Finding Elements With Given Factorization Lengths and Multiplicities

Paul Baginski, Ryan Rodriguez, George J. Schaeffer, and Yiwei She

Abstract. Many algebraic number rings exhibit nonunique factorization of elements into irreducibles. Not only can the irreducibles in the factorizations be different, but the *number* of irreducibles in the factorizations can also vary. A basic question then is: Which sets can occur as the set of factorization lengths of an element? Moreover, how often can each factorization length occur? While these questions are most pertinent in algebraic number rings, their pertinence extends to Dedekind domains and a broader class of structures called Krull monoids. Surprisingly, for a large subclass of Krull monoids, Kainrath was able to resolve completely the question of which length sets and length multiplicities can be realized. In this article, we explain the context of Kainrath's theorem and give a constructive proof for an important case, namely Krull monoids with infinite nontorsion class group. We also construct length sets in a case not covered by Kainrath's theorem to illustrate the difficulty of the general problem.

1. INTRODUCTION. Undergraduates learn in abstract algebra and number theory courses that extensions of the integers, such as the classic $\mathbb{Z}\left[\sqrt{-5}\right]$, have nonunique factorization. These courses expend quite some effort to verify that the ubiquitous equation $6 = 2 \cdot 3 = \left(1+\sqrt{-5}\right)\left(1-\sqrt{-5}\right)$ actually portrays two distinct factorizations of the same element. Properly verifying this claim involves norms, determining units, checking for associates, etc. Yet, after laying all that groundwork, many books terminate their exploration of nonunique factorization with this one example, content that a single equation has conveyed enough of the "problem" of nonunique factorization. The simplicity of this equation, though, can give a false impression to undergraduates. Students may look at the equation $6 = 2 \cdot 3 = \left(1+\sqrt{-5}\right)\left(1-\sqrt{-5}\right)$ and not be much perturbed: two "atoms" have recombined to become two other "atoms," but the "mass" has been conserved. Yet, nonunique factorization poses a far more complicated and intriguing obstacle than this example presents.

The standard testing ground, $\mathbb{Z}\left[\sqrt{-5}\right]$ turns out to be a rather tame and well-behaved ring with regard to nonunique factorization: For any element $x \in \mathbb{Z}[\sqrt{-5}]$, all its factorizations have the same number of irreducibles (counting multiplicity). This property is known as **half-factoriality**. For example, 18 has three distinct factorizations into irreducibles: $2 \cdot 3 \cdot 3$; $3 \cdot \left(1+\sqrt{-5}\right) \cdot \left(1-\sqrt{-5}\right)$; and $2 \cdot \left(2+\sqrt{-5}\right)\left(2-\sqrt{-5}\right)$, yet all these factorizations have three irreducibles. Thus, in a half-factorial ring, the factorizations of an element may not be unique, but the factorization *lengths* are. This is precisely the conservation of mass notion from above.

In more complicated algebraic number rings, we can find elements that have factorizations of different lengths. For example, in $\mathbb{Z}\left[\frac{1+\sqrt{-23}}{2}\right]$, we have

$$18 = \left(\frac{7+\sqrt{-23}}{2}\right)\left(\frac{7-\sqrt{-23}}{2}\right) = 3\left(\frac{1+\sqrt{-23}}{2}\right)\left(\frac{1-\sqrt{-23}}{2}\right).$$

http://dx.doi.org/10.4169/amer.math.monthly.123.9.849
MSC: Primary 13F15, Secondary 20M13; 13A05

The element 18 thus factors as a product of two atoms and as a product of three atoms; mass has not been preserved! We can say that 18 has two factorization lengths, 2 and 3, which we can collect into the **set of lengths** of 18, denoted $\mathsf{L}(18) = \{2, 3\}$. If we consider $324 = 18^2$, then any pair of factorizations of 18 will produce a factorization of 324. Considering all possible pairs, we obtain factorizations of length 4, 5, and 6 for 324. These turn out to be the only factorization lengths of 324, so $\mathsf{L}(324) = \{4, 5, 6\}$. Taking larger and larger powers of 18 (or any element with at least two factorization lengths), we obtain elements with larger and larger sets of lengths. One can show in general that $\mathsf{L}(18^k)$ is precisely $\{2k, 2k + 1, \ldots, 3k - 1, 3k\}$, an interval. Based on these computations, one might wonder if length sets are always intervals or whether an element factors as, say, a product of four irreducibles and a product of six irreducibles but not five irreducibles. For $\mathbb{Z}\left[\frac{1+\sqrt{-23}}{2}\right]$, the length sets turn out to be intervals, but in other algebraic rings, length sets can have gaps. This begs the question, which sets occurs as length sets? More precisely, we have two questions, depending on where we are allowed to look.

Question 1. If you have a set L, does there exist an algebraic number ring R and an element $x \in R$ such that $\mathsf{L}(x) = L$?

Question 2. If you fix an algebraic number ring R, which sets L occur as $\mathsf{L}(x)$ for $x \in R$?

The factorization lengths are one aspect, but one can also consider how frequently they appear. In $\mathbb{Z}\left[\sqrt{-5}\right]$, the element 6 had two distinct factorizations of length 2. Is there an element of that ring with three distinct factorizations of length 2? We are now specifying the **multiplicity** of different factorization lengths, a more intricate problem than specifying just the length set. For example, could there be an algebraic number ring R that has an element with one million factorizations of length 2 and no other factorizations? What would such a ring look like? These questions about length, multiplicities, and the connection to the ring structure are some of the central questions explored in the theory of nonunique factorization.

The astute reader may have noticed a pattern among our examples: $\mathbb{Z}\left[\sqrt{-5}\right]$ and $\mathbb{Z}\left[\frac{1+\sqrt{-23}}{2}\right]$ are the first imaginary quadratic number rings with class numbers 2 and 3, respectively. As it turns out, the larger the class group, the worse the nonuniqueness of factorization in the ring; this is a discovery that stymied Lamé's attempt to prove Fermat's last theorem [**12**]. A well-known result says that an algebraic number ring has unique factorization if and only if its class group is trivial. A slightly less well-known result by Carlitz [**7**] proved that an algebraic number ring is half-factorial if and only if its class number is less than or equal to 2. In general, questions about length sets can be translated cleanly into corresponding questions about the class group and, with care, questions about multiplicities can also be translated (see Sections 2 and 4). Factorization theory for algebraic number rings corresponds heavily to additive combinatorics within the class group and that combinatorics restricts the possible behavior for factorization. For example, one can show that a combinatorial constant known as the Davenport constant $D(G)$ plays an outsize role in the structure of length sets. Specifically, if an algebraic number ring R has class group G with $|G| \geq 2$ and L is the length set of some nonzero, nonunit $x \in R$, then we must have $\max L / \min L \leq D(G)/2$, and this bound is sharp. We recommend the expository article [**5**] to interested readers; it describes the role of the Davenport constant and the class group in the factorization of algebraic number rings. Two recent articles [**15, 21**] present the state of the art for determining the length sets of algebraic number rings and more general contexts.

While the theory of nonunique factorization grew out of algebraic number rings, its focus today is quite broad, due to the connections between factorization problems and other areas of mathematics, such as additive combinatorics, commutative algebra, and, recently, invariant theory [**11**]. The "classic" part of the theory has expanded from algebraic number rings, to Dedekind domains, and finally to a class of structures known as Krull monoids. Krull monoids, like algebraic number rings, have an associated abelian group called the class group, and these monoids provide the most general setting where the class group has full control over factorization properties. This connection between factorization and the class group is what makes this theory "classic" (excuse the pun), and Section 4 describes the connection in detail. The present article intends to highlight some of the surprisingly rich factorization theory in these general settings of Dedekind domains and Krull monoids, which have connections beyond number theory. Algebraic number rings, naturally, are also important, but they have been covered in detail in [**5**].

Unlike algebraic number rings, Dedekind domains and Krull monoids can have infinite class groups. In fact, every abelian group G occurs as the class group of some Dedekind domain [**10**]. Examples of Krull monoids with infinite class group naturally occur in number theory and module theory (see Section 4). While the questions we have asked about length sets and multiplicities remain a highly active area of research for algebraic number rings, for many Krull monoids with infinite class group the question was fully resolved in 1999 by Kainrath's theorem.

Kainrath's Theorem. *Let H be a Krull monoid with infinite class group G and primes in every divisor class. Then every finite subset L of $\mathbb{N}_{\geq 2}$ occurs as the length set of some $x \in H$.*
Furthermore, barring G of a certain form, we can prescribe multiplicities. For every $\ell \in L$, specify a multiplicity $m_\ell \geq 1$. We can find an $x \in H$ with precisely m_ℓ factorizations of length ℓ for each $\ell \in L$ and no other factorizations.

Kainrath's theorem says that *every* length set and length multiplicity can be realized in a Krull monoid with infinite class group and primes in every divisor class. This is in stark contrast to algebraic number rings, where we have many restrictions, including the previously mentioned bound on $\max L / \min L$. In fact, Kainrath's theorem is one of only two known contexts where all length sets and length multiplicities can be achieved. The second context was discovered by Frisch [**14**] in 2013, who showed that the ring of integer-valued polynomials $\mathrm{Int}(\mathbb{Z}) = \{f(x) \in \mathbb{Q}[x] \mid \forall n \in \mathbb{Z}\, f(n) \in \mathbb{Z}\}$ has all possible length sets and multiplicities. Notably, this ring is not Krull.

Kainrath's theorem is impressively general. For length sets, it covers Krull monoids with any infinite abelian group as its class group. For multiplicities, there is only one class of exceptions, namely finite extensions of an infinite elementary 2-group. In that case, the truth of theorem is not known, though partial results have been obtained [**16**, Section 7.4]. Despite the generality of Kainrath's theorem, it can be improved along two lines. First, Kainrath's theorem was nonconstructive. We know that elements with a prescribed length set and multiplicities exist, but we do not have a systematic way of finding them. Second, the theorem assumes there are primes in every divisor class. The technical details of this assumption are explained in Section 4, but suffice it to say that this hypothesis does not always occur and removing this hypothesis is the far greater obstacle to improving Kainrath's theorem.

In this paper, we shall prove a special case of Kainrath's theorem and discuss the issues surrounding generalizations of the theorem. In Section 2, we introduce block monoids, an important family of Krull monoids that are at the heart of factorization

theory arguments for all Krull monoids. Section 3 gives an elementary, constructive proof of Kainrath's theorem for $\mathcal{B}(\mathbb{Z})$, the block monoid over $\mathbb{Z}$. We illustrate the general algorithm and work through an extended example. In Section 4, we give a gentle introduction to Krull monoids and reveal the correspondence between Krull monoids and block monoids. This correspondence will allow us to extend our constructive proof of Kainrath's theorem from the block monoid $\mathcal{B}(\mathbb{Z})$ to all Krull monoids with an infinite nontorsion class group and primes in every class. While this may seem like an overly restrictive choice of class group, many of the known examples from number theory and module theory have class group $G \cong \mathbb{Z}$. After this discussion of constructibility, we shift our focus to removing the assumption of "primes in every class." Our final section gives a taste of the difficulties of this open problem by working out a particularly nice class of examples in Section 5.

