

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

Austin Alan Antoniou

January 22, 2020



# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Plan and Main Results . . . . .	1
1.2	Brief History and Motivation . . . . .	2
1.3	Notation and Conventions . . . . .	3
<b>2</b>	<b>Monoids and Factorizations</b>	<b>5</b>
2.1	Fundamentals of Factorization Theory . . . . .	5
2.2	Examples and Non-Examples . . . . .	7
2.3	Monoid and Equimorphism Basics . . . . .	8
2.4	Literature and Comparing Alternate Definitions . . . . .	10
<b>3</b>	<b>Power Monoids and Atomicity</b>	<b>13</b>
3.1	Subset Arithmetic . . . . .	13
3.2	Atomicity and Bounded Factorization in Power Monoids . . . . .	16
<b>4</b>	<b>Minimal Factorizations and Applications to Power Monoids</b>	<b>21</b>
4.1	Fundamentals of Minimal Factorizations . . . . .	21
4.2	Minimal Factorizations in Power Monoids . . . . .	26
4.3	Cyclic Monoids and Interval Length Sets . . . . .	31
<b>5</b>	<b>Atoms and Intervals in the Natural Power Monoid</b>	<b>37</b>
5.1	Construction of Residually Concentrated Atoms . . . . .	37
<b>6</b>	<b>Integer Partitions and the Natural Power Monoid</b>	<b>43</b>
6.1	Algorithmic Approaches and Partition Type . . . . .	43
6.2	Admissible and Forbidden Types for Intervals . . . . .	47
6.3	Subsums and Near Intervals . . . . .	52

<b>7 Subsets of Integer Lattices</b>	<b>55</b>
7.1 Passage Between Power Monoids . . . . .	55
7.2 Independence Arguments in the Natural Lattice . . . . .	58
7.3 Length Sets in High-Dimensional Lattices . . . . .	63
<b>Bibliography</b>	<b>69</b>

# 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 Plan and Main Results

In the remainder of this chapter, we will tell (some of) the story of factorization theory up to this point, by way of motivating the chapters to come. We will also set some notation and conventions to be used.

Chapter 2 begins by formulating the definitions necessary to have a detailed discussion of factorizations, including definitions which capture the various degrees to which a monoid may fail to have uniqueness of factorization (the conditions UF, HF, FF, BF). Following this is a discussion of some examples of these concepts. From here, we outline a few more general monoid concepts needed for later, and close with a comparison of the present framework to the existing body of work on factorization theory and the alternative definitions therein.

Chapter 3 will introduce our main object of study: the power monoid. In brief, for any monoid  $H$ , let  $\mathcal{P}_{\text{fin}}(H)$  be the collection of finite, nonempty subsets of  $H$  with the operation of setwise multiplication given by  $X \cdot Y = \{xy : x \in X, y \in Y\}$ . This forms a monoid which can behave wildly with respect to questions of factorization. However, the submonoid  $\mathcal{P}_{\text{fin},1}(H)$  of subsets containing 1 is more feasible for study, and yields some meaningful results which can be lifted back to the full monoid  $\mathcal{P}_{\text{fin}}(H)$  in some circumstances

(for instance, when  $H$  is a group). As it turns out,  $\mathcal{P}_{\text{fin},1}(H)$  is atomic exactly when  $H$  has no nontrivial idempotents or elements of order 2 (Theorem 3.2.3). Moreover,  $\mathcal{P}_{\text{fin},1}(H)$  has bounded factorization lengths if and only if  $H$  is torsion-free (Theorem 3.2.5).

When  $H$  is not torsion-free, the usual tools for measuring non-uniqueness of factorization in  $\mathcal{P}_{\text{fin},1}(H)$  become degenerate. In Chapter 4, we seek compensate for this by introducing the notion of *minimal factorizations* in a general (non-cancellative) monoid. We then classify the circumstances under which  $\mathcal{P}_{\text{fin},1}(H)$  satisfies minimal versions of the usual factorization properties (Factoriality, Half-Factoriality, FF-ness, BF-ness) in Theorems 4.2.4 and 4.2.5 and Corollary 4.2.6. Finally, we move to the specific case when  $H = \mathbb{Z}/n\mathbb{Z}$  is a finite cyclic group to exercise this new notion of minimal factorization and recover analogues of some results which are known for  $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ . Namely, each interval  $[2, k]$  for  $k \leq n - 1$  occurs as a set of lengths in  $\mathcal{P}_{\text{fin},0}(\mathbb{Z}/n\mathbb{Z})$  (Theorem 4.3.7).

Chapter 6 focuses on the specific case of  $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ . In this setting we can leverage the linear ordering of  $\mathbb{N}$  to introduce the partition type of a given factorization. We consider the set of partition types of factorizations of a given element (by analogy with the more familiar set of lengths). This is a new measure by which we can assess the degree to which an element fails to factor uniquely. In keeping with our previous findings, the intervals  $[0, n]$  realizes all but 4 possible partition types (Theorem 6.2.8), making them quantifiably the elements farthest from factoring uniquely. Continuing to view  $\mathcal{P}_{\text{fin},0}(\mathbb{N})$  through the lens of integer partitions, we also find another sharp bifurcation in factorization behavior between intervals and non-intervals: any non-interval  $X$  satisfies  $\max(\mathcal{L}_{\mathcal{P}_{\text{fin},0}(\mathbb{N})}(X)) \leq \max(X)/2$ .

Chapter 7 first establishes an intimate connection between the arithmetic of  $\mathcal{P}_{\text{fin},0}(\mathbb{N})$  and  $\mathcal{P}_{\text{fin},0}(\mathbb{N}^d)$ , for  $d > 1$ ; while it is clear that all phenomena encountered in  $\mathcal{P}_{\text{fin},0}(\mathbb{N})$  can be found in  $\mathcal{P}_{\text{fin},0}(\mathbb{N}^d)$ , the reverse is true as well (Theorem 7.1.6). This affords us the opportunity to use higher-dimensional geometric intuition to attack problems in  $\mathcal{P}_{\text{fin},0}(\mathbb{N})$  and leads us to develop some new methods for understanding factorizations in  $\mathcal{P}_{\text{fin},0}(\mathbb{N}^d)$ . In turn, this line of thought allows us to recover known results in  $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ ; namely, that, for any  $n \geq 2$ ,  $\{n\}$  and  $\{2, n + 1\}$  occur as sets of factorization lengths (Theorems 7.2.5 and 7.3.3, respectively). Finally, we push these methods further to obtain a new realization result for a family of length sets; namely, Theorem 7.3.5, which states that, for any  $n \geq 2$  and  $m \geq 1$ ,  $[2, m + 2] \cup \{m + n + 1\}$  occurs as a set of lengths.

## 1.2 Brief History and Motivation

The most elementary setting in which we study factorizations is the set  $\mathbb{Z}$  of integers. It is well known (as the Fundamental Theorem of Arithmetic) that every integer (other than  $-1$ ,  $0$ , and  $1$ ) factors uniquely as

a product of prime integers. For instance, 12 can be written as  $2 \cdot 2 \cdot 3$ . Of course, 12 can also be written as either of the products  $2 \cdot 3 \cdot 2$  or  $(-3) \cdot 2 \cdot (-2)$ , but we consider these factorizations to be fundamentally the same. This tells us that, in addition to identifying the prime factors involved, there should also be an equivalence of factorizations in play. Making these ideas rigorous is one of the challenges of extending this familiar example to a more general theory.

There are many settings other than the integers in which it is reasonable to decompose elements into atoms. However, most will not share the familiar unique factorization of the integers. Historically, one of the greatest examples comes from the ring of integers of an algebraic number field; namely,  $\mathbb{Z}[\sqrt{-5}]$ . Consider 6 as an element of this ring:  $6 = 2 \cdot 3$ , but we also have  $6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ . It is not a hard exercise to show that these two factorizations are not equivalent (meaning that 2 and 3 are not associate to  $1 \pm \sqrt{-5}$ ), so 6 has more than one type of factorization into irreducibles.

Much of the field has taken place in the setting of monoids which are not only commutative (satisfying  $ab = ba$ ) but also cancellative, meaning that  $ab = ac$  implies  $b = c$ . It is true that monoids of ideals in commutative rings and monoids of modules naturally give rise to examples of non-cancellative settings in which it is reasonable to study factorization properties. Our goal here is to explore a relatively new class of monoids which are non-cancellative, exhibit many rich properties, and yet are rooted in a simple and natural combinatorial construction.

## 1.3 Notation and Conventions

- $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ ,  $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$ , 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.
- For a subset  $S \subseteq \mathbb{R}$  and  $k \in \mathbb{N}$ , we set the notation  $S_{>k} := \{n \in S : n > k\}$  and  $S_{\geq k} := \{n \in S : n \geq k\}$ .
- 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 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,  $i, j, k, \ell, m$ , and  $n$  will usually stand for non-negative integers.  $H$  will stand for a monoid,  $G$  for a group, and  $R$  for a ring.
- For integers  $m, n$  with  $m > 1$ ,  $n \bmod m$  (or  $\bar{n}$ , when the modulus  $m$  is understood from context) will refer to the residue class of  $n$  modulo  $m$ .
- In general, we will refer to the operation of a not necessarily commutative monoid  $(H, \cdot)$  as “multiplication”. We will often adopt the practice of suppressing the symbol “ $\cdot$ ” when no confusion is likely to

arise; that is, we will write  $xy$  instead of  $x \cdot y$ .

- The identity of a multiplicative monoid  $(H, \cdot)$  will be called 1; the identity of an additive monoid  $(H, +)$  will be called 0.
- $X \subseteq Y$  will mean that  $X$  is a subset of  $Y$ ;  $X \subsetneq Y$  will mean that  $X \subseteq Y$  but  $X \neq Y$ ;  $K \leq H$  will mean that  $K$  is a submonoid of  $H$ .
- 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.
- 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  $k \in \mathbb{N}$  and objects  $x_i$  for  $i \in [1, k]$ , we will often write the family  $X := \{x_i : i \in [1, k]\}$  in “long form” as  $x_1, \dots, x_k$ . 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

### 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  $x \sim y$ .
- $a \in H \setminus H^\times$  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 **idempotent** (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  $x|_Hy$ , 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  $\varepsilon_S$  is said to have length zero).

The elements  $s_1, \dots, s_\ell$  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  $\pi_H : \mathcal{F}^*(H) \rightarrow H$  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 **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  $\llbracket 1, n \rrbracket$ ) such that  $b_i \sim a_{\sigma(i)}$  for all  $i \in \llbracket 1, k \rrbracket$ .
3.  $\mathfrak{a}$  and  $\mathfrak{b}$  have the same product; i.e.,  $\pi_H(\mathfrak{a}) = \pi_H(\mathfrak{b})$ .

It is not difficult to check that the relation defined here is indeed an equivalence relation on  $\mathcal{F}^*(\mathcal{A}(H))$ .

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

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

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

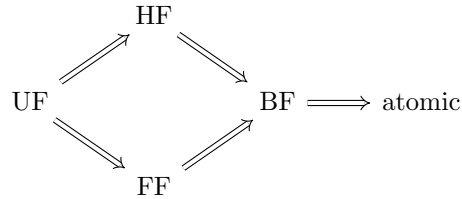
$$\mathsf{L}_H(x) := \{|\mathfrak{a}| : [\mathfrak{a}] \in \mathsf{Z}_H(x)\}.$$

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:



## 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.

- $\mathbb{Z} \setminus \{0\}$  is a unique factorization monoid (this is the Fundamental Theorem of Arithmetic).
- 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 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  $(2, 2)(3, 3)(2, 3) = (12, 18) = (2, 3)(2, 3)(3, 2)$ .
- 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  $r+i \notin R$  for  $r \neq 0$ , each  $r+i$  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.

(iv) Some of the richest factorization behavior is encountered in BF monoids. Here we mention some highly studied classes of BF monoids without going into too much detail, on the promise that we will discuss a new class of examples in heavy detail later.

