v-Noetherian and Krull Monoids of Algebraic Evaluations

Aaditya Bilakanti **Amrit Kandasamy**

Mentor: Dr. Felix Gotti, Dr. Marly Gotti, Dr. Harold Polo

MIT CMI

SWIM 2026

Outline

General Notation

- $\mathbb{N} = \{1, 2, 3, \ldots\}$ and $\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$.
- $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ are the integers, rationals, reals, and complex numbers respectively.
- Everything is written additively, meaning the operation is $+$ and the identity is 0.

Monoid Definition

Definition

A **monoid** $(M, +)$ is a nonempty set equipped with a binary operation $+$ that is **associative** for all $a, b, c \in M$, meaning $(a + b) + c = a + (b + c)$, and has an **identity** 0 such that $a + 0 = a$.

Examples

1. $(\mathbb{N}, \cdot)$ with identity 1.
2. Square matrices under multiplication.
3. Functions that map a set back to itself under composition.

Commutativity and Cancellativity

Definition

A monoid $(M, +)$ is **commutative** if $a + b = b + a$, and **cancellative** if $a + c = b + c$ implies $a = b$.

Examples

1. $(\mathbb{N}_0, +)$ is commutative and cancellative.
2. The square matrices under multiplication are neither commutative nor cancellative.

Units and Reduced Monoids

Definition

An element u is a **unit** if $u + v = 0$ for some v. A monoid is **reduced** if its only unit is 0.

Examples

1. $(\mathbb{N}_0, +)$ is reduced.
2. In $(\mathbb{Z}, +)$ every element is a unit, so $\mathbb{Z}$ is a group.
3. Any additive submonoid of $\mathbb{R}_{\geq 0}$ is reduced.

Divisibility and Grothendieck Group

Definition

We say a **divides** b, written as $a \mid_M b$, if $b = a + c$ for some $c \in M$. The **Grothendieck group** is $\mathcal{G}(M) = \{a - b \mid a, b \in M\}$, the smallest group containing M.

Examples

1. In $(\mathbb{N}_0, +)$, $a \mid b \iff a \leq b$, and $\mathcal{G}(\mathbb{N}_0) = \mathbb{Z}$.
2. For $M = (\mathbb{N}, \cdot)$, $\mathcal{G}(M) = (\mathbb{Q}_{>0}, \cdot)$.

Atoms

Definition

A nonzero unit $a \in M$ is an **atom** (irreducible) if $a = x + y$ forces $x = 0$ or $y = 0$.

Examples

1. The only atom of $(\mathbb{N}_0, +)$ is 1.
2. The atoms of $(\mathbb{N}, \cdot)$ are the primes.
3. The atoms of $(\{0\} \cup \mathbb{N}_{\geq 2}, +)$ are 2 and 3, as every $n \geq 4$ is $2 + (n - 2)$.

Atoms are the building blocks, similar to primes in $\mathbb{N}$.

Atomicity

Definition

M is atomic if every nonzero nonunit is a finite sum of atoms.

Examples

1. $(\mathbb{N}, \cdot)$ is atomic by the Fundamental Theorem of Arithmetic.
2. $(\{0\} \cup \mathbb{N}_{\geq 2}, +)$ is atomic.
3. $M = \{p(1/2) \mid p \in \mathbb{N}_0[x]\}$ is not atomic, as every a splits into $a/2 + a/2$. Hence, nothing is an atom.

Finite Generation

Definition

M is **finitely generated** if a finite set $\{g_1, \ldots, g_s\}$ yields every element as $c_1 g_1 + \cdots + c_s g_s$ with $c_i \in \mathbb{N}_0$. We denote this by $M = \langle g_1, \ldots, g_s \rangle$.

Examples

1. $(\mathbb{N}_0, +) = \langle 1 \rangle$.
2. $\mathbb{N}_0 + \mathbb{N}_0\sqrt{2} = \langle 1, \sqrt{2} \rangle$.

Finite generation is a key condition throughout this presentation.

