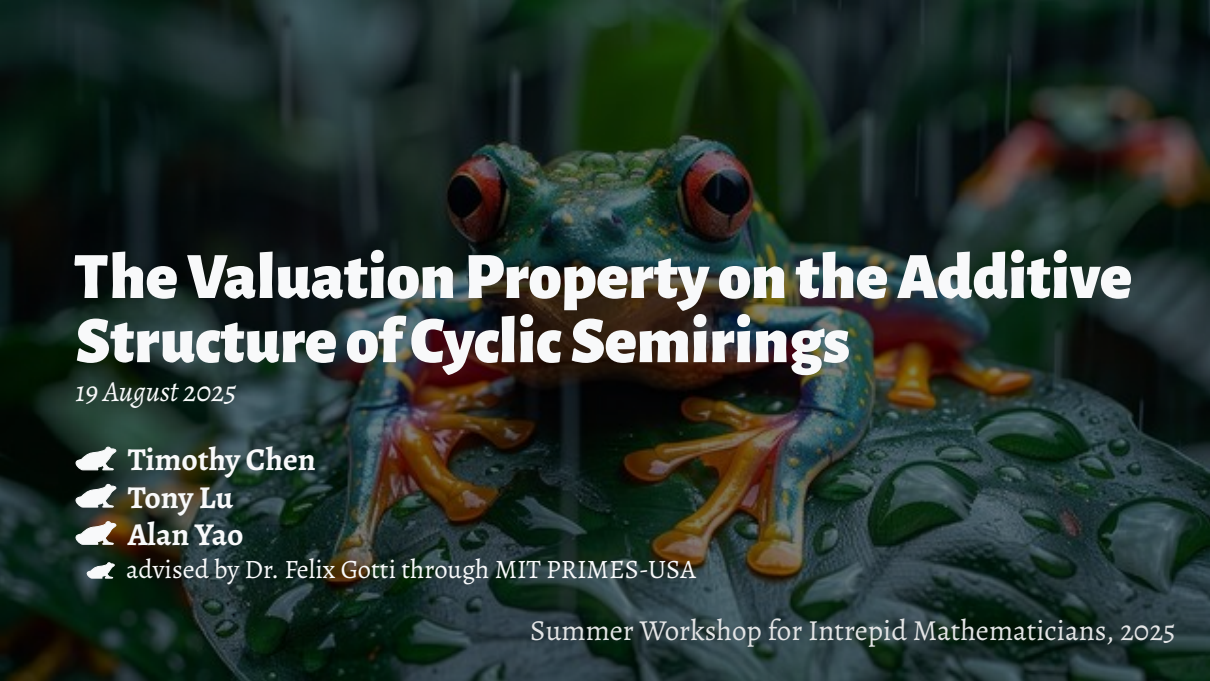

The Valuation Property on the Additive Structure of Cyclic Semirings

19 August 2025

- **Timothy Chen**
- **Tony Lu**
- **Alan Yao**
  - advised by Dr. Felix Gotti through MIT PRIMES-USA

Summer Workshop for Intrepid Mathematicians, 2025

Overview

The **valuation property** is an interesting topic in **semiring theory**. We completely characterize the additive monoids of **cyclic** semirings with this property in terms of other well-studied conditions and structures, and obtain results about the "density" of such valuation monoids.

$\mathbb{N}_0$ denotes the nonnegative integers, $\{0, 1, 2, \dots\}$. *What does* $\mathbb{N}_0$ *have?*

- It has an operation — **addition** $(+)$
  - *Commutativity*, so $a + b = b + a$
  - *Associativity*, so $a + (b + c) = (a + b) + c$
  - *Additive Identity*, so $a + 0 = a$

A **monoid** $(M, *)$ is a set M with a binary operation $*\colon M \to M$ satisfying these properties.

If the operations are clear, we refer to the entire monoid by just the set M itself.