2. BLOCK MONOIDS AND BASIC FACTORIZATION THEORY. In this section, we formalize some of the intuition given in the introduction. The modern definitions for factorization theory have been couched in the world of monoids rather than rings. Whenever we talk about factorization in a ring R, we are only referring to the monoid $R^\bullet = R\backslash\{0\}$ of nonzero elements under multiplication. Addition plays a peripheral role; concepts such as ideals, which ostensibly refer to addition, can be developed from the multiplicative structure. On the other hand, many important monoids with factorization theories, such as the block monoids we define below, cannot be obtained as the multiplicative monoid of a ring. Therefore, we need the added expressive power of the monoidal definitions to cover these essential cases. A full description of these nuances can be found in [**16**]. Despite the setting of monoids, the reader will find many of the basic definitions familiar from ring theory.

Let H be a commutative monoid with cancellation. An element $u \in H$ is a **unit** if there is $v \in H$ such that $uv = 1$. The set of units will be denoted $H^\times$. If $x \in H$ and $u \in H^\times$ is a unit, then the element ux is an **associate** of x. A nonunit $x \in H$ is **irreducible** if, whenever $x = yz$ for some $y, z \in H$, we have that y or z is a unit. We will denote the set of irreducibles by $\mathcal{A}(H)$. A nonunit $x \in H$ is **prime** if whenever $x \mid yz$ for some $y, z \in H$, then $x \mid y$ or $x \mid z$. As usual, all primes are irreducible but not vice versa. A monoid H is **atomic** if every nonunit of H can be written as a product of irreducibles. Most familiar rings and monoids are atomic; for example, any Noetherian domain is atomic, as is any finitely generated monoid.

In general monoids and rings, elements do not have to factor uniquely as a product of irreducibles. We wish to measure this nonuniqueness. Let $x \in H$ be a nonunit. If $x = a_1 \cdots a_n$ is a factorization of x into irreducibles, we say n is the **length** of the factorization. We collect the factorization lengths together as the **set of lengths** of x:

$$\mathsf{L}(x) = \{n \in \mathbb{N} \mid \exists a_1, \ldots, a_n \in \mathcal{A}(H) \text{ such that } x = a_1 \cdots a_n\}.$$

Two factorizations $a_1 \cdots a_n = x = b_1 \cdots b_m$ of x are essentially the same if $n = m$ and, after reordering, a_i is an associate of b_i for all i. Otherwise, the factorizations are essentially distinct. A monoid H has **unique factorization** if, for any nonunit $x \in H$, all factorizations of x are essentially the same. A weaker condition, that $|\mathsf{L}(x)| = 1$ for all nonunits $x \in H$, is called **half-factoriality**. We mentioned in the introduction that $\mathbb{Z}\left[\sqrt{-5}\right]$ is half-factorial but not factorial.

A few values of length sets are immediate from the definition. If $x \in H$ is a unit, then $\mathsf{L}(x) = \{0\}$. If x is irreducible, then $\mathsf{L}(x) = \{1\}$. Otherwise, $\mathsf{L}(x) \subseteq \mathbb{N}_{\geq 2} = \{n \in \mathbb{N} \mid n \geq 2\}$. In general, length sets can be infinite, but for Krull monoids, the focus of this article, they will always be finite.

We are not only interested in counting the lengths of factorizations but also the number of factorizations of each length. For each atomic monoid H, we have the **length multiplicity function** $\mu : H \times \mathbb{N} \to \mathbb{N} \cup \{\infty\}$, where, for each $x \in H$ and $n \geq 0$, we have $\mu(x, n) = m$ if x has exactly m essentially distinct factorizations of length n. We can make several immediate conclusions about the multiplicity function from the definition. If x is a unit, then $\mu(x, n) = 0$ for all $n \geq 1$, but $\mu(x, 0) = 1$. If x is an irreducible, then $\mu(x, 1) = 1$, and for all $n \neq 1$, we have $\mu(x, n) = 0$. Lastly, if x is a reducible nonunit, then $\mu(x, 0) = \mu(x, 1) = 0$ and $\mu(x, n) \geq 1$ for at least one $n > 1$. For all Krull monoids H and all $x \in H$, $\mu(x, n)$ is nonzero for only finitely many values of n and $\mu(x, n)$ is never ∞.

The reducible elements of H have the interesting length sets and multiplicity functions. We wish to determine which ones are possible. The extreme cases are that *every* set or function is possible; we give these cases a name.

Definition. An atomic monoid H is **length-set complete** if, for every nonempty finite subset $L \subset \mathbb{N}_{\geq 2}$, there is an $x \in H$ with $\mathsf{L}(x) = L$. The atomic monoid H is **length-multiplicity complete** if, for every function $f : \mathbb{N}_{\geq 2} \to \mathbb{N}$ with finite nonempty support, there is an $x \in H$ with $\mu(x, n) = f(n)$ for all $n \geq 2$.

In other words, H is length-set complete if, for any finite set L of possible factorization lengths, we can find an element x whose factorization lengths are precisely those in L. The monoid is length-multiplicity complete if we can also prescribe how many factorizations there are of each length. Clearly, length-multiplicity complete implies length-set complete. Kainrath's theorem can now be rephrased using this language.

Kainrath's Theorem. *Let H be a Krull monoid with infinite class group G and primes in every class. Then H is length-set complete. Furthermore, if G is not a finite extension of an elementary 2-group, then H is also length-multiplicity complete.*

At the center of all our arguments will be a class of monoids called block monoids. Block monoids are a particularly accessible example of Krull monoids, but as we will see in Section 4, they are also essential for the study of general Krull monoids. The idea of a block monoid derives from the notion of a zero-sum sequence from additive number theory.

Given an abelian group G, we can construct the free abelian monoid $\mathcal{F}(G)$ over G. Per convention, we will write G additively and $\mathcal{F}(G)$ multiplicatively. A typical element A of $\mathcal{F}(G)$ will be a formal product of elements of G. Thus, we can write A in the form $A = g_1^{e_1} g_2^{e_2} \cdots g_n^{e_n}$ for some distinct $g_i \in G$ and $e_i \geq 0$. The elements of $\mathcal{F}(G)$ are called **sequences** over G. The term "sequence" here is a bit of a misnomer since $\mathcal{F}(G)$ is abelian, and so the order of the terms does not matter. "Word" or "multiset" would be technically more accurate, but "sequence" remains the popular convention.

We have an evaluation function $\sigma : \mathcal{F}(G) \to G$ that takes each formal sequence and combines the terms using the group operation. Specifically, for $A = g_1^{e_1} g_2^{e_2} \cdots g_n^{e_n}$, we have

$$\sigma(A) := e_1 g_1 + e_2 g_2 + \cdots + e_n g_n.$$

The kernel of this evaluation map σ is precisely the **block monoid** over G. Specifically, the block monoid over G is the monoid

$$\mathcal{B}(G) = \left\{ x = \prod_{g \in G} g^{v_g} \in \mathcal{F}(G) \;\middle|\; \sum_{g \in G} v_g g = 0 \right\}.$$

The elements of $\mathcal{B}(G)$ are known as **zero-sum sequences** or **blocks**. The idea of a zero-sum sequence has had a long history in the field of additive number theory [**18**].

For example, if $G = \mathbb{Z}/4\mathbb{Z}$, the integers modulo 4, then

$$\mathcal{B}(\mathbb{Z}/4\mathbb{Z}) = \{0^{v_0}1^{v_1}2^{v_2}3^{v_3} \mid v_0 \cdot 0 + v_1 \cdot 1 + v_2 \cdot 2 + v_3 \cdot 3 \equiv 0 \mod 4\}.$$

The sequence $0^2 1^3 2^1 3^1$ is in $\mathcal{B}(\mathbb{Z}/4\mathbb{Z})$ since $2 \cdot 0 + 3 \cdot 1 + 2 + 3 \equiv 0 \mod 4$, but the sequence $0^1 1^4 2^1 3^2$ is not a block since $1 \cdot 0 + 4 \cdot 1 + 2 + 2 \cdot 3 \not\equiv 0 \mod 4$.

We can relativize these concepts to any subset G_0 of G. Specifically, we will consider $\mathcal{F}(G_0) \leq \mathcal{F}(G)$, the free abelian monoid generated by G_0. The block monoid over G_0, denoted $\mathcal{B}(G_0, G)$ (or simply $\mathcal{B}(G_0)$ if the ambient group G is understood), consists of all zero-sum sequences in $\mathcal{F}(G_0)$. Thus, $\mathcal{B}(G_0) = \mathcal{F}(G_0) \cap \mathcal{B}(G)$.

We can develop a theory of factorization in block monoids. If $A, C \in \mathcal{F}(G_0)$, we say A divides C, written $A \mid C$, if there exists $B \in \mathcal{F}(G_0)$ such that $AB = C$. Note that if $AB = C$ and A and C are both in $\mathcal{B}(G_0)$, then B will also be in $\mathcal{B}(G_0)$ since $\sigma(C) = \sigma(A) + \sigma(B)$. Thus, if elements of $\mathcal{B}(G_0)$ divide each other in $\mathcal{F}(G_0)$, they already do so in $\mathcal{B}(G_0)$; we say that $\mathcal{B}(G_0)$ is **saturated** in $\mathcal{F}(G_0)$. This fact will be used frequently when we factor blocks into products of other blocks.

Now we can implement the general definitions of factorization theory for block monoids. A block $A \in \mathcal{B}(G_0)$ is irreducible if A cannot be written as BC, the product of two nontrivial blocks $B, C \in \mathcal{B}(G_0)$. For example, in $\mathcal{B}(\mathbb{Z}/4\mathbb{Z})$, the irreducible blocks are exactly [0], $[1^4]$, $[2^2]$, $[3^4]$, $[1 \cdot 3]$, $[1^2 \cdot 2]$, and $[2 \cdot 3^2]$. The irreducible [0] is prime, but all the other irreducibles are not. The block monoid $\mathcal{B}(G_0)$ is atomic, but in general, factorization is not unique. For example, in $\mathcal{B}(\mathbb{Z}/4\mathbb{Z})$, the block $A = 1^4 2^2 3^4$ has a total of five factorizations:

$$\begin{array}{ll} \text{length 3:} & [1^4][2^2][3^4], \quad [1^2 \cdot 2]^2[3^4], \quad [3^2 \cdot 2]^2[1^4], \\ \text{length 4:} & [1^2 \cdot 2][3^2 \cdot 2][1 \cdot 3]^2, \\ \text{length 5:} & [1 \cdot 3]^4[2^2]. \end{array}$$

Thus, the length set of A is $\mathsf{L}(A) = \{3, 4, 5\}$ and the length multiplicities of A are $\mu(A, 3) = 3$, $\mu(A, 4) = \mu(A, 5) = 1$, and $\mu(A, n) = 0$ for all other n.

3. CONSTRUCTION FOR $\mathbb{Z}$. Kainrath's theorem applies to the block monoid $\mathcal{B}(\mathbb{Z})$, and in this section, we will give a constructive proof of this particular case. Specifically, we will show that $\mathcal{B}(\mathbb{Z})$ is length-multiplicity complete (and hence length-set complete) by constructing blocks with a given length multiplicity function. As an immediate consequence, we will have that for any infinite abelian group G, $\mathcal{B}(G)$ is constructively length-set complete and length-multiplicity complete if we can find some $g \in G$ of infinite order.

So far we have been using the standard notation for block monoids over an arbitrary group. However, we will have to make a slight notational adjustment when working over $\mathbb{Z}$. Here, we have a genuine ambiguity in the use of exponents as an arithmetic operation and as a count of repeated terms in a sequence. For example, if we write $2^4 \in \mathcal{F}(\mathbb{Z})$, it is ambiguous whether we mean a sequence with one term, 16, or a sequence with four terms, all of them 2. To disambiguate, we will reserve the unadorned exponent for the arithmetic operation and use brackets [] in the exponent

for counting repeated terms in a sequence. Thus, $2^4 \in \mathcal{F}(\mathbb{Z})$ will denote a sequence with one term, but $2^{[4]} \in \mathcal{F}(\mathbb{Z})$ denotes a sequence of four repeated 2's.