Dickson's Lemma

Dickson's Lemma

Every subset $S \subseteq \mathbb{N}_0^d$ has finitely many minimal elements under coordinatewise order. Equivalently, every upward-closed subset of $\mathbb{N}_0^d$ is generated by finitely many of its elements.

Example

We work in $\mathbb{N}_0^2$. Let $S = \{(3,0),(2,1),(1,2),(0,3),(5,4),(4,7)\}$. The only minimal elements are $\{(3,0),(2,1),(1,2),(0,3)\}$. Note that there isn't a smallest element, since none of them are less than other in all coordinates, but no other elements in S are smaller than them.

Algebraic Numbers and Integers

Definition

A number α is **algebraic** if it is a root of a nonzero polynomial with rational coefficients, and an **algebraic integer** if it is a root of a *monic* polynomial with integer coefficients.

Examples

1. $\sqrt{2}$: root of $X^2 - 2$, an algebraic integer.
2. $\varphi = \frac{1+\sqrt{5}}{2}$: root of $X^2 - X - 1$, an algebraic integer.
3. $\frac{3}{2}$: root of $2X - 3$, algebraic but not an algebraic integer.

Minimal Polynomials and Conjugates

Definition

The **minimal polynomial** $m_\alpha \in \mathbb{Q}[X]$ is the monic polynomial of least degree with $m_\alpha(\alpha) = 0$. Its other roots are **conjugates** of α. A conjugate γ is **peripheral** if $|\gamma| = \alpha$.

Examples

1. $\alpha = \sqrt{2} : m_\alpha = X^2 - 2$, conjugate $-\sqrt{2}$.
2. $\alpha = \varphi : m_\alpha = X^2 - X - 1$, conjugate $\frac{-1+\sqrt{5}}{2}$.

The size of the conjugates relative to α will be an important condition.

Embeddings, $\mathbb{Q}(\alpha)$, and $\mathbb{Z}[\alpha]$

Definition

$\mathbb{Q}(\alpha)$ is the smallest field containing α, of dimension $d = \deg m_\alpha$ over $\mathbb{Q}$.
$\mathbb{Z}[\alpha] = \{f(\alpha) \mid f \in \mathbb{Z}[X]\}$. An **embedding** $\sigma : \mathbb{Q}(\alpha) \hookrightarrow \mathbb{C}$ sends α to conjugate. There are exactly d of them.

Example $\alpha = \sqrt{2}$

$\mathbb{Q}(\alpha) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ and $\mathbb{Z}[\alpha] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$. The two embeddings (identity and conjugation) send $\sqrt{2} \mapsto \pm\sqrt{2}$.

Perron numbers

Definition

A positive real algebraic β is **weak Perron** if $|\gamma| \leq \beta$ for every conjugate γ, and **strict Perron** if $|\gamma| < \beta$ for every conjugate $\gamma \neq \beta$.

Examples

1. φ is **strict** Perron, as $|(1-\sqrt{5})/2| \approx 0.618 < \varphi$.
2. $\sqrt{2}$ is weak but not strict: conjugate $-\sqrt{2}$ has equal absolute value.
3. $\frac{1-\sqrt{5}}{2} \approx 0.618$ is not weak Perron, as its conjugate ≈ -1.68 has a larger modulus.

Ideals

Definition

Let H be a monoid. A subset $I \subseteq H$ is an **ideal** if $I + H \subseteq I$. Writing $(H : X) = \{y \in \mathcal{G}(H) \mid y + X \subseteq H\}$, an ideal I is **divisorial** if $I = (H : (H : I))$.

Examples

1. The ideals of $(\mathbb{N}_0, +)$ are the sets $[n, \infty)$, which are also divisorial.
2. Let $H = \langle 2, 3 \rangle$. The set $I = \{2, 3, 4, \ldots\}$ is an ideal, but $(H : (H : I)) = (H : H) = H \neq I$, so it is not divisorial.

