THE ARITHMETIC OF SEMIRINGS
PART I: IDEALS

JAY CHEN, TREVOR HYDE, DORIEN LAURENS, JASPER PIERMARINI, AND HARRIET SIMONS

Abstract. We study ideals in the semiring $\mathbb{N}$ of natural numbers, with a focus on those which are lost when extending from $\mathbb{N}$ to $\mathbb{Z}$. This leads to a new perspective on the classical theory of numerical semigroups, including the introduction of a natural multiplicative structure. We prove that unique factorization of ideals fails in $\mathbb{N}$ on several levels, introduce a handful of new tropical multiplicative invariants of numerical semigroups, characterize integral closures of ideals in terms of Newton polygons, and analyze the behavior of classical numerical semigroup invariants with respect to the product operation.

1. Introduction

Number theory traditionally begins with the semiring $\mathbb{N}$ of natural numbers: the home of the prime numbers and the fundamental theorem of arithmetic. Algebraic convenience leads us to introduce additive inverses and work instead with the ring $\mathbb{Z}$ of integers. We keep extending our numbers from $\mathbb{Z}$ to $\mathbb{Q}$ to $\mathbb{R}$ and ultimately $\mathbb{C}$. And while the virtues of $\mathbb{C}$ are widely acknowledged, at each stage of this extension a tradeoff occurs between useful, interesting structure and simplicity. Number theory, to a large extent, lives in this space between $\mathbb{Z}$ and $\mathbb{R}$, focused on the prime numbers which get diminished in passing from $\mathbb{Z}$ to $\mathbb{Q}$ and lose their distinction in passing from $\mathbb{Q}$ to $\mathbb{R}$. In this paper and its sequel, we take a step back to study the following question:

Question 1.1. What is lost when passing from $\mathbb{N}$ to $\mathbb{Z}$?

We find a wealth of structure hiding in this small gap waiting to be explored. The integers $\mathbb{Z}$ are obtained from $\mathbb{N}$ by adjoining an additive inverse of the unit 1. In this way we may view $\mathbb{Z}$ as an additive localization, analogous to the multiplicative localization which gives us $\mathbb{Q}$ from $\mathbb{Z}$. When localizing a ring, the main structures we lose are ideals and quotients. For example, all the prime ideals of $\mathbb{Z}$ degenerate to the trivial ideal $\langle 1\rangle$ in the field $\mathbb{Q}$ and none of the quotient maps $\mathbb{Z} \to \mathbb{F}_p$ extend to $\mathbb{Q}$. We begin our investigation of Question 1.1 by considering the ideals and quotients of $\mathbb{N}$ which get lost in translation to $\mathbb{Z}$. When localizing rings, these losses are related via the standard correspondence between ideals and quotients. Without subtraction, however, this correspondence breaks down for semirings like $\mathbb{N}$, leading to two rich stories. In this paper we analyze the lost ideals, and in a sequel we study the lost quotients of $\mathbb{N}$ and their analogs in number fields.

Every ideal in $\mathbb{Z}$ is, famously, principal. The first surprise is that this is far from true in $\mathbb{N}$. For example, the ideal

$$A := \langle 2, 3\rangle = \{2a + 3b : a, b \in \mathbb{N}\} = \{0\} \cup \{n \in \mathbb{N} : n \geq 2\}$$

is clearly not principal. Note that the generators 2 and 3 are coprime, hence generate a trivial ideal in $\mathbb{Z}$. Thus A is a nontrivial ideal in $\mathbb{N}$ which becomes trivial after the introduction of -1. The ideals in $\mathbb{N}$ with this property are known as *numerical semigroups* and have been intensively studied for more than a century, although not from this perspective.

- Numerical semigroups arise naturally in algebraic geometry as the possible orders of vanishing of polynomial functions along branches at a singular point (see [RG09, p. 5] for a list of references) and as the possible orders of poles of meromorphic functions at smooth points of algebraic curves (see [Sti09, Thm. 1.6.8]).

- Semigroup rings $K[A]$ with A a numerical semigroup are an important class of one-dimensional local rings in commutative algebra and are precisely the coordinate rings of one-dimensional affine toric varieties (see [RG09, p. 19] for a list of references).
- Numerical semigroups conjecturally correspond to power-sum bases for the field of symmetric functions [Kak25; Kak27].

Our arithmetic perspective on numerical semigroups as ideals in $\mathbb{N}$ suggests new structures and lines of inquiry. In particular, the natural multiplicative structure numerical semigroups inherit as ideals appears to have been completely overlooked. This leads to fundamental questions about factorizations, integrality, and the interaction between ideal multiplication and the many classical invariants defined for numerical semigroups.

1.1. **Results.** Ideals were introduced to arithmetic as a means of correcting the failure of unique factorization in extensions of the integers. For example, 6 has two incompatible factorizations in the ring $\mathbb{Z}[\sqrt{-5}]$, but the ideal $\langle 6\rangle$ does factor uniquely into prime ideals and in a way that resolves the ambiguity at the level of elements. It is natural to ask whether this celebrated property of ideals in Dedekind domains extends to ideals in $\mathbb{N}$. Unfortunately, this is not the case. For example, if

$$\begin{aligned} A &:= \langle 5, 17\rangle, \\ B &:= \langle 5, 17, 43\rangle, \\ C &:= \langle 5, 11, 19, 23\rangle, \end{aligned}$$

then one may check that each of these ideals of $\mathbb{N}$ is irreducible and distinct yet $AC = BC$. Note that the ideals A and B are quite similar; they agree up till 43. This sort of failure is common and stems from the fact that the multiplicative semigroup of ideals in $\mathbb{N}$ is not cancellative. To see past this issue we consider the universal cancellative quotient $[\mathrm{Ideal}(\mathbb{N})]$ of the semigroup of ideals. Elements of $[\mathrm{Ideal}(\mathbb{N})]$ are equivalence classes $[A]$ of ideals under the similarity relation $A \sim B$ if and only if $AC = BC$ for some nonzero ideal C. This semigroup brings the unique factorization question back to life, but only briefly.

Theorem 1.2. The semigroup $[\mathrm{Ideal}(\mathbb{N})]$ of similarity classes of ideals in $\mathbb{N}$ does not have unique factorization into irreducibles. Furthermore, the number of irreducible factors is also not well-defined.

We prove this result as Theorem 3.15, where we provide two infinite families demonstrating the extent of the failure. En route to proving Theorem 1.2 we introduce a number of new multiplicative invariants of ideals and numerical semigroups. Let $p \in \mathbb{N}$ be a prime and let $A \subseteq \mathbb{N}$ be an ideal.

- For each $k \geq 0$ define $m_{p,k}(A) := \min\{a \in A : v_p(a) \leq k\}$.
- Let $\mathbb{N}_{\min}[\![T]\!]$ be the semiring of formal power series in the variable T with coefficients in $\mathbb{N}_{\min}$, the tropical min-times semiring of natural numbers with ∞. The additive identity in $\mathbb{N}_{\min}[\![T]\!]$ is $\sum_{k\geq 0} \infty T^k$ and the multiplicative identity is $1 + \sum_{k\geq 1} \infty T^k$. In Lemma 3.9 we prove that the subset $\mathrm{Dec} \subseteq \mathbb{N}_{\min}[\![T]\!]$ of series with weakly decreasing coefficient sequences forms a semiring (although with a different multiplicative identity than in $\mathbb{N}_{\min}[\![T]\!]$). Let $S_p : \mathrm{Ideal}(\mathbb{N}) \to \mathrm{Dec}$ be defined by

$$S_p(A) := \sum_{k\geq 0} m_{p,k}(A) T^k.$$

- Let $\lambda \geq 1$ be a real number and let $\mathbb{R}^+_{\min}$ be the tropical min-times semiring of nonnegative real numbers with ∞. Define $\Phi_{p,\lambda} : \mathrm{Ideal}(\mathbb{N}) \to \mathbb{R}^+_{\min}$ by
$$\Phi_{p,\lambda}(A) := \min_{k\geq 0} m_{p,k}(A)\lambda^k.$$
- The p**th Newton polygon** of A is defined by
$$N_p(A) := \text{lower convex hull of } \{(k, \log m_{p,k}(A)) : k \geq 0\}.$$
Given convex sets X and Y, let $X + Y = \{x + y : x \in X, y \in Y\}$ denote their Minkowski sum. Let $\mathcal{C}$ denote the semigroup of convex subsets of $\mathbb{R}^2$ with respect to Minkowski sum.

Together with these new invariants, we also recall $m_0(A)$, the smallest positive element of A.

Theorem 1.3. Let $p \in \mathbb{N}$ be prime, let $\lambda \geq 1$ be real, and let $A, B \subseteq \mathbb{N}$ be ideals. Then
(1) $m_0(AB) = m_0(A)m_0(B)$,
(2) $m_{p,0}(AB) = m_{p,0}(A)m_{p,0}(B)$,
(3) $S_p(AB) = S_p(A)S_p(B)$,
(4) $\Phi_{p,\lambda}(AB) = \Phi_{p,\lambda}(A)\Phi_{p,\lambda}(B)$,
(5) $N_p(AB) = N_p(A) + N_p(B)$.

Furthermore, $m_0, m_{p,0}, \Phi_{p,\lambda}$, and N_p are cancellative invariants, hence are well-defined on similarity classes of ideals.

Theorem 1.3 is proved in pieces as Lemma 3.6, Lemma 3.10, and Proposition 5.3. Note that $\mathrm{Ideal}(\mathbb{N})$ forms a semiring with respect to addition and multiplication of ideals. The maps in Theorem 1.3 may all be upgraded to semiring homomorphisms. Multiplicative invariants provide methods for proving irreducibility of ideals and similarity classes of ideals.

Proposition 1.4. Let $p \in \mathbb{N}$ be prime and let $A \subseteq \mathbb{N}$ be an ideal.
(1) If either $m_0(A)$ or $m_{p,0}(A)$ is prime, then the similarity class $[A]$ is irreducible.
(2) If A is a numerical semigroup and any of the following conditions holds, then A is irreducible.
   (a) A has two minimal generators,
   (b) A has a prime minimal generator,
   (c) $m_{p,0}(A)$ and $m_{p,\ell}(A)$ are coprime, where ℓ is the smallest index such that $m_{p,\ell}(A) < m_{p,0}(A)$.

This result is proved as Lemma 3.11 and Proposition 3.12. To effectively work with the universal cancellative quotient $[\mathrm{Ideal}(\mathbb{N})]$ one needs a method for testing similarity of ideals. We show that every similarity class contains a unique maximal element. If $A \subseteq \mathbb{N}$ is an ideal, then we say $a \in \mathbb{N}$ is **integral** over A if there is some nonzero ideal $B \subseteq \mathbb{N}$ such that $aB \subseteq AB$. The **integral closure** $\overline{A}$ is the set of all natural numbers integral over A.

Proposition 1.5. If $A, B \subseteq \mathbb{N}$ are ideals, then
(1) $\overline{A}$ is an ideal,
(2) $A \sim \overline{A}$, and,
(3) $A \sim B$ if and only if $\overline{A} = \overline{B}$.

See Lemma 2.15 and Proposition 2.20. Thus the problem of testing similarity reduces to the problem of calculating integral closures of ideals, and further simplifications reduce this from ideals to numerical semigroups. One of our main results is an effective characterization of integral closures in terms of the p-Newton polygons of the ideal.

Theorem 1.6. Let $A \subseteq \mathbb{N}$ be an ideal and let $a \in \mathbb{N}$. The following are equivalent

(1) $a \in \overline{A}$,
(2) $a^k \in A^k$ for some $k \geq 1$,
(3) $(v_p(a), \log a) \in N_p(A)$ for all primes p,
(4) If A is nonzero, then $\Phi_{p,\lambda}(A) \leq a\lambda^{v_p(a)}$ for all primes p and all $\lambda \geq 1$.

This is proved as Lemma 5.2 and Theorem 5.4. The Newton polygons $N_p(A)$ only impose nontrivial conditions for primes p dividing the multiplicity $m_0(A)$. Hence Theorem 1.6 provides an efficient algorithm for computing the integral closure of an ideal in $\mathbb{N}$.

There are many classically defined invariants of numerical semigroups, such as the genus, Frobenius number, Apéry set, and type (see Sections 3.1, 4.1, 4.2). We study the behavior of these invariants with respect to ideal multiplication, and in particular under powers A^k.

Numerical semigroups with two generators $S = \langle m, n \rangle$ are exceptionally nice in that all the classical invariants may be computed explicitly with closed form formulas. We show the same is true for their powers S^k.

Theorem 1.7. Let $S = \langle m, n \rangle$ where $m < n$ are coprime and let $k \geq 1$.

(1) The Apéry set of S^k is
$$\mathrm{Ap}(S^k) = \{j_1 m^{k-1} n + \ldots + j_k n^k : 0 \leq j_i < m\}.$$
(2) The Frobenius number of S^k is
$$F(S^k) = \frac{(m-1)n^{k+1} - (n-1)m^{k+1}}{n-m}.$$
(3) The genus of S^k is
$$g(S^k) = \frac{n^{k+1}(m-1) + n - m^{k+1}(n-1) - m}{2(n-m)}.$$
(4) The type of S^k is $\mathrm{t}(S^k) = 1$. In other words, S^k is symmetric for all $k \geq 1$.

This theorem is proved as Theorem 4.1, Corollary 4.3, and Proposition 4.10. Leveraging our analysis of the two-generator case, we prove the following result on the asymptotic growth rate of Frobenius numbers and genera for any numerical semigroup. Let $m_{\max}(A) := \max_p m_p(A)$.

Theorem 1.8. Let A be a numerical semigroup. Then
$$\lim_{k \to \infty} \frac{\log F(A^k)}{k} = \lim_{k \to \infty} \frac{\log g(A^k)}{k} = \log m_{\max}(A).$$
This is proved as Theorem 4.11.

1.2. **Organization.** We begin in Section 2 with the foundations of ideals in semirings. This includes an analysis of notions of integrality which are equivalent for rings but fracture into a series of implications for semirings (see Section 2.2). Section 3 focuses on ideals in the natural numbers, reviews the basics of numerical semigroups, introduces multiplicative invariants, and studies factorization of ideals in $\mathbb{N}$. Section 4 contains our results about numerical semigroups with two generators and their consequences. Section 5 characterizes integral closures of ideals in $\mathbb{N}$.