- *Numerical monoids*: proper subsets  $H \subsetneq \mathbb{N}$  with finite complement which are closed under addition. [CITE SOME PAPERS]
- *Monoids of zero-sum sequences*: for a finite abelian group  $G$ , this monoid consists of formal words or “sequences” in the elements of  $G$  whose sums are equal to 0. 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). [CITE SOME PAPERS]
- *Integer-valued polynomials*: let  $D$  be a domain with field of fractions  $K$ ; then  $\text{Int}(D) := \{f(x) \in K[x] : f(D) \subseteq D\}$  is the ring of integer-valued polynomials of  $D$ . In addition to the rich theory developed 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  $f(x) \in \text{Int}(D)$ . Additionally, one can pose similar questions regarding the ring  $\text{Int}^{\mathbb{R}}(D)$  of integer-valued rational functions. [CITE SOME PAPERS]

(v) 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 Equiporphism Basics

Here we will define and examine some properties that pertain to arbitrary monoids, as well as our main tool for transporting factorization information between arbitrary monoids: equiporphisms.

**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  $\text{ord}_H(x) := |\langle x \rangle_H|$  (we may drop the subscript  $H$  when the monoid is clear from context).

$H$  is said to be

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

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

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

- **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  $\Rightarrow$  unit-cancellative  $\Rightarrow$  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  $x|_Hy$ , 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  $x \in M \setminus M^\times$ ,  $Z_M(x) = Z_H(x)$ ;
- (iv) For all  $x \in M \setminus M^\times$ ,  $L_M(x) = L_H(x)$ ;
- (v)  $\mathcal{L}(M) \subseteq \mathcal{L}(H)$ .

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

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

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

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

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

- (i)  $L_H(x) = L_K(\varphi(x))$  for all  $x \in H \setminus H^\times$ .
- (ii) If  $\varphi$  is essentially surjective, then for all  $y \in K \setminus K^\times$  there is  $x \in H \setminus H^\times$  with  $L_K(y) = L_H(x)$ .

*Proof.* See [FT18, Theorem 2.22(i)] and [Tri17, 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)  $x \neq 0_R$  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 [Fle69a], 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

### 3.1 Subset Arithmetic

Here we embark on the study of the (arithmetic and algebraic) structure of power monoids. We begin with some elementary but helpful observations we will often use without comment.

**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

$$\mathcal{P}_{\text{fin}, \times}(H) := \{X \subseteq H : X \cap H^\times \neq \emptyset \text{ and } |X| < \infty\};$$

and 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.

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. To do so in as all-encompassing a way as possible, we recall from [Tri17, Definition 3.2] a notion which formally packages the idea that, under suitable conditions, arithmetic may be transferred from one monoid to another.

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

- (i) If  $X_1, \dots, X_n \in \mathcal{P}_{\text{fin},1}(H)$ , then  $X_1 \cup \dots \cup X_n \subseteq X_1 \cdots X_n$ .
- (ii) If  $u, v \in H^\times$  and  $X_1, \dots, X_n \in \mathcal{P}_{\text{fin},\times}(H)$ , then  $|uX_1 \cdots X_nv| = |X_1 \cdots X_n| \geq \max_{1 \leq i \leq n} |X_i|$ .
- (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  $\mathcal{P}_{\text{fin}}(H)^\times = \mathcal{P}_{\text{fin},\times}(H)^\times = \{\{u\} : u \in H^\times\}$ .
- (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  $X \rightarrow H : x \mapsto uxv$  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.  $\square$

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

- (i) The natural embedding  $j : \mathcal{P}_{\text{fin},1}(H) \hookrightarrow \mathcal{P}_{\text{fin},\times}(H)$  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),  $j$  satisfies (E1). Moreover,  $j$  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  $j$  satisfies (E3). Pick  $X \in \mathcal{P}_{\text{fin}, 1}(H)$ . If  $X = \{1_H\}$ , the conclusion holds vacuously. Otherwise, let  $\mathbf{b} := B_1 * \cdots * B_n \in \mathcal{Z}_{\mathcal{P}_{\text{fin}, 1}(H)}(X)$ . Then there are  $u_1 \in B_1, \dots, u_n \in B_n$  such that  $1_H = u_1 \cdots u_n$ ; and as in the proof of (E2), it must be that  $u_1, \dots, u_n \in H^\times$ . 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),  $A_1, \dots, A_n$  are atoms of  $\mathcal{P}_{\text{fin}, 1}(H)$ . This shows that  $\mathbf{a} := A_1 * \cdots * A_n \in \mathcal{Z}_{\mathcal{P}_{\text{fin}, 1}(H)}(X)$ . Since  $A_i \simeq_{\mathcal{P}_{\text{fin}, \times}(H)} B_i$  for each  $i \in [1, n]$  (by construction), we thus conclude that  $\mathbf{a}$  is  $\mathcal{C}_{\mathcal{P}_{\text{fin}, \times}(H)}$ -congruent to  $\mathbf{b}$ , as wished.  $\square$

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

$$L : \mathcal{B} \rightarrow \mathcal{B} : (a_1, a_2, \dots) \mapsto (a_2, a_3, \dots) \quad (\text{left shift});$$

$$R : \mathcal{B} \rightarrow \mathcal{B} : (a_1, a_2, \dots) \mapsto (0, a_1, a_2, \dots) \quad (\text{right shift});$$

$$P : \mathcal{B} \rightarrow \mathcal{B} : (a_1, a_2, \dots) \mapsto (a_n, a_1, \dots, a_{n-1}, a_{n+1}, a_{n+2}, \dots) \quad (\text{cycle the first } n \text{ terms}).$$

In particular,  $P \in H^\times$ . Also,  $LR = \text{id}_{\mathcal{B}}$  but  $RL \neq \text{id}_{\mathcal{B}}$ ; whence  $H$  is not Dedekind-finite, and neither  $R$  nor  $L$  is invertible. With this in mind, we will prove that  $A := \{L, P\} \cdot \{R, P\} = \{\text{id}_{\mathcal{B}}, LP, PR, P^2\}$  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  $P^2 \neq PRLP$ , or else  $RL = \text{id}_B$  (a contradiction). Similarly,  $PRPR \neq P^2 \neq LPLP$ ; otherwise,  $P = RPR$  and hence  $R$  is invertible, or  $P = LPL$  and  $L$  is invertible (again a contradiction). Lastly, we see that  $P^2 \neq LP^2R$ , by applying both  $P^2$  and  $LP^2R$  to the constant sequence  $(1, 1, \dots)$ .

It follows that  $P^2$  must belong to  $X$  or  $Y$ , but not to both (which is the reason for choosing  $n \geq 5$ ). Accordingly, let  $P^2 \in X \setminus Y$  (the other case is analogous). Then  $Y = \{\text{id}_B\}$ , 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  $(1, 1, \dots)$  and  $(1, 0, 1, 1, \dots)$ . 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  $z = xv = ygv$ , 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.  $\square$

We have just seen that, to even *hope* for  $\mathcal{P}_{\text{fin}, 1}(H)$  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  $\geq 3$ .

*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  $\geq 3$ .  $\square$

**Theorem 3.2.3.** Let  $H$  be a monoid. Then  $\mathcal{P}_{\text{fin}, 1}(H)$  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  $X \in \mathcal{P}_{\text{fin},1}(H)$  with  $|X| \geq 2$ . We wish to show that

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

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  $Y \in \mathcal{P}_{\text{fin},1}(H)$  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  $A, B \in \mathcal{P}_{\text{fin},1}(H)$ , 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

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

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

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

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  $A_b B_b \subseteq A = A_b \cup \{b\} \subseteq A_b B_a \cup \{b\} \subseteq A_b B_a \cup B_a = A_b B_a$ ).  $\square$

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  $A_1, \dots, A_\ell \in \mathcal{A}(\mathcal{P}_{\text{fin},1}(H))$ . 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  $I = \{i_1, \dots, i_m\}$ , 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.,  $\{1_H, x, \dots, x^m\} \subseteq X$ . 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).  $\square$





## Chapter 4

# Minimal Factorizations and Applications to Power Monoids

### 4.1 Fundamentals of Minimal Factorizations

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.

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  $\varepsilon_X$  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  $\mathbf{a} \preceq_H \mathbf{b}$ , for some  $\mathcal{A}(H)$ -words  $\mathbf{a}$  and  $\mathbf{b}$  of length  $h$  and  $k$  respectively, if and only if one of the following conditions holds:

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

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

*minimal*) if there does not exist any  $A(H)$ -word  $\mathbf{b}$  such that  $\mathbf{b} \prec_H \mathbf{a}$ .

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  $\mathbf{a}, \mathbf{b} \in \mathcal{F}^*(A(H))$ . The following hold:

- (i)  $\preceq_H$  is a preorder (i.e., a reflexive and transitive binary relation) on  $\mathcal{F}^*(A(H))$ .
- (ii) If  $\mathbf{a} \preceq_H \mathbf{b}$  then  $\|\mathbf{a}\|_H \leq \|\mathbf{b}\|_H$ .
- (iii)  $\mathbf{a} \preceq_H \mathbf{b}$  and  $\mathbf{b} \preceq_H \mathbf{a}$  if and only if  $\mathbf{a} \preceq_H \mathbf{b}$  and  $\|\mathbf{a}\|_H = \|\mathbf{b}\|_H$ , if and only if  $(\mathbf{a}, \mathbf{b}) \in \mathcal{C}_H$ .

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

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

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

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

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

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

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

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

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  $\mathcal{L}_H^{\mathbf{m}}(x)$  (respectively,  $\mathcal{Z}_H^{\mathbf{m}}(x)$ ) is finite and non-empty for every  $x \in H \setminus H^\times$ ;

- HmF or *half-minimally-factorial* (respectively, *minimally factorial*) if  $\mathbf{L}_H^{\mathbf{m}}(x)$  (respectively,  $\mathbf{Z}_H^{\mathbf{m}}(x)$ ) is a singleton for all  $x \in H \setminus H^\times$ .

Note that we may write  $\mathbf{Z}^{\mathbf{m}}(x)$  for  $\mathbf{Z}_H^{\mathbf{m}}(x)$ ,  $\mathbf{L}^{\mathbf{m}}(x)$  for  $\mathbf{L}_H^{\mathbf{m}}(x)$ , 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  $\pi_H(\mathbf{a}) = x$  but  $x \neq \pi_H(\mathbf{b})$  for every non-empty  $\mathcal{A}$ -word  $\mathbf{b} = b_1 * \cdots * b_m$  of length  $m \leq n - 1$  for which there exists an injection  $\sigma : [1, m] \rightarrow [1, n]$  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  $\mu$ -reduced  $\mu$ -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 [Fle69b] 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

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

Accordingly, we take a GL-*factorization* of a non-unit  $x \in H$  to be a non-empty  $\mathcal{A}$ -word  $\mathbf{a} = a_1 * \cdots * a_n$  such that  $\pi_H(\mathbf{a}) = x$  and  $v_a^H(\mathbf{a}) \leq \text{ind}_H^{\text{GL}}(a)$  for every  $a \in \mathcal{A}$ , where

$$v_a^H(\mathbf{a}) := |\{i \in [1, n] : a_i = a\}|.$$

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  $\text{ind}_H^{\text{GL}}(u) = \infty$  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  $\mathbb{Z}/p\mathbb{Z} = \{\bar{0}, \bar{1}\} + \{\bar{0}, \bar{2}\} + \{\bar{0}, \bar{3}\}$ .