Algebraic Evaluation Monoids

Fix positive real algebraic $\alpha_1, \ldots, \alpha_n$ and set

$$H = \mathbb{N}_0[\alpha_1, \ldots, \alpha_n], \; K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$$

- As an additive monoid, H is generated by the monomials $\alpha_1^{u_1} \cdots \alpha_n^{u_n}$.
- $H \subseteq \mathbb{R}_{\geq 0}$, so it is reduced and positive.
- H is a **semiring**, which means it is closed under both $+$ and $\times$.
- For notational convenience, for $u \in \mathbb{N}_0^n$, we let

$$\alpha^u := \prod_{i=1}^{n} \alpha_i^{u_i}.$$

- These were introduced by Correa-Morris and Gotti in 2022 [1].

Mori (v-Noetherian) monoids

Definition

Let H be a monoid and $I_1, I_2, I_3, \ldots$ be any sequence of ideals such that $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$. If such a sequence stabilizes, meaning there exists an N such that for all $n, m \geq N$, $I_n = I_m$, then we say that H satisfies the **ascending chain on ideals**.

Definition

A monoid H is **Mori** (v-Noetherian) if it satisfies the ascending chain on divisorial ideals.

Example

1. Any finitely generated monoid forces the Mori property by Dickson's Lemma.
2. Let $M = \mathbb{N}_0 \cup \{q \in \mathbb{Q} \mid q \geq 1\}$. The divisorial ideals are $I_r = \{x \in M \mid x \geq r\}$, where $r \in \mathbb{R}_{\geq 0} \cup \{\infty\}$ (when $r = \infty$, I is the empty ideal).

Atoms are Monomials

Suppose all generators are greater than 1, so every nonzero element of H is ≥ 1. Note that none of the generators can be less than 1, as otherwise there would be no minimal element.

- Then H is atomic, and every atom is a **single monomial** α^u, as a value with two or more monomial terms already splits.
- The atom exponents $U = \{u : \alpha^u \text{ is an atom}\}$ for a **down-set** in $\mathbb{N}_0^n$.

Multiplication

If H is finitely generated with atoms $a_1, \ldots, a_s$, then $(a_1, \ldots, a_s)M_i = \alpha_i(a_1, \ldots, a_s)$ for some $M_i \in M_s(\mathbb{N}_0)$, so $\alpha_i = \rho(M_i)$ is a **Perron eigenvalue**.

Perron–Frobenius Consequence

Necessary Conditions for Finite Generation

If H is finitely generated then every α_i is an **algebraic integer**, and for every embedding $\sigma : K \hookrightarrow \mathbb{C}$, $|\sigma(\alpha_i)| \leq \alpha_i$, with equality when $\sigma(\alpha_i)/\alpha_i$ is a root of unity.

- Therefore, finite generation forces each of the α_i to be weak Perron.
- We "remove" the α_i that satisfy $|\sigma(\alpha_i)| = \alpha_i$ by raising it to the k_i-th power, where k_i is the order of ζ, with $\sigma(\alpha_i) = \alpha_i\zeta$. Then each $\beta_i = \alpha_i^{k_i}$ is strict Perron, which is necessary for our proofs.

Main Result

Theorem (Bilakanti–Kandasamy, 2026)

For positive algebraic $\alpha_1, \ldots, \alpha_n$ and $H = \mathbb{N}_0[\alpha_1, \ldots, \alpha_n]$, then H is v-Noetherian if and only if H is finitely generated.

- ($\Leftarrow$) is the standard direction, since all finitely generated monoids are v-Noetherian.
- ($\Rightarrow$) is the main part of the proof.

Rank of a Monoid

Definition

The **rank** of M is the largest r such that $\mathcal{G}(M)$ contains r elements $g_1, \ldots, g_r$ that are $\mathbb{Z}$-linearly independent: no nontrivial relation $n_1 g_1 + \cdots + n_r g_r = 0$ with $n_i \in \mathbb{Z}$. M is **finite-rank** if this r is finite.

