On Product and Sum Decompositions of Sets: The Factorization Theory of Power Monoids

Dissertation

Presented in Partial Fulfillment of the Requirements for the Degree
Doctor of Philosophy in the Graduate School of The Ohio State University

By

Austin Alan Antoniou, M.S.
Graduate Program in Mathematics

The Ohio State University
2020

Dissertation Committee:

K. Alan Loper
Ivo Herzog
Cosmin Roman

Abstract

Let $(H, \cdot)$ be a monoid. The *power monoid* of H, first studied in full generality by Y. Fan and S. Tringali, is the collection $\mathcal{P}_{\text{fin}}(H)$ of finite, nonempty subsets of H, with the operation of setwise multiplication given by $X \cdot Y := \{x \cdot y : x \in X, y \in Y\}$. This is a highly non-cancellative monoid in which many standard factorization questions (e.g., for which H is $\mathcal{P}_{\text{fin}}(H)$ BF, or which sets occur as sets of factorization lengths) have complicated and interesting answers. We pivot to the submonoid $\mathcal{P}_{\text{fin},1}(H)$ consisting of finite subsets containing 1, which is equimorphic to $\mathcal{P}_{\text{fin}}(H)$ when H is a group, but is also deserving of study in its own right.

We determine exact conditions on H for which $\mathcal{P}_{\text{fin},1}(H)$ is atomic (resp. BF). Due to its non-cancellative nature, $\mathcal{P}_{\text{fin},1}(H)$ eludes characterization by some of the usual tools of factorization theory. To respond in a systematic way to non-cancellative phenomena, we formulate the notion of "minimal" factorizations and the "minimal" versions of the usual properties BmF, FmF,HmF, and UmF (corresponding, respectively to BF, FF, HF, and UF or factoriality). With this in hand, we can give exact conditions on those H which make $\mathcal{P}_{\text{fin},1}(H)$ BmF (resp. FmF, HmF, UmF). As a further application, we show that all intervals of the form $[2, k]$ are realized as sets of factorization lengths in $\mathcal{P}_{\text{fin},0}(\mathbb{Z}/n\mathbb{Z})$ for $k \in [2, n-1]$.

Even $\mathcal{P}_{\text{fin},0}(\mathbb{N})$, the reduced power monoid of the naturals, is a rich object of study. Of particular interest are the quantifiable differences between the intervals $[0, n]$ and the other elements of $\mathcal{P}_{\text{fin},0}(\mathbb{N})$. It is already known, due to Fan and Tringali, that $\mathsf{L}_{\mathcal{P}_{\text{fin},0}(\mathbb{N})}([0, n]) = [2, n]$. We refine this result by introducing the *partition type* of a factorization and showing that $[0, n]$ has factorizations of almost every partition type, and that non-intervals sharply fail to do so. Intervals are further distinguished by giving an exponential lower bound on $|\mathsf{Z}_{\mathcal{P}_{\text{fin},0}(\mathbb{N})}([0, n])|$, the number of factorizations of $[0, n]$.

Following the idea of partition type beyond the realm of power monoids, we take a detour to show that the density of atoms of a given degree in any numerical semigroup algebra over a finite field is asymptotically zero (as we let the degree approach infinity).

Returning to power monoids, we end by focusing in particular on sets of factorization lengths in $\mathcal{P}_{\text{fin},0}(\mathbb{N})$. The study of which sets occur as sets of lengths in $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ is fairly difficult, and requires some new tools. To this end, we show that all factorization phenomena that occur in $\mathcal{P}_{\text{fin},0}(\mathbb{N}^d)$, for $d > 1$, also occur in $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ (and vice-versa). Consequently, we may leverage the intuition and geometry of the integer lattice. After developing the necessary methods, we recover some known results on sets of lengths; namely, that $\{n\}$

and $\{2, n+1\}$ occur as sets of lengths for any $n \geq 2$. Finally, we demonstrate that $[2, m+2] \cup \{m+n+1\}$ can be realized as a set of factorization lengths for all $m \geq 1$ and $n \geq 2$, representing progress toward the conjecture, made by Fan and Tringali, that $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ realizes all feasible sets of lengths.

Acknowledgements

I owe my thanks to many, many people whose generosity and support have helped me immeasurably while I pursued this degree.

To my parents Deane and Kim, without whom I would quite literally (and in many other senses) not be here. You have always encouraged me to do my best, flown me home for the holidays, and given me wisdom to help me navigate the world.

To my grandparents Fay and Al, who have shown me constant love and support.

To YiaYia, Jason, and Kyle, for hiding me safely away from work every Thanksgiving and July Fourth.

To Peter, for always making sure that I'm curious.

To my advisor, Alan Loper, for helping me to grow as a mathematician, for asking interesting questions, for encouraging me to think imaginatively, for helping me to look beyond accidents of small numbers, and for his patience.

To my collaborator, Salvo, who introduced me to power monoids and with whom I co-wrote an article which eventually became Section 2.4 and Chapters 3-4. Thank you for letting me work on such an interesting problem suited to my strengths, for being a thorough and thoughtful coathor, and for being a friend during my time in Austria and afterward.

To Alfred Geroldinger, whose work I greatly admire, for hosting me in Austria and for keeping factorization theory and combinatorial group theory fashionable.

To Daniel Madden, my first mathematical mentor, who taught me to always write things that are true.

To all the mathematicians I've encountered who cultivated my interest and encouraged me to learn more.

To all my friends in the math department for productive (and not) discussions about math (and not).

To Alex and Michael, for many dinners together, for celebrating and commiserating together, and for contemplating trivial things far more deeply than is reasonable—together.

I owe Alex a special thanks for his tolerance of my annoying habits in our shared office, for enjoying music with me, and for our many discussions toward solving all the world's problems.

To Jared, for always checking in on me and for reminding me of all the wonderful and silly things that exist in the world.

To all the people I've had the opportunity to know who have helped me to change and to grow. Few people will read this document, but many have helped shape it by shaping me.

Vita

1992	Born in Phoenix, AZ
2010	Graduated Mountain Ridge High School
2011-2014	Undergraduate Teaching Assistant, Department of Mathematics, University of Arizona
2014	B.S. in Mathematics, University of Arizona
2017	M.S. in Mathematics, The Ohio State University
2014-Present	Graduate Teaching Associate, Department of Mathematics, The Ohio State University

Fields of Study

Major Field: Mathematics

Specialization: Commutative Algebra, Factorization Theory

Table of Contents

Chapter 1

Introduction

Factorization theory pursues a full understanding of how complex objects decompose into their simplest constituent parts. Depending on the algebraic structure in question, the difficulty of gaining such an understanding can vary wildly. Some objects can be broken down in exactly one way, while others exhibit more exotic behavior and are able to be broken down into several qualitatively different combinations of simpler parts. Among our tasks are to test the bounds of this behavior, and to completely classify the circumstances under which it can occur. In the present work, we bring our attention to a fairly new class of algebraic objects – the titular "power monoids" – which possess many characteristics that make their study difficult, hence interesting.

1.1 Motivation

The motivation to study power monoids is drawn from two sources: factorization theory and arithmetic combinatorics.

Arithmetic combinatorics has historically involved sumsets in abelian groups (or even just in $\mathbb{Z}$). It has been concerned with questions such as "how large can a sumset be expected to be?" which is resolved in the case of $\mathbb{Z}/p\mathbb{Z}$ by the Cauchy-Davenport inequality: for $A, B \subseteq \mathbb{Z}/p\mathbb{Z}$, $|A+B| \geq \min\{p, |A|+|B|-1\}$. There is, of course, an accompanying inverse problem; namely, which pairs A and B satisfy $|A+B| = |A|+|B|-1$? This is resolved by Vosper's Theorem, which says that the extremal pairs A and B are arithmetic progressions with the same difference. Though this is but a small slice of what the subject has to offer, it brings to our attention the potential for structural questions in arithmetic combinatorics and consequently highlights its surprising ideological closeness to parts of factorization theory.

The broadest question in factorization theory is: "how do elements decompose into atoms?" Asking this question requires one to first specify (1) which elements, (2) which definition of "atom", and (3) which values of "how"? The first two points may be clear – or should be after Chapter 2 – but the third refers to what constitutes reasonable answers to the original question. Is it enough to specify that an element has more than one factorization? Or do we wish to distinguish factorizations by lengths, or by the types of atoms that they involve, or some further level of distinction? Making these ideas rigorous is one of the challenges but also one of the predominantly interesting features of factorization theory.

Once we have settled these parameters of the question, we can then think about various settings and how to characterize their factorization behavior. Historically, one of the first classes of rings which drew the attention of many was that of rings of integers inside number fields. In this setting, we find perhaps the most famous example of a ring which fails to have unique factorization, $\mathbb{Z}[\sqrt{-5}]$, as $2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. A significant effort, which furthered the study of ring theory while also drawing ideas from analysis and geometry, went toward understanding the full range of behaviors exhibited by elements of rings of integers. This eventually blossomed into the study of general Dedekind domains, Krull domains, and further generalizations.

From this, we see how even a single class of examples can have a lasting impact on factorization theory, and on mathematics. However, much of the field to date has focused on studying factorization in rings which are not only commutative but also *cancellative*, meaning $ab = ac$ implies that $b = c$. This is not to say that the subject has neglected non-cancellative settings altogether; monoids of modules or monoids of ideals in commutative rings are certainly well-studied. However, these settings can involve heavy algebraic machinery and make it difficult to interact with other areas of mathematics. On the other hand, power monoids are highly non-cancellative while being rooted in a simple and natural combinatorial construction: the collection of (finite) subsets of a monoid, endowed with setwise multiplication. We strive to open up the study of power monoids to bring attention to their own robust structure and also to explore their inevitable entanglement with combinatorics, number theory, and other areas of mathematics.

1.2 Plan and Main Results

In the remainder of this chapter, we will set some notation and conventions to be used hereafter.

Chapter 2 begins laying the foundation neessary to have a detailed discussion of factorizations. Here we will give definitions and examples of properties which characterize the extend to which a monoid may fail to have uniqueness of factorization (the conditions UF, HF, FF, BF). The chapter ends with a comparison of the present framework to the existing body of literature, especially the work of D.D. Anderson et al.

Chapter 3 introduces the main object of study: the power monoid, $\mathcal{P}_{\text{fin}}(H)$. We discuss the reduction, possible in many cases of interest, to the reduced power monoid $\mathcal{P}_{\text{fin},1}(H)$. We determine that $\mathcal{P}_{\text{fin},1}(H)$ is atomic exactly when H has no nontrivial idempotent elements or elements of order 2 (Theorem 3.2.3) and that $\mathcal{P}_{\text{fin},1}(H)$ is BF exactly when H is torsion free (Theorem 3.2.5).

Chapter 4 returns to a discussion of factorization theory in general as we address the degeneracy of some of the usual notions in a non-cancellative setting. In response to this problem, we formulate the notion of a *minimal factorization* and minimal versions of the usual factorization properties: UmF, HmF, FmF, BmF. We then apply our new framework to power monoids to find that $\mathcal{P}_{\text{fin},1}(H)$ is BmF or FmF if and only if $\mathcal{P}_{\text{fin},1}(H)$ is atomic (Theorem 4.2.4); that $\mathcal{P}_{\text{fin},1}(H)$ is HmF if and only if H is a group of order dividing 3

(Theorem 4.2.5); and that $\mathcal{P}_{\mathrm{fin},1}(H)$ is UmF if and only if H is trivial (Corollary 4.2.6).

In Chapter 5, we begin to focus on the specific case of the reduced power monoid of $\mathbb{N}$ with addition, which we refer to as $\mathcal{P}_{\mathrm{fin},0}(\mathbb{N})$. In this setting we can leverage the linear ordering on $\mathbb{N}$ to introduce the *partition type* of a given factorization in $\mathcal{P}_{\mathrm{fin},0}(\mathbb{N})$. This is a new measure by which we may asses the degree to which an element fails to factor uniquely. Indeed, we see that the intervals $[0, n]$ have factorizations of almost every possible partition type (Theorem 5.2.8). This signifies a sharp dichotomy with the other elements of $\mathcal{P}_{\mathrm{fin},0}(\mathbb{N})$, as any non-interval $X \in \mathcal{P}_{\mathrm{fin},0}(\mathbb{N})$ satisfies $\mathsf{L}_{\mathcal{P}_{\mathrm{fin},0}(\mathbb{N})}(X) \leq \max(X)/2$ (Theorem 5.3.5).

As a corollary to the idea of partition types, we conclude the chapter with an aside which shows that numerical semigroup algebras have zero asymptotic density; see Section 5.4 and Theorem 5.4.10 for the details.

Chapter 6 continues along the direction of quantifying the wild factorization behavior of intervals in $\mathcal{P}_{\mathrm{fin},0}(\mathbb{N})$. By constructing large families of atoms of $\mathcal{P}_{\mathrm{fin},0}(\mathbb{N})$ and tying their growth rates to the growth of generalized Fibonacci numbers, we demonstrate that the number of factorizations of the interval $[0, n]$ grows exponentially with n. In particular, for any $\varepsilon > 0$, there is a constant C such that, for sufficiently large n, $|\mathsf{Z}_{\mathcal{P}_{\mathrm{fin},0}(\mathbb{N})}([0, n])| \geq C(\sqrt[4]{2} - \varepsilon)^n$ (Theorem 6.3.4).

Chapter 7 first establishes that $\mathcal{P}_{\mathrm{fin},0}(\mathbb{N})$ and $\mathcal{P}_{\mathrm{fin},0}(\mathbb{N}^d)$ have, in a sense suitable for our purposes, identical factorization behavior for all $d > 1$. This affords us the opportunity to use higher-dimensional geometric intuition to attack problems in $\mathcal{P}_{\mathrm{fin},0}(\mathbb{N})$ and leads us to develop some new methods for understanding factorizations in $\mathcal{P}_{\mathrm{fin},0}(\mathbb{N}^d)$. This line of thought allows us to recover some known results for realizations of length sets in $\mathcal{P}_{\mathrm{fin},0}(\mathbb{N})$; namely, that $\{n\} \in \mathcal{L}(\mathcal{P}_{\mathrm{fin},0}(\mathbb{N}))$ for all $n \geq 2$ (Theorem 7.2.5 or [FT18, Proposition 4.9]) and that $\{2, n+1\} \in \mathcal{L}(\mathcal{P}_{\mathrm{fin},0}(\mathbb{N}))$ for all $n \geq 2$ (Theorem 7.3.3 or [FT18, Proposition 4.10]). Finally, we push the methods developed to realize a new family of sets as sets of lengths in $\mathcal{P}_{\mathrm{fin},0}(\mathbb{N})$; we show that $[2, m+2] \cup \{m+n+1\} \in \mathcal{L}(\mathcal{P}_{\mathrm{fin},0}(\mathbb{N}))$ for all $n \geq 2$ and $m \geq 1$ (Theorem 7.4.2).

It should be mentioned that large sections of what follows are the result of joint work with Salvatore Tringali, whose paper [FT18] with Yushuang Fan marks the first entry in the literature toward the general study of power monoids. Specifically, Section 2.4 and Chapters 3 and 4 are borrowed from [AT19]. Even further, the questions posed by Fan and Tringali – especially the conjecture that the system of sets of lengths of $\mathcal{P}_{\mathrm{fin},0}(\mathbb{N})$ is as large as possible, made in [FT18, Section 5] – inspired the work done in Chapter 7.

1.3 Notation and Conventions

- $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$, $\mathbb{Z} = \{0, \pm1, \pm2, \ldots\}$, and $\mathbb{R}$ denote the sets of natural numbers, integers, and real numbers, respectively. Here we adopt the French convention that $0 \in \mathbb{N}$ so that $\mathbb{N}$ is a monoid.
- In general, unless otherwise specified, lowercase letters (a, b, x, y, etc.) will usually refer to elements of a monoid; ordinary uppercase letters to sets and subsets (A, B, X, Y, etc.); script or calligraphic uppercase letters ($\mathcal{A}$, $\mathcal{C}$, $\mathcal{F}$, $\mathcal{P}$) to distinguished subsets or collections of subsets; math fraktur letters ($\mathfrak{a}$, $\mathfrak{b}$, etc.) to words in a free monoid over a given generating set (see Section 2.1 for more details on

free monoids). Specifically, i, j, k, ℓ, m, and n will usually stand for non-negative integers. H will stand for a monoid, G for a group, and R for a ring.

- $X \subseteq Y$ will mean that X is a subset of Y; $X \subsetneqq Y$ will mean that $X \subseteq Y$ but $X \neq Y$; $K \leq H$ will mean that K is a submonoid of H.
- For a subset $S \subseteq \mathbb{R}$ and $k \in \mathbb{N}$, we set the notation $S_{>k} := \{n \in S : n > k\}$ and $S_{\geq k} := \{n \in S : n \geq k\}$.
- For $a, b \in \mathbb{R} \cup \{\infty\}$, $[a, b] = \{n \in \mathbb{Z} : a \leq n \leq b\}$ shall denote the (integer) interval from a to b.
- For a real number x, $\lfloor x \rfloor := \max\{n \in \mathbb{Z} : n \leq x\}$ (read *floor of x*) is the greatest integer less than x. Similarly, $\lceil x \rceil := \min\{n \in \mathbb{Z} : n \geq x\}$ (read *ceiling of x*) is the least integer greater than x.
- If S is a set and $\mathcal{E}$ is an equivalence relation on S, the equivalence class of some $x \in S$ shall be denoted by $[x]_{\mathcal{E}}$. The subscript may be removed in situations where the implied equivalence is clear.
- Fix an integer $m > 1$. When m is understood from context, $\bar{a} \in \mathbb{Z}/m\mathbb{Z}$ will denote the residue class of a modulo m. We will write $a \equiv b \pmod{m}$ if $\bar{a} = \bar{b}$.
- On occasion, we will wish to lift residue classes to elements of $\mathbb{N}$. If $x \in \mathbb{Z}/m\mathbb{Z}$ and m is well understood from context, we set $\hat{x} := \min(x \cap \mathbb{N}) \in [0, m-1]$. By a similar token, for a subset $X \subseteq \mathbb{Z}/m\mathbb{Z}$, we set $\hat{X} := \{\hat{x} : x \in X\}$.
- In general, we will refer to the operation of a not necessarily commutative monoid $(H, \cdot)$ as "multiplication". We will often write xy instead of $x \cdot y$ when no confusion is likely to arise.
- The identity of a multiplicative monoid $(H, \cdot)$ will be called 1; the identity of an additive monoid $(H, +)$ will be called 0.
- For a $k \in \mathbb{N}$ and elements x_i of some set for $i \in [1, k]$, we will often write the family $X := \{x_i : i \in [1, k]\}$ in "long form" as $x_1, \ldots, x_k$. On the other hand, we may refer to its elements simply "the x_i" or $\{x_i\}_i$ for brevity. If X is a subset of a monoid $(H, \cdot)$, we will write the ordered product of the elements of X as $x_1 \cdots x_k$. In particular, if k happens to be 0, this product is empty and we set the convention $x_1 \cdots x_k = 1$ to avoid any confusion or ill-definedness.

Chapter 2

Monoids and Factorizations

Monoids, in general, have very little structure while still having enough to make their study tractible. This delicate balance makes the setting of monoids a desirable one for a broad and far-reaching exploration of factorization and other multiplcatively-focused topics. This chapter will include many definitions and elementary results which range from standard fixtures of the literature to specialized notions for the present work.

2.1 Fundamentals of Factorization Theory

We begin by laying out the framework in which we will study factorizations.

Definition 2.1.1. Let H be a monoid.

- $u \in H$ is a **unit** if there is $v \in H$ with $uv = vu = 1$. The group of units in H is denoted by $H^\times$. H is called *reduced* if $H^\times = \{1\}$.
- $x, y \in H$ are **associates** if there are units $u, v \in H^\times$ so that $x = uyv$. In this case, we write $x \simeq_H y$ (or just $x \simeq y$ if there is no chance of confusion).
- $a \in H \setminus H^\times$ is an **atom** if, whenever $a = xy$, either $x \in H^\times$ or $y \in H^\times$. The set of atoms of H is denoted by $\mathcal{A}(H)$.
- $x \in H$ is **idompotent** (or *an* idempotent) if $x^2 = x$.

The existing body of work on factorization theory contains several reasonable definitions of "associate" and "atom" which are not always equivalent. Here, we have chosen one such set of definitions; this choice has consequences on the definitions to be laid out in the remainder of this section, and on the nature of the results one may prove. Fortunately, previous entries in the literature have taken care to compare some of these alternative notions. Look to Section 2.4 for more a more detailed digression on different definitions of "associate" and "atom" and how they relate to one another.

Definition 2.1.2. Let H be a monoid and let $x, y \in H$. We say x **divides** y in H (written $x|_H y$, or $x|y$ if the monoid is clear from context) if there are $y, z \in H$ with $zxw = y$.

We will use the language of free monoids heavily throughout as a convenient way of precisely describing information about factorizations of elements. This method of bookkeeping is borrowed from [FT18], which is in turn based on the usage of free abelian monoids in [GHK06] and much of the subsequent literature on factorization theory as studied from the monoid point of view.

Definition 2.1.3. Let S be a set. The **free monoid** on S is the set

$$\mathcal{F}^*(S) := \{s_1 * \cdots * s_\ell : \ell \in \mathbb{N} \text{ and } s_i \in S \text{ for each } i \in [1, \ell]\}$$

of formal words whose letters belong to S. Its operation, denoted by $*$, is called *concatenation*.

Let $\mathfrak{s} = s_1 * \cdots * s_\ell \in \mathcal{F}^*(S)$, where each $s_i \in S$. The **length** of $\mathfrak{s}$ is $|\mathfrak{s}| := \ell$. (The empty word ε_S is said to have length zero).

The elements $s_1, \ldots, s_\ell$ are called the *factors* of $\mathfrak{s}$. A word $\mathfrak{t} \in \mathcal{F}^*(S)$ is said to be a **subword** of $\mathfrak{s}$ if there are $1 \leq i_1 < \cdots < i_k \leq \ell$ such that $\mathfrak{t} = s_{i_1} * \cdots * s_{i_k}$.

Definition 2.1.4. Let H be a monoid. The *factorization homomorphism* of H is the unique homomorphism $\pi_H : \mathcal{F}^*(H) \to H$ satisfying $\pi_H(x) = x$ for all $x \in H$.

The *factorization monoid* of H is the free monoid $\mathcal{F}^*(\mathcal{A}(H))$ generated by the atoms of H. Its elements are referred to as **factorizations**.

If $x \in H$ is a non-unit, then the **set of factorizations** of x is

$$\mathcal{Z}_H(x) := \{\mathfrak{a} \in \mathcal{F}^*(\mathcal{A}(H)) : \pi_H(\mathfrak{a}) = x\} = \mathcal{F}^*(\mathcal{A}(H)) \cap \pi_H^{-1}(x)$$

The subscript "H" may be omitted for brevity if the ambient monoid in which the factorization is being considered is clear from context.

For a non-empty word $\mathfrak{a} \in \mathcal{Z}_H(x)$, if we write $\mathfrak{a} = a_1 * \cdots * a_k$, the atoms a_i are said to be **factors** of x.

Definition 2.1.5. Let H be a monoid, $x \in H$ be a non-unit, and $\mathfrak{a}, \mathfrak{b} \in \mathcal{F}^*(\mathcal{A}(H))$. We will say that $\mathfrak{a}$ is **(H-)equivalent** to $\mathfrak{b}$ if, writing $\mathfrak{a} = a_1 * \cdots * a_k$ and $\mathfrak{b} = b_1 * \cdots * b_\ell$,

1. $k = \ell$.
2. The factors in $\mathfrak{b}$ are permuted associates of the factors of $\mathfrak{a}$; that is, there is a permutation $\sigma \in S_n$ (where S_n is the symmetric group on $[1, n]$) such that $b_i \simeq_H a_{\sigma(i)}$ for all $i \in [1, k]$.
3. $\mathfrak{a}$ and $\mathfrak{b}$ have the same product; i.e., $\pi_H(\mathfrak{a}) = \pi_H(\mathfrak{b})$.

In this case, we will write $\mathfrak{a} \simeq_H \mathfrak{b}$ (or just $\mathfrak{a} \simeq \mathfrak{b}$ if H is clear from context).

It is not difficult to check that $\simeq_H$ defined here is indeed an equivalence relation on $\mathcal{F}^*(\mathcal{A}(H))$. Note we are using the same notation for associates ($a \simeq_H b$) and for equivalence of factorizations ($\mathfrak{a} \simeq_H \mathfrak{b}$). This is suggestive of the close connection between the notions of associates and of factorization equivalence. Though they are not the same relation, context should make the meaning clear when each is being used.

Definition 2.1.6. Let H be a monoid and $x \in H \setminus H^\times$. The **set of factorization classes** of x is

$$\mathsf{Z}_H(x) := \{[\mathfrak{a}]_\simeq : \mathfrak{a} \in \mathcal{Z}_H(x)\} = \mathcal{Z}_H(x)/\simeq$$

and the **set of (factorization) lengths** of x is

$$\mathsf{L}_H(x) := \{|\mathfrak{a}| : [\mathfrak{a}]_\simeq \in \mathsf{Z}_H(x)\}.$$

Lastly, the **system of (sets of) lengths** of H is $\mathcal{L}(H) := \{\mathsf{L}_H(x) : x \in H \setminus H^\times\}$.

Definition 2.1.7. Let H be a monoid. Here we define some properties to measure the degree of uniqueness of factorization in H.

- H has **unique factorization (UF)** if, for all $x \in H \setminus H^\times$, $|\mathsf{Z}_H(x)| = 1$ (we may also say H is *factorial*).
- H is **half factorial (HF)** if, for all $x \in H \setminus H^\times$, $|\mathsf{L}_H(x)| = 1$.
- H has **finite factorization (FF)** if, for all $x \in H \setminus H^\times$, $|\mathsf{Z}_H(x)| < \infty$.
- H has **bounded factorization (BF)** if, for all $x \in H \setminus H^\times$, $|\mathsf{L}_H(x)| < \infty$.
- H is **atomic** if, for all $x \in H \setminus H^\times$, $\mathsf{Z}_H(x) \neq \emptyset$.

Proposition 2.1.8. We have the following logical implications among the properties defined just above:

$$\begin{tikzcd}
 & \text{HF} \arrow[dr, Rightarrow] & & \\
\text{UF} \arrow[ur, Rightarrow] \arrow[dr, Rightarrow] & & \text{BF} \arrow[r, Rightarrow] & \text{atomic} \\
 & \text{FF} \arrow[ur, Rightarrow] & &
\end{tikzcd}$$

2.2 Examples and Non-Examples

Here we will take a moment to examine the reversibility – or lack thereof – in the logical implications between the properties outlined in Proposition 2.1.8. We also remark on some well-studied classes of monoids which demonstrate some of those properties.

Example 2.2.1. $(\mathbb{Z} \setminus \{0\}, \cdot)$ is a unique factorization monoid (this is the Fundamental Theorem of Arithmetic).

Example 2.2.2. Let $\mathbb{P} \subseteq \mathbb{N}$ be the set of primes, and let $M = \langle \mathbb{P} \times \mathbb{P} \rangle$ be the monoid generated by pairs of primes under coordinatewise multiplication. Then, for any pair $(m, n) \in M$, it is clear that any factorization of (m, n) has length equal to the number of primes (counted with multiplicity) dividing m or n. However, this is not a UF monoid; we have, for instance, that $(2, 2)(3, 3)(2, 3) = (12, 18) = (2, 3)(2, 3)(3, 2)$.

Example 2.2.3. Most examples we will encounter from here onward will be FF, so it is perhaps more useful to see a non-example of an FF monoid. Let $R = \mathbb{R} + x\mathbb{C}[x]$ be the ring of polynomials with complex coefficients and real constant term. Then, for all nonzero $r \in \mathbb{R}$, we have

$$x^2 = ((r+i)x)\left(\frac{1}{r+i}\,x\right).$$

Since $r + i \notin \mathbb{R}$ for $r \neq 0$, $(r+i)x$ is a non-unit of R, so we have found infinitely many factorizations of x^2. However, any element of $R \setminus \{0\}$ has only finitely many factorization *lengths* by a degree argument. Thus the monoid $R \setminus \mathbb{Z}$ is BF but not FF.

Some of the richest factorization behavior is encountered in BF monoids. Since much of the discussion to come will center around power monoids which are BF, we will merely mention some other well-known classes of BF monoids.

Example 2.2.4. A *numerical monoid* or *numerical semigroup* is a submonoid $H \subsetneqq \mathbb{N}$ with finite complement. These exhibit a wide range of factorization behaviors and have been well studied in, among other works, [OP17, OP18, BOP17, GS18, CGH$^+$18]. We will encounter these in Section 5.4.

Example 2.2.5. Let G be a finite abelian group and let $\mathcal{B}(G)$ be the submonoid of the free monoid on G consisting of zequences whose sum is equal to 0 in G, called the *block monoid of* G or the *monoid of zero-sum sequences over* G. The interest in these monoids can be traced back to the study of the class group of a Dedekind domain (usually a ring of integers of a number field). They have been studied in some form or another since the late 1960s. The broad problems centered around zero-sum sequences are well-formulated in [GG06] and [GHK06]. More recent works with varying perspectives on the subject include [GLPW18, SC17, GS19, GS20].

Example 2.2.6. Let D be a domain with field of fractions K; then $\operatorname{Int}(D) := \{f(x) \in K[x] : f(D) \subseteq D\}$ is the ring of *integer-valued polynomials* of D which, of course, is well-discussed in [CC97]. In addition to the rich theory developed – in, for instance, [Lop97a],[Lop97b], or [CLS02] – around understanding the prime ideal structure of this ring, it is amenable to the study of factorization behavior, and exhibits some surprising behaviors. For example, any finite subset of $\mathbb{N}_{\geq 2}$ can be realized as the set of factorization lengths of some polynomial $f(x) \in \operatorname{Int}(D)$ whenever D is a Dedekind domain with infinitely many maximal ideals of finite index [FNR19, Fri13].

Example 2.2.7. Since we will usually be looking at atomic monoids, we offer a non-example here; consider the set $Q = \mathbb{Q}_{\geq 0}$ of non-negative rational numbers under addition. Q is reduced (its only unit is the identity, 0) and we have, for any non-zero element $x \in Q$, that $x = \frac{x}{2} + \frac{x}{2}$. This is a decomposition of x into two non-zero (hence non-unit) elements, so x is not an atom. Thus we learn that Q not only fails to have factorizations into atoms, but also to have atoms at all.

2.3 Monoid and Equimorphism Basics

Here we will define and examine some properties that pertain to monoids in general, as well as some notions which will help us understand the relationships between certain monoids.

Definition 2.3.1. Let H be a monoid. For any $x \in H$, let $\langle x \rangle_H := \{x^k : k \in \mathbb{N}_{>0}\}$ denote the *subsemigroup generated by* x in H. Then we define the **order** of x in H to be $\mathrm{ord}_H(x) := |\langle x \rangle_H|$ (we may drop the subscript H when the monoid is clear from context).

H is said to be

- **torsion** if, for all $x \in H$, $\mathrm{ord}_H(x) < \infty$;
- **non-torsion** if there exists $x \in H$ with $\mathrm{ord}_H(x) = \infty$;
- **torsion-free** if, for all $x \in H$, $\mathrm{ord}_H(x) = \infty$.

Note that, in the case when H is a group, $\langle x \rangle_H$ is the cyclic subgroup generated by x in H, and $\mathrm{ord}_H(x)$ therefore corresponds to the familiar sense of “order” from group theory.

Definition 2.3.2. Let H be a monoid and let $x, y, z \in H$. H is

- **reduced** if $H^\times = \{1\}$ is trivial;
- **cancellative** if $xz = yz$ or $zx = zy$ implies that $x = y$;
- **unit cancellative** if $xy = x$ or $yx = x$ implies that $y \in H^\times$;
- **Dedekind-finite** if $xy = 1$ implies that $yx = 1$ (i.e., one-sided inverses are actually two-sided).

The condition of Dedekind-finiteness will play a very important role in the remainder of this chapter. This is a very mild condition which one may almost expect of a “typical” monoid (we have cancellative ⇒ unit-cancellative ⇒ Dedekind-finite). Example 3.1.4 includes a monoid which is *not* Dedekind-finite.

Proposition 2.3.3. Let H be a monoid. The following hold:

(i) If $u, v \in H^\times$ then $uv \in H^\times$, and the converse holds whenever H is Dedekind-finite.

(ii) If $\mathcal{A}(H)$ is non-empty or H is commutative or unit-cancellative, then H is Dedekind-finite.

(iii) If $a \in \mathcal{A}(H)$ and $u, v \in H^\times$, then $uav \in \mathcal{A}(H)$.

(iv) If $x \in H \setminus H^\times$ and $u, v \in H^\times$, then $\mathsf{L}_H(uxv) = \mathsf{L}_H(x)$.

Proof. See [FT18, parts (i), (ii), and (iv) of Lemma 2.2, and Proposition 2.30]. □

Definition 2.3.4. Let H be a monoid with a submonoid M. M is **divisor closed** in H if, whenever $y \in M$ and $x|_H y$, we have $x \in M$.

Divisor closedness can help us gain a partial understanding of a monoid’s factorization behavior by way of examining submonoids. This strategy is made more precise by the following result, which is borrowed from [FT18, Proposition 2.21].

Proposition 2.3.5. Let H be monoid with a divisor-closed submonoid M. Then

(i) $M^\times = H^\times$;
(ii) $\mathcal{A}(M) = \mathcal{A}(H) \cap M$;
(iii) For all $x \in M \setminus M^\times$, $\mathsf{Z}_M(x) = \mathsf{Z}_H(x)$;
(iv) For all $x \in M \setminus M^\times$, $\mathsf{L}_M(x) = \mathsf{L}_H(x)$;
(v) $\mathcal{L}(M) \subseteq \mathcal{L}(H)$.

Proof. See the proof of [FT18, Proposition 2.21]. □

Now we will borrow from [Tri19, Definition 3.2] notion of an *equimorphism*, which formally packages the idea that, under suitable conditions, arithmetic may be transferred from one monoid to another.

Definition 2.3.6. Let H and K be monoids, and $\varphi : H \to K$ a monoid homomorphism. We denote by $\varphi^* : \mathcal{F}^*(H) \to \mathcal{F}^*(K)$ the (unique) monoid homomorphism such that $\varphi^*(x) = \varphi(x)$ for every $x \in H$, and we call φ an **equimorphism** if the following hold:

(E1) $\varphi^{-1}(K^\times) \subseteq H^\times$;
(E2) φ is **atom-preserving**, meaning that $\varphi(\mathcal{A}(H)) \subseteq \mathcal{A}(K)$;
(E3) If $x \in H$ and $\mathfrak{b} \in \mathcal{Z}_K(\varphi(x))$ is a non-empty $\mathcal{A}(K)$-word, then $\varphi^*(\mathfrak{a}) \in [\mathfrak{b}]_{\simeq_K}$ for some $\mathfrak{a} \in \mathcal{Z}_H(x)$.

Moreover, we say that φ is **essentially surjective** if $K = K^\times \varphi(H) K^\times$.

Proposition 2.3.7. Let H and K be monoids and $\varphi : H \to K$ an equimorphism. The following hold:

(i) $\mathsf{L}_H(x) = \mathsf{L}_K(\varphi(x))$ for all $x \in H \setminus H^\times$.
(ii) If φ is essentially surjective, then for all $y \in K \setminus K^\times$ there is $x \in H \setminus H^\times$ with $\mathsf{L}_K(y) = \mathsf{L}_H(x)$.

Proof. See [FT18, Theorem 2.22(i)] and [Tri19, Theorem 3.3(i)]. □

2.4 Literature and Comparing Alternate Definitions

Our approach to factorization in possibly non-cancellative or non-commutative monoids is borrowed from [FT18], where one can read thoroughly about differences and similarities with the classical approach to factorization in commutative and cancellative monoids (and hence in integral domains) pursued by A. Geroldinger and F. Halter-Koch in [GHK06], and with the much more recent approach to factorization in cancellative but possibly non-commutative monoids set forth by N.R. Baeth and D. Smertnig in [BS15]; in particular, see [FT18, Remarks 2.6 and 2.7].

This said, there are many previous entries in the literature that have treated (mainly algebraic) aspects of factorization theory in commutative (unital) rings with non-trivial zero divisors. Most notably, D.D. Anderson and collaborators have extensively studied factorizations in commutative rings corresponding to notions of “associate” and “irreducible” other than the ones adopted in the present paper, see e.g. [AAM85, AM85, AVL96, AVL97, AAVL01, AC11, CAVL11]. Below we review these alternative definitions and contrast them with our approach.