One major advantage of having an ordered group like $\mathbb{Z}$ is that we can canonically split the terms of a block. If $B \in \mathcal{B}(\mathbb{Z})$, then we may write out B as

$$B = a_1^{[e_1]} a_2^{[e_2]} \cdots a_n^{[e_n]} 0^{[g]} (-b_1)^{[f_1]} (-b_2)^{[f_2]} \cdots (-b_m)^{[f_m]}.$$

The positive part of B is $B^+ = a_1^{[e_1]} a_2^{[e_2]} \cdots a_n^{[e_n]}$, while the negative part of B is $B^- = b_1^{[f_1]} b_2^{[f_2]} \cdots b_m^{[f_m]}$. Note that the signs have been stripped from the negative terms, and thus, we can reconstruct B as $B = B^+ 0^g (-B^-)$. Splitting B into positive part and negative part also gives us a natural way of weighing B.

Definition. If $B \in \mathcal{B}(\mathbb{Z})$, then the **weight** of B is defined to be $w(B) = \sigma(B^+)$, the sum of the positive terms of B. Since B is zero-sum, we also have $w(B) = \sigma(B^-)$, the absolute value of the sum of the negative terms of B. In symbols, if

$$B = a_1^{[e_1]} a_2^{[e_2]} \cdots a_n^{[e_n]} 0^{[g]} (-b_1)^{[f_1]} (-b_2)^{[f_2]} \cdots (-b_m)^{[f_m]},$$

$$\text{then } w(B) = \sum_{i=1}^{n} e_k a_k = \sum_{i=1}^{m} f_i b_i \,.$$

For example, if $B = 1^{[5]} 3 (-4)(-2)^{[2]}$, then $w(B) = 5 \cdot 1 + 3 = 4 + 2 \cdot 2 = 8$. The weight function is clearly additive: If $B = A_1 A_2$, then $w(B) = w(A_1) + w(A_2)$. The definition of weight intentionally ignores the 0's in B because we will only care about blocks that are **zero-free**, i.e., which do not have 0 as a term. Every block $B \in \mathcal{B}(\mathbb{Z})$ can be written uniquely as $B = [0]^g B'$, where $B' \in \mathcal{B}(\mathbb{Z})$ and B' is zero-free. Since $[0]$ is prime in $\mathcal{B}(\mathbb{Z})$, any factorization of B consists of a factorization of B' with $[0]^g$ appended. Hence, the length set of B is just a shift by g of the length set of B', i.e., $\mathsf{L}(B) = g + \mathsf{L}(B')$, and the length multiplicity functions satisfy the similar relation $\mu(B', n) = \mu(B, n + g)$ for all $n \geq 0$. Thus, understanding the factorizations of elements of $\mathcal{B}(\mathbb{Z})$ reduces to understanding the factorizations of zero-free blocks.

Zero-free blocks work nicely with the weight function. If B is zero-free and $A|B$, then $w(A) = w(B)$ if and only if $A = B$. If B is zero-free and has only one positive or one negative term, then B is irreducible and $w(B)$ equals the absolute value of that term. By contrapositive, if B is zero-free and reducible, then $w(B) > |a|$ for each term a of B.

Our constructive proof for $\mathcal{B}(\mathbb{Z})$ relies on two lemmas, the shifting lemma and the augmenting lemma. The shifting lemma will allow us to increment all the lengths by 1, while the augmenting lemma will modify the multiplicities; used together, we will be able to construct any length-multiplicity function we desire. The shifting lemma works with very few assumptions, and so it will also be useful to us in Section 5. However, the augmenting lemma needs more hypotheses: as inputs, we will need zero-free sequences with a particular, but common, form.

Definition. Let $B \in \mathcal{B}(\mathbb{Z})$ be zero-free. Then B is **nice** if there are not $a \in B^+$ and $b \in B^-$ such that $w(B) = a + b$.

For example, the blocks $3^{[2]}(-2)(-4)$ and $1^{[5]}3(-2)(-6)$ are nice, but the block $C = 2^{[2]}6(-1)(-2)(-3)(-4)$ is not nice since $6 + 4 = 10 = w(C)$. Most blocks are nice. Indeed, if a block B were *not* nice because $a \in B^+$ and $b \in B^-$ satisfy

$w(B) = a + b$, then, since $w(B) = \sigma(B^+)$ by definition, we must have $b = \sigma(B^+) - a$, the sum of all the positive terms save a. By symmetry, $a = \sigma(B^-) - b$, the absolute value of the sum of all the negative terms save b. Niceness failed in our example C because $4 = 2 + 2$ (and, by symmetry, $6 = 1 + 2 + 3$). As we shall see, maintaining niceness will pose little trouble.

Our first lemma, the shifting lemma, takes a block B and creates a new block C, which increases the lengths of all factorizations by exactly 1, while maintaining the relative multiplicities. This can be achieved quickly if we multiply B by the prime element $[0]$ to get $C = [0]B$. However, we cannot use this quick solution, since we will also be using the augmenting lemma, which requires zero-free sequences. Instead, we have the zero-free solution below, which is still rather elementary.

Lemma 1 (Shifting Lemma). *Suppose $B \in \mathcal{B}(\mathbb{Z})$ is zero-free with at least two positive and two negative elements. Then we can construct a nice, zero-free, reducible block C from B such that $\mu(C, 0) = \mu(C, 1) = 0$ and $\mu(C, n + 1) = \mu(B, n)$ for all $n \geq 1$. Explicitly, for any $t \in \mathbb{N}$ with $t > w(B)$, we can choose C to be $B \cdot t \cdot (-t)$.*

Proof. Let B be zero-free with at least two positive and two negative elements. Choose $t \in \mathbb{N}$ such that $t > w(B)$ and set $C = B \cdot t \cdot (-t)$. By construction, C is in $\mathcal{B}(\mathbb{Z})$ and zero-free. Let $a \in C^+$ and $b \in C^-$. Since B has at least two positive elements, if $a \in B^+$, then $a < w(B)$; similarly, since B has at least two negative elements, if $b \in B^-$, then $b < w(B)$. So if $a \in B^+$ and $b \in B^-$, then $a + b < 2w(B) < t + w(B) = w(C)$. If $a \in B^+$ and $b = t$, then $a + b < w(B) + t = w(C)$. Similarly, if $a = t$ and $b \in B^-$, then $a + b < w(C)$. Lastly, if $a = b = t$, then $a + b = 2t > t + w(B) = w(C)$. In all cases, $a + b \neq w(C)$, so C is nice.

Clearly, $[t(-t)]$ is an irreducible of $\mathcal{B}(\mathbb{Z})$. We will show that every factorization of C is just a factorization of B with $[t(-t)]$ appended. This creates a bijection between the factorizations of C and the factorizations of B, where all the lengths increase by 1. Thus, $\mu(C, n + 1) = \mu(B, n)$ for all $n \geq 1$. Yet $C = B \cdot [t(-t)]$, so C is reducible, and thus, $\mu(C, 0) = \mu(C, 1) = 0$.

Suppose $C = A_1 \cdots A_n$ is a factorization of C into irreducibles. Then some factor, say A_n, contains $-t$. Since $t > w(B)$, A_n must contain t as well because no number of positive terms from B will have a sum greater than or equal to t on their own. But now, $[t(-t)]$ divides A_n in $\mathcal{F}(\mathbb{Z})$, and since $\mathcal{B}(\mathbb{Z})$ is saturated, $[t(-t)]$ divides A_n in $\mathcal{B}(\mathbb{Z})$. Since A_n was irreducible, $A_n = [t(-t)]$. The remaining terms $A_1 \cdots A_{n-1}$ must be a factorization of B, and the factorization of C had the claimed form. ∎

Whereas the shifting lemma increases all the lengths by 1, the augmenting lemma allows us to increase the multiplicities. Specifically, the augmenting lemma will allow us to create one new factorization of length 2 but maintain the multiplicities of all the other factorization lengths.

Lemma 2 (Augmenting Lemma). *Suppose $B \in \mathcal{B}(\mathbb{Z})$ is zero-free, reducible, and nice. Then we can construct a nice, zero-free, reducible $C \in \mathcal{B}(\mathbb{Z})$ from B such that $\mu(C, 2) = \mu(B, 2) + 1$ and $\mu(C, n) = \mu(B, n)$ for all $n \neq 2$.*

Proof. Suppose $B \in \mathcal{B}(\mathbb{Z})$ is zero-free, reducible, and nice. Write

$$B = a_1^{[u_1]} a_2^{[u_2]} \cdots a_n^{[u_n]} (-b_1)^{[v_1]} \cdots (-b_m)^{[v_m]}.$$

Set $w = w(B)$. Since B is reducible, $w > a_i$ and $w > b_j$ for all i and j. Set

$$C = a_1^{[u_1]}a_2^{[u_2]}\cdots a_n^{[u_n]}(w-b_1)^{[v_1]}\cdots(w-b_m)^{[v_m]}(-w)^{[v]},$$

where $v = v_1 + v_2 + \ldots + v_m$. Then C is zero-free because B was zero-free and $w > b_j$ for all j. By construction, we have that $C \in \mathcal{B}(\mathbb{Z})$.

We claim that C is nice. From C^-, we can only choose w. From C^+, we can choose either a_i or $w - b_j$ for some $1 \le i \le n$ or $1 \le j \le m$. So the sum of a positive and negative term of C is $w + a_i < 2w$ or $2w - b_j < 2w$. But $w(C) = vw \ge 2w$ because B was reducible and thus had at least two negative terms. Hence, C is nice.

Our construction of C has given us two long irreducible factors, D_1 and D_2. Specifically, let

$$D_1 = a_1^{[u_1]}a_2^{[u_2]}\cdots a_n^{[u_n]}(-w), \text{ and } D_2 = (w-b_1)^{[v_1]}\cdots(w-b_m)^{[v_m]}(-w)^{[v-1]},$$

which are both blocks by the definition of $w = w(B)$. Since D_1 has only one negative term, D_1 is irreducible. A factor of D_2 would need positive terms that add up to 0 mod w, which is only possible if we use all the positive terms since $\sum_{i=1}^m v_i b_i = w$. Thus, D_2 is irreducible. Since $C = D_1 D_2$ and both D_1 and D_2 are irreducible, this is the only factorization of C that has either D_1 or D_2 as a factor. This factorization will be precisely the "extra" factorization of C of length 2.

To handle the other factorizations, we will produce a bijection f from the factors (irreducible or reducible) of B to the factors of C other than D_1 and D_2. This map f will be sufficiently multiplicative to induce a bijection from the factorizations of B to the factorizations of C, omitting the factorization $C = D_1 D_2$.

Specifically, if the block $A = a_1^{[s_1]}a_2^{[s_2]}\cdots a_n^{[s_n]}(-b_1)^{[t_1]}\cdots(-b_m)^{[t_m]}$ divides B, then $s_i \le u_i$ and $t_j \le v_j$, and so we can define:

$$f(A) = a_1^{[s_1]}a_2^{[s_2]}\cdots a_n^{[s_n]}(w-b_1)^{[t_1]}\cdots(w-b_m)^{[t_m]}(-w)^{[t_1+t_2+\ldots+t_m]}.$$

Clearly, $f(A)$ is a block, $f(A)$ divides C, and $f(A)$ is a nonempty block if and only if A was. As a special case, we have $f(B) = C$. Since B was nice, $w - b_i \ne a_j$ for all $i \ne j$, so C has $n + m$ distinct positive terms. Hence, we can unambiguously determine each factor A from its image $f(A)$, and so f is injective.