1.3. **Acknowledgments.** We gratefully acknowledge the support of the URSI program at Vassar College and the Asprey endowment. The second author acknowledges support from an AMS-Simons Research Enhancement Grant for Primarily Undergraduate Institution Faculty. We acknowledge that Google's Gemini and OpenAI's ChatGPT were used in the research process for exploring ideas and for writing code to assist with computational experiments. That said, this paper is completely written and vetted by its authors. Finally, the second author would like to thank Jonathan Gerhard for his sustained interest in and enthusiasm for this project during its long gestation.

2. Ideals in Semirings

In this paper we use the following standard definitions of a (commutative) semiring.

Definition 2.1. A **semiring** R is a set with two associative, commutative binary operations called addition $+$ and multiplication $\cdot$ with identities 0 and 1 respectively, such that multiplication distributes over addition and $a \cdot 0 = 0$ for all $a \in R$. We require our semiring homomorphisms to respect both 0 and 1.

Definition 2.2. An R**-module** is a commutative monoid M together with a semiring homomorphism $\rho : R \to \mathrm{End}(M)$. Given $r \in R$ and $m \in M$ we write $rm := \rho(r)(m)$.

Definition 2.3. An **ideal** of R is an R-submodule A of R. Equivalently, $A \subseteq R$ is a subset closed under addition such that $ra \in A$ for all $r \in R$ and $a \in A$.

The standard operations of addition, multiplication, and intersection of ideals are defined the same for ideals in a semiring as they are for ideals in a commutative ring. Let $\mathrm{Ideal}(R)$ denote the set of all ideals of R. With the operations of addition and multiplication of ideals, $\mathrm{Ideal}(R)$ forms a semiring with identity elements $\langle 0 \rangle$ and $\langle 1 \rangle$. Note that $A + A = A$ for all $A \in \mathrm{Ideal}(R)$, so $\mathrm{Ideal}(R)$ is a $\mathbb{B}$-algebra where $\mathbb{B} = \{0, 1\}$ is the Boolean semiring.

Definition 2.4. An element $r \in R$ is said to be **regular** if $rs = 0$ implies $s = 0$. An ideal $A \subseteq R$ is **regular** if A contains at least one regular element.

Note that if r and s are regular elements, then rs is also regular. Hence it follows that the sum and product of regular ideals is regular. Let $\mathrm{Ideal}_{\mathrm{rfg}}(R) \subseteq \mathrm{Ideal}(R)$ be the subsemiring of all regular, finitely generated ideals together with $\langle 0 \rangle$.

2.1. Universal Cancellative Quotient.

Let M be a multiplicative commutative semigroup. If $a, b \in M$, then we write $a \sim b$ if there exists $c \in M$ such that $ac = bc$.

Lemma 2.5. The relation $\sim$ is a congruence on M. The quotient $[M]$ of M by $\sim$ is the universal cancellative semigroup quotient of M.

Proof. Clearly $\sim$ is reflexive and symmetric. Suppose that $a \sim b$ and $b \sim c$. Let $d, e \in M$ be elements such that $ad = bd$ and $be = ce$. Then

$$ade = (ad)e = (bd)e = (be)d = (ce)d = cde.$$

Hence $a \sim c$. Thus $\sim$ is an equivalence relation. Suppose that $a_1 \sim b_1$ and $a_2 \sim b_2$ and let $c_1, c_2 \in M$ be such that $a_i c_i = b_i c_i$. Then

$$(a_1a_2)(c_1c_2) = (a_1c_1)(a_2c_2) = (b_1c_1)(b_2c_2) = (b_1b_2)(c_1c_2),$$

hence $a_1a_2 \sim b_1b_2$. Thus $\sim$ is a congruence on M. The quotient $[M]$ is clearly cancellative and any cancellative quotient must factor through $[M]$, hence $[M]$ is the universal cancellative quotient of M. $\square$

Note that $M \mapsto [M]$ is a functor from commutative semigroups to cancellative commutative semigroups. This functor is the left adjoint to the natural forgetful functor. Our main interest in this construction stems from the case where $M = \mathrm{Ideal}_{\mathrm{rfg}}(R)$ is the multiplicative commutative semigroup of regular, finitely generated ideals in R. That is, if $A, B \in \mathrm{Ideal}_{\mathrm{rfg}}(R)$, we say $A \sim B$ if there is some $C \in \mathrm{Ideal}_{\mathrm{rfg}}(R)$ such that $AC = BC$. Lemma 2.5 implies that $[\mathrm{Ideal}_{\mathrm{rfg}}(R)]$ is the universal cancellative quotient for the multiplicative semigroup of regular finitely generated ideals. We would like to understand the multiplicative structure of $\mathrm{Ideal}_{\mathrm{rfg}}(R)$, especially in cases where R is arithmetic in nature. Similarity introduces many multiplicative relations in $\mathrm{Ideal}_{\mathrm{rfg}}(R)$; the quotient $[\mathrm{Ideal}_{\mathrm{rfg}}(R)]$ allows us to step past similarity in order to study more fundamental relations.

We noted above that $\mathrm{Ideal}_{\mathrm{rfg}}(R)$ is more than a multiplicative semigroup, it also carries the structure of a semiring. The next proposition shows that this is also true for $[\mathrm{Ideal}_{\mathrm{rfg}}(R)]$, hence that $[\mathrm{Ideal}_{\mathrm{rfg}}(R)]$ is a semiring quotient of $\mathrm{Ideal}_{\mathrm{rfg}}(R)$.

Proposition 2.6. Let $[\mathrm{Ideal}_{\mathrm{rfg}}(R)]$ denote the set of similarity classes of regular, finitely generated ideals in R together with the zero ideal. Then $[\mathrm{Ideal}_{\mathrm{rfg}}(R)]$ forms a semiring with operations defined representativewise.

Proof. We already know that similarity respects multiplication, so all that remains is to show that it respects ideal addition. Suppose that $A_1 \sim A_2$ and $B_1 \sim B_2$ with $C, D \in \mathrm{Ideal}_{\mathrm{rfg}}(R)$ such that $A_1C = A_2C$ and $B_1D = B_2D$. Then

$$(A_1 + B_1)CD = A_1CD + B_1CD = (A_1C)D + (B_1D)C = (A_2C)D + (B_2D)C = (A_2 + B_2)CD.$$

Hence $A_1 + B_1 \sim A_2 + B_2$. ☐

2.2. **Integral Extensions of Semirings.** Before proceeding with our study of $\mathrm{Ideal}_{\mathrm{rfg}}(R)$ we take an interlude into notions of integrality for semirings. Given an extension of commutative rings $R \subseteq S$, there are several equivalent definitions of what it means for an element $s \in S$ to be integral over R. If $R \subseteq S$ are commutative semirings, these equivalencies degenerate into a series of strict implications.

Definition 2.7. Suppose $R \subseteq S$ is an extension of semirings and let $s \in S$. We define five types of **integrality**:

(1) The semiring $R[s]$ is a finitely generated R-module.
(2) There exists a semiring $R[s] \subseteq R' \subseteq S$ such that R' is a finitely generated R-module.
(3) There exists a faithful $R[s]$-module $M \subseteq S$ which is finitely generated as an R-module.
(4) There exists a faithful $R[s]$-module M which is finitely generated as an R-module.
(5) There exists a $d \geq 1$ and polynomials $f(x), g(x) \in R[x]$ with degree less than d such that $s^d + f(s) = g(s)$.

Let $D := \mathbb{N}[\varepsilon]/\langle \varepsilon^2 = 0\rangle$. Note that every element of D may be uniquely represented as $a + b\varepsilon$ for some $a, b \in \mathbb{N}$. Let $u := 1 + \varepsilon$ and let $C := \mathbb{N}[u] \subseteq D$.

Lemma 2.8. If $M \subseteq C$ is a C-submodule which is finitely generated as an $\mathbb{N}$-module, then $M = \{0\}$.

Proof. Every nonzero element $a + b\varepsilon \in C$ has $a \neq 0$. Let $\sigma(a + b\varepsilon) := b/a$ be the *slope* of $a + b\varepsilon$. If $B \subseteq C$ is a finitely generated $\mathbb{N}$-module, say $B = \langle \beta_1, \ldots, \beta_n\rangle$, let $S := \max_i \sigma(\beta_i)$ be the maximum slope of a generator. If $\beta = \sum_{i=1}^n m_i\beta_i$ and $\beta_i = a_i + b_i\varepsilon$, then

$$\sigma(\beta) = \frac{\sum_{i=1}^n m_ib_i}{\sum_{i=1}^n m_ia_i} \leq S.$$

Hence finitely generated $\mathbb{N}$-submodules of C have uniformly bounded slope.

Now suppose that $\beta = a + b\varepsilon \in C$ is a nonzero element. Then

$$u^n\beta = (1 + n\varepsilon)(a + b\varepsilon) = a + (na + b)\varepsilon$$

has slope

$$\sigma(u^n\beta) = \frac{na+b}{a} = n + \frac{b}{a},$$

which is unbounded. Thus if $M \subseteq C$ is a C-submodule which is finitely generated as an $\mathbb{N}$-module, then $M = \{0\}$. $\square$

Proposition 2.9. The following implications between integrality types for commutative semirings are strict:

$$(1) \Longrightarrow (2) \Longrightarrow (3) \Longrightarrow (4) \Longrightarrow (5).$$

Proof. First we prove the implications. Clearly (1) implies (2). Suppose (2) holds and let $R[s] \subseteq R' \subseteq S$ be a semiring such that R' is finitely generated as an R-module. Then $R' \subseteq S$ is an $R[s]$-module and $1 \in R'$ implies that R' is faithful. Thus (3) holds. Clearly (3) implies (4).

Finally suppose (4) is true and let M be the module it provides. Suppose M is generated by d elements and let A_s be the multiplication-by-s linear endomorphism of M. Rutherford [Rut64] proved a semiring generalization of the Cayley-Hamilton theorem which tells us that for any linear endomorphism A of an R-module generated by d elements, there are polynomials $f(x), g(x) \in R[x]$ with degree less than d such that $A^d + f(A) = g(A)$. Applying this to A_s and using the assumption that M is a faithful $R[s]$-module, we conclude that $s^d + f(s) = g(s)$.

Now we show that (n) does not imply $(n-1)$ in general. Consider $R = \mathbb{N}$ and $R' = S := D$. Note that D is generated by 1 and ε as an $\mathbb{N}$-module. Let $s := u = 1 + \varepsilon$. Then $R[s] \subseteq R' \subseteq S$ and thus (2) is satisfied. However Lemma 2.8 implies that $R[s] = C$ is not a finitely generated R-module. Hence $(2) \not\Rightarrow (1)$.

Let $R := \mathbb{N}$ and let S be the semiring with underlying set $C \times D$ with componentwise addition and multiplication defined by

$$(c_1, d_1)(c_2, d_2) = (c_1c_2, c_1d_2 + c_2d_1).$$

Let $s := (u, 0) \in S$ and $M := \{0\} \times D$. Then $R[s] = C \times \{0\} \subseteq S$ and M is an $R[s]$-module. Since D is a finitely generated $\mathbb{N}$-module, M is finitely generated as an R-module. Finally note that if $(c_1, 0), (c_2, 0) \in C$ act the same on M, then

$$(0, c_1) = (c_1, 0)(0, 1) = (c_2, 0)(0, 1) = (0, c_2),$$

hence $c_1 = c_2$. Thus M is a faithful $R[s]$-module. Hence (3) holds. Suppose that (2) holds and let R' be the finitely generated R-module provided by (2). Let $\pi : S \to C$ be the projection onto the first component. Then $\pi(R')$ is an $R[s]$-submodule of C which is finitely generated over R. Since $R[s] \cong C$, Lemma 2.8 implies that $\pi(R')$ must be zero. However the multiplicative identity $(1, 0) \in R'$ maps to a nonzero element under π. This contradiction implies that $(3) \not\Rightarrow (2)$.

Let $R := \mathbb{N}$, $s := u$, $S := C$ and let $M := D$. Then M is a faithful $R[s]$-module and a finitely generated R-module. Hence (4) holds. However Lemma 2.8 implies that S does not contain any faithful $R[s] = C$-modules which are finitely generated over R. Hence $(4) \not\Rightarrow (3)$.

Finally, let $R := \mathbb{B}$ be the Boolean semiring and let $S := \mathbb{N}_{\min}$ be the tropical min-times semiring of natural numbers together with ∞. The addition on $\mathbb{N}_{\min}$ is min and the multiplication is the usual multiplication of natural numbers. We may identify the Boolean semiring $\mathbb{B}$ with the subsemiring $\{1, \infty\} \subseteq S$. Let $s := 2 \in S$. Then $s^2 + 1 = 1$, hence (5) is satisfied with $d = 2$ and $f(x) = g(x) = 1 \in \mathbb{B}[x]$. Note that $R[s] = \{2^n : 0 \leq n \leq \infty\}$ is infinite. Every finitely generated R-module is finite (a $\mathbb{B}$-module with n generators has at most 2^n elements). Hence if M is a finitely generated R-module, the R-endomorphism ring of M is also finite. But if M were a faithful $R[s]$-module, then the infinite semiring $R[s]$ maps injectively into the R-endomorphism ring of M, a contradiction. Thus $(5) \not\Rightarrow (4)$. $\square$

If R is a commutative ring and $A \in \mathrm{Ideal}_{\mathrm{rfg}}(R)$ is an ideal, there is also a notion of integrality of $r \in R$ over A. The simplest definition is that r is integral over A if there exists a faithful, finitely generated R-module M such that $rM \subseteq AM$. This notion of integrality is equivalent to a special case of integrality of an element in an extension applied to the Rees algebra $R[At] := \bigoplus_{i=0}^{\infty} A^i t^i$. Namely, $r \in R$ is integral over A when $rt \in R[t]$ is integral over $R[At]$. The Rees algebra construction works without change when R is a commutative semiring and $A \in \mathrm{Ideal}_{\mathrm{rfg}}(R)$ is an ideal. Hence we may translate the five types of integrality from Definition 2.7 into five notions of integrality of an element $r \in R$ over an ideal A. To perform the translations, we replace the base semiring R with the Rees algebra $R[At]$ and let $s := rt$. Note that $R[At][rt] = R[(A + \langle r\rangle)t]$ as graded R-algebras.

Definition 2.10. Let R be a semiring, let $A \in \mathrm{Ideal}_{\mathrm{rfg}}(R)$ be a finitely generated ideal, and let $r \in R$ be an element. We define five types of **integrality** of r over A.