To start with, let R be a commutative ring and denote by $R^\times$ the group of units of the multiplicative monoid of R. Given $x, y \in R$, we say in the parlance of [AVL96, Definition 2.1] that

- x is *associate* to y (in R), written $x \sim_R y$, if $xR = yR$;
- x is *strongly associate* to y, written $x \approx_R y$, if $x \in yR^\times$ (by Proposition 2.3.3(i), this is equivalent to x being associate (as per Definition 2.1.1) to y in the multiplicative monoid of R);
- x is *very strongly associate* to y, written $x \cong_R y$, if $x \sim_R y$ and one of the following holds:
  (i) $x = y = 0_R$ (where 0_R is the zero of R);
  (ii) $x \ne 0_R$ and if $x = yz$ for some $z \in R$ then $z \in R^\times$.

Accordingly, one has three notions of "irreducible", see [AVL96, Definition 2.4]. To wit, an element $a \in R$ is

- *irreducible* if $a \notin R^\times$ and $a = xy$ for some $x, y \in R$ implies that $a \sim_R x$ or $a \sim_R y$;
- *strongly irreducible* if $a \notin R^\times$ and $a = xy$ for some $x, y \in R$ implies that $a \approx_R x$ or $a \approx_R y$;
- *very strongly irreducible* if $a \notin R^\times$ and $a = xy$ for some $x, y \in R$ implies that $a \cong_R x$ or $a \cong_R y$.

It is obvious that very strongly irreducible elements of R are strongly irreducible, and strongly irreducible elements are irreducible. In general, none of these implications can be reversed, see the paragraph after the proof of Theorem 2.12 in [AVL96]. However, we get by [AVL96, Theorem 2.2(3)] that the three notions coincide when R is *présimplifiable* in the sense of [Bou74a], meaning that if $xy = x$ for some $x, y \in R$ then $x = 0_R$ or $y \in R^\times$ (e.g., this is the case when R is an integral domain). Moreover, [AVL96, Theorem 2.5] yields that a *non-zero* element of R is strongly irreducible if and only if it is an atom of the multiplicative monoid of R.

Putting it all together, we thus see that the ring R is *very strongly atomic* in the sense of [AVL96, Definition 3.1] if and only if one of the following holds:

(A1) R has non-trivial zero divisors and the multiplicative monoid of R is atomic (as per Section 2.1);

(A2) R is an integral domain and $R \setminus \{0_R\}$ is an atomic monoid under multiplication.

Similarly, R is a *bounded factorization ring* in the sense of [AVL96, Definition 3.8], a *half-factorial ring* in the sense of [AFRS03, p. 87], a *finite factorization ring* in the sense of [AVL96, Definition 6.5], or a unique factorization ring in the sense of [AVL96, Definition 4.3] if and only if one of conditions (A1) and (A2) in the above is satisfied with "atomic" replaced, respectively, by "BF", "HF", "FF", or "factorial".

As long as the scope is restricted to commutative rings, it is therefore possible to compare our approach to factorization with others based on irreducibles, strong irreducibles, or even alternative "elementary factors" (including the ones considered by C.R. Fletcher [Fle69], A. Bouvier [Bou74a, Bou74b], and S. Galovich [Gal78]) by referring to [AVL96, CAVL11], where these comparisons are worked out in great detail. (Incidentally, it appears that Galovich is *tacitly* assuming "irreducibles" in the sense of [Gal78] to be non-units.) See also [BBM17, Theorem 3.4 and Corollary 3.5] for a couple of results of a more arithmetic flavor concerning lengths of factorizations into irreducibles in commutative rings of the form D/xD, where D is a principal ideal domain and x is a non-zero, non-unit element of D.

Chapter 3

Power Monoids and Atomicity

Here we embark on the study of the (arithmetic and algebraic) structure of power monoids. These objects were first introduced and studied by Y. Fan and S. Tringali in [FT18]. They encode a very natural combinatorial construction: the collection of finite subsets of a monoid. Historically, combinatorial thinkers have been concerned primarily with subsets of abelian groups, or even just cycic groups. Throughout the remainder of this work, we will see that the prior concentration of the literature on the case of abelian groups has been well-founded: this is a very tractible and robust area of research, with many questions which are yet unanswered. However, we will also see that the phenomena which occur in subsets of more general monoids present vast challenges of their own, and are certainly deserving of attention.

3.1 Subset Arithmetic

Definition 3.1.1. Let $(H, \cdot)$ be a monoid. We define an operation (called *setwise* $\cdot$) by, for any subsets $X, Y \subseteq H$,

$$X \cdot Y := \{x \cdot y : x \in X \text{ and } y \in Y\}$$

(as before, we will usually drop the "$\cdot$" and simply write XY for $X \cdot Y$). With this operation, the following collections of subsets of H become monoids:

- The *power monoid* of H is $\mathcal{P}_{\text{fin}}(H) := \{X \subseteq H : X \neq \emptyset \text{ and } |X| < \infty\}$;
- The *restricted power monoid* of H is $\mathcal{P}_{\text{fin},\times}(H) := \{X \subseteq H : X \cap H^\times \neq \emptyset \text{ and } |X| < \infty\}$;
- The *reduced power monoid* of H is $\mathcal{P}_{\text{fin},1}(H) := \{X \subseteq H : 1_H \in X \text{ and } |X| < \infty\}$.

We may refer to H as the *ground monoid* of any of these power monoids.

We proceed first with some elementary but helpful observations we will often use without comment.

Proposition 3.1.2. Let H be a monoid. The following hold:

(i) If $X_1, \ldots, X_n \in \mathcal{P}_{\text{fin},1}(H)$, then $X_1 \cup \cdots \cup X_n \subseteq X_1 \cdots X_n$.

(ii) If $u, v \in H^\times$ and $X_1, \ldots, X_n \in \mathcal{P}_{\text{fin},\times}(H)$, then $|uX_1 \cdots X_n v| = |X_1 \cdots X_n| \geq \max_{1 \leq i \leq n} |X_i|$.

(iii) If K is a submonoid of H, then $\mathcal{P}_{\text{fin},1}(K)$ is a divisor-closed submonoid of $\mathcal{P}_{\text{fin},1}(H)$. (Note that the conclusion is valid regardless of whether K itself is divisor-closed.)

(iv) $\mathcal{P}_{\text{fin},1}(H)$ is a reduced monoid and $\mathcal{P}_{\text{fin}}(H)^\times = \mathcal{P}_{\text{fin},\times}(H)^\times = \big\{\{u\} : u \in H^\times\big\}$.

(v) $\mathcal{A}(\mathcal{P}_{\text{fin},\times}(H)) \subseteq H^\times \mathcal{A}(\mathcal{P}_{\text{fin},1}(H)) H^\times$.

Proof. (i) is trivial, upon considering that $(X \cdot 1_H) \cup (1_H \cdot Y) \subseteq XY$ for all $X, Y \in \mathcal{P}_{\text{fin},1}(H)$; (ii) is a direct consequence of (i) and the fact that the function $X \to H : x \mapsto uxv$ is injective for all $u, v \in H^\times$ and $X \subseteq H$; and (iii) and (iv) are immediate from (i) and (ii).

As for (v), let $A \in \mathcal{A}(\mathcal{P}_{\text{fin},\times}(H))$. Because A contains a unit of H, there is $u \in H^\times$ such that $1_H \in uA$. Then uA is an element of $\mathcal{P}_{\text{fin},1}(H)$, and by Proposition 2.3.3(iii) it is also an atom of $\mathcal{P}_{\text{fin},\times}(H)$. Thus, if $X, Y \in \mathcal{P}_{\text{fin},1}(H) \subseteq \mathcal{P}_{\text{fin},\times}(H)$ and $uA = XY$, then X or Y is the identity of $\mathcal{P}_{\text{fin},1}(H)$. This means that uA is an atom of $\mathcal{P}_{\text{fin},1}(H)$, and hence $A = u^{-1}(uA) \in H^\times \mathcal{A}(\mathcal{P}_{\text{fin},1}(H))$, as wished. □

Our ultimate goal is, for an arbitrary monoid H, to investigate factorizations in $\mathcal{P}_{\text{fin}}(H)$. However, this is a difficult task in general, due to a variety of "pathological situations" that might be hard to classify in a satisfactory way, see e.g. [FT18, Remark 3.3(ii)].

In practice, it is more convenient to start with $\mathcal{P}_{\text{fin},1}(H)$ and then lift arithmetic results from $\mathcal{P}_{\text{fin},1}(H)$ to $\mathcal{P}_{\text{fin},\times}(H)$, a point of view which is corroborated by the simple consideration that $\mathcal{P}_{\text{fin}}(H) = \mathcal{P}_{\text{fin},\times}(H)$ whenever H is a group (i.e., in the case of greatest interest in Arithmetic Combinatorics).

In turn, we will see that studying the arithmetic of $\mathcal{P}_{\text{fin},\times}(H)$ is tantamount to studying that of $\mathcal{P}_{\text{fin},1}(H)$, in a sense to be made precise presently.

Proposition 3.1.3. Let H be a Dedekind-finite monoid. The following hold:

(i) The natural embedding $\jmath : \mathcal{P}_{\text{fin},1}(H) \hookrightarrow \mathcal{P}_{\text{fin},\times}(H)$ is an essentially surjective equimorphism.

(ii) $\mathcal{A}(\mathcal{P}_{\text{fin},\times}(H)) = H^\times \mathcal{A}(\mathcal{P}_{\text{fin},1}(H)) H^\times$.

(iii) $\mathsf{L}_{\mathcal{P}_{\text{fin},1}(H)}(X) = \mathsf{L}_{\mathcal{P}_{\text{fin},\times}(H)}(X)$ for every $X \in \mathcal{P}_{\text{fin},1}(H)$.

(iv) $\mathcal{L}(\mathcal{P}_{\text{fin},\times}(H)) = \mathcal{L}(\mathcal{P}_{\text{fin},1}(H))$.

Proof. In view of Proposition 2.3.7, parts (iii) and (iv) are immediate from (i). Moreover, the inclusion from left to right in (ii) is precisely the content of Proposition 3.1.2(v), and the other inclusion will follow from (i) and Propositions 2.3.3(iii) and 3.1.2(iv). Therefore, we focus on (i) for the remainder of the proof.

(i) By Proposition 3.1.2(iv), $\jmath$ satisfies (E1). Moreover, $\jmath$ is essentially surjective, as any $X \in \mathcal{P}_{\text{fin},\times}(H)$ contains a unit $u \in H^\times$, so $u^{-1}X \in \mathcal{P}_{\text{fin},1}(H)$ and $X = u(u^{-1}X)$ is associate to an element of $\mathcal{P}_{\text{fin},1}(H)$.

To prove (E2), let $A \in \mathcal{A}(\mathcal{P}_{\text{fin},1}(H))$. We aim to show that A is an atom of $\mathcal{P}_{\text{fin},\times}(H)$. Suppose that $A = XY$ for some $X, Y \in \mathcal{P}_{\text{fin},\times}(H)$. Then there are $x \in X$ and $y \in Y$ with $xy = 1_H$; and using that H is Dedekind-finite, we get from Proposition 2.3.3(i) that $x, y \in H^\times$. It follows that

$$A = XY = (Xx^{-1})(xY) \quad \text{and} \quad Xx^{-1}, xY \in \mathcal{P}_{\text{fin},1}(H).$$

But then $Xx^{-1} = \{1_H\}$ or $xY = \{1_H\}$, since $\mathcal{P}_{\text{fin},1}(H)$ is a reduced monoid and A is an atom of $\mathcal{P}_{\text{fin},1}(H)$. So, X or Y is a 1-element subset of $H^\times$, and hence $A \in \mathcal{A}(\mathcal{P}_{\text{fin},\times}(H))$.

It remains to show that $\jmath$ satisfies (E3). Pick $X \in \mathcal{P}_{\text{fin},1}(H)$. If $X = \{1_H\}$, the conclusion holds vacuously. Otherwise, let $\mathfrak{b} := B_1 * \cdots * B_n \in \mathcal{Z}_{\mathcal{P}_{\text{fin},1}(H)}(X)$. Then there are $u_1 \in B_1, \ldots, u_n \in B_n$ such that $1_H = u_1 \cdots u_n$; and as in the proof of (E2), it must be that $u_1, \ldots, u_n \in H^\times$. Accordingly, we take, for every $i \in [1, n]$, $A_i := u_0 \cdots u_{i-1} B_i u_i^{-1} \cdots u_1^{-1}$, where $u_0 := 1_H$. Then

$$A_1 \cdots A_n = X \quad \text{and} \quad 1_H \in A_1 \cap \cdots \cap A_n;$$

and by Propositions 2.3.3(iii) and 3.1.2(v), $A_1, \ldots, A_n$ are atoms of $\mathcal{P}_{\text{fin},1}(H)$. This shows that $\mathfrak{a} := A_1 * \cdots * A_n \in \mathcal{Z}_{\mathcal{P}_{\text{fin},1}(H)}(X)$. Since $A_i \simeq_{\mathcal{P}_{\text{fin},\times}(H)} B_i$ for each $i \in [1, n]$ (by construction), we thus conclude that $\mathfrak{a}$ is $\mathcal{P}_{\text{fin},\times}(H)$-equivalent to $\mathfrak{b}$, as wished. □

The next example proves that Dedekind-finiteness is, to some extent, necessary for Proposition 3.1.3(ii), and hence for the subsequent conclusions.

Example 3.1.4. Let $\mathcal{B}$ be the set of all binary sequences $\mathfrak{s} : \mathbb{N}_{\ge 1} \to \{0, 1\}$, and let H denote the monoid of all functions $\mathcal{B} \to \mathcal{B}$ under composition. We will write H multiplicatively; so, if $f, g \in H$ then fg is the map $\mathcal{B} \to \mathcal{B} : \mathfrak{s} \mapsto f(g(\mathfrak{s}))$. Further, let $n \ge 5$ and consider the functions

$$\begin{aligned}
&L : \mathcal{B} \to \mathcal{B} : (a_1, a_2, \ldots) \mapsto (a_2, a_3, \ldots) && \text{(left shift);}\\
&R : \mathcal{B} \to \mathcal{B} : (a_1, a_2, \ldots) \mapsto (0, a_1, a_2, \ldots) && \text{(right shift);}\\
&P : \mathcal{B} \to \mathcal{B} : (a_1, a_2, \ldots) \mapsto (a_n, a_1, \ldots, a_{n-1}, a_{n+1}, a_{n+2}, \ldots) && \text{(cycle the first } n \text{ terms).}
\end{aligned}$$

In particular, $P \in H^\times$. Also, $LR = \mathrm{id}_\mathcal{B}$ but $RL \ne \mathrm{id}_\mathcal{B}$; whence H is not Dedekind-finite, and neither R nor L is invertible. With this in mind, we will prove that $A := \{L, P\} \cdot \{R, P\} = \{\mathrm{id}_\mathcal{B}, LP, PR, P^2\}$ is an atom of $\mathcal{P}_{\text{fin},1}(H)$, although it is not, by construction, an atom of $\mathcal{P}_{\text{fin},\times}(H)$.

Indeed, assume $A = XY$ for some $X, Y \in \mathcal{P}_{\text{fin},1}(H)$. Then $X, Y \subseteq A$, and it is clear that $P^2 \ne PRLP$, or else $RL = \mathrm{id}_\mathcal{B}$ (a contradiction). Similarly, $PRPR \ne P^2 \ne LPLP$; otherwise, $P = RPR$ and hence R is invertible, or $P = LPL$ and L is invertible (again a contradiction). Lastly, we see that $P^2 \ne LP^2R$, by applying both P^2 and LP^2R to the constant sequence $(1, 1, \ldots)$.

It follows that P^2 must belong to X or Y, but not to both (which is the reason for choosing $n \ge 5$). Accordingly, let $P^2 \in X \setminus Y$ (the other case is analogous). Then $Y = \{\mathrm{id}_\mathcal{B}\}$, since one can easily check that $P^2LP, P^3R \notin A$, by noting that the action of P^2LP and P^3R differ from that of A on the sequences $(1, 1, \ldots)$ and $(1, 0, 1, 1, \ldots)$. This makes A an atom of $\mathcal{P}_{\text{fin},1}(H)$.

3.2 Atomicity and Bounded Factorization in Power Monoids

We get from Proposition 3.1.3 that studying factorization properties of $\mathcal{P}_{\text{fin},1}(H)$ is sufficient for studying corresponding properties of $\mathcal{P}_{\text{fin},\times}(H)$, at least in the case when H is Dedekind-finite. Thus, as a starting point in the investigation of the arithmetic of $\mathcal{P}_{\text{fin},1}(H)$, one might wish to give a comprehensive description of the atoms of $\mathcal{P}_{\text{fin},1}(H)$. This is however an overwhelming task even in specific cases (e.g., when H is the additive group of the integers), let alone the general case. Nevertheless, we can obtain basic information about $\mathcal{A}(\mathcal{P}_{\text{fin},1}(H))$ in full generality.

Lemma 3.2.1. Let H be a monoid and $x \in H \setminus \{1_H\}$. The following hold:

(i) The set $\{1_H, x\}$ is an atom of $\mathcal{P}_{\text{fin},1}(H)$ if and only if $1_H \neq x^2 \neq x$.

(ii) If $x^2 = 1_H$ or $x^2 = x$, then $\{1_H, x\}$ factors into a product of atoms neither in $\mathcal{P}_{\text{fin},1}(H)$ nor in $\mathcal{P}_{\text{fin},\times}(H)$.

Proof. (i) If $x^2 = 1_H$ or $x^2 = x$, then it is clear that $\{1_H, x\} = \{1_H, x\}^2$, and therefore $\{1_H, x\}$ is not an atom of $\mathcal{P}_{\text{fin},1}(H)$. As for the converse, assume that $\{1_H, x\} = YZ$ for some non-units $Y, Z \in \mathcal{P}_{\text{fin},1}(H)$. Then we get from Proposition 3.1.2 that Y and Z are 2-element sets, namely, $Y = \{1_H, y\}$ and $Z = \{1_H, z\}$ with $y, z \in H \setminus \{1_H\}$. Hence $\{1_H, x\} = YZ = \{1_H, y, z, yz\}$, and immediately this implies $x = y = z$. Therefore, $\{1_H, x\} = \{1_H, x, x^2\}$, which is only possible if $x^2 = 1_H$ or $x^2 = x$.

(ii) Suppose that $x^2 = 1_H$ or $x^2 = x$. Then the calculation above shows that $\{1_H, x\} = \{1_H, x\}^2$ and there is no other decomposition of $\{1_H, x\}$ into a product of non-unit elements of $\mathcal{P}_{\text{fin},1}(H)$. So, $\{1_H, x\}$ is a non-trivial idempotent (hence, a non-unit) and has no factorization into atoms of $\mathcal{P}_{\text{fin},1}(H)$.

It remains to prove the analogous statement for $\mathcal{P}_{\text{fin},\times}(H)$. Assume to the contrary that $\{1_H, x\}$ factors into a product of n atoms of $\mathcal{P}_{\text{fin},\times}(H)$ for some $n \in \mathbb{N}_{>0}$. Then $n \geq 2$, since $\{1_H, x\}$ is a non-trivial idempotent (and hence not an atom itself). Consequently, we can write $\{1_H, x\} = YZ$, where Y is an atom and Z a non-unit of $\mathcal{P}_{\text{fin},\times}(H)$. In particular, we get from parts (i), (ii), and (iv) of Proposition 3.1.2 that both Y and Z are 2-element sets, say, $Y = \{u, y\}$ and $Z = \{v, z\}$. It is then immediate that there are only two possibilities: 1_H is the product of two units from Y and Z, or the product of two non-units from Y and Z. Without loss of generality, we are thus reduced to considering the following cases.

Case 1: $uv = 1_H$. Then $uz \neq 1_H$ (or else $z = u^{-1} = v$, contradicting the fact that Z is a 2-element set). So $uz = x$, and similarly $yv = x$. Then $y = xu = uzu$ and $z = xv = vyv$, and therefore

$$\{u, y\} = \{u, uzu\} = \{1_H, uz\} \cdot \{u\} = \{1_H, x\} \cdot \{u\} = \{u, y\} \cdot \{vu, zu\}$$

However, this shows that $\{u, y\}$ is not an atom of $\mathcal{P}_{\text{fin},\times}(H)$, in contrast with our assumptions.

Case 2: $yz = 1_H$ and $y, z \in H \setminus H^\times$. Then $u, v \in H^\times$, by the fact that $\{u, y\}, \{v, z\} \in \mathcal{P}_{\text{fin},\times}(H)$; and we must have $uz = x$, for $uz = 1_H$ would yield $z = u^{-1} \in H^\times$. In particular, $x = uz$ is not a unit in H, so $uv = 1_H$ and we are back to the previous case. □

We have just seen that, to even *hope* for $\mathcal{P}_{\mathrm{fin},1}(H)$ to be atomic, we must have that the "bottom layer" of 2-element subsets of H consists only of atoms, and it will turn out that such a condition is also sufficient. Before proving this, it seems appropriate to point out some structural implications of the fact that every non-identity element of H is neither an idempotent nor a square root of 1_H.

Lemma 3.2.2. Let H be a monoid such that $1_H \neq x^2 \neq x$ for all $x \in H \setminus \{1_H\}$. The following hold:

(i) H is Dedekind-finite.

(ii) If $x \in H$ and $\langle x \rangle_H$ is finite, then $x \in H^\times$ and $\langle x \rangle_H$ is a cyclic group of order ≥ 3.

Proof. (i) Let $y, z \in H$ such that $yz = 1_H$. Then $(zy)^2 = z(yz)y = zy$, and since H has no non-trivial idempotents, we conclude that $zy = 1_H$. Consequently, H is Dedekind-finite.

(ii) This is an obvious consequence of [Whi88, Ch. V, Exercise 4, p. 68], according to which every finite semigroup has an idempotent. The proof is short, so we give it here for the sake of self-containedness.

Because $\langle x \rangle_H$ is finite, there exist $n, k \in \mathbb{N}_{>0}$ such that $x^n = x^{n+k}$, and by induction this implies that $x^n = x^{n+hk}$ for all $h \in \mathbb{N}$. Therefore, we find that

$$(x^{nk})^2 = x^{2nk} = x^{(k+1)n} x^{(k-1)n} = x^n x^{(k-1)n} = x^{nk}.$$

But H has no non-trivial idempotents, thus it must be the case that $x^{nk} = 1_H$. That is, x is a unit of H, and we have $x^{-1} = x^{nk-1} \in \langle x \rangle_H$. So, $\langle x \rangle_H$ is a (finite) cyclic group of order ≥ 3. □

Theorem 3.2.3. Let H be a monoid. Then $\mathcal{P}_{\mathrm{fin},1}(H)$ is atomic if and only if $1_H \neq x^2 \neq x$ for every $x \in H \setminus \{1_H\}$.

Proof. The "only if" part is a consequence of Lemma 3.2.1(ii). As for the other direction, assume that $1_H \neq x^2 \neq x$ for each $x \in H \setminus \{1_H\}$, and fix $X \in \mathcal{P}_{\mathrm{fin},1}(H)$ with $|X| \geq 2$. We wish to show that

$$X = A_1 \cdots A_n, \quad \text{for some } A_1, \ldots, A_n \in \mathcal{A}(\mathcal{P}_{\mathrm{fin},1}(H)).$$

If X is a 2-element set, the claim is true by Lemma 3.2.1(i). So let $|X| \geq 3$, and suppose inductively that every $Y \in \mathcal{P}_{\mathrm{fin},1}(H)$ with $2 \leq |Y| < |X|$ is a product of atoms. If X is an atom, we are done. Otherwise, $X = AB$ for some non-units $A, B \in \mathcal{P}_{\mathrm{fin},1}(H)$, and by symmetry we can assume $|X| \geq |A| \geq |B| \geq 2$.

If $|A| < |X|$, then both A and B factor into a product of atoms (by the inductive hypothesis), and so too does $X = AB$. Consequently, we are only left to consider the case when $|X| = |A|$.

For, we notice that $A \cup B \subseteq AB = X$ (because $1_H \in A \cap B$), and this is only possible if $A = X$ (since $|A| = |X|$ and $A \subseteq X$). So, to summarize, we have that

$$|X| \geq 3, \quad |B| \geq 2, \quad \text{and} \quad B \subseteq AB = X = A. \tag{3.1}$$

In particular, since B is not a unit of $\mathcal{P}_{\text{fin},1}(H)$, we can choose an element $b \in B \setminus \{1_H\} \subseteq A$. Hence, taking $A_b := A \setminus \{b\}$, we have $|A_b| < |A|$, and it is easy to check that $A_b B = A = X$ (in fact, 1_H is in $A_b \cap B$, and therefore we derive from (3.1) that $A_b B \subseteq A = A_b \cup \{b\} \subseteq A_b B \cup \{b\} \subseteq A_b B \cup B = A_b B$).

If $|B| < |A|$, then we are done, because A_b and B are both products of atoms (by the inductive hypothesis), and thus so is $X = AB = A_b B$. Otherwise, it follows from (3.1) and the above that

$$X = A = B = A_b B \quad \text{and} \quad |A| \geq 3, \tag{3.2}$$

so we can choose an element $a \in A \setminus \{1_H, b\}$. Accordingly, set $B_a := B \setminus \{a\}$. Then $|B_a| < |B|$ (because $A = B$ and $a \in A$), and both A_b and B_a decompose into a product of atoms (again by induction). But this finishes the proof, since it is straightforward from (3.2) that $X = A = A_b B_a$ (indeed, $1_H \in A_b \cap B_a$ and $b \in B_a$, so we find that $A_b B_b \subseteq A = A_b \cup \{b\} \subseteq A_b B_a \cup \{b\} \subseteq A_b B_a \cup B_a = A_b B_a$). □

Now with Proposition 2.3.7 and Theorem 3.2.3 in hand, we can engage in a finer study of the arithmetic of Power monoids; in particular, we may wish to study their (systems of) sets of lengths. However, we are immediately met with a "problem" (i.e., some sets of lengths are infinite in a rather trivial way):

Example 3.2.4. Let H be a monoid with an element x of finite odd order $m \geq 3$, and set $X := \{x^k : k \in \mathbb{N}\}$. Then it is clear that X is the setwise product of n copies of $\{1_H, x\}$ for every $n \geq m$. This shows that the set of lengths of X relative to $\mathcal{P}_{\text{fin},1}(H)$ contains $[m, \infty]$ (and hence is infinite), since we know from Lemma 3.2.1 that $\{1_H, x\}$ is an atom of $\mathcal{P}_{\text{fin},1}(H)$.

The nature of this problem is better clarified by our next result, and we will more thoroughly address it in Section 4.1.

Theorem 3.2.5. Let H be a monoid. The following hold:

(i) If H is torsion-free and $X \in \mathcal{P}_{\text{fin},1}(H)$, then $\sup \mathsf{L}_{\mathcal{P}_{\text{fin},1}(H)}(X) \leq |X|^2 - |X|$.
(ii) $\mathcal{P}_{\text{fin},1}(H)$ is BF if and only if H is torsion-free.
(iii) $\mathcal{P}_{\text{fin},\times}(H)$ is BF if and only if so is $\mathcal{P}_{\text{fin},1}(H)$.

Proof. (i) Set $n := |X| \in \mathbb{N}_{>0}$, fix an integer $\ell \geq (n-1)n + 1$, and suppose for a contradiction that $X = A_1 \cdots A_\ell$ for some $A_1, \ldots, A_\ell \in \mathcal{A}(\mathcal{P}_{\text{fin},1}(H))$. By the Pigeonhole Principle, there are an element $x \in X$ and a subset $I \subseteq [1, \ell]$ such that $m := |I| \geq n$ and $x \in A_i$ for each $i \in I$. So, writing $I = \{i_1, \ldots, i_m\}$, we find that $x^k \in A_{i_1} \cdots A_{i_k} \subseteq A_1 \cdots A_\ell = X$ for every $k \in [1, m]$, i.e., $\{1_H, x, \ldots, x^m\} \subseteq X$. However, since H is torsion-free, each power of x is distinct, and hence $n = |X| \geq m + 1 > n$ (a contradiction).

(ii) First suppose for a contradiction that $\mathcal{P}_{\text{fin},1}(H)$ is BF and has an element x of finite order m. Then $\mathcal{P}_{\text{fin},1}(H)$ is also atomic, and we know by Theorem 3.2.3 and Lemma 3.2.2(ii) that $x^m = 1_H$. If m is even, then $(x^{m/2})^2 = 1_H$, contradicting the atomicity of $\mathcal{P}_{\text{fin},1}(H)$ since, by Theorem 3.2.3, no non-identity element of H can have order 2. If m is odd, then Example 3.2.4 shows that the set of lengths of $\{x^k : k \in \mathbb{N}\}$ is infinite, contradicting the assumption that $\mathcal{P}_{\text{fin},1}(H)$ is BF.

Conversely, assume H is torsion-free. Then all powers of non-identity elements are distinct, so Theorem 3.2.3 implies that $\mathcal{P}_{\text{fin},1}(H)$ is atomic, and (i) gives an explicit upper bound on the lengths of factorizations.

(iii) The "only if" part follows from [FT18, Theorem 2.28(iv) and Corollary 2.29], so suppose that $\mathcal{P}_{\text{fin},1}(H)$ is BF. Then $\mathcal{P}_{\text{fin},1}(H)$ is atomic, and hence, by Theorem 3.2.3, $1_H \neq x^2 \neq x$ for all $x \in H \setminus \{1_H\}$. By Lemma 3.2.2(i), this implies that H is Dedekind-finite, so the natural embedding $\mathcal{P}_{\text{fin},1}(H) \hookrightarrow \mathcal{P}_{\text{fin},\times}(H)$ is an essentially surjective equimorphism by Proposition 3.1.3(i). The result is then an immediate consequence of Proposition 3.1.3(iv). □

Chapter 4

Minimal Factorizations and Applications

Example 3.2.4 indicates that, in the presence of torsion in the ground monoid H, sets of lengths in $\mathcal{P}_{\text{fin},1}(H)$ blow up in a predictable fashion, with the result that most of the invariants classically studied in Factorization Theory lose their significance. In the case of Example 3.2.4, this phenomenon is due to the existence of non-trivial idempotents and has been previously addressed by many authors in the literature on *commutative* rings and monoids (see Remarks 4.1.4 and 4.1.5). Here we strive for a "natural approach" that applies to *arbitrary* monoids, spurring us to consider a refinement of the notions introduced in Section 2.1 and to investigate some of their fundamental properties (see, in particular, Definition 4.1.3 and Proposition 4.1.8), before focusing on the special case of power monoids.

4.1 Fundamentals of Minimal Factorizations

We start with the definition of a binary relation (in fact, a preorder) on the $\mathcal{A}(H)$-words of a monoid H that we shall use to "filter out the redundant factors" that may contribute to the factorizations of an element of H (recall that, given a set X, we denote by $\mathcal{F}^*(X)$ the free monoid with basis X and by ε_X the identity of $\mathcal{F}^*(X)$).

Definition 4.1.1. Let H be a monoid. We denote by $\preceq_H$ the binary relation on $\mathcal{F}^*(\mathcal{A}(H))$ determined by taking $\mathfrak{a} \preceq_H \mathfrak{b}$, for some $\mathcal{A}(H)$-words $\mathfrak{a}$ and $\mathfrak{b}$ of length h and k respectively, if and only if one of the following conditions holds:

- $\mathfrak{a} = \varepsilon_{\mathcal{A}(H)}$ and $\mathfrak{b}$ is arbitrary;
- $\mathfrak{a}$ and $\mathfrak{b}$ are non-empty words, say $\mathfrak{a} = a_1 * \cdots * a_h$ and $\mathfrak{b} = b_1 * \cdots * b_k$, and there is an injection $\sigma : [1, h] \to [1, k]$ such that $b_i \simeq_H a_{\sigma(i)}$ for every $i \in [1, h]$.

We shall write $\mathfrak{a} \prec_H \mathfrak{b}$ if $\mathfrak{a} \preceq_H \mathfrak{b}$ but $\mathfrak{b} \not\preceq_H \mathfrak{a}$, and say that a word $\mathfrak{a} \in \mathcal{F}^*(\mathcal{A}(H))$ is $\preceq_H$*-minimal* (or simply *minimal*) if there does not exist any
$A(H)$-word $\mathfrak{b}$ such that $\mathfrak{b} \prec_H \mathfrak{a}$.

The next result highlights a few basic properties of the relation introduced in Definition 4.1.1.

Proposition 4.1.2. Let H be a monoid, and let $\mathfrak{a}, \mathfrak{b} \in \mathcal{F}^*(\mathcal{A}(H))$. The following hold:

(i) $\preceq_H$ is a preorder (i.e., a reflexive and transitive binary relation) on $\mathcal{F}^*(\mathcal{A}(H))$.

(ii) If $\mathfrak{a} \preceq_H \mathfrak{b}$ then $|\mathfrak{a}| \le |\mathfrak{b}|$.

(iii) $\mathfrak{a} \preceq_H \mathfrak{b}$ and $\mathfrak{b} \preceq_H \mathfrak{a}$ if and only if $\mathfrak{a} \preceq_H \mathfrak{b}$ and $|\mathfrak{a}| = |\mathfrak{b}|$, if and only if $\mathfrak{a} \simeq_H \mathfrak{b}$.

Proof. Points (i) and (ii) are straightforward from our definitions.

As for (iii), set $h := |\mathfrak{a}|$ and $k := |\mathfrak{b}|$. By part (ii), $\mathfrak{a} \preceq_H \mathfrak{b}$ and $\mathfrak{b} \preceq_H \mathfrak{a}$ only if $\mathfrak{a} \preceq_H \mathfrak{b}$ and $h = k$; and it is immediate to check that $\mathfrak{a} \simeq_H \mathfrak{b}$ implies $\mathfrak{a} \preceq_H \mathfrak{b}$ and $\mathfrak{b} \preceq_H \mathfrak{a}$. So, to finish the proof, assume that $\mathfrak{a} \preceq_H \mathfrak{b}$ and $h = k$. We only need to show that $\mathfrak{a} \simeq_H \mathfrak{b}$. For, we have (by definition) that $\mathfrak{a} \preceq_H \mathfrak{b}$ if and only if $\pi_H(\mathfrak{a}) = \pi_H(\mathfrak{b})$ and there is an injection $\sigma : [1, h] \to [1, k]$ such that $a_i \simeq_H b_{\sigma(i)}$ for every $i \in [1, h]$. But σ is actually a bijection (because $h = k$), and we can thus conclude that $\mathfrak{a} \simeq_H \mathfrak{b}$. □

Definition 4.1.3. Let H be a monoid and $x \in H$. An H-word $\mathfrak{a}$ is a **$\preceq_H$-minimal factorization** of x, or simply a **minimal factorization** of x (in H), if $\mathfrak{a} \in \mathcal{Z}_H(x)$ and $\mathfrak{a}$ is $\preceq_H$-minimal. Accordingly,

$$\mathcal{Z}_H^{\mathsf{m}}(x) := \{\mathfrak{a} \in \mathcal{Z}_H(x) : \mathfrak{a} \text{ is } \preceq_H\text{-minimal}\} \quad \text{and} \quad \mathsf{Z}_H^{\mathsf{m}}(x) := \mathcal{Z}_H^{\mathsf{m}}(x)/\simeq_H$$

shall denote, respectively, the **set of $\preceq_H$-minimal factorizations** and the **set of $\preceq_H$-minimal factorization classes** of x (cf. the definitions from Section 2.1). In addition, we take

$$\mathsf{L}_H^{\mathsf{m}}(x) := \{|\mathfrak{a}| : \mathfrak{a} \in \mathcal{Z}_H^{\mathsf{m}}(x)\} \subseteq \mathbb{N}$$

to be the set of **$\preceq_H$-minimal factorization lengths** of x, and

$$\mathcal{L}^{\mathsf{m}}(H) := \{\mathsf{L}_H^{\mathsf{m}}(x) : x \in H\} \subseteq \mathcal{P}(\mathbb{N})$$

to be the **system of sets of $\preceq_H$-minimal lengths** of H. Lastly, we say that the monoid H is

- **BmF** or **bounded-minimally-factorial** (respectively, **FmF** or **finite-minimally-factorial**) if $\mathsf{L}_H^{\mathsf{m}}(x)$ (respectively, $\mathsf{Z}_H^{\mathsf{m}}(x)$) is finite and non-empty for every $x \in H \setminus H^\times$;
- **HmF** or **half-minimally-factorial** (respectively, **UmF** or **minimally factorial**) if $\mathsf{L}_H^{\mathsf{m}}(x)$ (respectively, $\mathsf{Z}_H^{\mathsf{m}}(x)$) is a singleton for all $x \in H \setminus H^\times$.

