Subset Decompositions: Factorization in Power Monoids

Austin A. Antoniou

October 24, 2019

Contents

Chapter 1

Introduction

Factorization theory pursues a full understanding of how complex objects decompose into their simplest constituent parts. Depending on the algebraic structure in question, the difficulty of gaining such an understanding can vary wildly. Some objects can be broken down in exactly one way, while others exhibit more exotic behavior and are able to be broken down into many 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 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.

1.2 Plan and Main Results

We will conclude this chapter by defining and recalling some preliminary notions which are necessary to move forward with our discussion, including the formal language we will use to encode the data of factorizations and some notions which capture the varying degrees of non-unique factorization.

Chapter 2 will introduce the main object of this paper: 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. 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 $\mathcal{P}_{\text{fin}}(H)$. We will see in Section 2.1 when it is reasonable to study factorizations in $\mathcal{P}_{\text{fin},1}(H)$. As it turns out, this monoid is atomic exactly when H has no nontrivial idempotents or elements of order 2 (Theorem 2.1.9). Moreover, $\mathcal{P}_{\text{fin},1}(H)$ has bounded factorization lengths if and only if H is torsion-free (Theorem 2.1.11).

When H is not torsion-free, the usual tools for measuring non-uniqueness of factorization in $\mathcal{P}_{\text{fin},1}(H)$ become degenerate. To compensate for this, we introduce the notion of *minimal factorizations* in a general 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). 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 $\mathcal{P}_{\text{fin},0}(\mathbb{Z}/n\mathbb{Z})$.

Chapter 3 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 3.2.8), 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 $\max(\mathsf{L}_{\mathcal{P}_{\text{fin},0}(\mathbb{N})}(X)) \leq \max(X)/2$.

Chapter 4 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 $d > 1$; namely, these monoids share essentially the same factorization behavior. 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. This affords us the opportunity to use higher-dimensional geometric intuition to attack problems in $\mathcal{P}_{\text{fin},0}(\mathbb{N})$. Ruminations in this vein bear the fruit of some new methods for understanding factorizations in $\mathcal{P}_{\text{fin},0}(\mathbb{N}^d)$. This line of thought also 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. Furthermore, we can push these methods to obtain Theorem 4.3.5, 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.

1.3 Preliminaries

1.3.1 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. In general, unless otherwise specified, lowercase letter will usually refer to elements of a monoid; ordinary uppercase letters to sets and subsets; script or calligraphic uppercase letters to collections of subsets. Specifically, i, j, k, ℓ, m, and n will usually stand for non-negative integers. 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.

The *free monoid* on some generating set S will be denoted by $\mathcal{F}^*(S)$. This monoid should be thought of as the set of formal words whose letters belong to S. Its operation, denoted by $*$ to avoid confusion where another multiplicationmis present, is meant to be interpreted as the concatenation of words. The elements of $\mathcal{F}^*(S)$ will usually be represented by the fraktur letters $\mathfrak{a}$, $\mathfrak{b}$, and so on. The *length* of a word $\mathfrak{s} = s_1 * \cdots * s_\ell \in \mathcal{F}^*(S)$, where each $s_i \in S$ and $|\mathfrak{s}| := \ell$. The empty word $\emptyset$ is said to have length zero.

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.

1.3.2 Fundamental Notions of Factorization Theory

Definition 1.3.1. A monoid is a pair $(H, \cdot)$, where H is a set and $\cdot$ is a binary operation (called multiplication in the absence of any other name) on H, satisfying

1. Associativity: for every $x, y, z \in H$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$

2. Identity: there is an element $1_H \in H$ such that $1 \cdot x = x \cdot 1 = x$ for all $x \in H$

Often, the operation will be omitted when no confusion can arise; it is standard practice to write xy instead of $x \cdot y$. Similarly, the identity 1_H will usually be written as 1.

A map $\varphi : H \to K$ between monoids is a **homomorphism** if $\varphi(1_H) = 1_K$ and $\varphi(xy) = \varphi(x)\varphi(y)$.

Definition 1.3.2. Let H be a monoid.

1. $u \in H$ is a **unit** if there is $v \in H$ with $uv = vu = 1$. The set of units of H is denoted by $H^\times$. H is called *reduced* if $H^\times = \{1\}$.

2. $a \in H \setminus H^\times$ 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 $\mathcal{A}(H)$.

3. $x, y \in H$ are **associates** if there are units $u, v \in H^\times$ so that $x = uyv$. In this case, we write $x \sim y$.

4. $x \in H$ is **idompotent** (or **an idempotent**) if $x^2 = x$.

Note that a is an atom if and only if every divisor of a is either an associate of a or a unit in H. This may be taken as a definition of an atom, or used as a starting point for generalized notions of an atom, as in [RANTHONY REFERENCE FOR DIFFERENT NOTIONS OF ASSOCIATE/ATOMS].

Proposition 1.3.3. Let H be a monoid, let $a \in \mathcal{A}(H)$, and let $u, v \in H^\times$. Then $uav \in \mathcal{A}(H)$.

Definition 1.3.4. Let H be a monoid. The **factorization homomorphism** of H is the unique homomorphism $\pi_H : \mathcal{F}^*(H) \to H$ satisfying $\pi_H(x) = x$ for all $x \in H$.

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

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

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

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

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

Definition 1.3.5. 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 $[\![1, n]\!]$) such that $b_i \sim a_{\sigma(i)}$ for all $i \in [\![1, k]\!]$.

3. $\mathfrak{a}$ and $\mathfrak{b}$ have the same product; i.e., $\pi_H(\mathfrak{a}) = \pi_H(\mathfrak{b})$.

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

Definition 1.3.6. Let H be a monoid and $x \in H \setminus H^\times$. The **set of factorization classes** of x is

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

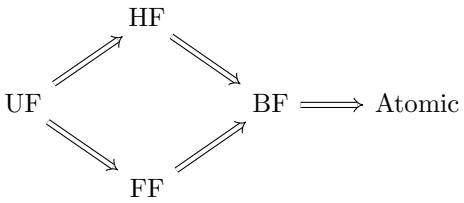
and the **set of (factorization) lengths** of x is

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

Definition 1.3.7. 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 $x \in H \setminus H^\times$, $|\mathsf{Z}_H(x)| = 1$.
- 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 1.3.8. We have the following logical implications among the properties defined just above:



Example 1.3.9. It is helpful to see some examples or non-examples of each of these properties.

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

(ii) 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 $(2,2)(3,3)(2,3) = (12,18) = (2,3)(2,3)(3,2)$.

(iii) 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 $\mathrm{Int}(D) := \{f(x) \in K[x] : f(D) \subseteq D\}$ 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 $f(x) \in \mathrm{Int}(D)$. Additionally, one can pose similar questions regarding the ring $\mathrm{Int}^{\mathrm{R}}(D)$ 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.

Chapter 2

Power Monoids and (Minimal) Factorization Properties

We begin by defining our central object of study: the power monoid. These objects were first introduced and studied by Y. Fan and S. Tringali in [8].

Definition 2.0.1. Let H be a monoid; for nonempty $X, Y \subset H$, we will define the operation of setwise multiplication by

$$X \cdot Y = \{xy : x \in X,\, y \in Y\}.$$

This operation endows several collections of subsets of H with a monoid structure. Namely, we have the *Power Monoid* of H:

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

the *Restricted Power Monoid* of H:

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

and the *Reduced Power Monoid* of H:

$$\mathcal{P}_{\text{fin},1}(H) = \{X \subseteq H : 1 \in X,\, |X| < \infty\}.$$

Remark 2.0.2. Let H be a monoid.

(i) $\mathcal{P}_{\text{fin}}(H) \supseteq \mathcal{P}_{\text{fin},\times}(H) \supseteq \mathcal{P}_{\text{fin},1}(H)$.

(ii) The identity of each of these monoids is $\{1_H\}$. Moreover, $\mathcal{P}_{\text{fin},1}(H)$ is indeed a reduced monoid; i.e., its only unit is $\{1_H\}$.

(iii) Unless H is trivial, $\mathcal{P}_{\text{fin}}(H)$ is non-cancellative.

2.1 Conditions for Atomicity and Bounded Factorization Lengths

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.

Proposition 2.1.1. Let H be a monoid. The following hold:

(i) If $u, v \in H^\times$ then $uv \in H^\times$, and the converse is also true if $H = H^\times$ or $\mathcal{A}(H) = \emptyset$.

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

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

Proof. See parts (i), (ii), and (iv) of [8, Lemma 2.2]. □

Proposition 2.1.2. Let H be a monoid. The following hold:

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

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

(iii) If K is a submonoid of H, then $\mathcal{P}_{\text{fin},1}(K)$ is a divisor-closed submonoid of $\mathcal{P}_{\text{fin},1}(H)$.

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

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

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

As for (v), let $A \in \mathcal{A}(\mathcal{P}_{\text{fin},\times}(H))$. Because A contains a unit of H, there is $u \in H^\times$ such that $1_H \in uA$. Then uA is an element of $\mathcal{P}_{\text{fin},1}(H)$, and by Proposition 2.1.1(ii) it is also an atom of $\mathcal{P}_{\text{fin},\times}(H)$. Thus, if $X, Y \in \mathcal{P}_{\text{fin},1}(H) \subseteq \mathcal{P}_{\text{fin},\times}(H)$ and $uA = XY$, then X or Y is the identity of $\mathcal{P}_{\text{fin},1}(H)$. This means that uA is an atom of $\mathcal{P}_{\text{fin},1}(H)$, and hence $A = u^{-1}(uA) \in H^\times \mathcal{A}(\mathcal{P}_{\text{fin},1}(H))$, as wished. □

Our ultimate goal is, for an arbitrary monoid H, to investigate factorizations in $\mathcal{P}_{\text{fin}}(H)$. However, this is a difficult task in general, due to a variety of "pathological situations" that might be hard to classify in a satisfactory way, see, for instance, [8, 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 [21, Definition 3.2] a notion which formally packages the idea that, under suitable conditions, arithmetic may be transferred from one monoid to another.

Definition 2.1.3. Let H and K be monoids, and $\varphi : H \to K$ a monoid homomorphism. We denote by $\varphi^* : \mathcal{F}^*(H) \to \mathcal{F}^*(K)$ the (unique) monoid homomorphism such that $\varphi^*(x) = \varphi(x)$ for every $x \in H$, and we call φ an *equimorphism* if the following hold:

(E1) $\varphi^{-1}(K^\times) \subseteq H^\times$;

(E2) φ is *atom-preserving*, meaning that $\varphi(\mathcal{A}(H)) \subseteq \mathcal{A}(K)$;

(E3) If $x \in H$ and $\mathfrak{b} \in \mathcal{Z}_K(\varphi(x))$ is a non-empty $\mathcal{A}(K)$-word, then $\varphi^*(\mathfrak{a}) \in [\![\mathfrak{b}]\!]_{\mathcal{C}_K}$ for some $\mathfrak{a} \in \mathcal{Z}_H(x)$.

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

Proposition 2.1.4. Let H and K be monoids and $\varphi : H \to K$ an equimorphism. The following hold:

(i) $\mathsf{L}_H(x) = \mathsf{L}_K(\varphi(x))$ for all $x \in H \setminus H^\times$.

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

Proof. See [8, Theorem 2.22(i)] and [21, Theorem 3.3(i)]. □

Proposition 2.1.5. Let H be a Dedekind-finite monoid. The following hold:

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

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

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

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

Proof. In view of Proposition 2.1.4, parts (iii) and (iv) are immediate from (i). Moreover, the inclusion from left to right in (ii) is precisely the content of Proposition 2.1.2(v), and the other inclusion will follow from (i) and Propositions 2.1.1(ii) and 2.1.2(iv). Therefore, we focus on (i) for the remainder of the proof.