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  $A(H)$ -word of length 0, 1, or 2 is minimal.
- (ii)  $\mathcal{Z}_H(x) \neq \emptyset$  if and only if  $\mathcal{Z}_H^{\mathfrak{m}}(x) \neq \emptyset$ .
- (iii) If  $\mathfrak{a} \in \mathcal{Z}_H^{\mathfrak{m}}(x)$  and  $(\mathfrak{a}, \mathfrak{b}) \in \mathcal{C}_H$ , then  $\mathfrak{b} \in \mathcal{Z}_H^{\mathfrak{m}}(x)$ .
- (iv) If  $K$  is a divisor-closed submonoid of  $H$  and  $x \in K$ , then  $\mathcal{Z}_K^{\mathfrak{m}}(x) = \mathcal{Z}_H^{\mathfrak{m}}(x)$  and  $\mathcal{L}_K^{\mathfrak{m}}(x) = \mathcal{L}_H^{\mathfrak{m}}(x)$ .
- (v) If  $H$  is commutative and unit-cancellative, then  $\mathcal{Z}_H^{\mathfrak{m}}(x) = \mathcal{Z}_H(x)$ , and hence  $\mathcal{L}_H^{\mathfrak{m}}(x) = \mathcal{L}_H(x)$ .

*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  $\mathcal{A}(H)$ -words  $\mathfrak{b}$  of length  $\geq 2$ ); 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  $\mathcal{L}_K(x) = \mathcal{L}_H(x)$ , 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  $a_1, \dots, a_n \in \mathcal{A}(H)$  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  $a_{k+1}, \dots, a_n \in H^\times$ , which is however impossible (by definition of an atom).  $\square$

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  $\mathcal{Z}_H^{\mathfrak{m}}(x) \rightarrow \mathcal{Z}_H^{\mathfrak{m}}(uxv)$ , and in particular  $\mathcal{L}_H^{\mathfrak{m}}(x) = \mathcal{L}_H^{\mathfrak{m}}(uxv)$ .

*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  $w\mathfrak{z}$  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

$$f : \mathcal{Z}_H^{\mathfrak{m}}(x) \rightarrow \mathcal{Z}_H^{\mathfrak{m}}(uxv) : \mathfrak{a} \mapsto u\mathfrak{a}v$$

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  $g : \mathcal{Z}_H^{\mathfrak{m}}(uxv) \rightarrow \mathcal{Z}_H^{\mathfrak{m}}(x) : \mathfrak{b} \mapsto u^{-1}\mathfrak{b}v^{-1}$  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  $\mathfrak{a} \in \mathcal{Z}_H^{\mathfrak{m}}(x)$ , and note that, by parts (i) and (ii) of Proposition 2.3.3,  $\|\mathfrak{a}\|_H$  is a positive integer, so that  $\mathfrak{a} = a_1 * \dots * a_n$  for some  $a_1, \dots, a_n \in \mathcal{A}(H)$ . 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),  $k := \|\mathfrak{b}\|_H \in [1, n-1]$  (recall that  $uxv \notin H^\times$ ). So,  $\mathfrak{b} = b_1 * \dots * b_k$  for some atoms  $b_1, \dots, b_k \in H$ , and there exists an injection  $\sigma : [1, k] \rightarrow [1, n]$  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  $c_1, \dots, c_k \in \mathcal{A}(H)$  such that  $\mathfrak{c} = c_1 * \dots * c_k$ ; 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  $\mathfrak{a}$ .  $\square$

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  $\varphi : H \rightarrow K$  an equimorphism. The following hold:

- (i) If  $x \in H \setminus H^\times$  and  $\mathfrak{b} \in \mathcal{Z}_K^{\mathfrak{m}}(\varphi(x))$ , then there is  $\mathfrak{a} \in \mathcal{Z}_H^{\mathfrak{m}}(x)$  with  $\varphi^*(\mathfrak{a}) \in [\mathfrak{b}]_{\mathcal{C}_K}$ .
- (ii)  $\mathcal{L}_K^{\mathfrak{m}}(\varphi(x)) \subseteq \mathcal{L}_H^{\mathfrak{m}}(x)$  for every  $x \in H \setminus H^\times$ .
- (iii) If  $\varphi$  is essentially surjective then, for all  $y \in K \setminus K^\times$ , there is  $x \in H \setminus H^\times$  with  $\mathcal{L}_K^{\mathfrak{m}}(y) \subseteq \mathcal{L}_H^{\mathfrak{m}}(x)$ .

*Proof.* (i) Pick  $x \in H \setminus H^\times$ , and let  $\mathfrak{b} \in \mathcal{Z}_K^{\mathfrak{m}}(\varphi(x))$ . 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  $\mathfrak{a} \in \mathcal{Z}_H^{\mathfrak{m}}(x)$  with  $\varphi^*(\mathfrak{a}) \in [\mathfrak{b}]_{\mathcal{C}_K}$ , and it only remains to show that  $\mathfrak{a}$  is  $\preceq_H$ -minimal.

Note that  $n := \|\mathfrak{a}\|_H = \|\varphi^*(\mathfrak{a})\|_K = \|\mathfrak{b}\|_K \geq 1$ , and write  $\mathfrak{a} = a_1 * \dots * a_n$  and  $\mathfrak{b} = b_1 * \dots * b_n$ , with  $a_1, \dots, a_n \in \mathcal{A}(H)$  and  $b_1, \dots, b_n \in \mathcal{A}(K)$ . 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  $\mathfrak{c} = c_1 * \dots * c_m$  and an injection  $\sigma : [1, m] \rightarrow [1, n]$  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

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

(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  $\varphi^*(\mathbf{c}) \prec_K \mathbf{b}$ , contradicting the  $\preceq_K$ -minimality of  $\mathbf{b}$ .

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

(iii) Assume  $\varphi$  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  $\mathbf{L}_K^{\mathbf{m}}(y) = \mathbf{L}_K^{\mathbf{m}}(\varphi(x)) \subseteq \mathbf{L}_H^{\mathbf{m}}(x)$ .  $\square$

## 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)  $\mathcal{Z}_{\mathcal{P}_{\text{fin}, 1}(H)}^{\mathbf{m}}(X) \subseteq \mathcal{Z}_{\mathcal{P}_{\text{fin}, \times}(H)}^{\mathbf{m}}(X)$ .
- (ii)  $\mathbf{L}_{\mathcal{P}_{\text{fin}, 1}(H)}^{\mathbf{m}}(X) = \mathbf{L}_{\mathcal{P}_{\text{fin}, \times}(H)}^{\mathbf{m}}(X)$ .
- (iii)  $\mathcal{L}^{\mathbf{m}}(\mathcal{P}_{\text{fin}, 1}(H)) = \mathcal{L}^{\mathbf{m}}(\mathcal{P}_{\text{fin}, \times}(H))$ .

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

Assume for the sake of contradiction that  $\mathbf{a}$  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  $\mathbf{b} = B_1 * \cdots * B_m$  and an injection  $\sigma : [1, m] \rightarrow [1, n]$  with

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

and on account of Proposition 4.1.2(iii) we must have  $1 \leq m < n$ . 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

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

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  $\mathbf{a}'$  be the  $\mathcal{A}(\mathcal{P}_{\text{fin},1}(H))$ -word  $A_{\sigma(1)} * \cdots * A_{\sigma(m)}$  and recalling from the above that  $m \leq n - 1$ , we see by Proposition 4.1.2(iii) that  $\mathbf{a}' \prec_{\mathcal{P}_{\text{fin},1}(H)} \mathbf{a}$ , which contradicts the hypothesis that  $\mathbf{a}$  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  $\mathcal{L}^{\mathfrak{m}}(\mathcal{P}_{\text{fin},1}(H)) \subseteq \mathcal{L}^{\mathfrak{m}}(\mathcal{P}_{\text{fin},\times}(H))$ . 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  $\mathbf{L}_{\mathcal{P}_{\text{fin},\times}(H)}^{\mathfrak{m}}(X) = \mathbf{L}_{\mathcal{P}_{\text{fin},1}(H)}^{\mathfrak{m}}(Y)$ . 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

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

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

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  $\varphi$  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  $p \geq 11$  and  $3 \leq n \bmod p \leq p - 3$  (where  $n \bmod p$  is the smallest non-negative integer  $\equiv r \bmod p$ ). Following [Gor80, p. 27], we take  $H$  to be the metacyclic group generated by the 2-element set  $\{r, s\}$  subject to  $\text{ord}_H(r) = p$ ,  $\text{ord}_H(s) = 3$ , 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),  $\mathcal{P}_{\text{fin},1}(H)$  and  $\mathcal{P}_{\text{fin},\times}(H)$  are both atomic monoids.

We claim that  $X := \langle r \rangle_H$  has minimal factorizations of length  $p - 1$  in  $\mathcal{P}_{\text{fin},1}(H)$  but not in  $\mathcal{P}_{\text{fin},\times}(H)$ . Pick  $g \in X \setminus \{1_H\}$ . Clearly  $\text{ord}_H(g) = p$ , and thus we get from Lemma 3.2.1(i) that  $\{1_H, g\}$  is an atom of  $\mathcal{P}_{\text{fin},1}(H)$ . Then it is immediate to see that  $\mathbf{a}_g := \{1_H, g\}^{*(p-1)}$  is a minimal factorization of  $X$  in  $\mathcal{P}_{\text{fin},1}(H)$ ; most notably,  $\mathbf{a}_g$  is minimal since otherwise there should exist an exponent  $k \in [1, p-2]$  such that  $g^{p-1} = g^k$ , contradicting that  $\text{ord}_H(g) = p$ . Yet,  $\mathbf{a}_g$  is not a minimal factorization of  $X$  in  $\mathcal{P}_{\text{fin},\times}(H)$ . 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  $\mathcal{P}_{\text{fin}, \times}(H)$ , 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

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

In particular, note here that we have used that  $3 \leq n \bmod p \leq p-3$  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  $\mathcal{P}_{\text{fin}, \times}(H)$ . Then by Propositions 3.1.3(i) and 4.1.8(i),  $\mathfrak{c}$  is  $\mathcal{C}_{\mathcal{P}_{\text{fin}, \times}(H)}$ -congruent to a  $\preceq_{\mathcal{P}_{\text{fin}, 1}(H)}$ -minimal factorization  $\mathfrak{a} = A_1 * \dots * A_{p-1}$  of  $X$  of length  $p-1$ ; and we aim to show that  $\mathfrak{a}$  is  $\mathcal{C}_{\mathcal{P}_{\text{fin}, 1}(H)}$ -congruent 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  $\mathcal{P}_{\text{fin}, \times}(H)$ , in contradiction to what established in the above.

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

We want to show that  $\mathfrak{b}$  is  $\preceq_{\mathcal{P}_{\text{fin}, 0}(H)}$ -minimal only if there is a non-zero  $x \in \mathbf{Z}/p\mathbf{Z}$  such that  $B_i = \{\bar{0}, x\}$  or  $B_i = \{\bar{0}, -x\}$ , or equivalently  $A_i = \{1_H, r^{\hat{x}}\}$  or  $A_i = \{1_H, r^{-\hat{x}}\}$ , for every  $i \in [1, p-1]$  (for notation, see Section 1.3). By the preceding arguments, this will suffice to conclude that  $p-1 \notin \mathbf{L}_{\mathcal{P}_{\text{fin}, \times}(H)}^{\mathfrak{m}}(X)$ , because it implies at once that  $\mathfrak{a}$  is  $\mathcal{C}_{\mathcal{P}_{\text{fin}, 1}(H)}$ -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  $s_K := \{k \in K : |B_k| \geq 3\}$ . Then we have by the Cauchy-Davenport inequality (see, e.g., [Gry13, Theorem 6.2]) that

$$|\mathcal{S}_K| = \mathbf{Z}/p\mathbf{Z} \quad \text{or} \quad |\mathcal{S}_K| \geq 1 + \sum_{k \in K} (|B_k| - 1) \geq 1 + |K| + s_K. \quad (4.1)$$

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  $\mathcal{S}_{I \cup J} \neq \mathbf{Z}/p\mathbf{Z}$ , otherwise  $\mathfrak{b}$  would not be a minimal factorization in  $\mathcal{P}_{\text{fin}, 0}(\mathbf{Z}/p\mathbf{Z})$ . So, another application of the Cauchy-Davenport inequality, combined with (4.1), yields

$$|\mathcal{S}_{I \cup J}| = |S_I + S_J| \geq |S_I| + |S_J| - 1 \geq 1 + |I| + |J| + s_I + s_J = p-1 + s_I + s_J. \quad (4.2)$$

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

It follows  $|B_1| = \dots = |B_{p-1}| = 2$ . So, taking  $I$  in (4.2) to range over all 1-element subsets of  $[1, p-1]$



and observing that, consequently,  $|S_J| \geq p - 1 - |S_I| = p - 3 \geq 8 > |S_I|$ , 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.,  $B_i = \{\bar{0}, x\}$  or  $B_i = \{\bar{0}, -x\}$  (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  $\leq |X| - 1$ .
- (ii) If  $H$  is Dedekind-finite, then a minimal factorization of  $X$  in  $\mathcal{P}_{\text{fin}, \times}(H)$  has length  $\leq |X| - 1$ .