Note that we may write $\mathcal{Z}^{\mathsf{m}}(x)$ for $\mathcal{Z}_H^{\mathsf{m}}(x)$, $\mathsf{L}^{\mathsf{m}}(x)$ for $\mathsf{L}_H^{\mathsf{m}}(x)$, etc. if there is no likelihood of confusion.

Remark 4.1.4. To the best of our knowledge, analogues of the notions introduced in Definition 4.1.3 have only been considered so far in a *commutative* setting, with one significant example being offered by the work of S. Chun, D.D. Anderson, and S. Valdes-Leon [CAVL11] on "reduced factorizations".

In detail, let H be the multiplicative monoid of a (unital) ring R and fix a set $\mathcal{A} \subseteq R$. We say that a non-empty $\mathcal{A}$-word $a_1 * \cdots * a_n$ of length n is a *minimal $\mathcal{A}$-factorization* of an element $x \in R$ if $\pi_H(\mathfrak{a}) = x$

but $x \neq \pi_H(\mathfrak{b})$ for every non-empty $\mathcal{A}$-word $\mathfrak{b} = b_1 * \cdots * b_m$ of length $m \le n-1$ for which there exists an injection $\sigma : [1,m] \to [1,n]$ such that $b_i \simeq_H a_{\sigma(i)}$ for each $i \in [1,m]$.

A minimal $\mathcal{A}(H)$-factorization of a non-unit $x \in R$ is the same as a $\preceq_H$-minimal factorization of x (as per Definition 4.1.3). Moreover, it follows from Section 2.4 and Proposition 2.3.3(iv) that, if R is a *commutative* ring and x is not the zero of R, then a minimal $\mathcal{A}(H)$-factorization of x is, in the parlance of [CAVL11, Definition 2.1 and Section 3], essentially the same as a *strongly μ-reduced μ-factorization* of x into very strongly irreducible elements of R. Insofar as the discussion is restricted to commutative rings, one can thus refer to [CAVL11] and [AFRS03] for a comparison of our approach to the study of "minimal factorizations" with others in the literature, including the one by C.R. Fletcher [Fle69] and generalizations thereof where the set $\mathcal{A}$ in the above consists of various types of "irreducible elements" of R (cf. Section 2.4).

Remark 4.1.5. Another approach for managing the "excess factorizations" arising from the presence of torsion (though still in a commutative setting), was outlined by A. Geroldinger and G. Lettl in [GL90].

In short, let H be a *commutative* monoid and denote by $\mathcal{A}$ the set of all $a \in H \setminus H^\times$ such that $b \mid_H a$ only if $b \in H^\times$ or $aH = bH$. Given $u \in H$, we define

$$\operatorname{ind}_H^{\mathrm{GL}}(u) := \inf\{r \in \mathbb{N} : u^i H = u^j H \text{ for all } i, j \ge r\}.$$

Accordingly, we take a GL-*factorization* of a non-unit $x \in H$ to be a non-empty $\mathcal{A}$-word $\mathfrak{a} = a_1 * \cdots * a_n$ such that $\pi_H(\mathfrak{a}) = x$ and $\mathsf{v}_a^H(\mathfrak{a}) \le \operatorname{ind}_H^{\mathrm{GL}}(a)$ for every $a \in \mathcal{A}$, where

$$\mathsf{v}_a^H(\mathfrak{a}) := \big|\{i \in [1,n] : a_i = a\}\big|.$$

A GL-factorization is fundamentally the same as the "canonical form" of a factorization in the sense of [GL90]; and since it is easily checked that $\mathcal{A}(H) \subseteq \mathcal{A}$, every $\preceq_H$-minimal factorization is also a GL-factorization. Moreover, the two notions coincide on the level of commutative, unit-cancellative monoids, in which case $\mathcal{A} = \mathcal{A}(H)$ and $\operatorname{ind}_H^{\mathrm{GL}}(u) = \infty$ for every non-unit $u \in H$. However, big differences exist in general. E.g., it follows from Lemma 3.2.1(i) and the above that $\{\bar{0}, \bar{1}\} * \{\bar{0}, \bar{2}\} * \{\bar{0}, \bar{3}\} * \{\bar{0}, \bar{4}\}$ is an essential factorization of $\mathbb{Z}/5\mathbb{Z}$ in the reduced power monoid of the cyclic group $(\mathbb{Z}/5\mathbb{Z}, +)$; but is not a minimal factorization as per Definition 4.1.3, because $\mathbb{Z}/5\mathbb{Z} = \{\bar{0}, \bar{1}\} + \{\bar{0}, \bar{2}\} + \{\bar{0}, \bar{3}\}$.

It is helpful, at this juncture, to observe some fundamental features of minimal factorizations.

Proposition 4.1.6. Let H be a monoid and let $x \in H$. The following hold:

(i) Any $\mathcal{A}(H)$-word of length 0, 1, or 2 is minimal.

(ii) $\mathcal{Z}_H(x) \neq \emptyset$ if and only if $\mathcal{Z}_H^{\mathsf{m}}(x) \neq \emptyset$.

(iii) If $\mathfrak{a} \in \mathcal{Z}_H^{\mathsf{m}}(x)$ and $\mathfrak{a} \simeq_H \mathfrak{b}$, then $\mathfrak{b} \in \mathcal{Z}_H^{\mathsf{m}}(x)$.

(iv) If K is a divisor-closed submonoid of H and $x \in K$, then $\mathcal{Z}_K^{\mathsf{m}}(x) = \mathcal{Z}_H^{\mathsf{m}}(x)$ and $\mathsf{L}_K^{\mathsf{m}}(x) = \mathsf{L}_H^{\mathsf{m}}(x)$.

(v) If H is commutative and unit-cancellative, then $\mathcal{Z}_H^{\mathsf{m}}(x) = \mathcal{Z}_H(x)$, and hence $\mathsf{L}_H^{\mathsf{m}}(x) = \mathsf{L}_H(x)$.

Proof. (i), (ii), and (iii) are an immediate consequence of parts (ii)-(iii) of Proposition 4.1.2 (in particular, note that, if $\mathfrak{a}$ is an $\mathcal{A}(H)$-word of length 1, then $\pi_H(\mathfrak{a})$ is an atom of H, and therefore $\pi_H(\mathfrak{a}) \neq \pi_H(\mathfrak{b})$ for every $\mathcal{A}(H)$-word $\mathfrak{b}$ of length ≥ 2); and (iv) follows at once from considering that, if K is a divisor-closed submonoid of H and $x \in K$, then $\mathcal{Z}_K(x) = \mathcal{Z}_H(x)$ and $\mathsf{L}_K(x) = \mathsf{L}_H(x)$, see [FT18, Proposition 2.21(ii)].

(v) Assume H is commutative and unit-cancellative. It suffices to check that no non-empty $\mathcal{A}(H)$-word has a proper subword with the same product. For, suppose to the contrary that there exist $a_1, \ldots, a_n \in \mathcal{A}(H)$ with $\prod_{i \in I} a_i = a_1 \cdots a_n$ for some $I \subsetneq [1, n]$. Since H is commutative, we can assume without loss of generality that $I = [1, k]$ for some $k \in [0, n-1]$. Then unit-cancellativity implies $a_{k+1} \cdots a_n \in H^\times$, and we get from parts (i) and (ii) of Proposition 2.3.3 that $a_{k+1}, \ldots, a_n \in H^\times$, which is however impossible (by definition of an atom). □

To further elucidate the behavior of minimal factorizations, we give an analogue of Proposition 2.3.3(iv) showing that multiplying a non-unit by units does not change its set of minimal factorizations.

Lemma 4.1.7. Let H be a monoid, and fix $x \in H \setminus H^\times$ and $u, v \in H^\times$. Then there is a length-preserving bijection $\mathcal{Z}_H^{\mathsf{m}}(x) \to \mathcal{Z}_H^{\mathsf{m}}(uxv)$, and in particular $\mathsf{L}_H^{\mathsf{m}}(x) = \mathsf{L}_H^{\mathsf{m}}(uxv)$.

Proof. Given $w, z \in H$ and a non-empty word $\mathfrak{z} = y_1 * \cdots * y_n \in \mathcal{F}^*(H)$ of length n, denote by $w\mathfrak{z}z$ the length-n word $\bar{y}_1 * \cdots * \bar{y}_n \in \mathcal{F}^*(H)$ defined by taking $\bar{y}_1 := wy_1z$ if $n = 1$, and $\bar{y}_1 := wy_1$, $\bar{y}_n := y_nz$, and $\bar{y}_i := y_i$ for all $i \in [2, n-1]$ otherwise. We claim that the function

$$\begin{aligned} f : \mathcal{Z}_H^{\mathsf{m}}(x) &\to \mathcal{Z}_H^{\mathsf{m}}(uxv) \\ \mathfrak{a} &\mapsto u\mathfrak{a}v \end{aligned}$$

is a well-defined length-preserving bijection. In fact, it is sufficient to show that f is well-defined, since this will in turn imply that the map $g : \mathcal{Z}_H^{\mathsf{m}}(uxv) \to \mathcal{Z}_H^{\mathsf{m}}(x) : \mathfrak{b} \mapsto u^{-1}\mathfrak{b}v^{-1}$ is also well-defined (observe that $uxv \in H \setminus H^\times$ and $x = u^{-1}uxvv^{-1}$), and then it is easy to check that g is the inverse of f.

For the claim, let $\mathfrak{a} \in \mathcal{Z}_H^{\mathsf{m}}(x)$, and note that, by parts (i) and (ii) of Proposition 2.3.3, $|\mathfrak{a}|$ is a positive integer, so that $\mathfrak{a} = a_1 * \cdots * a_n$ for some $a_1, \ldots, a_n \in \mathcal{A}(H)$. In view of Proposition 2.3.3(iii), $u\mathfrak{a}v$ is a factorization of uxv, and we only need to verify that it is also $\preceq_H$-minimal. For, suppose to the contrary that $\mathfrak{b} \prec_H u\mathfrak{a}v$ for some $\mathfrak{b} \in \mathcal{F}^*(\mathcal{A}(H))$. Then $\pi_H(\mathfrak{b}) = \pi_H(u\mathfrak{a}v) = uxv$ and, by Proposition 4.1.2(iii), $k := |\mathfrak{b}| \in [1, n-1]$ (recall that $uxv \notin H^\times$). So, $\mathfrak{b} = b_1 * \cdots * b_k$ for some atoms $b_1, \ldots, b_k \in H$, and there exists an injection $\sigma : [1, k] \to [1, n]$ such that $b_i \simeq_H a_{\sigma(i)}$ for each $i \in [1, k]$. Define $\mathfrak{c} := u^{-1}\mathfrak{b}v^{-1}$.

By construction and Proposition 2.3.3(iii), there are $c_1, \ldots, c_k \in \mathcal{A}(H)$ such that $\mathfrak{c} = c_1 * \cdots * c_k$; and it follows from the above that $\pi_H(\mathfrak{c}) = u^{-1}\pi_H(\mathfrak{b})v^{-1} = x$ and $c_i \simeq_H a_{\sigma(i)}$ for every $i \in [1, k]$. Since $k < n$, we can thus conclude from Proposition 4.1.2(iii) that $\mathfrak{c} \prec_H \mathfrak{a}$, contradicting the $\preceq_H$-minimality of $\mathfrak{a}$. □

We saw in the previous section that equimorphisms transfer factorizations between monoids (Proposition 2.3.7). Equimorphisms have a similar compatibility with minimal factorizations, in the sense that an equimorphism also satisfies a "minimal version" of condition (E3) from Definition 2.3.6.

Proposition 4.1.8. Let H and K be monoids and $\varphi : H \to K$ an equimorphism. The following hold:

(i) If $x \in H \setminus H^\times$ and $\mathfrak{b} \in \mathscr{Z}_K^{\mathsf{m}}(\varphi(x))$, then there is $\mathfrak{a} \in \mathscr{Z}_H^{\mathsf{m}}(x)$ with $\varphi^*(\mathfrak{a}) \in [\mathfrak{b}]_{\simeq_K}$.

(ii) $\mathsf{L}_K^{\mathsf{m}}(\varphi(x)) \subseteq \mathsf{L}_H^{\mathsf{m}}(x)$ for every $x \in H \setminus H^\times$.

(iii) If φ is essentially surjective then, for all $y \in K \setminus K^\times$, there is $x \in H \setminus H^\times$ with $\mathsf{L}_K^{\mathsf{m}}(y) \subseteq \mathsf{L}_H^{\mathsf{m}}(x)$.

Proof. (i) Pick $x \in H \setminus H^\times$, and let $\mathfrak{b} \in \mathscr{Z}_K^{\mathsf{m}}(\varphi(x))$. Then $\mathfrak{b} \neq \varepsilon_{\mathcal{A}(K)}$, otherwise $\varphi(x) = \pi_K(\mathfrak{b}) = 1_K$ and, by (E1), $x \in \varphi^{-1}(\varphi(x)) = \varphi^{-1}(1_K) \subseteq H^\times$ (a contradiction). Consequently, (E3) yields the existence of a factorization $\mathfrak{a} \in \mathscr{Z}_H(x)$ with $\varphi^*(\mathfrak{a}) \in [\mathfrak{b}]_{\simeq_K}$, and it only remains to show that $\mathfrak{a}$ is $\preceq_H$-minimal.

Note that $n := |\mathfrak{a}| = |\varphi^*(\mathfrak{a})| = |\mathfrak{b}| \geq 1$, and write $\mathfrak{a} = a_1 * \cdots * a_n$ and $\mathfrak{b} = b_1 * \cdots * b_n$, with $a_1, \ldots, a_n \in \mathcal{A}(H)$ and $b_1, \ldots, b_n \in \mathcal{A}(K)$. Then suppose to the contrary that $\mathfrak{a}$ is not $\preceq_H$-minimal, i.e., there exist a (necessarily non-empty) $\mathcal{A}(H)$-word $\mathfrak{c} = c_1 * \cdots * c_m$ and an injection $\sigma : [1, m] \to [1, n]$ such that $\pi_H(\mathfrak{c}) = \pi_H(\mathfrak{a}) = x$ and $c_i \simeq_H a_{\sigma(i)}$ for every $i \in [1, m]$. Then

$$\pi_K(\varphi^*(\mathfrak{c})) = \varphi(c_1) \cdots \varphi(c_m) = \varphi(x) \quad \text{and} \quad \varphi(c_1) \simeq_K \varphi(a_{\sigma(1)}), \ldots, \varphi(c_m) \simeq_K \varphi(a_{\sigma(m)})$$

(recall that monoid homomorphisms map units to units; so, if $u \simeq_H v$, then $\varphi(u) \simeq_K \varphi(v)$); and together with Proposition 4.1.6(iii), this proves that $\varphi^*(\mathfrak{c}) \prec_K \mathfrak{b}$, contradicting the $\preceq_K$-minimality of $\mathfrak{b}$.

(ii) Fix $x \in H \setminus H^\times$, and suppose $\mathsf{L}_K^{\mathsf{m}}(\varphi(x)) \neq \emptyset$ (otherwise there is nothing to prove). Accordingly, let $k \in \mathsf{L}_K^{\mathsf{m}}(\varphi(x))$ and $\mathfrak{b} \in \mathscr{Z}_K^{\mathsf{m}}(\varphi(x))$ such that $k = |\mathfrak{b}|$. It is sufficient to check that $k \in \mathsf{L}_H^{\mathsf{m}}(x)$, and this is straightforward: Indeed, we have by (i) that $\varphi^*(\mathfrak{a})$ is K-equivalent to $\mathfrak{b}$ for some $\mathfrak{a} \in \mathscr{Z}_H^{\mathsf{m}}(x)$, which implies in particular that $k = |\varphi^*(\mathfrak{a})| = |\mathfrak{a}| \in \mathsf{L}_H^{\mathsf{m}}(x)$.

(iii) Assume φ is essentially surjective, and let $y \in K \setminus K^\times$. Then $y = u\varphi(x)v$ for some $u, v \in K^\times$ and $x \in H$, and neither x is a unit of H nor $\varphi(x)$ is a unit of K (because $\varphi(H^\times) \subseteq K^\times$ and $y \notin K^\times$). Accordingly, we have by Lemma 4.1.7 and part (ii) that $\mathsf{L}_K^{\mathsf{m}}(y) = \mathsf{L}_K^{\mathsf{m}}(\varphi(x)) \subseteq \mathsf{L}_H^{\mathsf{m}}(x)$. □

4.2 Minimal Factorizations in Power Monoids

Let H be a monoid. Similarly as in Section 3.2, we would like to simplify the study of minimal factorizations in $\mathcal{P}_{\text{fin},\times}(H)$ as much as possible by passing to consideration of the reduced monoid $\mathcal{P}_{\text{fin},1}(H)$. For, it is of primary importance to make clear the nature of the relationship between minimal factorizations in $\mathcal{P}_{\text{fin},\times}(H)$ and those in $\mathcal{P}_{\text{fin},1}(H)$. We shall see that this is possible under *some* circumstances.

Proposition 4.2.1. Let H be a commutative monoid, and let $X \in \mathcal{P}_{\text{fin},1}(H)$. The following hold:

(i) $\mathscr{Z}^{\mathsf{m}}_{\mathcal{P}_{\text{fin},1}(H)}(X) \subseteq \mathscr{Z}^{\mathsf{m}}_{\mathcal{P}_{\text{fin},\times}(H)}(X)$.

(ii) $\mathsf{L}^{\mathsf{m}}_{\mathcal{P}_{\text{fin},1}(H)}(X) = \mathsf{L}^{\mathsf{m}}_{\mathcal{P}_{\text{fin},\times}(H)}(X)$.

(iii) $\mathcal{L}^{\mathsf{m}}(\mathcal{P}_{\text{fin},1}(H)) = \mathcal{L}^{\mathsf{m}}(\mathcal{P}_{\text{fin},\times}(H))$.

Proof. (i) Let $\mathfrak{a}$ be a minimal factorization of X relative to $\mathcal{P}_{\text{fin},1}(H)$. In light of Proposition 4.1.6(i), $\mathfrak{a}$ is a non-empty $\mathcal{A}(\mathcal{P}_{\text{fin},1}(H))$-word, i.e., $\mathfrak{a} = A_1 * \cdots * A_n$ for some atoms $A_1, \ldots, A_n \in \mathcal{P}_{\text{fin},1}(H)$.

Assume for the sake of contradiction that $\mathfrak{a}$ is not a minimal factorization relative to $\mathcal{P}_{\text{fin},\times}(H)$. Then there exist a non-empty $\mathcal{A}(\mathcal{P}_{\text{fin},\times}(H))$-word $\mathfrak{b} = B_1 * \cdots * B_m$ and an injection $\sigma : [1, m] \to [1, n]$ with

$$X = A_1 \cdots A_n = B_1 \cdots B_m \quad \text{and} \quad B_1 \simeq_{\mathcal{P}_{\text{fin},\times}(H)} A_{\sigma(1)}, \ldots, B_m \simeq_{\mathcal{P}_{\text{fin},\times}(H)} A_{\sigma(m)},$$

and on account of Proposition 4.1.2(iii) we must have $1 \le m < n$. Since H is a commutative monoid, this means in particular that, for each $i \in [1, m]$, there is $u_i \in H^\times$ such that $B_i = u_i A_{\sigma(i)}$. Thus we have

$$A_1 \cdots A_n = B_1 \cdots B_m = (u_1 A_{\sigma(1)}) \cdots (u_m A_{\sigma(m)}) = u \cdot A_{\sigma(1)} \cdots A_{\sigma(m)},$$

where $u := u_1 \cdots u_m \in H^\times$. In view of Proposition 3.1.2(ii), it follows that

$$|A_1 \cdots A_n| = \left| A_{\sigma(1)} \cdots A_{\sigma(m)} \right|,$$

which is only possible if

$$X = A_1 \cdots A_n = A_{\sigma(1)} \cdots A_{\sigma(m)},$$

because $1_H \in A_i$ for every $i \in [1, n]$, and hence $A_{\sigma(1)} \cdots A_{\sigma(m)} \subseteq A_1 \cdots A_n$ (note that here we use again that H is commutative). So, letting $\mathfrak{a}'$ be the $\mathcal{A}(\mathcal{P}_{\text{fin},1}(H))$-word $A_{\sigma(1)} * \cdots * A_{\sigma(m)}$ and recalling from the above that $m \le n - 1$, we see by Proposition 4.1.2(iii) that $\mathfrak{a}' \prec_{\mathcal{P}_{\text{fin},1}(H)} \mathfrak{a}$, which contradicts the hypothesis that $\mathfrak{a}$ is a minimal factorization of X in $\mathcal{P}_{\text{fin},1}(H)$.

(ii) It is an immediate consequence of part (i) and Propositions 3.1.3(i) and 4.1.8(ii), when considering that every commutative monoid is Dedekind-finite.

(iii) We already know from part (ii) that $\mathcal{L}^{\mathsf{m}}(\mathcal{P}_{\text{fin},1}(H)) \subseteq \mathcal{L}^{\mathsf{m}}(\mathcal{P}_{\text{fin},\times}(H))$. For the opposite inclusion, fix $X \in \mathcal{P}_{\text{fin},\times}(H)$. We claim that there exists $Y \in \mathcal{P}_{\text{fin},1}(H)$ with $\mathsf{L}^{\mathsf{m}}_{\mathcal{P}_{\text{fin},\times}(H)}(X) = \mathsf{L}^{\mathsf{m}}_{\mathcal{P}_{\text{fin},1}(H)}(Y)$. Indeed, pick $x \in X \cap H^\times$. Then $x^{-1}X \in \mathcal{P}_{\text{fin},1}(H)$, and we derive from Lemma 4.1.7 and part (ii) that

$$\mathsf{L}^{\mathsf{m}}_{\mathcal{P}_{\text{fin},\times}(H)}(X) = \mathsf{L}^{\mathsf{m}}_{\mathcal{P}_{\text{fin},\times}(H)}(x^{-1}X) = \mathsf{L}^{\mathsf{m}}_{\mathcal{P}_{\text{fin},1}(H)}(x^{-1}X),$$

which proves our claim and suffices to finish the proof (since X was arbitrary). □

We will now discuss an instance in which equality in Proposition 4.2.1(ii) does not necessarily hold true in the absence of commutativity, and the best we can hope for is the containment relation implied by Proposition 4.1.8(ii) when φ is the natural embedding of Proposition 3.1.3(i).

Example 4.2.2. Let n be a (positive) multiple of 105, and p a (positive) prime dividing $n^2 + n + 1$; note that $p \ge 11$ and $3 \le n \bmod p \le p - 3$ (where $n \bmod p$ is the smallest non-negative integer $\equiv n \bmod p$). Following [Gor80, p. 27], we take H to be the metacyclic group generated by the 2-element set $\{r, s\}$ subject to $\mathrm{ord}_H(r) = p$, $\mathrm{ord}_H(s) = 3$, and $s^{-1}rs = r^n$. Then H is a non-abelian group of (odd) order $3p$, and by Theorem 3.2.3 and Propositions 2.3.7(ii) and 3.1.3(i), $\mathcal{P}_{\mathrm{fin},1}(H)$ and $\mathcal{P}_{\mathrm{fin},\times}(H)$ are both atomic monoids.

We claim that $X := \langle r \rangle_H$ has minimal factorizations of length $p-1$ in $\mathcal{P}_{\mathrm{fin},1}(H)$ but not in $\mathcal{P}_{\mathrm{fin},\times}(H)$. Pick $g \in X \setminus \{1_H\}$. Clearly $\mathrm{ord}_H(g) = p$, and thus we get from Lemma 3.2.1(i) that $\{1_H, g\}$ is an atom of $\mathcal{P}_{\mathrm{fin},1}(H)$. Then it is immediate to see that $\mathfrak{a}_g := \{1_H, g\}^{*(p-1)}$ is a minimal factorization of X in $\mathcal{P}_{\mathrm{fin},1}(H)$; most notably, $\mathfrak{a}_g$ is minimal since otherwise there should exist an exponent $k \in [1, p-2]$ such that $g^{p-1} = g^k$, contradicting that $\mathrm{ord}_H(g) = p$. Yet, $\mathfrak{a}_g$ is not a minimal factorization of X in $\mathcal{P}_{\mathrm{fin},\times}(H)$. Indeed, Proposition 3.1.3(ii) and Lemma 3.2.1(i) guarantee that $\{1_H, g\}$ and $\{1_H, g^n\}$ are associate atoms of $\mathcal{P}_{\mathrm{fin},\times}(H)$, because $s^{-1}g^n s = g$ and, hence, $s^{-1}\{1, g\}s = \{1_H, g^n\}$. So, in view of Proposition 4.1.2(iii), it is straightforward that

$$\{1_H, g\}^{*(p-2)} * \{1_H, g^n\} \prec_{\mathcal{P}_{\mathrm{fin},\times}(H)} \mathfrak{a}_g,$$

In particular, note here that we have used that $3 \le n \bmod p \le p-3$ to obtain

$$\{1_H, g, \dots, g^{p-2}\} \cup \{g^n, g^{n+1}, \dots, g^{n+p-2}\} = \{1_H, g, \dots, g^{p-1}\} = X.$$

Given that, suppose for a contradiction that X has a minimal factorization $\mathfrak{c}$ of length $p-1$ in $\mathcal{P}_{\mathrm{fin},\times}(H)$. Then by Propositions 3.1.3(i) and 4.1.8(i), $\mathfrak{c}$ is $\mathcal{P}_{\mathrm{fin},\times}(H)$-equivalent to a $\preceq_{\mathcal{P}_{\mathrm{fin},1}(H)}$-minimal factorization $\mathfrak{a} = A_1 * \cdots * A_{p-1}$ of X of length $p-1$; and we aim to show that $\mathfrak{a}$ is $\mathcal{P}_{\mathrm{fin},1}(H)$-equivalent to $\mathfrak{a}_g$ for some $g \in X \setminus \{1_H\}$, which is however impossible as it would mean that $\mathfrak{a}_g$ is a minimal factorization of X in $\mathcal{P}_{\mathrm{fin},\times}(H)$, in contradiction to what established in the above.

Indeed, let B_i be, for $i \in [1, p-1]$, the image of $\{k \in [0, p-1] : r^k \in A_i\} \subseteq \mathbb{Z}$ under the canonical map $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$. Then $\mathfrak{a}$ is a minimal factorization of X in $\mathcal{P}_{\mathrm{fin},1}(H)$ only if $\mathfrak{b} := B_1 * \cdots * B_{p-1}$ is a minimal factorization of $\mathbb{Z}/p\mathbb{Z}$ in the reduced power monoid of $(\mathbb{Z}/p\mathbb{Z}, +)$, herein denoted by $\mathcal{P}_{\mathrm{fin},0}(\mathbb{Z}/p\mathbb{Z})$.

We want to show that $\mathfrak{b}$ is $\preceq_{\mathcal{P}_{\mathrm{fin},0}(H)}$-minimal only if there is a non-zero $x \in \mathbb{Z}/p\mathbb{Z}$ such that $B_i = \{\overline{0}, x\}$ or $B_i = \{\overline{0}, -x\}$, or equivalently $A_i = \{1_H, r^{\hat{x}}\}$ or $A_i = \{1_H, r^{-\hat{x}}\}$, for every $i \in [1, p-1]$ (recall the notation that $\hat{x}$ is the lift of the residue class x to the interval $[0, p-1]$, established in Section 1.3). By the preceding arguments, this will suffice to conclude that $p - 1 \notin \mathsf{L}^{\mathsf{m}}_{\mathcal{P}_{\mathrm{fin},\times}(H)}(X)$, because it implies at once that $\mathfrak{a}$ is $\mathcal{C}_{\mathcal{P}_{\mathrm{fin},1}(H)}$-congruent to $\mathfrak{a}_g$ with $g := r^{\hat{x}} \in X \setminus \{1_H\}$.

To begin, let K be a subset of $[1, p-1]$, and define $\mathcal{S}_K := \sum_{k \in K} B_k$ and $s_K := \{k \in K : |B_k| \ge 3\}$. Then we have by the Cauchy-Davenport inequality (see, e.g., [Gry13, Theorem 6.2]) that

$$\mathcal{S}_K = \mathbb{Z}/p\mathbb{Z} \quad \text{or} \quad |\mathcal{S}_K| \ge 1 + \sum\nolimits_{k \in K} \big(|B_k| - 1\big) \ge 1 + |K| + s_K. \tag{4.1}$$

Now, let I and J be disjoint subsets of $[1, p-1]$ with $|I \cup J| = |I| + |J| = p-2$. We claim $s_I = s_J = 0$. Indeed, it is clear that $\mathcal{S}_{I \cup J} \neq \mathbb{Z}/p\mathbb{Z}$, otherwise $\mathfrak{b}$ would not be a minimal factorization in $\mathcal{P}_{\mathrm{fin},0}(\mathbb{Z}/p\mathbb{Z})$. So, another application of the Cauchy-Davenport inequality, combined with (4.1), yields

$$|S_{I\cup J}| = |S_I + S_J| \ge |S_I| + |S_J| - 1 \ge 1 + |I| + |J| + s_I + s_J = p - 1 + s_I + s_J. \tag{4.2}$$

This suffices to prove that $|S_I + S_J| = p - 1$ and $s_I = s_J = 0$, or else $S_{I\cup J} = \mathbb{Z}/p\mathbb{Z}$ (a contradiction).

It follows $|B_1| = \cdots = |B_{p-1}| = 2$. So, taking I in (4.2) to range over all 1-element subsets of $[1, p-1]$ and observing that, consequently, $|S_J| \ge p - 1 - |S_I| = p - 3 \ge 8 > |S_I|$, we infer from Vosper's theorem (see, e.g., [Gry13, Theorem 8.1]) that there exists a non-zero $x \in \mathbb{Z}/p\mathbb{Z}$ such that, for every $i \in [1, p-1]$, B_i is an arithmetic progression of $\mathbb{Z}/p\mathbb{Z}$ with difference x, i.e., $B_i = \{\overline{0}, x\}$ or $B_i = \{\overline{0}, -x\}$ (as wished).

We proceed with an analogue of Theorem 3.2.5(i) and then prove the main results of the section.

Proposition 4.2.3. Let H be a monoid and $X \in \mathcal{P}_{\text{fin},\times}(H)$. The following hold:

(i) If $X \in \mathcal{P}_{\text{fin},1}(H)$, then a minimal factorization of X in $\mathcal{P}_{\text{fin},1}(H)$ has length $\le |X| - 1$.

(ii) If H is Dedekind-finite, then a minimal factorization of X in $\mathcal{P}_{\text{fin},\times}(H)$ has length $\le |X| - 1$.

Proof. (i) The claim is trivial if $X = \{1_H\}$, when the only factorization of X is the empty word; or if $X \in \mathcal{A}(\mathcal{P}_{\text{fin},1}(H))$, in which case $|X| \ge 2$ and X has a unique factorization (of length 1). So, assume that X is neither the identity nor an atom of $\mathcal{P}_{\text{fin},1}(H)$, and let $\mathfrak{a}$ be a minimal factorization of X (relative to $\mathcal{P}_{\text{fin},1}(H)$). Then $\mathfrak{a} = A_1 * \cdots * A_n$, where $A_1, \ldots, A_n \in \mathcal{A}(\mathcal{P}_{\text{fin},1}(H))$ and $n \ge 2$; and we claim that

$$A_1 \cdots A_i \subsetneq A_1 \cdots A_{i+1}, \quad \text{for every } i \in [1, n-1].$$

In fact, let $i \in [1, n-1]$. Since $1_H \in A_{i+1}$, it is clear that $A_1 \cdots A_i \subsetneq A_1 \cdots A_{i+1}$; and the inclusion must be strict, or else $A_1 * \cdots * A_i * \mathfrak{b} \prec_{\mathcal{P}_{\text{fin},1}(H)} \mathfrak{a}$, where $\mathfrak{b} := \varepsilon_{\mathcal{A}(\mathcal{P}_{\text{fin},1}(H))}$ if $i = n-1$ and $\mathfrak{b} := A_{i+2} * \cdots * A_n$ otherwise (contradicting the minimality of $\mathfrak{a}$). Consequently, we see that $2 \le |A_1 \cdots A_i| < |A_1 \cdots A_{i+1}| \le |X|$ for all $i \in [1, n-1]$, and this implies at once that $n \le |X| - 1$.

(ii) The conclusion is immediate from part (i) and Propositions 3.1.3(i) and 4.1.8(iii). □

Theorem 4.2.4. Let H be a monoid. Then the following are equivalent:

(a) $1_H \ne x^2 \ne x$ for every $x \in H \setminus \{1_H\}$.

(b) $\mathcal{P}_{\text{fin},1}(H)$ is atomic.

(c) $\mathcal{P}_{\text{fin},1}(H)$ is BmF.

(d) $\mathcal{P}_{\text{fin},1}(H)$ is FmF.

(e) Every 2-element subset X of H with $1_H \in X$ is an atom of $\mathcal{P}_{\text{fin},1}(H)$.

(f) $\mathcal{P}_{\text{fin},\times}(H)$ is atomic.

(g) $\mathcal{P}_{\text{fin},\times}(H)$ is BmF.

(h) $\mathcal{P}_{\text{fin},\times}(H)$ is FmF.

(i) Every 2-element subset X of H with $X \cap H^\times \ne \emptyset$ is an atom of $\mathcal{P}_{\text{fin},\times}(H)$.

Proof. We already know from Theorem 3.2.3 and Lemma 3.2.1 that (b) ⇔ (a) ⇔ (e) and (i) ⇒ (a); while it is straightforward from our definitions that (h) ⇒ (g) ⇒ (f). So, it will suffice to prove that (b) ⇒ (c) ⇒ (d) ⇒ (h) and (f) ⇒ (i).

(b) ⇒ (c): If $X \in \mathcal{P}_{\mathrm{fin},1}(H)$ is a non-unit, then $\mathcal{Z}_{\mathcal{P}_{\mathrm{fin},1}(H)}(X)$ is non-empty, and by Propositions 4.1.6(ii) and 4.2.3(i) we have that $\emptyset \neq \mathsf{L}^{\mathsf{m}}_{\mathcal{P}_{\mathrm{fin},1}(H)}(X) \subseteq [1, |X| - 1]$. So, $\mathcal{P}_{\mathrm{fin},1}(H)$ is BmF.

(c) ⇒ (d): Let $X \in \mathcal{P}_{\mathrm{fin},1}(H)$ be a non-unit. By Proposition 3.1.2(i), any atom of $\mathcal{P}_{\mathrm{fin},1}(H)$ dividing X must be a subset of X, and there are only finitely many of these (since X is finite). Because a minimal factorization of X is a bounded $\mathcal{A}(\mathcal{P}_{\mathrm{fin},1}(H))$-word (by the assumption that H is BmF), it follows that X has finitely many minimal factorizations, and hence $\mathcal{P}_{\mathrm{fin},1}(H)$ is FmF (since X was arbitrary).

(d) ⇒ (h): Pick a non-unit $X \in \mathcal{P}_{\mathrm{fin},\times}(H)$, and let $u \in H^\times$ such that $uX \in \mathcal{P}_{\mathrm{fin},1}(H)$. Since $\mathcal{P}_{\mathrm{fin},1}(H)$ is FmF (by hypothesis), it is also atomic. Hence, by Theorem 3.2.3 and Lemma 3.2.2(i), H is Dedekind-finite, and so we have by Proposition 3.1.3(i) that the natural embedding $\mathcal{P}_{\mathrm{fin},1}(H) \hookrightarrow \mathcal{P}_{\mathrm{fin},\times}(H)$ is an essentially surjective equimorphism. In particular, we infer from Proposition 4.1.8(i) that any minimal factorization of uX in $\mathcal{P}_{\mathrm{fin},\times}(H)$ is $\mathcal{C}_{\mathcal{P}_{\mathrm{fin},\times}(H)}$-congruent to a minimal factorization of uX in $\mathcal{P}_{\mathrm{fin},1}(H)$. However, this makes $\mathsf{Z}^{\mathsf{m}}_{\mathcal{P}_{\mathrm{fin},\times}(H)}(uX)$ finite, whence $\mathsf{Z}^{\mathsf{m}}_{\mathcal{P}_{\mathrm{fin},\times}(H)}(X)$ must also be finite as a consequence of Lemma 4.1.7.