(i) By Proposition 2.1.2(iv), $\jmath$ satisfies (E1). Moreover, $\jmath$ is essentially surjective, as any $X \in \mathcal{P}_{\mathrm{fin},\times}(H)$ contains a unit $u \in H^\times$, so $u^{-1}X \in \mathcal{P}_{\mathrm{fin},1}(H)$ and $X = u(u^{-1}X)$ is associate to an element of $\mathcal{P}_{\mathrm{fin},1}(H)$.

To prove (E2), let $A \in \mathcal{A}(\mathcal{P}_{\mathrm{fin},1}(H))$. We aim to show that A is an atom of $\mathcal{P}_{\mathrm{fin},\times}(H)$. For, suppose that $A = XY$ for some $X, Y \in \mathcal{P}_{\mathrm{fin},\times}(H)$. Then there are $x \in X$ and $y \in Y$ with $xy = 1_H$; and using that H is Dedekind-finite, we get from [8, Lemma 2.30] that $x, y \in H^\times$. It follows that

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

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

It remains to show that $\jmath$ satisfies (E3). For, pick $X \in \mathcal{P}_{\mathrm{fin},1}(H)$. If $X = \{1_H\}$, the conclusion holds vacuously. Otherwise, let $\mathfrak{b} := B_1 * \cdots * B_n \in \mathcal{Z}_{\mathcal{P}_{\mathrm{fin},1}(H)}(X)$. 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

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

and by Propositions 2.1.1(ii) and 2.1.2(v), $A_1, \dots, A_n$ are atoms of $\mathcal{P}_{\mathrm{fin},1}(H)$. This shows that $\mathfrak{a} := A_1 * \cdots * A_n \in \mathcal{Z}_{\mathcal{P}_{\mathrm{fin},1}(H)}(X)$; and since $A_i \simeq_{\mathcal{P}_{\mathrm{fin},\times}(H)} B_i$ for each $i \in [\![1, n]\!]$ (by construction), we conclude that $\mathfrak{a}$ is $\mathcal{C}_{\mathcal{P}_{\mathrm{fin},\times}(H)}$-congruent to $\mathfrak{b}$, as wished. □

The next example shows that Dedekind-finiteness is, to some extent, necessary for Proposition 2.1.5(ii), and hence for the subsequent conclusions.

Example 2.1.6. Let $\mathcal{B}$ be the set of all binary sequences $\mathfrak{s} : \mathbb{N}^+ \to \{0, 1\}$, and let H denote the monoid of all functions $\mathcal{B} \to \mathcal{B}$ under composition: We will write $\mathcal{B}$ multiplicatively; so, if $f, g \in \mathcal{B}$ then fg is the map $\mathcal{B} \to \mathcal{B} : \mathfrak{s} \mapsto f(g(\mathfrak{s}))$. Further, let $n \geq 5$ and consider the functions

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

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

$$P : \mathcal{B} \to \mathcal{B} : (a_1, a_2, \dots) \mapsto (a_n, a_1, \dots, a_{n-1}, a_{n+2}, a_{n+3}, \dots,) \qquad \text{(cycle the first } n \text{ terms)}.$$

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

Indeed, assume $A = XY$ for some $X, Y \in \mathcal{P}_{\mathrm{fin},1}(H)$. Then $X, Y \subseteq A$, and it is clear that $P^2 \neq PRLP$, or else $RL = \mathrm{id}_\mathcal{B}$ (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 functions to the constant sequence $1, 1, \ldots$).

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

We get from Proposition 2.1.5 that studying factorization properties of $\mathcal{P}_{\mathrm{fin},1}(H)$ is sufficient for studying corresponding properties of $\mathcal{P}_{\mathrm{fin},\times}(H)$, at least in the case when H is Dedekind-finite. Thus, as a starting point in the investigation of the arithmetic of $\mathcal{P}_{\mathrm{fin},1}(H)$, one might wish to give a comprehensive description of the atoms of $\mathcal{P}_{\mathrm{fin},1}(H)$. 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 $\mathcal{A}(\mathcal{P}_{\mathrm{fin},1}(H))$ in full generality.

Lemma 2.1.7. 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 $\mathcal{P}_{\mathrm{fin},1}(H)$ if and only if $1_H \neq x^2 \neq x$.

(ii) If $x^2 = 1_H$ or $x^2 = x$, then $\{1_H, x\}$ does not factor into a product of atoms neither in $\mathcal{P}_{\mathrm{fin},1}(H)$ nor in $\mathcal{P}_{\mathrm{fin},\times}(H)$.

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 $\mathcal{P}_{\mathrm{fin},1}(H)$. As for the converse, assume that $\{1_H, x\} = YZ$ for some non-units $Y, Z \in \mathcal{P}_{\mathrm{fin},1}(H)$. Then we get from Proposition 2.1.2 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 $\mathcal{P}_{\mathrm{fin},1}(H)$. So, $\{1_H, x\}$ is a non-trivial idempotent (hence, a non-unit) and has no factorization into atoms of $\mathcal{P}_{\mathrm{fin},1}(H)$.

It remains to prove the analogous statement for $\mathcal{P}_{\mathrm{fin},\times}(H)$. For, assume to the contrary that $\{1_H, x\}$ factors into a product of n atoms of $\mathcal{P}_{\mathrm{fin},\times}(H)$ for some $n \in \mathbb{N}^+$. 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 $\mathcal{P}_{\mathrm{fin},\times}(H)$. In particular, we get from parts (i), (ii), and (iv) of Proposition 2.1.2 that both Y and Z are 2-element sets, say, $Y = \{u, y\}$ and $Z = \{v, z\}$. It is then immediate that there are only two possibilities: 1_H is the product of two units from Y and Z, or the product of two non-units from Y and Z. Without loss of generality, we are thus reduced to considering the following cases.

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

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

However, this shows that $\{u, y\}$ is not an atom of $\mathcal{P}_{\mathrm{fin},\times}(H)$, 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 $\{u, y\}, \{v, z\} \in \mathcal{P}_{\mathrm{fin},\times}(H)$; and we must have $uz = x$, for $uz = 1_H$ would yield $z = u^{-1} \in H^\times$. In particular, $x = uz$ is not a unit in H, so $uv = 1_H$ and we are back to the previous case. □

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

Lemma 2.1.8. Let H be a monoid such that $1_H \neq x^2 \neq x$ for all $x \in H \setminus \{1_H\}$. The following hold:

(i) H is Dedekind-finite.

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

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

(ii) This is an obvious consequence of [22, 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 $n, k \in \mathbb{N}^+$ such that $x^n = x^{n+k}$, and by induction this implies that $x^n = x^{n+hk}$ for all $h \in \mathbb{N}$. Therefore, we find that

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

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

Theorem 2.1.9. 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 2.1.7(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

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

If X is a 2-element set, the claim is true by Lemma 2.1.7(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

$$|X| \geq 3, \quad |B| \geq 2, \quad \text{and} \quad B \subseteq AB = X = A. \tag{2.1}$$

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 $A_bB = A = X$ (in fact, 1_H is in $A_b \cap B$, and therefore we derive from (2.1) that $A_bB \subseteq A = A_b \cup \{b\} \subseteq A_bB \cup \{b\} \subseteq A_bB \cup B = A_bB$).

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 $X = AB = A_bB$. Otherwise, it follows from (2.1) and the above that

$$X = A = B = A_bB \quad \text{and} \quad |A| \geq 3, \tag{2.2}$$

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 (2.2) that $X = A = A_bB_a$ (indeed, $1_H \in A_b \cap B_a$ and $b \in B_a$, so we find that $A_bB_b \subseteq A = A_b \cup \{b\} \subseteq A_bB_a \cup \{b\} \subseteq A_bB_a \cup B_a = A_bB_a$). □

Now with Proposition 2.1.4 and Theorem 2.1.9 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 2.1.10. 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 2.1.7 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 § 2.2.

Theorem 2.1.11. 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 H is torsion-free.

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

(ii) First suppose for a contradiction that $\mathcal{P}_{\text{fin},1}(H)$ is BF and has an element x of finite order m; then $\mathcal{P}_{\text{fin},1}(H)$ is also atomic, and we know by Theorem 2.1.9 and Lemma 2.1.8(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 2.1.9, no non-identity element of H can have order 2. If m is odd then Example 2.1.10 shows us that the set of lengths of $\{x^k : k \in \mathbb{N}\}$ is infinite, a contradiction to the assumption that $\mathcal{P}_{\text{fin},1}(H)$ is BF.

Conversely, suppose H is torsion-free; then all powers of non-identity elements are distinct, so Theorem 2.1.9 implies that $\mathcal{P}_{\text{fin},1}(H)$ is atomic, and (i) gives an explicit upper bound on the lengths of factorizations.

(iii) By part (ii), it is sufficient to show that $\mathcal{P}_{\text{fin},\times}(H)$ is BF if and only if $\mathcal{P}_{\text{fin},1}(H)$ is BF. The "only if" direction follows from [8, 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 2.1.9, $1_H \neq x^2 \neq x$ for all $x \in H \setminus \{1_H\}$. In view of Lemma 2.1.8(ii), 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 2.1.5(i). The result then follows from Proposition 2.1.5(iv). □

2.2 Minimal factorizations and conditions for bounded minimal lengths

Example 2.1.10 seems to indicate that, in the presence of torsion in the ground monoid H, the sets of lengths in $\mathcal{P}_{\text{fin},1}(H)$ can blow up in a predictable fashion. In the commutative setting, we could counteract such phenomena directly by considering only factorizations involving "sufficiently low" powers of atoms (cf. the notion of "index" and the corresponding sets of factorization classes defined in [14]). We strive instead to axiomatize an approach which responds to *all* non-cancellative phenomena in a general monoid, spurring us to introduce a refinement of our notion of factorization (recall that, given a set X, we let ε_X be the identity of $\mathcal{F}^*(X)$, the free monoid with basis X).

Definition 2.2.1. Let H be a monoid. We denote by $\preceq_H$ the binary relation on $\mathcal{F}^*(\mathcal{A}(H))$ determined by taking $\mathfrak{a} \preceq_H \mathfrak{b}$, for some $\mathcal{A}(H)$-words $\mathfrak{a}$ and $\mathfrak{b}$ of length h and k respectively, if and only if

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

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

The next result highlights a few basic properties of the relation introduced in Definition 2.2.1.

Proposition 2.2.2. Let H be a monoid, and let $\mathfrak{a}, \mathfrak{b} \in \mathcal{F}^*(\mathcal{A}(H))$. The following hold:

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

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

(iii) $\varepsilon_{\mathcal{A}(H)} \preceq_H \mathfrak{a}$ if and only if $\mathfrak{a} = \varepsilon_{\mathcal{A}(H)}$.

(iv) $\mathfrak{a} \preceq_H \mathfrak{b}$ and $\mathfrak{b} \preceq_H \mathfrak{a}$ if and only if $\mathfrak{a} \preceq_H \mathfrak{b}$ and $\|\mathfrak{a}\|_H = \|\mathfrak{b}\|_H$, if and only if $(\mathfrak{a}, \mathfrak{b}) \in \mathcal{C}_H$.

Proof. Points (i) and (ii) are straightforward from our definitions, and for (iii) it suffices to note that, by Proposition 2.1.1(i), $\pi_H(\mathfrak{a}) = 1_H$ if and only if $\mathfrak{a} = \varepsilon_{\mathcal{A}(H)}$.

As for (iv), set $h := \|\mathfrak{a}\|_H$ and $k := \|\mathfrak{b}\|_H$. By part (ii), $\mathfrak{a} \preceq_H \mathfrak{b}$ and $\mathfrak{b} \preceq_H \mathfrak{a}$ only if $\mathfrak{a} \preceq_H \mathfrak{b}$ and $h = k$; and it is immediate to check that $(\mathfrak{a}, \mathfrak{b}) \in \mathcal{C}_H$ implies $\mathfrak{a} \preceq_H \mathfrak{b}$ and $\mathfrak{b} \preceq_H \mathfrak{a}$.