- But, $\mathbb{N}_0$ is more than addition — it has **multiplication** $(\cdot)$
  - *Commutativity*, *Associativity*, and *Multiplicative Identity* $(a \cdot 1 = a)$
  - Both an additive and a multiplicative monoid!
  - Multiplication *distributes* over addition, so $a \cdot (b + c) = a \cdot b + a \cdot c$
- Together, these conditions make $\mathbb{N}_0$ a **semiring**
  - This blend leads to a very rich and interesting structure

(We use $\mathbb{N}$ to represent the positive integers, $\{1, 2, 3, \dots\} = \mathbb{N}_0 \setminus \{0\}$.)

$\mathbb{N}_0$ = *prototypical* semiring. What are some others?

- **Rings** are semirings with negatives (additive inverses)
  - Each a has $-a$ with $a + (-a) = 0$, so the additive monoid is an **abelian group**
  - $\mathbb{Z}$ — **(rational) integers**, i.e., $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$
  - $\mathbb{Q}$ — **rationals**
  - $\mathbb{R}$ — **reals**
  - $\mathbb{C}$ — **complex numbers**
  - $\mathbb{Z}[x]$ — **polynomials** with **integer coefficients**
    - Under standard polynomial addition and multiplication
  - $\mathbb{Z}[i]$ $(i^2 = -1)$ — **Gaussian integers** — $\{a + bi \mid a, b \in \mathbb{Z}\}$
  - $\mathbb{Z}[\omega]$ $(\omega^3 = 1 \neq \omega)$ — **Eisenstein integers** — $\{a + b\omega + c\omega^2 \mid a, b, c \in \mathbb{Z}\}$
- $\mathbb{N}_0[x]$ — semiring of polynomials with coefficients in $\mathbb{N}_0$

- What is $\mathbb{N}_0[i]$? Is the set $\{a + bi \mid a, b \in \mathbb{N}_0\}$ still what we want?
  - **No!** — not even a semiring since this lacks *multiplicative closure*
  - Cannot define multiplication because $i \cdot i = -1$ is not in the semiring
- Instead, explicitly define $\mathbb{N}_0[\alpha]$ as **smallest semiring containing α**
  - Formally, smallest by containment (but then, prove a minimal one exists)
- Hard to work with — explicit definition, no explicit construction
  - **Fact** — we can get $\mathbb{N}_0[\alpha]$ by evaluating any polynomial in $\mathbb{N}_0[x]$ at $x = \alpha$
  - One can show $\mathbb{Z}[i] = \{f(i) \mid f(x) \in \mathbb{Z}[x]\}$ and $\mathbb{Z}[\omega] = \{f(\omega) \mid f(x) \in \mathbb{Z}[x]\}$
- $\mathbb{N}_0[\alpha] = \{f(\alpha) \mid f(x) \in \mathbb{N}_0[x]\}$ — **evaluation semiring**
  - **Cyclic** — formed from a single element α
- **Fact** — additive monoid is **generated** by powers of α
  - $\mathbb{N}_0[\alpha]$ consists of all finite sum of **generators** α^k, e.g., $17 + 3\alpha^7 + \alpha^{2025}$
  - Non-uniquely — $\omega^6 + \omega^2 + 2\omega = \omega^4$ in the Eisenstein integers

Each of those three characterizations of $\mathbb{N}_0[\alpha]$ is useful.

- $\mathbb{N}_0[n] = \mathbb{N}_0 \implies n \in \mathbb{N}_0$ as, otherwise, the semiring must expand
- $\mathbb{N}_0[n] = \mathbb{N}_0 \impliedby n \in \mathbb{N}_0$ as it is the smallest semiring with n
- $\mathbb{N}_0[-1] = \mathbb{Z}$ as -1 generates all the negative integers
- $\mathbb{N}_0\left[\sqrt{2}\right] = \left\{a + b\sqrt{2} \;\middle|\; a, b \in \mathbb{N}_0\right\}$ as $\left(\sqrt{2}\right)^k$ is redundant for $k > 1$
- $\mathbb{N}_0\left[\frac{1}{2}\right] = \left\{\frac{a}{2^n} \;\middle|\; a, n \in \mathbb{N}_0\right\}$ since the $c_i x^i$ term in $f(x)$ maps to $\frac{c_i}{2^i}$
- They get scarier — we allow α to be any complex number

What is $\mathbb{N}_o[\pi]$?