(f) ⇒ (i): Let X be a 2-element subset of H with $X \cap H^\times \neq \emptyset$. Then $X = uA$ for some unit $u \in H^\times$, where $A := u^{-1}X$ is a 2-element subset of H with $1_H \in H$; and since $\mathcal{P}_{\mathrm{fin},\times}(H)$ is atomic (by hypothesis), we are guaranteed by Lemmas 3.2.1 and 3.2.2(i) that A is an atom of $\mathcal{P}_{\mathrm{fin},1}(H)$ and H is Dedekind-finite. Therefore, we conclude from Proposition 3.1.3(ii) that $X \in \mathcal{A}(\mathcal{P}_{\mathrm{fin},\times}(H))$. □

Theorem 4.2.5. Let H be a monoid. Then $\mathcal{P}_{\mathrm{fin},1}(H)$ is HmF if and only if H is trivial or a cyclic group of order 3.

Proof. The "if" part is an easy consequence of Theorem 4.2.4 and Propositions 4.2.3(i) and 4.1.6(i), when considering that, if H is trivial or a cyclic group of order 3, then $1_H \neq x^2 \neq x$ for all $x \in H \setminus \{1_H\}$ and every non-empty subset of H has at most 3 elements.

As for the other direction, suppose $\mathcal{P}_{\mathrm{fin},1}(H)$ is HmF and H is non-trivial. Then $\mathcal{P}_{\mathrm{fin},1}(H)$ is atomic, and we claim that H is a 3-group. By Theorem 3.2.3 and Lemma 3.2.2(ii), it suffices to show that $x^3 \in \{1_H, x, x^2\}$ for every $x \in H$, since this in turn implies (by induction) that $\langle x \rangle_H \subseteq \{1_H, x, x^2\}$ and $\mathrm{ord}_H(x) \leq 3$.

Assume to the contrary that $x^3 \notin \{1_H, x, x^3\}$ for some $x \in H$, and set $X := \{1_H, x, x^2, x^3\}$. By Theorem 4.2.4, $\mathfrak{a} := \{1_H, x\}^{*3}$ and $\mathfrak{b} := \{1_H, x\} * \{1_H, x^2\}$ are both factorizations of X in $\mathcal{P}_{\mathrm{fin},1}(H)$; and in light of Proposition 4.1.6(i), $\mathfrak{b}$ is in fact a minimal factorization (of length 2). Then $\mathfrak{a}$ cannot be minimal, because $\mathcal{P}_{\mathrm{fin},1}(H)$ is HmF and $\mathfrak{a}$ has length 3. However, since $\mathcal{P}_{\mathrm{fin},1}(H)$ is a reduced monoid (and X is not an atom), this is only possible if $x^3 \in X = \{1_H, x\}^2$, a contradiction.

So, H is a 3-group, and as such it has a non-trivial center $Z(H)$, see e.g. [Gor80, Theorem 2.11(i)]. Let z be an element in $Z(H) \setminus \{1_H\}$, and suppose for a contradiction that H is not cyclic. Then we can choose some element $y \in H \setminus \langle z \rangle_H$, and it follows from the above that $K := \langle y, z \rangle_H$ is an abelian subgroup of H

with $\operatorname{ord}_H(y) = \operatorname{ord}_H(z) = 3$ and $|K| = 9$. We will prove that K has $\preceq_{\mathcal{P}_{\mathrm{fin},1}(H)}$-minimal factorizations of more than one length, which is a contradiction and finishes the proof.

Indeed, we are guaranteed by Theorem 4.2.4 that $\mathfrak{c} := \{1_H, y\}^{*2} * \{1_H, z\}^{*2}$ is a length-4 factorization of K in $\mathcal{P}_{\mathrm{fin},1}(H)$; and it is actually a minimal factorization, because removing one or more atoms from $\mathfrak{c}$ yields an $\mathcal{A}(\mathcal{P}_{\mathrm{fin},1}(H))$-word whose image under $\pi_{\mathcal{P}_{\mathrm{fin},1}(H)}$ has cardinality at most 8 (whereas we have already noted that $|K| = 9$). On the other hand, it is not difficult to check that $A := \{1_H, y, z\}$ is an atom of $\mathcal{P}_{\mathrm{fin},1}(H)$: If $\{1_H, y, z\} = YZ$ for some $Y, Z \in \mathcal{P}_{\mathrm{fin},1}(H)$ with $|Y|, |Z| \ge 2$, then $Y, Z \subseteq \{1_H, y, z\}$ and $Y \cap Z = \{1_H\}$, whence $YZ = \{1_H, y\} \cdot \{1_H, z\} = K \ne A$. This in turn implies that A^{*2} is a length-2 factorization of K in $\mathcal{P}_{\mathrm{fin},1}(H)$, and it is minimal by Proposition 4.1.6(i). So, we are done. □

Corollary 4.2.6. Let H be a monoid. Then $\mathcal{P}_{\mathrm{fin},1}(H)$ is minimally factorial if and only if H is trivial.

Proof. The "if" part is obvious. For the other direction, assume by way of contradiction that $\mathcal{P}_{\mathrm{fin},1}(H)$ is minimally factorial but H is non-trivial. Then $\mathcal{P}_{\mathrm{fin},1}(H)$ is HmF, and we obtain from Theorem 4.2.5 that H is a cyclic group of order 3. Accordingly, let x be a generator of H. By Lemma 3.2.1(i) and Proposition 4.1.6(i), $\mathfrak{a} := \{1_H, x\}^{*2}$ and $\mathfrak{b} := \{1_H, x^2\}^{*2}$ are both minimal factorizations of H in $\mathcal{P}_{\mathrm{fin},1}(H)$. However, $\mathfrak{a} \not\simeq_{\mathcal{P}_{\mathrm{fin},1}(H)} \mathfrak{b}$, because $\mathcal{P}_{\mathrm{fin},1}(H)$ is a reduced monoid. Therefore, $\mathcal{P}_{\mathrm{fin},1}(H)$ is not minimally factorial, so leading to a contradiction and completing the proof. □

At this point, we have completely characterized the correlation between the ground monoid H and whether $\mathcal{P}_{\mathrm{fin},1}(H)$ has factorization properties such as atomicity, BFness, etc., and their minimal counterparts. In most cases, this extends to a characterization of whether the same properties hold for $\mathcal{P}_{\mathrm{fin},\times}(H)$, with the exception of the gap suggested by Theorem 4.2.5 and Corollary 4.2.6. In particular, it still remains to determine the monoids H which make $\mathcal{P}_{\mathrm{fin},\times}(H)$ HmF or minimally factorial. However, what we have shown indicates, we believe, that the arithmetic of $\mathcal{P}_{\mathrm{fin},1}(H)$ and $\mathcal{P}_{\mathrm{fin},\times}(H)$ is robust and ripe for more focused study.

4.3 Cyclic Monoids and Interval Length Sets

For those monoids H with $\mathcal{P}_{\mathrm{fin},1}(H)$ atomic, we have by Proposition 3.2.2 that the semigroup generated by an element $x \in H$ is isomorphic either to $\mathbb{Z}/n\mathbb{Z}$ or to $\mathbb{N}$ under addition. As such, we will concentrate throughout on factorizations in $\mathcal{P}_{\mathrm{fin},0}(\mathbb{Z}/n\mathbb{Z})$ and also mention some results on $\mathcal{P}_{\mathrm{fin},0}(\mathbb{N})$ which are discussed in detail in [FT18, Section 4]. At the end we will return to the general case, where the preceding discussion will culminate in a realization result (Theorem 4.3.7) for sets of minimal lengths of $\mathcal{P}_{\mathrm{fin},1}(H)$.

We invite the reader to review the notation $\hat{x}$ and $\hat{X}$ for lifting elements and subsets of $\mathbb{Z}/n\mathbb{Z}$ to $\mathbb{N}$ (as set in Section 1.3) before reading further. Also, note that, through the whole section, we have replaced the notation $\mathcal{P}_{\mathrm{fin},1}(H)$ with $\mathcal{P}_{\mathrm{fin},0}(H)$ when H is written additively (cf. Example 4.2.2).

Definition 4.3.1. Let $X \in \mathcal{P}_{\mathrm{fin},0}(\mathbb{Z}/n\mathbb{Z})$. We say that a non-empty factorization $\mathfrak{a} = A_1 * \cdots * A_\ell \in \mathcal{Z}(X)$ is a *non-reducible factorization* (or, more briefly, an NR-*factorization*) if $\max \hat{A}_1 + \cdots + \max \hat{A}_\ell = \max \hat{X}$.

This condition on factorizations will allow us to bring calculations up to the integers, where sumsets are more easily understood. More importantly, NR-factorizations are very immediately relevant to our investigation of minimal factorizations.

Lemma 4.3.2. Any NR-factorization in $\mathcal{P}_{\mathrm{fin},0}(\mathbb{Z}/n\mathbb{Z})$ is a minimal factorization.

Proof. Let $\mathfrak{a} = A_1 * \cdots * A_\ell$ be an NR-factorization in $\mathcal{P}_{\mathrm{fin},0}(\mathbb{Z}/n\mathbb{Z})$ of length ℓ, and assume for the sake of contradiction that $\mathfrak{a}$ is not minimal. Since $\mathcal{P}_{\mathrm{fin},0}(\mathbb{Z}/n\mathbb{Z})$ is reduced and commutative, the factorizations which are $\mathcal{P}_{\mathrm{fin},0}(\mathbb{Z}/n\mathbb{Z})$-equivalent to $\mathfrak{a}$ are exactly the words $A_{\sigma(1)} * \cdots * A_{\sigma(\ell)}$, where σ is an arbitrary permutation of the interval $[1, \ell]$. So, on account of Proposition 4.1.6(i), the non-minimality of $\mathfrak{a}$ implies without loss of generality that $\ell \geq 3$ and $X := A_1 + \cdots + A_\ell = A_1 + \cdots + A_k$ for some $k \in [1, \ell - 1]$.

Now, let $x \in X$ such that $\hat{x} = \max \hat{X}$. Using that $\mathfrak{a}$ is an NR-factorization, and considering that, for each $i \in [1, \ell]$, A_i is an atom of $\mathcal{P}_{\mathrm{fin},0}(\mathbb{Z}/n\mathbb{Z})$ and hence $\max \hat{A}_i \geq 1$, it follows from the above that

$$\hat{x} = \max \hat{A}_1 + \max \hat{A}_2 + \cdots + \max \hat{A}_\ell > \max \hat{A}_1 + \cdots + \max \hat{A}_k, \tag{4.3}$$

On the other hand, since $X = A_1 + \cdots + A_k$, there are $a_1 \in A_1, \ldots, a_k \in A_k$ such that $a_1 + \cdots + a_k = x$, from which we see that $\hat{x} \equiv \hat{a}_1 + \cdots + \hat{a}_k \bmod n$. But it follows from (4.3) that $0 \leq \hat{a}_1 + \cdots + \hat{a}_k < \hat{x} < n$, and this implies $\hat{x} \not\equiv \hat{a}_1 + \cdots + \hat{a}_k \bmod n$ (recall that, by definition, $\hat{X} \subseteq [0, n-1]$). We have found a contradiction, showing that $\mathfrak{a}$ was minimal and completing the proof. □

We are aiming to find, for every $k \in [2, n-1]$, a set $X_k \in \mathcal{P}_{\mathrm{fin},0}(\mathbb{Z}/n\mathbb{Z})$ for which $\mathsf{L}^{\mathsf{m}}(X_k) = [2, k]$, on the assumption that $n \geq 5$ is odd: Surprisingly, most of the difficulty lies in showing that $2 \in \mathsf{L}^{\mathsf{m}}(X_k)$. To do this, we first need to produce some large atoms.

Proposition 4.3.3. Let $n \geq 5$ be odd. Then the following sets are atoms of $\mathcal{P}_{\mathrm{fin},0}(\mathbb{Z}/n\mathbb{Z})$:

(i) $B_h := \{\overline{0}\} \cup \{\overline{1}, \overline{3}, \ldots, \overline{h}\}$ for odd $h \in [1, (n-1)/2]$.

(ii) $C_1 := \{\overline{0}, \overline{2}\}$, $C_3 := \{\overline{0}, \overline{2}, \overline{3}, \overline{4}\}$, and $C_\ell := B_\ell \cup \{\overline{\ell + 1}\}$ for odd $\ell \in [5, (n-1)/2]$.

Proof. (i) Let $h \in [1, (n-1)/2]$ be odd, and suppose that $B_h = X + Y$ for some $X, Y \in \mathcal{P}_{\mathrm{fin},0}(\mathbb{Z}/n\mathbb{Z})$. Then X and Y are subsets of B_h, so

$$\max \hat{X} + \max \hat{Y} \leq 2 \max \hat{B}_h = 2h \leq n - 1.$$

Because $\overline{1} \in B_h$, we must have $\overline{1} \in X \cup Y$. However, if $\overline{1} \in X$ and $a \in Y$ for some $a \in B_h \setminus \{\overline{0}\}$, then $1 + \hat{a} \in \hat{X} + \hat{Y}$ is even, which is impossible since $\max \hat{X} + \max \hat{Y} < n$ and $\hat{B}_h \setminus \{0\}$ consists only of odd numbers. Thus $Y = \{\overline{0}\}$, and hence B_h is an atom.

(ii) C_1 is an atom by Lemma 3.2.1(i) and it is not too difficult to see that so is C_3. Therefore, let $\ell \ge 5$ and suppose $C_\ell = X + Y$ for some $X, Y \in \mathcal{P}_{\text{fin},0}(\mathbb{Z}/n\mathbb{Z})$ with $X, Y \neq \{\overline{0}\}$.

First assume that $\overline{\ell+1} \notin X \cup Y$. Then $\hat{X}$ and $\hat{Y}$ consist only of odd integers, so $\hat{x} + \hat{y}$ is an even integer in the interval $[2, n-1]$ for all $x \in X \setminus \{\overline{0}\}$ and $y \in Y \setminus \{\overline{0}\}$. However, $\hat{X} + \hat{Y} = \hat{C}_\ell$ and the only non-zero even element of $\hat{C}_\ell$ is $\ell + 1$. Thus, it must be that $X = \{\overline{0}, x\}$ and $Y = \{\overline{0}, y\}$ for some non-zero $x, y \in \mathbb{Z}/n\mathbb{Z}$, with the result that $|X + Y| \le 4 < |C_\ell|$, a contradiction.

It follows (without loss of generality) that $\overline{\ell+1} \in Y$. Then $X \subseteq \{\overline{0}, \overline{\ell}, \overline{\ell+1}\}$, for, if $x \in X$ with $0 < \hat{x} < \ell$, then $\hat{x} + \ell + 1 \in \hat{C}_\ell$, which is impossible since $\hat{x} + \ell + 1 \in [\max \hat{C}_\ell + 1, n-1]$. This in turn implies that $Y \subseteq \{\overline{0}, \overline{1}, \overline{\ell}, \overline{\ell+1}\}$ for similar reasons. As a consequence,

$$X + Y \subseteq \{\overline{0}, \overline{\ell}, \overline{\ell+1}\} + \{\overline{0}, \overline{1}, \overline{\ell}, \overline{\ell+1}\} = \{\overline{0}, \overline{1}, \overline{\ell}, \overline{\ell+1}, \overline{2\ell}, \overline{2\ell+1}, \overline{2\ell+2}\}$$

However, $\ell + 1 < 2\ell \le n - 1$, so we cannot have $\overline{2\ell} \in X + Y$. Then $2\ell + 1 = n$, in which case $\overline{2\ell+1} = \overline{0}$ and $\overline{2\ell+2} = \overline{1}$; or $2\ell + 1 < n$, so that $\overline{2\ell+1}, \overline{2\ell+2} \notin C_h$ (recall that $\ell \le (n-1)/2$). In either case, we get $X + Y \subseteq \{\overline{0}, \overline{1}, \overline{\ell}, \overline{\ell+1}\}$, hence $|X + Y| \le 4 < |C_\ell|$, which is a contradiction and leads us to conclude that C_ℓ is an atom. □

Now that we have found large atoms in $\mathcal{P}_{\text{fin},0}(\mathbb{Z}/n\mathbb{Z})$, we can explicitly give, for each $k \in [2, n-1]$, an element $X_k \in \mathcal{P}_{\text{fin},0}(\mathbb{Z}/n\mathbb{Z})$ which has a (minimal) factorization of length 2.

Lemma 4.3.4. Fix an odd integer $n \ge 5$ and let $k \in [2, n-1]$. Then the set $X_k = \{\overline{0}, \overline{1}, \ldots, \overline{k}\}$ has an NR-factorization into two atoms in $\mathcal{P}_{\text{fin},0}(\mathbb{Z}/n\mathbb{Z})$.

Proof. We will use the atoms B_h and C_ℓ as defined in Proposition 4.3.3. We claim that, for every $r \in \{0, 1\}$ and all odd $h \in [1, (n-1)/2]$,

$$\hat{B}_{h+2r} + \hat{C}_h = [0, 2h + 2r + 1] \quad \text{and} \quad \hat{C}_{h+2r} + \hat{C}_h = [0, 2r + 2h + 2].$$

We will only demonstrate that $\hat{B}_h + \hat{C}_h = [0, 2h+1]$ (the other cases are an easy consequence). The claim is trivial if $h = 1$ or $h = 3$, so suppose $h \ge 5$. Then

$$\hat{B}_h + \hat{C}_h \supseteq \{1, 3, \ldots, h\} + \{0, h+1\} = \{1, 3, \ldots, 2h+1\}$$

and

$$\hat{B}_h + \hat{C}_h \supseteq \{1, 3, \ldots, h\} + \{1, h\} = \{2, 4, \ldots, 2h\},$$

so $\hat{B}_h + \hat{C}_h \supseteq [0, 2h+1]$. This gives that $\hat{B}_h + \hat{C}_h = [0, 2h+1]$, since $\max \hat{B}_h + \max \hat{C}_h = h + (h+1)$.

Accordingly, we now prove that X_k can be expressed as a two-term sum involving B_h and C_ℓ, for some suitable choices of h and ℓ depending on the parity of k.

Case 1: $k = 2m + 1$ (i.e., k is odd). Then it is immediate to verify that $X_k = B_m + C_m$ if m is odd, and $X_k = B_{m+1} + C_{m-1}$ if m is even.

Case 2: $k = 2m$ (i.e., k is even). Since $X_2 = B_1 + B_1$ and $X_4 = B_1 + B_3$, we may assume $m \geq 3$. Then it is seen that $X_k = C_m + C_{m-2}$ if m is odd, and $X_k = C_{m-1} + C_{m-1}$ if m is even.

We are left to show that the decompositions given above do in fact correspond to minimal factorizations. As an example, consider the case when $k = 2m + 1$ and m is odd (the computation will be essentially identical in the other cases). Then $\max \hat{B}_m + \max \hat{C}_m = 2m + 1$, so that $B_m * C_m$ is an NR-factorization of X_k, and is hence minimal by Proposition 4.3.2. □

Lemma 4.3.5. Fix an odd integer $n \geq 3$ and, for each $k \in [2, n-1]$, let $X_k := \{\overline{0}, \overline{1}, \ldots, \overline{k}\} \in \mathcal{P}_{\text{fin},0}(\mathbb{Z}/n\mathbb{Z})$. Then $\mathsf{L}^{\mathsf{m}}(X_k) = [2, k]$.

Proof. We have already established in Lemma 4.3.4 that X_2 has an NR-factorization of length 2. Now fix $k \in [3, n-1]$ and suppose that, for all $h \in [2, k-1]$ and $\ell \in [2, h]$, X_h has an NR-factorization of length ℓ. Choose some $\ell \in [2, k-1]$; X_{k-1} has an NR-factorization $\mathfrak{a}$, and it is straightforward to see that $\{\overline{0}, \overline{1}\} * \mathfrak{a}$ is an NR-factorization of X_k. Letting ℓ range over $[2, k-1]$, this argument, Lemma 4.3.2, and Lemma 4.3.4 imply that $\mathsf{L}^{\mathsf{m}}(X_k) \supseteq [2, k]$. Moreover, Proposition 4.2.3(i) yields the other inclusion and so we have $\mathsf{L}^{\mathsf{m}}(X_k) = [2, k]$. □

Lemma 4.3.6. Let H be a non-torsion monoid. Then $\mathcal{L}(\mathcal{P}_{\text{fin},0}(\mathbb{N})) \subseteq \mathcal{L}^{\mathsf{m}}(\mathcal{P}_{\text{fin},1}(H))$, and for every $k \geq 2$ there exists $Y_k \in \mathcal{P}_{\text{fin},1}(H)$ with $\mathsf{L}^{\mathsf{m}}(Y_k) = [2, k]$.

Proof. Suppose that $y \in H$ has infinite order, and set $Y := \{y^k : k \in \mathbb{N}\}$. Clearly, Y is a submonoid of H, and the (monoid) homomorphism $(\mathbb{N}, +) \to Y : k \mapsto y^k$ determined by sending 1 to y induces an isomorphism $\mathcal{P}_{\text{fin},0}(\mathbb{N}) \to \mathcal{P}_{\text{fin},1}(Y)$. Since, by Proposition 3.1.2(iii), $\mathcal{P}_{\text{fin},1}(Y)$ is a divisor-closed submonoid of $\mathcal{P}_{\text{fin},1}(H)$, we thus have by parts (iv) and (v) of Proposition 4.1.6 that

$$\mathcal{L}(\mathcal{P}_{\text{fin},0}(\mathbb{N})) = \mathcal{L}^{\mathsf{m}}(\mathcal{P}_{\text{fin},0}(\mathbb{N})) = \mathcal{L}^{\mathsf{m}}(\mathcal{P}_{\text{fin},1}(Y)) \subseteq \mathcal{L}^{\mathsf{m}}(\mathcal{P}_{\text{fin},1}(H)).$$

The rest of the statement now follows from the above and [FT18, Proposition 4.8]. □

Theorem 4.3.7. Assume H is a monoid such that $1_H \neq x^2 \neq x$ for all $x \in H \setminus \{1_H\}$, and set $N := \sup\{\text{ord}_H(x) : x \in H\}$. Then $[2, k] \in \mathcal{L}^{\mathsf{m}}(\mathcal{P}_{\text{fin},1}(H))$ for every $k \in [2, N-1]$.

Proof. If H is non-torsion, this follows immediately from Lemma 4.3.6. Otherwise, let $k \in [2, N-1]$ and $y \in H$ with $n := \text{ord}_H(x) > k$. Then $Y := \langle y \rangle_H \cong \mathbb{Z}/n\mathbb{Z}$, so we have by Proposition 3.1.2(iii), Lemma 4.3.5, and Proposition 4.1.6(iv) that $[2, k] \in \mathcal{L}^{\mathsf{m}}(\mathcal{P}_{\text{fin},1}(Y)) \subseteq \mathcal{L}^{\mathsf{m}}(\mathcal{P}_{\text{fin},1}(H))$. □

Chapter 5

Partitions in the Natural Power Monoid

In [FT18, Section 4], Fan and Tringali took a thorough look at $\mathcal{P}_{\text{fin},0}(\mathbb{N})$. They established, among other things, some significant results on which sets may occur as sets of lengths of elements of $\mathcal{P}_{\text{fin},0}(\mathbb{N})$. Several of their results (which will be addressed further in Chapter 7) specify some elements of $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ with very well-controlled sets of factorizations. To contrast with this, they also proved [FT18, Proposition 4.8], which says that $\mathsf{L}_{\mathcal{P}_{\text{fin},0}(\mathbb{N})}([0,n]) = [2,n]$ for every $n \geq 2$. In essence, the intervals $[0,n] \in \mathcal{P}_{\text{fin},0}(\mathbb{N})$ seem to have the most wild factorization behavior. However, as points are removed from $[0,n]$, one expects a transition to relative tameness as the set of factorizations becomes smaller. In this chapter, we formulate some additional ways of understanding and quantifying the differences between wild and tame factorization behavior.

5.1 Algorithmic Approaches and Partition Type

In this section, we hope to indicate some practical methods that can be implemented to assist in computational approaches to factorization in $\mathcal{P}_{\text{fin},0}(\mathbb{N})$. Specifically, we will outline some inductive approaches (i.e., recursive algorithms) for exhaustively finding all factorizations of a subset into atoms.

Consider the following algorithm for finding the prime factorization of an element $n \in \mathbb{N}$:

- For every prime $p \leq \sqrt{n}$, check if p divides n.
  - If no such p divides n then n is a prime; return the factorization n.
  - If some p does divide n, find a factorization $\mathfrak{a}$ of n/p and return $p * \mathfrak{a}$.

One might wish to imitate this algorithm in $\mathcal{P}_{\text{fin},0}(\mathbb{N})$. We would begin, for a given $X \in \mathcal{P}_{\text{fin},0}(\mathbb{N})$, whether there is some irreducible A which divides X. If A divides X, then there exists some Y with $A + Y = X$; however, since $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ is not cancellative, there is not a unique such Y. This is part of what derails an initial attempt at a factorization algorithm. To make the best of our situation, we have the following definition and proposition.

Definition 5.1.1. Let G be an abelian group, let $H \subseteq G$ be a monoid, and let $X, A \in \mathcal{P}_{\text{fin},0}(H)$. We define the **saturated cofactor of A in X** by

$$X{:}A := \bigcap_{a \in A} (X - a)$$

$X{:}A$ is the largest possible set Y such that $X = A + Y$, in the sense of the following proposition.

Proposition 5.1.2. Let $X, A \in \mathcal{P}_{\text{fin},0}(H)$.

(i) $A + X{:}A \subseteq X$.
(ii) If $X = A + Y$ then $Y \subseteq X{:}A$.
(iii) If A divides X if and only if $A + X{:}A = X$.

Proof. Point (i) is straightforward to see; suppose $a \in A$ and $x \in X{:}A$. Then, by construction, $x \in X - a$ so that $x + a \in (X - a) + a = X$.

For (ii), suppose $y \in Y$ and $a \in A$. Then $a + y \in A + Y = X$, so $y \in X - a$; this was true for any $a \in A$, so $y \in \bigcap_{a \in A}(X - a) = X{:}A$.

To see (iii), first suppose that A divides X; then there is some Y so that $A + Y = X$. Then, using (ii) and then (i), we have that $X = A + Y \subseteq A + (X{:}A) \subseteq X$, whence all the inclusions are equalities. □

Now, if A divides X, $Y := X{:}A$ is a somewhat canonical choice satisfying $A + Y = X$. With this in hand, we can make another attempt at an algorithm for factoring in $\mathcal{P}_{\text{fin},0}(\mathbb{N})$:

- For every atom $A \subsetneqq X$, check if A divides X (that is, whether $A + X{:}A = X$).
  - If no such A divides X then X is an atom; return X.
  - If A divides X, return the set $\{A * \mathfrak{a} : \mathfrak{a} \in \mathcal{Z}_{\mathcal{P}_{\text{fin},0}(H)}(X)\}$.

This algorithm comes up short since it fails in general to obtain the entire set of factorizations of X, as we will see now.

Example 5.1.3. Let $H = \mathbb{N}$ and take $X := [0, n]$ for some odd $n \geq 11$. We can show that $A := \{0, 1, 3\}$ and $B := \{0, 1, 3, \ldots, n - 2, n - 3\}$ are both atoms, and that $X = A + B$ (so $A * B$ is a factorization of X). However, $X{:}A = [0, n] \cap [-1, n - 1] \cap [-3, n - 3] = [0, n - 3] \neq B$ and $X{:}B \neq A$. Thus the above algorithm will find factorizations of the form $A * \mathfrak{b}$ for $\mathfrak{b}$ a factorization of $[0, n - 3]$ (and similarly $B * \mathfrak{a}$ for $\mathfrak{a}$ a factorization of $[0, 3]$), but it will fail to find $A * B$.

This example suggests an adjustment to the algorithm presented just above.

Definition 5.1.4. We define the function fac which assigns to a given X a set of factorizations of X (which we will later assert is the entire set of factorizations of X). Given any $X \in \mathcal{P}_{\text{fin},0}(H)$,

(1) Start with $\mathsf{fac}(X) = \emptyset$.
(2) If $X = \{0\}$, return $\mathsf{fac}(X) = \emptyset$.

```
(3) If $X$ is an atom, return $\mathsf{fac}(X) = \{X\}$.
(4) For each atom $A \subseteq X$, if $A + X{:}A = X$,
    (5) For every subset $Y \subseteq X{:}A$ with $\max(Y) = \max(X{:}A)$, if $A + Y = X$,
        (6) For every $\mathfrak{b} \in \mathsf{fac}(Y)$, add $A * \mathfrak{b}$ to $\mathsf{fac}(X)$.
(7) Return $\mathsf{fac}(X)$.
```

Proposition 5.1.5. For any $X \in \mathcal{P}_{\text{fin},0}(\mathbb{N})$, $\mathsf{fac}(X) = \mathcal{Z}_{\mathcal{P}_{\text{fin},0}(\mathbb{N})}(X)$.

Proof. We can prove this by inducting on the size of X. If $|X| = 1$ then $X = \{1\}$ and $\mathcal{Z}_{\mathcal{P}_{\text{fin},0}(H)}(X) = \emptyset = \mathsf{fac}(X)$ (in accordance with step (2) in the definition of fac). If $|X| = 2$ then, since H is reduced and contains no nontrivial idempotents (as it lies inside G), X is an atom by Lemma 3.2.1. Hence $\mathcal{Z}_{\mathcal{P}_{\text{fin},0}(H)}(X) = \{X\} = \mathsf{fac}(X)$ by step (3).

It is apparent by construction that $\mathsf{fac}(X) \subseteq \mathcal{Z}_{\mathcal{P}_{\text{fin},0}(H)}(X)$, so we only need to show that the other inclusion holds. Suppose $A_1 * \cdots * A_k \in \mathcal{Z}_{\mathcal{P}_{\text{fin},0}(H)}$. Then $A_1 + (A_2 + \cdots + A_k) = X$, so Proposition 5.1.2(iii) implies that $A_1 + (X{:}A_1) = X$. At this point, step (5) of the procedure for generating $\mathsf{fac}(X)$ will find $Y := A_2 + \cdots + A_k$ in its search of all subsets of $X{:}A_1$. By induction, we have that $A_2 * \cdots * A_k \in \mathcal{Z}_{\mathcal{P}_{\text{fin},0}(X)}(Y) = \mathsf{fac}(Y)$. Thus $A_1 * \cdots * A_k \in \mathsf{fac}(X)$, as we wished. □

This algorithm still proceeds by brute force, and can be computationally cumbersome. There are several refinements that we can make by taking advantage of the specific situation of factoring inside $\mathcal{P}_{\text{fin},0}(\mathbb{N})$.

Definition 5.1.6. For $n \geq 0$, we distinguish the following collections of subsets:

$$\begin{aligned}
\mathcal{P}^{(n)} &= \{X \subseteq [0, n] : 0, n \in X\} \\
\mathcal{A}^{(n)} &= \mathcal{A}(\mathcal{P}_{\text{fin},0}(\mathbb{N})) \cap \mathcal{A}^{(n)} \\
\mathcal{N}^{(n)} &= \mathcal{P}^{(n)} \setminus \mathcal{A}^{(n)}
\end{aligned}$$

Remark 5.1.7. Note that

- $\mathcal{P}_{\text{fin},0}(\mathbb{N}) = \bigsqcup_{n=0}^{\infty} \mathcal{P}^{(n)}$.
- For any $m, n \geq 0$, $\mathcal{P}^{(m)} + \mathcal{P}^{(n)} \subseteq \mathcal{P}^{(m+n)}$.

From this we see that the sets $\mathcal{P}^{(n)}$ give a grading of our monoid.

For any nonunit x in a monoid H, the set $\mathcal{Z}_H(x)$ houses the full data of the factorization behavior of x. Since it is sometimes a tall order to understand all of the information of $\mathcal{Z}_H(x)$ at once, we can consider the set $\mathsf{L}_H(x)$ to gain an incomplete yet often adequate understanding of $\mathcal{Z}_H(x)$. With the following definition, we aim to leverage the structure of $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ to formulate an invariant which contains more data than the set of lengths. This will help us in our endeavor to develop a more effecient algorithm for factoring in $\mathcal{P}_{\text{fin},0}(\mathbb{N})$, and also in our larger goal to quanitfy the "wildness" of factorizations of $[0, n]$.

Definition 5.1.8. Let $n \geq 1$. A *partition of* n is $P = (m_1, \dots, m_k)$, where $m_1 \geq \cdots \geq m_k \geq 1$ and $m_1 + \cdots + m_k = n$. Each m_i is said to be a *part* of P, and k is said to be the *length* or number of parts of P. For brevity, we occasionally write $P \vdash n$.

For a factorization $\mathfrak{a} \in \mathcal{F}^*(\mathcal{A}(\mathcal{P}_{\text{fin},0}(\mathbb{N})))$ satisfying $\mathfrak{a} = A_1 * \cdots * A_k$ with $\max(A_1) \geq \cdots \geq \max(A_k)$, the **partition type** of any $\mathfrak{b} \in [\mathfrak{a}]_{\simeq}$ is $\mathsf{ptype}(\mathfrak{b}) := (\max(A_1), \dots, \max(A_k))$.

In general, for any $X \in \mathcal{P}_{\text{fin},0}(\mathbb{N})$ and for any partition $P = (m_1, \dots, m_k)$ of $\max(X)$, we define the **set of factorizations of** X and **set of factorization classes of (partition) type** P to be

$$\mathcal{Z}^P(X) := \{\mathfrak{a} \in \mathcal{Z}(X) : \mathsf{ptype}(\mathfrak{a}) = P\}$$

and

$$\mathsf{Z}^P(X) := \{[\mathfrak{a}]_{\simeq} \in \mathsf{Z}(X) : \mathsf{ptype}(\mathfrak{a}) = P\},$$

respectively. We also define the **set of (partition) types of** X to be

$$\mathsf{T}(X) := \{P \vdash \max(X) : \mathcal{Z}^P(X) \neq \emptyset\}.$$

Note that, since $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ is reduced, for any factorizations $\mathfrak{a}, \mathfrak{b} \in \mathcal{F}^*(\mathcal{A}(\mathcal{P}_{\text{fin},0}(\mathbb{N})))$, $\mathfrak{a} \simeq \mathfrak{b}$ if and only if $\mathfrak{a}$ and $\mathfrak{b}$ are the same up to reordering of factors. This tells us that ptype as written above is well-defined.

Remark 5.1.9. There are some elementary observations to be made which connect factorization behavior with partition type. Say $X \in \mathcal{P}_{\text{fin},0}(\mathbb{N})$ with $n = \max(X)$.

(i) $\mathcal{Z}(X) = \bigsqcup_P \mathcal{Z}^P(X)$, a disjoint union taken over all partitions P of n.

(ii) $\mathcal{Z}^{(n)}(X) = \emptyset$ if and only if X is not an atom.

Though the disjoint union in (i) is not too hard to see, it is not clear that each $\mathcal{Z}^P(X)$ is nonempty. In fact, we will soon see evidence to the contrary in Section 5.2.

To conclude this section, we suggest an outline of another algorithm for calculating sets of factorizations in $\mathcal{P}_{\text{fin},0}(\mathbb{N})$. In contrast with fac from Definition 5.1.4, this one will proceed constructively rather than inductively.

First define, for $X \in \mathcal{P}_{\text{fin},0}(\mathbb{N})$ and $P = (m_1, \dots, m_k)$ a partition of $\max(X)$, $\mathsf{fac\_of\_type}(X, P)$ in the following way: For every $(A_1, \dots, A_k) \in \mathcal{A}^{(m_1)} \times \cdots \times \mathcal{A}^{(m_k)}$, if $A_1 + \cdots + A_k = X$, then add $A_1 * \cdots * A_k$ to $\mathsf{fac\_of\_type}(X, P)$.

After this, we can define a new function, $\mathsf{fac\_by\_type}(X)$. The end result is an algorithm of the following form:

```
(1) Start with $\mathsf{fac\_by\_type}(X) = \emptyset$.
(2) For each partition $P = (m_1, \dots, m_k)$ of $\max(X)$, if $\{0, m_1\} + \cdots + \{0, m_k\} \subseteq X$,
    (3) Add $\mathsf{facs\_of\_type}(X, P)$ to $\mathsf{fac\_by\_type}(P)$.
```

(4) Return $\mathsf{fac\_by\_type}(X)$.

Though this procedure for generating $\mathsf{fac\_by\_type}(X)$ still relies on brute force, it does work fast relative to fac—especially for "small" subsets $X \subseteq \mathbb{N}$. It requires that one computes the sets $\mathcal{A}^{(m)}$ for $m < \max(X)$, which is a computational endeavor in its own right. However, calculating and recording the elements of $\mathcal{A}^{(m)}$ a single time compares favorably with fac, as fac essentially requires the calculation of all atoms which are subsets of the input set X each time the algorithm is used. It also affords some opportunities for avoiding unnecessary calculations; for instance, step (2) identifies which partition types are feasible by examining the subsums $\Sigma(P)$ of P. We will have more to say about subsums in Section 5.3.