So, to finish the proof, assume that $\mathfrak{a} \preceq_H \mathfrak{b}$ and $h = k$. We only need to show that $(\mathfrak{a}, \mathfrak{b}) \in \mathcal{C}_H$. For, we have (by definition) that $\mathfrak{a} \preceq_H \mathfrak{b}$ if and only if $\pi_H(\mathfrak{a}) = \pi_H(\mathfrak{b})$ and there is an injection $\sigma : [\![1, h]\!] \to [\![1, k]\!]$

such that $a_i \simeq_H b_{\sigma(i)}$ for every $i \in [\![1, h]\!]$. But σ is actually a bijection (because $h = k$), and we can thus conclude that $(\mathfrak{a}, \mathfrak{b}) \in \mathcal{C}_H$. □

Definition 2.2.3. Let H be a monoid and $x \in H$. An H-word $\mathfrak{a}$ is a *$\preceq_H$-minimal factorization* of x, or simply a *minimal factorization* of x (in or relative to H), if $\mathfrak{a} \in \mathcal{Z}_H(x)$ and $\mathfrak{a}$ is $\preceq_H$-minimal. Accordingly,

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

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 § 1.3.2). In addition, we take

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

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

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

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

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

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

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

Proposition 2.2.4. Let H be a monoid and let $x \in H$. The following hold:

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

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

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

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

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

Proof. (i), (ii), and (iii) are an immediate consequence of parts (ii)-(iv) of Proposition 2.2.2 (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 ≥ 2); and (iv) follows at once from considering that, if K is a divisor-closed submonoid of H and $x \in K$, then $\mathsf{Z}_K(x) = \mathsf{Z}_H(x)$ and $\mathsf{L}_K(x) = \mathsf{L}_H(x)$, see [8, 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 [8, Proposition 2.30] that $a_{k+1}, \dots, a_n \in H^\times$, which is however impossible (by definition of an atom). □

To further elucidate the behavior of minimal factorizations, we give an analogue of Proposition 2.1.1(iii) showing that multiplying a non-unit by units does not change its set of minimal factorizations.

Lemma 2.2.5. 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 $\mathsf{Z}^{\mathsf{m}}_H(x) \to \mathsf{Z}^{\mathsf{m}}_H(uxv)$, and in particular $\mathsf{L}^{\mathsf{m}}_H(x) = \mathsf{L}^{\mathsf{m}}_H(uxv)$.

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

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

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 $g : \mathsf{Z}^{\mathsf{m}}_H(uxv) \to \mathsf{Z}^{\mathsf{m}}_H(x) : \mathfrak{b} \mapsto u^{-1}\mathfrak{b}v^{-1}$ 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 $\mathfrak{a} \in \mathsf{Z}^{\mathsf{m}}_H(x)$, and note that, by Proposition 2.1.1(i), $\|\mathfrak{a}\|_H$ is a positive integer, so that $\mathfrak{a} = a_1 * \cdots * a_n$ for some $a_1, \dots, a_n \in \mathcal{A}(H)$. In view of Proposition 2.1.1(ii), $u\mathfrak{a}v$ 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 2.2.2(iv), $k := \|\mathfrak{b}\|_H \in [\![1, n-1]\!]$ (recall that $uxv \notin H^\times$). So, $\mathfrak{b} = b_1 * \cdots * b_k$ for some atoms $b_1, \dots, b_k \in H$, and there exists an injection $\sigma : [\![1, k]\!] \to [\![1, n]\!]$ such that $b_i \simeq_H a_{\sigma(i)}$ for each $i \in [\![1, k]\!]$. Define $\mathfrak{c} := u^{-1}\mathfrak{b}v^{-1}$.

By construction and Proposition 2.1.1(ii), there are $c_1, \dots, c_k \in \mathcal{A}(H)$ such that $\mathfrak{c} = c_1 * \cdots * c_k$; and it follows from the above that $\pi_H(\mathfrak{c}) = u^{-1}\pi_H(\mathfrak{b})v^{-1} = x$ and $c_i \simeq_H a_{\sigma(i)}$ for every $i \in [\![1, k]\!]$. Since $k < n$, we can thus conclude from Proposition 2.2.2(iv) that $\mathfrak{c} \prec_H \mathfrak{a}$, contradicting the $\preceq_H$-minimality of $\mathfrak{a}$. □

We saw in the previous section that equimorphisms transfer factorizations between monoids (Proposition 2.1.4). Equimorphisms have a similar compatibility with minimal factorizations, in the sense that an equimorphism also satisfies a "minimal version" of condition (E3) from Definition 2.1.3.

Proposition 2.2.6. Let H and K be monoids and $\varphi : H \to K$ an equimorphism. The following hold:

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

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

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

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

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

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

(recall that monoid homomorphisms map units to units; so, if $u \simeq_H v$, then $\varphi(u) \simeq_K \varphi(v)$); and together with Proposition 2.2.4(iii), this proves that $\varphi^*(\mathfrak{c}) \prec_K \mathfrak{b}$, contradicting the $\preceq_K$-minimality of $\mathfrak{b}$.

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

(iii) Assume φ is essentially surjective, and let $y \in K \setminus K^\times$. Then $y = u\varphi(x)v$ for some $u, v \in K^\times$ and $x \in H$, and neither x is a unit of H nor $\varphi(x)$ is a unit of K (because $\varphi(H^\times) \subseteq K^\times$ and $y \notin K^\times$). Accordingly, we have by Lemma 2.2.5 and part (ii) that $\mathsf{L}_K^{\mathsf{m}}(y) = \mathsf{L}_K^{\mathsf{m}}(\varphi(x)) \subseteq \mathsf{L}_H^{\mathsf{m}}(x)$. □

Let H be a monoid. As in § 2.1, 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, we have 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 2.2.7. Let H be a commutative monoid, and let $X \in \mathcal{P}_{\text{fin},1}(H)$. The following hold:

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

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

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

Proof. (i) Let $\mathfrak{a}$ be a minimal factorization of X relative to $\mathcal{P}_{\mathrm{fin},1}(H)$. In light of Proposition 2.2.4(i), $\mathfrak{a}$ is a non-empty $\mathcal{A}(\mathcal{P}_{\mathrm{fin},1}(H))$-word, i.e., $\mathfrak{a} = A_1 * \cdots * A_n$ for some atoms $A_1, \ldots, A_n \in \mathcal{P}_{\mathrm{fin},1}(H)$.

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

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

and on account of Proposition 2.2.2(iv) we must have $1 \le m < n$. Since H is a commutative monoid, this means in particular that, for each $i \in [\![1, m]\!]$, there is $u_i \in H^\times$ such that $B_i = u_i A_{\sigma(i)}$. Thus we have

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

where $u := u_1 \cdots u_m \in H^\times$. In view of Proposition 2.1.2(ii), it follows that

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

which is only possible if

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

because $1_H \in A_i$ for every $i \in [\![1, n]\!]$, and hence $A_{\sigma(1)} \cdots A_{\sigma(m)} \subseteq A_1 \cdots A_n$ (note that here we use again that H is commutative). So, letting $\mathfrak{a}'$ be the $\mathcal{A}(\mathcal{P}_{\mathrm{fin},1}(H))$-word $A_{\sigma(1)} * \cdots * A_{\sigma(m)}$ and recalling from the above that $m \le n - 1$, we see by Proposition 2.2.2(iv) that $\mathfrak{a}' \prec_{\mathcal{P}_{\mathrm{fin},1}(H)} \mathfrak{a}$, which contradicts the hypothesis that $\mathfrak{a}$ is a minimal factorization of X in $\mathcal{P}_{\mathrm{fin},1}(H)$.

(ii) It is an immediate consequence of part (i) and Propositions 2.1.5(i) and 2.2.6(ii), when considering that every commutative monoid is Dedekind-finite.

(iii) We already know from part (ii) that $\mathcal{L}^{\mathsf{m}}(\mathcal{P}_{\mathrm{fin},1}(H)) \subseteq \mathcal{L}^{\mathsf{m}}(\mathcal{P}_{\mathrm{fin},\times}(H))$. For the opposite inclusion, fix $X \in \mathcal{P}_{\mathrm{fin},\times}(H)$. We claim that there exists $Y \in \mathcal{P}_{\mathrm{fin},1}(H)$ with $\mathsf{L}^{\mathsf{m}}_{\mathcal{P}_{\mathrm{fin},\times}(H)}(X) = \mathsf{L}^{\mathsf{m}}_{\mathcal{P}_{\mathrm{fin},1}(H)}(Y)$. Indeed, pick $x \in X \cap H^\times$. Then $x^{-1}X \in \mathcal{P}_{\mathrm{fin},1}(H)$, and we derive from Lemma 2.2.5 and part (ii) that

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

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

We will now discuss an instance in which equality in Proposition 2.2.7(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 2.2.6(ii) when φ is the natural embedding of Proposition 2.1.5(i).

Example 2.2.8. 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 [18, p. 27], we take H to be the metacyclic group generated by the 2-element set $\{r,s\}$ subject to $\mathrm{ord}_H(r) = p$, $\mathrm{ord}_H(s) = 3$, and $s^{-1}rs = r^n$. Then H is a non-abelian group of (odd) order $3p$, and by Theorem 2.1.9 and Propositions 2.1.4(ii) and 2.1.5(i), $\mathcal{P}_{\mathrm{fin},1}(H)$ and $\mathcal{P}_{\mathrm{fin},\times}(H)$ are both atomic monoids.

We claim that $X := \langle r \rangle_H$ has minimal factorizations of length $p-1$ in $\mathcal{P}_{\mathrm{fin},1}(H)$ but not in $\mathcal{P}_{\mathrm{fin},\times}(H)$. For, pick $g \in X \setminus \{1_H\}$. Clearly $\mathrm{ord}_H(g) = p$, and thus we get from Lemma 2.1.7(i) that $\{1_H, g\}$ is an atom of $\mathcal{P}_{\mathrm{fin},1}(H)$. Then it is immediate to see that $\mathfrak{a}_g := \{1_H, g\}^{*(p-1)}$ is a minimal factorization of X in $\mathcal{P}_{\mathrm{fin},1}(H)$; most notably, $\mathfrak{a}_g$ is minimal since otherwise there should exist an exponent $k \in [\![1, p-2]\!]$ such that $g^{p-1} = g^k$, contradicting that $\mathrm{ord}_H(g) = p$. Yet, $\mathfrak{a}_g$ is not a minimal factorization of X in $\mathcal{P}_{\mathrm{fin},\times}(H)$. Indeed, Proposition 2.1.5(ii) and Lemma 2.1.7(i) guarantee that $\{1_H, g\}$ and $\{1_H, g^n\}$ are associate atoms of $\mathcal{P}_{\mathrm{fin},\times}(H)$, because $s^{-1}g^n s = g$ and, hence, $s^{-1}\{1,g\}s = \{1_H, g^n\}$. So, in view of Proposition 2.2.2(iv), it is straightforward that

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

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

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

Given that, suppose for a contradiction that X has a minimal factorization $\mathfrak{c}$ of length $p-1$ in $\mathcal{P}_{\mathrm{fin},\times}(H)$. Then by Propositions 2.1.5(i) and 2.2.6(i), $\mathfrak{c}$ is $\mathcal{C}_{\mathcal{P}_{\mathrm{fin},\times}(H)}$-congruent to a $\preceq_{\mathcal{P}_{\mathrm{fin},1}(H)}$-minimal factorization $\mathfrak{a} = A_1 * \cdots * A_{p-1}$ of X of length $p-1$; and we aim to show that $\mathfrak{a}$ is $\mathcal{C}_{\mathcal{P}_{\mathrm{fin},1}(H)}$-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 $\mathcal{P}_{\mathrm{fin},\times}(H)$, in contradiction to what established in the above.