*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  $|X| \geq 2$  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  $\mathbf{a}$  be a minimal factorization of  $X$  (relative to  $\mathcal{P}_{\text{fin}, 1}(H)$ ). Then  $\mathbf{a} = A_1 * \cdots * A_n$ , where  $A_1, \dots, A_n \in \mathcal{A}(\mathcal{P}_{\text{fin}, 1}(H))$  and  $n \geq 2$ ; 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  $A_1 * \cdots * A_i * \mathbf{b} \prec_{\mathcal{P}_{\text{fin}, 1}(H)} \mathbf{a}$ , where  $\mathbf{b} := \varepsilon_{\mathcal{A}(\mathcal{P}_{\text{fin}, 1}(H))}$  if  $i = n - 1$  and  $\mathbf{b} := A_{i+2} * \cdots * A_n$  otherwise (contradicting the minimality of  $\mathbf{a}$ ). Consequently, we see that  $2 \leq |A_1 \cdots A_i| < |A_1 \cdots A_{i+1}| \leq |X|$  for all  $i \in [1, n - 1]$ , and this implies at once that  $n \leq |X| - 1$ .

- (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)  $1_H \neq x^2 \neq x$  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  $X \cap H^\times \neq \emptyset$  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)  $\Leftrightarrow$  (a)  $\Leftrightarrow$  (e) and (i)  $\Rightarrow$  (a); while it is straightforward from our definitions that (h)  $\Rightarrow$  (g)  $\Rightarrow$  (f). So, it will suffice to prove that (b)  $\Rightarrow$  (c)  $\Rightarrow$

(d)  $\Rightarrow$  (h) and (f)  $\Rightarrow$  (i).

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

(c)  $\Rightarrow$  (d): Let  $X \in \mathcal{P}_{\text{fin},1}(H)$  be a non-unit. By Proposition 3.1.2(i), any atom of  $\mathcal{P}_{\text{fin},1}(H)$  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  $\mathcal{A}(\mathcal{P}_{\text{fin},1}(H))$ -word (by the assumption that  $H$  is BmF), it follows that  $X$  has finitely many minimal factorizations, and hence  $\mathcal{P}_{\text{fin},1}(H)$  is FmF (since  $X$  was arbitrary).

(d)  $\Rightarrow$  (h): Pick a non-unit  $X \in \mathcal{P}_{\text{fin},\times}(H)$ , and let  $u \in H^\times$  such that  $uX \in \mathcal{P}_{\text{fin},1}(H)$ . Since  $\mathcal{P}_{\text{fin},1}(H)$  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  $\mathcal{P}_{\text{fin},1}(H) \hookrightarrow \mathcal{P}_{\text{fin},\times}(H)$  is an essentially surjective equimorphism. In particular, we infer from Proposition 4.1.8(i) that any minimal factorization of  $uX$  in  $\mathcal{P}_{\text{fin},\times}(H)$  is  $\mathcal{C}_{\mathcal{P}_{\text{fin},\times}(H)}$ -congruent to a minimal factorization of  $uX$  in  $\mathcal{P}_{\text{fin},1}(H)$ . However, this makes  $\mathcal{Z}_{\mathcal{P}_{\text{fin},\times}(H)}^{\mathfrak{m}}(uX)$  finite, whence  $\mathcal{Z}_{\mathcal{P}_{\text{fin},\times}(H)}^{\mathfrak{m}}(X)$  must also be finite as a consequence of Lemma 4.1.7.

(f)  $\Rightarrow$  (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  $1_H \in A$ ; and since  $\mathcal{P}_{\text{fin},\times}(H)$  is atomic (by hypothesis), we are guaranteed by Lemmas 3.2.1 and 3.2.2(i) that  $A$  is an atom of  $\mathcal{P}_{\text{fin},1}(H)$  and  $H$  is Dedekind-finite. Therefore, we conclude from Proposition 3.1.3(ii) that  $X \in \mathcal{A}(\mathcal{P}_{\text{fin},\times}(H))$ .  $\square$

**Theorem 4.2.5.** Let  $H$  be a monoid. Then  $\mathcal{P}_{\text{fin},1}(H)$  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  $\mathcal{P}_{\text{fin},1}(H)$  is HmF and  $H$  is non-trivial. Then  $\mathcal{P}_{\text{fin},1}(H)$  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  $\text{ord}_H(x) \leq 3$ .

Assume to the contrary that  $x^3 \notin \{1_H, x, x^2\}$  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  $\mathcal{P}_{\text{fin},1}(H)$ ; 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  $\mathcal{P}_{\text{fin},1}(H)$  is HmF and  $\mathfrak{a}$  has length 3. However, since  $\mathcal{P}_{\text{fin},1}(H)$  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  $\text{ord}_H(y) = \text{ord}_H(z) = 3$  and  $|K| = 9$ . We will prove that  $K$  has  $\preceq_{\mathcal{P}_{\text{fin},1}(H)}$ -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  $\mathbf{c} := \{1_H, y\}^{*2} * \{1_H, z\}^{*2}$  is a length-4 factorization of  $K$  in  $\mathcal{P}_{\text{fin},1}(H)$ ; and it is actually a minimal factorization, because removing one or more atoms from  $\mathbf{c}$  yields an  $\mathcal{A}(\mathcal{P}_{\text{fin},1}(H))$ -word whose image under  $\pi_{\mathcal{P}_{\text{fin},1}(H)}$  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  $\mathcal{P}_{\text{fin},1}(H)$ : If  $\{1_H, y, z\} = YZ$  for some  $Y, Z \in \mathcal{P}_{\text{fin},1}(H)$  with  $|Y|, |Z| \geq 2$ , then  $Y, Z \subseteq \{1_H, y, z\}$  and  $Y \cap Z = \{1_H\}$ , whence  $YZ = \{1_H, y\} \cdot \{1_H, z\} = K \neq A$ . This in turn implies that  $A^{*2}$  is a length-2 factorization of  $K$  in  $\mathcal{P}_{\text{fin},1}(H)$ , and it is minimal by Proposition 4.1.6(i). So, we are done.  $\square$

**Corollary 4.2.6.** Let  $H$  be a monoid. Then  $\mathcal{P}_{\text{fin},1}(H)$  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  $\mathcal{P}_{\text{fin},1}(H)$  is minimally factorial but  $H$  is non-trivial. Then  $\mathcal{P}_{\text{fin},1}(H)$  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),  $\mathbf{a} := \{1_H, x\}^{*2}$  and  $\mathbf{b} := \{1_H, x^2\}^{*2}$  are both minimal factorizations of  $H$  in  $\mathcal{P}_{\text{fin},1}(H)$ . However,  $(\mathbf{a}, \mathbf{b}) \notin \mathcal{C}_{\mathcal{P}_{\text{fin},1}(H)}$ , because  $\mathcal{P}_{\text{fin},1}(H)$  is a reduced monoid. Therefore,  $\mathcal{P}_{\text{fin},1}(H)$  is not minimally factorial, so leading to a contradiction and completing the proof.  $\square$

At this point, we have completely characterized the correlation between the ground monoid  $H$  and whether  $\mathcal{P}_{\text{fin},1}(H)$  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  $\mathcal{P}_{\text{fin},\times}(H)$ , 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  $\mathcal{P}_{\text{fin},\times}(H)$  HmF or minimally factorial. However, what we have shown indicates, we believe, that the arithmetic of  $\mathcal{P}_{\text{fin},1}(H)$  and  $\mathcal{P}_{\text{fin},\times}(H)$  is robust and ripe for more focused study.

### 4.3 Cyclic Monoids and Interval Length Sets

For those monoids  $H$  with  $\mathcal{P}_{\text{fin},1}(H)$  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  $\mathcal{P}_{\text{fin},0}(\mathbb{Z}/n\mathbb{Z})$  and also mention some results on  $\mathcal{P}_{\text{fin},0}(\mathbb{N})$  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  $\mathcal{P}_{\text{fin},1}(H)$ .

We invite the reader to review Section 1.3 before reading further. Also, note that, through the whole section, we have replaced the notation  $\mathcal{P}_{\text{fin},1}(H)$  with  $\mathcal{P}_{\text{fin},0}(H)$  when  $H$  is written additively (cf. Example 4.2.2).

**Definition 4.3.1.** Let  $X \in \mathcal{P}_{\text{fin},0}(\mathbb{Z}/n\mathbb{Z})$ . We say that a non-empty factorization  $\mathbf{a} = A_1 * \cdots * A_\ell \in \mathcal{Z}(X)$  is a *non-reducible factorization* (or, shortly, 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  $\mathcal{P}_{\text{fin},0}(\mathbb{Z}/n\mathbb{Z})$  is a minimal factorization.

*Proof.* Let  $\mathbf{a} = A_1 * \cdots * A_\ell$  be an NR-factorization in  $\mathcal{P}_{\text{fin},0}(\mathbb{Z}/n\mathbb{Z})$  of length  $\ell$ , and assume for the sake of contradiction that  $\mathbf{a}$  is not minimal. Since  $\mathcal{P}_{\text{fin},0}(\mathbb{Z}/n\mathbb{Z})$  is reduced and commutative, the factorizations which are  $\mathcal{C}_{\mathcal{P}_{\text{fin},0}(\mathbb{Z}/n\mathbb{Z})}$ -congruent to  $\mathbf{a}$  are exactly the words  $A_{\sigma(1)} * \cdots * A_{\sigma(\ell)}$ , where  $\sigma$  is an arbitrary permutation of the interval  $[1, \ell]$ . So, on account of Proposition 4.1.6(i), the non-minimality of  $\mathbf{a}$  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  $\mathbf{a}$  is an NR-factorization, and considering that, for each  $i \in [1, \ell]$ ,  $A_i$  is an atom of  $\mathcal{P}_{\text{fin},0}(\mathbb{Z}/n\mathbb{Z})$  and hence  $\max \hat{A}_i \geq 1$ , it follows from the above that

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

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

We are aiming to find, for every  $k \in [2, n-1]$ , a set  $X_k \in \mathcal{P}_{\text{fin},0}(\mathbb{Z}/n\mathbb{Z})$  for which  $\mathbf{L}^m(X_k) = [2, k]$ , on the assumption that  $n \geq 5$  is odd: Surprisingly, most of the difficulty lies in showing that  $2 \in \mathbf{L}^m(X_k)$ . 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  $\mathcal{P}_{\text{fin},0}(\mathbb{Z}/n\mathbb{Z})$ :

- (i)  $B_h := \{\overline{0}\} \cup \{\overline{1}, \overline{3}, \dots, \overline{h}\}$  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  $X, Y \in \mathcal{P}_{\text{fin},0}(\mathbb{Z}/n\mathbb{Z})$ . 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  $\bar{1} \in B_h$ , we must have  $\bar{1} \in X \cup Y$ . However, if  $\bar{1} \in X$  and  $a \in Y$  for some  $a \in B_h \setminus \{\bar{0}\}$ , 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  $Y = \{\bar{0}\}$ , 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  $\ell \geq 5$  and suppose  $C_\ell = X + Y$  for some  $X, Y \in \mathcal{P}_{\text{fin},0}(\mathbb{Z}/n\mathbb{Z})$  with  $X, Y \neq \{\bar{0}\}$ .