- π is *transcendental* — it satisfies no algebraic relations (over $\mathbb{Q}$)
  - Where else do we see a variable with no algebraic relations? $\mathbb{N}_o[x]$
- x is a *formal indeterminate* — it also satisfies no algebraic relations
- $\implies \mathbb{N}_o[\pi] \cong \mathbb{N}_o[x]$, and the same for any transcendental
- The symbol $\cong$ means **isomorphic**, or *essentially the same*
  - Loosely speaking, the two structures have all the same algebraic properties
  - All we need is to relabel their elements for them to be identical
  - Formally, this relabeling is a **bijection** (one-to-one and onto) φ that satisfies $\varphi(a+b) = \varphi(a) + \varphi(b)$, $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$, $\varphi(0) = 0$, and $\varphi(1) = 1$
  - 0 and 1 are the additive and multiplicative identities of any general semiring

Why are semirings interesting?

- Interplay between additive and multiplicative structures
  - Related to much (Goldbach's conjecture, Fermat's Last Theorem, etc.)
- Natural setting to investigate factorization theory + divisibility
  - Applicable to commutative algebra (e.g., monoid algebras)
- Our research ties together many seemingly disparate areas
  - field + Galois theory,
  - theory of linear recurrences,
  - and linear algebra
- It is just cool!

- Exclusively focus on the **additive monoid** (set aside multiplication)
  - $M_\alpha := (\mathbb{N}_0[\alpha], +)$ — what terminology do we use to explore this structure?
- "a **divides** b" (or "$a \mid b$") if there exists some c with $a + c = b$
  - $2 \mid 3$ in any M_α because $2 + 1 = 3$
  - $a \mid a$ for every a because $a + 0 = a$
    - **Reflexivity** of divisibility
  - The additive identity divides everything because $0 + a = a$
  - If $a \mid b$ and $b \mid c$, then $a \mid c$ (since $a + b' = b$ and $b + c' = c$, so $a + b' + c' = c$)
    - **Transitivity** of divisibility
- "a is an **unit**" if a divides every other element
  - Unit $\iff$ divides the additive identity 0 — if $a \mid 0$, then $a \mid b$ because $0 \mid b$
  - α is positive $\implies$ M_α has only nonnegative elements $\implies$ the only unit is 0
    - "M_α is **reduced**" when no nonzero units — happens if (but not only if) $\alpha > 0$
  - An **abelian group** is where every element is a unit (each has a negative)

- "a is an **atom**" if non-unit & if $b + c = a$, then b or c is a unit
  - Also called "**irreducibles**" — all you can shave off are units, nothing sizable
  - If $\alpha > 1$, then 1 is an atom in M_α (meaning 1 has no interesting factorizations)
  - 2 is never an atom since $2 = 1 + 1$ (even if 1 is a unit, then $1 + 1$ is a unit)
- Atoms are similar to primes in the natural numbers
  - **Fundamental Theorem of Arithmetic** — every $n \in \mathbb{N}$ can be expressed uniquely as a product of primes; we call this unique factorization
  - Atoms are like the building blocks of a monoid
  - "$b \in M$ is **atomic**" if b is a unit or can be expressed as a finite sum of atoms
  - "M is **atomic**" if every element is atomic