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

We want to show that $\mathfrak{b}$ is $\preceq_{\mathcal{P}_{\mathrm{fin},0}(H)}$-minimal only if there is a non-zero $x \in \mathbb{Z}/p\mathbb{Z}$ such that $B_i = \{\overline{0}, x\}$ or $B_i = \{\overline{0}, -x\}$, or equivalently $A_i = \{1_H, r^{\hat{x}}\}$ or $A_i = \{1_H, r^{-\hat{x}}\}$, for every $i \in [\![1, p-1]\!]$ (for notation,

see § 1.3.1). By the preceding arguments, this will suffice to conclude that $p-1 \notin \mathsf{L}^{\mathsf{m}}_{\mathcal{P}_{\mathrm{fin},\times}(H)}(X)$, because it implies at once that $\mathfrak{a}$ is $\mathcal{C}_{\mathcal{P}_{\mathrm{fin},1}(H)}$-congruent to $\mathfrak{a}_g$ with $g := r^{\hat{x}} \in X \setminus \{1_H\}$.

To begin, let K be a subset of $[\![1, p-1]\!]$, and define $\mathcal{S}_K := \sum_{k\in K} B_k$ and $s_K := \{k \in K : |B_k| \ge 3\}$. Then we have by the Cauchy-Davenport inequality (see, e.g., [19, Theorem 6.2]) that

$$\mathcal{S}_K = \mathbb{Z}/p\mathbb{Z} \quad \text{or} \quad |\mathcal{S}_K| \ge 1 + \sum\nolimits_{k\in K} \big(|B_k| - 1\big) \ge 1 + |K| + s_K. \tag{2.3}$$

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 $\mathcal{S}_{I\cup J} \ne \mathbb{Z}/p\mathbb{Z}$, otherwise $\mathfrak{b}$ would not be a minimal factorization in $\mathcal{P}_{\mathrm{fin},0}(\mathbb{Z}/p\mathbb{Z})$. So, another application of the Cauchy-Davenport inequality, combined with (2.3), yields

$$|S_{I\cup J}| = |S_I + S_J| \ge |S_I| + |S_J| - 1 \ge 1 + |I| + |J| + s_I + s_J = p - 1 + s_I + s_J. \tag{2.4}$$

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

It follows $|B_1| = \cdots = |B_{p-1}| = 2$. So, taking I in (2.4) to range over all 1-element subsets of $[\![1, p-1]\!]$ and observing that, consequently, $|S_J| \ge p - 1 - |S_I| = p - 3 \ge 8 > |S_I|$, we infer from Vosper's theorem (see, e.g., [19, Theorem 8.1]) that there exists a non-zero $x \in \mathbb{Z}/p\mathbb{Z}$ such that, for every $i \in [\![1, p-1]\!]$, B_i is an arithmetic progression of $\mathbb{Z}/p\mathbb{Z}$ with difference x, i.e., $B_i = \{\overline{0}, x\}$ or $B_i = \{\overline{0}, -x\}$ (as wished).

We proceed with an analogue of Theorem 2.1.11(i) and then prove the main results of the section.

Proposition 2.2.9. Let H be a monoid and $X \in \mathcal{P}_{\mathrm{fin},\times}(H)$. The following hold:

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

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

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

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

In fact, let $i \in [\![1, n-1]\!]$. Since $1_H \in A_{i+1}$, it is clear that $A_1 \cdots A_i \subsetneq A_1 \cdots A_{i+1}$; and the inclusion must be strict, or else $A_1 * \cdots * A_i * \mathfrak{b} \prec_{\mathcal{P}_{\mathrm{fin},1}(H)} \mathfrak{a}$, where $\mathfrak{b} := \varepsilon_{\mathcal{A}(\mathcal{P}_{\mathrm{fin},1}(H))}$ if $i = n-1$ and $\mathfrak{b} := A_{i+2} * \cdots * A_n$ otherwise

(contradicting the minimality of $\mathfrak{a}$). Consequently, we see that $2 \le |A_1 \cdots A_i| < |A_1 \cdots A_{i+1}| \le |X|$ for all $i \in [\![1, n-1]\!]$, and this implies at once that $n \le |X| - 1$.

(ii) The conclusion is immediate from part (i) and Propositions 2.1.5(i) and 2.2.6(iii). □

Theorem 2.2.10. Let H be a monoid. Then the following are equivalent:

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

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

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

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

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

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

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

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

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

Proof. We already know from Theorem 2.1.9 and Lemma 2.1.7 that (b) ⇔ (a) ⇔ (e) and (i) ⇒ (a); while it is straightforward from our definitions that (h) ⇒ (g) ⇒ (f). So, it will suffice to prove that (b) ⇒ (c) ⇒ (d) ⇒ (h) and (f) ⇒ (i).

(b) ⇒ (c): If $X \in \mathcal{P}_{\text{fin},1}(H)$ is a non-unit, then $\mathcal{Z}_{\mathcal{P}_{\text{fin},1}(H)}(X)$ is non-empty, and by Propositions 2.2.4(ii) and 2.2.9(i) we have that $\emptyset \ne \mathsf{L}^{\mathsf{m}}_{\mathcal{P}_{\text{fin},1}(H)}(X) \subseteq [\![1, |X| - 1]\!]$. So, $\mathcal{P}_{\text{fin},1}(H)$ is BmF.

(c) ⇒ (d): Let $X \in \mathcal{P}_{\text{fin},1}(H)$ be a non-unit. By Proposition 2.1.2(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) ⇒ (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 2.1.9 and Lemma 2.1.8(i), H is Dedekind-finite, and so we have by Proposition 2.1.5(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 2.2.6(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 $\mathsf{Z}^{\mathsf{m}}_{\mathcal{P}_{\text{fin},\times}(H)}(uX)$ finite, whence $\mathsf{Z}^{\mathsf{m}}_{\mathcal{P}_{\text{fin},\times}(H)}(X)$ must also be finite as a consequence of Lemma 2.2.5.

(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 $1_H \in H$; and since $\mathcal{P}_{\text{fin},\times}(H)$ is atomic (by hypothesis), we are guaranteed by Lemmas 2.1.7 and 2.1.8(i) that A is an atom of $\mathcal{P}_{\text{fin},1}(H)$ and H is Dedekind-finite. Therefore, we conclude from Proposition 2.1.5(ii) that $X \in \mathcal{A}(\mathcal{P}_{\text{fin},\times}(H))$. □

Theorem 2.2.11. 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 2.2.10 and Propositions 2.2.9(i) and 2.2.4(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 2.1.9 and Lemma 2.1.8(ii), it suffices to show that $x^3 \in \{1_H, x, x^2\}$ for every $x \in H$, since this in turn implies (by induction) that $\langle x \rangle_H \subseteq \{1_H, x, x^2\}$ and $\mathrm{ord}_H(x) \leq 3$.

For, assume to the contrary that $x^3 \notin \{1_H, x, x^3\}$ for some $x \in H$, and set $X := \{1_H, x, x^2, x^3\}$. By Theorem 2.2.10, $\mathfrak{a} := \{1_H, x\}^{*3}$ 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 2.2.4(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. [18, 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 $\mathrm{ord}_H(y) = \mathrm{ord}_H(z) = 3$ 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 2.2.10 that $\mathfrak{c} := \{1_H, y\}^{*2} * \{1_H, z\}^{*2}$ 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 $\mathfrak{c}$ 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 2.2.4(i). So, we are done. □

Corollary 2.2.12. 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 2.2.11 that H is a cyclic group of order 3. Accordingly, let x be a generator of H. By Lemma 2.1.7(i) and Proposition 2.2.4(i), $\mathfrak{a} := \{1_H, x\}^{*2}$ and $\mathfrak{b} := \{1_H, x^2\}^{*2}$ are both minimal factorizations of H in $\mathcal{P}_{\text{fin},1}(H)$. However, $(\mathfrak{a}, \mathfrak{b}) \notin \mathcal{C}_{\mathcal{P}_{\text{fin},1}}(H)$, 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. □

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 2.2.11 and Corollary 2.2.12. 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.

2.3 Cyclic monoids and interval length sets

For those monoids H with $\mathcal{P}_{\text{fin},1}(H)$ atomic, we have by Proposition 2.1.8 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 $\mathcal{P}_{\text{fin},0}($

ZZ/n

$ZZ)$ and also mention some results on $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ which are discussed in detail in [8, § 4]. At the end we will return to the general case, where the preceding discussion will culminate in a realization result (Theorem 2.3.7) for sets of minimal lengths of $\mathcal{P}_{\text{fin},1}(H)$.

We invite the reader to review § 1.3.1 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 2.2.8).

Definition 2.3.1. Let $X \in \mathcal{P}_{\text{fin},0}(\mathbb{Z}/n\mathbb{Z})$. We say that a non-empty factorization $\mathfrak{a} = A_1 * \cdots * A_\ell \in \mathcal{Z}(X)$ is a *non-reducible factorization* (or, 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 2.3.2. Any NR-factorization in $\mathcal{P}_{\text{fin},0}($

ZZ/n

$ZZ)$ is a minimal factorization.

Proof. Let $\mathfrak{a} = A_1 * \cdots * A_\ell$ be an NR-factorization in $\mathcal{P}_{\mathrm{fin},0}(\mathbb{Z}/n\mathbb{Z})$ of length ℓ, and assume for the sake of contradiction that $\mathfrak{a}$ is not minimal. Since $\mathcal{P}_{\mathrm{fin},0}($

ZZ/n

$ZZ)$ is reduced and commutative, the factorizations which are $\mathcal{C}_{\mathcal{P}_{\mathrm{fin},0}(ZZ/nZZ)}$-congruent to $\mathfrak{a}$ are exactly the words $A_{\sigma(1)} * \cdots * A_{\sigma(\ell)}$, where σ is an arbitrary permutation of the interval $[\![1, \ell]\!]$. So, on account of Proposition 2.2.4(i), the non-minimality of $\mathfrak{a}$ implies without loss of generality that $\ell \ge 3$ and $X := A_1 + \cdots + A_\ell = A_1 + \cdots + A_k$ for some $k \in [\![1, \ell - 1]\!]$.

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

$$\hat{x} = \max \hat{A}_1 + \max \hat{A}_2 + \cdots + \max \hat{A}_\ell > \max \hat{A}_1 + \cdots + \max \hat{A}_k, \tag{2.5}$$

On the other hand, since $X = A_1 + \cdots + A_k$, there are $a_1 \in A_1, \ldots, a_k \in A_k$ such that $a_1 + \cdots + a_k = x$, from which we see that $\hat{x} \equiv \hat{a}_1 + \cdots + \hat{a}_k \bmod n$. But it follows from (2.5) that $0 \le \hat{a}_1 + \cdots + \hat{a}_k < \hat{x} < n$, and this implies $\hat{x} \not\equiv \hat{a}_1 + \cdots + \hat{a}_k \bmod n$ (recall that, by definition, $\hat{X} \subseteq [\![0, n-1]\!]$). So we got a contradiction, showing that $\mathfrak{a}$ was minimal and completing the proof. □

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

Proposition 2.3.3. Let $n \ge 5$ be odd. Then the following sets are atoms of $\mathcal{P}_{\mathrm{fin},0}(\mathbb{Z}/n\mathbb{Z})$:

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

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

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

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

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

(ii) C_1 is an atom by Lemma 2.1.7(i) and it is not too difficult to see that so is C_3. Therefore, let $\ell \ge 5$ and suppose $C_\ell = X + Y$ for some $X, Y \in \mathcal{P}_{\mathrm{fin},0}(\mathbb{Z}/n\mathbb{Z})$ with $X, Y \ne \{\overline{0}\}$.