Examples

- $\operatorname{rank}(\mathbb{N}_0) = 1$: $\mathcal{G}(\mathbb{N}_0) = \mathbb{Z}$, generated by 1.
- $\operatorname{rank}(\mathbb{N}_0 + \mathbb{N}_0\sqrt{2}) = 2$: 1 and $\sqrt{2}$ are $\mathbb{Z}$-independent.
- $\operatorname{rank}(\mathbb{N}_0[\alpha]) = [\mathbb{Q}(\alpha) : \mathbb{Q}]$: $1, \alpha, \ldots, \alpha^{d-1}$ are $\mathbb{Z}$-independent.
- $\operatorname{rank}(\mathbb{N}_0[x]) = \infty$: $1, x, x^2, \ldots$ are all $\mathbb{Z}$-independent.

Main Part of the Forward Direction

Theorem (Bilakanti–Kandasamy, 2026)

*Let $M \subseteq \mathbb{R}_{\geq 0}$ be a finite-rank Mori monoid, and let $\beta > 1$ be strict Perron with $\beta^m \in M$ for all m. Then $\beta, \beta^2, \beta^3, \ldots$ **cannot all** be atoms of M.*

How this finishes the proof:

- If H was Mori but not finitely generated, then it would be atomic with infinitely many atoms; the down-set U of atom exponents must then be unbounded along some coordinate i.
- Hence $(0, \ldots, 0, m, 0, \ldots, 0) = me_i \in U$ for arbitrary $m \in \mathbb{N}$, so every power α_i^m would be an atom.
- Setting $\beta_i := \alpha_i^{k_i}$ still yields an atom whose powers are atoms, however, they must also be strict Perron, contradicting the above theorem.

The semidomain $\mathbb{N}_0[\alpha]$

Definition

For a positive algebraic number $\alpha > 0$ let

$$\mathbb{N}_0[\alpha] = \{p(\alpha) \in \mathbb{R} : p(x) \in \mathbb{N}_0[x]\}$$

Because $\mathbb{N}_0[\alpha]$ is a subsemiring of $\mathbb{R}$ which is an integral domain, we know that it is inherently a semidomain.

- For an algebraic $\alpha > 0$ the set $\mathbb{N}_0[\alpha]$ is called the algebraic cyclic semidomain of α.
- We denote the additive structure of this semidomain as the monoid $M_\alpha = (\mathbb{N}_0[\alpha], +)$.

Here are some examples:

- $M_{3/2} = \langle (3/2)^k : k \in \mathbb{N}_0 \rangle$
- $M_{1/2} = \{\frac{n}{2^k} : n, k \in \mathbb{N}_0\}$
- $M_{\sqrt{2}} = \{a + b\sqrt{2} : a, b \in \mathbb{N}_0\}$

Relevant Definitions

There are two closure constructions of M inside $\mathcal{G}(M)$ that are relevant here.

Definition

For a monoid M the root closure of M, denoted by $\bar{M}$, is the following subset of $\mathcal{G}(M)$:

$$\bar{M} := \{x \in \mathcal{G}(M) : nx \in M \text{ for some } n \in \mathbb{N}\}.$$

We say that M is **root closed** if $\bar{M} = M$.
Here are some examples:

- $M = \mathbb{N}_0 \times \mathbb{N}_0$ is root closed.
- $M = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x > 0\} \cup \{(0, 0)\}$ is root closed.

Relevant Definitions

An element $g \in \mathcal{G}(M)$ is called **almost integral** if there exists a $c \in M$ such that $cg^n \in M$ for all $n \in \mathbb{N}$.

Definition

The set

$$\hat{M} := \{x \in \mathcal{G}(M) : \exists c \in M \text{ such that } nx + c \in M \text{ for all } n \in \mathbb{N}\}$$

is called the complete integral closure of M.

We say M is **completely integrally closed** if $\hat{M} = M$.

Here are some examples:

- $M = \mathbb{N}_0 \times \mathbb{N}_0$ is completely integrally closed
- $M = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x > 0\} \cup \{(0, 0)\}$ is not completely integrally closed (for example $(0, 1) \in \hat{M}$).

It is not hard to check that

$$M \subseteq \bar{M} \subseteq \hat{M} \subseteq \mathcal{G}(M).$$

Relevant Definitions

Definition

A submonoid H of an abelian group G is **integer divisor closed** in G, if for an element $x \in G$, the condition $nx \in H$ for $n \in \mathbb{N}$ implies $x \in H$.