- **Traditionally**, the focus is on the *factorization properties*
  - A **factorization** is writing something as a sum of atoms
  - We ask *is there unique factorization? If not, what is there?*
- Consider $M_{1/n}$ for any integer $n > 1$
  - E.g., $M_{1/2} =$ *dyadic rationals* — anything whose denominator is a power of two
  - For any a, $a = \frac{a}{2} + \frac{a}{2}$, so a is not an atom
  - $\implies$ no atoms, so no building blocks, and no factorizations!
  - So, $M_{1/n}$ is not atomic
- **Antimatter** — no atoms, no element has a factorization
  - Still an interesting case to study
  - Other examples — $\mathbb{Q}_{\geqslant 0}$, $\mathbb{Q}_{\geqslant 0} \cup \mathbb{R}_{>1}$, and many more

- But, $M_{1/1} = \mathbb{N}_0$ has atoms — find something of $M_{1/n}$ *for all* $n \in \mathbb{N}$
  - For **any** $n \in \mathbb{N}$, if $a, b \in M_{1/n}$, either $a \mid b$ or $b \mid a$
  - Clear in $\mathbb{N}_0$ since $|a - b| \in \mathbb{N}_0$, so the smaller divides the bigger
  - In $M_{1/2}$, $|a - b|$ is nonnegative and dyadic (denominator still a power of two)
- **Valuation property** — for any two elements, one divides the other
  - Alternatively, we say that any two elements are **comparable**
  - This makes divisibility a *total order* — everything fits on a line
- Any abelian group is valuation (everything divides everything else)
  - Valuation monoids are like "half" of an abelian group
- What is not a valuation monoid?
  - $M_{\sqrt{2}}$ is not — $\sqrt{2} \nmid 1$ (1 is the smallest positive element), but also $1 \nmid \sqrt{2}$
  - M_π is not — π^n is an atom for each $n \in \mathbb{N}_0$ — same for any transcendental
    - Atoms mess things up — in reduced monoids, atoms don't divide each other

Which M_α are valuation? Can M_α be valuation if α is irrational?

- **Yes.** $\varphi^{-1} = \dfrac{\sqrt{5}-1}{2}$, where φ is the golden ratio. *Proof.* Technical.
  - Can we delineate further than (ir)rational? Are they arbitrarily complicated?
- We use **rank** to measure this sense of "intricacy"
  - $M_{1/n}$ is rank one because $1/n$ is rational (if $n \in \mathbb{N}$)
  - $M_{\varphi^{-1}}$ is rank two because φ^{-1} satisfies a quadratic polynomial $x^2 + x - 1 = 0$
- Every algebraic α has a **minimal polynomial**, $m_\alpha(x) \in \mathbb{Q}[x]$
  - Monic (leading coefficient 1) polynomial of least degree with α as a root
  - "α is **algebraic**" if α satisfies a polynomial in $\mathbb{Q}[x]$ (else **transcendental**)
- "M_α is a monoid of **rank** r" if $\deg m_\alpha(x) = r$ (deg is the degree)
  - Not the most general definition of rank, but suffices here
  - Instead of (ir)rational, *are there ∞-ly many non-isomorphic valuation of each rank?*

We first address some algebraic considerations.

- **Transcendental = boring**, since never valuation
  - Other redundant cases?
- "α and β are **algebraic conjugates**" if $m_\alpha(x) = m_\beta(x)$
  - (and, both are algebraic)
  - e.g., $\sqrt{2}$ and $-\sqrt{2}$, or $7 + 17i$ and $7 - 17i$
- **Fact** — if $f(\alpha) = 0$ for $f(x) \in \mathbb{Q}[x]$, then $m_\alpha(x)$ is a factor of $f(x)$
- **Consequence** — if $f(\alpha) = 0$, then $f(\beta) = 0$
- Algebraic conjugates satisfy the same relations!
  - Do they generate the same monoids?

Theorem (Correa-Morris and Gotti, 2022)

If α and β are algebraic conjugates, then $M_\alpha \cong M_\beta$.

In fact, we can say more about algebraic conjugates.

- If α is positive, M_α is reduced… good!
  - If α has a positive conjugate, M_α is reduced… good!
- If α has no positive conjugates… opposite of reduced!

Theorem (Gotti, Hong, and Li, 202?)