By niceness, every $f(A)$ contains a_i and $w - b_j$ for some $1 \le i \le n$ and $1 \le j \le m$. Hence, D_1 and D_2 are not in the range of f, but we claim all other factors of C are. Suppose

$$D = a_1^{[y_1]}a_2^{[y_2]}\cdots a_n^{[y_n]}(w-b_1)^{[z_1]}\cdots(w-b_m)^{[z_m]}(-w)^{[z]}$$

is a factor of C other than D_1 or D_2. Since $D \in \mathcal{B}(\mathbb{Z})$, we have

$$0 = \sum_{i=1}^n y_i a_i + \sum_{j=1}^m (w-z_j)b_j - zw = \sum_{i=1}^n y_i a_i - \sum_{j=1}^m z_j b_j + w\sum_{j=1}^m z_j - zw,$$

and thus, w divides $\sum_{i=1}^n y_i a_i - \sum_{j=1}^m z_j b_j$. If $z_j = 0$ for all j, then w divides $\sum_{i=1}^n y_i a_i$. Yet $y_i \le u_i$ for all i, so $0 < \sum_{i=1}^n y_i a_i \le w$. Thus, $\sum_{i=1}^n y_i a_i = w$, and $y_j = u_j$ for all i, and so $D = D_1$, a contradiction. Similarly, if instead $y_i = 0$ for all i, then w divides $\sum_{j=1}^m z_j b_j$ and an analogous argument shows $D = D_2$, another contradiction. Thus, we have $y_i > 0$ for some i and $z_j > 0$ for some j.

Since $y_i > 0$ for some i, we have $0 < \sum_{i=1}^n y_i a_i \le \sum_{i=1}^n u_i a_i = w$. Similarly, since $z_j > 0$ for some j, we have $0 < \sum_{j=1}^m z_j b_j \le \sum_{j=1}^m v_j b_j = w$. Since w divides

$\sum_{i=1}^{n} y_i a_i - \sum_{j=1}^{m} z_j b_j$, the inequalities and divisibility condition force $\sum_{i=1}^{n} y_i a_i = \sum_{j=1}^{m} z_j b_j$. Hence, the sequence

$$A = a_1^{[y_1]} a_2^{[y_2]} \cdots a_n^{[y_n]} (-b_1)^{[z_1]} \cdots (-b_m)^{[z_m]}$$

is in $\mathcal{B}(\mathbb{Z})$ and A is clearly a factor of B with $f(A) = D$, as desired.

Our map f is sufficiently multiplicative. That is to say, if $A_1, A_2 \in \mathcal{B}(\mathbb{Z})$ and $A_1 A_2 | B$, then $f(A_1 A_2) = f(A_1) f(A_2)$. Hence, if $f(A)$ is irreducible, then so is A. On the other hand, if $f(A) \neq C$ and $f(A)$ is reducible, then $f(A) = DD'$ for some $D, D' \notin \{D_1, D_2\}$. By surjectivity, we can find factors E, E' of B such that $f(E) = D$ and $f(E') = D'$. Because we can determine E and E' from their images, we can check that the exponents match up so that $EE' = A$ and A is reducible. Thus, A is irreducible if and only if $f(A)$ is irreducible. By multiplicativity, if $B = A_1 \cdots A_k$ is a factorization of B into k irreducibles, then $C = f(B) = f(A_1) \cdots f(A_k)$ is a factorization of C into k irreducibles. The injectivity of f assures that distinct factorizations of B get mapped to distinct factorizations of C, while the surjectivity of f assures that we get every factorization of C other than $C = D_1 D_2$. Thus, C has exactly the same number of factorizations as B of each length, except length 2, where C has the additional factorization $C = D_1 D_2$. ∎

We are now ready to explicitly construct blocks with a given multiplicity function.

Theorem 3. *Let G be an additive abelian group with a given element $g \in G$ of infinite order. Then $\mathcal{B}(G)$ is length-multiplicity complete. For each function $f : \mathbb{N}_{\geq 2} \to \mathbb{N}$ with finite, nonempty support, one can recursively construct a nice, zero-free, reducible $B_f \in \mathcal{B}(G)$ with $\mu(B_f, n) = f(n)$ for all $n \geq 2$.*

Proof. Since $g \in G$ has infinite order, $\langle g \rangle \cong \mathbb{Z}$, and so, after identifying these groups, we may assume $\mathcal{B}(\mathbb{Z}) \subseteq \mathcal{B}(G)$. We will construct our blocks in $\mathcal{B}(\mathbb{Z})$.

Given such a function $f : \mathbb{N}_{\geq 2} \to \mathbb{N}$, we can evaluate the finite sum $\sigma(f) = \sum_{n=2}^{\infty} n f(n)$. We will prove by induction on $N \in \mathbb{N}$ that, if $\sigma(f) \leq N$, then one can recursively construct a block $B_f \in \mathcal{B}(\mathbb{Z})$ with $\mu(B_f, n) = f(n)$ for all $n \geq 2$.

Note that $\sigma(f) \geq 2$. In the base case, if $\sigma(f) = 2$, then necessarily $f(2) = 1$ and $f(n) = 0$ for all $n \geq 3$. For this f, take $B_f = 1^{[2]} 2^{[2]} (-3)^{[2]}$, which is nice, zero-free, and clearly has the requisite multiplicity function since its only factorization is as $[1 \cdot 2 \cdot (-3)]^2$.

Now assume we have an explicit construction whenever $\sigma(f) \leq N$ for some $N \geq 2$. Suppose we have a function $f : \mathbb{N}_{\geq 2} \to \mathbb{N}$ with finite, nonempty support and $\sigma(f) = N + 1$. If $f(2) \geq 1$, then set $g(2) = f(2) - 1$ and $g(n) = f(n)$ for all $n \geq 3$. Then $g : \mathbb{N}_{\geq 2} \to \mathbb{N}$ has finite, nonempty support and $\sigma(g) = \sigma(f) - 2 > 0$. By the induction hypothesis, we can explicitly construct a nice, zero-free, reducible B_g with $\mu(B_g, n) = g(n)$ for all $n \geq 2$. Now use the augmenting lemma to construct a nice, zero-free, reducible B_f from B_g with $\mu(B_f, 2) = g(2) + 1 = f(2)$ and $\mu(B_f, n) = g(n)$ for all $n \geq 3$.

If instead $f(2) = 0$, then set $g(n) = f(n + 1)$ for all $n \geq 2$. By the shifting lemma, we can construct a nice, zero-free, reducible B_f from B_g with $\mu(B_f, 2) = 0 = f(2)$ and $\mu(B_f, n + 1) = \mu(B_g, n) = g(n) = f(n + 1)$ for all $n \geq 2$. ∎

Our technique of augmenting and shifting can also be used for a constructive version of Kainrath's theorem in torsion groups of infinite exponent. However, we need to have

an explicit list of elements of arbitrarily high order, and there are some subtle technical obstacles to reducing blocks from $\mathcal{B}(\mathbb{Z})$ to blocks in $\mathcal{B}(\mathbb{Z}/m\mathbb{Z})$ while maintaining factorization multiplicities. The details appear in [**6**].

The proof of Theorem 3 provides a recursive construction of a block $B_f \in \mathcal{B}(\mathbb{Z})$ whose multiplicity function matches a given function f with nonempty, finite support. We will list such functions f as an infinite tuple, $(f(2), f(3), f(4), \ldots)$. In order to apply our recursive algorithm, we need to determine how f was constructed from the base function $(1, 0, 0, 0, \ldots)$ using shifts and augments. We work backwards from f: Any time we have a nonzero number in the first coordinate, then that came from an augment. If instead we have zero in the first coordinate, then that came from a shift. We illustrate this algorithm with an example.

Example 4. Suppose we wish to find a block B whose multiplicity function is $\mu(B, 2) = 1$, $\mu(B, 3) = 3$, $\mu(B, 5) = 1$, and $\mu(B, n) = 0$ for all other n. First, we want to construct the tuple $(1, 3, 0, 1, 0, \ldots)$ from the base tuple $(1, 0, 0, 0, 0, \ldots)$ using shifts and augments using the heuristic above:

$$(1,3,0,1,0,\ldots) \xleftarrow{\text{aug}} (0,3,0,1,0,\ldots) \xleftarrow{\text{shift}} (3,0,1,0,0,\ldots) \xleftarrow{\text{aug}}$$
$$(2,0,1,0,0,\ldots) \xleftarrow{\text{aug}} (1,0,1,0,0,\ldots) \xleftarrow{\text{aug}} (0,0,1,0,0,\ldots) \xleftarrow{\text{shift}}$$
$$(0,1,0,0,0,\ldots) \xleftarrow{\text{shift}} (1,0,0,0,0,\ldots).$$

To obtain B from the base, we reverse the order of the operations: shift, shift, augment, augment, augment, shift, augment. Now, we generate the blocks.

Base: $B_0 = 1^{[2]}2^{[2]}(-3)^{[2]}$.
Shift: Pick $t > w(B_0) = 6$. Say $t = 7$. Then $B_1 = 1^{[2]}2^{[2]}7(-3)^{[2]}(-7)$.
Shift: Pick $t > w(B_1) = 13$. Say $t = 14$. Then

$$B_2 = 1^{[2]}2^{[2]} \cdot 7 \cdot 14 \cdot (-3)^{[2]}(-7)(-14).$$

Augment: We have $w(B_2) = 27$. So

$$B_3 = 1^{[2]}2^{[2]}7 \cdot 14 \cdot 24^{[2]} \cdot 20 \cdot 13 \cdot (-27)^{[4]} = 1^{[2]}2^{[2]}7 \cdot 13 \cdot 14 \cdot 20 \cdot 24^{[2]}(-27)^{[4]}.$$

Augment: We have $w(B_3) = 108$. So

$$B_4 = 1^{[2]}2^{[2]} \cdot 7 \cdot 13 \cdot 14 \cdot 20 \cdot 24^{[2]}81^{[4]}(-108)^{[4]}.$$

Augment: We have $w(B_4) = 432$. So

$$B_5 = 1^{[2]}2^{[2]} \cdot 7 \cdot 13 \cdot 14 \cdot 20 \cdot 24^{[2]}81^{[4]}324^{[4]}(-432)^{[4]}.$$

Shift: Pick $t > w(B_5) = 1728$, say $t = 1729$. Then

$$B_6 = 1^{[2]}2^{[2]} \cdot 7 \cdot 13 \cdot 14 \cdot 20 \cdot 24^{[2]}81^{[4]}324^{[4]} \cdot 1729 \cdot (-432)^{[4]}(-1729).$$

Augment: We have $w(B_6) = 3457$. So

$$\begin{aligned} B_7 &= 1^{[2]}2^{[2]} \cdot 7 \cdot 13 \cdot 14 \cdot 20 \cdot 24^{[2]}81^{[4]}324^{[4]} \cdot 1729 \cdot 3025^{[4]} \cdot 1728 \cdot (-3457)^{[5]} \\ &= 1^{[2]}2^{[2]} \cdot 7 \cdot 13 \cdot 14 \cdot 20 \cdot 24^{[2]}81^{[4]}324^{[4]} \cdot 1728 \cdot 1729 \cdot 3025^{[4]}(-3457)^{[5]}. \end{aligned}$$