Definition

We say that M is a Krull monoid if M is both v-Noetherian and completely integrally closed.

So every Krull monoid is root-closed and satisfies the ACCP.
Here are some examples:

- $\mathbb{N}_0 \times \mathbb{N}_0$ is Krull
- $M = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} : x > 0\} \cup \{(0, 0)\}$ is not Krull

$\mathbb{N}_0[\alpha]$ Krull

Theorem (Bilakanti–Kandasamy, 2026)

Let $\alpha > 0$ be algebraic. Then M_α is a Krull monoid if and only if

1. M_α is finitely generated
2. M_α is integer divisor closed in $\mathbb{Z}[\alpha]$

Note that El-Asal et al, [3] provides a terminating classification for the first condition:

Theorem

M_α is finitely generated if and only if

1. $m_\alpha(X) \in \mathbb{Z}[X]$
2. *α is the only positive real root of $m_\alpha(X)$*
3. *Every conjugate β of α satisfies $|\beta| \leq \alpha$.*

So for a finite time algorithm to test Krull, it remains to study the second condition.

Relevant Objects and Notions

Assume $v_0, \ldots, v_{k-1} \in \mathbb{Z}^d$ generate M_α. Let

$$S_\alpha = \left\{ \sum_{j=0}^{k-1} c_j v_j : c_j \in \mathbb{N}_0 \right\}, R_\alpha = \left\{ \sum_{j=0}^{k-1} r_j v_j : r_j \in \mathbb{R}_{\geq 0} \right\}.$$

Definition

The **Hilbert basis** $\mathrm{Hilb}(R_\alpha)$ is the finite minimal set of lattice points generating $R_\alpha \cap \mathbb{Z}^d$.

It turns out that

$$\overline{S_\alpha} = R_\alpha \cap \mathbb{Z}^d.$$

Therefore,

$$S_\alpha \text{ is integer divisor closed} \iff S_\alpha = R_\alpha \cap \mathbb{Z}^d \iff \mathrm{Hilb}(R_\alpha) \subseteq S_\alpha.$$

Testing Integer Divisor Closedness

Hilbert basis can turn this into a terminating process because if all of its finitely many elements are in S_α, then so are all the cone's lattice points.

With that being said, the following process determines integer divisor closedness.

- Construct S_α and R_α.
- Compute $\mathrm{Hilb}(R_\alpha)$.
- Check whether every $h \in \mathrm{Hilb}(R_\alpha)$ belongs to S_α.

Combining this with the minimal polynomial process to test finite generation, we have the desired algorithm.

Central Computational Problem

Both the Krull Classifications and Mori classifications relied on the monoid being finitely generated. The cyclic case has already been fully classified as stated previously, and we provide a finitely terminating algorithm to classify when $\mathbb{N}_0[\alpha_1, \ldots, \alpha_n]$ is finitely generated.

Theorem (Bilakanti–Kandasamy)

There is a terminating algorithm that decides whether $\mathbb{N}_0[\alpha_1, \ldots, \alpha_n]$ is finitely generated, and on a positive instance returns an explicit generating box $0 \leq u_i < N_i$.

Easy Reductions

Lemma (Bilakanti–Kandasamy, 2026)

*Delete generators $\alpha_i \in \mathbb{N}$. If some remaining $0 < \alpha_i < 1$, then H is **not** finitely generated. If all remaining exceed 1, then H is finitely generated if and only if each α_i has a reducible power $\alpha_i^{N_i}$.*

- Testing one fixed α_i^N is a **finite** nonnegative integer feasability problem and standard algorithms exist for this
- The Perron–Frobenius conditions act as a filter to reject any "trivially" bad inputs initially

Peripheral Conjugate Restrictions

Perron–Frobenius gives, for each "axis" i (the generator α_i), the set of embeddings that "peripherize" α_i: $P_i = \{\sigma : K \hookrightarrow \mathbb{C} \mid |\sigma(\alpha_i)| = \alpha_i\}$.

Lemma (Peripheral Assistance)

A reduction of α_i^N into other monomials can only use axes j such that $P_i \subseteq P_j$.