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  $x \in X \setminus \{\bar{0}\}$  and  $y \in Y \setminus \{\bar{0}\}$ . 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  $X = \{\bar{0}, x\}$  and  $Y = \{\bar{0}, y\}$  for some non-zero  $x, y \in \mathbb{Z}/n\mathbb{Z}$ , with the result that  $|X + Y| \leq 4 < |C_\ell|$ , a contradiction.

It follows (without loss of generality) that  $\overline{\ell+1} \in Y$ . Then  $X \subseteq \{\bar{0}, \bar{\ell}, \overline{\ell+1}\}$ , 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  $Y \subseteq \{\bar{0}, \bar{1}, \bar{\ell}, \overline{\ell+1}\}$  for similar reasons. As a consequence,

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

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

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  $n \geq 5$  and let  $k \in [2, n-1]$ . Then the set  $X_k = \{\bar{0}, \bar{1}, \dots, \bar{k}\}$  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  $C_\ell$  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  $h \geq 5$ . Then

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

and

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

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  $C_\ell$ , for some suitable choices of  $h$  and  $\ell$  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

$$X_k = B_{m+1} + C_{m-1} \text{ if } m \text{ is even.}$$

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

$$\text{it is seen that } X_k = C_m + C_{m-2} \text{ if } m \text{ is odd, and } X_k = C_{m-1} + C_{m-1} \text{ if } m \text{ is even.}$$

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.  $\square$

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

*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  $\ell$ . Choose some  $\ell \in [2, k - 1]$ ;  $X_{k-1}$  has an NR-factorization  $\mathfrak{a}$ , and it is straightforward to see that  $\{\bar{0}, \bar{1}\} * \mathfrak{a}$  is an NR-factorization of  $X_k$ . Letting  $\ell$  range over  $[2, k - 1]$ , this argument, Lemma 4.3.2, and Lemma 4.3.4 imply that  $\mathsf{L}^m(X_k) \supseteq [2, k]$ . Moreover, Proposition 4.2.3(i) yields the other inclusion and so we have  $\mathsf{L}^m(X_k) = [2, k]$ .  $\square$

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

*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  $(\mathbb{N}, +) \rightarrow Y : k \mapsto y^k$  determined by sending 1 to  $y$  induces an

isomorphism  $\mathcal{P}_{\text{fin},0}(\mathbb{N}) \rightarrow \mathcal{P}_{\text{fin},1}(Y)$ . 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

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

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

**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  $[2, k] \in \mathcal{L}^{\text{m}}(\mathcal{P}_{\text{fin},1}(H))$  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  $n := \text{ord}_H(y) > k$ . 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  $[2, k] \in \mathcal{L}^{\text{m}}(\mathcal{P}_{\text{fin},1}(Y)) \subseteq \mathcal{L}^{\text{m}}(\mathcal{P}_{\text{fin},1}(H))$ .  $\square$





## Chapter 5

### Atoms and Intervals in the Natural Power Monoid

Our goal in this chapter is to construct some families of atoms as a means of helping to give a lower bound on the number of factorizations in  $\mathcal{P}_{\text{fin},0}(\mathbb{N})$  of an interval of the form  $[0, n]$ .

#### 5.1 Construction of Residually Concentrated Atoms

As one finds when studying  $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ , determining whether a given subset of  $\mathbb{N}$  is an atom can be difficult. We will see later in Section 6.1 some ways of thinking about subset arithmetic which make this task simpler. A separate challenge is to systematically generate large collections of atoms; this is our primary undertaking in this section.

**Definition 5.1.1.** 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

$$|\{s \in S_{>0} : s \equiv t \pmod{m}\}| \leq 1 \quad \text{for all } t \in [0, m - 1] \setminus \{r\}. \quad (*)$$

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  $\{0\} \cup R \cup B$  with  $R$  and  $B$  as above, i.e., the collection of all subsets of  $\mathbb{N}$  which are  $r$ -concentrated modulo  $m$ .

We claim that, under suitable conditions on  $R$  and  $B$ , many elements of the collection  $\mathcal{X}_{m,r}$  are atoms. Toward proving this, we give the following lemmas.

**Lemma 5.1.2.** 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 5.1.1),  $x + y = x + y'$ . From here it is clear that  $y = y'$  and the result follows.  $\square$

The next lemma amounts to a mere unpacking of 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 5.1.3.** 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

$$|R| \leq (1 + \delta_0(Y \cap B))n_1 + (1 + \delta_0(X \cap B))n_2 + \delta_0(R)n_1n_2 + |2B \cap R|,$$

where

$$\delta_0(S) = \begin{cases} 1 & \text{if } S \text{ has an element } s \equiv 0 \pmod m \\ 0 & \text{otherwise.} \end{cases}$$

(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

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

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  $R \cap (X \cap R + Y \cap B)$ . If  $x \in X \cap R$  and  $y \in Y \cap B$  with  $x + y \in R$  then we must have  $y \equiv 0 \pmod m$ . There is at most one such  $y \in Y \cap B$ , so  $|R \cap (X \cap R + Y \cap B)| = \delta_0(Y \cap B)|X \cap R| = \delta_0(Y \cap B)n_1$ . Similarly,  $|R \cap (X \cap B + Y \cap R)| = \delta_0(X \cap B)n_2$ .

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  $|R \cap (X \cap R + Y \cap R)| \leq \delta_0(R)n_1n_2$ . 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  $|R| \leq (1 + \delta_0(Y))n_1 + (1 + \delta_0(X))n_2 + \delta_0(R)n_1n_2 + |2B \cap R|$ .

We can see (ii) by using what we have just proved, and by showing that at most one of  $\delta_0(X \cap B)$ ,  $\delta_0(Y \cap B)$ , and  $\delta_0(R)$  is nonzero. Firstly,  $\delta_0(R) = 1$  if and only if  $r = 0$ . 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  $b \equiv 0 \pmod m$  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  $\delta_0(X \cap B) + \delta_0(Y \cap B) + \delta_0(R) \leq 1$  and the inequality from (i) reduces to  $|R| \leq (1 + \delta_0(Y \cap B))n_1 + (1 + \delta_0(X \cap B))n_2 + \delta_0(R)n_1n_2 + |2B \cap R| \leq 3 + |2B \cap R|$ .  $\square$

**Proposition 5.1.4.** Let  $m \geq 2$ ,  $r \in [0, m - 1]$ , and let  $A := \{0\} \cup R \cup B$  with  $R$  and  $B$  as in Definition 5.1.1. If

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

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

*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  $m$ ,  $x, y \not\equiv 0 \pmod m$ . Now, by two applications of Lemma 5.1.2,  $|X \cap R|, |Y \cap R| \leq 1$ . Using Lemma 5.1.3, 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  $x, y \not\equiv \max(A) \pmod m$ , so  $x, y \not\equiv 0 \pmod m$  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  $r + r \equiv r \pmod m$ , so  $r = 0$ . Since  $B \subseteq A = X + Y$  but  $R + R \subseteq Nm$ , we must have  $B \subseteq X \cup Y$ . However, if  $b \in B \cap X$  then  $b + y \equiv b \pmod m$ , 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  $A = X + Y = \{0\} \cup (X \cap R) + \{0\} \cup (Y \cap R) \subseteq Nm$ , from which we conclude that  $B = \emptyset$ . This is a contradiction to condition (2) in the statement 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 5.1.2,  $|X \cap R| \leq 1$ . If  $x \in X \setminus \{0, a\}$  then  $x \not\equiv 0 \pmod{m}$  and so we also have  $|Y \cap R| \leq 1$ , whence we may finish by using Lemma 5.1.3 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 we now have  $A = X + Y = \{0, b\} + \{0\} \cup (Y \cap R) = \{0, b\} \cup (Y \cap R) \cup (b + Y \cap R)$ . From this, we deduce that  $R = \{b\}$ ; since we know that  $b \equiv 0 \pmod{m}$  and  $X = \{0, b\}$  is a factor of  $A$ , this yields a contradiction of condition (3), finishing the proof.  $\square$

**Definition 5.1.5.** Let  $S = \{s_0, \dots, s_k\} \subseteq \mathbb{N}$  be a nonempty subset with  $s_0 < \dots < s_k$ . 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  $S$   $\text{maxgap}(S) := \max\{s_i - s_{i-1} : i \in [1, k]\}$  to be the largest distance between consecutive elements of  $S$ .

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

For the sake of noting some concrete examples, we have  $\text{maxgap}([0, n]) = 1$  for every  $n$ ,  $\text{maxgap}(\{0, 2, 4, 6\}) = 2$ , and  $\text{maxgap}(\{0, 1, 2, 4, 8\}) = 4$ . 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  $\text{maxgap}(A) \leq h$ ; 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). Let  $\mathcal{A}_{m,r}^{(n)} := \mathcal{A}^{(n)} \cap \mathcal{X}_{m,r}$  be the set of  $r$ -concentrated atoms (modulo  $m$ ) with maximum equal to  $n$ . For our purposes, it will suffice to give an asymptotic lower bound for the size of  $\mathcal{A}_{m,r}^{(n)} \cap \mathcal{G}_h$ .

We begin by estimating the size of  $\mathcal{X}_{m,r} \cap \mathcal{G}_h$ , with the intent of later estimating how many members of this collection are atoms.

**Lemma 5.1.6.** Let  $m \geq 2$ ,  $r \in [0, m-1]$ , and  $h \geq 2$ . Then the number  $|\mathcal{P}^{(n)} \cap \mathcal{X}_{m,r} \cap \mathcal{G}_h|$  of sets  $S$  which are  $r$ -concentrated (modulo  $m$ ) with  $\max(S) = n$  and  $\text{maxgap}(S) \leq h$  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.* Given  $S \in \mathcal{P}^{(n)} \cap \mathcal{X}_{m,r}$ , 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  $\text{maxgap}(R) \leq h$  then  $\text{maxgap}(S) \leq h$ . This is because the consecutive elements of  $S$  are at least as close as the consecutive elements of  $R$ , since  $R, S \subseteq [0, n]$  and  $R \subseteq S$ . 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.

We may write  $R$  as  $R = \{\varepsilon_k(km + r) : k \in [0, \lfloor n/m \rfloor]\}$  for some  $\vec{\varepsilon}_R = (\varepsilon_0, \dots, \varepsilon_{\lfloor n/m \rfloor}) \in \{0, 1\}^{\lfloor n/m \rfloor + 1}$  (here we are essentially associating to  $R$  an “indicator function”).

Claim: if  $\vec{\varepsilon}_R$  does not have more than  $\lfloor h/m \rfloor$  consecutive zeros, then  $\max\text{gap}(R) \leq h$ .

Suppose that  $\vec{\varepsilon}_R$  does not have any string of more than  $\lfloor h/m \rfloor$  zeros. If this is the case, then any consecutive elements of  $R$  may be written as  $km + r$  and  $(k + t)m + r$ , where  $t \leq h/m$ . Then we have that  $(k + t)m + r - (km + r) = tm \leq \lfloor h/m \rfloor m \leq h$ , as we wished.

Thus  $R$  corresponds via  $\vec{\varepsilon}_R$  to an element of  $\mathcal{E}(\lfloor n/m \rfloor + 1, \lfloor h/m \rfloor)$ . Given another  $R' \subseteq [1, n] \cap (\mathbb{N}m + r)$  and a similarly chosen  $\vec{\varepsilon}_{R'} \in \mathcal{E}(\lfloor n/m \rfloor + 1, \lfloor h/m \rfloor)$ , it is not too difficult to see that  $\vec{\varepsilon}_R = \vec{\varepsilon}_{R'}$  only if  $R = R'$ , so this correspondence is one-to-one. Thus we have that

$$|\mathcal{P}^{(n)} \cap \mathcal{X}_{m,r} \cap \mathcal{G}_h| \geq |\{R \subseteq [1, n] \cap (\mathbb{N}m + r) : \max\text{gap}(R) \leq h\}| \geq |\mathcal{E}(\lfloor n/m \rfloor, \lfloor h/m \rfloor)|,$$

which is what we set out to show. □

**Lemma 5.1.7.** Let  $\mathcal{E}(N, t)$  be as in Lemma 5.1.6 and let  $f_t(N) := |\mathcal{E}(N, t)|$ . Then  $f_t(N) = 2^{N+1}$  for each  $N \leq t$  and, for  $N > t$ ,  $f_t(N)$  satisfies the recurrence relation

$$f_t(N) = f_t(N - 1) + \dots + f_t(N - t - 1).$$

(The sequence  $(f_1(N))$  is known as the *Fibonacci numbers*, and we will call  $(f_t(N))$  the *t-nacci numbers*).