If α is algebraic with no positive conjugates, then M_α is an abelian group.

Abelian groups are valuation $\Longrightarrow$ focus on **positive real algebraic α**.

More easy cases. Remember, $\alpha \in \mathbb{R}_{>0}$ is algebraic.

- If $\alpha \geqslant 1$, M_α is valuation $\iff$ α is an integer
  - *Proof.* Consider the atoms in M_α — if $\alpha \notin \mathbb{N}_0$, then 1 and α are atoms
  - In fact, M_α is valuation $\implies$ M_α antimatter (or $M_\alpha = \mathbb{N}_0$)
  - We therefore focus on **positive** $\alpha < 1$
- What if α is **rational** (take $q \in \mathbb{Q} \cap (0, 1)$)?
  - We already know M_q is valuation if $q^{-1} \in \mathbb{N}$ (the unit fractions)
  - What if $\mathsf{n}(q) \neq 1$, where $\mathsf{n}(q)$ is the numerator of q
  - In $M_{2/3}$, the generators are $\frac{2}{3}$, $\frac{4}{9}$, $\frac{8}{27}$, and so on
    - They are all even! Every element < 1 has an even numerator, but 1 is odd
  - So, 1 is an atom if $\mathsf{n}(q) \neq 1$
    - In fact, q^n is an atom for any $n \in \mathbb{N}_0$ by considering p-adic valuations
  - M_q **is valuation** $\iff q^{-1} \in \mathbb{N}$ (this idea of integers will return later)

Widely applicable theorem (e.g., to find when M_α is an abelian group)

Theorem (Descartes' Rule of Signs)

The number of sign changes in $f(x) \in \mathbb{R}[x]$ has the same parity and is at least the number of positive roots (counting multiplicity).

Polynomial	Sign Changes	Positive Roots
$x+1$	0	0
$x^3 - x^2 + x - 1 = (x^2+1)(x-1)$	3	1
$x^{2025} - 1$	1	1
$\pi x^{17} - x^7 + \frac{1}{7}$	2	0

Can we show α has no positive conjugate (aside from itself)?

- Essentially, can $m_\alpha(x)$ have > 1 positive root if valuation?
- If M_α is valuation, M_α is antimatter (since $\alpha < 1$)
  - 1 is not an atom $\implies$ we can write $1 = a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + \cdots + a_n\alpha^n$
  - Formally, $1 = h(\alpha)$ where $h(x) \in x\mathbb{N}_0[x]$ — **antimatter decomposition**
- $h(x) - 1$ has one sign change $\implies$ $h(x) - 1$ has 1 positive root
- But, $m_\alpha(x)$ is a factor of $h(x) - 1 \implies h(x) - 1$ has > 1 positive root
  - Because each root to $m_\alpha(x)$ is also a root to any of its multiples
- Contradiction!

Valuation $\implies$ α has one positive conjugate (itself)

- So, we know one thing that valuation implies
  - Cannot be sufficient — every rational has no conjugates (i.e., rank one)
- For rationals, recall $\alpha^{-1} \in \mathbb{N}$ — we must generalize the integers
  - "β is an **algebraic integer**" if $m_\beta(x) \in \mathbb{Z}[x]$
  - Agrees with the normal notion of integers for the rationals
    - 17 (as $m_{17}(x) = x - 17$), not $\frac{1}{7}$ (as $m_{1/7}(x) = x - \frac{1}{7}$)
  - φ as $\varphi^2 - \varphi - 1 = 0$ (recall $M_{\varphi^{-1}}$ is valuation)

Presented at SWIM < 2 weeks ago!

Theorem (D-D-G-L-P-V-Z, 2025)

*If $\alpha \in (0, 1)$ is algebraic, then M_α is **antimatter** if and only if*

- *α has no positive conjugate aside from itself,*
- *α^{-1} is an algebraic integer,*
- *$|\rho| \leqslant \alpha^{-1}$ for every conjugate ρ to α^{-1}* — so, α^{-1} **dominates**.