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

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

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

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

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

Lemma 2.3.4. Fix an odd integer $n \geq 5$ and let $k \in [\![2, n-1]\!]$. Then the set $X_k = \{\overline{0}, \overline{1}, \ldots, \overline{k}\}$ has an NR-factorization into two atoms in $\mathcal{P}_{\text{fin},0}($
ZZ/n
$ZZ)$.

Proof. We will use the atoms B_h and C_ℓ as defined in Proposition 2.3.3. 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

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

and

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

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

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

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

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

We are left to show that the decompositions given above do in fact correspond to minimal factorizations. As an example, consider the case when $k = 2m+1$ and m is odd (the computation will be essentially identical in the other cases). Then $\max \hat{B}_m + \max \hat{C}_m = 2m+1$, so that $B_m * C_m$ is an NR-factorization of X_k, and is hence minimal by Proposition 2.3.2. □

Lemma 2.3.5. Fix an odd integer $n \geq 3$ and, for each $k \in [\![2, n-1]\!]$, let $X_k := \{\overline{0}, \overline{1}, \ldots, \overline{k}\} \in \mathcal{P}_{\text{fin},0}(\mathbb{Z}/n\mathbb{Z})$. Then $\mathsf{L}^{\mathsf{m}}(X_k) = [\![2, k]\!]$.

Proof. We have already established in Lemma 2.3.4 that X_2 has an NR-factorization of length 2. Now fix $k \in [\![3, n-1]\!]$ and suppose that, for all $h \in [\![2, k-1]\!]$ and $\ell \in [\![2, h]\!]$, X_h has an NR-factorization of length ℓ. Choose some $\ell \in [\![2, k-1]\!]$; X_{k-1} has an NR-factorization $\mathfrak{a}$, and it is straightforward to see that $\{\overline{0}, \overline{1}\} * \mathfrak{a}$ is an NR-factorization of X_k. Letting ℓ range over $[\![2, k-1]\!]$, this argument, Lemma 2.3.2, and Lemma 2.3.4 imply that $\mathsf{L}^{\mathsf{m}}(X_k) \supseteq [\![2, k]\!]$. Moreover, Proposition 2.2.9(i) yields the other inclusion and so we have $\mathsf{L}^{\mathsf{m}}(X_k) = [\![2, k]\!]$. □

Lemma 2.3.6. Let H be a non-torsion monoid. Then $\mathcal{L}(\mathcal{P}_{\text{fin},0}(\mathbb{N})) \subseteq \mathcal{L}^{\mathsf{m}}(\mathcal{P}_{\text{fin},1}(H))$, and for every $k \geq 2$ there exists $Y_k \in \mathcal{P}_{\text{fin},1}(H)$ with $\mathsf{L}^{\mathsf{m}}(Y_k) = [\![2, k]\!]$.

Proof. Suppose that $y \in H$ has infinite order, and set $Y := \{y^k : k \in \mathbb{N}\}$. Clearly, Y is a submonoid of H, and the (monoid) homomorphism $(\mathbb{N}, +) \to Y : k \mapsto y^k$ determined by sending 1 to y induces an isomorphism $\mathcal{P}_{\text{fin},0}(\mathbb{N}) \to \mathcal{P}_{\text{fin},1}(Y)$. Since, by Proposition 2.1.2(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 2.2.4 that

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

The rest of the statement now follows from the above and [8, Proposition 4.8]. □

Theorem 2.3.7. Assume H is a monoid such that $1_H \neq x^2 \neq x$ for all $x \in H \setminus \{1_H\}$, and set $N := \sup\{\text{ord}_H(x) : x \in H\}$. Then $[\![2, k]\!] \in \mathcal{L}^{\mathsf{m}}(\mathcal{P}_{\text{fin},1}(H))$ for every $k \in [\![2, N-1]\!]$.

Proof. If H is non-torsion, this follows immediately from Lemma 2.3.6. Otherwise, let $k \in [\![2, N-1]\!]$ and $y \in H$ with $n := \mathrm{ord}_H(x) > k$. Then $Y := \langle y \rangle_H \cong \mathbb{Z}/n\mathbb{Z}$, so we have by Proposition 2.1.2(iii), Lemma 2.3.5, and Proposition 2.2.4(iv) that $[\![2, k]\!] \in \mathcal{L}^{\mathsf{m}}(\mathcal{P}_{\mathrm{fin},1}(Y)) \subseteq \mathcal{L}^{\mathsf{m}}(\mathcal{P}_{\mathrm{fin},1}(H))$. □

Chapter 3

Integer Partitions and the Natural Power Monoid

In [8, 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 4) 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 [8, Proposition 4.8], which says that $\mathsf{L}_{\mathcal{P}_{\text{fin},0}(\mathbb{N})}(\llbracket 0, n\rrbracket) = \llbracket 2, n\rrbracket$ for every $n \geq 2$. In essence, the intervals $\llbracket 0, n\rrbracket \in \mathcal{P}_{\text{fin},0}(\mathbb{N})$ seem to have the most wild factorization behavior. However, as points are removed from $\llbracket 0, n\rrbracket$, 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.

3.1 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 3.1.1. 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 3.1.2. Let $X, A \in \mathcal{P}_{\text{fin},0}(H)$.

(i) $A + X{:}A \subseteq X$.

(ii) If $X = A + Y$ then $Y \subseteq X{:}A$.

(iii) If A divides X if and only if $A + X{:}A = X$.

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

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

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

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

- For every atom $A \subsetneq X$, 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 3.1.3. Let $H = \mathbb{N}$ and take $X := [\![0, n]\!]$ for some odd $n \geq 11$. We can show that $A := \{0, 1, 3\}$ and $B := \{0, 1, 3, \ldots, n-2, n-3\}$ are both atoms, and that $X = A + B$ (so $A * B$ is a factorization of X). However, $X{:}A = [\![0, n]\!] \cap [\![-1, n-1]\!] \cap [\![-3, n-3]\!] = [\![0, n-3]\!] \neq B$ and $X{:}B \neq A$. Thus the above algorithm will find factorizations of the form $A * \mathfrak{b}$ for $\mathfrak{b}$ a factorization of $[\![0, n-3]\!]$ (and similarly $B * \mathfrak{a}$ for $\mathfrak{a}$ a factorization of $[\![0, 3]\!]$), but it will fail to find $A * B$.

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

Definition 3.1.4. 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 $\mathfrak{b} \in \mathbf{fac}(Y)$, add $A * \mathfrak{b}$ to $\mathbf{fac}(X)$.

(7) Return $\mathbf{fac}(X)$.

Proposition 3.1.5. 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 2.1.7. 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 3.1.2(iii) implies that $A_1 + (X{:}A_1) = X$. At this point, step (5) of the procedure for generating $\mathbf{fac}(X)$ 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. □

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

$$\mathcal{P}_n = \{X \subseteq [\![0, n]\!] : 0, n \in X\}$$
$$\mathcal{A}_n = \mathcal{A}(\mathcal{P}_{\text{fin},0}(\mathbb{N})) \cap \mathcal{P}_n$$
$$\mathcal{N}_n = \mathcal{P}_n \setminus \mathcal{A}_n$$

Remark 3.1.7. Note that

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

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

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

Definition 3.1.8. Let $n \geq 1$. A *partition of* n is $P = (m_1, \ldots, m_k)$, where $m_1 \geq \cdots \geq m_k \geq 1$ and $m_1 + \cdots + m_k = n$. Each m_i is said to be a *part* of P, and k is said to be the *length* or number of parts of P. For brevity, we occasionally write $P \vdash n$.

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

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

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

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

Remark 3.1.9. 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 3.2.

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 3.1.4, 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 $P = (m_1, \ldots, m_k)$ a partition of $\max(X)$, $\mathsf{fac\_of\_type}(X, P)$ in the following way: For every $(A_1, \ldots, A_k) \in \mathcal{A}_{m_1} \times \cdots \times \mathcal{A}_{m_k}$, if $A_1 + \cdots + A_k = X$, then add $A_1 * \cdots * A_k$ to $\mathbf{fac\_of\_type}(X, P)$.

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

(1) Start with $\mathbf{fac\_by\_type}(X) = \emptyset$.

(2) For each partition $P = (m_1, \ldots, m_k)$ of $\max(X)$, if $\{0, m_1\} + \cdots + \{0, m_k\} \subseteq X$,

  (3) Add $\mathbf{facs\_of\_type}(X, P)$ to $\mathbf{fac\_by\_type}(P)$.

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

Though this procedure for generating $\mathsf{fac\_by\_type}(X)$ still relies on brute force, it does work fast relative to fac—especially for "small" subsets $X \subseteq \mathbb{N}$. It 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 3.3.

3.2 Admissible and Forbidden Types for Intervals

Proposition 3.2.1. 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 3.1.2. 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 $X \supsetneq \{0, c\} + Y$; then there is $x \in X$ with $x \notin \{0, c\} + Y$. This means that $x \notin X \cap (X - c)$ and $x \notin X \cap (X - c)$; all together, this means $x + c, x - c \notin X$. However, this contradicts part (i), taking $b = 2c$ and $k = x + c$. Thus we must have $X = \{0, c\} + X{:}\{0, c\}$. □

Proposition 3.2.2. Let $n \geq 1$.

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

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

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

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

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

Proof. For (i), we can use the second part of Lemma 3.2.1 with $c = 1$ to see that there can be no atom A with $A + \{0, 2\} = [\![0, n]\!]$.

It is easy to see (ii) because $\{0, 2\}$ is the only atom in $\mathcal{A}_2$, and no sum of the form $\{0, 2\} + \cdots + \{0, 2\}$ can contain 1, let alone a whole interval.

For (iii), write $n = 2m + 1$. We note that $\mathcal{A}_3 = \{\{0, 2, 3\}, \{0, 1, 3\}\}$. Since 1 belongs to the interval, if $[\![0, 2m + 1]\!]$ is to have a factorization of partition type $(3, 2, \ldots, 2)$, then that factorization must include $\{0, 1, 3\}$. However, we see that

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

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

The arguments for the remaining parts proceed along similar lines. For (iv), we note that the only atoms in $\mathcal{A}_4$ which contain 1 are $\{0, 1, 4\}$ and $\{0, 1, 2, 4\}$. However, if $n = 2m$, we have

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

which again fails to contain $n - 1$.

Finally, we turn to (v). We similarly begin by observing that the only atoms in $\mathcal{A}_5$ which contain 1 are $\{0,1,5\}$, $\{0,1,2,5\}$, and $\{0,1,3,5\}$. Let $n = 2m+1$. By calculations similar to those above, one can see that $n-2 \notin \{0,1,2,5\} + (m-2)\{0,2\}$ and $n-1 \notin \{0,1,3,5\} + (m-2)\{0,2\}$. □

As we have just seen above, several partition types fail to appear because of the limited number of atoms available in $\mathcal{A}_N$ for small N. Even in $\mathcal{A}_5$, where there are a few choices of atoms containing 1, there is no atom which contains both 1 as well as enough "comparably larger" elements closer to 5. However, this issue does not seem to arise for atoms with larger maximum; indeed, in $\mathcal{A}_7$ we have several choices which fit this requirement: for example, $\{0,1,2,4,6,7\}$, and $\{0,1,3,5,6,7\}$ seem promising if one hopes to produce factorizations of type $(7,2,\ldots,2)$. Indeed, the problems that occur for atoms of sizes between 2 and 5 do not persist, for we have the following.

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

Proposition 3.2.3. Each of the following sets is an atom of $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ for the given values of the parameter h.

(i) $B_{2h-1} := \{0,1,3,\ldots,2h-1\}$ for $h \geq 1$.

(ii) $B_{2h} := \{0,1,3,\ldots,2h-1,2h\}$ for $h \geq 3$.