(1*) The semiring $R[(A + \langle r\rangle)t]$ is a finitely generated $R[At]$-module.
(2*) There exists a semiring $R[At] \subseteq R' \subseteq R[t]$ such that R' is a finitely generated graded $R[At]$-module.
(3*) There exists a faithful graded $R[(A + \langle r\rangle)t]$-module $B \subseteq R[At]$ which is finitely generated as an $R[At]$-ideal.
(4*) There exists a faithful graded $R[(A + \langle r\rangle)t]$-module M which is finitely generated as an $R[At]$-module.
(5*) There is some $d \geq 1$ and elements $a_i, b_i \in A^i$ such that

$$r^d + \sum_{i=1}^{d} a_i r^{d-i} = \sum_{i=1}^{d} b_i r^{d-i}.$$

Finally, to make these definitions more practical we may extract equivalent conditions at each graded level to get a notion of integrality without reference to the auxiliary variable t.

Definition 2.11. Let R be a semiring, let $A \in \mathrm{Ideal}_{\mathrm{rfg}}(R)$ be an ideal, and let $r \in R$ be an element. We define five types of **integrality** of r over A.

(1) There is some $k \geq 1$ such that $(A + \langle r\rangle)^k = A(A + \langle r\rangle)^{k-1}$.
(2) There exists a sequence of finitely generated ideals $B_k \subseteq R$ such that $(A + \langle r\rangle)^k \subseteq B_k$, $B_j B_k \subseteq B_{j+k}$, and there exists some $d \geq 0$ such that $B_{k+1} = AB_k$ for all $k \geq d$.
(3) There exists a regular finitely generated R-ideal B such that $rB \subseteq AB$.
(4) There exists a faithful finitely generated R-module M such that $rM \subseteq AM$.
(5) There is some $d \geq 0$ and elements $a_i, b_i \in A^i$ such that

$$r^d + \sum_{i=1}^{d} a_i r^{d-i} = \sum_{i=1}^{d} b_i r^{d-i}.$$

Proposition 2.12. Let R be a semiring, let $A \in \mathrm{Ideal}_{\mathrm{rfg}}(R)$ be an ideal, and let $r \in R$ be an element. Then $(i^*) \Leftrightarrow (i)$ for $1 \leq i \leq 5$.

Proof. $(1^*) \Leftrightarrow (1)$. If $R[(A + \langle r\rangle)t]$ is a finitely generated $R[At]$-module, then there is some largest degree $k - 1 \geq 0$ which arises in a generator of $R[(A + \langle r\rangle)t]$. Consider the degree k component of $R[(A + \langle r\rangle)t]$ which is $(A + \langle r\rangle)^k t^k$. By assumption we must have

$$(A + \langle r\rangle)^k t^k = \bigoplus_{j=1}^{k} (At)^j (A + \langle r\rangle)^{k-j} t^{k-j} \subseteq (At)(A + \langle r\rangle)^{k-1} t^{k-1}.$$

Thus $(A + \langle r\rangle)^k \subseteq A(A + \langle r\rangle)^{k-1}$. The reverse inclusion is automatic, hence

$$(A + \langle r\rangle)^k = A(A + \langle r\rangle)^{k-1}.$$

Hence $(1^*) \Rightarrow (1)$. For the reverse implication, note that since A is finitely generated, so is $(A+\langle r\rangle)^j$ for all $j \geq 0$. Thus $S = \bigoplus_{i=0}^{k-1}(A+\langle r\rangle)^i t^i$ is finitely generated as an R-module, and $(A+\langle r\rangle)^k = A(A+\langle r\rangle)^{k-1}$ implies that S generates $R[(A+\langle r\rangle)t]$ as an $R[At]$-module.

$(2^*) \Leftrightarrow (2)$. By assumption we have $R' = \bigoplus_{k=0}^{\infty} B_k t^k$ where each B_k is an R-ideal. The grading on R' implies that $B_j B_k \subseteq B_{j+k}$ for all $j, k \geq 0$. The containment $R[At] \subseteq R'$ of graded semirings implies that $(A+\langle r\rangle)^k \subseteq B_k$. If R' is a finitely generated $R[At]$-module, then there is some $d \geq 0$ such that R' is generated by elements in degree at most d. Thus for $k \geq d$ we have

$$B_{k+1} = \sum_{i=0}^{d} A^{k+1-i} B_i \subseteq AB_k,$$

and the reverse inclusion is immediate, hence $B_{k+1} = AB_k$. That shows $(2^*) \Rightarrow (2)$. In the other direction, if $B_{k+1} = AB_k$ for all $k \geq d$, then it follows that R' is generated as an $R[At]$-module by elements of degree at most d. Since each B_k is finitely generated as an R-module, it follows that R' is finitely generated as an $R[At]$-module.

$(3^*) \Leftrightarrow (3)$. Suppose $B = \bigoplus_{k=0}^{\infty} B_k t^k \subseteq R[At]$ is a faithful, graded $R[(A+\langle r\rangle)t]$-module which is finitely generated as an $R[At]$-ideal. Then there is some $d \geq 0$ such that B is generated by elements in degree at most d. Thus, as argued in previous steps, this implies that for $n \geq d$ we have $B_{n+1} = AB_n$. On the other hand, note that

$$rB_n t^{n+1} = (rt)B_n t^n \subseteq B_{n+1}t^{n+1} = AB_n t^{n+1}.$$

Hence $rB_n \subseteq AB_n$. Conversely, if B_0 is a regular finitely generated R-ideal such that $rB_0 \subseteq AB_0$, then consider the graded $R[At]$-ideal generated by B_0, namely

$$B := R[At]B = \bigoplus_{k=0}^{\infty}(A^k B_0)t^k.$$

Our assumption implies that B is a faithful, graded $R[(A+\langle r\rangle)t]$-module. As an $R[At]$-ideal, B is generated by elements in degree 0, hence is finitely generated.

$(4^*) \Leftrightarrow (4)$. Suppose $M = \bigoplus_{k=0}^{\infty} M_k t^k$ is a faithful, graded $R[(A+\langle r\rangle)t]$-module which is finitely generated as an $R[At]$-module. Then there is some $d \geq 0$ such that M is generated by elements in degree at most d. Thus, as argued in previous steps, this implies that for $n \geq d$ we have $M_{n+1} = AM_n$. On the other hand, note that

$$rM_n t^{n+1} = (rt)M_n t^n \subseteq M_{n+1}t^{n+1} = AM_n t^{n+1}.$$

Hence $rM_n \subseteq AM_n$. Conversely, if M_0 is a finitely generated faithful R-module such that $rM_0 \subseteq AM_0$, then consider the graded module $M := \bigoplus_{k=0}^{\infty}(A^k M_0)t^k$. Our assumption implies that M is a faithful graded $R[(A+\langle r\rangle)t]$-module. As an $R[At]$-module, M is generated by elements in degree 0, hence is finitely generated.

$(5^*) \Leftrightarrow (5)$. These conditions are identical. □

Each of these notions of integrality may have their merits. For our purposes of studying factorizations of ideals, type (3) integrality of elements over an ideal is the one we need. From now on, we adopt this as our standard notion of integrality over an ideal.

We extract one practical sufficient condition for integrality from Proposition 2.12.

Corollary 2.13. Let $A \in \mathrm{Ideal}_{\mathrm{rfg}}(R)$ be an ideal and let $r \in R$. If there is some $k \geq 1$ such that $r^k \in A^k$, then r is type (1) integral over A, hence also type (3) integral over A.

Proof. Suppose that $r^k \in A^k$. Then

$$(A+\langle r\rangle)^k = A^k + rA^{k-1} + \ldots + r^{k-1}A + \langle r^k\rangle \subseteq A^k + rA^{k-1} + \ldots + r^{k-1}A = A(A+\langle r\rangle)^{k-1}.$$

This is the definition of type (1) integrality. □

2.3. **Integral Closure.** Let A be an ideal in a semiring R. From now on, when we refer to integrality over an ideal, we mean type (3) integrality.

Definition 2.14. We say $r \in R$ is **integral** over A if there exists $B \in \mathrm{Ideal}_{\mathrm{rfg}}(R)$ such that $rB \subseteq AB$. The **integral closure** of A is $\overline{A} := \{r \in R : r \text{ is integral over } A\}$.

Lemma 2.15. If $A \subseteq R$ is an ideal, then $\overline{A}$ is an ideal.

Proof. Suppose $r_1, r_2 \in \overline{A}$ and let $B_1, B_2 \in \mathrm{Ideal}_{\mathrm{rfg}}(R)$ be such that $r_i B_i \subseteq AB_i$. Then $B_1 B_2 \in \mathrm{Ideal}_{\mathrm{rfg}}(R)$ and

$$(r_1 + r_2)B_1B_2 \subseteq r_1B_1B_2 + r_2B_1B_2 \subseteq (AB_1)B_2 + (AB_2)B_1 = AB_1B_2.$$

Hence $r_1 + r_2 \in \overline{A}$. Suppose $s \in \overline{A}$ and $B \in \mathrm{Ideal}_{\mathrm{rfg}}(R)$ is an ideal such that $sB \subseteq AB$. If $r \in R$, then

$$rsB \subseteq rAB \subseteq AB,$$

since A is an ideal. Thus $rs \in \overline{A}$ and $\overline{A}$ is an ideal of R. $\square$

Similarity of ideals implies equality of their integral closures.

Lemma 2.16. If $A, B \in \mathrm{Ideal}_{\mathrm{rfg}}(R)$, then $A \sim B$ implies that $\overline{A} = \overline{B}$.

Proof. Let $C \in \mathrm{Ideal}_{\mathrm{rfg}}(R)$ be such that $AC = BC$. If $r \in \overline{A}$, then there is some $D \in \mathrm{Ideal}_{\mathrm{rfg}}(R)$ such that $rD \subseteq AD$. Hence $rCD \subseteq ACD = BCD$. Therefore $r \in \overline{B}$, which proves that $\overline{A} \subseteq \overline{B}$. Thus by symmetry we conclude that $\overline{A} = \overline{B}$. $\square$

Lemma 2.17. Let $A \in \mathrm{Ideal}_{\mathrm{rfg}}(R)$. If $r \in R$, then $A + \langle r \rangle \sim A$ if and only if $r \in \overline{A}$.

Proof. Suppose that $B \in \mathrm{Ideal}_{\mathrm{rfg}}(R)$ is an ideal such that

$$AB = (A + \langle r \rangle)B = AB + rB.$$

This is equivalent to $rB \subseteq AB$, which is precisely what it means for $r \in \overline{A}$. Thus $A + \langle r \rangle \sim A$ if and only if $r \in \overline{A}$. $\square$

Lemma 2.18. If $A \subseteq B \subseteq R$ are ideals, then $\overline{A} \subseteq \overline{B}$.

Proof. Suppose $a \in \overline{A}$ and let $C \in \mathrm{Ideal}_{\mathrm{rfg}}(R)$ be an ideal such that $aC \subseteq AC$. Then $A \subseteq B$ implies that $AC \subseteq BC$, hence $aC \subseteq BC$. Therefore $a \in \overline{B}$. $\square$

Definition 2.19. We say a semiring R is **Noetherian** if every ascending chain of ideals eventually stabilizes.

Proposition 2.20. If R is Noetherian, then $A \sim \overline{A}$ for all $A \in \mathrm{Ideal}_{\mathrm{rfg}}(R)$. In particular, $A \sim B$ if and only if $\overline{A} = \overline{B}$.

Proof. Since R is Noetherian, there are finitely many elements $b_1, \ldots, b_n \in \overline{A}$ such that $A + \langle b_1, \ldots, b_n \rangle = \overline{A}$. Let $A_0 := A$ and then recursively define $A_{i+1} := A_i + \langle b_{i+1} \rangle$. Then Lemma 2.16 and Lemma 2.17 imply that $A_i \sim A_{i+1}$ for each i. Therefore $A \sim \overline{A}$. The final assertion follows from what was just shown and Lemma 2.16. $\square$

Proposition 2.20 implies that if R is Noetherian, every similarity class in $\mathrm{Ideal}_{\mathrm{rfg}}(R)$ contains a maximal element, namely the common integral closure of all the elements in the similarity class. Thus in this case we can, in principle, determine similarity between ideals by checking if their integral closures are equal. The problem is that calculating integral closures of ideals appears to be a challenging problem, even for the simplest semirings.

Problem 2.1. Given a semiring R, find an effective algorithm to compute $\overline{A}$ for $A \in \mathrm{Ideal}_{\mathrm{rfg}}(R)$.

Given an ideal A and an element $r \in R$, in order to show that $r \in \overline{A}$ one needs to construct an ideal $B \in \mathrm{Ideal}_{\mathrm{rfg}}(R)$ such that $rB \subseteq AB$. Note that this is essentially equivalent to constructing a matrix with entries in A which has r as an eigenvalue. If such an ideal exists, there is an algorithm which, depending on R, is often effective for finding the maximal witness B. The construction uses iterated colon ideals.

Definition 2.21. If $A, B \subseteq R$ are ideals, then the **colon ideal** $(A : B)$ is defined by

$$(A : B) := \{r \in R : rB \subseteq A\}.$$

Now let $A \in \mathrm{Ideal}_{\mathrm{rfg}}(R)$ and let $r \in R$ be a candidate for $\overline{A}$. Consider the recursive sequence of ideals defined by $B_0 = R$ and

$$B_{k+1} = (AB_k : \langle r \rangle) = \{b \in R : rb \in AB_k\}.$$

The sequence B_k is monotone decreasing, $B_k \supseteq B_{k+1}$ for all $k \geq 0$.

Lemma 2.22. With notation as above, if there exists $B \in \mathrm{Ideal}_{\mathrm{rfg}}(R)$ such that $rB \subseteq AB$, then $B \subseteq \bigcap_{k \geq 0} B_k$.

Proof. We proceed by induction. For the base case, clearly $B \subseteq R = B_0$. Now suppose that $B \subseteq B_k$. Then $rB \subseteq AB \subseteq AB_k$, which implies that $B \subseteq B_{k+1}$. Thus $B \subseteq \bigcap_{k \geq 0} B_k$. □

If there are only finitely many ideals between any given pair $B \subseteq C$ and if such a witness exists, then this lemma implies the sequence B_k must converge to a fixed point after finitely many steps, and that fixed point is the maximal witness. However, it is not clear how to bound the number of iterations required to reach stabilization. Thus this only gives us a semi-decision procedure for checking if elements belong to the integral closure.

3. Ideals in the Natural Numbers

We now turn from general theory to the special case of $R = \mathbb{N}$, the initial semiring. Here we may leverage the well-ordering and arithmetic structure of $\mathbb{N}$ to construct refined invariants for studying similarity classes of ideals.

3.1. Numerical Semigroups.

Every ideal in the ring $\mathbb{Z}$ is principal. However the semiring $\mathbb{N}$ has non-principal ideal which get lost in translation when passing from $\mathbb{N}$ to $\mathbb{Z}$. These ideals, known as *numerical semigroups*, have been extensively studied for their many interesting properties and connections to geometry, algebra, and combinatorics. We briefly review the fundamentals we require.