- Valuation $\implies$ antimatter (so long as $\alpha \notin \mathbb{N}_0$)
- Does antimatter $\implies$ valuation?
  - $\alpha = \sqrt{\frac{1}{2}} \implies M_\alpha = \left\{ \frac{b}{2^m}\sqrt{\frac{1}{2}} + \frac{a}{2^n} \;\middle|\; a, n, b, m \in \mathbb{N}_0 \right\}$ — so, **no**
  - Quite closely resembles $M_{\alpha^2} = \left\{ \frac{a}{2^n} \;\middle|\; a, n \in \mathbb{N}_0 \right\}$ — where $\alpha^2 = \frac{1}{2}$
  - In fact, $M_\alpha \cong M_{\alpha^2} \times M_{\alpha^2} = M_{\alpha^2}^2$ (the *product* of the two monoids)
  - Everything in M_α can be expressed as a tuple (2-ple) of elements in M_{α^2}
  - M_α is the **product** of 2 component monoids, each of which looks like M_{α^2}
- Non-trivial products (neither is a group) are never valuation
  - Take non-units $x \in M$ and $y \in N$, so $(x, 0), (0, y) \in M \times N$ are incomparable
- Can we salvage?

- $m_{\alpha^2}(x) = x - \frac{1}{2}$, while $m_\alpha(x) = x^2 - \frac{1}{2}$
- $m_\alpha(x)$ is more complicated — explains the product structure
  - What specifically about $m_\alpha(x)$ indicates the product (with two components)?
- **Support** (supp) — set of exponents attached to nonzero coefficients
  - $\operatorname{supp} m_\alpha(x) = \{0, 2\}$, while $\operatorname{supp} m_{\alpha^2}(x) = \{0, 1\}$
- "$f(x)$ is **simple**" if $\gcd \operatorname{supp} f(x) = 1$, so $m_{\alpha^2}(x)$, not $m_\alpha(x)$
  - If $k = \gcd \operatorname{supp} f(x)$, then $g(x) = f(x^{1/k})$ is simple (and $g(x^k) = f(x)$)
- "M_α is **simple**" if α algebraic and $m_\alpha(x)$ simple, so M_{α^2}, not M_α

Theorem (Chen, Gotti, Lu, and Yao, 2025)

For any algebraic α, if $k = \gcd \operatorname{supp} m_\alpha(x)$, then $M_\alpha \cong M_{\alpha^k}^k$.

Every semiring M_α is a **product of simple semirings**!

- Consider $\alpha = \sqrt[d]{\frac{1}{n}}$ for some $d, n \in \mathbb{N}$
- M_α is clearly antimatter… but not valuation ($1 \nmid \alpha$ and $\alpha \nmid 1$)
- On the other hand, any element in M_α is a linear combination of

$$\{1, \alpha, \ldots, \alpha^{d-1}\}$$

- By linear independence, each element can be represented as a d-tuple of elements in $M_{1/n}$
- $\implies M_\alpha \cong M_{\alpha^d}^d$

- **Hope** — antimatter $\implies$ **product** of valuation
- **Goal** — simple antimatter $\implies$ valuation
- **Tool** — **antimatter decompositions**
  - α is antimatter $\implies$ there exists $p(x) \in x\mathbb{N}_0[x] - 1$ that has α as a root
  - $p(x)$ is much easier to work with — nice form, and a multiple of $m_\alpha(x)$

Theorem (Handelman, 1992 (Reformulation))

For positive α, if M_α is simple and antimatter, then $m_\alpha(x)$ has a simple multiple in $x\mathbb{N}_0[x] - 1$.

Simple is all we need!

Theorem (Chen, Gotti, Lu, and Yao 2025)

If α is algebraic and there exists a simple polynomial $p(x) \in x\mathbb{N}_0[x] - 1$ such that $p(\alpha) = 0$, then M_α is a valuation monoid.

Sketch of Proof.