*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  $f_t(N) = 2^{N+1}$ . All that remains is to verify the recurrence relation. 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

$$\vec{\varepsilon} = (\underbrace{\varepsilon_0, \dots, \varepsilon_{s-1}}_{s \text{ leading zeros}}, 1, \vec{\varepsilon}_*),$$

where  $\vec{\varepsilon}_*$  has length  $N + 1 - (s + 1)$ , 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 the recurrence  $f_t(N) = f_t(N - 1) + \dots + f_t(N - t - 1)$ . □

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 maximum gap.

**Lemma 5.1.8.** Let  $m \geq 2$ ,  $r \in [0, m-1]$ ,  $R \subseteq \mathbb{N}m + r$ , 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  $\max\text{gap}(R) \leq h$ ,  $|B| \geq 2$ , and  $n \geq \dots$

## Chapter 6

# Integer Partitions and 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.

## 6.1 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 6.1.1.** 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 6.1.2.** 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.  $\square$

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  $A \subsetneq X$ , 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 6.1.3.** Let  $H = \mathbb{N}$  and take  $X := [0, n]$  for some odd  $n \geq 11$ . We can show that  $A := \{0, 1, 3\}$  and  $B := \{0, 1, 3, \dots, n-2, n-3\}$  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 6.1.4.** 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  $\mathbf{fac}(X) = \emptyset$ .
- (2) If  $X = \{0\}$ , return  $\mathbf{fac}(X) = \emptyset$ .
- (3) If  $X$  is an atom, return  $\mathbf{fac}(X) = \{X\}$ .
- (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  $\mathbf{b} \in \mathbf{fac}(Y)$ , add  $A * \mathbf{b}$  to  $\mathbf{fac}(X)$ .
- (7) Return  $\mathbf{fac}(X)$ .

**Proposition 6.1.5.** For any  $X \in \mathcal{P}_{\text{fin},0}(\mathbb{N})$ ,  $\mathbf{fac}(X) = \mathcal{Z}_{\mathcal{P}_{\text{fin},0}(\mathbb{N})}(X)$ .

*Proof.* We can prove this by inducting on the size of  $X$ . If  $|X| = 1$  then  $X = \{1\}$  and  $\mathcal{Z}_{\mathcal{P}_{\text{fin},0}(H)}(X) = \emptyset = \mathbf{fac}(X)$  (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  $\mathcal{Z}_{\mathcal{P}_{\text{fin},0}(H)}(X) = \{X\} = \mathbf{fac}(X)$  by step (3).

It is apparent by construction that  $\mathbf{fac}(X) \subseteq \mathcal{Z}_{\mathcal{P}_{\text{fin},0}(H)}(X)$ , 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 6.1.2(iii) implies that  $A_1 + (X:A_1) = X$ . At this point, step (5) of the procedure for generating **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  $A_2 * \cdots * A_k \in \mathcal{Z}_{\mathcal{P}_{\text{fin},0}(X)}(Y) = \mathbf{fac}(Y)$ . Thus  $A_1 * \cdots * A_k \in \mathbf{fac}(X)$ , as we wished.  $\square$

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 6.1.6.** 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 6.1.7.** 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  $\mathcal{L}_H(x)$  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 efficient algorithm for factoring in  $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ , and also in our larger goal to quantify the “wildness” of factorizations of  $[0, n]$ .

**Definition 6.1.8.** Let  $n \geq 1$ . A *partition of  $n$*  is  $P = (m_1, \dots, m_k)$ , where  $m_1 \geq \dots \geq m_k \geq 1$  and  $m_1 + \dots + m_k = n$ . 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  $X \in \mathcal{P}_{\text{fin},0}(\mathbb{N})$  and for any partition  $P = (m_1, \dots, m_k)$  of  $\max(X)$ , we define the **set of factorizations of  $X$  of (partition) type  $P$**  to be

$$\mathcal{Z}^P(X) := \{A_1 * \dots * A_k \in \mathcal{Z}(X) : A_i \in \mathcal{A}^{(m_i)} \text{ for } i \in [1, k]\}.$$

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

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

**Remark 6.1.9.** 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 6.2.

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 6.1.4, this one will proceed constructively rather than inductively. It also supposes that one has found the sets  $\mathcal{A}^{(m)}$  for  $m < \max(X)$ . This is a computational endeavor in its own right, but removes some of the labor from the process of finding all factorizations of a given set  $X$ .

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

to **fac\_of\_type**( $X, P$ ).

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

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

Though this procedure for generating **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 also affords some opportunities for 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 6.3.

## 6.2 Admissible and Forbidden Types for Intervals

**Proposition 6.2.1.** 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 6.1.2. 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  $X \not\supseteq \{0, c\} + Y$ ; 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  $X = \{0, c\} + X : \{0, c\}$ .  $\square$

**Proposition 6.2.2.** Let  $n \geq 1$ .

- (i) For  $n \geq 4$ ,  $\mathcal{Z}^{(n-2,2)}([0, n]) = \emptyset$ .
- (ii) For even  $n \geq 4$ ,  $\mathcal{Z}^{(2,\dots,2)}([0, n]) = \emptyset$ .
- (iii) For odd  $n \geq 5$ ,  $\mathcal{Z}^{(3,2,\dots,2)}([0, n]) = \emptyset$ .

- (iv) For even  $n \geq 6$ ,  $\mathcal{Z}^{(4,2,\dots,2)}([0, n]) = \emptyset$ .
- (v) For odd  $n \geq 7$ ,  $\mathcal{Z}^{(5,2,\dots,2)}([0, n]) = \emptyset$ .

*Proof.* For (i), we can use the second part of Lemma 6.2.1 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  $\{0, 2\} + \dots + \{0, 2\}$  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  $(3, 2, \dots, 2)$ , then that factorization must include  $\{0, 1, 3\}$ . However, we see that

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

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

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

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

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  $n - 1 \notin \{0, 1, 3, 5\} + (m - 2)\{0, 2\}$ .  $\square$

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  $(7, 2, \dots, 2)$ . 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 6.2.3.** 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)  $B_{2h-1} := \{0, 1, 3, \dots, 2h-1\}$  for  $h \geq 1$ .
- (ii)  $B_{2h} := \{0, 1, 3, \dots, 2h-1, 2h\}$  for  $h \geq 3$ .
- (iii)  $C_{2h} := \{0, 2, 4, \dots, 2h\} \cup \{1\}$  for  $h \geq 2$ .
- (iv)  $C_{2h+1} := \{0, 2, 4, \dots, 2h\} \cup \{1, 2h+1\}$  for  $h \geq 3$ .

*Proof.* 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  $h \geq 3$ .  $\square$

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 6.2.4.** 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  $A'_r \in \mathcal{A}^{(r)}$  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

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

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:  $3 \leq r \leq 5 < q$ .

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:  $3 \leq r \leq q \leq 5$ .

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

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

*Proof.* 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.  $\square$

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 6.2.6.** For  $q \geq 6$  and  $t \geq 2$ , 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  $D_{3h} + t\{0, 2\} = [0, 3h + 2t]$ .  $\square$

**Remark 6.2.7.** 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 6.2.2, which says that  $D_q + \{0, 2\}$  cannot be an interval since  $D_q$  is an atom.

**Theorem 6.2.8.** 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,  $|\mathcal{T}([0, n])| = p(n) - 4$ , 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 6.2.6 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 6.2.4 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  $\mathbf{a}' \in \mathcal{Z}^{P'}([0, n - m_k])$ , we have that  $\mathbf{a} := \mathbf{a}' * \{0, m_k\} \in \mathcal{Z}^P([0, n])$ .

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  $P = (m_1, \dots, m_k, 1)$ .

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 6.2.3. Similarly, if  $k = 2$  we have by Lemma 6.2.4 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  $P' = (m_1, \dots, m_k)$ . If  $m_k = 1$ , then there is some  $\mathbf{a}' \in \mathcal{Z}^{P'}([0, n - 1])$  by induction, so that  $\mathbf{a} = \mathbf{a}' * \{0, 1\} \in \mathcal{Z}^P([0, n])$ . However, if  $m_k > 1$ , set  $Q = (m_1, \dots, m_{k-1}, 1)$  (a partition of  $n - m_k$ ). Again, we have by induction that there is some  $\mathbf{b} \in \mathcal{Z}^Q([0, n - m_k])$ . 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  $\mathbf{a} = \mathbf{b} * \{0, m_k\} \in \mathcal{Z}^P([0, n])$ , proving what we wished.  $\square$

### 6.3 Subsums and Near 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.



**Definition 6.3.1.** Let  $m_1, \dots, m_k$  be integers. We will refer to  $S = (m_1, \dots, m_k)$  as a *sequence* of integers. Define the **set of subsums of  $S$**  to be  $\Sigma(S) := \{\sum_{i \in I} m_i : I \subseteq [1, k]\}$ .

**Remark 6.3.2.** 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 [\[CITE SOME PAPERS\]](#). Ours 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  $S = (m_1, \dots, m_k)$  as a sum in  $\mathcal{P}_{\text{fin},0}(\mathbb{Z})$ :  $\Sigma(S) = \{0, m_1\} + \dots + \{0, m_k\}$ .

**Lemma 6.3.3.** Let  $m_1, \dots, m_k$  be positive integers with  $m_1 \geq \dots \geq m_k \geq 1$  and let  $n = m_1 + \dots + m_k$ . If  $k > n/2$  then  $\Sigma(m_1, \dots, m_k) = [0, n]$ .

*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

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

Thus  $k-1 > \frac{m_2 + \dots + m_k}{2}$  and we can apply the inductive hypothesis to  $T := (m_2, \dots, m_k)$ . 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  $m_1 \leq m_2 + \dots + m_k + 1$ , 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

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

Using this inequality twice, we have that

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

exactly as we wished. □

**Lemma 6.3.4.** 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  $P = (n/2 + 1, 1, \dots, 1)$ .

- $\Sigma(P) = 2 \cdot [0, n/2]$  and  $P = (2, \dots, 2)$

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

If  $m_k = 2$  then  $m_1 = n - (m_2 + \dots + m_k) \leq n - (k-1)(2) = n - (n/2 - 1)2 = 2$ . Thus we have  $m_1 = \dots = m_k = 2$  and so  $\Sigma(P) = \{0, 2\} + \dots + \{0, 2\} = \{0, 2, \dots, n\} = 2 \cdot [0, n/2]$  (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,

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

so  $k-1 > (m_2 + \dots + m_k)/2$ ; by Lemma 6.3.3,  $\Sigma(m-2, \dots, m_k) = [0, n - m_1]$ .

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

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

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

**Theorem 6.3.5.** Let  $X \in \mathcal{P}_{\text{fin},0}(\mathbb{N})$  and suppose that there is  $k \in \mathbb{L}(X)$  with  $k > \max(X)/2$ . Then  $X = [0, \max(X)]$ .