5.2 Admissible and Forbidden Types for Intervals

As alluded to in Remark 5.1.9, it is not always clear for which P is $\mathcal{Z}^P(X) \neq \emptyset$ for a given X. In this section we fully address this question in the case when $X = [0, n]$ is an interval.

Proposition 5.2.1. Let $X \in \mathcal{P}_{\text{fin},0}(\mathbb{N})$.

(i) Let $n = \max(X) + b$. $X + \{0, b\} = [0, n]$ if and only if $X \cap \{k, k - b\} \neq \emptyset$ for every $k \in [0, n]$.

(ii) For any $c \geq 1$, $X + \{0, 2c\} = [0, \max(X) + 2c]$ implies that $\{0, c\}$ divides X.

Proof. For (i), we first prove the "only if" direction. Suppose $k \in [0, n]$; then $k \in X + \{0, b\}$. We must have that $k \in X + 0$ or that $k \in X + b$, which is the same as saying $k \in X$ or $k - b \in X$.

Conversely, suppose that $k \in [0, n]$. If $k \in X \subseteq X + \{0, b\}$, we are done. If $k \notin X$, then we have by assumption that $k - b \in X$, meaning $k \in X + b \subseteq X + \{0, b\}$. We conclude that $X + \{0, b\} \supseteq [0, n]$, and the other inclusion is clear since $\max(X + \{0, b\}) = \max(X) + b = n$.

For (ii), we use Proposition 5.1.2. Let $Y = X{:}\{0, c\} = X \cap (X - c)$; we know that $\{0, c\} + Y \subseteq X$, so we just need to show the other inclusion. Suppose $X \supsetneqq \{0, c\} + Y$; then there is $x \in X$ with $x \notin \{0, c\} + Y$. This means that $x \notin X \cap (X - c)$ and $x \notin X \cap (X - c)$; all together, this means $x + c, x - c \notin X$. However, this contradicts part (i), taking $b = 2c$ and $k = x + c$. Thus we must have $X = \{0, c\} + X{:}\{0, c\}$. □

Proposition 5.2.2. Let $n \geq 1$.

(i) For $n \geq 4$, $\mathcal{Z}^{(n-2,2)}([0, n]) = \emptyset$.

(ii) For even $n \geq 4$, $\mathcal{Z}^{(2,\ldots,2)}([0, n]) = \emptyset$.

(iii) For odd $n \geq 5$, $\mathcal{Z}^{(3,2,\ldots,2)}([0, n]) = \emptyset$.

(iv) For even $n \geq 6$, $\mathcal{Z}^{(4,2,\ldots,2)}([0, n]) = \emptyset$.

(v) For odd $n \geq 7$, $\mathcal{Z}^{(5,2,\ldots,2)}([0, n]) = \emptyset$.

Proof. For (i), we can use the second part of Lemma 5.2.1 with $c = 1$ to see that there can be no atom A with $A + \{0, 2\} = [0, n]$.

It is easy to see (ii) because $\{0,2\}$ is the only atom in $\mathcal{A}^{(2)}$, and no sum of the form $\{0,2\}+\cdots+\{0,2\}$ can contain 1, let alone a whole interval.

For (iii), write $n = 2m+1$. We note that $\mathcal{A}^{(3)} = \{\{0,2,3\},\{0,1,3\}\}$. Since 1 belongs to the interval, if $[0,2m+1]$ is to have a factorization of partition type $(3,2,\ldots,2)$, then that factorization must include $\{0,1,3\}$. However, we see that

$$\{0,1,3\}+(m-1)\{0,2\} = \{0,1,3\}+\{0,2,\ldots,2m-2\} = [0,2m-1]\cup\{2m+1\}$$

which does not contain $2m = n-1$, so $[0,2m+1]$ cannot have a factorization of type $(3,2,\ldots,2)$.

The arguments for the remaining parts proceed along similar lines. For (iv), we note that the only atoms in $\mathcal{A}^{(4)}$ which contain 1 are $\{0,1,4\}$ and $\{0,1,2,4\}$. However, if $n = 2m$, we have

$$\{0,1,2,4\}+(m-2)\{0,2\} = \{0,1,4\}+\{0,2,\ldots,2m-4\} = [0,2m-2]\cup\{2m\}$$

which again fails to contain $n-1$.

Finally, we turn to (v). We similarly begin by observing that the only atoms in $\mathcal{A}^{(5)}$ which contain 1 are $\{0,1,5\}$, $\{0,1,2,5\}$, and $\{0,1,3,5\}$. Let $n = 2m+1$. By calculations similar to those above, one can see that $n-2 \notin \{0,1,2,5\}+(m-2)\{0,2\}$ and $n-1 \notin \{0,1,3,5\}+(m-2)\{0,2\}$. □

As we have just seen above, several partition types fail to appear because of the limited number of atoms available in $\mathcal{A}^{(N)}$ for small N. Even in $\mathcal{A}^{(5)}$, where there are a few choices of atoms containing 1, there is no atom which contains both 1 as well as enough "comparably larger" elements closer to 5. However, this issue does not seem to arise for atoms with larger maximum; indeed, in $\mathcal{A}^{(7)}$ we have several choices which fit this requirement: for example, $\{0,1,2,4,6,7\}$, and $\{0,1,3,5,6,7\}$ seem promising if one hopes to produce factorizations of type $(7,2,\ldots,2)$. Indeed, the problems that occur for atoms of sizes between 2 and 5 do not persist, for we have the following.

Our goal now will be to verify that intervals have factorizations of various partition types. To aid in this, we will need a few classes of specifically structured "large atoms" to populate the sets $\mathcal{A}^{(N)}$.

Proposition 5.2.3. Each of the following sets is an atom of $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ for the given values of the parameter h.

(i) $B_{2h-1} := \{0,1,3,\ldots,2h-1\}$ for $h \geq 1$.
(ii) $B_{2h} := \{0,1,3,\ldots,2h-1,2h\}$ for $h \geq 3$.
(iii) $C_{2h} := \{0,2,4,\ldots,2h\}\cup\{1\}$ for $h \geq 2$.
(iv) $C_{2h+1} := \{0,2,4,\ldots,2h\}\cup\{1,2h+1\}$ for $h \geq 3$.

Proof. One who has read ahead will realize that, for $h > 5$, each of these is an instance of a *residually concentrated atom* as defined and explored in Chapter 6. The proof is then finished by citing Proposition 6.1.4 and applying one of the algorithms from Section 5.1 to handle the comparatively cases when $h \leq 5$.

However, we will also give a direct proof which has the benefit of giving insight into the way in which these atoms were constructed, and into how one might generally argue about factorizations in $\mathcal{P}_{\text{fin},0}(\mathbb{N})$.

Beginning with (i), we suppose that there are $X, Y \in \mathcal{P}_{\text{fin},0}(\mathbb{N})$ so that $B_{2h-1} = X + Y$. Without loss of generality, $1 \in X$. Then $Y \subseteq B_{2h-1}$ cannot contain any nonzero elements; if $y \in Y \setminus \{0\}$ then $1 + y \in B_{2h-1}$ is even, a contradiction. Thus $Y = \{0\}$ and B_{2h-1} is an atom.

For (ii), we start similarly by assuming that $B_{2h} = X + Y$ and that $1 \in X$. If $y \in Y \setminus \{0\}$, then $1 + y \in B_{2h}$ is even, meaning that $y = 2h - 1$. We now have that $Y = \{0\}$ or $Y = \{0, 2h-1\}$. In the first case, we are done; but we are nearly done in the second case as well. Since $\max(X) + \max(Y) = 2h$, it must be that $X = \{0, 1\}$, so $B_{2h} = X + Y = \{0, 1\} + \{0, 2h-1\} = \{0, 1, 2h-1, 2h\}$. However, this is impossible since we have assumed that $h \geq 3$.

Turning to (iii), suppose that $C_{2h} = X + Y$ and that $1 \in X$. We know that if Y has a nonzero even element then $C_{2h} = X + Y$ contains the odd element $y + 1 > 1$. Thus $Y \subseteq \{0, 1\}$; but then $C_{2h} \subseteq \{0, 1\} + \{0, 1\} = \{0, 1, 2\}$, which is incompatible with the assumption that $h \geq 2$.

Finally, for (iv), let X and Y be subsets such that $C_{2h+1} = X + Y$, and say $1 \in X$. Similarly to (iii), we see that Y can have no nonzero even elements y *unless* $y = 2h$. This means that the only possibilities are $Y = \{0\}$ (in which case we are done), $Y = \{0, 1\}$, or $\max(Y) = 2h$. These last two cases are symmetric, so suppose $\max(Y) = 2h$. Then $X = \{0, 1\}$ and $Y \subseteq \{0, 1, 2h\}$, so $C_{2h+1} \subseteq \{0, 1\} + \{0, 1, 2h\} = \{0, 1, 2, 2h, 2h+1\}$. This last inequality is seen to be infeasible by recalling that $h \geq 3$. □

We will see that the above constructions are helpful because sums of small numbers of these atoms will be able to form relatively large intervals.

Lemma 5.2.4. If $q \geq r \geq 3$ then $[0, q+r] \in \mathcal{A}^{(q)} + \mathcal{A}^{(r)}$; that is, there are atoms $A_q \in \mathcal{A}^{(q)}$ and $A'_r \in \mathcal{A}^{(q)}$ such that $A_q + A'_r = [0, q+r]$.

Proof. There are several cases to consider; roughly, these amount to when both, one of, or none of q and r is large.

Case 1: $q, r \geq 6$.

Subcase 1.a: $q = 2s$ and $r = 2t + 1$. Then

$$\begin{aligned} B_{2s} + C_{2t+1} &\supseteq \{0, 1\} \cup \{2s-1, 2s\} + \{0, 1, 2, 4, \ldots, , 2t, 2t+1\} \\ &= [0, 2t+2] \cup [2s-1, 2s+2t+1] \end{aligned}$$

and, switching the roles of s and t in the calculation we just saw, we also have

$$B_{2s} + C_{2t+1} \supseteq [0, 2s+1] \cup [2t, 2s+2t+1].$$

Thus we conclude that $[0, 2s+2t+1] \subseteq B_{2s} + C_{2t+1} \subseteq [0, 2s+2t+1]$ and so $B_r + C_q = [0, q+r]$.

Subcase 1.b: $q = 2s+1$ and $r = 2t$. Because the above computation does not depend on which of q and r is smaller, we may recycle that argument to see that $C_q + B_r = [0, q+r]$.

Subcase 1.c: $q = 2s+1$ and $r = 2t+1$.

One can show that $C_q + C_r = [0, q+r]$ by a calculation similar to the one above.

Subcase 1.d: $q = 2s$ and $r = 2t+1$.

Again, similar methods will tell us that $B_q + C_r = [0, q+r]$.

Case 2: $3 \le r \le 5 < q$.

There are only a few possibilities here. Let $A_3 = \{0, 1, 3\}$, $A_4 = \{0, 2, 3, 4\}$, and $A_5 = \{0, 2, 4, 5\}$; then we can see that $B_q + A_r = [0, q+r]$ when q is even and $C_q + A_r = [0, q+r]$ when q is odd.

Case 3: $3 \le r \le q \le 5$.

This leaves only a handful of (q, r) pairs to check; namely $(3, 3)$, $(4, 3)$, $(5, 3)$, $(4, 4)$, $(5, 4)$, and $(5, 5)$. By judicious choice of atoms like A_3, A_4, and A_5 in the previous case, the result can be realized for each of these pairs. □

Proposition 5.2.5. For $h \ge 2$, each of the following subsets of $\mathbb{N}$ is an atom in $\mathcal{P}_{\text{fin},0}(\mathbb{N})$:

(i) $D_{3h} := \{0, 3, 6, \ldots, 3h\} \cup \{1, 3h-1\}$.

(ii) $D_{3h+1} := \{0, 3, 6, \ldots, 3h\} \cup \{1, 3h+1\}$.

(iii) $D_{3h+1} := \{0, 3, 6, \ldots, 3h\} \cup \{1, 3h+1, 3h+2\}$.

Proof. As in the proof of Proposition 5.2.3, we note that these sets may be verified to be atoms by applying Proposition 6.1.4. Yet we will, once again, outline a more direct argument for the sake of clarity.

The arguments for each are similar, but (i) and (ii) are comparatively easier than (iii), so we will just prove (iii). Suppose that there are X and Y so that $D_{3h+2} = X + Y$. We may freely suppose that $1 \in X$ this implies that $Y \subseteq \{0, 3h, 3h+1\}$. We cannot have $\max(Y) = 3h$, for then $\max(X) = 3h + 2 - \max(Y) = 2$. This is impossible since $2 \notin D_{3h+2}$.

If $\max(Y) = 3h+1$ then $X = \{0, 1\}$, so $D_{3h+2} \subseteq \{0, 1\} + \{0, 3h, 3h+1\} = \{0, 1, 3h, 3h+1, 3h+2\}$. However, this cannot be the case since $3, 6 \in D_{3h+2}$. The only remaining possibility is that $Y = \{0\}$, which implies that D_{3h+2} is an atom, as we wished. □

These atoms will help us obtain more decompositions of intervals, with the following rough justification: we know that $3\mathbb{N} + 2\mathbb{N} = \mathbb{N} \setminus \{1\}$. We hope to mimic this for finite subsets by adding a truncated (and slightly modified) copy of $3\mathbb{N}$ to a truncated copy of $2\mathbb{N}$. To make this precise, we have the following lemma.

Lemma 5.2.6. For $q \ge 6$ and $t \ge 2$, there is an atom $A \in \mathcal{A}^{(q)}$ with $A + t\{0, 2\} = [0, q+2t]$.

Proof. This essentially depends on the congruence class of q modulo 6. In the spirit of the argument from the preceding proposition, we demonstrate the result for the most representatively difficult of these cases.

Suppose $q \equiv 0 \pmod 6$, so $q = 3h$ for some even h. We first note that

$$\begin{aligned} D_{3h} + t\{0,2\} &\supseteq \{0,6,\dots,3h\} + \{0,2,4,\dots,2t\} \\ &= \{0,2,4,\dots,3h+2t\} \end{aligned}$$

and similarly that

$$\begin{aligned} D_{3h} + t\{0,2\} &\supseteq \{3,9,\dots,3(h-1)\} \cup \{1,3h-1\} + \{0,2,4,\dots,2t\} \\ &= \{3,5,\dots,3h-3+2t\} \cup \{1,3h-1+2t\} \\ &= \{1,3,5,\dots,3h+2t-1\} \end{aligned}$$

Putting these together, we see that $D_{3h} + t\{0,2\} = [0, 3h+2t]$. □

Remark 5.2.7. The most important details that make this argument work are

(i) $1, q-1 \in D_q$
(ii) $\{0,2,4\} \subseteq t\{0,2\}$

Point (i) enables us to "perturb" $t\{0,2\}$ in a way which ensures that the points near the ends of the desired interval are included. Point (ii) is significant because it allows us to include the middle portion of the interval by covering it with "patches" of length 6. This is also a comforting constraint in light of Proposition 5.2.2, which says that $D_q + \{0,2\}$ cannot be an interval since D_q is an atom.

Theorem 5.2.8. Let $n \geq 1$ and suppose P is a partition of n with $P \notin \{(n-2,2)\} \cup \{(m,2\dots,2) : 2 \leq m \leq 5\}$. Then $\mathcal{Z}^P([0,n]) \neq \emptyset$. In particular, for $n \geq 8$, $|\mathsf{T}([0,n])| = p(n) - 4$, where $p(n)$ is the number of integer partitions of n.

Proof. It is helpful to first classify the ways in which P can avoid being a partition not of the types prescribed above. We have several possibilities.

Case 1: $P = (q, 2, \dots, 2)$ with $m \geq 6$.

Here, Lemma 5.2.6 implies that $\mathcal{Z}^P([0,n]) \neq \emptyset$.

Case 2: P has two parts, both of which are larger than 2.

The content of Lemma 5.2.4 is exactly that $\mathcal{Z}^P([0,n]) \neq \emptyset$ for any such partition.

Case 3: $P = (m_1, \dots, m_k)$ with $k \geq 3$ and $m_1 \geq m_2 \geq 3$.

To resolve this possibility, we proceed by induction. The constraints on P imply that $n \geq 8$. Enumerating the factorizations of $[0,8]$ by hand (or, preferably, by computer) is not prohibitively difficult and indeed confirms that $[0,8]$ has factorizations of every type other than those excluded in the statement of the theorem.

Suppose now that $n > 8$ and, for $8 \leq m < n$, $[0,m]$ has factorizations of each type fitting the description in (iii). Consider $P' = (m_1, \dots, m_{k-1})$. If $k = 3$ then $P' = (m_1, m_2)$ is a partition of $n - m_k$ as described in case 2, and if $k > 3$ then P' is as in case 3. In any event, either by the result from case 2 or by our inductive assumption, we know that $\mathcal{Z}^{P'}([0, n-m_k]) \neq \emptyset$. Taking $\mathfrak{a}' \in \mathcal{Z}^{P'}([0, n-m_k])$, we have that $\mathfrak{a} := \mathfrak{a}' * \{0, m_k\} \in \mathcal{Z}^P([0, n])$.

Case 4: P has smallest part equal to 1.

Finally, we have the partitions described in (iv): those with smallest part equal to 1. The result is reasonable to check by hand for $n = 1, 2, 3$. We proceed by induction on n, assuming that $n > 3$ and that the proposition is true for $m < n$. Let us write $P = (m_1, \ldots, m_k, 1)$.

If $k = 1$, we can see that $C_{n-1} * \{0, 1\} \in \mathcal{Z}^P([0, n])$, where C_{n-1} is one of the atoms constructed in Proposition 5.2.3. Similarly, if $k = 2$ we have by Lemma 5.2.4 that there are atoms $A \in \mathcal{A}^{(m_1)}$ and $A' \in \mathcal{A}^{(m_2)}$ with $A + A' = [0, m_1 + m_2]$, so $A * A' * \{0, 1\} \in \mathcal{Z}^P([0, n])$.

Now assume that $k > 2$ and write $P' = (m_1, \ldots, m_k)$. If $m_k = 1$, then there is some $\mathfrak{a}' \in \mathcal{Z}^{P'}([0, n-1])$ by induction, so that $\mathfrak{a} = \mathfrak{a}' * \{0, 1\} \in \mathcal{Z}^P([0, n])$. However, if $m_k > 1$, set $Q = (m_1, \ldots, m_{k-1}, 1)$ (a partition of $n - m_k$). Again, we have by induction that there is some $\mathfrak{b} \in \mathcal{Z}^Q([0, n-m_k])$. Since $k > 2$ and $m_k \leq m_i$ for all $i \geq 1$, we also have that $m_k < n/2$ and so $n - m_k > m_k$. This allows us to conclude that $\mathfrak{a} = \mathfrak{b} * \{0, m_k\} \in \mathcal{Z}^P([0, n])$, proving what we wished. □

5.3 Subsums and Non-Intervals

We have just seen that intervals of the form $[0, n]$ have factorizations of most partition types. There is a very sharp dichotomy between the wildly varied factorization behavior of intervals and that of any other subset of $\mathbb{N}$, which we will see presently.

We have just seen that intervals of the form $[0, n]$ have factorizations of almost every partition type. However, this section will demonstrate that non-intervals a very far from satisfying this sort of behavior. This helps us begin to distinguish intervals from the rest of $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ in a quantifiable way.

Definition 5.3.1. Let $m_1, \ldots, m_k$ be integers. We will refer to $S = (m_1, \ldots, m_k)$ as a *sequence* of integers. Define the **set of subsums of S** to be $\Sigma(S) := \left\{\sum_{i \in I} m_i : I \subseteq [1, k]\right\}$.

Remark 5.3.2. The notion of "set of subsums" of a sequence can be compared with the similar notion which appears in much of the literature on zero-sum problems in finite abelian groups; see [GHK06, Definition 5.1.1] or many papers on zero-sum problems for similar notation in a different context. Our definition is nearly identical, except for its inclusion of the empty sum. Since we are not focused on the appearance of zero sums, including the empty sum does not put us at any disadvantage in our setting. To the contrary, it is convenient for us as it allows us to express the set of subsums of $S = (m_1, \ldots, m_k)$ as a sum in $\mathcal{P}_{\text{fin},0}(\mathbb{Z})$: $\Sigma(S) = \{0, m_1\} + \cdots + \{0, m_k\}$.

Lemma 5.3.3. Let $m_1, \ldots, m_k$ be positive integers with $m_1 \geq \cdots \geq m_k \geq 1$ and let $n = m_1 + \cdots + m_k$. If $k > n/2$ then $\Sigma(m_1, \ldots, m_k) = [0, n]$.

Proof. To prove this, we will induct on k; if $k = 1 > n/2$, then $n \leq 1$ and the result is trivial. Now suppose $k > 1$ and that, for any sequence T consisting of $\ell < k$ terms satisfying $\ell > \max(\Sigma(T))/2$, $\Sigma(T) = [0, \max(\Sigma(T))]$.

First observe that the maximum term of S is at least the average of the terms of S; that is, $m_1 \geq \frac{n}{k}$. From here, we have

$$\frac{m_2 + \cdots + m_k}{k-1} = \frac{n - m_1}{k-1} \leq \frac{n - n/k}{k-1} = \frac{n}{k} < 2$$

Thus $k - 1 > \frac{m_2 + \cdots + m_k}{2}$ and we can apply the inductive hypothesis to $T := (m_2, \ldots, m_k)$. Now we have $\Sigma(T) = [0, n - m_1]$, so $\Sigma(S) = \{0, m_1\} + [0, n - m_1] = [0, n - m_1] \cup [m_1, n]$. This union of intervals is equal to $[0, n]$ if $m_1 \leq m_2 + \cdots + m_k + 1$, so all that remains is to verify this last inequality.

From our assumption that $k > n/2$, we have $k - 1 \geq (n-1)/2$, so

$$m_2 + \cdots + m_k \geq 1 + \cdots + 1 = k - 1 \geq \frac{n-1}{2}.$$

Using this inequality twice, we have that

$$m_1 = n - (m_2 + \cdots + m_k) \leq n - \frac{n-1}{2} = \frac{n+1}{2} \leq m_2 + \cdots + m_k + 1,$$

exactly as we wished. □

Lemma 5.3.4. Let n be even and let P be a partition into $n/2$ parts. Then one of the following holds:

- $\Sigma(P) = [0, n]$.
- $\Sigma(P) = [0, n] \setminus \{n/2\}$ and $P = (n/2 + 1, 1, \ldots, 1)$.
- $\Sigma(P) = 2 \cdot [0, n/2]$ and $P = (2, \ldots, 2)$

Proof. Let $P = (m_1, \ldots, m_k)$ with $k = n/2$ and $m_1 \geq \cdots \geq m_k \geq 1$. Note that the average size of the parts of P is $(m_1 + \cdots + m_k)/k = n/(n/2) = 2$. Thus the smallest part m_k satisfies $m_k \leq 2$.

If $m_k = 2$ then $m_1 = n - (m_2 + \cdots + m_k) \leq n - (k-1)(2) = n - (n/2 - 1)2 = 2$. Thus we have $m_1 = \cdots = m_k = 2$ and so $\Sigma(P) = \{0, 2\} + \cdots + \{0, 2\} = \{0, 2, \ldots, n\} = 2 \cdot [0, n/2]$ (recalling that $2 \cdot X = \{2x : x \in X\}$, as opposed to $2X = X + X$).

Suppose now that $m_k = 1$. Then, since the average of the parts m_i is equal to 2, we must have that the greatest part $m_1 > 2$. As a result,

$$\frac{m_2 + \cdots + m_k}{k-1} = \frac{n - m_1}{n/2 - 1} < \frac{n-2}{n/2 - 1} = 2,$$

so $k - 1 > (m_2 + \cdots + m_k)/2$; by Lemma 5.3.3, $\Sigma(m - 2, \ldots, m_k) = [0, n - m_1]$.

Now we have $\Sigma(P) = \{0, m_1\} + [0, n - m_1] = [0, n - m_1] \cup [m_1, n]$, so $\Sigma(P) = [0, n]$ provided $2m_1 < n + 1$.

If not, then $2m_1 \geq n+2$, so $m_1 \geq \frac{n+2}{2}$. From this, it follows that

$$m_2 + \cdots + m_k = n - m_1 \leq n - \frac{n+2}{2} = \frac{n}{2} - 1 = k - 1.$$

Since each $m_i \geq 1$, we must have $m_2 = \cdots = m_k = 1$, so $P = (n/2+1, 1, \ldots, 1)$ and $\Sigma(P) = [0, n/2-1] \cup [n/2+1, n]$. □

Theorem 5.3.5. Let $X \in \mathcal{P}_{\text{fin},0}(\mathbb{N})$ and say $n := \max(X)$.

(i) If there is $k \in \mathsf{L}(X)$ with $k > n/2$ then $X = [0, n]$

(ii) If $n/2 \in \mathsf{L}(X)$ then $X = [0, n]$, $X = [0, n] \setminus \{n/2\}$, or $X = (n/2) \cdot \{0, 2\}$

Proof. Begin with (i): let $n = \max(X)$ and let $\mathfrak{a} \in \mathcal{Z}(X)$ be a factorization with length $|\mathfrak{a}| = k$. Then there are integers $m_1 \geq \cdots \geq m_k \geq 1$ and atoms $A_i \in \mathcal{A}^{(m_i)}$ with $\mathfrak{a} = A_1 * \cdots * A_k$. The result is immediate from Lemma 5.3.3, since we have

$$X = A_1 + \cdots + A_k \supseteq \{0, m_1\} + \cdots + \{0, m_k\} = \Sigma(m_1, \cdots, m_k) = [0, n]$$

and we know $X \subseteq [0, \max(X)] = [0, n]$.

The argument for (ii) is identical, except we instead use Lemma 5.3.4. □

Corollary 5.3.6. If $X \in \mathcal{P}_{\text{fin},0}(\mathbb{N})$ and X is not an interval or an atom, then $\mathsf{L}(X) \subseteq [2, \max(X)/2]$. In particular, X has no factorizations of partition type P for any P with $|P| > \max(X)/2$.

Proof. This is immediate, as it is the contrapositive of Theorem 5.3.5. □

5.4 An Aside on Asymptotic Density in Numerical Monoid Rings

To complete our discussion of partition types, we show an application of the idea of partition types to an area seemingly unrelated to power monoids. Rather than being a direct application of the concepts and techniques we have formulated, it represents a more abstract ideological connection to the type of thinking employed in the previous sections. An optimist might hope that the success found in the techniques employed here can be extended far beyond the present scope.

The particular problem addressed here is directly informed and inspired by the work of S. Talbott, C. O'Neill, R. Edmonds, and B. Kubik in [EKOT20]. They show that the *atomic density* of $\mathbb{F}_2[x^2, x^3]$ is asymptotically zero (see their Sections 2 and 3) and go on to give (in Section 4) an exact formula for counting the atoms in $\mathbb{F}_2[x^2, x^3]$ of any fixed degree. Here, we see that their approach can be generalized to show that the atomic density in any numerical monoid polynomial ring is asymptotically zero. This is but one of many questions along these lines in what promises to be a meaningful expansion on the study of numerical monoids.

Definition 5.4.1. A numerical monoid is an additive submonoid $H \leq \mathbb{N}$ such that $\mathbb{N} \setminus H$ is a finite set.

We set $G(H) := \mathbb{N} \setminus H$. The elements of this set are called the *gaps* of H, and $g(H) := |G(H)|$ is called the *genus* of H. Moreover, since $G(H)$ is finite, it has a maximum; $F(H) := \max(G(H))$ is called the *Frobenius number* of H. Finally, for a finite set $S = \{s_1, \ldots, s_r\} \subseteq \mathbb{N}$, we will denote the *numerical monoid generated by* S by $\langle s_1, \ldots, s_r \rangle$.

We wish to study numerical monoid algebras, a family of polynomial rings constructed from numerical monoids. These have been studied before in [ACIS93], [AJ95], and [Bar06], among other places.

Definition 5.4.2. Let H be a numerical monoid and let K be a field. Then the *numerical monoid ring of over* K *associated to* H is $K[H] := K[x^h : h \in H]$.

Note that, if $H = \langle S \rangle$, then we may of course write $K[H] = K[x^s : s \in S]$.

Example 5.4.3. Let $H = \langle 3, 4 \rangle = \{0, 3, 4, 6, 7, 8, \ldots\}$ be the numerical semigroup generated by 3 and 4. Then $G(H) = \{1, 2, 3, 5\}$ and $F(H) = 5$. For any field K, $K[H] = K[x^3, x^4, x^6, x^7, x^8, \ldots] \subseteq K[x]$ is the ring of polynomials with coefficients in K whose x^d coefficient is zero for $d = 1, 2, 3, 5$.

Before moving onward, we set some notation for some quantities which are necessary in the discussion that follows.

Definition 5.4.4. Let K be a field and let $n \in \mathbb{N}$. For any subset $S \subseteq K[x]$, let $S^{(n)} := \{f \in S : \deg(f) = n\}$.

Let H be a numerical monoid, and let q be a prime power. For any $n \in \mathbb{N}$, we define

$$a_q^H(n) := \#\{f \in \mathbb{F}_q[H]^{(n)} : f \text{ is irreducible in } \mathbb{F}_q[H]\}$$

to be the number of irreducibles in $\mathbb{F}_q[H]$ of degree n. For convenience, we write $\rho_q^H(n) := a_q^H(n)/|\mathbb{F}_q[H]^{(n)}|$ for the proportion of degree-n elements of $\mathbb{F}_q[H]$ which are irreducible. The function ρ_q^H is called the *atomic density* of $\mathbb{F}_q[H]$. For the special case when $H = \mathbb{N}$, we let $a_q(n) := a_q^{\mathbb{N}}(n)$ and $\rho_q(n) := \rho_q^{\mathbb{N}}(n)$.

The following can be considered the classical case of the main result of this section.

Proposition 5.4.5. Let q be a prime power and let $n \in \mathbb{N}$. Then the number $a_q(n)$ of degree-n irreducibles in $\mathbb{F}_q[x]$ satisfies $a_q(n) \leq \frac{q^n}{n}$. In particular, $\rho_q(n) \to 0$ as $n \to \infty$.

Proof. This can be argued by counting the elements of $\mathbb{F}_{q^n}$ and then applying the Möbius inversion formula. We do not include the proof here, as it has already been presented well in [DF91, Section 14.3] and [LN97, Section 2.3]. □

We seek to understand the atoms of $\mathbb{F}_q[H]$, for an arbitrary numerical monoid H, in terms of the irreducibles of $\mathbb{F}_q[x]$. This next lemmas will aid us in doing so.

Lemma 5.4.6. Let q be a prime power, let $N \in \mathbb{N}$ be positive, and let $k \geq q^{N-1}$. If $f_1, \ldots, f_k \in \mathbb{F}_q[x]$ with $f_i(0) \neq 0$ then there is some a sub-product f of $f_1 \ldots f_k$ with $f \in \mathbb{F}_q + x^N \mathbb{F}_q[x]$. That is, there are $1 \leq i_1 < \cdots < i_\ell \leq k$ with $f = f_{i_1} \cdots f_{i_\ell} \in \mathbb{F}_q + x^N \mathbb{F}_q[x]$.

Proof. If $N = 1$ then $\mathbb{F}_q + x^N\mathbb{F}_q[x] = \mathbb{F}_q[x]$, so the statement is trivial. Suppose, by way of induction, that the statement of the lemma is true for some $N \geq 1$, and let $f_1, \dots, f_k \in \mathbb{F}_q[x]$ with $k \geq q^N$ and $f_i(0) \neq 0$ for all $i \leq k$.

Since $k \geq qq^{N-1}$, we can inductively apply the lemma q times to find $g_1, \dots, g_q \in \mathbb{F}_q + x^N\mathbb{F}_q[x]$ with $g_1 \cdots g_q | f_1 \cdots f_k$. To be precise, we may treat the q^N polynomials as q separate collections of q^{N-1} polynomials, applying the lemma to each collection. Notice, since each $f_i(0) \neq 0$, that any factor of $f_1 \cdots f_k$ – in particular, each of the g_i – also has nonzero constant term. Replacing g_i with $g_i/g_i(0)$ where needed, we may assume that $g_i(0) = 1$ for every $i \in [1, q]$

Let a_i be the x^N coefficient of g_i, so that $g_i = a_ix^N + 1 \pmod{x^{N+1}}$. We then see, whenever $1 \leq s < t \leq q$, that

$$g_s \cdots g_t \equiv (a_sx^N + 1) \cdots (a_tx^N + 1) \equiv \left(\sum_{i=s}^{t} a_i\right) x^N + 1 \pmod{x^{N+1}}.$$

Now, if one of the q sums $\sum_{i=1}^{t} a_i$ for $t \in [1, q]$ is zero, we see that $h := g_1 \cdots g_t \in \mathbb{F}_q + x^N\mathbb{F}_q[x]$. On the other hand, if none of these sums is zero, then two of them must be the same; suppose, for some $s < t$, that $\sum_{i=1}^{s} a_i = \sum_{i=1}^{t} a_i$. Then $\sum_{i=s+1}^{t} a_i = \sum_{i=1}^{t} a_i - \sum_{i=1}^{s} a_i = 0$, so we have that $h := g_{s+1} \cdots g_t$ has no x^N term. In either case, we have found an $h \in \mathbb{F}_q + x^{N+1}\mathbb{F}_q[x]$ such that $h | g_1 \cdots g_q | f_1 \cdots f_k$, as we wished. □

Lemma 5.4.7. Let K be a field and H be a numerical monoid. Suppose $g \in K[H]$ with $g(0) \neq 0$ and $h \in K[x]$ such that $gh \in K[H]$. Then $h \in K[H]$.

Proof. Suppose to the contrary that $h \notin K[H]$. Then, writing $h = \sum_{j=0}^{n} b_jx^j$, let $d = \min\{j : b_j \neq 0 \text{ and } j \notin H\}$. Let $g = \sum_{i=1}^{m} a_ix^i$; then, since $gh \in K[H]$, the degree-d term of gh in 0. On the other hand, we may also express the degree-d term of gh in terms of the a_i and b_j to get that

$$\sum_{i+j=d} a_ib_j = 0$$

Since $s + t \in H$ for all $s, t \in H$, any pair (i, j) appearing in the above sum must satisfy $i \notin H$ or $j \notin H$. However, $a_i = 0$ for all $i \notin H$ and, because of the minimality of d, $b_j = 0$ for all $j \notin H$ with $j < d$. As a result, the only nonzero term in the sum is the $(i, j) = (0, d)$ term, a_0b_d. Recalling that $a_0 = g(0) \neq 0$ and that $b_d \neq 0$ by definition, $a_0b_d \neq 0$. Thus gh has a nonzero x^d term, which contradicts the assumption that $gh \in K[H]$ and finishes the proof. □

We can now give a characterization of the irreducibles of $\mathbb{F}_q[H]$ in terms of those of $\mathbb{F}_q[x]$.

Proposition 5.4.8. Let H be a numerical monoid and let $f \in \mathbb{F}_q[H]$ be irreducible. Then $f = x^mf_1 \cdots f_k$, where

- $f_1, \dots, f_k \in \mathbb{F}_q[x]$ are irreducible with $f_i(0) \neq 0$ for each $i \in [1, k]$
- $0 \leq m < 2(F(H) + 1)$

- $1 \leq k < q^{F(H)}$.

Proof. For our later convenience and to match our earlier notation, we will let $N = F(H) + 1$. Suppose $f \in \mathbb{F}_q[H]$ is irreducible; if f is also irreducible in $\mathbb{F}_q[x]$ then we are done, so suppose otherwise.

Case 1: x does not divide f. Then we may write $f = f_1 \cdots f_k$ for some irreducibles $f_1, \ldots, f_k \in \mathbb{F}_q[x]$ (and $f_i(0) \neq 0$ for each i). Suppose $k \geq q^{F(H)} = q^{N-1}$; then, by Lemma 5.4.6, there is a $g | f_1 \ldots f_k$ with $g \in \mathbb{F}_q + x^N \mathbb{F}_q[x]t$. Let $h = (f_1 \cdots f_k)/g$. Since $gh = f_1 \cdots f_k = f \in \mathbb{F}_q[H]$, we must have that $g(0) \neq 0$ (otherwise $f(0) = 0$ and f would be divisible by x). Now, by Lemma 5.4.7, $h \in K[H]$, which produces a contradiction to the irreducibility of f in $\mathbb{F}_q[H]$ and implies that $k < q^{F(H)}$.