This block $B = B_7$ has one factorization of length 2, three factorizations of length 3, one factorization of length 5, and no others. Explicitly, we have

Length 2:

$[1^{[2]}2^{[2]} \cdot 7 \cdot 13 \cdot 14 \cdot 20 \cdot 24^{[2]}81^{[4]}324^{[4]}1729(-3457)][1728 \cdot 3025^{[4]}(-3457)^{[4]}];$

Length 3: $[1^{[2]}2^{[2]}7 \cdot 13 \cdot 14 \cdot 20 \cdot 24^{[2]}81^{[4]}3025(-3457)]\cdot$

$[324^{[4]}3025^{[3]}(-3457)^{[3]}] \cdot [1728 \cdot 1729 \cdot (-3457)];$

Length 3: $[1^{[2]}2^{[2]} \cdot 7 \cdot 13 \cdot 14 \cdot 20 \cdot 24^{[2]} \cdot 324 \cdot 3025(-3457)]\cdot$

$[81^{[4]}324^{[3]}3025^{[3]}(-3457)^{[3]}][1728 \cdot 1729 \cdot (-3457)];$

Length 3: $[1^{[2]}2^{[2]} \cdot 7 \cdot 14 \cdot 81 \cdot 324 \cdot 3025(-3457)]\cdot$

$[13 \cdot 20 \cdot 24^{[2]}81^{[3]}324^{[3]}3025^{[3]}(-3457)^{[3]}][1728 \cdot 1729(-3457)];$

Length 5: $[1 \cdot 2 \cdot 24 \cdot 81 \cdot 324 \cdot 3025(-3457)]^2[7 \cdot 20 \cdot 81 \cdot 324 \cdot 3025(-3457)]\cdot$

$[13 \cdot 14 \cdot 81 \cdot 324 \cdot 3025(-3457)][1728 \cdot 1729(-3457)].$

As one can see, the process of shift and augment constructs blocks with the desired length multiplicity, but the weights and cardinalities grow very quickly. Our method is likely not the most efficient, and so we ask the following.

Question: Given a function $f : \mathbb{N}_{\geq 2} \to \mathbb{N}$ with finite nonempty support, what is the smallest weight or smallest cardinality block $B \in \mathcal{B}(\mathbb{Z})$ whose multiplicity function equals f? We also ask the analogous question about length sets.

4. AN INTRODUCTION TO KRULL MONOIDS. As mentioned earlier, Krull monoids generalize algebraic number rings and Dedekind domains, but they also include monoids like block monoids, which cannot be the multiplicative monoid of a domain. They are the most general setting to have a class group that controls the factorization; other settings either do not have a class group or have one that contains only partial information about the factorization. One might expect that generalizing the constructions from algebraic number rings and Dedekind domains to the realm of monoids would produce an inherently complicated definition for a Krull monoid. Such a complicated, ideal-theoretic definition does exist. However, there is an equivalent, much simpler definition that we will present instead. This definition involves only general ideas, like free monoids and homomorphisms. With this alternate definition, the difficulty does not lie in understanding the definition but, rather, in verifying its correspondence with the classical ideal-theoretic formulation from number theory.

Let $\mathcal{F}(P)$ be a free abelian monoid on a set P. This monoid has unique factorization, and the elements of P are precisely the irreducibles (in fact, primes) of $\mathcal{F}(P)$. Given two elements $x = p_1^{d_1} \cdots p_n^{d_n}$ and $y = p_1^{e_1} \cdots p_n^{e_n}$ of $\mathcal{F}(P)$, where $d_i, e_i \geq 0$ for all i, the uniqueness of factorization allows us to define the **greatest common divisor** of x and y as $\gcd(x, y) = p_1^{f_1} \cdots p_n^{f_n}$, where $f_i = \min\{d_i, e_i\}$ for all $1 \leq i \leq n$. We can extend this definition in the natural way to take the $\gcd(A)$ of subsets A of $\mathcal{F}(P)$. We now have all we need to define Krull monoids.

Definition. Let H be a commutative, cancellative, atomic monoid, and let $\mathcal{F}(P)$ be a free abelian monoid. A monoid homomorphism $\phi : H \to \mathcal{F}(P)$ is a **divisor theory** for H if

(i) for each $p \in P$, there exists a finite subset $X \subseteq H$ such that $p = \gcd(\phi(X))$, and
(ii) for all $x, y \in H$, if $\phi(x) | \phi(y)$ in $\mathcal{F}(P)$, then we already have $x | y$ in H.

A monoid H is **Krull** if it has a divisor theory in some free abelian monoid $\mathcal{F}(P)$.

Intuitively, the divisor theory reveals that elements of Krull monoids have a secret decomposition into atoms from some external monoid, namely $\mathcal{F}(P)$. Condition (i) ensures that the Krull monoid, while it does not have explicit knowledge of these secret atoms in P, can encode those secret atoms using finite subsets. Condition (ii) ensures that factorization in $\mathcal{F}(P)$ aligns well with factorization in H; specifically, $\mathcal{F}(P)$ does not know more than H does about how elements of H fit inside each other. Condition (ii) also implies that $\phi(x) = \phi(y)$ if and only if x and y are associates in H.

The full connection between this definition and the classical, ideal-theoretic definition is explained in Chapter 2.4 of [**16**]. We will be content to sketch some illustrative examples of Krull monoids.

Example 5. Every block monoid $\mathcal{B}(G)$ over a finite abelian group G can be shown to have a divisor theory. If $|G| = 1$, then each block $B \in \mathcal{B}(G)$ is just $[0]^n$ for some $n \geq 0$. Thus, $\mathcal{B}(G)$ is isomorphic to the free abelian monoid $\mathcal{F}(G)$, and this isomorphism is trivially a divisor theory. Similarly, if $|G| = 2$, then write $G = \{0, g\}$. Each block $B \in \mathcal{B}(G)$ is just $[0]^n[g^2]^m$ for some $n, m \geq 0$. Let $A = [0]$ and $A' = [g^2]$. Then clearly $\mathcal{B}(G)$ is isomorphic to the free abelian monoid $\mathcal{F}(\{A, A'\})$, and this isomorphism is trivially a divisor theory.

If $|G| \geq 3$, then $\mathcal{B}(G)$ will not be isomorphic to a free abelian monoid, but we claim that the inclusion map of $\mathcal{B}(G)$ in $\mathcal{F}(G)$ is a divisor theory. In Section 2, we showed $\mathcal{B}(G)$ is saturated, which is precisely condition (ii). Let $g \in G$. If $g = 0$, then $g = \gcd([0], [0])$. If $g \neq 0$ and $\operatorname{ord}(g) = n \geq 3$, then $g = \gcd([g(-g)], [g^n])$. If $g \neq 0$ and $\operatorname{ord}(g) = 2$, then, since $|G| \geq 3$, we may choose some $h \in G \backslash \{0, g\}$. Then $g = \gcd([g^2], [g \cdot h \cdot (-g - h)])$. Hence, every $g \in G$ is the gcd of a finite set of blocks, so condition (i) is true.

One can adapt these arguments with some additional care to show that, if $G_0 \subseteq G$, then the block monoid $\mathcal{B}(G_0)$ is also Krull.

Example 6. Every Dedekind domain D is Krull. We will sketch how the classical theory matches up with the definition of Krull monoids using a divisor theory.

Let P be the set of prime ideals of D. Every nonzero proper ideal I of D factors uniquely as a product of prime ideals, and thus, the elements of $\mathcal{F}(P)$ can be identified with the nonzero ideals I of D (here, $1 \in \mathcal{F}(P)$ is identified with the ideal D). This yields a function $\phi : D^\bullet \to \mathcal{F}(P)$, where, for each nonzero $x \in D$, we define $\phi(x)$ to be (x), the principal ideal generated by x. Since $(xy) = (x)(y)$, we have that ϕ is a monoid homomorphism. If $(x)J = (y)$ for some ideal J of D, one can show that J must be principal and $J = (z)$ for some $z \in D$ such that $xz = y$. Hence, if $\phi(x) | \phi(y)$ in $\mathcal{F}(P)$, we have argued that $x | y$ already in D.

Now, let $\mathfrak{p}$ be a prime ideal. Choose a nonzero $a \in \mathfrak{p} \backslash \mathfrak{p}^2$. Then $\mathfrak{p}$ appears exactly once in the unique factorization of the ideal (a). If $(a) = \mathfrak{p}$, then clearly $\mathfrak{p} = \gcd((a), (a))$. Otherwise, $(a) = \mathfrak{p}\mathfrak{q}_1^{e_i} \cdots \mathfrak{q}_k^{e_k}$ for some prime ideals $\mathfrak{q}_i$ with $k \geq 1$ and $e_i \geq 1$ for all i. For each $1 \leq i \leq k$, let $J_i = \mathfrak{p}\mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_{i-1}^{e_{i-1}} \mathfrak{q}_{i+1}^{e_{i+1}} \cdots \mathfrak{q}_k^{e_k}$. Then we may choose a nonzero $a_i \in J_i \backslash J_i \mathfrak{q}_i$. Since $a_i \in J_i$, we are guaranteed that the unique factorization of (a_i) has $\mathfrak{p}$ and $\mathfrak{q}_j^{e_j}$ for $j \neq i$. However, since $a_i \notin J_i \mathfrak{q}_i$, we know that $\mathfrak{q}_i$ cannot appear in the unique factorization of (a_i). By construction, $\gcd((a), (a_1), \ldots, (a_k)) = \mathfrak{p}$, and so every prime ideal is the gcd of a finite set of principal ideals. Thus, the Dedekind domain has a divisor theory.

Example 7. We now can give more details why $\mathbb{Z}\left[\sqrt{-5}\right]$ is half-factorial. The class group of $\mathbb{Z}\left[\sqrt{-5}\right]$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, where the identity element is the class of principal prime ideals, and the nonidentity element is the class of all nonprincipal prime ideals. Because of the structure of the class group, the product of any two nonprincipal prime ideals is a principal ideal in $\mathbb{Z}\left[\sqrt{-5}\right]$. Conversely, if $x \in \mathbb{Z}\left[\sqrt{-5}\right]$ is irreducible, then we can show that $(x) = \mathfrak{p}$, a principal prime ideal (in which case x is prime), or $(x) = \mathfrak{p}_1\mathfrak{p}_2$, a product of two nonprincipal prime ideals. Indeed, if $(x) = \mathfrak{p}_1 \cdots \mathfrak{p}_n$ and $\mathfrak{p}_i$ is a principal prime ideal for some i, then $\mathfrak{p}_i = (y)$ for some nonunit $y \in \mathbb{Z}[\sqrt{-5}]$. Thus $y|x$ and by irreducibility, x and y are associates, so $(x) = (y) = \mathfrak{p}_i$. If all the $\mathfrak{p}_i$ are nonprincial instead, then $\mathfrak{p}_1\mathfrak{p}_2$ is a principal ideal (y) for some nonunit y. So $y|x$ and by irreducibility $(x) = (y) = \mathfrak{p}_1\mathfrak{p}_2$. Hence, for any nonzero, nonunit $z \in \mathbb{Z}[\sqrt{-5}]$, if we factor $(z) = \mathfrak{p}_1 \cdots \mathfrak{p}_k\mathfrak{q}_1 \cdots \mathfrak{q}_m$, where the $\mathfrak{p}_i$ are principal and the $\mathfrak{q}_i$ are nonprincipal, then m is even and by the uniqueness of ideal factorization, every factorization of z in $\mathbb{Z}[\sqrt{-5}]$ involves exactly k prime irreducibles and $m/2$ nonprime irreducibles.