Hence the axes with equal P_i form a **block**, and the algorithm proceeds block by block, from those with the largest P_i down to the smallest.

Reduction to a strict Perron Semiring

Within a block B, we once again convert all the generators to strict Perron (relative to K's embeddings that survive to B), by setting $\gamma_i = \alpha_i^{k_i}$ for $i \in B$.
Using the finite set S_B of block-invariant elements (that is, fixed by the embeddings in the shared P_i set), this produces the semiring

$$V_B = \left\langle s \prod_{i \in B} \gamma_i^{u_i} \mid s \in S_B, u \in \mathbb{N}_0^B \right\rangle_{\mathbb{N}_0}.$$

Block Reduction

H is finitely generated if and only if V_B is finitely generated for every block B.

Minkowski Embeddings

Let $F \subseteq \mathbb{R}$ be a number field with $[F : \mathbb{Q}] = d$ and embeddings $\sigma_1 = \mathrm{id}$, $\sigma_2, \ldots, \sigma_d : F \hookrightarrow \mathbb{C}$.

Definition

The **Minkowski embedding** is $\Phi : F \to \mathbb{R}^d$ where $\Phi(x) = (x, \sigma_2(x), \ldots, \sigma_d(x))$, with pairs of complex conjugate embeddings identified with $\mathbb{R}^2 \cong \mathbb{C}$.

Example $F = \mathbb{Q}\sqrt{2}$

There are two real embeddings $\sqrt{2} \mapsto \pm\sqrt{2}$, so $\Phi(a + b\sqrt{2}) = (a + b\sqrt{2}, a - b\sqrt{2}) \in \mathbb{R}^2$.

Geometric Interpretation

Apply the Minkowski embedding Φ to V_B and normalize each generator $s\gamma^u$ by dividing by its identity/first coordinate. This forces every generator to have its first coordinate as $(1, 0, \ldots, 0)$. Since γ_i is strict Perron, every non-identity coordinate shrinks toward 0, and hence the normalized generators pile up near $p = (1, 0, \ldots, 0)$. We write $\Phi(s\gamma^u)/(s\gamma^u) = p + z_s(u)$ for error correction.

Main Criterion

V_B is finitely generated if and only if $0 \in \operatorname{relint} \operatorname{conv}\{z_s(u) \in S_B, u \in \mathbb{N}_0^B\}$.

Each $z_s(u)$ satisfies $z_s(u) = T_1^{u_1} \cdots T_m^{u_m} z_s(0)$ for commuting invertible linear maps T_j, which is an instance of **Dong's commuting-loop problem** [2]. This problem is decidable with an explicit algorithm, and remains effective over real algebraic numbers.

The algorithm

Algorithm 1

Input: exact positive real algebraic numbers $\alpha_1, \ldots, \alpha_n$

Output: **True** iff $H = \mathbb{N}_0[\alpha_1, \ldots, \alpha_n]$ is finitely generated

1: delete every $\alpha_i \in \mathbb{N}$
2: **if** some remaining $\alpha_i < 1$ **then return False**
3: **end if**
4: **if** spectral filter fails (not an algebraic integer, or $|\sigma(\alpha_i)| > \alpha_i$) **then return False**
5: **end if**
6: partition the axes into peripheral blocks and order them
7: **for** each block B, from maximal to minimal **do**
8: **if** V_B is not finitely generated (Dong test) **then return False**
9: **end if**
10: for each $i \in B$, search increasing N for a reducible α_i^N (using the bound from Dong's problem)
11: **end for**
12: **return True** with the box $0 \leq u_i < N_i$

References I

[1] Jyrko Correa-Morris and Felix Gotti. On the additive structure of algebraic valuations of polynomial semirings. *Journal of Pure and Applied Algebra*, 226(11):107104, November 2022.

[2] Ruiwen Dong. Termination of linear loops under commutative updates, 2023.

[3] Mohammad El-Asal and Wael Mahboub. Finite generation in polynomial semirings: M. el-asal, w. mahboub. pages 1–11, 2026.