Definition 3.1. A **numerical semigroup** is an ideal $A \subseteq \mathbb{N}$ which contains a pair of coprime integers.

Our definition differs slightly from the standard definition of a numerical semigroup. We adopt this definition with an eye towards generalizations to be explored in a sequel to this paper. The following well-known result proves equivalence between our definition and the more standard one.

Proposition 3.2. If A is a numerical semigroup, then $\mathbb{N} \setminus A$ is finite.

Proof. Let A be a numerical semigroup and suppose that $a, b \in A$ are coprime elements. Then a, b generate the trivial ideal in $\mathbb{Z}$, which implies there are natural numbers m, n such that $ma = 1 + nb$. If $0 \leq r < b$, then $rma = r + rnb \equiv r \bmod b$ is an element of A which is congruent to r modulo b. Furthermore, since $b \in A$ all natural numbers larger than rma which are congruent to $r \bmod b$ will also belong to A. Thus there are finitely many natural numbers which do not belong to A. □

Numerical semigroups always have a generating set of coprime elements.

Lemma 3.3. Let A be a nonzero ideal in $\mathbb{N}$. Then A is a numerical semigroup if and only if $A = \langle a_1, \ldots, a_n \rangle$ for some a_i such that $\gcd(a_1, \ldots, a_n) = 1$.

Proof. First suppose that A is a numerical semigroup. Let $a_1 < a_2 < \ldots$ be an enumeration of the nonzero elements of A in order. Let $A_k := \langle a_1, \ldots, a_k \rangle$. Then $A_k \subseteq A_{k+1}$ and $A = \bigcup_{k \geq 1} A_k$. Since A is a numerical semigroup, there must be some m such that $\gcd(a_1, \ldots, a_m) = 1$. Hence A_m is a numerical semigroup. Proposition 3.2 implies that $A \setminus A_m$ is finite. Therefore $A = A_n$ for some $n \geq m$.

Next suppose that $A = \langle a_1, \ldots, a_n \rangle$ for some a_i such that $\gcd(a_1, \ldots, a_n) = 1$. Since $a_1, \ldots, a_n$ generate the trivial ideal in $\mathbb{Z}$, it follows that, after possibly reordering the a_i, there are natural numbers m_i and some $1 \leq \ell \leq n$ such that

$$m_1 a_1 + \ldots + m_\ell a_\ell = 1 + m_{\ell+1} a_{\ell+1} + \ldots + m_n a_n.$$

Note that $m_1 a_1 + \ldots + m_\ell a_\ell$ and $m_{\ell+1} a_{\ell+1} + \ldots + m_n a_n$ are both elements of A, and the above identity implies that they are coprime. Hence A is a numerical semigroup. □

Every ideal in $\mathbb{N}$ canonically factors as a principal ideal times a numerical semigroup.

Lemma 3.4. If $A \subseteq \mathbb{N}$ is an ideal, then $A = gB$ for some $g \in \mathbb{N}$ and numerical semigroup B.

Proof. If $A = \{0\}$, then $g := 0$ and $B = \mathbb{N}$ will do. Now suppose A is nonzero and let $g := \gcd(A)$. Let $B := \{a/g : a \in A\} \subseteq \mathbb{N}$ and note that B is an ideal of $\mathbb{N}$. Let $b_1 < b_2 < \ldots$ be an enumeration of B and define $g_n := \gcd(b_1, \ldots, b_n)$. Then g_n is a weakly decreasing sequence of natural numbers which converges to 1. Hence there is some n such that $g_n = 1$. Thus $\langle b_1, \ldots, b_n \rangle$ is a numerical semigroup by Lemma 3.3. Therefore B itself is a numerical semigroup. The identity $A = gB$ follows by construction. □

Let A be a numerical semigroup. The **Frobenius number** of A, denoted $F(A)$, is the largest element of $\mathbb{N} \setminus A$. The **genus** of A is the cardinality of $\mathbb{N} \setminus A$. Every numerical semigroup has a unique minimal set of generators. The **embedding dimension** of A is the number of minimal generators of A. For a general overview of numerical semigroups and many references to the literature, we recommend the book by Rosales and García-Sánchez [RG09].

Let NS denote the set of all numerical semigroups together with the zero ideal $\langle 0 \rangle$. Lemma 3.3 together with Lemma 3.4 implies that $\mathbb{N}$ is a Noetherian semiring. Every nonzero element of $\mathbb{N}$ is regular, hence every nonzero ideal in $\mathbb{N}$ is regular and finitely generated. Thus $\mathrm{Ideal}_{\mathrm{rfg}}(\mathbb{N}) = \mathrm{Ideal}(\mathbb{N})$. Furthermore, Lemma 3.3 implies that NS is closed under addition and multiplication of ideals. Thus $\mathrm{NS} \subseteq \mathrm{Ideal}(\mathbb{N})$ is a subsemiring.

While numerical semigroups have been intensely studied, their natural multiplicative structure appears to have been completely overlooked. The multiplicative structure of ideals is of central interest from a number theoretic perspective. One natural question to ask is whether or not ideals in $\mathbb{N}$ factor uniquely into irreducibles. We show in Theorem 3.15 that unique factorization fails at several levels for numerical semigroups. That leaves open the problem of analyzing the multiplicative relations in NS.

3.2. **Multiplicities.** If $A \subseteq \mathbb{N}$ is a nonzero ideal, then the **multiplicity** $m_0(A)$ is the smallest positive element in A. We define $m_0(\{0\}) := \infty$. Clearly we have $m_0(AB) = m_0(A)m_0(B)$ for all ideals A, B. To help us analyze the multiplicative structure of ideals in $\mathbb{N}$ we construct variations on the multiplicity associated to prime ideals in $\mathbb{N}$. Prime ideals are defined identically for semirings as in rings. First we classify the prime ideals in $\mathbb{N}$.

Lemma 3.5. If $P \subseteq \mathbb{N}$ is a prime ideal, then either

(1) $P = \langle p \rangle$ for p a prime number,
(2) $P = \langle 0 \rangle$, or

(3) $P = \langle 2,3\rangle$.

Proof. Clearly $\langle p\rangle$ is a prime ideal when p is prime or $p=0$. Let $P = \langle 2,3\rangle = \{0\}\cup\{n\in\mathbb{N} : n\geq 2\}$. If $a,b\in\mathbb{N}$ are positive integers such that $ab\in P$, then $ab\geq 2$, which implies that either $a\geq 2$ or $b\geq 2$. Thus P is prime.

Conversely, suppose $P\subseteq\mathbb{N}$ is a nonzero prime ideal. Lemma 3.4 implies that $P = gB$ where $g := \gcd(P)$ and B is a numerical semigroup. Let m be the multiplicity of B. Then $gm\in P$, which implies that either $g\in P$ or $m\in P$. Since gm is the smallest positive element of gB, the only way $g\in P$ is if $m=1$. In that case $B=\mathbb{N}$ and $P=\langle p\rangle$. If $m\in P$, then $g=1$ and $P=B$. Proposition 3.2 implies that P is cofinite. Hence $p^k\in P$ for every prime p and all sufficiently large k. Thus $p\in P$ for all primes p. In particular, $2,3\in P$ which implies that $\langle 2,3\rangle\subseteq P$. Since P is a proper ideal, we must have $P=\langle 2,3\rangle$. □

Remark. There are many examples in number theory of objects which are parametrized by prime numbers with one exception. The ur-example of this phenomenon is equivalence classes of absolute values on $\mathbb{Q}$. These patterns led to the idea of a *missing prime* which completes our classification. Motivated by a geometric analogy, this missing prime is often referred to as the *prime at infinity.* Many instances of this phenomenon may be linked back to absolute values. The concept of *places* was created in an attempt to put all the primes, including the prime at infinity, on an equal footing.

However, the analogy is incomplete. Thus it is notable that $\mathbb{N}$ contains exactly one prime ideal not visible in $\mathbb{Z}$. In the sequel we study quotients of arithmetic semirings generalizing $\mathbb{N}$ to higher degree extensions. Although the link between ideals and quotients fractures for semirings, it is also the case that $\mathbb{N}$ has one more semifield quotient than $\mathbb{Z}$. □

Let $P\subseteq\mathbb{N}$ be a prime ideal and let A be an ideal. We define the **prime-to-P multiplicity** $m_P(A) := \min(A\setminus P)$, where we set $\min(\emptyset) := \infty$.

Lemma 3.6. If $A,B\subseteq\mathbb{N}$ are ideals and $P\subseteq\mathbb{N}$ is a prime ideal, then

$$m_P(AB) = m_P(A)m_P(B).$$

Proof. Let $a_P := m_P(A)$ and $b_P := m_P(B)$. Suppose at least one of a_P or b_P is ∞; without loss of generality suppose $a_P=\infty$. Then every element of A belongs to P, hence the same is true for AB. Thus $m_P(AB) = \infty = m_P(A)m_P(B)$.

Now suppose that $a_P, b_P < \infty$. Then $a_Pb_P\in AB\setminus P$ by the definition of a prime ideal. Let $m_P(AB) = a_1b_1+\ldots+a_nb_n$. If a sum belongs to the complement of an ideal, then at least one summand must be in that complement, hence $a_ib_i\in AB\setminus P$ for some i. Hence $a_i, b_i\notin P$. Since $a_i\geq a_P$ and $b_i\geq b_P$ we have $m_P(AB) = a_ib_i\geq a_Pb_P$. Thus $m_P(AB) = a_Pb_P$. □

If $P=\langle p\rangle$, then we write m_p as a shorthand for $m_{\langle p\rangle}$. This is consistent with our notation $m_0(A)$ for the multiplicity of A. If $P=\langle 2,3\rangle$, then

$$m_P(A) = \begin{cases} 1 & \text{if } A=\mathbb{N},\\ \infty & \text{otherwise.}\end{cases}$$

Hence this invariant just captures triviality.

Suppose A,B are numerical semigroups. Then $m_p(A), m_p(B) < \infty$. If $A\sim B$, then there is some ideal C such that $AC=BC$. Thus

$$m_p(A)m_p(C) = m_p(AC) = m_p(BC) = m_p(B)m_p(C).$$

Positive integers are multiplicatively cancellative, hence $m_p(A) = m_p(B)$. Therefore the functions m_p are invariants of similarity classes.

Let $\mathbb{N}_{\min}$ be the semiring with underlying set $\mathbb{N}\cup\{\infty\}$ and operations $a\oplus b := \min(a,b)$ and $a\otimes b := ab$. We call $\mathbb{N}_{\min}$ the **tropical min-times semiring**. Note that ∞ is the additive identity and 1 is the multiplicative identity in $\mathbb{N}_{\min}$. Observe that each m_p defines a semiring homomorphism from Ideal($\mathbb{N}$) to $\mathbb{N}_{\min}$.

The m_p invariants may be usefully extended to sequence $m_{p,k}$ of invariant functions. Given a prime $p \in \mathbb{N}$ let v_p denote the p-adic valuation. If A is an ideal, let

$$m_{p,k}(A) := \min\{a \in A : v_p(a) \leq k\}.$$

Note that $m_{p,0}(A) = m_p(A)$. The values of $m_{p,k}(A)$ may in general be infinite, but if A is a numerical semigroup, then $m_{p,k}(A) < \infty$.

The $m_{p,k}$ invariants always take values among the generators of an ideal.

Lemma 3.7. *If $A = \langle a_1, \ldots, a_n \rangle$ is a numerical semigroup, then for each k we have $m_{p,k}(A) = a_i$ for some i.*

Proof. Let $a := m_{p,k}(A)$. Then $a \in A$ implies there are some $b_i \in \mathbb{N}$ such that

$$a = a_1 b_1 + \ldots + a_n b_n.$$

The ultrametric inequality implies that

$$k \geq v_p(a) \geq \min_i \{v_p(a_i) + v_p(b_i)\}.$$

Hence there is some i such that $b_i \neq 0$ and $v_p(a_i) \leq k$. Since $a_i \leq a$, the minimality of a implies that $a_i = a = m_{p,k}(A)$. □

When $k > 0$ the invariants $m_{p,k}$ are not multiplicative, but rather satisfy a min-times convolution identity.

Lemma 3.8. *Let p be a prime and let $A, B \subseteq \mathbb{N}$ be ideals. Then*

$$m_{p,k}(AB) = \min_{i+j=k} \{m_{p,i}(A) m_{p,j}(B)\}.$$

Proof. Suppose that $c := a_1 b_1 + \ldots + a_n b_n \in AB$ has $v_p(c) \leq k$. Then the ultrametric inequality implies that $v_p(a_i b_i) \leq k$ for some i. Hence $\min\{c \in AB : v_p(c) \leq k\}$ is achieved by some product ab. In particular,

$$\begin{aligned} m_{p,k}(AB) &= \min\{ab : a \in A, b \in B, v_p(ab) \leq k\} \\ &= \min_{i+j \leq k} \{m_{p,i}(A) m_{p,j}(B)\} \\ &= \min_{i+j=k} \{m_{p,i}(A) m_{p,j}(B)\}, \end{aligned}$$

where the last equality follows from the fact that $m_{p,k}(A)$ is weakly decreasing with k. □

Lemma 3.8 suggests that the $m_{p,k}$ invariants may be nicely packaged into a tropical generating function. Note that the well-ordering principle implies that arbitrary sums (finite or infinite) in $\mathbb{N}_{\min}$ are well-defined. Let $\mathbb{N}_{\min}[\![T]\!]$ be the semiring of formal power series in the variable T with coefficients in $\mathbb{N}_{\min}$. The additive identity in $\mathbb{N}_{\min}[\![T]\!]$ is $\sum_{k \geq 0} \infty T^k$ and the multiplicative identity is $1 + \sum_{k \geq 1} \infty T^k$.