Case 2: The remaining case is that $f = x^m f_1 \cdots f_k$, with m maximal (so x does not divide $f_1 \cdots f_k$). We need to show that $m < 2(F(H) + 1) = 2N$ and that $k < q$. The first part is easy: if $m \geq 2N$ then we may write $f = x^{m-N}(x^N f_1 \cdots f_k)$. Now we have produced a factorization of f in $\mathbb{F}_q[H]$, for $x^{m-N}, x^N(f_1 \cdots f_k) \in \mathbb{F}_q + x^N \mathbb{F}_q[x] \subseteq \mathbb{F}_q[H]$.

All that remains is to manage k; suppose $k \geq q^{N-1}$. Since x does not divide $f_1 \cdots f_k$, we have that $f_i(0) \neq 0$ for each $i \leq r$ and, as before, Lemma 5.4.6 gives us a $g \in \mathbb{F}_q + x^N \mathbb{F}_q[x]$ with $g | f_1 \cdots f_k$. Then, choosing $h \in \mathbb{F}_q[x]$ so that $gh = f_1 \cdots f_k$, we now wish to show that $x^m h \in \mathbb{F}_q[H]$. Noting that $g(x^m h) \in K[H]$ and $g(0) \neq 0$ (since $g | f_1 \cdots f_k$), Lemma 5.4.7 implies that $x^m h \in K[H]$. This yields a contradiction and we conclude, as in the previous case, that $k < q$. □

Proof. For our later convenience and to match our earlier notation, we will let $N = F(H) + 1$. Suppose $f \in \mathbb{F}_q[H]$ is irreducible; if f is also irreducible in $\mathbb{F}_q[x]$ then we are done, so suppose otherwise.

Case 1: x does not divide f. Then we may write $f = f_1 \cdots f_k$ for some irreducibles $f_1, \ldots, f_k \in \mathbb{F}_q[x]$ (and $f_i(0) \neq 0$ for each i). Suppose $k \geq q^{F(H)} = q^{N-1}$; then, by Lemma 5.4.6, there is a $g | f_1 \ldots f_k$ with $g \in \mathbb{F}_q + x^N \mathbb{F}_q[x]t$. Let $h = (f_1 \cdots f_k)/g$. Since $gh = f_1 \cdots f_k = f \in \mathbb{F}_q[H]$, we must have that $g(0) \neq 0$ (otherwise $f(0) = 0$ and f would be divisible by x). Then we claim that $h \in \mathbb{F}_q[H]$; if not, then there is some $d \in G(H)$ so that the x^d term of h is ax^d for some $a \in \mathbb{F}_q \setminus \{0\}$. Consequently, the x^d coefficient of $f = gh$ is $g(0)a \neq 0$, so $f \notin \mathbb{F}_q[H]$, a contradiction. However, this implies that $g, h \in \mathbb{F}_q[H]$, which produces a contradiction to the irreducibility of f in $\mathbb{F}_q[H]$ and implies that $k < q^{F(H)}$.

Case 2: The remaining case is that $f = x^m f_1 \cdots f_k$, with m maximal (so x does not divide $f_1 \cdots f_k$). We need to show that $m < 2(F(H) + 1) = 2N$ and that $k < q$. The first part is easy: if $m \geq 2N$ then we may write $f = x^{m-N}(x^N f_1 \cdots f_k)$. Now we have produced a factorization of f in $\mathbb{F}_q[H]$, for $x^{m-N}, x^N(f_1 \cdots f_k) \in \mathbb{F}_q + x^N \mathbb{F}_q[x] \subseteq \mathbb{F}_q[H]$.

All that remains is to manage k; suppose $k \geq q^{N-1}$. Since x does not divide $f_1 \cdots f_k$, we have that $f_i(0) \neq 0$ for each $i \leq r$ and, as before, Lemma 5.4.6 gives us a $g \in \mathbb{F}_q + x^N \mathbb{F}_q[x]$ with $g | f_1 \cdots f_k$. Then, choosing $h \in \mathbb{F}_q[x]$ so that $gh = f_1 \cdots f_k$, we now wish to show that $x^m h \in \mathbb{F}_q[H]$. However, since $g(x^m h) = f \in \mathbb{F}_q[H]$, we can argue this in the same manner as in Case 1 (with our $x^m h$ playing the role of h from Case 1). This yields a contradiction and we conclude, as in the previous case, that $k < q$. □

Before finally reaching our main goal for the section, we need one more auxiliary result.

Lemma 5.4.9. Let $n \geq k \geq 1$. Then

$$\sum_{m_1,\ldots,m_k} \frac{1}{m_1 \cdots m_k} \leq \frac{2^{k-1}\log^{k-1}(n)}{n},$$

where the sum is taken over all partitions $(m_1, \ldots, m_k)$ of n into k parts.

Proof. The result trivially holds If $k = 1$ because there is only one partition of n into one part. To show the general case, we proceed by induction on k; suppose the lemma holds for a fixed $k \geq 1$. We will show that it holds for $k + 1$. For our later convenience, let $M := \lfloor n/(k-1) \rfloor$.

$$\begin{aligned}
\sum_{m_1,\ldots,m_{k+1}} \frac{1}{m_1 \cdots m_{k+1}} &\leq \sum_{m=1}^{M} \frac{1}{m} \sum_{m_1,\ldots,m_k} \frac{1}{m_1 \cdots m_k} && \text{(inner sum taken over partitions of } n-m\text{)} \\
&\leq \sum_{m=1}^{M} \frac{1}{m} \frac{2^{k-1}\log^{k}(n-m)}{n-m} && \text{(using the inductive hypothesis)} \\
&\leq 2^{k-1}\log^{k-1}(n) \sum_{m=1}^{M} \frac{1}{m(n-m)} && (1)
\end{aligned}$$

Now, because $\frac{1}{x(n-x)}$ is decreasing on the interval $(0, n/2)$ (and $M = \lfloor n/(k-1) \rfloor \leq n/2$), a right Riemann sum of width-1 rectangles is an under approximation of the area under the graph of $\frac{1}{x(n-x)}$ from $x = 0$ to $x = n/2$. In particular, we may replace the sum in the last line with an integral to get

$$\begin{aligned}
\sum_{m=1}^{M} \frac{1}{m(n-m)} &\leq \int_1^M \frac{1}{x(n-x)}\,dx \\
&= \frac{1}{n}\int_1^M \left[\frac{1}{x} + \frac{1}{n-x}\right] dx && \text{(partial fraction decomposition of the integrand)} \\
&= \frac{1}{n}\left[\int_1^M \frac{1}{x}\,dx + \int_{n-M}^{n-1} \frac{1}{u}\,du\right] && \text{(substituting } u = n-x\text{)} \\
&= \frac{1}{n}\left[\log(M) - \log(1) + \log(n-1) - \log(n-M)\right] \\
&= \frac{1}{n}\log\left(\frac{M(n-1)}{n-M}\right) \\
&\leq \frac{1}{n}\log(n^2) \\
&= \frac{2}{n}\log(n) && (2)
\end{aligned}$$

Finally, stringing together the inequalities (1) and (2), we have

$$\sum_{m_1,\ldots,m_k k+1} \frac{1}{m_1 \cdots m_{k+1}} \leq 2^{k-1} \log^{k-1}(n) \left(\frac{2}{n} \log(n)\right) = \frac{2^k \log^k(n)}{n}$$

As we wished to show. □

Now we are ready to prove our main result.

Theorem 5.4.10. Let H be a numerical monoid and let q be a prime power. Then $\lim\limits_{n\to\infty} \rho_q^H(n) = 0$.

Proof. Let $n \in \mathbb{N}$. Since we wish to calculate a limit as $n \to \infty$, we may assume $n > F(H)$. Any polynomial $f \in \mathbb{F}_q[H]^{(n)}$ has the form $f = \sum_{i=0}^n a_i x^i$, where $a_n \in \mathbb{F}_q \setminus \{0\}$, $a_i = 0$ for all $i \in G(H)$, and the remaining a_i can be freely chosen from $\mathbb{F}_q$. Thus $|\mathbb{F}_q[H]^{(n)}| = (q-1)q^{n-g(H)}$.

Next, we can make crude estimates on the number of each of the types of irreducibles from the characterization given in Proposition 5.4.8. Let $A_{\neq 0}(n) = |\{f \in \mathbb{F}_q[H]^{(n)} : f \text{ is irreducible and } f(0) \neq 0\}|$ and $A_0(n) = |\{f \in \mathbb{F}_q[H]^{(n)} : f \text{ is irreducible and } f(0) = 0\}|$.

Let $M := q^{F(H)}$; $A_{\neq 0}(n)$ is the number of degree-n elements which are products of k irreducibles for some $k \in [1, M-1]$. This quantity is certainly no larger than the number of *all* tuples $(f_1, \ldots, f_k)$ of k irreducibles of $\mathbb{F}_q[x]$ with $k \in [1, M-1]$ and $\deg(f_1 \cdots f_k) = n$. For any such tuple, we know that $\deg(f_1) + \cdots \deg(f_k) = n$, so we can take a sum over all partitions of n into fewer than M parts to help us estimate $A_{\neq 0}(n)$ in the following way:

$$\begin{aligned} A_{\neq 0}(n) &\leq \overbrace{\sum_{\substack{m_1,\ldots,m_k \\ k<M}} a_q(m_1) \cdots a_q(m_k)}^{\substack{\text{Number of degree } n \text{ products} \\ \text{of } k \text{ irreducibles of } \mathbb{F}_q[x]}} \\ &= \sum_{m_1,\ldots,m_k} \left(\frac{q^{m_1}}{m_1}\right) \cdots \left(\frac{q^{m_k}}{m_k}\right) \\ &= \sum_{m_1,\ldots,m_k} \frac{q^n}{m_1 \cdots m_k} \qquad (*) \end{aligned}$$

We can handle $A_0(n)$ similarly; for an irreducible $f \in \mathbb{F}_q[H]$ which can be written as $f = x^m f_1 \cdots f_k$ in $\mathbb{F}_q[x]$, we similarly observe that $\deg(m_1) + \cdots + \deg(m_k) = n - m$. Because m can take on at most $2F(H)+1$ different values, we can estimate $A_0(n)$ (rather carelessly) by using the same bound we found for $A_{\neq 0}(n)$ in $(*)$ another $2F(H)+1$ times. This yields that

$$a_q^H(n) = A_{\neq 0}(n) + A_0(n) \leq (2F(H)+2) \sum_{\substack{m_1,\ldots,m_k \\ k<M}} \frac{q^n}{m_1 \cdots m_k}.$$

Now we are in a position to show that $\lim_{n\to\infty} \rho_q^H(n) = 0$:

$$\begin{aligned}
\rho_q^H(n) &= \frac{a_q^H(n)}{|\mathbb{F}_q[H]^{(n)}|} \\
&\leq \frac{2F(H)+2}{(q-1)q^{n-g(H)}} \sum_{\substack{m_1,\ldots,m_k \\ k<M}} \frac{q^n}{m_1\cdots m_k} \\
&= C\sum_{k=1}^{M} \sum_{m_1,\ldots,m_k} \frac{1}{m_1\cdots m_k} && \text{(letting } C := (2F(H)+2)q^{g(H)}/(q-1)\text{)} \\
&\leq C\sum_{k=1}^{M} \frac{2^{k-1}\log^{k-1}(n)}{n} && \text{(by Lemma 5.4.9)}
\end{aligned}$$

From here we can see that each summand tends to 0 as $n \to \infty$ (and the number M of summands does not depend on n), so it follows that $\rho_q^H(n) \to 0$ as $n \to \infty$. □

Chapter 6

Enumerating Factorizations of Intervals

This chapter will continue to focus on the natural power monoid $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ and on the intervals $[0,n]$. We saw in Theorem 5.2.8 that intervals have factorizations of almost every partition type, which already implies the cardinality of $\mathsf{Z}_{\mathcal{P}_{\text{fin},0}(\mathbb{N})}([0,n])$ is at least about as large as $p(n)$, which is asmpytotic to $\frac{1}{4n\sqrt{3}}\exp\left(\pi\sqrt{\frac{2n}{3}}\right)$ (see [HR00], [Erd42], or [Nat02]). Thus the cardinality of $\mathsf{Z}_{\mathcal{P}_{\text{fin},0}(\mathbb{N})}([0,n])$ grows at least sub-exponentially in n; we show here that it in fact grows exponentially (Theorem 6.3.4). We will build toward this goal in several steps, beginning with the construction of a large and easily parameterizable family of atoms.

6.1 Construction of Residually Concentrated Atoms

Definition 6.1.1. Let $m \geq 2$, $r \in [0, m-1]$. We will say that $S \in \mathcal{P}_{\text{fin},0}(\mathbb{N})$ is **r-concentrated (modulo m)** if

$$|S_{>0} \cap (\mathbb{N}m + t)| \leq 1 \text{ for all } t \in [0, m-1] \setminus \{r\}. \tag{$*$}$$

Equivalently, if S is r-concentrated, then there are (unique) $R, B \subseteq \mathbb{N}$ such that

- $0 \notin R \subseteq \mathbb{N}m + r$;
- $0 \notin B \subseteq \mathbb{N} \setminus (\mathbb{N}m + r)$;
- $S = \{0\} \cup R \cup B$;
- For each $b \in B$ and $s \in S_{>0}$, $s \equiv b \pmod{m}$ implies that $s = b$.

For our later convenience, let $\mathcal{X}_{m,r}$ be the collection of all subsets of $\mathbb{N}$ which are r-concentrated modulo m.

We claim that many elements of the collection $\mathcal{X}_{m,r}$ are atoms of $\mathcal{P}_{\text{fin},0}(\mathbb{N})$. Toward proving this, we give the following lemmas. Throughout what follows, m, r, R, and B are all assumed to be as in Definition 6.1.1 unless otherwise specified.

Lemma 6.1.2. Let $Z := \{0\} \cup R \cup B \in \mathcal{X}_{m,r}$ and suppose that $Z = X + Y$. If there is $x \in X$ with $x \not\equiv 0 \pmod{m}$ then $|Y \cap R| \leq 1$.

Proof. If $Y \cap R = \emptyset$ then the result is trivial, so suppose $y, y' \in Y \cap R$. Then $x + y \equiv x + y' \not\equiv r \pmod{m}$ so, by the r-concentratedness of Z (condition $(*)$ in Definition 6.1.1), $x + y = x + y'$. From here it is clear that $y = y'$ and the result follows. □

The next lemma amounts merely to unpacking a sum decomposition of an r-concentrated set, but a special case of this result will serve us several times in constructing atoms out of members of $\mathcal{X}_{m,r}$.

Lemma 6.1.3. Let $Z := \{0\} \cup R \cup B \in \mathcal{X}_{m,r}$, suppose that $Z = X + Y$, and say $n_1 = |X \cap R|$ and $n_2 = |Y \cap R|$.

(i) Then $|R| \leq (1 + \delta_{\bar{0}}(Y \cap B))n_1 + (1 + \delta_{\bar{0}}(X \cap B))n_2 + \delta_{\bar{0}}(R)n_1 n_2 + |2B \cap R|$, where

$$\delta_{\bar{0}}(S) = \begin{cases} 1 & \text{if } S \text{ has an element } s \equiv 0 \pmod{m} \\ 0 & \text{otherwise.} \end{cases}$$

(ii) If $n_1, n_2 \leq 1$ then $|R| \leq 3 + |2B \cap R|$.

Proof. For (i): first observe that $X = \{0\} \cup (X \cap R) \cup (X \cap B)$ and $Y = \{0\} \cup (Y \cap R) \cup (Y \cap B)$. Then, since each of X and Y is the union of 3 sets, $X + Y$ can be written as a union of 9 sets; namely, the sums of each pair chosen from $\{\{0\}, X \cap R, X \cap B\} \times \{\{0\}, Y \cap R, Y \cap B\}$, as in:

$$\begin{aligned} X + Y &= \{0\} \cup (X \cap R) \cup (X \cap B) + \{0\} \cup (Y \cap R) \cup (Y \cap B) \\ &= \{0\} \cup (X \cap R) \cup (X \cap B) \cup (Y \cap R) \cup (Y \cap B) \\ &\quad \cup (X \cap R + Y \cap B) \cup (X \cap B + Y \cap R) \\ &\quad \cup (X \cap R + Y \cap R) \cup (X \cap B + Y \cap B). \end{aligned}$$

To bound the size of $R = R \cap (X + Y)$, we will look at the intersection of R with each of these 9 sets. Fortunately, it is easy to see that $\{0\}$, $X \cap B$, and $Y \cap B$ have trivial intersection with R and that $X \cap R$ and $Y \cap R$ are already subsets of R. In total, these contribute $|X \cap R| + |Y \cap R| = n_1 + n_2$ to our running estimate for $|R|$.

We turn toward examining the remaining sets; first look at $R \cap (X \cap R + Y \cap B)$. Suppose $x \in X \cap R$ and $y \in Y \cap B$ with $x + y \in R$; then we must have $y \equiv 0 \pmod{m}$. If B has such a y then

$$|R \cap (X \cap R + Y \cap B)| \leq |X \cap R + \{y\}| = |X \cap R| = n_1.$$

Otherwise, $X \cap R + Y \cap B$ does not intersect R, so we have $|R \cap (X \cap R + Y \cap B)| \leq \delta_{\bar{0}}(Y \cap B)n_1$.

If $r \not\equiv 0 \pmod{m}$ then $R \cap (X \cap R + Y \cap R) = \emptyset$; on the other hand, if $r \equiv 0 \pmod{m}$ then $(X \cap R + Y \cap R) \subseteq R$, so we may say that $|R \cap (X \cap R + Y \cap R)| \leq \delta_{\bar{0}}(R)n_1 n_2$. Finally, we may note that $R \cap (X \cap B + Y \cap B) \subseteq R \cap 2B$.

Putting all of these observations together, we obtain our desired estimate that $|R| \leq (1+\delta_{\bar{0}}(Y))n_1 + (1+\delta_{\bar{0}}(X))n_2 + \delta_{\bar{0}}(R)n_1n_2 + |2B \cap R|$.

We can see (ii) by using what we have just proved, and by showing that at most one of $\delta_{\bar{0}}(X \cap B)$, $\delta_{\bar{0}}(Y \cap B)$, and $\delta_{\bar{0}}(R)$ is nonzero. Firstly, note that

$$\delta_{\bar{0}}(R) = \begin{cases} 1 & \text{if } r = 0 \\ 0 & \text{if } r \neq 0 \end{cases}.$$

By construction, B and R don't share any residue classes modulo m, so B cannot have any elements congruent to 0 if R does (and vice-versa). All that remains is to see that $X \cap B$ and $Y \cap B$ cannot both have an element congruent to 0; if they do, then there is a single $b \equiv 0 \,(\mathrm{mod}\ m)$ (by r-concentratedness) with $b \in X \cap Y \cap B$. However, we immediately see that this is impossible because we would have that $2b \in X+Y$, but $2b \equiv b$, which contradicts the r-concentratedness of $X+Y$. Thus $\delta_{\bar{0}}(X \cap B) + \delta_{\bar{0}}(Y \cap B) + \delta_{\bar{0}}(R) \leq 1$ and the inequality from (i) reduces to $|R| \leq (1+\delta_{\bar{0}}(Y \cap B) + (1+\delta_{\bar{0}}(X \cap B)) + \delta_{\bar{0}}(R) + |2B \cap R| \leq 3 + |2B \cap R|$. □

Proposition 6.1.4. Let $m \geq 2$, $r \in [0, m-1]$, and let $A := \{0\} \cup R \cup B$ with R and B as in Definition 6.1.1. If

(1) $B \neq \emptyset$ or $r \neq 0$,
(2) $|R| > 3 + |R \cap 2B|$, and
(3) $B \neq \{b\}$ with $b \equiv 0 \,(\mathrm{mod}\ m)$ such that $\{0, b\}$ divides A,

then A is an atom in $\mathcal{P}_{\mathrm{fin},0}(\mathbb{N})$.

Proof. Suppose $A = X + Y$ with $X, Y \neq \{0\}$.
Case 1: $\max(A) \in B$.

Then there exist $x \in X_{>0}$ and $y \in Y_{>0}$ such that $x + y = \max(A)$. Since, by r-concentratedness, $\max(A)$ is the only element of A of its residue class modulo m, $x, y \not\equiv 0 \,(\mathrm{mod}\ m)$. Now, by two applications of Lemma 6.1.2, $|X \cap R|, |Y \cap R| \leq 1$. Using Lemma 6.1.3, we see that $|R| \leq 3 + |R \cap 2B| < |R|$, a contradiction.
Case 2: $\max(A) \in R$.
Subcase 2A: There are $x \in X \cap B$ and $y \in Y \cap B$ so that $x + y = \max(A)$.

Then $x, y \not\equiv \max(A) \,(\mathrm{mod}\ m)$, so $x, y \not\equiv 0 \,(\mathrm{mod}\ m)$ and we may proceed as in the preceding case.
Subcase 2B: There are $x \in X \cap R$ and $y \in Y \cap R$ so that $x + y = \max(A)$.

Now we have that $r + r \equiv r \,(\mathrm{mod}\ m)$, so $r = 0$. Since $B \subseteq A = X + Y$ but $R + R \subseteq \mathbb{N}m$, we must have $B \subseteq X \cup Y$. However, if $b \in B \cap X$ then $b + y \equiv b \,(\mathrm{mod}\ m)$, which is a violation of the r-concentratedness of A (since $y \neq 0$ and so $b + y \neq b$). It must be that $X \cap B = \emptyset$ (and similarly, $Y \cap B = \emptyset$). Now $A = X + Y = \{0\} \cup (X \cap R) + \{0\} \cup (Y \cap R) \subseteq \mathbb{N}m$, from which we conclude that $B = \emptyset$. This is a contradiction to condition (2) in the statment of the proposition.
Subcase 2C: There are $b \in X \cap B$ and $y \in Y \cap R$ such that $b + y = \max(A)$.

Immediately, we have that $b+r \equiv r \pmod{m}$, so $b \equiv 0 \pmod{m}$ and $r \neq 0$. By Lemma 6.1.2, $|X \cap R| \leq 1$. If $x \in X \setminus \{0, b\}$ then $x \not\equiv 0 \pmod{m}$ and so we also have $|Y \cap R| \leq 1$, whence we may finish by using Lemma 6.1.3 as in Case 1.

Let us suppose, instead, that $X = \{0, b\}$. If $c \in Y \cap B$ then $b + c \equiv c \pmod{m}$, which violates r-concentratedness. Thus $Y \cap B = \emptyset$ and so $Y \subseteq \{0\} \cup R$. From this, we can deduce that since the elements of $A = X + Y$ are either b or congruent to r, $B = \{b\}$. This yields a contradiction of condition (3), finishing the proof. □

6.2 Nacci Numbers and Sets with Bounded Maximum Gap

Definition 6.2.1. Let $S = \{s_0, \dots, s_k\} \subseteq \mathbb{N}$ be a nonempty subset with $s_0 < \cdots < s_k$. We will say that, for each $i \in [1, k]$, s_{i-1} and s_i are *consecutive* elements of S, and we define the **maximum gap** of S $\operatorname{maxgap}(S) := \max\{s_i - s_{i-1} : i \in [1, k]\}$ to be the largest distance between consecutive elements of S.

For a fixed $h \geq 1$, let $\mathcal{G}_h := \{S \subseteq \mathbb{N} : \operatorname{maxgap}(S) \leq h\}$.

For the sake of noting some concrete examples: we have $\operatorname{maxgap}([0, n]) = 1$, $\operatorname{maxgap}(\{0, 2, 4, 6\}) = 2$, and $\operatorname{maxgap}(\{0, 1, 2, 4, 8\}) = 4$. This is meant to be a rudimentary measure of how sparse a set S is.

Our next goal, for a fixed n and h, is to estimate the number of atoms with $\max(A) = n$ and $\operatorname{maxgap}(A) \leq h$; that is, the size of the set $\mathcal{A}^{(n)} \cap \mathcal{G}_h$. We have just shown the existence of a fairly sizable class of atoms (the residually concentrated atoms) with a specific structure. Our next step is to exploit this structure to gain a lower bound on the number of these atoms. Specifically, we would like to give a lower estimate for the number of elements of $\mathcal{A}^{(n)} \cap \mathcal{X}_{m,r} \cap \mathcal{G}_h$, the collection of atoms with maximum equal to n, which are r-concentrated (modulo m), and have a maximum gap of at most h.

Given $S \in \mathcal{A}^{(n)} \cap \mathcal{X}_{m,r}$, we may write $S = \{0\} \cup R \cup B$, where $R \subseteq [1, n] \cap (\mathbb{N}m + r)$ and $B \subseteq \mathbb{N} \setminus (\mathbb{N}m + r)$. We first observe that if $\operatorname{maxgap}(R) \cup \{0, n\} \leq h$ then $\operatorname{maxgap}(S) \leq h$. This is because $R \subseteq S \subseteq [0, n]$, so the consecutive elements of S are at least as close as those of $R \cup \{0, n\}$. Thus, to find a lower bound on the number of possible $S \in \mathcal{P}^{(n)} \cap \mathcal{X}_{m,r} \cap \mathcal{G}_h$, it suffices to find a lower bound on the number of possible R arising from such S. We pivot now to characterizing such R to answer this question.

Lemma 6.2.2. Let $m \geq 2$, $r \in [0, m-1]$, and $h \geq 2$. Then the number of subsets $R \subseteq [1, n] \cap (\mathbb{N}m + r)$ which satisfy $\operatorname{maxgap}(\{0, n\} \cup R) \leq h$ is at least $|\mathcal{E}(\lfloor n/m \rfloor, \lfloor h/m \rfloor)|$, where

$$\mathcal{E}(N, t) := \{\vec{\varepsilon} \in \{0, 1\}^{N+1} : \vec{\varepsilon} \text{ has no more than } t \text{ consecutive zeros}\}.$$

Proof. Begin by defining a map

$$\begin{aligned} \mathcal{E}(N, t) &\to \{R \subseteq [1, (N+1)m] \cap (\mathbb{N}m + r) : \operatorname{maxgap}(R \cup \{0, (N+1)m\}) \leq tm\} \\ \vec{\varepsilon} &\to R_{\vec{\varepsilon}} \end{aligned}$$

where, for any $\vec{\varepsilon} = (\varepsilon_0, \dots, \varepsilon_N) \in \mathcal{E}(N,t)$, we set $R_{\vec{\varepsilon}} := \{\varepsilon_k(km + r) : k \in [0, N]\}$. We wish to show that this map is an injection, which will then prove the statement of the lemma when we take $N = \lfloor n/m \rfloor$ and $t = \lfloor h/m \rfloor$.

Let $\vec{\varepsilon} \in \mathcal{E}(N,t)$. It is immediate that $R_{\vec{\varepsilon}} \subseteq [1, (N+1)m] \cap (\mathbb{N}m + r)$ since $\max(R_{\vec{\varepsilon}}) \leq Nm + r$. To see that $\operatorname{maxgap}(R \cup \{0, (N+1)m\}) \leq tm$, suppose that $km + r$ and $(k+\ell)m + r$ are the consecutive elements of $R_{\vec{\varepsilon}}$ which are farthest apart. Then, by the definition of $\mathcal{E}(N,t)$, $k \leq t$, so $\operatorname{maxgap}(R \cup \{0, (N+1)m\}) \leq (k+\ell)m + r - (km + r) \leq \ell m \leq tm$. What we have just observed amounts to showing that the map $\vec{\varepsilon} \to R_{\vec{\varepsilon}}$ is well-defined and, from here, it is not too difficult to see that the map is injective. □

Now that we can reframe our question in terms of counting special binary sequences, we make an aside on the natue of the growth $\mathcal{E}(N,t)$ as N increases.

Definition 6.2.3. Let $t \geq 1$. We will define a function $f_t : \mathbb{N} \to \mathbb{N}$ by $f_t(N) = 2^{N+1}$ if $N \leq t$ and

$$f_t(N) = f_t(N-1) + \cdots + f_t(N-t-1)$$

for all $N > t$. We shall call $f_t(1), f_t(2), \dots$ the sequence of ***t*-nacci numbers** (as f_1 produces the familiar sequence of *Fibonacci numbers*).

One notes that our notation differs from that of D. Wolfram in [Wol98]. For instance, in his notation, $k = 2$ corresponds to the ordinary Fibonacci numbers, leading us to conclude that our t is the same as his $k+1$. Our initial values are also different; in particular, the first few terms of "traditional" nacci sequences may be zero, with the first nonzero term being equal to 1. Thus our t-nacci numbers are the same, up to some offset of indices, as the usual $(k+1)$-nacci numbers. We keep our choice of notation here for the way in which it assists in counting binary sequences which avoid long strings of 0s, which we will make precise now.

Proposition 6.2.4. Let $\mathcal{E}(N,t)$ be as in Lemma 6.2.2. Then $|\mathcal{E}(N,t)| = f_t(N)$ (with f_t as above).

Proof. For $N \leq t$, any sequence $\vec{\varepsilon} \in \{0,1\}^{N+1}$ trivially satisfies the condition of having no more than t consecutive zeros, so we see easily that $|\mathcal{E}(N,t)| = 2^{N+1} = f_t(N)$. All that remains is to verify that $|\mathcal{E}(N,t)|$ satisfies the same recurrence relation as $f_t(N)$. We set the notation, for each $s \in [0,t]$, that $\mathcal{E}_s(N,t) := \{\vec{\varepsilon} \in \mathcal{E}(N,t) : \varepsilon_s = 1 \text{ and } \varepsilon_i = 0 \text{ for all } i \in [0, s-1]\}$ (note that these sets are all well-defined, for we adopt the convention that our sequences $\vec{\varepsilon}$ are zero-indexed; that is, of the form $\vec{\varepsilon} = (\varepsilon_0, \varepsilon_1, \dots, \varepsilon_N)$).

We can see that $\mathcal{E}(N,t) = \bigsqcup_{s=0}^{t} \mathcal{E}_s(N,t)$ for, given any $\vec{\varepsilon} \in \mathcal{E}(N,t)$, the number of leading zeros in $\vec{\varepsilon}$ is $s \leq t$ (this shows the left-to-right inclusion, and the other is clear by construction). To show the recurrence from here, we merely need to determine $|\mathcal{E}_s(N,t)|$. We have that $\vec{\varepsilon} \in \mathcal{E}_s(N,t)$ if and only if

$$\vec{\varepsilon} = (\underbrace{0, \dots, 0}_{s \text{ leading zeros}}, 1, \vec{\varepsilon}_*),$$

where $\vec{\varepsilon}_*$ has length $N+1-(s+1) = N-s$, so $\vec{\varepsilon}_* \in \mathcal{E}(N-s-1,t)$. Thus $|\mathcal{E}_s(N,t)| = |\mathcal{E}(N-s-1,t)| = f_t(N-s-1)$ which, with the disjoint union above, implies that $|\mathcal{E}(N,t)| = f_t(N-1)+\cdots+f_t(N-t-1) = f_t(N)$. □

Now that we have shown the atoms we are concerned with are counted (in part) by t-nacci numbers, we borrow some general facts from [Wol98] about the rate of growth with respect to N of $f_t(N)$.

Proposition 6.2.5. Let $t \geq 1$.

(i) The limit $r_t := \lim\limits_{N\to\infty} \frac{f_t(N+1)}{f_t(N)}$ exists;

(ii) $2 - 2^{-t} < r_t < 2$.

Proof. Both of these facts (and others) are proved in [Wol98, Lemma 3.6 and Corollary 3.7]. □

6.3 Lower Bounds for Numbers of Atoms and Factorizations

Here we return to our main task of determining lower bounds for (1) the number of atoms with a given maximum and (2) the number of factorizations of an interval. To aid us, we begin with a lemma that makes practical use of a bounded maximum gap as a "density" condition.

Lemma 6.3.1. Let $m \geq 2$, $r \in [0, m-1]$ and $R \subseteq [1,n] \cap (\mathbb{N}m + r)$ such that $\operatorname{maxgap}(\{0,n\} \cup R) \leq h$. If $n \geq kh$ then $|R| \geq k$.

Proof. First observe that $\max(R) \geq \lfloor n/m \rfloor m$ and $\min(R) \leq m$. Now we note that R has $|R|-1$ pairs of consecutive elements, each of which has a difference no larger than h. Thus we get

$$\lfloor n/m \rfloor m - m \leq \max(R) - \min(R) \leq (|R|-1)\operatorname{maxgap}(R) \leq (|R|-1)h,$$

which in turn yields that

$$|R| \geq \frac{(\lfloor n/m \rfloor - 1)m}{h} + 1 = \frac{\lfloor n/m \rfloor - 1}{h/m} + 1 \geq \frac{n/m - 2}{h/m} + 1 = \frac{n - 2/m}{h} + 1 \geq \frac{n}{h} \geq k. \qquad □$$

Now we are in a position to give a lower estimate for the number of *atoms* which are r-concentrated modulo m and have fixed maximum and bounded maximum gap.

Lemma 6.3.2. Let $m \geq 2$, $r \in [0, m-1]$, $R \subseteq [1,n] \cap (\mathbb{N}m + r)$, and $B \subseteq \mathbb{N} \setminus (\mathbb{N}m + r)$ such that, for all $b, b' \in B$, $b \equiv b' \pmod{m}$ only if $b = b'$. Set $A := \{0\} \cup R \cup B$ and say that $n := \max(A)$. If $\operatorname{maxgap}(R) \leq h$, $|B| \geq 2$, and $n > (|B|+3)h$ then A is an atom.

Proof. By construction, A is r-concentrated (modulo m). We can see that the assumption $|B| \geq 2$ satisfies conditions (1) and (3) of Proposition 6.1.4. To guarantee that A is an atom, we need to show that $|R| > 3 + |R \cap 2B|$.

Here, we note that $R \cap 2B \subseteq (\mathbb{N}m + r) \cap 2B$, so it suffices to estimate the number of possible pairs $(a, b) \in B \times B$ such that $a + b \equiv r \,(\mathrm{mod}\ m)$. Because of the assumption that B only has at most one element of each congruence class modulo m, for any $a \in B$ there is at most a single $b \in B$ with $a + b \equiv r$. Thus we have $|(\mathbb{N}m + r) \cap 2B| \leq |B|$ and so

$$|R| > |B| + 3 \geq |(\mathbb{N}m + r) \cap 2B| \geq |R \cap 2B| + 3,$$

where the first inequality follows from applying Lemma 6.3.1 and our assumption that $n \geq (|B| + 3)h$. □

Proposition 6.3.3. Let $h \geq 2$. Then, for sufficiently large n, the number $|\mathcal{A}^{(n)} \cap \mathcal{G}_h|$ of atoms with maximum equal to n and maximum gap bounded by h grows exponentially with respect to n, with a growth rate of at least $\sqrt{(2 - 2^{-\lfloor h/2 \rfloor})}$.

Proof. First fix $m \in [2, h]$ and $r \in [0, m - 1]$. We can count the members of $\mathcal{A}^{(n)} \cap \mathcal{X}_{m,r} \cap \mathcal{G}_h$, which will in turn give a lower bound for $|\mathcal{A}^{(n)} \cap \mathcal{G}_h|$. To enumerate members of the former, we have discovered (via Lemma 6.3.2) that it is sufficient to count the number of

- subsets $B \subseteq [1, n] \setminus (\mathbb{N}m + r)$ such that $|B \cap (\mathbb{N}m + s)| \leq 1$ for all $s \in [0, m - 1]$ and
- subsets $R \subseteq [1, n] \cap (\mathbb{N}m + r)$ such that $\mathrm{maxgap}(\{0, n\} \cup R) \leq h$ and $|R| > |B| + 3$.

To guarantee that the atoms we enumerate have maximum equal to n, let us also impose the restriction that $n \in R \cup B$. Whether $n \in R$ or $n \in B$ depends on if $n \equiv r \,(\mathrm{mod}\ m)$, but in either case we may always ensure that $n \in R \cup B$.

Let us start by determining the number of feasible B. Since $|B \cap (\mathbb{N}m + s)| \leq 1$ for all $s \in [0, m - 1]$, we have $|[1, n] \cap (\mathbb{N}m + s)| \geq \lfloor n/m \rfloor$ choices for each s. Assuming (in the worst case) that $n \not\equiv r \,(\mathrm{mod}\ m)$, one of these choices is not free and we are forced to choose $n \in B$. This still leaves at least $\lfloor n/m \rfloor^{m-2}$ choices for B.