Concretely, we have ideal factorizations

$$(2) = \mathfrak{p}^2 \qquad (3) = \mathfrak{q}_1\mathfrak{q}_2 \qquad \left(1 + \sqrt{-5}\right) = \mathfrak{p}\mathfrak{q}_1 \qquad \left(1 - \sqrt{-5}\right) = \mathfrak{p}\mathfrak{q}_2$$

where the nonprincipal ideals are $\mathfrak{p} = (2, 1 + \sqrt{5}) = (2, 1 - \sqrt{-5})$, $\mathfrak{q}_1 = (3, 1 + \sqrt{-5})$, and $\mathfrak{q}_2 = (3, 1 - \sqrt{-5})$. The earlier example of nonunique factorization was

$$2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}),$$

which corresponds to factorizations $(\mathfrak{p}^2) \cdot (\mathfrak{q}_1\mathfrak{q}_2) = (\mathfrak{p}\mathfrak{q}_1) \cdot (\mathfrak{p}\mathfrak{q}_2)$.

The formulation of Krull monoids in terms of a divisor theory also reveals a simple construction of the class group. If M is a submonoid of N, then we can define an equivalence relation $\sim_M$ by saying for $x, y \in N$, $x \sim_M y$ if there exists $m, m' \in M$ such that $mx = m'y$. We will denote the equivalence class of x by $[x]$. This equivalence relation is also a congruence, for if $x \sim_M y$ and $x' \sim_M y'$, then $xx' \sim_M yy'$. Thus, the quotient $N/\sim_M$ has the natural structure of a commutative monoid. However, in general, it need not be cancellative, and it may very well collapse to the trivial monoid $\{1\}$ even if $M \neq N$.

If H is a Krull monoid with divisor theory $\phi : H \to \mathcal{F}(P)$, then the quotient $G = \mathcal{F}(P)/\sim_{\phi(H)}$ has a particularly rich structure. Let $x \in \mathcal{F}(P)$, and assume $x \sim_{\phi(H)} 1$. Then there are $\phi(m), \phi(m') \in \phi(H)$ such that $\phi(m)x = \phi(m')$. So $\phi(m) \mid \phi(m')$ in $\mathcal{F}(P)$, and so by condition (i), we have that $m \mid m'$ in H. Let $m' = my$ for some $y \in H$. Then $\phi(m)x = \phi(m') = \phi(m)\phi(y)$, and since $\mathcal{F}(P)$ is cancellative, we conclude $x = \phi(y)$. Thus, $[1] = \phi(H)$, and so the quotient G is not trivial.

On the other hand, if $p \in P$, then by condition (ii), $p = \gcd(\phi(X))$ for some finite set X. Choose some $x \in X$. Then $p|\phi(x)$, so we may pick $y \in \mathcal{F}(P)$ such that $py = \phi(x)$. But then $[p][y] = [\phi(x)] = [1]$, so $[p]$ is invertible. Since the $p \in P$ generate $\mathcal{F}(P)$, all the elements of G are invertible, and thus, G is a group, called the **class group**. We set $G_0 = \{[p] \mid p \in P\}$ to be the **set of classes with primes** and henceforth will write G additively. Since $\mathcal{F}(P)$ is generated as a monoid by P, the subset G_0 generates G as a monoid (which is stronger than generating as a group).

The observant reader may notice that we have not used the full power of condition (ii) here to show that the quotient G is a group. That power is needed to show that

factorization in H can be controlled by factorization in $\mathcal{B}(G_0)$. We will not go into detail here, but the interested reader may wish to consult [**5**] as a starting point.

Theorem 8. *Let H be a Krull monoid with class group G and $G_0 \subseteq G$ the set of classes containing primes. Then there is a surjective monoid homomorphism $\theta : H \to \mathcal{B}(G_0)$ satisfying, for all $x \in H$:*

- *x is a unit if and only if $\theta(x) = 1$, the empty sequence;*
- *x is irreducible if and only if $\theta(x)$ is an irreducible block; and*
- *if $\theta(x) = B_1 \cdots B_n$ for some irreducible blocks B_i, then there exist irreducibles $y_1, \ldots, y_n \in H$ such that $x = y_1 \cdots y_n$ and $\theta(y_i) = B_i$ for all i.*

Consequently, $\mathsf{L}(x) = \mathsf{L}(\theta(x))$ and for all $n \geq 1$, $\mu(x, n) \geq \mu(\theta(x), n)$.

Proof. Sketch: Given $x \in H$, consider $\phi(x) \in \mathcal{F}(P)$, which we can write as $\phi(x) = p_1^{e_1} \cdots p_n^{e_n}$. Define $\theta(x) = [p_1]^{e_1} \cdots [p_n]^{e_n}$, which is a sequence in $\mathcal{F}(G_0)$. However, if we evaluate this sequence in G, we get:

$$\sigma(\theta(x)) = e_1[p_1] + \cdots + e_n[p_n] = [\phi(x)] = 0,$$

so $\theta(x)$ is in fact in $\mathcal{B}(G_0)$, as desired. We leave the other claims to the reader. ∎

Thus, the block monoid $\mathcal{B}(G_0)$ contains all the information about the length *sets* of H. However, distinct irreducibles of H may be identified by θ, implying that distinct factorizations of an element $x \in H$ may collapse to a single factorization of $\theta(x)$. So $\mathcal{B}(G_0)$ unfortunately does not contain all the information about the length *multiplicities* of H, and we only have an inequality between the values of the multiplicity function. Even so, the connection is strong enough to pull back properties of the block monoid to the original Krull monoid.

Corollary 9. *Let H be a Krull monoid with class group G and $G_0 \subseteq G$ the set of classes containing primes. Then H is length-set complete if and only if $\mathcal{B}(G_0)$ is.*

For every $B \in \mathcal{B}(G_0)$, there exists an $x \in H$ with $\theta(x) = B$ and for each $n \geq 1$, $\mu(x, n) = \mu(B, n)$. Hence, if $\mathcal{B}(G_0)$ is length-multiplicity complete, then so is H.

Proof. The statement about length sets follows from the previous theorem. For length multiplicities, we need some additional care. Let $\phi : H \to \mathcal{F}(P)$ be a divisor theory for H. Given $B \in \mathcal{B}(G_0)$, write out $B = g_1^{e_1} \cdots g_n^{e_n}$. For each $1 \leq i \leq n$, choose $p_i \in P$ such that $[p_i] = g_i$. Consider the element $y = p_1^{e_1} \cdots p_n^{e_n} \in \mathcal{F}(P)$. The congruence class of y in the additive group G is

$$[y] = e_1[p_1] + \cdots + e_n[p_n] = e_1 g_1 + \cdots + e_n g_n = \sigma(B) = 0$$

since B is zero-sum. But we argued that, for a divisor theory, the kernel of the projection $\mathcal{F}(P) \to G = \mathcal{F}(P)/\sim_{\phi(H)}$ is precisely $\phi(H)$, so $y \in \phi(H)$. Therefore, we may pick $x \in H$ such that $\phi(x) = y$. The definition of θ in Theorem 8 indicates that $\theta(x) = B$. We omit the details, but one can argue that $\mu(x, n) = \mu(B, n)$ for each n. Essentially, by picking only one $p \in P$ for each $g \in G_0$, we assured that multiple, nonassociate irreducibles do not collapse to the same irreducible of $\mathcal{B}(G_0)$. ∎

As an immediate consequence, Theorem 3 gains a wider application.

Corollary 10. *Let H be a Krull monoid with class group G and primes in every class. Assume we are given $g \in G$ of infinite order. Let $\theta : H \to \mathcal{B}(G)$ be the homomorphism above, and assume that preimages under θ of the elements of $\langle g \rangle$ can be found constructively. Then H is constructively length-set complete and length-multiplicity complete.*

Proof. By Theorem 3, any length set or length multiplicity function can be realized by some recursively constructed $B \in \mathcal{B}(\langle g \rangle) \subseteq \mathcal{B}(G)$. By the assumptions on θ, we can constructively find a preimage $x \in H$ of B under θ. ∎

We finish this section with two additional examples of Krull monoids with infinite class group that have been found in recent years. They do not always have primes in every class, however, which gives an impetus to removing that hypothesis from Kainrath's theorem.

Example 11. Let $n, m \geq 2$, and choose $a_1, \ldots, a_n, b_1, \ldots, b_k \in \mathbb{N}_{\geq 2}$. We can construct the homogeneous linear Diophantine monoid $\mathcal{M}(a_1, \ldots, a_n; b_1, \ldots, b_k)$ as

$$\mathcal{M}(a_1, \ldots, a_n; b_1, \ldots, b_k) = \left\{ (x_1, \ldots, x_{n+k}) \in \mathbb{N}^{n+k} \;\middle|\; \sum_{i=1}^{n} a_i x_i = \sum_{i=1}^{k} b_i y_{n+i} \right\}.$$

In [**8, 9**], the authors show that these monoids are Krull with class group congruent to $\mathbb{Z}$. However, they also showed that there are only finitely many classes with primes, i.e., that $G_0 \subseteq \mathbb{Z}$ is finite. Hence, Kainrath's theorem does not apply to these examples.

Example 12. Module theory also contains interesting examples of Krull monoids with infinite class group [**3, 4, 13**]. For example, if R is a local complete Noetherian commutative ring, we can consider the class $\mathcal{C}$ of finitely generated right-modules over R. Let $\mathcal{V}(\mathcal{C})$ be the isomorphism classes of elements of $\mathcal{C}$. Then $\mathcal{V}(\mathcal{C})$ can be turned into a monoid with the operation $[M] \oplus [N] = [M \oplus N]$. In a MONTHLY article [**3**], the authors show that if R is one-dimensional with reduced completion, then $\mathcal{V}(\mathcal{C})$ is cancellative and, in fact, a Krull monoid. The authors provide an explicit example (Example 4.17) where the class group is congruent to $\mathbb{Z}$ and contains a prime in every class. In general, varying the ring or the class of modules will give different class groups G and subsets G_0.

5. SUBSETS OF $\mathbb{Z}$. Kainrath's theorem assumes that every class contains a prime. However, as the final two examples from the previous section attest, this does not always occur. In fact, results by Claborn [**10**], Grams [**17**], and Leedham-Green [**20**] show that, for any abelian group G and any subset $G_0 \subseteq G$ that generates G as a monoid, there is a Dedekind domain D whose class group is G and set of classes with primes is G_0. Ideally, then, we would like to know whether these general Krull monoids are length-set complete and length-multiplicity complete. However, both Kainrath's proof for all infinite G and our constructive proof for $G \cong \mathbb{Z}$ heavily use the fact $G_0 = G$, so new techniques must be developed. We will still use the techniques from Section 4 to transfer most of the problem from the Krull monoid to the block monoid $\mathcal{B}(G_0)$. However, depending on the subset G_0, there can still be complicated additive combinatorics involved.

In this section, we work through a fairly simple example by having $G \cong \mathbb{Z}$ and $G_0 = \{\pm b^k \mid k \in \mathbb{N}_0\}$ for some fixed $b \geq 2$. Even in this simple example, we are only

able to construct length sets, not length multiplicities, though we have determined *all* the possible length sets. Finding the length sets for arbitrary $G_0 \subsetneq \mathbb{Z}$ is still an open problem; the upcoming article [**6**] by the first and third authors makes considerable headway toward a solution.