Lemma 3.9. *Let $\mathrm{Dec} \subseteq \mathbb{N}_{\min}[\![T]\!]$ be the set of all series $\sum_{k \geq 0} a_k T^k$ such that (a_k) is a weakly decreasing sequence. Then Dec forms a semiring with the same operations and additive identity as $\mathbb{N}_{\min}[\![T]\!]$, but with multiplicative identity $\frac{1}{1-T} := \sum_{k \geq 0} T^k$.*

Proof. Let (a_k) be an arbitrary sequence in $\mathbb{N}_{\min}$. If we define (b_k) by

$$\sum_{k \geq 0} b_k T^k := \frac{1}{1-T} \sum_{k \geq 0} a_k T^k,$$

then expanding the product we have

$$\sum_{k\geq 0} b_k T^k = \sum_{k\geq 0}\Big(\bigoplus_{j=0}^{k} a_j\Big)T^k = \sum_{k\geq 0}\min_{0\leq j\leq k}\{a_j\}T^k$$

The sequence $b_k = \min_{0\leq j\leq k}\{a_j\}$ is weakly decreasing. Furthermore, if a_k is already weakly decreasing, then $b_k = a_k$. In particular $\left(\frac{1}{1-T}\right)^2 = \frac{1}{1-T}$. Thus $\frac{1}{1-T}$ is an idempotent which projects $\mathbb{N}_{\min}[\![T]\!]$ onto Dec, which implies that Dec is precisely all multiples of $\frac{1}{1-T}$ in $\mathbb{N}_{\min}[\![T]\!]$. Hence Dec is closed under addition and multiplication; Dec contains the zero element $\frac{\infty}{1-T}$ by definition. □

Let $S_p : \mathrm{Ideal}(\mathbb{N}) \to \mathrm{Dec}$ be the function defined by

$$S_p(A) := \sum_{k\geq 0} m_{p,k}(A)T^k.$$

If $A \neq \langle 0\rangle$, then we have the alternative formula

$$S_p(A) = \frac{1}{1-T}\sum_{a\in A} aT^{v_p(a)}. \tag{3.2.1}$$

Lemma 3.10. If p is a prime, then S_p is a semiring homomorphism.

Proof. Let $A, B \in \mathrm{Ideal}(\mathbb{N})$. The ultrametric inequality $v_p(a+b) \geq \min\{v_p(a), v_p(b)\}$ and $a+b \geq a, b$ imply that the min $m_{p,k}(A+B)$ is achieved by an element of A or B, hence that $m_{p,k}(A+B) = \min\{m_{p,k}(A), m_{p,k}(B)\}$. Hence

$$\begin{aligned}
S_p(A+B) &= \sum_{k\geq 0} m_{p,k}(A+B)T^k\\
&= \sum_{k\geq 0}\min\{m_{p,k}(A), m_{p,k}(B)\}T^k\\
&= \sum_{k\geq 0}(m_{p,k}(A)\oplus m_{p,k}(B))T^k\\
&= S_p(A)\oplus S_p(B).
\end{aligned}$$

If A or B is the zero ideal, then so is AB and thus $S_p(AB) = S_p(A)S_p(B)$. Now suppose that neither A nor B is zero, hence neither is AB. As we argued in Lemma 3.8, the minimum defining $m_{p,k}(AB)$ is achieved by a product ab. Therefore

$$\begin{aligned}
S_p(AB) &= \frac{1}{1-T}\sum_{\substack{a\in A\\ b\in B}} abT^{v_p(ab)}\\
&= \frac{1}{1-T}\sum_{\substack{a\in A\\ b\in B}} abT^{v_p(a)+v_p(b)}\\
&= \Big(\frac{1}{1-T}\Big)^2\sum_{a\in A} aT^{v_p(a)}\sum_{b\in B} bT^{v_p(b)}\\
&= S_p(A)S_p(B).
\end{aligned}$$

Clearly $S_p(\langle 0\rangle) = \frac{\infty}{1-T}$ and $S_p(\langle 1\rangle) = \frac{1}{1-T}$. Thus S_p is a semiring homomorphism. □

3.3. **Irreducibility Criteria.** The m_p invariants provide a simple means by which to test the irreducibility of ideals and, even better, similarity classes of ideals.

Lemma 3.11. Let $A \subseteq \mathbb{N}$ be an ideal and let $p \in \mathbb{N}$ be prime or zero. If $m_p(A)$ is prime, then A is irreducible in $\mathrm{Ideal}(\mathbb{N})$ and $[A]$ is irreducible in $[\mathrm{Ideal}(\mathbb{N})]$.

Proof. If $A = BC$, then $[A] = [B][C]$, hence it suffices to prove that $m_p(A)$ being prime implies $[A]$ is irreducible. If $[A] = [B][C]$, then $m_p(A) = m_p(B)m_p(C)$. Note that $m_p(B) = 1$ if and only if $B = \langle 1 \rangle$. Thus if $[B]$ and $[C]$ are nontrivial classes, then $m_p(A)$ is composite. This is the contrapositive of our claim. □

Remark. The notion of an *irreducible numerical semigroup* has other meanings in the literature. For instance, in [RG09] they define an irreducible numerical semigroup to be one that is not the intersection of two numerical semigroups which properly contain it. We will not be making any further reference to that notion of irreducibility with respect to intersections, and hence for this work, we use irreducibility to mean irreducibility with respect to multiplication of ideals.

The next result provides three more irreducibility tests, none of which apply to similarity classes.

Proposition 3.12. Let $A \subseteq \mathbb{N}$ be a numerical semigroup. If any of the following conditions holds, then A is irreducible.

(1) A has two minimal generators.
(2) A has a prime minimal generator.
(3) $m_{p,0}(A)$ and $m_{p,\ell}(A)$ are coprime, where p is prime and ℓ is the smallest index such that $m_{p,\ell}(A) < m_{p,0}(A)$.

Proof. (1) Let $A = \langle m, n \rangle$ with $m < n$ coprime. Suppose $A = BC$ where $B = \langle b_1, \dots, b_r \rangle$ and $C = \langle c_1, \dots, c_s \rangle$ are minimal generators where $b_1, c_1 > 1$ and the b_i, c_i are strictly increasing. Then $m = b_1c_1$. The next two smallest generators of BC are b_1c_2 and b_2c_1. Suppose without loss of generality that $b_1c_2 \le b_2c_1$. If b_1c_2 is not a minimal generator for BC, then it must be a multiple of b_1c_1, but that is equivalent to c_2 being a multiple of c_1. This contradicts our assumption that c_2 is a minimal generator of C. Hence $n = b_1c_2$. However $b_1 > 1$ divides both m and n, which contradicts our assumption that m and n are coprime. Thus A is irreducible.

(2) If $B = \langle b_1, \dots, b_m \rangle$ and $C = \langle c_1, \dots, c_n \rangle$, then $BC = \langle b_ic_j : 1 \le i \le m, 1 \le j \le n \rangle$. The minimal generators for BC are contained in this list of products. Thus, if any minimal generator of A is prime, then either B or C must contain 1, which implies that A is irreducible.

(3) Suppose that $A = BC$. Then Lemma 3.8 implies that for all $k \ge 0$ we have

$$m_{p,k}(A) = \min_{i+j=k} \{m_{p,i}(B)m_{p,j}(C)\}.$$

If i' and j' are the first indices where $m_{p,i'}(B) < m_{p,0}(B)$ and $m_{p,j'}(C) < m_{p,0}(C)$ and $\ell = \min\{i', j'\}$, then for all $k < \ell$ and $i+j = k$, we must have $m_{p,i}(B) = m_{p,0}(B)$ and $m_{p,j}(C) = m_{p,0}(C)$. Thus $m_{p,k}(A) = m_{p,0}(B)m_{p,0}(C) = m_{p,0}(A)$. At index $k = \ell$ we get the first decrease in $m_{p,k}(A)$,

$$m_{p,\ell}(A) = \min_{i+j=\ell} \{m_{p,i}(B)m_{p,j}(C)\} = \min\{m_{p,\ell}(B)m_{p,0}(C), m_{p,0}(B)m_{p,\ell}(C)\} < m_{p,0}(A).$$

This identity implies that $m_{p,\ell}(A)$ is divisible by either $m_{p,0}(B)$ or $m_{p,0}(C)$, which are proper factors of $m_{p,0}(A)$. Thus, taking the contrapositive, if $m_{p,0}(A)$ and $m_{p,\ell}(A)$ are coprime where ℓ is the index of the first decrease, then A must be irreducible. □

3.4. **Failure of Unique Factorization.** In this section we show that unique factorization fails for the multiplicative monoids $\mathrm{Ideal}(\mathbb{N})$ and $[\mathrm{Ideal}(\mathbb{N})]$.

Let $S = \langle m, n \rangle$ where $m < n$ are coprime. Proposition 3.12(1) implies that S is irreducible.

Lemma 3.13. The minimal generators of S^k are $m^i n^j$ where $i, j \geq 0$ and $i + j = k$. Hence S^k has embedding dimension $k + 1$.

Proof. Note that since $m < n$, if $i_1 + j_1 = i_2 + j_2$, then we have $m^{i_1} n^{j_1} < m^{i_2} n^{j_2}$ if and only if $j_1 < j_2$. Suppose for the sake of contradiction that $m^i n^j$ with $i + j = k$ is the smallest redundant generator. Then we must have $j > 0$ since m^k is the smallest element in S^k. Hence $m^i n^j \in S' := \langle m^k, m^{k-1}n, \ldots, m^{i+1}n^{j-1}\rangle$. However, note that each of the generators of S' is divisible by m^{i+1}, which implies that m^{i+1} divides $m^i n^j$. But then we must have $m \mid n^j$, which contradicts m and n coprime. Therefore none of the $m^i n^j$ are redundant. $\square$

Given a finite set $E \subseteq \mathbb{N}$ with $\max E = k$, let

$$S^E := \langle m^{k-j} n^j : j \in E\rangle.$$

Note that S^E is a numerical semigroup if and only if $0 \in E$. For example, let $[k] := \{0, 1, \ldots, k\}$, then $S^{[k]} = S^k$. If $E_1, E_2 \subseteq \mathbb{N}$, let $E_1 + E_2 = \{e_1 + e_2 : e_i \in E_i\}$ denote the sumset. By comparing generators we have

$$S^{E_1} S^{E_2} = S^{E_1 + E_2}.$$

Let $[k]^* := \{0, k\}$. Then $S^{[k]^*} = \langle m^k, n^k\rangle$ is an irreducible numerical semigroup by Proposition 3.12(1). Observe that

$$[2] + [3]^* = \{0, 1, 2\} + \{0, 3\} = [5].$$

Hence we have

$$S^2 S^{[3]^*} = S^{[2]+[3]^*} = S^{[5]} = S^5. \tag{3.4.1}$$

The left hand side of this product has three irreducible factors, and the right side has five. Thus unique factorization fails for Ideal($\mathbb{N}$).

Another similar example:

$$[1] + [2]^* + [2]^* = \{0, 1\} + \{0, 2\} + \{0, 2\} = [5].$$

Hence we also have

$$S^1 S^{[2]^*} S^{[2]^*} = S^5. \tag{3.4.2}$$

Digit expansions, including with mixed base, give rise to endless variations on these examples. This encoding of sumset arithmetic into the multiplicative structure of numerical semigroups demonstrates how flexible the failure of unique factorization is for ideals in $\mathbb{N}$.

Remark. If $A = \langle a_1, \ldots, a_m\rangle$ and $B = \langle b_1, \ldots, b_n\rangle$ are ideals, then the minimal generators of AB are a subset of the products $a_i b_j$. Thus we may effectively compute all factorizations of a given ideal. We have implemented this factorization algorithm in Python together with all the other invariants and operations discussed in this paper as part of a class of ideals in $\mathbb{N}$. This code is available at `https://github.com/tghyde/numerical-ideals`.

All the examples of non-unique factorization constructed so far may be resolved by passing to similarity classes.

Lemma 3.14. If $E \subseteq \mathbb{N}$ is a finite set with $\min E = 0$ and $\max E = k$, then $S^E \sim S^k$.

Proof. Since $S^{[k]^*} \subseteq S^E \subseteq S^k$, we have $\overline{S^{[k]^*}} \subseteq \overline{S^E} \subseteq \overline{S^k}$ by Lemma 2.18. Thus it suffices to prove that each generator of S^k is integral over $S^{[k]^*}$ by Proposition 2.20. Let $m^i n^j$ with $i + j = k$ be a generator of S^k. Observe that $(m^i n^j)^k = m^{ki} n^{kj} \in (S^{[k]^*})^k$. Hence Corollary 2.13 implies that $m^i n^j$ is integral over $S^{[k]^*}$. $\square$

Thus Lemma 3.14 implies that the factorizations in (3.4.1) and (3.4.2) both resolve to $[S]^5$ in [Ideal($\mathbb{N}$)]. This leaves open the possibility that similarity classes factor uniquely into irreducibles. However, the next theorem shows that unique factorization also fails in [Ideal($\mathbb{N}$)]. We produce an infinite family of counterexamples to unique factorization and another family of examples to show that the number of irreducible factors in a factorization is also not an invariant of a similarity class.

Theorem 3.15. The semigroup [Ideal($\mathbb{N}$)] of similarity classes of ideals in $\mathbb{N}$ does not have unique factorization. More precisely,

(1) If $a < b$ are primes and $c \geq 1$ such that $b < ac$ and $b \nmid c$, let $A = \langle a, b\rangle$ and $B = \langle b, ac\rangle$ be numerical semigroups. Suppose $d \in AB$ is any prime such that $d > a$. Let $C = \langle ab, a^2c, d\rangle$ and $D = \langle a^2, ab, d\rangle$. Then $[A], [B], [C], [D]$ are irreducible, distinct similarity classes and
$$AC = BD.$$

(2) The number of irreducible factors is not invariant. Let $k \geq 2$ and define numerical semigroups $A := \langle 2, 3\rangle$ and $B := \langle 2, 3^k\rangle$. Let $d \in A^kB$ be any odd prime. Define $C := \langle 4, 2\cdot 3^k, d\rangle$ and $D := \langle 2^{k+1}, 2^k \cdot 3, \ldots, 2 \cdot 3^k, d\rangle$. Then $[A], [B], [C], [D]$ are irreducible, distinct similarity classes and
$$A^kC = BD.$$

Proof. (1) The numerical semigroups A and B have prime multiplicities, hence $[A]$ and $[B]$ are irreducible. Note that a is a prime distinct from d. Hence $m_a(C) = m_a(D) = d$ and Lemma 3.11 implies that $[C]$ and $[D]$ are irreducible. The ideals A, B, C, D have distinct multiplicities, hence generate pairwise distinct similarity classes. Observe that
$$C = \langle ab, a^2c, d\rangle = aB + \langle d\rangle \qquad D = \langle a^2, ab, d\rangle = aA + \langle d\rangle.$$
Thus
$$AC = aAB + dA \qquad BD = aAB + dB.$$
We have $dA = \langle ad, bd\rangle$ and $dB = \langle bd, acd\rangle$. Since $d \in AB$ by assumption, $ad, acd \in aAB$. Therefore
$$AC = aAB + dA = aAB + \langle bd\rangle = aAB + dB = BD.$$

(2) The argument that $[A], [B], [C], [D]$ are irreducible is the same as in part (1). The similarity classes are distinguished by considering m_0 and m_2 for each ideal. The proof of equality is also essentially the same: Observe that $C = 2B + \langle d\rangle$ and $D = 2A^k + \langle d\rangle$. Thus
$$A^kC = 2A^kB + dA^k \qquad BD = 2A^kB + dB.$$
Since $d \in A^kB$ by assumption, we have
$$A^kC = 2A^kB + \langle 3^kd\rangle = BD.$$
Thus one similarity class can have an irreducible factorization with 2 terms or $k + 1$ terms. ☐

Ideals were introduced to arithmetic as a means of correcting the failure of unique factorization in extensions of the integers. It is ironic that ideals bring non-unique factorization to the natural numbers, the genesis of unique factorization. Could there be some extension or refinement of similarity classes that resolves the distinct factorizations highlighted in Theorem 3.15? It seems unlikely to us, based on the nature of these examples, but we would be happy to be proven wrong.