(iii) $C_{2h} := \{0,2,4,\ldots,2h\} \cup \{1\}$ for $h \geq 2$.

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

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

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

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

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

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

Lemma 3.2.4. 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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Lemma 3.2.6. 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 $q \equiv 0 \mod 6$, so $q = 3h$ for some even h. We first note that

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

and similarly that

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

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

Remark 3.2.7. 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 3.2.2, which says that $D_q + \{0,2\}$ cannot be an interval since D_q is an atom.

Theorem 3.2.8. Let $n \geq 1$ and suppose P is a partition of n with $P \notin \{(n-2,2)\} \cup \{(m, 2 \ldots, 2) : 2 \leq m \leq 5\}$. Then $\mathcal{Z}^P([\![0,n]\!]) \neq \emptyset$. In particular, $|\mathsf{T}([\![0,n]\!])| = p(n) - 4$, where $p(n)$ is the number of integer partitions of n.

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

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

Here, Lemma 3.2.6 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 3.2.4 is exactly that $\mathcal{Z}^P([\![0,n]\!]) \neq \emptyset$ for any such partition.

Case 3: $P = (m_1, \ldots, m_k)$ 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 $P' = (m_1, \ldots, m_{k-1})$. If $k = 3$ then $P' = (m_1, m_2)$ is a partition of $n - m_k$ as described in case 2, and if $k > 3$ then P' is as in case 3. In any event, either by the result from case 2 or by our inductive assumption, we know that $\mathcal{Z}^{P'}([\![0, n-m_k]\!]) \neq \emptyset$. Taking $\mathfrak{a}' \in \mathcal{Z}^{P'}([\![0, n-m_k]\!])$, we have that $\mathfrak{a} := \mathfrak{a}' * \{0, m_k\} \in \mathcal{Z}^P([\![0,n]\!])$.

Case 4: P has smallest part equal to 1.

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

If $k = 1$, we can see that $C_{n-1} * \{0,1\} \in \mathcal{Z}^P([\![0,n]\!])$, where C_{n-1} is one of the atoms constructed in Proposition 3.2.3. Similarly, if $k = 2$ we have by Lemma 3.2.4 that there are atoms $A \in \mathcal{A}_{m_1}$ and $A' \in \mathcal{A}_{m_2}$ with $A + A' = [\![0, m_1 + m_2]\!]$, so $A * A' * \{0,1\} \in \mathcal{Z}^P([\![0,n]\!])$.

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

3.3 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 3.3.1. Let $m_1, \ldots, m_k$ be integers. We will refer to $S = (m_1, \ldots, m_k)$ as a *sequence* of integers. Define the **set of subsums of S** to be $\Sigma(S) := \left\{\sum_{i \in I} m_i : I \subseteq [\![1,k]\!]\right\}$.

Remark 3.3.2. 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 $S = (m_1, \ldots, m_k)$ as a sum in $\mathcal{P}_{\text{fin},0}(\mathbb{Z})$: $\Sigma(S) = \{0, m_1\} + \cdots + \{0, m_k\}$.

Lemma 3.3.3. Let $m_1, \ldots, m_k$ be positive integers with $m_1 \geq \cdots \geq m_k \geq 1$ and let $n = m_1 + \cdots + m_k$. If $k > n/2$ then $\Sigma(m_1, \ldots, m_k) = [\![0,n]\!]$.

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

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

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

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

$\Sigma(T) = [\![0, n-m_1]\!]$, so $\Sigma(S) = \{0, m_1\} + [\![0, n-m_1]\!] = [\![0, n-m_1]\!] \cup [\![m_1, n]\!]$. This union of intervals is equal to $[\![0, n]\!]$ if $m_1 \leq m_2 + \cdots + m_k + 1$, so all that remains is to verify this last inequality.

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

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

Using this inequality twice, we have that

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

exactly as we wished. □

Lemma 3.3.4. Let n be even and let P be a partition into $n/2$ parts. Then one of the following holds:

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

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

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

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

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

so $k - 1 > (m_2 + \cdots + m_k)/2$; by Lemma 3.3.3, $\Sigma(m-2, \ldots, m_k) = [\![0, n - m_1]\!]$.

Now we have $\Sigma(P) = \{0, m_1\} + [\![0, n-m_1]\!] = [\![0, n-m_1]\!] \cup [\![m_1, n]\!]$, so $\Sigma(P) = [\![0, n]\!]$ provided $2m_1 < n+1$. If not, then $2m_1 \geq n + 2$, so $m_1 \geq \frac{n+2}{2}$. From this, it follows that

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

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

$[\![n/2+1, n]\!]$. □

Theorem 3.3.5. Let $X \in \mathcal{P}_{\text{fin},0}(\mathbb{N})$ and suppose that there is $k \in \mathsf{L}(X)$ with $k > \max(X)/2$. Then $X = [\![0, \max(X)]\!]$.

Proof. Let $n = \max(X)$ and let $\mathfrak{a} \in \mathcal{Z}(X)$ be a factorization with length $|\mathfrak{a}| = k$. Then there are integers $m_1 \geq \cdots \geq m_k \geq 1$ and atoms $A_i \in \mathcal{A}_{m_i}$ with $\mathfrak{a} = A_1 * \cdots * A_k$. The result is immediate from Lemma 3.3.3, since we have

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

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

Chapter 4

Techniques in Abelian Groups and Applications

4.1 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 4.1.2). This yields especially powerful results when we consider $\mathbb{N}^d$; as we will see in Theorem 4.1.6 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 [8, 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 4.1.1. Let H be a non-torsion monoid. Then there is an equimorphism from $\mathcal{P}_{\text{fin},0}(\mathbb{N}) \to \mathcal{P}_{\text{fin},1}(H)$.

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

a bijection $f^* : \mathcal{Z}_{\mathcal{P}_{\text{fin},0}(\mathbb{N})}(X) \to \mathcal{Z}_{\mathcal{P}_{\text{fin},1}(\langle x \rangle)}(f(X)) = \mathcal{Z}_{\mathcal{P}_{\text{fin},1}(H)}(f(X))$, where the last inequality follows from Proposition 2.1.2 (ii) (that is, $\mathcal{P}_{\text{fin},1}(\langle x \rangle)$ is divisor-closed in $\mathcal{P}_{\text{fin},1}(H)$). □

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 4.1.2. 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 $f : H \to K$ such that

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

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

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

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

Lemma 4.1.3. Let $\varphi : H \to K$ 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) $\varphi : \mathcal{P}_{\text{fin},0}(H) \to \mathcal{P}_{\text{fin},0}(K)$ is an atom-preserving map.

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

Proof. Point (i) is clear by taking $z = 0$ in property ($*$). To see (ii), suppose $A \subseteq W$ and $\varphi(A) = Y + Z$. Then, since $Y, Z \subseteq \varphi(A)$, we may write $Y = \varphi(B)$ and $Z = \varphi(C)$ for some $B, C \subseteq A$. For any $a \in A$, $\varphi(a) \in \varphi(B) + \varphi(C)$, so there are $b \in B$ and $c \in C$ with $\varphi(a) = \varphi(b) + \varphi(c)$. By ($*$), $a = b + c \in B + C$,

so $A \subseteq B + C$. A nearly identical argument yields the other inclusion, so that $A = B + C$. Thus, if A is an atom, so too must be $\varphi(A)$.

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

Remark 4.1.4. Note that the property $(*)$ in Lemma 4.1.3 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 4.1.5. 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 $\pi_r : \mathbb{N}^{r+1} \to \mathbb{N}$ is the projection map from the rth coordinate. Define $\varphi : \mathbb{N}^{r+1} \to \mathbb{N}^r$ by $\varphi(w_1, \ldots, w_{r+1}) = (w_1, \ldots, w_{r-1}, w_r + Nw_{r+1})$. Then

(i) φ is a homomorphism.

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

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

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

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

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

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

Finally, (iii) follows from (i) and (ii) by Lemma 4.1.3. □

Theorem 4.1.6. 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 4.1.5 gives us an X-transfer to $\varphi : \mathcal{P}_{\text{fin},0}(\mathbb{N}^2) \to \mathcal{P}_{\text{fin},0}(\mathbb{N})$, so we are done.

Now suppose $d > 2$ and assume by way of induction that $\mathcal{P}_{\text{fin},0}(\mathbb{N}^{d-1})$ is locally transferrable to $\mathcal{P}_{\text{fin},0}(\mathbb{N})$. Let $X \in \mathcal{P}_{\text{fin},0}(\mathbb{N}^d)$. As above, Proposition 4.1.5 yields an X-transfer φ to $\mathcal{P}_{\text{fin},0}(\mathbb{N}^{d-1})$. Since we have

assumed $\mathcal{P}_{\text{fin},0}(\mathbb{N}^{d-1})$ to be locally transferrable to $\mathcal{P}_{\text{fin},0}(\mathbb{N})$, there is a $\varphi(X)$-transfer $\psi : \mathcal{P}_{\text{fin},0}(\mathbb{N}^{d-1}) \to \mathcal{P}_{\text{fin},0}(\mathbb{N})$. Then $\psi \circ \varphi : \mathcal{P}_{\text{fin},0}(\mathbb{N}^d) \to \mathcal{P}_{\text{fin},0}(\mathbb{N})$ is an X-transfer, so we conclude that $\mathcal{P}_{\text{fin},0}(\mathbb{N}^d)$ is locally transferrable to $\mathcal{P}_{\text{fin},0}(\mathbb{N})$. □

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.

4.2 Independence Arguments in the Natural Lattice

Theorem 4.1.6 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., $\mathsf{L}(X)$).

Definition 4.2.1. 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 4.2.2. 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 $u_1 - v - 1 = v_2 - u_2 \in \mathbb{Z}U_1 \cap \mathbb{Z}U_2 = \{0\}$, so $u_1 = v_1$ and $u_2 = v_2$.

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

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

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

Proposition 4.2.3. Let $U, V \subseteq \mathbb{N}^d$ be $\mathbb{Z}$-independent and let $A_1, \ldots, A_k$ 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) $k \leq \max \mathsf{L}(U) + \max \mathsf{L}(V)$.

Proof. (i) For each i, let $u_i \in U \cap A_i$. Then $\sum_i u_i \in \sum_i A_i = U + V$, and there are $u \in U$ and $v \in V$ with $\sum_i u_i = u + v$. By Proposition 4.2.2(ii), $v = 0$ and $\sum_i u_i = u \in U$

The other inclusion is similar; for any $u \in U \subseteq \sum_i A_i$, we can find $u_1, \ldots, u_k \in U$ and $v_1, \ldots, v_k \in V$ such that $u_i + v_i \in A_i$ for each i and $u = \sum_i (u_i + v_i)$. Again by Proposition 4.2.2(ii), $\sum_i v_i = 0$, and each $v_i = 0$ by Proposition 4.2.2(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 $\ell = \max \mathsf{L}(U)$ and $m = \max \mathsf{L}(V)$. Without loss of generality, say $[\![1, s]\!] = \{i : U \cap A_i \neq \{0\}\}$ and $[\![t, k]\!] = \{i : V \cap A_i \neq \{0\}\}$. Since, by (i), $U = \sum_i U \cap A_i = \sum_{i \leq s} U \cap A_i$, $|[\![1, s]\!]| \leq \ell$ (similarly, $|[\![t, k]\!]| \leq m$). By (iii), $[\![1, k]\!] = [\![1, s]\!] \cup [\![t, k]\!]$, so $k \leq \ell + m$ as we wished. □

Lemma 4.2.4. Let $U, V_1, \ldots, V_m \subseteq \mathbb{N}^d$ be totally $\mathbb{Z}$-independent. Suppose each V_j is an atom, and let $V := \sum_j V_j$. Further suppose that $A_1, \ldots, A_k$ are nonzero subsets with $U + V = \sum_{i=1}^k A_i$.