*Proof.* Let  $n = \max(X)$  and let  $\mathbf{a} \in \mathcal{Z}(X)$  be a factorization with length  $|\mathbf{a}| = k$ . Then there are integers  $m_1 \geq \dots \geq m_k \geq 1$  and atoms  $A_i \in \mathcal{A}^{(m_i)}$  with  $\mathbf{a} = A_1 * \dots * A_k$ . The result is immediate from Lemma 6.3.3, since we have

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

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

# Chapter 7

## Subsets of Integer Lattices

### 7.1 Passage Between Power Monoids

The natural power monoid  $\mathcal{P}_{\text{fin},0}(\mathbb{N})$  is connected to the study of many other power monoids. In this section we will mention some ways relating the study of  $\mathcal{P}_{\text{fin},0}(\mathbb{N})$  to other classes of power monoids. In some cases, we will be able to *locally transfer* the factorization behavior between  $\mathcal{P}_{\text{fin},0}(\mathbb{N})$  and other power monoids, (the meaning of this is made precise in Definition 7.1.2). This yields especially powerful results when we consider  $\mathbb{N}^d$ ; as we will see in Theorem 7.1.6 that the study of factorizations in  $\mathcal{P}_{\text{fin},0}(\mathbb{N})$  is essentially the same as that of  $\mathcal{P}_{\text{fin},0}(\mathbb{N}^d)$ . Highlighting these relationships between  $\mathcal{P}_{\text{fin},0}(\mathbb{N})$  and other monoids serves to further motivate the study of both  $\mathcal{P}_{\text{fin},0}(\mathbb{N})$  and its relatives.

As Fan and Tringali prove in [FT18, Theorem 3.8, Theorem 4.11], all of the factorization information of  $\mathcal{P}_{\text{fin},0}(\mathbb{N})$  embeds into *any* non-torsion monoid  $H$ . We briefly recall the basic ideas underpinning this fact below.

**Proposition 7.1.1.** Let  $H$  be a non-torsion monoid. Then there is an equimorphism from  $\mathcal{P}_{\text{fin},0}(\mathbb{N}) \rightarrow \mathcal{P}_{\text{fin},1}(H)$ .

*Proof.* If  $H$  is a non-torsion monoid, let  $x \in H$  be an element with infinite multiplicative order. Then the map  $f : \mathbb{N} \rightarrow \langle x \rangle$  given by  $n \mapsto x^n$  is an isomorphism (specifically, from  $(\mathbb{N}, +) \rightarrow (\langle x \rangle, \cdot)$ ). On the level of sets, this yields an isomorphism  $f : \mathcal{P}_{\text{fin},0}(\mathbb{N}) \rightarrow \mathcal{P}_{\text{fin},1}(\langle x \rangle)$ . In turn, this isomorphism induces an isomorphism  $f^* : \mathcal{F}(\mathcal{A}(\mathcal{P}_{\text{fin},0}(\mathbb{N}))) \rightarrow \mathcal{F}(\mathcal{A}(\mathcal{P}_{\text{fin},1}(\langle x \rangle)))$ . As a consequence, for any  $X \in \mathcal{P}_{\text{fin},0}(\mathbb{N})$ , we have a bijection  $f^* : \mathcal{Z}_{\mathcal{P}_{\text{fin},0}(\mathbb{N})}(X) \rightarrow \mathcal{Z}_{\mathcal{P}_{\text{fin},1}(\langle x \rangle)}(f(X)) = \mathcal{Z}_{\mathcal{P}_{\text{fin},1}(H)}(f(X))$ , where the last inequality follows from Proposition 3.1.2 (ii) (that is,  $\mathcal{P}_{\text{fin},1}(\langle x \rangle)$  is divisor-closed in  $\mathcal{P}_{\text{fin},1}(H)$ ).  $\square$

Thus the study of factorizations of  $\mathcal{P}_{\text{fin},0}(\mathbb{N})$  actually tells us about the factorization of certain subsets of  $H$ . 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 7.1.2.** 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  $f : H \rightarrow K$  such that

- (i)  $f$  is atom-preserving; for every  $a \in \mathcal{A}(H)$ ,  $f(a) \in \mathcal{A}(K)$ .
- (ii)  $f^* : \mathcal{Z}_H(x) \rightarrow \mathcal{Z}_K(f(x))$  is a bijection (here  $f^*$  is identified with the restriction to  $\mathcal{Z}_H(x)$  of the induced map  $f^* : \mathcal{F}^*(\mathcal{A}(H)) \rightarrow \mathcal{F}^*(\mathcal{A}(K))$ ).

We will refer to  $f$  as an  $x$ -**transfer** to  $K$ . One may also note that, by construction,  $f^* : \mathcal{Z}_H(x) \rightarrow \mathcal{Z}_K(f(x))$  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 7.1.3.** Let  $\varphi : H \rightarrow K$  be a homomorphism of (additively written) 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)  $\varphi : \mathcal{P}_{\text{fin},0}(H) \rightarrow \mathcal{P}_{\text{fin},0}(K)$  is an atom-preserving map.
- (iii) The induced map  $\varphi^* : \mathcal{Z}_{\mathcal{P}_{\text{fin},0}(H)}(W) \rightarrow \mathcal{Z}_{\mathcal{P}_{\text{fin},0}(K)}(\varphi(W))$  is a length-preserving bijection.

*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  $\Phi$  is a bijection; we will show that  $\Phi$  has an inverse. Let  $\mathbf{b} = B_1 * \cdots * B_k \in \mathcal{Z}(\varphi(W))$ . 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  $\mathbf{b} \mapsto \varphi^{-1}(B_1) * \cdots * \varphi^{-1}(B_k)$  is inverse to  $\varphi^*$ , which is all we needed to show.  $\square$

**Remark 7.1.4.** Note that the property  $(*)$  in Lemma 7.1.3 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 7.1.5.** 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  $\pi_r : \mathbb{N}^{r+1} \rightarrow \mathbb{N}$  is the projection map from the  $r$ th coordinate. Define  $\varphi : \mathbb{N}^{r+1} \rightarrow \mathbb{N}^r$  by  $\varphi(w_1, \dots, w_{r+1}) = (w_1, \dots, w_{r-1}, w_r + Nw_{r+1})$ . Then

- (i)  $\varphi$  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)  $\varphi^* : \mathcal{Z}_{\mathcal{P}_{\text{fin},0}(\mathbb{N}^{r+1})}(W) \rightarrow \mathcal{Z}_{\mathcal{P}_{\text{fin},0}(\mathbb{N}^r)}(\varphi(W))$  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  $x = (x_1, \dots, x_{r+1})$  (and so on), and suppose that  $\varphi(x) = \varphi(y) + \varphi(z)$ . Then we immediately have  $x_i = y_i + z_i$  for all  $i < r$ . For the  $r$ th 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 7.1.3. □

**Theorem 7.1.6.** 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  $X \in \mathcal{P}_{\text{fin},0}(\mathbb{N}^2)$ . Proposition 7.1.5 gives us an  $X$ -transfer to  $\varphi : \mathcal{P}_{\text{fin},0}(\mathbb{N}^2) \rightarrow \mathcal{P}_{\text{fin},0}(\mathbb{N})$ , 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 7.1.5 yields an  $X$ -transfer  $\varphi$  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  $\psi : \mathcal{P}_{\text{fin},0}(\mathbb{N}^{d-1}) \rightarrow \mathcal{P}_{\text{fin},0}(\mathbb{N})$ . Then  $\psi \circ \varphi : \mathcal{P}_{\text{fin},0}(\mathbb{N}^d) \rightarrow \mathcal{P}_{\text{fin},0}(\mathbb{N})$  is an  $X$ -transfer, so we conclude that  $\mathcal{P}_{\text{fin},0}(\mathbb{N}^d)$  is locally transferrable to  $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ . □

We will revisit the connection between  $\mathcal{P}_{\text{fin},0}(\mathbb{N})$  and the natural lattice in the next section. For now, we will mention some more connections to other power monoids.

## 7.2 Independence Arguments in the Natural Lattice

Theorem 7.1.6 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.,  $\mathcal{L}(X)$ ).

**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  $H$  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  $u_1 - v_1 = u_2 - v_2 \in \mathbb{Z}U_1 \cap \mathbb{Z}U_2 = \{0\}$ , 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

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

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.  $\square$

**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)  $U_j = \sum_{i=1}^k U_j \cap A_i$ .
- (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)  $k \leq \max \mathbf{L}(U) + \max \mathbf{L}(V)$ .

*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  $u_1, \dots, u_k \in U$  and  $v_1, \dots, v_k \in V$  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 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  $A_i = (U + V) \cap A_i = V \cap A_i = \{0\}$  (we used (ii) at the second equal sign).

Finally, for (iv): let  $\ell = \max \mathbf{L}(U)$  and  $m = \max \mathbf{L}(V)$ . 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.  $\square$

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

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

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

*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  $V_j = V_j \cap A_{f(j)} \subseteq A_{f(j)}$ .

To prove (ii), 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  $V_1, \dots, V_m$  are totally  $\mathbb{Z}$ -independent,  $V'$  and  $V''$  are  $\mathbb{Z}$ -independent.

For each  $j \in J$  and each  $i \neq h$ ,  $V_j \cap A_i = \{0\}$ . An easy induction on  $|J|$  then yields that  $V' \cap A_i = \{0\}$  for each  $i \neq h$ . As a result, we have (using Proposition 7.2.3(i)) that  $V' = \sum_i V' \cap A_i = V' \cap A_h$ .

On the other hand, for  $j \in K$ ,  $V_j \cap A_h = \{0\}$ , so  $(V' + V_j) \cap A_h = V' \cap A_h$  (using Prop 7.2.3 (ii)). By induction on  $|K|$ , we can see that  $V'' \cap A_h = 0$ , so that  $A_h = V \cap A_h = (V' + V'') \cap A_h = V' \cap A_h = V'$ , completing the proofs of both (ii) and (iii).  $\square$

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

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

Let  $A_1, \dots, A_k$  be atoms with  $V = \sum_i A_i$ . As in Lemma 7.2.4(i), there is  $f : [1, m] \rightarrow [1, k]$  with  $V_j \subseteq A_{f(j)}$  for each  $j \in [1, m]$ . We wish to show that  $f$  is injective; let  $h \in [1, k]$  and let  $J = f^{-1}(h)$ . By Lemma 7.2.4(ii),  $A_h = V \cap A_h = \sum_{j \in J} V_j$ , which is only an atom if  $|J| = 1$ , making  $f$  injective.

We have shown more; we in fact have, for each  $j \in [1, m]$ ,  $V_j = A_{f(j)}$ . All that remains to see is that  $f$  is a surjection. To see this, suppose  $A_i \notin f([1, m])$ . Then  $V_j \cap A_i = \{0\}$  for all  $j \in [1, m]$ , and we have by Proposition 7.2.3(ii) and induction that  $A_i = \{0\}$ . However, this is impossible since  $A_i$  is an atom.

We conclude that  $f$  is a bijection and that the only factorization of  $V$  (up to reordering) is  $V_1 * \dots * V_m$ .  $\square$

**Example 7.2.6.** Theorem 7.2.5 allows us to partially recover [FT18, Proposition 4.9]. We recall here the content of Fan and Tringali's result: Let  $a_1, \dots, a_\ell \in \mathbb{N}$  such that  $a_1 + \dots + a_i < \frac{1}{2}a_{i+1}$  for  $i \in [1, \ell - 2]$  and (if  $\ell \geq 2$ )  $a_1 + \dots + a_{\ell-1} < a_\ell - a_{\ell-1}$ . Then  $Z(\{0, a_1\} + \dots + \{0, a_\ell\}) = \{\{0, a_1\} * \dots * \{0, a_\ell\}\}$ .

There are many sequences of integers  $a_1, \dots, a_\ell$  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  $i$ th standard basis vector (whose entries are all zero, except for a 1 in the  $i$ th coordinate). Let  $V = \{0, e_1\} + \dots + \{0, e_\ell\}$ ; by Theorem 7.2.5,  $V$  factors uniquely. We will follow the procedure given in Theorem 7.1.6 to “flatten”  $V$  into a subset of  $\mathbb{N}$  which still factors uniquely. According to this procedure, we need maps  $\mathbb{N}^\ell \rightarrow \mathbb{N}^{\ell-1} \rightarrow \dots \rightarrow \mathbb{N}$ .