Now we turn to count the subsets R fitting the specifications above. Assume $n \geq (m + 3)h$. If $R \subseteq [1, n] \cap (\mathbb{N}m + r)$ such that $\mathrm{maxgap}(\{0, n\} \cup R) \leq h$ then Lemma 6.3.1 yields that $|R| > m + 2 \geq |B| + 3$ (where the second inequality follows from the restriction that B may have at most one element of any residue class $\not\equiv r$ modulo m). This ensures, by Lemma 6.3.2, that $A := \{0\} \cup R \cup B$ is an atom.

The number of such R as specified above is at least $|\mathcal{E}(\lfloor n/m \rfloor, \lfloor h/m \rfloor)| = f_{\lfloor h/m \rfloor}(\lfloor n/m \rfloor)$ (Lemmas 6.2.2 and 6.2.4), whence Proposition 6.2.5 implies that the number of such R grows exponentially as n increases. That is, there is some absolute constant $C_{h,m}$ which depends possibly on m and h (but not on n) such that

$$|\{R \subseteq [1, n] \cap (\mathbb{N}m + r) : \mathrm{maxgap}(\{0, n\} \cup R)\}| \geq f_{\lfloor h/m \rfloor}(\lfloor n/m \rfloor) \geq C_{h,m}(2 - 2^{-\lfloor h/m \rfloor})^{\lfloor n/m \rfloor}.$$

We conclude then that $|\mathcal{A}^{(n)} \cap \mathcal{G}_h| \geq C_{h,m}(2 - 2^{-\lfloor h/m \rfloor})^{\lfloor n/m \rfloor}$, so $|\mathcal{A}^{(n)} \cap \mathcal{G}_h|$ has an exponential growth rate of at least $(2 - 2^{-\lfloor h/m \rfloor})^{1/m}$. One can further maximize this quantity by choosing $m = 2$ to obtain a growth factor of at least $\sqrt{(2 - 2^{-\lfloor h/2 \rfloor})}$. □

As a consequence of this, we may now produce many distinct factorizations of intervals into atoms.

Theorem 6.3.4. Let $n \geq 2$. Then the number $|\mathsf{Z}([0,n])|$ of factorizations of the interval $[0,n]$ into atoms of $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ grows exponentially with n. Specifically, for every $\varepsilon > 0$ there is a constant C such that $|\mathsf{Z}([0,n])| \geq C\left(\sqrt[4]{2}-\varepsilon\right)^n$ for all sufficiently large n.

Proof. Let $P = (m_1, \dots, m_k)$ be a partition of n such that $m_1 > m_2$. For notational hygiene, set m_1 and let $Q = (m_2, \dots, m_k)$ be the partition of $n-m$ obtained by removing the first part of P.

Observe that, if $A \in \mathcal{A}^{(m_1)} \cap \mathcal{G}_{n-m_1}$ and $\mathfrak{a} \in \mathcal{Z}^Q([0, n-m_1])$, then $A * \mathfrak{a} \in \mathcal{Z}^P([0,n])$. Indeed, we can write $A = \{a_0, a_1, \dots, a_\ell\}$ with $0 = a_0 < a_1 < \cdots < a_\ell = m_1$ such that $a_i - a_{i-1} \leq n - m_1$ for all $i \in [1, \ell]$. Then

$$\pi_{\mathcal{P}_{\text{fin},0}(\mathbb{N})}(A * \mathfrak{a}) = A + [0, n-m_1] = \bigcup_{i=0}^{\ell}([a_i, a_i + n - m_1]) = [0,n],$$

where the last inequality follows since $a_i \leq a_{i-1} + n - m_1$ for each $i \in [1,\ell]$, by the assumption that $\operatorname{maxgap}(A) \leq n - m_1$.

Also, suppose $A, B \in \mathcal{A}^{(m_1)}$ and $\mathfrak{a}, \mathfrak{b} \in \mathcal{Z}^Q([0, n-m_1])$. Then, since $m_1 > m_2 \geq \cdots \geq m_k$, none of the factors in $\mathfrak{b}$ is equal to A (and similarly, none of the factors in $\mathfrak{a}$ is equal to B). Thus $A * \mathfrak{a}$ is equivalent to $B * \mathfrak{b}$ as a factorization in $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ if and only if $A = B$ and $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent factorizations, implying that $|\mathsf{Z}^P([0,n])| \geq |\mathcal{A}^{(m_1)} \cap \mathcal{G}_{n-m_1}| \cdot |\mathsf{Z}^Q([0, n-m_1])|$

From Proposition 6.3.3 it follows that, for any $h \geq 2$, there is a constant C_h such that $|\mathcal{A}^{(M)} \cap \mathcal{G}_h| \geq C_h\left(\sqrt{2-2^{-h/2}}\right)^M$. Putting our observations together and using $M := m_1$, we find that

$$|\mathsf{Z}^P([0,n])| \geq |\mathcal{A}^{(m_1)} \cap \mathcal{G}_{n-m_1}| \cdot \underbrace{|\mathsf{Z}^Q([0, n-m_1])|}_{\geq 1 \text{for large } n} \geq C\left(\sqrt{2-2^{-(n-m_1)}}\right)^{m_1}. \qquad (*)$$

Now we may guarantee the desired rate of growth by making more specific assumptions about the partitions P and Q involved above.

Assume N is large enough that $2^{-\lfloor N/2 \rfloor} < \varepsilon$ and let $n \geq N$. Choose a partition $P = (m_1, \dots, m_k)$ of n such that $m_1 = \lceil n/2 \rceil$; then $Q = (m_2, \dots, m_k)$ is a partition of $\lfloor n/2 \rfloor$. Note that $|\mathsf{Z}^Q([0, \lfloor n/2 \rfloor])| \geq 1$ since $\mathsf{Z}^Q([0, \lfloor n/2 \rfloor]) \neq \emptyset$ by Theorem 5.2.8. Thus, using $(*)$ above for our specific choice of P, we obtain that

$$|\mathsf{Z}([0,n])| \geq |\mathsf{Z}^P([0,n])| \overset{(*)}{\geq} C\left(\sqrt{2-2^{-\lfloor N/2 \rfloor}}\right)^{\lceil n/2 \rceil} \geq C\left(\sqrt{2-\varepsilon}\right)^{\lceil n/2 \rceil} \geq C\left(\sqrt[4]{2}-\varepsilon\right)^n$$

which shows that $\mathsf{Z}([0,n])$ has at least the exponential growth rate we wished to demonstrate. □

In the above argument, there are many choices for partitions P and Q which could have yielded similar growth rates. By the nature of partition types, different choices of P or Q in fact yield disjoint sets of factorizations. This means we could increase our lower estimate of $|\mathsf{Z}([0,n])|$, possibly significantly. Though we will not pursue this here, it is worth remarking that a more thorough probe into this topic and application of deeper analytic tools might yield a meaningfully higher rate of growth for $|\mathsf{Z}([0, n])|$.

Chapter 7

Length Sets in High-Dimensional Integer Lattices

From the point of view of geometry and other fields, setwise sums (also called *Minkowski* sums) of integer lattice points are already well-studied. A geometer might typically be concerned with the nature of Minkowski sum decompositions of polyhedra into convex polyhedra, or other questions with a similar geometric leaning ([Mor93] and [WG07] are some – but certainly not all – of the writings on problems of this sort). A arithmetic combinatorialist, on the other hand, might care about problems such as establishing size estimates on sumsets (comprehensive treatises on the subject include [TV06],[Gry13], or [GR09]). While these are interesting questions on their own, they usually do not consider the algebraic aspects of setwise addition. For instance, when geometers consider decompositions into *convex* polyhedra, one can effectively ignore the highly non-cancellative nature of Minkowsi sum. Working in this way has great practical implications for geometric problems, but leaves open many algebraic questions. We wish to determine how the inherent geometry of the integer lattice interacts with algebraic and factorization theoretic questions.

In particular, we will focus on sets of lengths in $\mathcal{P}_{\text{fin},0}(\mathbb{N}^d)$. Frisch et al. show in [Fri13, FNR19] that rings of integer-valued polynomials realize all possible subsets of $\mathbb{N}$ as sets of factorization lengths. Geroldinger and Schmid give a result of a similar flavor for numerical monoids in [GS18]. Returning to the realm of sumsets and power monoids, Fan and Tringali show some first realization results for length sets in [FT18]. They further conjecture that $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ realizes all possible subsets of $\mathbb{N}$ as sets of factorization lengths. That is:

Conjecture 7.0.1. For any finite $S \subseteq \mathbb{N}_{\geq 2}$, there is $W \in \mathcal{P}_{\text{fin},0}(\mathbb{N})$ such that $\mathsf{L}_{\mathcal{P}_{\text{fin},0}(\mathbb{N})}(W) = S$.

We aim to build toward to this conjecture by realizing new length sets in $\mathcal{P}_{\text{fin},0}(\mathbb{N}^d)$ and by demonstrating some new methods for furthering research in this area.

7.1 Passage Between Power Monoids

It is perhaps most natural to study $\mathcal{P}_{\text{fin}}(G)$, for an abelian group G. In this section we will discuss why one can sensibly reduce to the study of $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ and how we can incorporate $\mathcal{P}_{\text{fin},0}(\mathbb{N}^d)$ to aid us in understanding $\mathcal{P}_{\text{fin},0}(\mathbb{N})$. In broad terms, we will approach this reduction via the following steps:

(1) Reduce from $\mathcal{P}_{\text{fin}}(G)$ to $\mathcal{P}_{\text{fin},0}(G)$; we have done this already in Proposition 3.1.3 and its minimal analogue, Proposition 4.2.1.

(2) Understand subset arithmetic of direct summands of G; by the Fundamental Theorem of Finitely Generated Abelian Groups, this means understanding subset arithmetic in cyclic groups.

    (i) Study $\mathcal{P}_{\text{fin},0}(\mathbb{Z}/n\mathbb{Z})$; a preliminary exploration into this topic can be found in Section 4.3.

    (ii) Study $\mathcal{P}_{\text{fin},0}(\mathbb{Z})$; by Lemma 7.1.1 below, one can instead study $\mathcal{P}_{\text{fin},0}(\mathbb{N})$. Much has been said about this case in Chapters 5 and 6 and in [FT18, Section 4].

(3) Connect $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ to $\mathcal{P}_{\text{fin},0}(\mathbb{N}^d)$; this is the content of this section and, in particular, Theorem 7.1.7.

Lemma 7.1.1. The embedding $\mathcal{P}_{\text{fin},0}(\mathbb{N}) \hookrightarrow \mathcal{P}_{\text{fin},0}(\mathbb{Z})$ induced by the embedding $\mathbb{N} \hookrightarrow \mathbb{Z}$ is an essentially surjective equimorphism. In particular, $\mathcal{L}(\mathcal{P}_{\text{fin},0}(\mathbb{Z})) = \mathcal{L}(\mathcal{P}_{\text{fin},0}(\mathbb{N}))$.

Proof. The "essentially surjective" part is easily verified by noting that, for any $Y \in \mathcal{P}_{\text{fin},0}(\mathbb{Z})$, $Y - \min(Y) \in \mathcal{P}_{\text{fin},0}(\mathbb{N})$. Consequently, $Y = (Y - \min(Y)) + \min(Y)$, so Y is associate to an element of $\mathcal{P}_{\text{fin},0}(\mathbb{N})$.

Now we aim to verify the properties of an essentially surjective equimorphism laid forth in Section 2.3. that the only unit of $\mathcal{P}_{\text{fin},0}(\mathbb{Z})$ is $\{0\}$, which does indeed pull back to $\{0\} \in \mathcal{P}_{\text{fin},0}(\mathbb{N})$, satisfying (E1)

To see (E2) – that the embedding is atom-preserving – suppose $A \in \mathcal{P}_{\text{fin},0}(\mathbb{N})$ is an atom and suppose that $A = X + Y$ for some $X, Y \in \mathcal{P}_{\text{fin},0}(\mathbb{Z})$. Then, letting $x = \min(X)$ and $y = \min(Y)$, there are $X', Y' \in \mathcal{P}_{\text{fin},0}(\mathbb{N})$ with $X = x + X'$ and $Y = y + Y'$. Since $x + y = \min(X) + \min(Y) = \min(A) = 0$, we have that $A = X + Y = (x + X') + (y + Y') = X' + Y'$ is a decomposition in $\mathcal{P}_{\text{fin},0}(\mathbb{N})$, so (with no loss of generality), $X' = \{0\}$. Then $X = \{x\}$ is an invertible element of $\mathcal{P}_{\text{fin},0}(\mathbb{Z})$ (so we actually have $x = 0$), and A is an atom of $\mathcal{P}_{\text{fin},0}(\mathbb{Z})$.

Finally, we verify (E3) Let $X \in \mathcal{P}_{\text{fin},0}(\mathbb{N})$ such that there is a nontrivial factorization $\mathfrak{b} = B_1 * \cdots * B_k \in \mathcal{Z}_{\mathcal{P}_{\text{fin},0}(\mathbb{Z})}(X)$. Then, letting $b_i = \min(B_i)$ and $A_i = B_i - b_i$ for each $i \in [1, k]$, we have that $A_i \simeq_{\mathcal{P}_{\text{fin},0}(\mathbb{Z})} B_i$ and so A_i is an atom of $\mathcal{P}_{\text{fin},0}(\mathbb{Z})$ for each $i \in [1, k]$. Since $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ is a divisor-closed submonoid of $\mathcal{P}_{\text{fin},0}(\mathbb{Z})$, each A_i is also an atom of $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ (this is a straightforward exercise, or a consequence of [FT18, Lemma 2.2]). Furthermore, since $\sum_{i=1}^{k} b_i = \min(A_i) = 0$, we have that $X = A_1 + \cdots + A_k$, so $\mathfrak{a} := A_1 * \cdots * A_k \in \mathcal{Z}_{\mathcal{P}_{\text{fin},0}(\mathbb{N})}(X)$. Since A_i is associate to B_i, it is apparent that $\mathfrak{a} \simeq_{\mathcal{P}_{\text{fin},0}(\mathbb{Z})} \mathfrak{b}$. □

The study of power monoids, in general, is vast and far transcends the already wild behavior of sumsets in $\mathbb{N}$. Indeed; the phenomena we discover in $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ are, in some sense, a lower bound for how pathological we may expect factorization to be in power monoids.

Proposition 7.1.2. Let H be a non-torsion monoid. Then there is an equimorphism from $\mathcal{P}_{\text{fin},0}(\mathbb{N}) \hookrightarrow \mathcal{P}_{\text{fin},1}(H)$, the reduced power monoid of H. In particular, $\mathcal{L}(\mathcal{P}_{\text{fin},0}(\mathbb{N})) \subseteq \mathcal{L}(\mathcal{P}_{\text{fin},1}(H))$.

Proof. This is part of the content of [FT18, Theorem 4.11]. We do not prove all the details here, but one may start by considering the equimorphism induced by the embedding $\mathbb{N} \hookrightarrow H$ which maps $1 \mapsto x$ for some element $x \in H$ with infinite order. □

Of course, there is much more to be studied in $\mathcal{P}_{\text{fin},1}(H)$ when we include subsets of $\langle x, y\rangle \subseteq H$, especially when x and y do not commute. At a minimum, what we have observed above does tell us that every behavior encountered in $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ actually occurs in many more power monoids.

It is not always possible to find a large-scale structural embedding of the factorization behavior of one monoid into another. However, it is possible for the study of factorizations of two monoids to be closely linked in a somewhat weaker sense.

Definition 7.1.3. Let H and K be monoids. We will say that H is **locally transferrable** to K if, for every non-unit $x \in H$, there is a homomorphism $f : H \to K$ such that

(LT1) f is atom-preserving; for every $a \in \mathcal{A}(H)$, $f(a) \in \mathcal{A}(K)$.

(LT2) $f^* : \mathcal{Z}_H(x) \to \mathcal{Z}_K(f(x))$ is a bijection (here f^* is identified with the restriction to $\mathcal{Z}_H(x)$ of the induced map $f^* : \mathcal{F}^*(\mathcal{A}(H)) \to \mathcal{F}^*(\mathcal{A}(K))$).

We will refer to f as an x-**transfer** to K. One may also note that, by (LT1), $f^* : \mathcal{Z}_H(x) \to \mathcal{Z}_K(f(x))$ preserves factorization lengths.

The remaining results in this section highlight the motivating example for the definition of local transferrability; namely, the monoids $\mathcal{P}_{\text{fin},0}(\mathbb{N}^d)$ for $d > 1$.

Lemma 7.1.4. Let $\varphi : H \to K$ be a homomorphism of commutative monoids. If $W \subseteq H$ is a subset with the property:

($*$) For all $x, y, z \in W$, $\varphi(x) = \varphi(y) + \varphi(z)$ if and only if $x = y + z$.

Then we have that

(i) The restriction $\varphi|_W$ is injective.

(ii) $\varphi : \mathcal{P}_{\text{fin},0}(H) \to \mathcal{P}_{\text{fin},0}(K)$ is an atom-preserving map.

(iii) The induced map $\varphi^* : \mathcal{Z}_{\mathcal{P}_{\text{fin},0}(H)}(W) \to \mathcal{Z}_{\mathcal{P}_{\text{fin},0}(K)}(\varphi(W))$ is a (length-preserving) bijection.

(iv) φ is a W-transfer.

Proof. Point (i) is clear by taking $z = 0$ in property ($*$). To see (ii), suppose $A \subseteq W$ and $\varphi(A) = Y + Z$. Then, since $Y, Z \subseteq \varphi(A)$, we may write $Y = \varphi(B)$ and $Z = \varphi(C)$ for some $B, C \subseteq A$. For any $a \in A$, $\varphi(a) \in \varphi(B) + \varphi(C)$, so there are $b \in B$ and $c \in C$ with $\varphi(a) = \varphi(b) + \varphi(c)$. By ($*$), $a = b + c \in B + C$, so $A \subseteq B + C$. A nearly identical argument yields the other inclusion, so that $A = B + C$. Thus, if A is an atom, so too must be $\varphi(A)$.

For (iii), we wish to see that φ^* is a bijection; we will show that φ^* has an inverse. Let $\mathfrak{b} = B_1 * \cdots * B_k \in \mathcal{Z}_{\mathcal{P}_{\text{fin},0}(K)}(\varphi(W))$. Each $B_i = \varphi(A_i)$ for some $A_i \subseteq W$ and, by (i), $\varphi^{-1}(\varphi(A_i)) = A_i$. This implies that the map sending $\mathfrak{b} \mapsto \varphi^{-1}(B_1) * \cdots * \varphi^{-1}(B_k)$ is inverse to φ^*, which is all we needed to show.

Item (iv) is immediate from (i)-(iii). □

Remark 7.1.5. Note that property $(*)$ in Lemma 7.1.4 is *not* equivalent to the restriction $\varphi|_W$ being injective, because we have not made any assumption of algebraic structure on W; in particular, W is not necessarily closed under addition.

Proposition 7.1.6. Let $r \geq 1$ and $W \in \mathcal{P}_{\text{fin},0}(\mathbb{N}^{r+1})$. Let $N > 2\max\{\pi_r(w) : w \in W\}$, where $\pi_r : \mathbb{N}^{r+1} \to \mathbb{N}$ is the projection map from the rth coordinate. Define $\varphi : \mathbb{N}^{r+1} \to \mathbb{N}^r$ by $\varphi(w_1, \ldots, w_{r+1}) = (w_1, \ldots, w_{r-1}, w_r + Nw_{r+1})$. Then

(i) φ is a homomorphism.

(ii) For all $x, y, z \in W$, $\varphi(x) = \varphi(y) + \varphi(z)$ if and only if $x = y + z$.

(iii) $\varphi^* : \mathcal{Z}_{\mathcal{P}_{\text{fin},0}(\mathbb{N}^{r+1})}(W) \to \mathcal{Z}_{\mathcal{P}_{\text{fin},0}(\mathbb{N}^{r})}(\varphi(W))$ is a bijection.

Proof. It is easy to see (i), for this follows from the distributivity of multiplication in $\mathbb{Z}$.

Point (ii) will follow from our choice of N (Recall that $N > 2m$, where $m = \max\{\pi_r(w) : w \in W\}$). Let $x, y, z \in W$, writing $x = (x_1, \ldots, x_{r+1})$, $y = (y_1, \ldots, y_{r+1})$, and $z = (z_1, \ldots, z_{r+1})$. Suppose that $\varphi(x) = \varphi(y) + \varphi(z)$; we will make a coordinate-wise comparison of both sides. We immediately have $x_i = y_i + z_i$ for all $i < r$. For the rth component, we have $x_r + Nx_{r+1} = y_r + Ny_{r+1} + z_r + Nz_{r+1}$, so $x_r - y_r - z_r = N(y_{r+1} + z_{r+1} - x_{r+1})$. Since

$$|x_r - y_r - z_r| \leq ||x_r - y_r| - |z_r|| \leq |x_r - y_r| + |z_r| \leq 2m < N,$$

it must be that both sides of this last equation are equal to zero, so that $x_r = y_r + z_r$ and $x_{r+1} = y_{r+1} + z_{r+1}$. Now we have $x = y + z$, as we wished.

Finally, (iii) follows from (i) and (ii) by Lemma 7.1.4. □

Theorem 7.1.7. Let $d > 1$. Then $\mathcal{P}_{\text{fin},0}(\mathbb{N}^d)$ is locally transferrable to $\mathcal{P}_{\text{fin},0}(\mathbb{N})$.

Proof. We can prove this by inducting on d. Begin with the case $d = 2$ and let $X \in \mathcal{P}_{\text{fin},0}(\mathbb{N}^2)$ with $X \neq \{0\}$. Proposition 7.1.6 gives us an X-transfer to $\varphi : \mathcal{P}_{\text{fin},0}(\mathbb{N}^2) \to \mathcal{P}_{\text{fin},0}(\mathbb{N})$, so we are done.

Now suppose $d > 2$ and assume by way of induction that $\mathcal{P}_{\text{fin},0}(\mathbb{N}^{d-1})$ is locally transferrable to $\mathcal{P}_{\text{fin},0}(\mathbb{N})$. Let $X \in \mathcal{P}_{\text{fin},0}(\mathbb{N}^d)$. As above, Proposition 7.1.6 yields an X-transfer φ to $\mathcal{P}_{\text{fin},0}(\mathbb{N}^{d-1})$. Since we have assumed $\mathcal{P}_{\text{fin},0}(\mathbb{N}^{d-1})$ to be locally transferrable to $\mathcal{P}_{\text{fin},0}(\mathbb{N})$, there is a $\varphi(X)$-transfer $\psi : \mathcal{P}_{\text{fin},0}(\mathbb{N}^{d-1}) \to \mathcal{P}_{\text{fin},0}(\mathbb{N})$. Then $\psi \circ \varphi : \mathcal{P}_{\text{fin},0}(\mathbb{N}^d) \to \mathcal{P}_{\text{fin},0}(\mathbb{N})$ is an X-transfer, so we conclude that $\mathcal{P}_{\text{fin},0}(\mathbb{N}^d)$ is locally transferrable to $\mathcal{P}_{\text{fin},0}(\mathbb{N})$. □

7.2 Independence Arguments in Integer Lattices

Theorem 7.1.7 states that the factorization theory of $\mathcal{P}_{\text{fin},0}(\mathbb{N}^d)$ is locally included in that of $\mathcal{P}_{\text{fin},0}(\mathbb{N})$. Thus, to study $\mathcal{P}_{\text{fin},0}(\mathbb{N}^d)$, we need only look inside $\mathcal{P}_{\text{fin},0}(\mathbb{N})$. Another perspective is the following: to study factorizations in $\mathcal{P}_{\text{fin},0}(\mathbb{N})$, we now have access to the space and geometric intuition afforded to us by working inside the d-dimensional lattice $\mathbb{N}^d$. To make effective use of this intuition, we will formulate and exploit some techniques suitable to this setting.

Throughout this section, all subsets of $\mathbb{N}^d$ that we instantiate will be assumed to be finite and to contain 0 (that is, they will be assumed to be elements of $\mathcal{P}_{\text{fin},0}(\mathbb{N}^d)$). Furthermore, we will drop the subscripts from the sets of factorizations (resp., lengths) of elements of $\mathcal{P}_{\text{fin},0}(\mathbb{N}^d)$, as in $\mathcal{Z}(X)$ (resp., $\mathsf{L}(X)$).

Definition 7.2.1. First we set the notation that, for any subset $X \subseteq \mathbb{Z}^d$, $\mathbb{Z}X := \langle X \rangle_{\mathbb{Z}^d}$ is the subgroup of $\mathbb{Z}^d$ generated by X. We say that subsets U and V of $\mathbb{N}^d$ are **$\mathbb{Z}$-independent (or V is $\mathbb{Z}$-independent from U)** if $\mathbb{Z}U \cap \mathbb{Z}V = \{0\}$.

We will say that subsets $U_1, \dots, U_n \subseteq \mathbb{N}^d$ are **(totally) $\mathbb{Z}$-independent** if, for every pair of disjoint subsets $I, J \subseteq [1, n]$, $\sum_{i \in I} U_i$ and $\sum_{j \in J} U_j$ are $\mathbb{Z}$-independent.

We begin by outlining some basic properties of $\mathbb{Z}$-independence. More often than not, we will use these without mention, or by simply citing "$\mathbb{Z}$-independence."

Proposition 7.2.2. Let $u_1, \dots, u_k \in \mathbb{N}^d$ be nonzero elements.

(i) $\{u_1, \dots, u_k\}$ is a $\mathbb{Z}$-linearly independent set if and only if $\{0, u_1\}, \dots, \{0, u_k\}$ are totally $\mathbb{Z}$-independent.

(ii) If $\sum_i u_i = 0$ then $u_i = 0$ for all $i = 1, \dots, k$.

(iii) If $U_1, \dots, U_k$ are totally $\mathbb{Z}$-independent and $u_i, v_i \in U_i$ for each $i \in [1, k]$, then $\sum_i u_i = \sum_i v_i$ implies that $u_i = v_i$ for $i = 1, \dots, k$.

Proof. (i) is a straightforward exercise in the definition of total $\mathbb{Z}$-independence and (ii) is simply a consequence of $\mathbb{N}^d$ being a reduced monoid.

For (iii), we can induct on k. The result is trivial if $k = 1$, so let $k = 2$. $u_1 + v_1 = u_2 + v_2$ implies that $u_1 - v_1 = v_2 - u_2 \in \mathbb{Z}U_1 \cap \mathbb{Z}U_2 = \{0\}$, so $u_1 = v_1$ and $u_2 = v_2$.

For the inductive step, suppose $k > 2$ and that the result holds for integers smaller than k. The equation $\sum_i u_i = \sum_i v_i$ implies that $u_1 - v_1 = \sum_{i \geq 2}(v_i - u_i)$, and we have that

$$u_1 - v_1 \in \mathbb{Z}U_1 \cap \mathbb{Z}(U_2 + \cdots + U_k) = \{0\},$$

yielding that $u_1 = v_1$ and $\sum_{i \geq 2} u_i = \sum_{i \geq 2} v_i$. By induction, the last equation implies that $u_i = v_i$ for all i and we are done. □

Proposition 7.2.3. Let $U, V \subseteq \mathbb{N}^d$ be $\mathbb{Z}$-independent and let $A_1, \dots, A_k$ be nonzero subsets with $U + V = \sum_{i=1}^k A_i$.

(i) $U = \sum_{i=1}^k U \cap A_i$ and $V = \sum_{i=1}^k V \cap A_i$.

(ii) If $U \cap A_i = \{0\}$ then, for any $V' \subseteq V$, $(U + V') \cap A_i = V' \cap A_i$.

(iii) For each i, $U \cap A_i \neq \{0\}$ or $V \cap A_i \neq \{0\}$.

(iv) $k \leq \max \mathsf{L}(U) + \max \mathsf{L}(V)$.

Proof. (i) For each i, let $u_i \in U \cap A_i$. Then $\sum_i u_i \in \sum_i A_i = U + V$, and there are $u \in U$ and $v \in V$ with $\sum_i u_i = u + v$. By Proposition 7.2.2(ii), $v = 0$ and $\sum_i u_i = u \in U$

The other inclusion is similar; for any $u \in U \subseteq \sum_i A_i$, we can find $u_1, \ldots, u_k \in U$ and $v_1, \ldots, v_k \in V$ such that $u_i + v_i \in A_i$ for each i and $u = \sum_i (u_i + v_i)$. Again by Proposition 7.2.2(ii), $\sum_i v_i = 0$, and each $v_i = 0$ by Proposition 7.2.2(i).

Moving on to (ii), it is sufficient to prove the result for $i = 1$ by renumbering the A_i if necessary. Suppose $u \in U$, $v \in V'$, and $u + v \in A_1$. Since $U \cap A_1 = \{0\}$, we know from (i) that

$$U = \sum_{i \geq 1} U \cap A_i = \sum_{i \geq 2} U \cap A_i,$$

so $u + v + U \subseteq A_1 + \sum_{i \geq 2} A_i \subseteq U + V$. Thus, for any $w \in U$, there are $u' \in U$ and $v' \in V$ so that $u + v + w = u' + v'$. By the $\mathbb{Z}$-independence of U and V, $v' = v$ and so, since $w \in U$ was arbitrary, we actually have that $u + v + U \subseteq U + v$. We can cancel v to get $u + U \subseteq U$. Since $|u + U| = |U| < \infty$, we must actually have $u + U = U$; however, this implies that $u = 0$. We now have that $v = u + v \in A_1$, so $(U + V') \cap A_1 \subseteq V' \cap A_1$. The reverse inclusion is trivial since $0 \in U$, so we are done.

(iii) follows quickly from (ii); suppose $U \cap A_i = \{0\} = V \cap A_i$. Then $A_i = (U + V) \cap A_i = V \cap A_i = \{0\}$, where we used (ii) at the second equal sign. This contradicts the assumption that the A_i are nonzero subsets.

Finally, for (iv): let $\ell = \max \mathsf{L}(U)$ and $m = \max \mathsf{L}(V)$. Without loss of generality, say $[1, s] = \{i : U \cap A_i \neq \{0\}\}$ and $[t, k] = \{i : V \cap A_i \neq \{0\}\}$. Since, by (i), $U = \sum_i U \cap A_i = \sum_{i \leq s} U \cap A_i$, $|[1, s]| \leq \ell$ (similarly, $|[t, k]| \leq m$). By (iii), $[1, k] = [1, s] \cup [t, k]$, so $k \leq \ell + m$ as we wished. □

Lemma 7.2.4. Let $U, V_1, \ldots, V_m \subseteq \mathbb{N}^d$ be totally $\mathbb{Z}$-independent. Suppose each V_j is an atom, and let $V := \sum_j V_j$. Further suppose that $A_1, \ldots, A_k$ are nonzero subsets with $U + V = \sum_{i=1}^k A_i$.

(i) There is a function $f : [1, m] \to [1, k]$ with $V_j \subset A_{f(j)}$ for each $j \in [1, m]$.

(ii) For each $h \in [1, k]$, $\left(\sum\limits_{j \notin f^{-1}(h)} V_j \right) \cap A_h = \{0\}$.

(iii) For each $h \in [1, k]$, $V \cap A_h = \sum\limits_{j \in f^{-1}(h)} V_j$.

Proof. For (i), fix $j \in [1, m]$. Then, by Proposition 7.2.3(i), $V_j = \sum_i V_j \cap A_i$. Since V_j is an atom, only one summand on the right side of this equation can be zero; let $f(j)$ denote the index of that summand. Then we have $V_j = V_j \cap A_{f(j)} \subseteq A_{f(j)}$.

Now let $J := f^{-1}(h) = \{j : V_j \subseteq A_h\}$ and call $V' = \sum_{j \in J} V_j$. Similarly, let $K = [1, m] \setminus J$ and call $V'' = \sum_{j \in K} V_j$. Because $V_1, \ldots, V_m$ are totally $\mathbb{Z}$-independent, V' and V'' are $\mathbb{Z}$-independent.

We can prove (ii) as follows: for each $j \in K$, $V_j \cap A_h = \{0\}$. Proposition 7.2.3(ii) and an easy induction on $|K|$ then yields that $V'' \cap A_h = \{0\}$, completing the proof.

For (iii): a similar induction on $|J|$ shows that, for each $i \neq h$, $V' \cap A_i = \{0\}$. As a result, Proposition 7.2.3(i) implies that $V' = \sum_i V' \cap A_i = V' \cap A_h$. To conclude, we use Proposition 7.2.3(ii) to get that $V \cap A_h = (V' + V'') \cap A_h = V' \cap A_h = V'$. □

Theorem 7.2.5. If $V_1, \ldots, V_m \subseteq \mathbb{N}^d$ are totally $\mathbb{Z}$-independent atoms then $V_1 + \cdots + V_m$ factors uniquely (up to reordering of factors). That is, $\mathsf{Z}(V_1 + \cdots + V_m) = \{V_1 * \cdots * V_m\}$.

Proof. Let $V = V_1 + \cdots + V_m$. The result will essentially follow from Lemma 7.2.4, taking $U = \{0\}$.

Let $A_1, \ldots, A_k$ be atoms with $V = \sum_i A_i$. As in Lemma 7.2.4(i), there is $f : [1, m] \to [1, k]$ with $V_j \subseteq A_{f(j)}$ for each $j \in [1, m]$. We wish to show that f is a bijection.

To see that f is surjective, suppose $h \in [1, k] \setminus f([1, m])$. Then $V_j \cap A_h = \{0\}$ for all $j \in [1, m]$, so Lemma 7.2.4(ii) implies that $A_h = V \cap A_h = \{0\}$. This is a contradiction since A_h is an atom and hence nonzero.

To demonstrate the injectivity of f, let $h \in [1, m]$; Lemma 7.2.4(iii) says that $A_h = V \cap A_h = \sum_{j \in f^{-1}(h)} V_j$. However, since A_h is an atom it must be the case that $|f^{-1}(h)| = 1$.

Now f is a bijection with $V_j = A_{f(j)}$ for each $j \in [1, m]$. This proves that $A_1 * \cdots * A_k \simeq V_1 * \cdots * V_m$, as we wished. □

We will now see how Theorem 7.2.5 allows us to partially recover [FT18, Proposition 4.9] which, for any $\ell \geq 1$, gives sufficient conditions guaranteeing that a subset $U \in \mathcal{P}_{\text{fin},0}(\mathbb{N})$ factors uniquely into exactly ℓ atoms. Before giving the details of this process in the following example, we outline the intuition behind the calculation.

To begin, we will look at the set V of vertices of an ℓ-dimensional cube in $\mathbb{N}^\ell$. We will then iteratively "flatten" the cube in one dimension at a time, essentially by removing a codimension-1 facet and placing it "far away" from the rest of the set. Each step will preserve all relevant factorization data, per Proposition 7.1.6. After flattening to one dimension, we will then use Fan and Tringali's result to verify that our initial construction indeed factored uniquely.

Example 7.2.6. First recall the content of [FT18, Proposition 4.9]: Let $a_1, \ldots, a_\ell \in \mathbb{N}$ such that $a_1 + \cdots + a_i < \frac{1}{2}a_{i+1}$ for $i \in [1, \ell - 2]$ and (if $\ell \geq 2$) $a_1 + \cdots + a_{\ell-1} < a_\ell - a_{\ell-1}$. Then $\mathsf{Z}_{\mathcal{P}_{\text{fin},0}(\mathbb{N})}(\{0, a_1\} + \cdots + \{0, a_\ell\}) = \{\{0, a_1\} * \cdots * \{0, a_\ell\}\}$.

There are many sequences of integers $a_1, \ldots, a_\ell$ satisfying the specified properties; for simplicity, let us use the sequence given by $a_i = b^{i-1}$, for some integer $b \geq 3$.

For $i \in [1, \ell]$, let $e_i \in \mathbb{N}^\ell$ be the ith standard basis vector (whose entries are all zero, except for a 1 in the ith coordinate). Let $V = \{0, e_1\} + \cdots + \{0, e_\ell\}$; by Theorem 7.2.5, V factors uniquely. We will follow the procedure given in Theorem 7.1.7 to "flatten" V into a subset of $\mathbb{N}$ which still factors uniquely. According to this procedure, we need maps $\mathbb{N}^\ell \to \mathbb{N}^{\ell-1} \to \cdots \to \mathbb{N}$.