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

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

(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 4.2.3(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 $V_1, \ldots, V_m$ 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 4.2.3(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 4.2.3 (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). □

Theorem 4.2.5. If $V_1, \ldots, V_m \subseteq \mathbb{N}^d$ are totally $\mathbb{Z}$-independent then $V_1 + \cdots + V_m$ factors uniquely (up to reordering of factors).

Proof. Let $V = V_1 + \cdots + V_m$. The result will essentially follow from Lemma 4.2.4, taking $U = \{0\}$.

Let $A_1, \ldots, A_k$ be atoms with $V = \sum_i A_i$. As in Lemma 4.2.4(i), there is $f : [\![1, m]\!] \to [\![1, k]\!]$ with $V_j \subseteq A_{f(j)}$ for each $j \in [\![1, m]\!]$. We wish to show that f is injective; let $h \in [\![1, k]\!]$ and let $J = f^{-1}(h)$. By Lemma 4.2.4(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 4.2.3(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 $V_1 * \cdots * V_m$. □

Example 4.2.6. Theorem 4.2.5 allows us to partially recover [8, 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 $a_1 + \cdots + a_i < \frac{1}{2}a_{i+1}$ for $i \in [\![1, \ell-2]\!]$ and (if $\ell \geq 2$) $a_1 + \cdots + a_{\ell-1} < a_\ell - a_{\ell-1}$. Then $\mathcal{Z}(\{0, a_1\} + \cdots + \{0, a_\ell\}) = \{\{0, a_1\} * \cdots * \{0, a_\ell\}\}$.

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 ith standard basis vector (whose entries are all zero, except for a 1 in the ith coordinate). Let $V = \{0, e_1\} + \cdots + \{0, e_\ell\}$; by Theorem 4.2.5, V factors uniquely. We will follow the procedure given in Theorem 4.1.6 to "flatten" V into a subset of $\mathbb{N}$ which still factors uniquely. According to this procedure, we need maps $\mathbb{N}^\ell \to \mathbb{N}^{\ell-1} \to \cdots \to \mathbb{N}$.

For $i \in [\![1, \ell-1]\!]$, define $\varphi_i : \mathbb{N}^{i+1} \to \mathbb{N}^i$ by $v \mapsto \hat{v} + be_i$ (where $\hat{v}$ is the vector consisting of the first i components of v, and we have identified e_i with the ith standard basis vector in $\mathbb{N}^i$). Let $V_\ell = V$ and $V_i = \varphi_i(V_i + 1)$ for $i < \ell$. By Proposition 4.1.5, φ_i is a homomorphism which essentially preserves the set of factorizations of V_{i+1}. Letting $\varphi := \varphi_1 \circ \cdots \circ \varphi_{\ell-1}$, we have that $U := \varphi(V)$ factors uniquely.

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

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

Theorem 4.2.7. Let $U \in \mathcal{P}_{\text{fin},0}(\mathbb{N}^d)$ be an element whose two longest factorizations have lengths $\ell < N$. Suppose $V_1, \dots, V_m \subseteq \mathbb{N}^d$ are atoms so that $U, V_1, \dots, V_k$ are totally $\mathbb{Z}$-independent. Further assume that U has a unique longest factorization (of length N). Then $\mathsf{L}(U + V_1 + \cdots + V_k) \cap [\![\ell + 1, \infty]\!] = \{N + m\}$.

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 4.2.3(iv), we know that $k \leq N + m$.

By Proposition 4.2.3(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 4.2.4 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 4.2.4(ii),(iii).

Claim B: $A_i \subseteq U$ for $i < t$ and $A_i \subseteq V$ for $i > s$.

Proposition 4.2.3(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 $u_1, \ldots, u_s \in U$ and $v_t, \ldots, v_k \in V$ 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 $U, V_1, \ldots, V_m$ implies that $u = \sum_{i \leq s} u_i$, $v_s = v$, and $v_i = 0$ for all $i \neq s$. Now $u + v = \sum_{i<s} u_i + (u_s + v) \in \sum_{i<s} U \cap A_i + (U + v) \cap A_s$.

For the other inclusion, let $u_1, \ldots, u_s \in U$ with $u_i \in A_i$ for all $i < s$ and $u_s + v \in A_s$. Then $\sum_{i \leq s} u_i + v \in \sum_{i \leq s} A_i \subseteq U + V$, so we can find $u' \in U$ and $v' \in V$ with

$$\sum_{i \leq s} u_i + v = u' + v',$$

at which point we can use $\mathbb{Z}$-independence again to see that $v' = v$, so that $\sum_{i \leq s} u_i + v \in U + v$.

Claim D: $(U + v) \cap A_s = U \cap A_s + v$.

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 $\mathcal{P}_{\mathrm{fin},0}(\mathbb{Z}^n)$), yielding

$$U = \sum_{i<s} U \cap A_i + A. \tag{D1}$$

On the other hand, we also have that

$$U = \sum_{i<s} U \cap A_i + U \cap A_s. \tag{D2}$$

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 intial 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 ℓ atoms. Say $B_1, \ldots, B_N$ are the atoms with $U = \sum_{i=1}^{N} B_i$. Then, by renumbering if needed, there is some h for which $\sum_{i<s} U \cap A_i = B_1 + \cdots + B_h$.

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

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

and we have proved the claim.

Claim E: A_s is not an atom.

To see this, we compute

$$\begin{aligned} A_s = (U+V) \cap A_s &= (U + V' + V'') \cap A_s \\ &= (U + V') \cap A_s && \text{(by Claim A and Proposition 4.2.3)} \\ &= \bigcup_{v \in V'} (U+v) \cap A_s \\ &= \bigcup_{v \in V'} (U \cap A_s + v) && \text{(by Claim D)} \\ &= U \cap A_s + V'. \end{aligned}$$

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 4.2.3(iii). For $i \leq s$, since $V \cap A_i = \{0\}$, Proposition 4.2.3(ii) implies that $A_i = (U+V) \cap A_i = U \cap A_i \subseteq U$. Then we have, by Proposition 4.2.3(i), that $U = \sum_{i \leq s} U \cap A_i = \sum_{i \leq s} A_i$. This means that $s \in \mathsf{L}(U)$ and, by identical reasoning for V, that $|[\![t, k]\!]| = m$. We conclude that $k \in \mathsf{L}(U) + m$ and, due to the assumption that $k > \ell + m$, it must be the case that $k = N + m$. □

4.3 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 [8, 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 4.3.1. 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 ith standard basis vector, whose components are all zero except for a single 1 in the ith 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 4.3.3) 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 4.3.2. Let U_{n+1} be as in Definition 4.3.1, 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 $f \notin \text{span}_{\mathbb{Z}}(\{e_1, \ldots, e_{n-1}\} \cup V)$ 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, $g \notin \text{span}_{\mathbb{Z}}(\{e_1, \ldots, e_{n-1}\} \cup V)$. 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. □

Theorem 4.3.3. Let $n \geq 2$ and let $e_1, \ldots, e_n \in \mathbb{N}^n$ 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

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

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 [8, 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 $2e_1 + e_{K \setminus \{k\}} = e_1 + e_K \in X + Y$, 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 ≥ 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 ≥ 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 4.2.5, Y factors uniquely and we have $\{0,e_1\} * \cdots \{0,e_n\} * \{0,g\} \in \mathcal{Z}_{\mathcal{P}_{\mathrm{fin},0}(\mathbb{N}^n)}(U)$.

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

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

We can completely determine the structure of Y. First observe that we cannot have $f = e_{[\![1,n]\!]} \in Y$ since we would then have $(g + e_{I_X}) + f \in X + Y$, but this is not an element of U. This allows us to use 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 3.1.2, 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 4.2.5) 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 4.2.5) as the sum of $\{0,g\}$ and the $\{0,e_i\}$ for $i\in I_X$. This can only produce – up to reordering, of course – the factorization $\{0,g\}*\{0,e_1\}*\cdots*\{0,e_n\}\in\mathcal{Z}_{\mathcal{P}_{\mathrm{fin},0}(\mathbb{N}^n)}(U)$.

If $f\in X$, then $X=\left[\{0,g\}+\sum_{i\in I_X}\{0,e_i\}\right]\cup\{f\}$ (and $Y=\{0,e_n\}$ per our considerations in (F3′)). By Lemma 4.3.2, X is an atom, producing the factorization $X*\{0,e_n\}\in\mathcal{Z}_{\mathcal{P}_{\mathrm{fin},0}(\mathbb{N}^n)}(U)$ and completing the proof. □

Remark 4.3.4. In the same vein as Example 4.2.6, one may use Theorem 4.3.3 to recover some cases of [8, Proposition 4.8].

Corollary 4.3.5. Fix $n\geq 2$ and $m\geq 1$, and let $V_1,\ldots,V_m\subseteq\mathbb{N}^d$ be atoms such that $U_{n+1},V_1,\ldots,V_m$ are totally $\mathbb{Z}$-independent. Then $\mathsf{L}(U_{n+1}+V_1+\cdots+V_m)=[\![2,m+2]\!]\cup\{m+n+1\}$.

Proof. For convenience, let $U:=U_{n+1}$ and $V:=V_1+\cdots+V_m$. We will start by verifying the values that most clearly belong to $\mathsf{L}(U+V)$. It is easiest to see that $m+n+1=\max\mathsf{L}(V)+\max\mathsf{L}(U)\in\mathsf{L}(U+V)$. For the rest, suppose $0\leq h\leq m$. Then, by Lemma 4.3.2,

$$B_h:=\left(\sum_{i=1}^{n-1}\{0,e_i\}+\{0,g\}+\sum_{j\in[\![h+1,m]\!]}V_j\right)\cup\{f\}$$

is an atom. From here, it is straightforward to check that

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

so $h+2\in\mathsf{L}(U+V)$. As we allow h to range over $[\![0,m]\!]$, we get that $[\![2,m+2]\!]\in\mathsf{L}(U+V)$.

For the other inclusion, we need to show that no other values are included in $\mathsf{L}(U+V)$. To do this, we note that U has a unique longest factorization by Theorem 4.3.3 and hence, using Theorem 4.2.7, $\mathsf{L}(U+V)\cap[\![m+3,m+n+1]\!]=\{m+n+1\}$. □

Chapter 5

Polynomial Rings

In this chapter we will connect the arithmetic of subsets of $\mathbb{N}$ to the study of polynomials, with a view toward understanding the distribution of atoms inside $\mathcal{P}_{\text{fin},0}(\mathbb{N})$. In the same spirit, we will also discuss the asymptotic density of irreducible elements in numerical monoid rings over finite fields.

5.1 Identifying Subsets with Polynomials

5.2 Atomic Density in Numerical Monoid Rings

In this section we shift to a discussion of polynomials which is entirely independent of the subset arithmetic. In particular, we will focus on rings constructed from numerical monoids, which have already been studied extensively [REFERENCES FOR NUMERICAL MONOIDS].

Definition 5.2.1. A numerical monoid is an additive submonoid $H \leq \mathbb{N}$ such that $\mathbb{N} \setminus H$ is a finite set.

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

We wish to study a family of polynomial rings constructed from numerical monoids [REFERENCES??].

Definition 5.2.2. Let H be a numerical monoid and let K be a field. Then the *numerical monoid ring of over* K *associated to* H is $K[H] := K[x^h : h \in H]$.

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

Example 5.2.3. Let $H = \langle 2, 3\rangle = \mathbb{N} \setminus \{1\}$ be the numerical monoid generated by $\{2, 3\}$. Then, for any field K, $K[H] = K[x^2, x^3] \subseteq K[x]$ is the ring of polynomials with coefficients in K whose linear coefficient is zero.

We have one more collection of definitions to state before we can proceed toward the main goal of this section.