4. Two-Generator Numerical Semigroups

Numerical semigroups with two generators $\langle m, n\rangle$ play a special role in the theory. These are the simplest numerical semigroups and many of their properties and invariants can be worked out explicitly (whereas such formulas for numerical semigroups with more than two minimal generators are generally unavailable). In this section we show that these exceptional properties extend to powers of two-generator numerical semigroups as well. Finally, we use our analysis of this particular family in order to study the asymptotic behavior of the genus and Frobenius numbers along the sequence of powers of any numerical semigroup (see Theorem 4.11).

4.1. **Apéry Sets.** The **Apéry set** of a numerical semigroup A with respect to an integer m is

$$\mathrm{Ap}_m(A) := \{a \in A : a - m \notin A\}.$$

Equivalently, $\mathrm{Ap}_m(A)$ consists of the smallest elements in each congruence class modulo m (which exist by Proposition 3.2). Typically we consider the Apéry set of A with respect to the multiplicity $m = m_0(A)$, and we denote that case simply by $\mathrm{Ap}(A)$ and call it the Apéry set of A. The Apéry set is a fundamental invariant of a numerical semigroup, essential for computing other invariants and testing membership in A. If $S = \langle m, n\rangle$, then m coprime to n clearly implies that

$$\mathrm{Ap}(S) = \{jn : 0 \le j < m\}.$$

The following proposition extends this Apéry calculation to all powers of $\langle m, n\rangle$.

Theorem 4.1. If $S = \langle m, n\rangle$ where $m < n$ are coprime, then

$$\mathrm{Ap}(S^k) = \{j_1 m^{k-1} n + j_2 m^{k-2} n^2 + \ldots + j_k n^k : 0 \le j_i < m\}.$$

Proof. Let $M := \{j_1 m^{k-1} n + j_2 m^{k-2} n^2 + \ldots + j_k n^k : 0 \le j_i < m\}$. Suppose that

$$j_1 m^{k-1} n + \ldots + j_k n^k \equiv \ell_1 m^{k-1} n + \ldots + \ell_k n^k \bmod m^k \tag{4.1.1}$$

for some $0 \le j_i, \ell_i < m$. We will prove by strong induction on i that $j_{k-i} = \ell_{k-i}$ for all $0 \le i < k$. Now suppose that $0 \le i < k$ and that $j_{k-i'} = \ell_{k-i'}$ for $0 \le i' < i$. Then (4.1.1) simplifies to

$$j_1 m^{k-1} n + \ldots + j_{k-i} m^i n^{k-i} \equiv \ell_1 m^{k-1} n + \ldots + \ell_{k-i} m^i n^{k-i} \bmod m^k,$$

which is equivalent to

$$j_1 m^{k-i-1} n + \ldots + j_{k-i} n^{k-i} \equiv \ell_1 m^{k-i-1} n + \ldots + \ell_{k-i} n^{k-i} \bmod m^{k-i}.$$

Reducing this congruence modulo m gives us

$$j_{k-i} n^{k-i} \equiv \ell_{k-i} n^{k-i} \bmod m,$$

and n coprime to m implies that $j_{k-i} \equiv \ell_{k-i} \bmod m$. Since $0 \le j_{k-i}, \ell_{k-i} < m$, this is equivalent to $j_{k-i} = \ell_{k-i}$. That completes our induction and allows us to conclude that all the elements of M are distinct modulo m^k.

Suppose $a \in \mathrm{Ap}(S^k)$. Then

$$a = j_1 m^{k-1} n + \ldots + j_k n^k$$

for some natural numbers $j_i \ge 0$; note that no m^k term is needed by the definition of the Apéry set. Since M contains m^k elements which are all distinct modulo m^k, it follows that there is some $b = \ell_1 m^{k-1} n + \ldots + \ell_k n^k \in M$ such that $a \equiv b \bmod m^k$. The definition of the Apéry set implies that $a \le b$. Reducing $a \equiv b \bmod m^k$ modulo m we conclude that $j_k \equiv \ell_k \bmod m$, hence $j_k \ge \ell_k$.

Let $\delta_i := \ell_i - j_i$. Then $\delta_i < m$ for each i, $\delta_k \le 0$, $m \mid \delta_k$, and

$$\delta_1 m^{k-1} n + \ldots + \delta_k n^k \equiv 0 \bmod m^k. \tag{4.1.2}$$

For $1 \le j \le k$, reducing (4.1.2) modulo m^j and canceling common powers of n from both sides we see that there exists an integer g_j such that

$$\delta_{k-j+1}m^{j-1} + \delta_{k-j+2}m^{j-2}n + \ldots + \delta_k n^{j-1} = g_j m^j.$$

We prove by induction that $g_j \le 0$ for all j; the base case follows immediately from $g_1 m = \delta_k \le 0$. Now suppose $g_j \le 0$ and observe that

$$g_j m^{j+1} = \delta_{k-j}m^j + ng_j m^j,$$

hence

$$g_{j+1}m = g_j n + \delta_{k-j} \le \delta_{k-j} < m.$$

Hence $g_{j+1} \le 0$, which completes our induction. On the other hand,

$$g_k m^k = \delta_1 m^{k-1}n + \ldots + \delta_k n^k = b - a \ge 0,$$

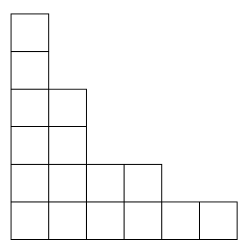
which implies that $g_k \ge 0$. Combined with $g_k \le 0$ we conclude that $g_k = 0$ and hence that $a = b$. Therefore every element of the Apéry set belongs to M and comparing cardinalities we conclude that $M = \mathrm{Ap}(S^k)$. □

4.2. **Symmetry.** If A is a numerical semigroup, let χ_A denote its characteristic function. Proposition 3.2 implies that the sequence $(\chi_A(n))_{n\in\mathbb{N}}$ is eventually all 1's. A binary sequence which is eventually constant equal to 1 encodes a partition: Starting at $(0, g(A))$ on the y-axis, interpret each 0 as a step down, and each 1 as a step to the right. The resulting path, together with the positive x- and y-axes, bounds a Young diagram of a partition.

Example 4.2. Let $A = \langle 3, 7\rangle$. The characteristic sequence of A is

$$100100110110111\ldots$$

and the corresponding Young diagram is



□

Note that the partition in Example 4.2 is symmetric with respect to reflection across the diagonal. A **symmetric** numerical semigroup is one for which its corresponding partition is symmetric. Equivalently, A is symmetric when $n \in A$ if and only if $F(A) - n \notin A$ (see [BM07, Prop. 2.2, Cor. 2.3]). Thus Example 4.2 shows that $\langle 3, 7\rangle$ is symmetric. Furthermore, it is known that every two-generator numerical semigroup is symmetric (see, e.g. [RG09, Cor. 4.7]). We show that powers of two-generator numerical semigroups are always symmetric.

Corollary 4.3. If $S = \langle m, n\rangle$ where $m < n$ are coprime, then S^k is symmetric for all $k \ge 0$.

Proof. If $k = 0$, then $S^k = \mathbb{N}$ which corresponds to the empty partition, hence is trivially symmetric. Suppose that $k \ge 1$. Theorem 4.1 implies that

$$F(S^k) = \max_{w\in \mathrm{Ap}(S^k)} w - m_0(S^k) = (m-1)m^{k-1}n + \ldots + (m-1)n^k - m^k.$$

If $a \in \mathbb{N}$, then we can write

$$a = j_1 m^{k-1}n + \ldots + j_k n^k + bm^k,$$

where $0 \le j_i < m$ and $b \in \mathbb{Z}$. Note that $a \in S^k$ if and only if $b \ge 0$. Thus

$$F(S^k) - a = (m-1-j_1)m^{k-1}n + \ldots + (m-1-j_k)n^k - (b+1)m^k.$$

Since $0 \le m-1-j_i < m$ for each i, Theorem 4.1 implies that $F(S^k) - a \in S^k$ if and only if $b < 0$. Therefore $a \in S^k$ if and only if $F(S^k) - a \notin S^k$, which is to say that S^k is symmetric. □

Remark. Powers of $\langle m, n\rangle$ provide a simple family of examples of symmetric numerical semigroups with arbitrary embedding dimension.

Moving beyond two-generator numerical semigroups, the situation is more complicated. There are numerical semigroups A that are symmetric, but which have non-symmetric powers. For example, $A = \langle 4, 6, 7\rangle$ is symmetric, but A^2 is not symmetric. There are also examples where A is not symmetric but A^2 is symmetric, though these are harder to find. For example, $A = \langle 12, 18, 20, 39, 67\rangle$ is not symmetric, but A^2 is symmetric.

We can refine this analysis by consider how *type* behaves under taking powers. Let $A \subseteq \mathbb{N}$ be a numerical semigroup. Given $a, b \in \mathbb{N}$ we say $a \le_A b$ if $b - a \in A$. The relation $\le_A$ defines a partial order on $\mathbb{N}$. The **pseudo-Frobenius numbers** of A are the maximal elements of $\mathbb{N} \setminus A$ with respect to $\le_A$. Let $\mathrm{PF}(A)$ denote the set of all pseudo-Frobenius numbers. The **type** of A is $\mathrm{t}(A) := |\mathrm{PF}(A)|$. If $m \in \mathbb{N}$, let $\mathrm{Max}_m(A)$ denote the set of maximal elements of $\mathrm{Ap}_m(A)$ with respect to $\le_A$. A numerical semigroup A is symmetric if and only if $\mathrm{t}(A) = 1$ (see [RG09, Prop. 2.19]).

Question 4.4. Let $A \subseteq \mathbb{N}$ be a numerical semigroup. Does $\lim_{k\to\infty} \log \mathrm{t}(A^k)/k$ exist? If so, how do we express this limit in terms of other invariants of A?

Note that $\mathrm{t}(A) \le m_0(A) - 1$ for all numerical semigroups A (see [RG09, Cor. 2.23]). Hence $\mathrm{t}(A^k) \le m_0(A)^k - 1$, which implies that

$$\limsup_{k\to\infty} \frac{\log \mathrm{t}(A^k)}{k} \le m_0(A).$$

However Corollary 4.3 implies this bound is not sharp.

The next proposition allows us to show that $\mathrm{t}(A^k)$ grows monotonically in many examples; it generalizes a result due to Nari [Nar13, Prop. 6.6].

Proposition 4.5. Let $A, B \subseteq \mathbb{N}$ be numerical semigroups and let $m, n \in \mathbb{N}$ be coprime natural numbers such that $n \in A$. Then

$$\mathrm{PF}(mA + nB) = m\mathrm{PF}(A) + n\mathrm{Max}_m(B),$$

and

$$\mathrm{t}(mA + nB) = \mathrm{t}(A)|\mathrm{Max}_m(B)|.$$

Proof. Let $C := mA + nB$. Given $b \in \mathrm{Ap}_m(B)$, let $C_b := mA + nb$. Since m and n are coprime we have

$$C = \bigsqcup_{b\in \mathrm{Ap}_m(B)} C_b. \tag{4.2.1}$$

Suppose $a \in \mathrm{PF}(A)$ and $b \in \mathrm{Max}_m(B)$ and define

$$c := ma + nb.$$

Note that $a \notin A$ implies that $c \notin C$. Let $d \in C$ be a nonzero element. The decomposition (4.2.1) implies that $d = ma' + nb'$ for some $a' \in A$ and some $b' \in \mathrm{Ap}_m(B)$. The definition of $\mathrm{Ap}_m(B)$ tells us that

$$b + b' = b'' + me$$

for some $b'' \in \mathrm{Ap}_m(B)$ and $e \in \mathbb{N}$. Thus

$$\begin{aligned} c + d &= (ma + nb) + (ma' + nb') \\ &= m(a + a') + n(b + b') \\ &= m(a + a') + n(b'' + me) \\ &= m(a + a' + ne) + nb''. \end{aligned}$$

Since $a \in \mathrm{PF}(A)$ and $a', n \in A$ we have $a + a' + ne \in A$ if and only if $a' + ne \neq 0$. If $a' + ne = 0$, then $a' = e = 0$. Hence $b + b' = b''$, which gives us $b \leq_B b''$. Our assumption that $b \in \mathrm{Max}_m(B)$ then implies that $b = b''$, which is to say that $b' = 0$. But then $d = ma' + nb' = 0$, contradicting our assumption that d was nonzero. Hence $c \in \mathrm{PF}(C)$. Therefore $m\mathrm{PF}(A) + n\mathrm{Max}_m(B) \subseteq \mathrm{PF}(C)$.

Let $c \in \mathrm{PF}(C)$ and define b to be the unique element of $\mathrm{Ap}_m(B)$ such that $c \equiv nb \bmod m$. Hence $c = ma + nb$ for some integer a. Since $c \notin C$ we must have $a \notin A$ by (4.2.1). For every positive $a' \in A$ we have $c + ma' \in C$ by definition of pseudo-Frobenius elements. Hence

$$c + ma' = (ma + nb) + ma' = m(a + a') + nb \in C$$

and (4.2.1) implies that $a + a' \in A$. Therefore $a \in \mathbb{N}$ and in fact $a \in \mathrm{PF}(A)$. Suppose $b \notin \mathrm{Max}_m(B)$. Then we can write $b + b' = b''$ where $b'' \in \mathrm{Ap}_m(B)$ and $b' \in B$ is positive. Hence $nb' \in C$ is positive and thus $c + nb' \in C$. However

$$c + nb' = (ma + nb) + nb' = ma + n(b + b') = ma + nb'' \in C,$$

and (4.2.1) implies that $a \in A$, a contradiction. Therefore $b \in \mathrm{Max}_m(B)$. Hence $\mathrm{PF}(C) \subseteq m\mathrm{PF}(A) + n\mathrm{Max}_m(B)$, and we conclude that the sets are equal. Since m and n are coprime, the decomposition

$$\mathrm{PF}(C) = m\mathrm{PF}(A) + n\mathrm{Max}_m(B)$$

gives us a bijection $\mathrm{PF}(C) \cong \mathrm{PF}(A) \times \mathrm{Max}_m(B)$. Thus

$$\mathrm{t}(C) = \mathrm{t}(A)|\mathrm{Max}_m(B)|. \qquad \square$$

Remark. If $m \in B$, then $\mathrm{Max}_m(B) = \mathrm{PF}(B) + m$ and $|\mathrm{Max}_m(B)| = \mathrm{t}(B)$. Thus we get

$$\mathrm{t}(mA + nB) = \mathrm{t}(A)\mathrm{t}(B)$$

in that case, which is precisely the conclusion of Nari's result. Our result does not require $m \in B$, but gives a similar conclusion.