For $i \in [1, \ell - 1]$, define $\varphi_i : \mathbb{N}^{i+1} \to \mathbb{N}^i$ by $v \mapsto \hat{v} + be_i$ (where $\hat{v}$ is the vector consisting of the first i components of v, and we have identified e_i with the ith standard basis vector in $\mathbb{N}^i$). Let $V_\ell = V$ and $V_i = \varphi_i(V_i + 1)$ for $i < \ell$. By Proposition 7.1.6, φ_i is a homomorphism which essentially preserves the set of factorizations of V_{i+1}. Letting $\varphi := \varphi_1 \circ \cdots \circ \varphi_{\ell-1}$, we have that $U := \varphi(V)$ factors uniquely.

To see what elements actually comprise U, it is enough to check the value of φ on $e_1, \ldots, e_\ell$ (since φ is a homomorpism). It is not too difficult to see that $\varphi(e_i) = b^{i-1}$, so that $U = \{0, 1\} + \{0, b\} + \cdots + \{0, b^{\ell-1}\}$ which is indeed already known to factor uniquely by Fan and Tringali's result.

7.3 Recovering the Two-Lengths Realization Result

Now we are in a position to obtain a high-dimensional version of [FT18, Proposition 4.10] which says that, for any $n \geq 2$, there is an element $U \in \mathcal{P}_{\text{fin},0}(\mathbb{N})$ which has exactly two factorizations: one of length 2, and one of length $n+1$. Applying our viewpoint to Fan and Tringali's result gives us some new insights on their construction and how it may be pushed further. For now, we begin by fixing some notation for our examination of Fan and Tringali's construction.

Definition 7.3.1. Fix an integer $n \geq 2$ and let $d \geq n$. Let $\{e_1, \dots, e_n\}$ be a $\mathbb{Z}$-linearly independent subset of $\mathbb{Z}^d$.

For any $I \subseteq [1, n]$, we will let $e_I := \sum_{i \in I} e_i$. Further, let $f := e_{[1,n]} = \sum_{i=1}^{n} e_i$ and let $g := f + e_n$. Finally, we set

$$U_{n+1} := \sum_{i=1}^{n} \{0, e_i\} + \{0, g\}.$$

We will show (in Theorem 7.3.3) that U_{n+1} has exactly two factorizations. One of these factorizations is apparent from the construction given, since any two element set is an atom of $P_{\text{fin},0}(\mathbb{N}^d)$ (this is an easy exercise, or one can look to [FT18, Proposition 4.1(iv)]). Before proving the Theorem, we construct a class of atoms which will continue to appear through the remainder of the section.

Lemma 7.3.2. Let U_{n+1} be as in Definition 7.3.1, and let $V \subseteq \mathbb{N}^d$ be $\mathbb{Z}$-independent from U_{n+1}. Then the set

$$B := \left(\sum_{i=1}^{n-1} \{0, e_i\} + \{0, g\} + V \right) \cup \{f\}$$

is an atom.

Proof. Suppose that $B = X + Y$. It will suffice to prove that one of X or Y is equal to $\{0\}$.

We first claim that $f \in X \cup Y$; in particular, that f cannot be written as the sum of two nonzero elements of B. Suppose, for a contradiction, that one can write $f = (\delta g + e_I + v) + (\delta' g + e_J + v')$ for some $I, J \subseteq [1, n-1]$, $\delta, \delta' \in \{0, 1\}$, and $v, v' \in V$. By Proposition 7.2.2(iii) and the assumption that V is $\mathbb{Z}$-independent from U_{n+1}, $v = v' = 0$. Since the e_n-coefficient of f is 1, $\delta = \delta' = 0$. Now $f = e_I + e_J$; however, since $n \notin I \cup J$, the e_n-coefficient must be 0, a contradiction.

We also similarly claim that $g \in X \cup Y$. Suppose, for $I, J, \delta, \delta', v, v'$ as above, that $g = (\delta f + e_I + v) + (\delta' f + e_J + v')$. As before, $v = v' = 0$. Now, since the e_n-coefficient of g is 2 but $n \notin I \cup J$, $\delta = \delta' = 1$, implying that $g = 2f + e_I + e_J$. This gives a contradiction, as $2f + e_I + e_J$ has an e_1-coefficient of at least 2, but g has an e_1-coefficient of 1.

We now have that $f, g \in X \cup Y$. Noting that $f + g \notin B$, we may say (without loss of generality) that $f, g \in X$. Now we aim to show that $Y = \{0\}$. Suppose $b := \varepsilon g + e_I + v \in Y$ for some $\varepsilon \in \{0, 1\}$, $I \subseteq [1, n-1]$, and $v \in V$. Then we must have $f + b \in X + Y = B \subseteq U_{n+1} + V$, so choose some $u' \in U_{n+1}$ and $v' \in V$ with $f + b = u' + v'$. By the $\mathbb{Z}$-independence of U_{n+1} and V, it must be that $v' = v$ and $f + \varepsilon g + e_I = u' \in U_{n+1} \cap B$.

We can finish the proof by noting that the only element of $U_{n+1} \cap B$ with an odd e_n coefficient is f, meaning that $\varepsilon = 0$ and $I = \emptyset$. Then $f + b = f + v \in B$, at which point we see that $v = 0$. Thus $Y = \{0\}$ as we wished. □

Theorem 7.3.3. Let $n \geq 2$ and let $e_1, \dots, e_n \in \mathbb{N}^d$ be $\mathbb{Z}$-linearly independent. Set $f = \sum_{i=1}^n e_i$, $g = f + e_n$. Then $U := \sum_{i=1}^n \{0, e_i\} + \{0, g\}$ has exactly two factorizations in $\mathcal{P}_{\text{fin},0}(\mathbb{N}^d)$:

$$\underbrace{\{0, e_1\} * \cdots * \{0, e_n\} * \{0, g\}}_{\text{length } n+1} \quad \text{and} \quad \underbrace{\left[\sum_{i=1}^{n-1} \{0, e_i\} + \{0, g\}\right] \cup \{f\} * \{0, e_n\}}_{\text{length } 2}$$

Our strategy for the proof imitates that of Fan and Tringali's proof of [FT18, Theorem 4.10], but uses $\mathbb{Z}$-linear independence to stand in for parts of their arguments which relied on certain inequalities.

We aim to show that, if $U = X + Y$, then both X and Y are very neatly structured: roughly speaking, it will turn out that each must be the set of vertices of some parallelepiped, thus implying that each factors uniquely (by Theorem 7.2.5). Ranging over all decompositions $X + Y$ will allow us to enumerate all decompositions of U into atoms—of course, there will only end up being two of these, as we will see now.

To help us in this method for understanding sum decompositions, we will use the idea of a *saturated cofactor* as formulated in Definition 5.1.1, as well as Proposition 5.1.2(ii). We recall them here (in notation more convenient to the current situation) for ease of reading. If $Y \subseteq U$ then the *saturated cofactor* of Y in U is $U{:}Y = \bigcap_{y \in Y} (U - y)$. $U{:}Y$ is the largest solution X to the equation $X + Y = U$ in the sense that, if $X + Y = U$, then $X \subseteq U{:}Y$.

Proof. Suppose $U = X + Y$ for some $X, Y \subseteq U$ with $X, Y \neq \{0\}$. First we set some notation by analogy with the proof of [FT18, Theorem 4.10]: $I_X := \{i \in [1, n] : e_i \in X\}$, $I_Y := \{i \in [1, n] : e_i \in Y\}$. For further convenience and compactness, we let $e_I := \sum_{i \in I} e_i$ for any $I \subseteq [1, n]$.

Begin by noting that $[1, n] = I_X \sqcup I_Y$; indeed, for each $i \in [1, n]$, $e_i \in X + Y$, and it must be that $e_i \in X \cup Y$ since all the e_i are linearly independent. Moreover, we cannot have $e_i \in X \cap Y$ since $2e_i \notin U$.

To prove some of the claims which follow, we will use a basic understanding of which linear combinations of the e_i appear as elements of U. Every element of U has one of the following forms:

(F1) e_I: the coefficient to each e_i is either 0 or 1.

(F2) $g + e_I$: the e_n coefficient is either 2 or 3, and all other e_i-coefficients are either 1 or 2.

We now wish to determine the structure of X and Y. For the ease of understanding the argument, we state and prove several small claims about X (which will also hold for Y by symmetry).

Claim A. If $I \subseteq I_X$ then $e_I \in X$.

Suppose $I = J \sqcup K$ with $e_J \in X$ and $e_K \in Y$. If $K \neq \emptyset$ then let $k \in K \subseteq I_X$; we have $2e_k + e_{K\setminus\{k\}} = e_k + e_K \in X + Y$, which is impossible unless $K = [1, n]$, so that $e_K = f$. However, since $1 \in K \subseteq I \subseteq I_X$, this implies that $2e_1 + e_{K\setminus\{k\}} = e_1 + e_K \in X + Y$, a contradiction to (F1)

Claim B. For $I \subsetneqq [1, n]$, $e_I \in X$ only if $I \subseteq I_X$.

Suppose $K := I \cap I_Y$ is nonempty (otherwise, we are done). Then $e_{I\setminus K} + 2e_K = e_I + e_K \in X + Y$ has at least one coefficient equal to 0 and at least one coefficient ≥ 2, which is a contradiction to (F1)

Claim C. If $g + e_I \in X$ then $e_I \in X$.

Let $K := I \cap I_Y$; then $g + e_{I\setminus K} + 2e_K = (g + e_I) + e_K \in X + Y$, which is not possible unless $K = \emptyset$ (since no element of U has more than one coefficient > 2 by (F2)). This implies the desired conclusion.

Claim D. Exactly one of X or Y has an element of the form $g + e_I$.

This is easy to see; if neither X nor Y has such an element then no element of $X + Y$ has a coefficient larger than two. On the other hand, if $g + e_J \in X$ and $g + e_K \in Y$ then $2g + e_J + e_K \in X + Y$, which is a contradiction to (F2) since this element has an e_n-coefficient ≥ 4.

Claim E. If $g + e_H \in X$ for some $H \subseteq [1, n]$ then $g + e_I \in X$ for every $I \subseteq I_X$ with $I \subsetneqq [1, n]$.

Let $I \subseteq I_X$ with $I \subsetneqq [1, n]$. Since $g + e_I \in U = X + Y$, we may write $g + e_I = x + y$ with $x = \delta g + e_J \in X$ (for $\delta \in \{0, 1\}$) and $y = e_K \in Y$ by Claim D. Now $g + e_I = \delta g + e_J + e_K$.

Case 1: If $\delta = 1$ then $e_I = e_J + e_K$, hence $I = J \sqcup K$. Since $I \neq [1, n]$, $K \subsetneqq [1, n]$ and so $K \subseteq I_Y$ by Claim B. However, we now have that $K = \emptyset$ since $K \subseteq I \subseteq I_X$. Thus $g + e_I = g + e_J \in X$, as we wished.

Case 2: If $\delta = 0$ then $g + e_I = e_J + e_K$. We must have $n \in J \cap K$ but, since $I_X \cap I_Y = \emptyset$, Claim B implies that $J + K = [1, n]$ and so $e_J = e_K = f$. Moreover, $I = [1, n-1]$. Now however, since $[1, n-1] \subseteq I_X$, we have $e_1 + f \in X + Y$, which is a contradiction (no element of U has an e_n-coefficient of 1 and an e_1-coefficient of 2), finishing the proof of the claim.

Assume without loss of generality that $g \in X$. If $I_X = \emptyset$ then $I_Y = [1, n]$ so $X = \{0, g\}$ by Claims B and C, and $Y = \sum_{i=1}^{n}\{0, e_i\}$ by Claim A. By Theorem 7.2.5, Y factors uniquely and we have $\{0, e_1\} * \cdots \{0, e_n\} * \{0, g\} \in \mathcal{Z}_{\mathcal{P}_{\mathrm{fin},0}(\mathbb{N}^n)}(U)$.

Now suppose $I_X \neq \emptyset$. Then, by Claims C and E,

$$X \supseteq \{0, g\} + \sum_{i \in I_X} \{0, e_i\}. \tag{1}$$

We can completely determine the structure of Y. First observe that we cannot have $f = e_{[1,n]} \in Y$ since we would then have $(g + e_{I_X}) + f \in X + Y$, but this is not an element of U. This allows us to use Claims B, A, and D to say that $Y = \sum_{i \in I_Y}\{0, e_i\}$ (with $I_Y \neq \emptyset$, otherwise $Y = \{0\}$). Since the e_i are linearly independent, the $\{0, e_i\}$ are $\mathbb{Z}$-independent, so Y factors uniquely as the sum of the $\{0, e_i\}$ for $i \in I_Y$ by Theorem 7.2.5.

Now we can say more about the structure of X by calculating the saturated cofactor of Y in U. By Proposition 5.1.2, we have

$$X \subseteq U{:}Y = \bigcap_{y \in Y} (U - y) = \bigcap_{K \subseteq I_Y} \underbrace{\{e_I - e_K, g + e_I - e_K : I \subseteq [1,n]\}}_{=:U_K} \tag{2}$$

Recalling the forms (F1) and (F2) of all elements of U that we outlined earlier, we can similarly express the forms of elements of $U{:}Y$:

(F1′) e_I for $I \subseteq I_X$. To see this, observe that $e_I = e_{I \cup K} - e_K \in U_K$ for any $K \subseteq I_Y$. On the other hand note that, for $H \subseteq [1,n]$ with $H \cap I_Y \neq \emptyset$, $g + e_H \notin U_{H \cap I_Y}$, so these are the only elements of form (F1) which remain in $U{:}Y$.

(F2′) $g + e_I$ for $I \subseteq I_X$. For this, we observe $g + e_{I \cup K} - e_K \in U_K$. Similar to the argument just above, we see that $g + e_H \notin U_{H \cap I_Y}$ whenever $H \cap I_Y \neq \emptyset$.

(F3′) $f \in U{:}Y$ only if $I_Y = \{n\}$. First, it is clear that $f = e_{[1,n]} \in U_\emptyset$. For any $K \subseteq I_Y$ with $n \in K$, $f = g + e_{K \setminus \{n\}} - e_K \in U_K$. However, if $n \notin K$ but K is non-empty, then $f \notin U_K = \{e_I, g + e_I - e_K : I \subseteq [1,n]\}$. This is because $e_I - e_K \neq f$ (since K is non-empty), and $g + e_I - e_K$ has an e_n coefficient larger than 1 (since $n \notin K$).

We now have, combining (1) and (2) with our work here, that

$$\{0, g\} + \sum_{i \in I_X} \{0, e_i\} \subseteq X \subseteq \left[\{0, g\} + \sum_{i \in I_X} \{0, e_i\}\right] \cup \{f\},$$

so we have determined X almost exactly, up to the choice of whether $f \in X$.

First suppose $f \notin X$. Then $X = \{0, g\} + \sum_{i \in I_X} \{0, e_i\}$ and, since $I_Y \neq \emptyset$, $I_X \subsetneqq [1,n]$. Consequently, $\{e_i : i \in I_X\} \cup \{g\}$ is a $\mathbb{Z}$-linearly independent subset of $\mathbb{Z}^n$, so the summands of X are $\mathbb{Z}$-independent by Proposition 7.2.2(i). In turn, we have that X factors uniquely (by Theorem 7.2.5) as the sum of $\{0, g\}$ and the $\{0, e_i\}$ for $i \in I_X$. This can only produce – up to reordering, of course – the factorization $\{0, g\} * \{0, e_1\} * \cdots * \{0, e_n\} \in \mathcal{Z}_{\mathcal{P}_{\mathrm{fin},0}(\mathbb{N}^n)}(U)$.

If $f \in X$, then $X = \left[\{0, g\} + \sum_{i \in I_X} \{0, e_i\}\right] \cup \{f\}$ (and $Y = \{0, e_n\}$ per our considerations in (F3′)). By Lemma 7.3.2, X is an atom, producing the factorization $X * \{0, e_n\} \in \mathcal{Z}_{\mathcal{P}_{\mathrm{fin},0}(\mathbb{N}^n)}(U)$ and completing the proof. □

Remark 7.3.4. In the same vein as Example 7.2.6, one may use Theorem 7.3.3 to recover some cases of [FT18, Proposition 4.8].

7.4 A New Family of Length Sets

Our work thus far culminates in realizing a new family of sets, parameterized by two integers m and n, as sets of lengths for elements of $\mathcal{P}_{\text{fin},0}(\mathbb{N}^d)$ (and consequently for elements of $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ by Theorem 7.1.7). This builds toward Conjecture 7.0.1; but before explicitly showing how to construct these elements, we extract a more general result that lies at the heart of what makes the construction work.

Lemma 7.4.1. Let $U \in \mathcal{P}_{\text{fin},0}(\mathbb{N}^d)$ be an element whose two longest factorizations have lengths M and N, with $M < N$. Further assume that U has a *unique* longest factorization (of length N). Suppose $m \geq 1$ and that $V_1, \ldots, V_m \subseteq \mathbb{N}^d$ are atoms such that $U, V_1, \ldots, V_m$ are totally $\mathbb{Z}$-independent. Then $\mathsf{L}(U + V_1 + \cdots + V_m) \cap [M + m + 1, \infty] = \{N + m\}$.

This Lemma is the workhorse of our main result, Theorem 7.4.2. Before descending into the details of the proof, we highlight the broad strokes of our strategy. We start with a decomposition of $U + V$ into many (more than $M + m$) atoms. The result will easily follow if each atom involves only elements of U or only elements of V. As such, most of our work will center around the case in which (at least) one atom contains nontrivial sums from $U + V$.

In the spirit of the proofs of Theorem 7.2.5 and Theorem 7.3.3, we will get that this atom, call it A, has neat enough structure for us to produce a nontrivial decomposition of the form $A = U \cap A + V \cap A$, a contradiction.

Proof. For convenience, let $V := V_1 + \cdots + V_m$. Suppose that $k > M + m$ and that there are atoms $A_1, \ldots, A_k$ with $U + V = A_1 + \cdots + A_k$. By Proposition 7.2.3(iv), we know that $k \leq N + m$.

By Proposition 7.2.3(iii), we can say (renumbering if necessary)

$$[1, s] = \{i : U \cap A_i \neq \{0\}\} \quad \text{and} \quad [t, k] = \{i : V \cap A_i \neq \{0\}\}.$$

Since we know that $[1, k] = [1, s] \cup [t, k]$, we know that $t \leq s + 1$. The arguments to follow hinge on whether these two intervals overlap. First suppose that the intervals overlap; i.e., that $t \leq s$. We will show that this cannot happen by showing that, in this case, A_s is not an atom.

Let $J = \{j \in [1, m] : V_j \subseteq A_s\}$ and set $V' = \sum_{j \in J} V_j$; we know by Lemma 7.2.4 that $V' = V \cap A_s$. Also let $K = [1, m] \setminus J$ and $V'' = \sum_{j \in K} V_j$.

Claim A. $V' = V \cap A_s$ and $V'' \cap A_s = \{0\}$.

This follows directly from Lemma 7.2.4(ii), (iii).

Claim B. $A_i \subseteq U$ for $i < t$ and $A_i \subseteq V$ for $i > s$.

Proposition 7.2.3(ii) implies both statements since $V \cap A_i = \{0\}$ for $i < t$ (and $U \cap A_i = \{0\}$ for $i > s$).

Claim C. For all $v \in V'$, $U + v = \sum\limits_{i<s} U \cap A_i + (U + v) \cap A_s$.

We will show both inclusions. First suppose $u \in U$. Then $u+v \in \sum_{i=1}^k A_i$, and we can find $u_1, \ldots, u_s \in U$ and $v_t, \ldots, v_k \in V$ so that (by Claim B) $u_i \in A_i$ if $i < t$, $u_i + v_i \in A_i$ if $t \leq i \leq s$, and $v_i \in A_i$ if $i > s$. Then we will have

$$u + v = \sum_{i<t} u_i + \sum_{i=t}^{s} (u_i + v_i) + \sum_{i>s} v_i,$$

whence the $\mathbb{Z}$-independence of $U, V_1, \ldots, V_m$ implies that $u = \sum_{i \leq s} u_i$, $v_s = v$, and $v_i = 0$ for all $i \neq s$. Now $u + v = \sum_{i<s} u_i + (u_s + v) \in \sum_{i<s} U \cap A_i + (U + v) \cap A_s$.

For the other inclusion, let $u_1, \ldots, u_s \in U$ with $u_i \in A_i$ for all $i < s$ and $u_s + v \in A_s$. Then $\sum_{i \leq s} u_i + v \in \sum_{i \leq s} A_i \subseteq U + V$, so we can find $u' \in U$ and $v' \in V$ with

$$\sum_{i \leq s} u_i + v = u' + v',$$

at which point we can use $\mathbb{Z}$-independence again to see that $v' = v$, so that $\sum_{i \leq s} u_i + v \in U + v$.

Claim D. We have $s > M$.

Suppose instead that $s \leq M$. Then $U = \sum_{i \leq s} U \cap A_i$ has $s \leq m$ summands and $V = \sum_{i \geq t} V \cap A_i$ has $|[t, k]| \leq m$ summands (since V factors uniquely as the product of m atoms). Consequently, $k = |[1, s] \cup [t, k]| \leq |[1, s]| + |[t, k]| \leq M + m$, contradicting the assumption that $k > M + m$.

Claim E. For all $v \in V'$, $(U + v) \cap A_s = U \cap A_s + v$.

We can write $(U + v) \cap A_s = A + v$ for some $A \subseteq U$. Now $U + v = \sum_{i<s} U \cap A_i + (U + v) \cap A_s = \sum_{i<s} U \cap A_i + A + v$. We can cancel v from both sides of this set equality (since v is a unit in $\mathcal{P}_{\text{fin},0}(\mathbb{Z}^n)$), yielding

$$U = \sum_{i<s} U \cap A_i + A. \tag{DEC1}$$

On the other hand, Claim C (with $v = 0$) gives us the decomposition

$$U = \sum_{i<s} U \cap A_i + U \cap A_s. \tag{DEC2}$$

We will now show that we can cancel the common factors that appear in these two decompositions. By Claim D, $s > M$, so both decompositions (DEC1) and (DEC2) involve more than M atoms. However, U has only one factorization with more than M atoms; call it $\mathfrak{b} = B_1 * \cdots * B_N \in \mathcal{Z}(U)$.

Then the atoms which appear in both decompositions (DEC1) and (DEC2) of U must be some reorderings of the B_i. Renumbering if needed, there is some h for which $\sum_{i<s} U \cap A_i = B_1 + \cdots + B_h$. By the uniqueness of the atoms B_i, it must be that $B_1 + \cdots + B_h$ can be cancelled in the decompositions (DEC1) and (DEC2), leaving

$$A = B_{h+1} + \cdots + B_N = U \cap A_s,$$

and we have proved the claim.

Claim F. A_s is not an atom.

To see this, we compute

$$\begin{aligned}
A_s = (U+V) \cap A_s &= (U+V'+V'') \cap A_s \\
&= (U+V') \cap A_s && \text{(by Claim A and Proposition 7.2.3)} \\
&= \bigcup_{v \in V'} (U+v) \cap A_s \\
&= \bigcup_{v \in V'} (U \cap A_s + v) && \text{(by Claim E)} \\
&= U \cap A_s + V'.
\end{aligned}$$

Since $U \cap A_s$ and $V' = V \cap A_s$ are both nonzero, A_s is not an atom. This is a contradiction which followed from our assumption that some of the A_i may intersect nontrivially with *both* U and V.

Now suppose this does not occur; necessarily, $s < t$ and we in fact have that $t = s+1$ by Proposition 7.2.3(iii). For $i \leq s$, since $V \cap A_i = \{0\}$, Proposition 7.2.3(ii) implies that $A_i = (U+V) \cap A_i = U \cap A_i \subseteq U$. Then we have, by Proposition 7.2.3(i), that $U = \sum_{i \leq s} U \cap A_i = \sum_{i \leq s} A_i$. This means that $s \in \mathsf{L}(U)$ and, by identical reasoning for V, that $|[t,k]| = m$. We conclude that $k \in \mathsf{L}(U) + m$ and, due to the assumption that $k > M + m$, it must be the case that $k = N + m$. □

Finally, we give some new evidence toward Conjecture 7.0.1 by constructing, for each $m \geq 1$ and $n \geq 2$, a subset of $\mathbb{N}^d$ whose set of factorization lengths is exactly $[2, m+2] \cup \{m+n+1\}$.

Theorem 7.4.2. Fix $n \geq 2$, $m \geq 1$, and $d \geq m+n$. Let U_{n+1} be as in Definition 7.3.1 so that, in particular, U_{n+1} has exactly two factorizations, of lengths 2 and $n+1$, respectively. Suppose $V_1, \ldots, V_m \subseteq \mathbb{N}^d$ are atoms such that $U_{n+1}, V_1, \ldots, V_m$ are totally $\mathbb{Z}$-independent. Then $\mathsf{L}(U_{n+1}+V_1+\cdots+V_m) = [2, m+2] \cup \{m+n+1\}$.

Proof. For convenience, let $U := U_{n+1}$ and $V := V_1 + \cdots + V_m$. We will start by verifying the values that most clearly belong to $\mathsf{L}(U+V)$. It is easiest to see that $m+n+1 = \max \mathsf{L}(V) + \max \mathsf{L}(U) \in \mathsf{L}(U+V)$. For the rest, suppose $0 \leq h \leq m$. Then, by Lemma 7.3.2,

$$B_h := \left(\sum_{i=1}^{n-1} \{0, e_i\} + \{0, g\} + \sum_{j \in [h+1, m]} V_j \right) \cup \{f\}$$

is an atom. From here, it is straightforward to check that

$$U + V = \{0, e_n\} + B_h + V_1 + \cdots + V_h$$

so $h+2 \in \mathsf{L}(U+V)$. As we allow h to range over $[0,m]$, we get that $[2, m+2] \in \mathsf{L}(U+V)$.

For the other inclusion, we need to show that no other values are included in $\mathsf{L}(U+V)$. To do this, we note that U has a unique longest factorization by Theorem 7.3.3 and hence, using Lemma 7.4.1, $\mathsf{L}(U+V) \cap [m+3, m+n+1] = \{m+n+1\}$. □

Corollary 7.4.3. For every $m \geq 1$ and $n \geq 2$, there is an element $W \in \mathcal{P}_{\text{fin},0}(\mathbb{N})$ with $\mathsf{L}_{\mathcal{P}_{\text{fin},0}(\mathbb{N})}(W) = [2, m+2] \cup \{m+n+1\}$.

Proof. One simply needs to apply Theorems 7.4.2 and 7.1.7 to see that $[2, m+2] \cup \{m+n+1\} \in \mathcal{L}(\mathcal{P}_{\text{fin},0}(\mathbb{N}^d)) = \mathcal{L}(\mathcal{P}_{\text{fin},0}(\mathbb{N}))$. □

There is certainly room to progress further toward Conjecture 7.0.1. For instance, using Lemma 7.4.1, which was the workhorse of proving Theorem 7.4.2, relied largely on constructing a set which had factorizations of different lengths *and* a unique longest factorization. The only such construction is that of Fan and Tringali's from [FT18, Proposition 4.10], or its $\mathbb{N}^d$ counterpart from Definitions 7.3.1. It would therefore be of some interest to characterize the subsets of $\mathbb{N}$ which have a unique longest factorization into irreducibles. Predicting a best path toward Conjecture 7.0.1 is difficult, but it is likely that most diretions of further research into power monoids have potential to be revelatory.

Bibliography

[AAM85] D. D. Anderson, David F. Anderson, and Raj Markanda. The rings $R(X)$ and $R\langle X\rangle$. *J. Algebra*, 95(1):96–115, 1985.

[AAVL01] Ahmet G. Ağargün, D. D. Anderson, and Silvia Valdes-Leon. Factorization in commutative rings with zero divisors. III. *Rocky Mountain J. Math.*, 31(1):1–21, 2001.

[AC11] Dan Anderson and Sangmin Chun. Irreducible elements in commutative rings with zero-divisors. *Houston Journal of Mathematics*, 37, 01 2011.

[ACIS93] David F. Anderson, Scott T. Chapman, Faith Inman, and William W. Smith. Factorization ink[x2,x3]. *Archiv der Mathematik*, 61:521–528, 1993.

[AFRS03] Michael Axtell, Sylvia Forman, Nick Roersma, and Joe Stickles. Properties of u-factorizations. *International Journal of Commutative Rings*, 2, 01 2003.

[AJ95] David F. Anderson and Susanne Jenkens. Factorization in $K[X^n, X^{n+1}, \cdots, X^{2n-1}]$. *Comm. Algebra*, 23(7):2561–2576, 1995.

[AM85] D. D. Anderson and Raj Markanda. Unique factorization rings with zero divisors. *Houston J. Math.*, 11(1):15–30, 1985.

[AT19] Austin A. Antoniou and Salvatore Tringali. On the arithmetic of power monoids and sumsets in cyclic groups, 2019.

[AVL96] D. D. Anderson and Silvia Valdes-Leon. Factorization in commutative rings with zero divisors. *Rocky Mountain J. Math.*, 26(2):439–480, 1996.

[AVL97] D. D. Anderson and Silvia Valdes-Leon. Factorization in commutative rings with zero divisors. II. In *Factorization in integral domains (Iowa City, IA, 1996)*, volume 189 of *Lecture Notes in Pure and Appl. Math.*, pages 197–219. Dekker, New York, 1997.

[Bar06] Valentina Barucci. Numerical semigroup algebras. In *Multiplicative ideal theory in commutative algebra*, pages 39–53. Springer, New York, 2006.

[BBM17] Nicholas R. Baeth, Brandon Burns, and James Mixco. A fundamental theorem of modular arithmetic. *Period. Math. Hungar.*, 75(2):356–367, 2017.

[BOP17] Thomas Barron, Christopher O'Neill, and Roberto Pelayo. On dynamic algorithms for factorization invariants in numerical monoids. *Math. Comp.*, 86(307):2429–2447, 2017.

[Bou74a] A. Bouvier. Anneaux présimplifiables. *Rev. Roumaine Math. Pures Appl.*, 19:713–724, 1974.

[Bou74b] Alain Bouvier. Structure des anneaux à factorisation unique. *Publ. Dép. Math. (Lyon)*, 11(3):39–49, 1974.

[BS15] Nicholas R. Baeth and Daniel Smertnig. Factorization theory: from commutative to noncommutative settings. *J. Algebra*, 441:475–551, 2015.

[CAVL11] Sangmin Chun, D. D. Anderson, and Silvia Valdez-Leon. Reduced factorizations in commutative rings with zero divisors. *Communications in Algebra*, 39(5):1583–1594, 2011.

[CC97] Paul-Jean Cahen and Jean-Luc Chabert. *Integer-valued polynomials*, volume 48 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 1997.

[CGH$^+$18] Rebecca Conaway, Felix Gotti, Jesse Horton, Christopher O'Neill, Roberto Pelayo, Mesa Pracht, and Brian Wissman. Minimal presentations of shifted numerical monoids. *Internat. J. Algebra Comput.*, 28(1):53–68, 2018.

[CLS02] Scott T. Chapman, Alan Loper, and William W. Smith. The strong two-generator property in rings of integer-valued polynomials determined by finite sets. *Arch. Math. (Basel)*, 78(5):372–377, 2002.

[DF91] David S. Dummit and Richard M. Foote. *Abstract algebra.* Prentice Hall, Inc., Englewood Cliffs, NJ, 1991.

[EKOT20] R. A. C. Edmonds, B. Kubik, C. O'Neill, and S. Talbott. On atomic density of numerical semigroup algebras, 2020.

[Erd42] P. Erdös. On an elementary proof of some asymptotic formulas in the theory of partitions. *Ann. of Math. (2)*, 43:437–450, 1942.

[Fle69] C. R. Fletcher. Unique factorization rings. *Proc. Cambridge Philos. Soc.*, 65:579–583, 1969.

[FNR19] Sophie Frisch, Sarah Nakato, and Roswitha Rissner. Sets of lengths of factorizations of integer-valued polynomials on Dedekind domains with finite residue fields. *J. Algebra*, 528:231–249, 2019.

[Fri13] Sophie Frisch. A construction of integer-valued polynomials with prescribed sets of lengths of factorizations. *Monatsh. Math.*, 171(3-4):341–350, 2013.

[FT18] Yushuang Fan and Salvatore Tringali. Power monoids: a bridge between factorization theory and arithmetic combinatorics. *J. Algebra*, 512:252–294, 2018.

[Gal78] Steven Galovich. Unique factorization rings with zero divisors. *Math. Mag.*, 51(5):276–283, 1978.

[GG06] Weidong Gao and Alfred Geroldinger. Zero-sum problems in finite abelian groups: a survey. *Expo. Math.*, 24(4):337–369, 2006.

[GHK06] Alfred Geroldinger and Franz Halter-Koch. *Non-unique factorizations*, volume 278 of *Pure and Applied Mathematics (Boca Raton)*. Chapman & Hall/CRC, Boca Raton, FL, 2006. Algebraic, combinatorial and analytic theory.

[GL90] Alfred Geroldinger and Günter Lettl. Factorization problems in semigroups. *Semigroup Forum*, 40(1):23–38, 1990.

[GLPW18] Weidong Gao, Yuanlin Li, Jiangtao Peng, and Guoqing Wang. A unifying look at zero-sum invariants. *Int. J. Number Theory*, 14(3):705–711, 2018.

[Gor80] Daniel Gorenstein. *Finite groups*. Chelsea Publishing Co., New York, second edition, 1980.

[GR09] Alfred Geroldinger and Imre Z. Ruzsa. *Combinatorial number theory and additive group theory*. Advanced Courses in Mathematics. CRM Barcelona. Birkhäuser Verlag, Basel, 2009. Courses and seminars from the DocCourse in Combinatorics and Geometry held in Barcelona, 2008.

[Gry13] David J. Grynkiewicz. *Structural additive theory*, volume 30 of *Developments in Mathematics*. Springer, Cham, 2013.

[GS18] Alfred Geroldinger and Wolfgang Alexander Schmid. A realization theorem for sets of lengths in numerical monoids. *Forum Math.*, 30(5):1111–1118, 2018.

[GS19] Benjamin Girard and Wolfgang A. Schmid. Direct zero-sum problems for certain groups of rank three. *J. Number Theory*, 197:297–316, 2019.

[GS20] B. Girard and W. A. Schmid. Inverse zero-sum problems for certain groups of rank three. *Acta Math. Hungar.*, 160(1):229–247, 2020.

[HR00] G. H. Hardy and S. Ramanujan. Asymptotic formulæin combinatory analysis [Proc. London Math. Soc. (2) **17** (1918), 75–115]. In *Collected papers of Srinivasa Ramanujan*, pages 276–309. AMS Chelsea Publ., Providence, RI, 2000.

[LN97] Rudolf Lidl and Harald Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997. With a foreword by P. M. Cohn.

[Lop97a] Alan Loper. Sequence domains and integer-valued polynomials. *J. Pure Appl. Algebra*, 119(2):185–210, 1997.

[Lop97b] K. Alan Loper. Ideals of integer-valued polynomial rings. *Comm. Algebra*, 25(3):833–845, 1997.

[Mor93] Robert Morelli. A theory of polyhedra. *Adv. Math.*, 97(1):1–73, 1993.

[Nat02] M. B. Nathanson. On Erdős's elementary method in the asymptotic theory of partitions. In *Paul Erdős and his mathematics, I (Budapest, 1999)*, volume 11 of *Bolyai Soc. Math. Stud.*, pages 515–531. János Bolyai Math. Soc., Budapest, 2002.

[OP17] Christopher O'Neill and Roberto Pelayo. Factorization invariants in numerical monoids. In *Algebraic and geometric methods in discrete mathematics*, volume 685 of *Contemp. Math.*, pages 231–249. Amer. Math. Soc., Providence, RI, 2017.

[OP18] Christopher O'Neill and Roberto Pelayo. Realisable sets of catenary degrees of numerical monoids. *Bull. Aust. Math. Soc.*, 97(2):240–245, 2018.

[SC17] Svetoslav Savchev and Fang Chen. An inverse problem about minimal zero-sum sequences over finite cyclic groups. *J. Number Theory*, 177:381–427, 2017.

[Tri19] Salvatore Tringali. Structural properties of subadditive families with applications to factorization theory. *Israel J. Math.*, 234(1):1–35, 2019.

[TV06] Terence Tao and Van H. Vu. *Additive Combinatorics*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2006.

[WG07] R. Wang and D. Gong. Minkowski decomposition of convex lattice polytopes. *Journal of Information and Computational Science*, 4:767–774, 06 2007.

[Whi88] Thomas A. Whitelaw. *Introduction to abstract algebra*. Blackie, Glasgow, 2nd ed. edition, 1988.

[Wol98] D. A. Wolfram. Solving generalized Fibonacci recurrences. *Fibonacci Quart.*, 36(2):129–145, 1998.