Definition 5.2.4. Let K be a field and let $n \in \mathbb{N}$. For any subset $S \subseteq K[x]$, let $S^{(n)} := \{f \in S : \deg(f) = n\}$.

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

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

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

Proposition 5.2.5. Let q be a prime power and let $n \in \mathbb{N}$. Then the number of irreducibles in $\mathbb{F}_q[x]$ satisfies $a_q^{\mathbb{N}}(n) \leq \frac{q^n}{n}$. In particular, $\rho_q(n) \to 0$ as $n \to \infty$.

Proof. This can be argued by counting the irreducible elements of $\mathbb{F}_{q^n}$ and then applying the Möbius inversion formula. A complete proof of this is outlined in [DUMMIT AND FOOTE, OTHER FINITE FIELDS BOOK. CHECK THAT PROOF WORKS FOR $q = p^n$ AND NOT JUST p] □

Lemma 5.2.6. Let $n \in \mathbb{N}$ and let $k \geq 1$. Then

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

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

Proof. We will prove this by induction on k. For $k = 1$, the result is trivial as there is only one partition of n into 1 part. Now suppose, for some $k \geq 1$, that $\sum_{m_1+\cdots+m_k=n} \frac{1}{m_1\cdots m_k} \leq \frac{\log^{k-1}(n)}{n}$. Then we calculate

$$\begin{aligned}
\sum_{m_1,\ldots,m_{k+1}} \frac{1}{m_1 \cdots m_k} &= \sum_{m=1}^{\lfloor n/(k+1)\rfloor} \frac{1}{m} \sum_{m_1,\ldots,m_k} \frac{1}{m_1 \cdots m_k} \qquad \text{(inner sum taken over partitions of } n-m\text{)} \\
&\leq \sum_{m=1}^{\lfloor n/(k+1)\rfloor} \frac{1}{m} \left(\frac{\log^{k-1}(n-m)}{n-m}\right) \\
&\leq \underbrace{\log^k(n) \sum_{m=1}^{\lfloor n/(k+1)\rfloor} \frac{1}{m(n-m)}}_{S:=}
\end{aligned}$$

Now, because $\frac{1}{x(n-x)}$ is decreasing on the interval $(0, n/2)$, a right Riemann sum of width-1 rectangles is an under-approximation of the area under the graph of $\frac{1}{x(n-x)}$. That is, we may replace the sum in the last line with an integral and continue with

$$S \leq \log^k(n) \int_1^{n/(k+1)} \frac{1}{x(n-x)}\, dx \leq \log^k(n) \left(\frac{\log(n)}{n}\right)$$

where the last integral was evaluated by first finding the partial fraction decomposition of the integrand. This proves the inequality we wanted to show for the inductive step, completing the proof. □

Lemma 5.2.7. Let q be a prime power, let $N \in \mathbb{N}$ be positive, and let $r \geq q^{N-1}$. If $f_1, \ldots, f_k \in \mathbb{F}_q[x]$ with $f_i(0) \neq 0$ then there is some $f \in \mathbb{F}_q + x^N \mathbb{F}_q[x]$ with $f | f_1 \ldots f_k$. That is, there is a sub-product of $f_1 \cdots f_k$ which whose coefficients of degree $1 \leq d < N$ are all zero.

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

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

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

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

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

Proposition 5.2.8. Let H be a numerical monoid and let $f \in \mathbb{F}_q[H]$ be irreducible. Then f is of one of the following types:

(1) There are $k < q^{F(H)}$ and irreducibles $f_1, \ldots, f_k \in \mathbb{F}_q[x]$ with $f = f_1 \cdots f_k$.

(2) There are $m < 2(F(H) + 1)$, $k < q^{F(H)}$, and irreducibles $f_1, \ldots, f_k \in \mathbb{F}_q[x]$ with $f = x^m f_1 \cdots f_k$.

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

Case 1: x does not divide f. Then we may write $f = f_1 \cdots f_k$ for some irreducibles $f_1, \ldots, f_k \in \mathbb{F}_q[x]$ (and $f_i(0) \neq 0$ for each i). Suppose $k \geq q^{F(H)} = q^{N-1}$; then, by Lemma 5.2.7, there is a $g | f_1 \ldots f_k$ with $g \in \mathbb{F}_q + x^N \mathbb{F}_q[x]t$. Let $h = (f_1 \cdots f_k)/g$. Since $gh = f_1 \cdots f_k = f \in \mathbb{F}_q[H]$, we must have that $g(0) \neq 0$ (otherwise $f(0) = 0$ and f would be divisible by x). Then we claim that $h \in \mathbb{F}_q[H]$; if not, then there is some $d \in G(H)$ so that the x^d term of h is ax^d for some $a \in \mathbb{F}_q \setminus \{0\}$. Consequently, the x^d coefficient of $f = gh$ is $g(0)a \neq 0$, so $f \notin \mathbb{F}_q[H]$, a contradiction. However, this implies that $g, h \in \mathbb{F}_q[H]$, which produces a contradiction to the irreducibility of f in $\mathbb{F}_q[H]$ and implies that $k < q^{F(H)}$.

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

All that remains is to manage k; suppose $k \geq q^{N-1}$. Since x does not divide $f_1 \cdots f_k$, we have that $f_i(0) \neq 0$ for each $i \leq r$ and, as before, Lemma 5.2.7 gives us a $g \in \mathbb{F}_q + x^N \mathbb{F}_q[x]$ with $g | f_1 \cdots f_k$. Then, choosing $h \in \mathbb{F}_q[x]$ so that $gh = f_1 \cdots f_k$, we now wish to show that $x^m h \in \mathbb{F}_q[H]$. However, since $g(x^m h) = f \in \mathbb{F}_q[H]$, we can argue this in the same manner as in Case 1 (with our $x^m h$ playing the role of h from Case 1). This yields a contradiction and we conclude, as in the previous case, that $k < q$. □

Theorem 5.2.9. Let H be a numerical monoid and let q be a prime power. Then $\lim_{n \to \infty} \rho_q^H(n) = 0$.

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

Next, we can make crude estimates on the number of each of the types of irreducibles from the characterization given in Proposition 5.2.8. Let $A^1(n)$ and $A^2(n)$ denote the numbers of irreducibles of types (1) and (2) from Proposition 5.2.8, respectively.

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

$$A^1(n) \leq \underbrace{\sum_{\substack{m_1,\ldots,m_k \\ k<M}} a_q(m_1)\cdots a_q(m_k)}_{\substack{\text{Number of degree } n \text{ products} \\ \text{of } k \text{ irreducibles of } \mathbb{F}_q[x]}} = \sum_{m_1,\ldots,m_k} \left(\frac{q^{m_1}}{m_1}\right)\cdots\left(\frac{q^{m_k}}{m_k}\right) = \sum_{m_1,\ldots,m_k} \frac{q^n}{m_1\cdots m_k}. \qquad (*)$$

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

$$a_q^H(n) = A^1(n) + A^2(n) \leq (2F(H)+2) \sum_{\substack{m_1,\ldots,m_k \\ k<M}} \frac{q^n}{m_1\cdots m_k}.$$

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

$$\begin{aligned}
\rho_q^H(n) &= \frac{a_q^H(n)}{|\mathbb{F}_q[H]^{(n)}|} \\
&\leq \frac{2F(H)+2}{(q-1)q^{n-g(H)}} \sum_{\substack{m_1,\ldots,m_k \\ k<M}} \frac{q^n}{m_1\cdots m_k} \\
&= C\sum_{k=1}^{M} \sum_{m_1,\ldots,m_k} \frac{1}{m_1\cdots m_k} && \text{(letting } C := (2F(H)+2)q^{g(H)}/(q-1)\text{)} \\
&\leq C\sum_{k=1}^{M} \frac{\log^{k-1}(n)}{n} && \text{(by Lemma 5.2.6)}
\end{aligned}$$

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

Bibliography

[1] Paul-Jean Cahen and Jean-Luc Chabert. *Integer-valued polynomials*, volume 48 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 1997.

[2] Scott T. Chapman. On the Davenport constant, the cross number, and their application in factorization theory. In *Zero-dimensional commutative rings (Knoxville, TN, 1994)*, volume 171 of *Lecture Notes in Pure and Appl. Math.*, pages 167–190. Dekker, New York, 1995.

[3] Scott T. Chapman. A tale of two monoids: a friendly introduction to nonunique factorizations. *Math. Mag.*, 87(3):163–173, 2014.

[4] Scott T. Chapman, Marly Corrales, Andrew Miller, Chris Miller, and Dhir Patel. The catenary degrees of elements in numerical monoids generated by arithmetic sequences. *Comm. Algebra*, 45(12):5443–5452, 2017.

[5] Scott T. Chapman and Ulrich Krause. A closer look at non-unique factorization via atomic decay and strong atoms. In *Progress in commutative algebra 2*, pages 301–315. Walter de Gruyter, Berlin, 2012.

[6] Kálmán Cziszter, Mátyás Domokos, and Alfred Geroldinger. The interplay of invariant theory with multiplicative ideal theory and with arithmetic combinatorics. In *Multiplicative ideal theory and factorization theory*, volume 170 of *Springer Proc. Math. Stat.*, pages 43–95. Springer, [Cham], 2016.

[7] Yushuang Fan, Alfred Geroldinger, Florian Kainrath, and Salvatore Tringali. Arithmetic of commutative semigroups with a focus on semigroups of ideals and modules. *J. Algebra Appl.*, 16(12):1750234, 42, 2017.

[8] Yushuang Fan and Salvatore Tringali. Power monoids: a bridge between factorization theory and arithmetic combinatorics. *J. Algebra*, 512:252–294, 2018.

[9] Sophie Frisch. A construction of integer-valued polynomials with prescribed sets of lengths of factorizations. *Monatsh. Math.*, 171(3-4):341–350, 2013.

[10] Weidong Gao and Alfred Geroldinger. Zero-sum problems in finite abelian groups: a survey. *Expo. Math.*, 24(4):337–369, 2006.

[11] Weidong Gao, Yuanlin Li, Jiangtao Peng, and Guoqing Wang. A unifying look at zero-sum invariants. *Int. J. Number Theory*, 14(3):705–711, 2018.

[12] Alfred Geroldinger. Sets of lengths. *Amer. Math. Monthly*, 123(10):960–988, 2016.

[13] 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.

[14] Alfred Geroldinger and Günter Lettl. Factorization problems in semigroups. *Semigroup Forum*, 40(1):23–38, 1990.

[15] Alfred Geroldinger and Imre Z. Ruzsa. *Combinatorial number theory and additive group theory*. Advanced Courses in Mathematics. CRM Barcelona. Birkhäuser Verlag, Basel, 2009. Courses and seminars from the DocCourse in Combinatorics and Geometry held in Barcelona, 2008.

[16] Alfred Geroldinger and Wolfgang Alexander Schmid. A realization theorem for sets of lengths in numerical monoids. *Forum Math.*, 30(5):1111–1118, 2018.

[17] Alfred Geroldinger and Emil Daniel Schwab. Sets of lengths in atomic unit-cancellative finitely presented monoids. *Colloq. Math.*, 151(2):171–187, 2018.

[18] Daniel Gorenstein. *Finite groups*. Chelsea Publishing Co., New York, second edition, 1980.

[19] David J. Grynkiewicz. *Structural additive theory*, volume 30 of *Developments in Mathematics*. Springer, Cham, 2013.

[20] Alan Loper and Paul-Jean Cahen. Rings of integer-valued rational functions. *J. Pure Appl. Algebra*, 131(2):179–193, 1998.

[21] Salvatore Tringali. Structural properties of subadditive families with applications to factorization theory. *arXiv e-prints*, page arXiv:1706.03525, Jun 2017.

[22] Thomas A. Whitelaw. *Introduction to abstract algebra*. Blackie, Glasgow, 2nd ed. edition, 1988.