First, we should remark that length-set (and, consequently, length-multiplicity) completeness is not guaranteed. By [**1, 2**], if $G_0 \subseteq \mathbb{Z}$ has only finitely many positive elements or finitely many negative elements, then there is a finite rational number d such that for any length set $L = \mathsf{L}(B)$ for a nontrivial $B \in \mathcal{B}(G_0)$, we have $\max L / \min L \leq d$. Thus, a necessary condition for length-set and length-multiplicity completeness in $\mathbb{Z}$ is that G_0 has infinitely many positive and negative elements. We start with some lemmas.

Proposition 13. *Let $n \geq 2$. Suppose $a_1, a_2, \ldots, a_n \in \mathbb{N}$ such that $a_1 | a_2 | \ldots | a_n$. If $v_1, v_2, \ldots, v_n \geq 1$ such that $\sum_{i=1}^{n-1} v_i a_i = v_n a_n$, then for each $1 \leq w \leq v_n$, there exists $0 \leq v_{i,w} \leq v_i$ for each $1 \leq i \leq n-1$ such that $\sum_{i=1}^{n-1} v_{i,w} a_i = w a_n$.*

Proof. By induction on $n \geq 2$. Base case: If $v_1 a_1 = v_2 a_2$ and $v_2 \geq 1$, then $v_1 \geq 1$ as well. Since $a_2 = a_1 m$ for some $m \in \mathbb{N}$, we have $v_1 = v_2 m$, so for each $1 \leq w \leq v_2$, we may take $v_{1,w} = wm$.

Assume the statement is true for some $n \geq 2$. Let $a_1, \ldots, a_n, a_{n+1} \in \mathbb{N}$ such that $a_1 | a_2 | \ldots | a_n | a_{n+1}$ and $v_1, v_2, \ldots, v_n, v_{n+1} \geq 1$ such that $\sum_{i=1}^{n} v_i a_i = v_{n+1} a_{n+1}$. Let $1 \leq w \leq v_{n+1}$ be given, and choose $m \in \mathbb{N}$ such that $a_{n+1} = a_n m$. If $wm \leq v_n$, then setting $v_{n,w} = wm$ and $v_{i,w} = 0$ for all $1 \leq i \leq n-1$, we get our desired equality. Assume instead that $wm > v_n$. We have

$$\sum_{i=1}^{n-1} v_i a_i = v_{n+1} a_{n+1} - v_n a_n = (v_{n+1} m - v_n) a_n.$$

Since $1 \leq wm - v_n \leq v_{n+1} m - v_n$, we may let $w' = wm - v_n$. By the induction hypothesis, for each $1 \leq i \leq n-1$, we may pick $0 \leq v_{i,w'} \leq v_i$ such that $\sum_{i=1}^{n-1} v_{i,w'} a_i = w' a_n$. Now, set $v_{i,w} = v_{i,w'}$ for all $1 \leq i \leq n-1$, and set $v_{n,w} = v_n$. We have, as desired, that

$$\sum_{i=1}^{n} v_{i,w} a_i = w' a_n + v_{n,w} a_n = (wm - v_n) a_n + v_n a_n = wm a_n = w v_{n+1}. \qquad \blacksquare$$

Lemma 14. *Let $b \geq 2$ be given, and let $G_0 = \{\pm b^k \mid k \in \mathbb{N}_0\}$ be the set of positive powers of b and their negatives. If $X \in \mathcal{B}(G_0)$ is irreducible, then X has only one positive or one negative term.*

Proof. Suppose $X = (b^{k_1})^{[e_1]} \cdots (b^{k_m})^{[e_m]} (-b^{\ell_1})^{[f_1]} \cdots (-b^{\ell_n})^{[f_n]}$, where $k_1 < k_2 < \ldots < k_m$ and $\ell_1 < \ldots < \ell_n$. If any $k_i = \ell_j$, then the irreducible $(b^{k_i})(-b^{k_i})$ divides X, and since X is irreducible, we have $X = (b^{k_i})(-b^{k_i})$. Thus, assume that $k_i \neq \ell_j$ for all $1 \leq i \leq m$ and $1 \leq j \leq n$. Without loss of generality, assume $k_1 < \ell_1$. Choose $1 \leq r \leq m$ maximal such that $k_r < \ell_1$.

We have $w(X) = \sum_{j=1}^{n} f_j b^{\ell_j}$ so $w(X) \equiv 0 \mod b^{\ell_1}$ since $\ell_j \geq \ell_1$ for all $1 \leq j \leq n$. On the other hand, we also have $w(X) = \sum_{i=1}^{m} e_i b^{k_i}$, and so

$$0 \equiv w(X) = \sum_{i=1}^{m} e_i b^{k_i} \equiv \sum_{i=1}^{r} e_i b^{k_i} \mod b^{\ell_1}.$$

Thus, $\sum_{i=1}^{r} e_i b^{k_i} = e b^{\ell_1}$ for some $e \geq 1$. Since $b^{k_1} | b^{k_2} | \ldots | b^{k_r} | b^{\ell_1}$, we may apply Proposition 13 to find $0 \leq e_i' \leq e_i$ for all $1 \leq i \leq r$, such that $\sum_{i=1}^{r} e_i' b^{k_i} = b^{\ell_1}$. Thus, the irreducible block $(b^{k_1})^{[e_1']} \cdots (b^{k_r})^{[e_r']}(-b^{\ell_1})$ divides X, and since X is irreducible, we have $X = (b^{k_1})^{[e_1']} \cdots (b^{k_r})^{[e_r']}(-b^{\ell_1})$. ∎

The principal consequence of the previous lemma is that, when we factor some $B \in \mathcal{B}(G_0)$, we can track the irreducible factors X of B by their single positive or single negative terms. In particular, the weight, $w(X)$, will just be the absolute value of that single term. This structure forces the length set of B to have a uniform spacing, as described in the next theorem.

Theorem 15. *Let $b \geq 2$ be given, and let $G_0 = \{\pm b^k \mid k \in \mathbb{N}\}$ be the set of positive powers of b and their negatives. Let $B \in \mathcal{B}(G_0)$. Each factorization $B = X_1 \cdots X_\ell$ of B satisfies $\ell \equiv w(B) \mod (b-1)$. Thus, if $\mathsf{L}(B) = \{\ell_1, \ldots, \ell_r\}$, then for each $1 \leq i \leq j \leq r$ we have $\ell_i \equiv \ell_j \mod (b-1)$.*

Proof. Let X be any irreducible factor of B. By Lemma 14, X has exactly one positive or one negative term, say b^k or $-b^k$. In either case, $w(X) = b^k$, and hence, $w(X) \equiv 1 \mod b-1$. If $B = X_1 \ldots X_\ell$ is a factorization of B, then

$$w(B) = w(X_1) + \cdots + w(X_\ell) \equiv 1 + \cdots + 1 = \ell \mod (b-1)$$

as desired. The rest of the theorem follows. ∎

This theorem immediately implies that, if $b \geq 3$ and $G_0 = \{\pm b^k \mid k \in \mathbb{N}\}$, then $\mathcal{B}(G_0)$ is not length-set complete, in stark contrast to $\mathcal{B}(\mathbb{Z})$. However, if $b = 2$, then this theorem does not exclude any length sets. It turns out that, when $b = 2$, $\mathcal{B}(G_0)$ is length-set complete, and for $b \geq 3$, the spacing required by the previous theorem turns out to be the only restriction on length sets, as we will demonstrate in Theorem 17.

We will need a new approach for constructing blocks in $\mathcal{B}(G_0)$ with a given length set, compared to $\mathcal{B}(\mathbb{Z})$. The shifting lemma still works in our context since its proof only required us to find a $t \in G_0$ that is greater than a given weight $w(B)$ and for which $-t \in G_0$ as well. However, adapting the augmenting lemma poses a greater challenge. In that lemma, we took an existing sequence B and created a new sequence with terms like $-w(B)$ and $w(B) - b_i$. While the terms of B come from G_0, we cannot guarantee in general that $w(B)$ and $w(B) - b_i$ will also land in G_0. Thus, we will have to replace the augmenting lemma with a new lemma catered to the structure of G_0. Our replacement gives an explicit, rather than recursive, construction of length sets. The arguments are slightly more involved, and unfortunately, the additional complications force us to only study length sets and not length multiplicities.

Lemma 16. *Let $b \geq 2$ and $0 = a_0 < a_1 < a_2 < \cdots < a_k < a_{k+1} = n$. Set*

$$B = 1^{[b]} b^{[b-1]} (b^2)^{[b-1]} \cdots (b^{n-1})^{[b-1]} (b^n) \cdot (-b^n)(-b^{a_k})^{[e_k]}(-b^{a_{k-1}})^{[e_{k-1}]} \cdots (-b^{a_1})^{[e_1]}(-1)^{[e_0]},$$

where $e_0 = b^{a_1}$, *and for each* $1 \le i \le k$, *we have* $e_i = b^{a_{i+1}-a_i} - 1$. *Then*

$$\begin{aligned}\mathsf{L}(B) &= \{2 + (b-1)(n-a_j) \mid 0 \le j \le k+1\} \\ &= \{2, 2 + (b-1)(n-a_k), \ldots, 2 + (b-1)(n-a_1), 2 + (b-1)n\}.\end{aligned}$$

Proof. Let $0 = a_0 < a_1 < a_2 < \cdots < a_k < a_{k+1} = n$ and B be given satisfying the hypotheses. Note that the choice of exponents e_i makes

$$\sum_{i=0}^{j} e_i b^{a_i} = b^{a_{j+1}} \tag{5.1}$$

for every $0 \le j \le k$. In particular, $\sum_{i=0}^{k} e_i b^{a_i} + b^n = b^{a_{k+1}} + b^n = 2b^n$, and since

$$b \cdot 1 + (b-1)b + (b-1)b^2 + \ldots + (b-1)b^{n-1} + b^n = 2b^n,$$

the sum of the negative terms will cancel with the positive terms, so $B \in \mathcal{B}(G_0)$.

We now establish several factorizations of B, starting with the longest one. For each $0 \le m \le n$, choose $j_m \le k$ maximal such that $a_{j_m} \le m$. Set

$$A_m = b^m (-b^{a_{j_m}})^{[f_m]},$$

where $f_m = b^{m-a_{j_m}}$. Since A_m has only one positive term, A_m is an irreducible of $\mathcal{B}(G_0)$. Note that if $a_j \le m \le m' < a_{j+1}$, then $a_{j_m} = a_j = a_{j_{m'}}$. Thus, for each $1 \le j \le k$ we have

$$\begin{aligned}(b-1)\sum_{m=a_j}^{a_{j+1}-1} f_m &= (b-1)\sum_{m=a_j}^{a_{j+1}-1} b^{m-a_{j_m}} = (b-1)\sum_{m=a_j}^{a_{j+1}-1} b^{m-a_j} \\ &= (b-1)\sum_{i=0}^{a_{j+1}-a_j-1} b^i = (b-1)\frac{b^{a_{j+1}-a_j}-1}{b-1} = e_j.\end{aligned}$$

As a result,

$$A_{a_j}^{b-1} A_{a_j+1}^{b-1} \cdots A_{a_{j+1}-1}^{b-1} = (b^{a_j})^{[b-1]} (b^{a_j+1})^{[b-1]} \cdots (b^{a_{j+1}-1})^{[b-1]} (-b^{a_j})^{[e_j]},$$

so this product of irreducibles divides B and uses up all the instances of $-b^{a_j}$ in B. For $j = 0$, we have $A_0 = 1 \cdot (-1)$ and

$$1 + (b-1)\sum_{m=a_0}^{a_1-1} f_m = 1 + (b-1)\sum_{m=0}^{a_1-1} b^m = 1 + (b-1)\frac{b^{a_1}-1}{b-1} = b^{a_1} = e_0.$$

Thus,

$$A_0^b A_1^{b-1} \cdots A_{a_1-1}^{b-1} = 1^{[b]} (b^1)^{[b-1]} (b^2)^{[b-1]} \cdots (b^{a_1-1})^{[b-1]} (-1)^{[e_0]}$$

uses up all the instances of -1 in B. Combining these observations for all $0 \le j \le k$, we have

$$B = A_0^b A_1^{b-1} A_2^{b-1} \cdots A_{n-1}^{b-1} A_n,$$

which is a factorization of B as a product of $b + (n-1)(b-1) + 1 = 2 + (b-1)n$ irreducibles.