For  $i \in [1, \ell - 1]$ , define  $\varphi_i : \mathbb{N}^{i+1} \rightarrow \mathbb{N}^i$  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  $i$ th standard basis vector in  $\mathbb{N}^i$ ). Let  $V_\ell = V$  and  $V_i = \varphi_i(V_{i+1})$  for  $i < \ell$ . By Proposition 7.1.5,  $\varphi_i$  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  $\varphi$  on  $e_1, \dots, e_\ell$  (since  $\varphi$  is a homomorphism). 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.

We end this section with a result with a result asserting some degree of compatibility between uniqueness of factorization and  $\mathbb{Z}$ -independence.

**Theorem 7.2.7.** Let  $U \in \mathcal{P}_{\text{fin},0}(\mathbb{N}^d)$  be an element whose two longest factorizations have lengths  $\ell$  and  $N$ , with  $\ell < N$ . Suppose  $V_1, \dots, V_m \subseteq \mathbb{N}^d$  are atoms so that  $U, V_1, \dots, V_m$  are totally  $\mathbb{Z}$ -independent. Further assume that  $U$  has a unique longest factorization (of length  $N$ ). Then  $\mathcal{L}(U + V_1 + \cdots + V_m) \cap [\ell + 1, \infty] = \{N + m\}$ .

*Proof.* For convenience, let  $V := V_1 + \cdots + V_m$ . Suppose that  $k > \ell + m$  and that there are atoms  $A_1, \dots, A_k$  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  $J = \{j : V_j \subseteq A_s\}$  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  $v \in V$ ,  $U + v = \sum_{i < s} U \cap A_i + (U + v) \cap A_s$ .

We move to show both inclusions. First suppose  $u \in U$ . Then  $u + v \in \sum_{i=1}^\ell A_i$ , and we can find  $u_1, \dots, u_s \in U$  and  $v_t, \dots, v_k \in V$  so that  $u_i \in A_i$  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  $U, V_1, \dots, V_m$  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  $u_1, \dots, u_s \in U$  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:  $(U + v) \cap A_s = U \cap A_s + v$ .

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

$$U = \sum_{i < s} U \cap A_i + A. \quad (\text{D1})$$

On the other hand, we also have that

$$U = \sum_{i < s} U \cap A_i + U \cap A_s. \quad (\text{D2})$$

We will now show that we can cancel the common factors that appear in these two decompositions.

First, as an aside, note that  $t > \ell$ . If this were not the case and  $t \leq \ell$ , then  $k = |[1, s] \cup [t, k]| \leq \ell + |[t, k]| \leq \ell + m$ , which contradicts our initial assumption about  $k$ .

This is significant because  $\sum_{i < t} U \cap A_i = \sum_{i < t} A_i$  is a sum of at least  $\ell + 1$  atoms, and  $U$  has only one factorization consisting of more than  $\ell$  atoms. Say  $B_1, \dots, B_N$  are the atoms with  $U = \sum_{i=1}^N B_i$ . Then, by renumbering if needed, there is some  $h$  for which  $\sum_{i < s} U \cap A_i = B_1 + \dots + B_h$ .

Consequently, by the uniqueness of the atoms  $B_i$ , it must be that  $B_1 + \dots + B_h$  can be cancelled in the decompositions (D1) and (D2), leaving

$$A = B_{h+1} + \dots + B_N = U \cap A_s,$$

and we have proved the claim.

Claim E:  $A_s$  is not an atom.

To see this, we compute

$$\begin{aligned}
A_s &= (U + V) \cap A_s = (U + V' + V'') \cap A_s \\
&= (U + V') \cap A_s && \text{(by Claim A and Proposition 7.2.3)} \\
&= \bigcup_{v \in V'} (U + v) \cap A_s \\
&= \bigcup_{v \in V'} (U \cap A_s + v) && \text{(by Claim D)} \\
&= U \cap A_s + V'.
\end{aligned}$$

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  $s \in \mathbf{L}(U)$  and, by identical reasoning for  $V$ , that  $|[t, k]| = m$ . We conclude that  $k \in \mathbf{L}(U) + m$  and, due to the assumption that  $k > \ell + m$ , it must be the case that  $k = N + m$ .  $\square$

### 7.3 Length Sets in High-Dimensional Lattices

In this section, we wish to show that certain prescribed sets occur as sets of lengths of elements of  $\mathcal{P}_{\text{fin},0}(\mathbb{N}^d)$  (and hence as sets of lengths of elements of  $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ ). First, we will recover a version of [FT18, Proposition 4.10] which says that, for any  $n \geq 2$ , there is an element  $U$  which has exactly two factorizations: one of length 2, and one of length  $n + 1$ . Then we will extend this construction to a class of constructions which realizes some new sets of lengths.

We will be working with a particular construction for most of this section, so we take a moment to set some notation.

**Definition 7.3.1.** Fix an integer  $n \geq 2$  and let  $d \geq n$ . For  $i \in [1, n]$ , let  $e_i \in \mathbb{N}^d$  be the  $i$ th standard basis vector, whose components are all zero except for a single 1 in the  $i$ th coordinate.

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. Before proving this fact or

making use of it, 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  $\{0\}$ . Observe first that  $f$  cannot be written as a sum of two or more elements of  $B$ , since  $f \notin \text{span}_{\mathbb{Z}}(\{e_1, \dots, e_{n-1}\} \cup V)$  and the  $e_n$  coefficient of  $g$  is larger than that of  $f$ .

One can also see that  $g$  cannot be written as a sum of two or more elements of  $B$ . As above,  $g \notin \text{span}_{\mathbb{Z}}(\{e_1, \dots, e_{n-1}\} \cup V)$ . The only remaining possibility is that  $f$  is included at least twice in the sum so that  $g = 2f + b$  for some  $b \in B$ . This is impossible, as the  $e_1$  coefficient of  $2f + b$  is at least 2, whereas that of  $g$  is 1.

We conclude from these observations 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.  $\square$

**Theorem 7.3.3.** Let  $n \geq 2$  and let  $e_1, \dots, e_n \in \mathbb{N}^n$  be  $\mathbb{Z}$ -linearly independent. Set  $f = \sum_{i=1}^n e_i$ ,  $g = f + e_n$ . Letting  $U = \sum_{i=1}^n \{0, e_i\} + \{0, g\}$ , we have

$$\mathcal{Z}_{\mathcal{P}_{\text{fin},0}(\mathbb{N}^n)}(U) = \left\{ \{0, e_1\} * \dots * \{0, e_n\} * \{0, g\}, \left[ \sum_{i=1}^{n-1} \{0, e_i\} + \{0, g\} \right] \cup \{f\} * \{0, e_n\} \right\}.$$

*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  $2e_i \notin C =$

$$\{e_I : I \subseteq [1, n]\}.$$

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  $2e_1 + e_{K \setminus \{1\}} = e_1 + e_K \in X + Y$ , a contradiction.

Claim B: For  $I \subsetneq [1, n]$ ,  $e_I \in X$  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  $\geq 2$ , which is a contradiction.

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  $> 2$ ). 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 since this element has an  $e_n$ -coefficient  $\geq 4$ .

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  $I \subsetneq [1, n]$ .

Let  $I \subseteq I_X$  with  $I \subsetneq [1, n]$ . 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 (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  $I \neq [1, n]$ ,  $K \subsetneq [1, n]$  and so  $K \subseteq I_Y$  by (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  $g + e_I = e_J + e_K$ , and the only possibility is that  $I = [1, n - 1]$  and  $J = K = [1, n]$  (so  $e_J = e_K = f$ ). 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  $X = \{0, g\}$  and  $Y = \sum_{i=1}^n \{0, e_i\}$  by Claim A. By Theorem 7.2.5,  $Y$  factors uniquely and we have  $\{0, e_1\} * \cdots * \{0, e_n\} * \{0, g\} \in \mathcal{Z}_{\mathcal{P}_{\text{fin}, 0}(\mathbb{N}^n)}(U)$ .

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

$$X \supseteq \{0, g\} + \sum_{i \in I_X} \{0, e_i\} \quad (1)$$

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 Claim (B), as well as (A) and (D), to say that  $Y = \sum_{i \in I_Y} \{0, e_i\}$ .

With this, we can say more about the structure of  $X$ . By Proposition 6.1.2, we have

$$X \subseteq U:Y = \bigcap_{y \in Y} (U - y) = \bigcap_{K \subseteq I_Y} \underbrace{\{e_I - e_K, g + e_I - e_K : I \subseteq [1, n]\}}_{=: U_K}$$

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 our work here with (1) above, that

$$\{0, g\} + \sum_{i \in I_X} \{0, e_i\} \subseteq X \subseteq U:Y \subseteq \left[ \{0, g\} + \sum_{i \in I_X} \{0, e_i\} \right] \cup \{f\},$$

so we have determined  $X$  almost exactly, up to the choice of whether  $f \in X$ .

Before discussing the possible factorizations of  $X$ , recall that  $Y = \sum_{i \in I_Y} \{0, e_i\}$  and so  $Y$  factors uniquely (by Theorem 7.2.5) as the sum of the  $\{0, e_i\}$  for  $i \in I_Y$ .

Now we turn to  $X$ ; first suppose  $f \notin X$ . Then  $X = \{0, g\} + \sum_{i \in I_X} \{0, e_i\}$ , which has a unique factorization (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  $\{0, g\} * \{0, e_1\} * \cdots * \{0, e_n\} \in \mathcal{Z}_{\mathcal{P}_{\text{fin},0}(\mathbb{N}^n)}(U)$ .

If  $f \in X$ , then  $X = [\{0, g\} + \sum_{i \in I_X} \{0, e_i\}] \cup \{f\}$  (and  $Y = \{0, e_n\}$  per our considerations in (F3')).

By Lemma 7.3.2,  $X$  is an atom, producing the factorization  $X * \{0, e_n\} \in \mathcal{Z}_{\mathcal{P}_{\text{fin},0}(\mathbb{N}^n)}(U)$  and completing the proof.  $\square$

**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].

**Corollary 7.3.5.** Fix  $n \geq 2$  and  $m \geq 1$ , and let  $V_1, \dots, V_m \subseteq \mathbb{N}^d$  be atoms such that  $U_{n+1}, V_1, \dots, V_m$  are totally  $\mathbb{Z}$ -independent. Then  $\mathsf{L}(U_{n+1} + V_1 + \dots + V_m) = [2, m+2] \cup \{m+n+1\}$ .

*Proof.* For convenience, let  $U := U_{n+1}$  and  $V := V_1 + \dots + V_m$ . 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

$$U + V = \{0, e_n\} + B_h + V_1 + \dots + V_h$$

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 Theorem 7.2.7,  $\mathsf{L}(U + V) \cap [m+3, m+n+1] = \{m+n+1\}$ .  $\square$





# 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.
- [AFRS03] Michael Axtell, Sylvia Forman, Nick Roersma, and Joe Stickles. Properties of u-factorizations. *International Journal of Commutative Rings*, 2, 01 2003.
- [AM85] D. D. Anderson and Raj Markanda. Unique factorization rings with zero divisors. *Houston J. Math.*, 11(1):15–30, 1985.
- [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.
- [BBM17] Nicholas R. Baeth, Brandon Burns, and James Mixco. A fundamental theorem of modular arithmetic. *Period. Math. Hungar.*, 75(2):356–367, 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.
- [Fle69a] C. R. Fletcher. Unique factorization rings. *Proc. Cambridge Philos. Soc.*, 65:579–583, 1969.
- [Fle69b] C. R. Fletcher. Unique factorization rings. *Mathematical Proceedings of the Cambridge Philosophical Society*, 65(3):579–583, 1969.
- [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.
- [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.
- [Gor80] Daniel Gorenstein. *Finite groups*. Chelsea Publishing Co., New York, second edition, 1980.
- [Gry13] David J. Gryniewicz. *Structural additive theory*, volume 30 of *Developments in Mathematics*. Springer, Cham, 2013.
- [Tri17] Salvatore Tringali. Structural properties of subadditive families with applications to factorization theory. *arXiv e-prints*, page arXiv:1706.03525, Jun 2017.
- [Whi88] Thomas A. Whitelaw. *Introduction to abstract algebra*. Blackie, Glasgow, 2nd ed. edition, 1988.