- View any difference $|f(\alpha) - g(\alpha)|$ in $\mathbb{Z}[x]$; we need to add or subtract multiples of $m_\alpha(x)$ to turn it into an element of $x\mathbb{N}_0[x]$
- Not too different from antimatter, where we decompose 1 into $p(x) + 1 \in x\mathbb{N}_0[x]$ by Handelman's result

Heavily relies on the exact characterization of antimatter M_α

Can we combine those results?

- Given some algebraic α with M_α antimatter, identify M_α as $M_{\alpha^k}^k$
  - $k = \gcd \operatorname{supp} m_\alpha(x)$ (as in our theorem) to make M_{α^k} simple
  - M_{α^k} remains antimatter (a slight modification to $p(x)$ works — just $p(x^{1/k})$)
- Handelman $\implies p(x) \in x\mathbb{N}_0[x] - 1$ with $p\left(\alpha^k\right) = 0$ and simple
- $\implies M_{\alpha^k}$ is valuation
- $\implies M_\alpha \cong M_{\alpha^k}^k$ **is a product of k valuation monoids**

Theorem (Chen, Gotti, Lu, and Yao 2025)

If M_α is antimatter, it is the product of finitely many valuation monoids.

Putting everything together.

Theorem (Chen, Gotti, Lu, and Yao 2025)

The following statements are equivalent for positive α.

- *M_α is valuation.*
- *M_α is simple and antimatter.*
- *α^{-1} is an algebraic integer, has no positive conjugate aside from itself, and exceeds each of its conjugates by norm.*

$\implies$ Quick to verify if M_α is valuation

- Our last example — prove that valuation is "dense"
  - Let $V \subset (0,1)$ be the set of α for which M_α is valuation
- Is V **dense** in $(0,1)$?
  - For any $r \in (0,1)$ and $\varepsilon > 0$, can we can find $\alpha \in V$ with $|r - \alpha| < \varepsilon$?
  - Easy for antimatter — take $\sqrt[d]{\frac{1}{n}}$ for $d, n \in \mathbb{N}$
    - If d is big, d^{th} roots of consecutive integers are close
- However, minimal polynomial is $nx^d - 1$ — not valuation
  - What about making a small shift $\implies (n-1)x^d + x^{d-1} - 1$?
  - Can easily check all conditions to show valuation (no need for irreducibility)
  - By substituting $n \to n^k$ and $d \to kd$, we approach the desired $\sqrt[d]{\frac{1}{n}}$
- V is dense around a set dense in $(0,1) \implies V$ **is dense in** $(0,1)$

- D. Handelman (1992). “Spectral radii of primitive integral companion matrices and log concave polynomials”. In: *Symbolic Dynamics and its Applications*. Vol. 135. Contemporary Mathematics. American Mathematical Society, pp. 223–228.
- D. W. Boyd (1994). “Irreducible polynomials with many roots of maximal modulus”. In: *Acta Arithmetica* 68, pp. 85–88.
- J. Correa-Morris and F. Gotti (2022). “On the additive structure of algebraic valuations of polynomial semirings”. In: *Journal of Pure and Applied Algebra* 226.11.
- J. Dani, A. Deng, M. Gotti, B. Li, A. Paladiya, J. Vulakh, and J. Zeng (2025). *On the set of atoms and strong atoms in additive monoids of cyclic semidomains*. Preprint on arXiv. URL: https://arxiv.org/abs/2508.11319v1.
- F. Gotti, L. Hong, and B. Li (202?). “On Divisibility and Factorizations in Cyclic Semidomains”. Preprint (Submitted).

Thank you!

The presenters

- are incredibly appreciative of their wonderful mentor **Dr. Felix Gotti** for his constant guidance, support, and wisdom,
- are deeply indebted to the entire **MIT PRIMES-USA** program and its organizers for making this collaboration possible,
- would like to thank the **SWIM organizers** for initiating these sessions and providing the opportunity to present our work,
- especially **Jared Kettinger** for offering helpful feedback.