We can define several other important irreducible factors of B. When $a_1 > 1$, we define $X_1 = 1^{[b]}b^{[b-1]}(b^2)^{[b-1]} \cdots (b^{a_1-1})^{[b-1]}(-b^{a_1})$, and when $a_1 = 1$, we define $X_1 = 1^{[b]}(-b)$. We also define $Y_1 = b^{a_1}(-1)^{[e_0]}$. For each $2 \le j \le k$, we can define

$$X_j = 1^b b^{[b-1]}(b^2)^{[b-1]} \cdots (b^{a_j-1})^{[b-1]}(-b^{a_j})$$

$$Y_j = (b^{a_j})(-b^{a_{j-1}})(-b^{a_{j-2}})^{[e_{j-2}]} \cdots (-b^{a_1})^{[e_1]}(-1)^{[e_0]}.$$

The X_j clearly sum to zero, while the Y_j also do by Equation (5.1). Since they only have one positive or one negative term, the X_j and Y_j are irreducible in $\mathcal{B}(G_0)$ for each $1 \le j \le k$. When $j = k$, we have $B = X_k Y_k$, which is a factorization of B as a product of two irreducibles. For every $1 \le j < k$, we have $B = X_j Y_j B_j$, where

$$B_j = (b^{a_j})^{[b-2]}(b^{a_j+1})^{[b-1]}(b^{a_j+2})^{[b-1]} \cdots b^n \cdot (-b^n)(-b^{a_k})^{[e_k]} \cdots (-b^{a_{j+1}})^{[e_{j+1}]}(-b^{a_j})^{[e_j-1]}.$$

Examining the terms, we can see that

$$B_j = A_{a_j}^{b-2} A_{a_j+1}^{b-1} A_{a_j+2}^{b-1} \cdots A_{n-1}^{b-1} A_n$$

so B_j factors as a product of $b - 2 + (b-1)(n-1-a_j) + 1 = (b-1)(n-a_j)$ irreducibles. Since $B = X_j Y_j B_j$, we have that B factors as a product of $2 + (b-1)(n-a_j)$ irreducibles for each $1 \le j < k$. Recounting all the factorizations of B we have found, we have established that

$$\mathsf{L}(B) \supseteq \{2, 2 + (b-1)(n-a_k), \ldots, 2 + (b-1)(n-a_1), 2 + (b-1)n\}.$$

To conclude the proof, we will show that B has no other factorization lengths. In fact, one can show that B has no other *factorizations* beyond the ones we have described, but this is beyond our needs and rather technical.

By Lemma 14, every irreducible that divides B has exactly one positive or one negative term. Suppose X is an irreducible factor of B with at least two positive terms and, hence, exactly one negative term. That negative term cannot be -1 because the weight of the positive side is greater than 1. Hence, the negative term is $-b^{a_j}$ for some $1 \le j \le k+1$. So $w(X) = b^{a_j}$, and thus, X cannot contain b^m for any $m > a_j$. We also know X cannot contain b^{a_j} because by irreducibility, we would have $X = b^{a_j}(-b^{a_j})$, contradicting the assumption that X had at least two positive terms. So the positive terms of X are all powers of b smaller than b^{a_j}. Yet those terms must sum to $w(X) = b^{a_j}$, meaning we need to use all the smaller powers of b, i.e., $X = X_j = 1^{[b]}b^{[b-1]}(b^2)^{[b-1]} \cdots (b^{a_j-1})^{[b-1]}(-b^{a_j})$. In particular, such an X would use all the 1's from B, and thus, a given factorization of B can have at most one irreducible factor with more than one positive term.

Let $B = Z_1 \cdots Z_r$ be a factorization of B. If each Z_i has exactly one positive term, then $r = 2 + (b-1)n$, the number of positive terms in B. Suppose instead that some Z_i, say Z_1, has more than one positive term. Then $Z_1 = X_j$ for some $1 \le j \le k$. All the other Z_i have exactly one positive term each, so $r - 1$ equals the number of positive terms outside of Z_1, i.e.,

$$r - 1 = 2 + (b-1)n - (b + (b-1)(a_j - 1)) = 1 + (b-1)(n - a_j).$$

Thus, $r = 1 + n - (a_j - 1) = 2 + n - a_j$, as desired. ∎

Theorem 17. *Let $b \geq 2$ be given and let $G_0 = \{\pm b^k \mid k \in \mathbb{N}\}$ be the set of positive powers of b and their negatives. Let L be a finite, nonempty subset of $\mathbb{N}_{\geq 2}$, and write $L = \{\ell_1, \ldots, \ell_m\}$. Then $L = \mathsf{L}(B)$ for some $B \in \mathcal{B}(G_0)$ if and only if for all $1 \leq i \leq j \leq m$ we have $\ell_i \equiv \ell_j \mod (b-1)$.*

Proof. The "only if" is Theorem 15. For the "if," the hypothesis tells us that for each $1 \leq i \leq m$, we have $\ell_i - \ell_1 \equiv 0 \mod (b-1)$. Consider the set $L' = \{2, 2 + \ell_2 - \ell_1, \ldots, 2 + \ell_m - \ell_1\}$, which is a finite subset of $2 + (b-1)\mathbb{N}_0$. Hence, we can choose n such that $\ell_m - \ell_1 = (b-1)n$, and for each $1 \leq j \leq m-1$, we can now choose a_j such that

$$L' = \{2, 2 + (b-1)(n - a_{m-2}), \ldots, 2 + (b-1)(n - a_1), 2 + (b-1)n\}.$$

By Lemma 16, there is a $B \in \mathcal{B}(G_0)$ with $\mathsf{L}(B) = L'$. Now we can use the shifting lemma $\ell_1 - 2$ many times to shift B to some $B' \in \mathcal{B}(G_0)$ with $\mathsf{L}(B') = L$. We note that to apply the shifting lemma, we only need to find some $t > w(B)$, so we can take $t = b^k$ for a suitably large exponent k. ∎

ACKNOWLEDGMENT. The authors were supported by NSF grant #DMS-0648390.

REFERENCES

1. D. F. Anderson, S. T. Chapman, W. W. Smith, Some factorization properties of Krull domains with infinite cyclic divisor class group, *J. Pure Appl. Algebra* **96** (1994) 97–112.
2. ———, On Krull half-factorial domains with infinite cyclic divisor class group, *Houston J. Math.* **20** (1994) 561–570.
3. N. R. Baeth, A. Geroldinger, Monoids of modules and arithmetic of direct-sum decompositions, *Pacific J. Math.* **271** no. 2 (2014) 257–319.
4. ———, R. Wiegand, Factorization theory and decompositions of modules, *Amer. Math. Monthly* **120** no. 1 (2013) 3–34.
5. P. Baginski, S. T. Chapman, Factorizations of algebraic integers, block monoids, and additive number theory, *Amer. Math. Monthly* **118** no. 10 (2011) 901–920.
6. ———, G. J. Schaeffer, Length-set completeness for Krull monoids with infinite class group, (preprint).
7. L. Carlitz, A characterization of algebraic number fields with class number two, *Proc. Amer. Math. Soc.* **11** (1960) 391–392.
8. S. T. Chapman, U. Krause, E. Oeljeklaus, Monoids determined by a homogeneous linear Diophantine equation and the half-factorial property, *J. Pure Appl. Algebra* **151** no. 2 (2000) 107–133.
9. ———, On Diophantine monoids and their class groups, *Pacific J. Math.* **207** no. 1 (2002) 125–147.
10. L. Claborn, Every abelian group is a class group, *Pacific J. Math.* **18** (1966) 219–222.
11. K. Cziszter, M. Domokos, On the generalized Davenport constant and the Noether number, *Cent. Eur. J. Math.* **11** no. 9 (2013) 1605–1615.
12. H. M. Edwards, *Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory*. Corrected reprint of the first (1977) ed., Graduate Texts in Mathematics, Vol. 50, Springer-Verlag, New York, 1996.
13. A. Facchini, Krull monoids and their application in module theory, in *Algebras, Rings and Their Representations*, Ed. A. Facchini, K. Fuller, C. M. Ringel, and C. Santa-Clara, World Scientific Publishing, Hackensack, NJ, 2006. 53–71.
14. S. Frisch, A construction of integer-valued polynomials with prescribed sets of lengths of factorizations, *Monatsh. Math.* **171** no. 3–4 (2013) 341–350.
15. A. Geroldinger, Sets of lengths, *Amer. Math. Monthly* (forthcoming).
16. ———, F. Halter-Koch, *Non-Unique Factorizations. Algebraic, Combinatorial and Analytical Theory*. Chapman & Hall, Boca Raton, FL, 2006.
17. A. P. Grams, The distribution of prime ideals of a Dedekind domain, *Bull. Austr. Math. Soc.* **11** (1974) 429–441.
18. D. J. Grynkiewicz, *Structural Additive Theory*. Developments in Mathematics, Vol. 30. Springer, New York, 2013.
19. F. Kainrath, Factorization in Krull monoids with infinite class group, *Colloq. Math.* **80** (1999) 23–30.

20. C. R. Leedham-Green, The class group of Dedekind domains, *Trans. Amer. Math. Soc.* **163** (1972) 493–500.
21. W. A. Schmid, Some recent results and open problems on sets of lengths of Krull monoids with finite class group (2015), http://arxiv.org/abs/1511.08080 .

PAUL BAGINSKI received his Ph.D. from the University of California, Berkeley in 2009. He spent an NSF postdoc at Université Lyon I in France, followed by a visiting position at Smith College. He has been an assistant professor of mathematics at Fairfield University since 2013.
Department of Mathematics, Fairfield University, 1073 North Benson Rd., Fairfield, CT 06824
baginski@gmail.com

RYAN RODRIGUEZ received his mathematics Ph.D. in 2014 from the University of California, San Diego.

GEORGE J. SCHAEFFER received his B.S. and M.S. in mathematical sciences at Carnegie Mellon University in 2007 and his Ph.D. from the University of California, Berkeley in 2012. He is currently a lecturer in the Department of Mathematics at Stanford University.
Department of Mathematics, 450 Serra Mall / Building 380, Stanford, CA 94305-2125
gschaeff.research@gmail.com

YIWEI SHE is a Prize Postdoctoral Fellow at Columbia University. She received her B.S. from Northwestern University in 2010 and her Ph.D. from the University of Chicago in 2015.
Department of Mathematics, Columbia University, 2990 Broadway, New York, NY 10027
yiwei@math.columbia.edu