Example 4.6. Proposition 4.5 gives an alternative proof that for $A := \langle m, n\rangle$ the powers A^k is symmetric for all $k \geq 1$. Note that $A^{k+1} = \langle m, n\rangle A^k = mA^k + n^k A$, m and n^k are coprime, and $n^k \in A^k$. Hence Proposition 4.5 implies that $\mathrm{t}(A^{k+1}) = \mathrm{t}(A^k)|\mathrm{Max}_m(A)|$. Since $m \in A$, Remark 4.2 gives $|\mathrm{Max}_m(A)| = \mathrm{t}(A) = 1$, and thus by induction that $\mathrm{t}(A^k) = \mathrm{t}(A) = 1$ for all $k \geq 1$. Hence A^k is symmetric for all $k \geq 1$. $\square$

The next proposition allows us to construct examples where we can answer Question 4.4.

Proposition 4.7. Let $m \geq 1$ and let B be a numerical semigroup with $n \in B$ coprime to m. If $A := \langle m\rangle + B$ and $B^2 \subseteq mA + nB$, then $\mathrm{t}(A^k) = \mathrm{t}(A)|\mathrm{Max}_m(B)|^{k-1}$ for all $k \geq 1$. In particular,

$$\lim_{k\to\infty} \frac{\log \mathrm{t}(A^k)}{k} = \log |\mathrm{Max}_m(B)|.$$

Proof. First observe that

$$A^{k+1} = (\langle m\rangle + B)A^k = mA^k + B^{k+1}.$$

Our assumption $B^2 \subseteq mA + nB$ allows us to make a simple inductive argument that for all $k \geq 1$

$$B^{k+1} \subseteq mA^k + n^k B,$$

hence

$$A^{k+1} = mA^k + n^k B.$$

Since $n^k \in A^k$, Proposition 4.5 implies that

$$\mathrm{t}(A^{k+1}) = \mathrm{t}(A^k)|\mathrm{Max}_m(B)|.$$

Thus a simple induction implies that $\mathrm{t}(A^k) = \mathrm{t}(A)|\mathrm{Max}_m(B)|^{k-1}$ for all $k \geq 1$. Hence

$$\lim_{k\to\infty} \frac{\log \mathrm{t}(A^k)}{k} = \log|\mathrm{Max}_m(B)|. \qquad \square$$

Example 4.8. Let $A := \langle 4, 7, 9\rangle = \langle 4\rangle + B$ where $B := \langle 7, 9\rangle$, and let $n = 7$. Then $B^2 = \langle 49, 63, 81\rangle$. Clearly $49, 63 \in 7B$ and $81 = 4\cdot 8 + 7\cdot 7 \in 4A + 7B$, hence $B^2 \subseteq 4A + 7B$. Therefore Proposition 4.7 implies that

$$\mathrm{t}(A^{k+1}) = \mathrm{t}(A^k)|\mathrm{Max}_4(B)|.$$

Note that $\mathrm{Ap}_4(B) = \{0, 7, 9, 14\}$, hence $\mathrm{Max}_4(B) = \{9, 14\}$. Thus by induction and $\mathrm{t}(A) = 2$ it follows that $\mathrm{t}(A^k) = 2^k$. $\square$

We close this section with one final application of Proposition 4.5.

Proposition 4.9. Let $1 < m < n_1 < n_2$ be coprime integers. If $n_1 \equiv n_2 \bmod m$, then the product $\langle m, n_1\rangle\langle m, n_2\rangle$ is symmetric.

Proof. Let $A := \langle m, n_1\rangle$, $B := \langle m, n_2\rangle$, and $C := AB$. By definition we have

$$C = \langle m, n_1\rangle\langle m, n_2\rangle = mA + n_2A. \tag{4.2.2}$$

Since $n_1 < n_2$ and $n_1 \equiv n_2 \bmod m$, we have $n_2 \in A$. Thus Proposition 4.5 and Remark 4.2 imply that $\mathrm{t}(C) = \mathrm{t}(A)|\mathrm{Max}_m(A)| = \mathrm{t}(A)^2 = 1$. Therefore C is symmetric. $\square$

4.3. **Frobenius Number and Genus of Powers.** Our determination of the Apéry set of S^k when $S = \langle m, n\rangle$ also allows us to deduce closed formulas for the Frobenius number and genus of these powers. Recall that $F(A)$ is the largest element of $\mathbb{N} \setminus A$ and the genus of A is the cardinality of $\mathbb{N} \setminus A$.

Proposition 4.10. If $S = \langle m, n\rangle$ for $m < n$ coprime, then for $k \geq 1$ we have

$$F(S^k) = \frac{(m-1)n^{k+1} - (n-1)m^{k+1}}{n-m},$$

$$g(S^k) = \frac{n^{k+1}(m-1) + n - m^{k+1}(n-1) - m}{2(n-m)}.$$

Proof. If A is a numerical semigroup, then

$$F(A) = \max_{w\in \mathrm{Ap}(A)} w - m_0(A).$$

Thus Theorem 4.1 implies that

$$\begin{aligned} F(S^k) &= (m-1)(m^{k-1}n + \ldots + n^k) - m^k \\ &= (m-1)n\frac{n^k - m^k}{n-m} - m^k \\ &= \frac{(m-1)n^{k+1} - (n-1)m^{k+1}}{n-m}. \end{aligned}$$

Recall Selmer's formula [RG09, Prop. 2.12] for the genus of a numerical semigroup A with multiplicity m,

$$g(A) = \frac{1}{m}\Big(\sum_{w\in \mathrm{Ap}(A)} w\Big) - \frac{m-1}{2}.$$

The multiplicity of S^k is m^k. We use Theorem 4.1 to calculate the sum over the Apéry set of S^k:

$$\begin{aligned}
\sum_{w\in \mathrm{Ap}(S^k)} w &= \sum_{j\in\{0,\dots,m-1\}^k} \sum_{i=1}^{k} j_i m^{k-i} n^i \\
&= m^{k-1}\sum_{j=0}^{m-1} j \sum_{i=1}^{k} m^{k-i} n^i \\
&= m^k \frac{m-1}{2}\Big(n\sum_{i=0}^{k-1} m^{k-i-1} n^i\Big) \\
&= m^k n\frac{m-1}{2}\Big(\frac{n^k - m^k}{n-m}\Big).
\end{aligned}$$

Therefore

$$\begin{aligned}
g(S^k) &= \frac{1}{m^k}\Big(\sum_{w\in \mathrm{Ap}(A^k)} w\Big) - \frac{m^k-1}{2} \\
&= n\frac{m-1}{2}\Big(\frac{n^k-m^k}{n-m}\Big) - \frac{m^k-1}{2} \\
&= \frac{n^{k+1}(m-1) + n - m^{k+1}(n-1) - m}{2(n-m)}.
\end{aligned}$$

□

These results about numerical semigroups with two generators allow us to determine the asymptotic growth rate of genera and Frobenius numbers for powers of an arbitrary numerical semigroup A. Suppose A is a numerical semigroup and let

$$m_{\max}(A) := \max_p m_p(A).$$

Since $m_p(A) = m_0(A)$ for all primes $p \nmid m_0(A)$, this maximum is well-defined.

Theorem 4.11. Let A be a numerical semigroup. Then

$$\lim_{k\to\infty} \frac{\log g(A^k)}{k} = \lim_{k\to\infty}\frac{\log F(A^k)}{k} = \log m_{\max}(A).$$

Proof. First we consider $g(A^k)$. Let $m := m_0(A)$ and $n := m_{\max}(A)$. Let p be a prime such that $n = m_p(A)$. Then $m_p(A^k) = n^k$ and any natural number $j \le n^k$ which is not divisible by p is not an element of A^k. Thus

$$g(A^k) \ge \Big(1 - \frac{1}{p}\Big) n^k,$$

which implies that

$$\liminf_{k\to\infty} \frac{\log g(A^k)}{k} \ge \log n. \tag{4.3.1}$$

Let $m = p_1^{e_1}\cdots p_s^{e_s}$ be the prime factorization of $m_0(A)$, and let $n_i := m_{p_i}(A)$. Let $d_i := \gcd(m, n_i)$ and define $A_i := \langle m, n_i\rangle$. Note that $p_i \nmid d_i$. Setting $m = d_i m_i'$ and $n_i = d_i n_i'$ we have $A_i = d_i A_i'$, where $A_i' := \langle m_i', n_i'\rangle$ is a numerical semigroup.

For each i, let $W_i := d_i^k \mathrm{Ap}({A'_i}^k)$. Since $A_i = d_i A'_i$, we have $W_i \subseteq A_i^k \subseteq A^k$. The elements of $\mathrm{Ap}({A'_i}^k)$ represent every residue class modulo ${m'_i}^k$, hence W_i represents all the elements of the subgroup

$$H_i := d_i^k \mathbb{Z}/\langle m^k \rangle \subseteq \mathbb{Z}/\langle m^k \rangle.$$

Since $p_i \nmid d_i$ for each i we have $\gcd(d_1^k, \ldots, d_s^k, m^k) = 1$. Thus

$$H_1 + \cdots + H_s = \mathbb{Z}/\langle m^k \rangle. \tag{4.3.2}$$

If

$$W := W_1 + \cdots + W_s = \{w_1 + \cdots + w_s : w_i \in W_i\} \subseteq A^k,$$

then (4.3.2) implies that W contains representatives of every congruence class modulo m^k. Hence

$$\max_{w \in \mathrm{Ap}(A^k)} w \leq \max W \leq \sum_{i=1}^{s} \max W_i.$$

For each i, Proposition 4.10 implies that there is a positive constant c_i, independent of k, such that

$$\max \mathrm{Ap}({A'_i}^k) = F({A'_i}^k) + {m'_i}^k \leq c_i {n'_i}^k.$$

Therefore

$$\max W_i = d_i^k \max \mathrm{Ap}({A'_i}^k) \leq c_i d_i^k {n'_i}^k = c_i n_i^k \leq c_i n^k.$$

Setting $c := \sum_{i=1}^{s} c_i$, we get

$$\max_{w \in \mathrm{Ap}(A^k)} w \leq c n^k.$$

Selmer's formula [RG09, Prop. 2.12] now gives

$$g(A^k) = \frac{1}{m^k} \sum_{w \in \mathrm{Ap}(A^k)} w - \frac{m^k - 1}{2} \leq c n^k.$$

Hence

$$\limsup_{k \to \infty} \frac{\log g(A^k)}{k} \leq \log n.$$

Together with (4.3.1) this proves

$$\lim_{k \to \infty} \frac{\log g(A^k)}{k} = \log n.$$

Next we turn to $F(A^k)$. Let $S(A)$ denote the number of $a \in A$ such that $a < F(A)$. Then $F(A) = g(A) + S(A) - 1$. Note that if $a \in A$ is smaller than $F(A)$, then $F(A) - a$ must be an element of the gap set. Hence $S(A) \leq g(A)$, which implies $F(A) \leq 2g(A) - 1$. Thus

$$\limsup_{k \to \infty} \frac{\log F(A^k)}{k} \leq \lim_{k \to \infty} \frac{\log g(A^k)}{k} = \log n.$$

For the other direction, note that $g(A) \leq F(A)$ for any numerical semigroup A. Hence

$$\liminf_{k \to \infty} \frac{\log F(A^k)}{k} \geq \lim_{k \to \infty} \frac{\log g(A^k)}{k} = \log n.$$

Thus

$$\lim_{k \to \infty} \frac{\log F(A^k)}{k} = \log n. \qquad \square$$

5. Integral Closure of Ideals in $\mathbb{N}$

In this section we provide a simple and efficient characterization of the integral closure of an ideal $A \subseteq \mathbb{N}$. We begin with the following corollary of Theorem 4.11.

Corollary 5.1. Let $A \subseteq \mathbb{N}$ be a numerical semigroup. If $a \geq m_{\max}(A)$, then for all sufficiently large $k \geq 1$ we have $a^k \in A^k$. In particular, $a \geq m_{\max}(A)$ implies $a \in \overline{A}$.

Proof. Since $a = m_{\max}(A) \in A$, that case is immediate. Suppose that $a > m_{\max}(A)$. Then Theorem 4.11 implies that

$$\lim_{k\to\infty} \frac{\log F(A^k)}{k} = \log m_{\max}(A) < \log a,$$

hence for all sufficiently large k we have

$$F(A^k) < a^k.$$

Thus by definition of the Frobenius number, $a^k \in A^k$. Therefore $a \in \overline{A}$ by Corollary 2.13. $\square$

In Section 3.2 we constructed the S_p homomorphisms defined by $S_p(A) = \sum_{k\geq 0} m_{p,k}(A)T^k$. The semiring $\mathbb{N}_{\min}[T]$ is not multiplicatively cancellative, hence the S_p are not well-defined on similarity classes. Note that evaluating the series $S_p(A)$ at $T = \lambda \geq 1$ yields a nonzero real number for all nonzero ideals A. Let $\mathbb{R}^+_{\min}$ denote the tropical min-times semiring of nonnegative real numbers together with ∞. We define the ***p*-support functions**

$$\Phi_{p,\lambda}(A) := S_p(A)(\lambda) = \min_{k\geq 0} m_{p,k}(A)\lambda^k \in \mathbb{R}^+_{\min},$$

where $\lambda \geq 1$ is a real parameter. If $A \neq \langle 0 \rangle$, then our alternative formula (3.2.1) for S_p translates to

$$\Phi_{p,\lambda}(A) = \min_{a\in A\setminus\{0\}} a\lambda^{v_p(a)}. \tag{5.0.1}$$

With p and λ fixed, Lemma 3.10 implies that $\Phi_{p,\lambda} : \mathrm{Ideal}(\mathbb{N}) \to \mathbb{R}^+_{\min}$ is a semiring homomorphism. If $A \neq 0$, then $\Phi_{p,\lambda}(A)$ is a positive real number. Hence $\Phi_{p,\lambda}$ is cancellative on nonzero ideals. The data packaged in the functions $\Phi_{p,\lambda}$ with p fixed and λ varying can also be encoded as a Newton polygon. Given a prime p, let

$$N_p(A) := \text{lower convex hull of } \{(k, \log m_{p,k}(A)) : k \geq 0\}.$$

We call $N_p(A)$ the ***p*th Newton polygon** of A. Let $V_p(a) := (v_p(a), \log(a))$.

Lemma 5.2. Let p be prime, let $A \subseteq \mathbb{N}$ be an ideal, and let $a \in \mathbb{N}$. Then $V_p(a) \in N_p(A)$ if and only if $\Phi_{p,\lambda}(A) \leq a\lambda^{v_p(a)}$ for all $\lambda \geq 1$.

Proof. Every point (x_0, y_0) which does not belong to the convex set $N_p(A)$ is separated from it by a line. Thus $(x_0, y_0) \in N_p(A)$ if and only if

$$x_0u + y_0 \geq \min_{k\geq 0}\{ku + \log m_{p,k}(A)\}$$

for all $u \geq 0$. Substituting $u = \log \lambda$, this becomes

$$x_0 \log \lambda + y_0 \geq \min_{k\geq 0}\{k \log \lambda + \log m_{p,k}(A)\} = \min_{k\geq 0} \log\left(m_{p,k}(A)\lambda^k\right) = \log \Phi_{p,\lambda}(A)$$

for all $\lambda \geq 1$. Exponentiating we get $(x_0, y_0) \in N_p(A)$ if and only if

$$\Phi_{p,\lambda}(A) \leq e^{y_0}\lambda^{x_0}$$

for all $\lambda \geq 1$. Applying this criterion to $V_p(a) = (v_p(a), \log a)$ gives us the result. $\square$

Given convex sets X and Y, let $X + Y = \{x + y : x \in X, y \in Y\}$ denote their Minkowski sum. Let $\mathcal{C}$ denote the semigroup of convex subsets of $\mathbb{R}^2$ with respect to Minkowski sum.

Proposition 5.3. Given a prime p, the map $N_p : \mathrm{Ideal}(\mathbb{N}) \to \mathcal{C}$ is a semigroup homomorphism factoring through the universal cancellative quotient $A \mapsto [A]$. That is, $A \sim B$ implies that $N_p(A) = N_p(B)$.

Proof. Lemma 3.8 implies that

$$\log m_{p,k}(AB) = \min_{i+j=k}\{\log m_{p,i}(A) + \log m_{p,j}(B)\},$$

which is precisely the expression for the vertices of the Minkowski sum of $N_p(A)$ and $N_p(B)$. Hence

$$N_p(AB) = N_p(A) + N_p(B).$$

Suppose $C \neq \langle 0\rangle$ and $AC = BC$. Then $N_p(AC) = N_p(BC)$ and Lemma 5.2 implies that

$$\Phi_{p,\lambda}(A)\Phi_{p,\lambda}(C) = \Phi_{p,\lambda}(AC) = \Phi_{p,\lambda}(BC) = \Phi_{p,\lambda}(B)\Phi_{p,\lambda}(C)$$

for all $\lambda \geq 1$. Then C nonzero implies that $\Phi_{p,\lambda}(A) = \Phi_{p,\lambda}(B)$ for all $\lambda \geq 1$, which in turn implies $N_p(A) = N_p(B)$. Hence N_p factors through $[\mathrm{Ideal}(\mathbb{N})]$. ☐

We now present the main result of this section, an effective characterization of integral closures of ideals in $\mathbb{N}$.

Theorem 5.4. Let $A \subseteq \mathbb{N}$ be an ideal and let $a \in \mathbb{N}$. Then the following are equivalent

(1) $a^k \in A^k$ for some $k \geq 1$,
(2) $a \in \overline{A}$,
(3) $V_p(a) \in N_p(A)$ for all primes p.

Proof. Corollary 2.13 implies (1) $\Rightarrow$ (2). Proposition 5.3 and Proposition 2.20 imply that $N_p(A) = N_p(\overline{A})$. If $a \in \overline{A}$, then $V_p(a) \in N_p(\overline{A}) = N_p(A)$ for all primes p, which proves (2) $\Rightarrow$ (3). Hence it suffices to prove (3) $\Rightarrow$ (1). Note that if $A = \langle 0\rangle$, then the assertion is immediate.

So suppose that A is a nonzero ideal and that p is a prime. By assumption we have $V_p(a) \in N_p(A)$. If $v_p(a) \geq v_p(m_0(A))$ and $m_0(A) \leq a$, let $e_p = 1$ and $b_p = m_0(A)$. Otherwise there is some $k_1 < k_2$ such that the point $(v_p(a), \log a)$ lies above the line segment connecting $(k_1, \log m_{p,k_1}(A))$ and $(k_2, \log m_{p,k_2}(A))$. Let $w_i := m_{p,k_i}(A)$ and note that $k_i = v_p(w_i)$. This geometric assertion about $V_p(a)$ translates to

$$\frac{k_2 - v_p(a)}{k_2 - k_1}\log w_1 + \frac{v_p(a) - k_1}{k_2 - k_1}\log w_2 \leq \log a,$$

or equivalently

$$b_p := w_1^{k_2 - v_p(a)} w_2^{v_p(a) - k_1} \leq a^{k_2 - k_1}.$$

Let $e_p := k_2 - k_1$. Finally, observe that $w_1, w_2 \in A$ imply that $b_p \in A^{e_p}$ and

$$v_p(b_p) = (k_2 - v_p(a))k_1 + (v_p(a) - k_1)k_2 = e_p v_p(a).$$

If $p \nmid m_0(A)$, then $V_p(a) \in N_p(A)$ is equivalent to $m_0(A) \leq a$. Since $0 = v_p(m_0(A)) \leq v_p(a)$, we can let $e_p = 1$ and $b_p = m_0(A)$.

Thus for each prime p there is an element b_p and an integer $e_p \geq 1$ such that $b_p \leq a^{e_p}$ and $v_p(b_p) \leq e_p v_p(a)$. Since $e_p = 1$ for all but finitely many primes p, $e := \mathrm{lcm}_p e_p$ exists. Replacing b_p with b_p^{e/e_p} we have $b_p \leq a^e$ and $v_p(b_p) \leq e v_p(a)$ for all primes p. Let $g := \gcd_p b_p$ and write $b_p = g b'_p$. Then $v_p(g) \leq e v_p(a)$ for all primes p, which is to say that $a^e = g a'$ for some $a' \in \mathbb{N}$. Consider the ideal $B := \langle b_p : p \text{ prime}\rangle \subseteq A^e$ and the numerical semigroup $B' = \langle b'_p : p \text{ prime}\rangle$. Then $B = gB'$.

Since $b'_p \leq a'$ for all p, Lemma 3.7 implies that $m_{\max}(B') \leq a'$. Thus Corollary 2.13 implies there is some $k \geq 1$ such that ${a'}^k \in {B'}^k$. Hence

$$a^{ek} = g^k {a'}^k \in g^k {B'}^k = B^k \subseteq A^{ek}. \qquad \square$$

Theorem 5.4 implies that types (1), (2), and (3) integrality are equivalent for ideals in $\mathbb{N}$. The characterization of $\overline{A}$ in terms of Newton polygons is analogous to the theorem characterizing the integral closure of a monomial ideal in terms of the Newton polyhedron defined by its exponent vectors [HS06, Prop. 1.4.6]. From this perspective, natural numbers can be thought of as monomials in the primes. Translating between Newton polygons and the support functions, Theorem 5.4 may also be viewed as an analog of Rees's theorem characterizing integral closures of ideals in Noetherian rings (original proof by Rees [Ree56], see Huneke and Swanson [HS06, Thm. 10.2.2] for a contemporary statement). The functions $\log \Phi_{p,\lambda}$ define tropical valuations on ideals of $\mathbb{N}$, and Theorem 5.4 asserts that finitely many of these valuations determine the integral closure of A, namely those corresponding to nontrivial slopes of $N_p(A)$, which only exist for the finitely many primes $p \mid m_0(A)$.

Example 5.5. Let $A = \langle 8, 11 \rangle$. Then every $a \geq 11$ belongs to $\overline{A}$ by Corollary 5.1 and it remains to decide whether 9 or 10 belong to $\overline{A}$. The only relevant prime here is $p = 2$. The Newton polygon $N_2(A)$ consists of a single segment and a computation shows that $V_2(9) \notin N_2(A)$ and $V_2(10) \in N_2(A)$. Therefore,

$$\overline{A} = \{0, 8, 10, 11, 12, \ldots\}.$$

This example nicely highlights the value of our theoretical analysis of integral closures. If we try to use the iterated colon ideal method to find an ideal B such that $10B \subseteq AB$, the convergence happens incredibly slowly. The sequence B_k strictly decreases for at least $0 \leq k \leq 20$. The ideal B_{20} has 370 minimal generators and multiplicity 512. It is unclear how many more iterates are required to reach stabilization; the computations become prohibitively slow. Theorem 5.4 shows that $10^k \in A^k$ for some sufficiently large k. Using the characterization of the Apéry set of $\langle 8, 11 \rangle^k$ provided by Theorem 4.1 one may show that the first k for which $10^k \in A^k$ is $k = 198$. $\square$

If m is squarefree, the Newton polygon conditions are vacuous.

Corollary 5.6. Let $S := \langle m, n \rangle$ where $2 \leq m < n$ are coprime. If m is squarefree, then

$$\overline{S} = \langle m \rangle + \{k \in \mathbb{N} : k \geq n\}.$$

Proof. If m is squarefree, then for each prime $p \mid m$, the Newton polygon $N_p(S)$ consists of a single segment of width one. Corollary 5.1 implies that every $a \geq n$ belongs to $\overline{S}$, and clearly no $a < m$ belongs to $\overline{S}$. Thus if $m < a < n$ and $V_p(a) \in N_p(S)$, then $v_p(a) \geq v_p(m) = 1$. Hence if such an a belongs to $\overline{S}$, it follows that $m \mid a$. Thus $\overline{S} = \langle m \rangle + \{k \in \mathbb{N} : k \geq n\}$. $\square$

Although $\overline{AB} \neq \overline{A} \cdot \overline{B}$ in general, this does hold for scaling.

Proposition 5.7. If $A \subseteq \mathbb{N}$ is a numerical semigroup and $g \in \mathbb{N}$, then $\overline{gA} = g\overline{A}$.

Proof. If $g = 0$, then $\overline{gA} = \{0\} = g\overline{A}$. Now suppose that $g \neq 0$. If $a \in \overline{A}$, then there exists a nonzero ideal B such that $aB \subseteq AB$. Hence $gaB \subseteq gAB$, and we conclude that $ga \in \overline{gA}$. Thus $g\overline{A} \subseteq \overline{gA}$. Conversely, suppose $a \in \overline{gA}$. Let B be a nonzero ideal such that $aB \subseteq gAB$. Lemma 3.4 implies we can express $B = hC$ for some nonzero h and some numerical semigroup C. Thus

$$ahC \subseteq ghAC.$$

Since $h \neq 0$, we can cancel it from both sides of this containment to get

$$aC \subseteq gAC.$$

The numerical semigroup C contains n and $n+1$ for some sufficiently large n. The above containment implies that g divides both an and $a(n+1)$. Thus $a = gc$ for some $c \in \mathbb{N}$ and substitution yields

$$gcC \subseteq gAC.$$

Canceling g we see that $c \in \overline{A}$. Therefore $a = gc \in g\overline{A}$, completing our proof that $g\overline{A} = \overline{gA}$. $\square$

References

[BM07] Maria Bras-Amorós and Anna de Mier. "Representation of Numerical Semigroups by Dyck Paths". In: *Semigroup Forum* 75 (2007), pp. 676–681. DOI: `10.1007/s00233-007-0717-7`.

[HS06] C. Huneke and I. Swanson. *Integral Closure of Ideals, Rings, and Modules*. London Mathematical Society Lecture Note Series. Cambridge University Press, 2006. ISBN: 9780521688604.

[Kak25] Sôichi Kakeya. "On Fundamental Systems of Symmetric Functions". In: *Japanese Journal of Mathematics* 2 (1925), pp. 69–80. DOI: `10.4099/jjm1924.2.0_69`.

[Kak27] Sôichi Kakeya. "On Fundamental Systems of Symmetric Functions II". In: *Japanese Journal of Mathematics* 4 (1927), pp. 77–85. DOI: `10.4099/jjm1924.4.0_77`.

[Nar13] Hirokatsu Nari. "Symmetries on almost symmetric numerical semigroups". In: *Semigroup Forum* 86.1 (2013), pp. 140–154. DOI: `10.1007/s00233-012-9397-z`.

[Ree56] David Rees. "Valuations associated with ideals (II)". In: *Journal of the London Mathematical Society* s1-31.2 (1956), pp. 221–228. DOI: `10.1112/jlms/s1-31.2.221`.

[RG09] J.C. Rosales and P. A. García-Sánchez. *Numerical Semigroups*. Vol. 20. Developments in Mathematics. Springer New York, NY, 2009. ISBN: 978-1-4419-0159-0. DOI: `10.1007/978-1-4419-0160-6`.

[Rut64] D. E. Rutherford. "XIX.—The Cayley-Hamilton Theorem for Semi-rings". In: *Proceedings of the Royal Society of Edinburgh Section A: Mathematics* 66.4 (1964), pp. 211–215. DOI: `doi:10.1017/S0080454100007871`.

[Sti09] Henning Stichtenoth. *Algebraic Function Fields and Codes*. 2nd ed. Vol. 254. Graduate Texts in Mathematics. Berlin, Heidelberg: Springer, 2009. ISBN: 978-3-540-76877-7. DOI: `10.1007/978-3-540-76878-4`.

Dept. of Mathematics and Statistics, Vassar College, Poughkeepsie, NY 12604,
Email address: `jaychen@vassar.edu`

Dept. of Mathematics and Statistics, Vassar College, Poughkeepsie, NY 12604,
Email address: `thyde@vassar.edu`

Dept. of Mathematics and Statistics, Vassar College, Poughkeepsie, NY 12604,
Email address: `dlaurens@vassar.edu`

Dept. of Mathematics and Statistics, UMass Amherst, Amherst, MA 01003,
Email address: `jasperpierma@umass.edu`

Dept. of Mathematics and Statistics, Vassar College, Poughkeepsie, NY 12604,
Email address: `hsimons@vassar.edu`