Subset Arithmetic and the Factorization Theory of Power Monoids

Austin A. Antoniou

June 27, 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.

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).

1.3 Preliminaries

1.3.1 Notation and Conventions

$\mathbb{N} = \{0, 1, 2, 3, \dots\}$ will denote the set of non-negative integers. i, j, k, ℓ, m, and n will usually stand for non-negative integers, unless otherwise specified. In general unless otherwise specified, lowercase letter will usually refer to elements of a monoid; ordinary uppercase letters to subsets; script or calligraphic uppercase letters to collections of subsets. For real numbers a and b, $[\![a, b]\!] = \{n \in \mathbb{Z} : a \le n \le b\}$ shall denote the integer interval (or just “interval”) from a to b.

The *free monoid* on some generating set S will be denoted by $\mathscr{F}^*(S)$. 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 multiplicative operation is present, is meant to be interpreted as the concatenation of words. The elements of $\mathscr{F}^*(S)$ will usually be represented by the fraktur letters $\mathfrak{a}$, $\mathfrak{b}$, and so on. The *length* of a word $\mathfrak{s} = s_1 * \cdots * s_\ell \in \mathscr{F}^*(S)$, 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 $\mathscr{A}(H)$.

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 $a \in \mathscr{A}(H)$, and let $u, v \in H^\times$. Then $uav \in \mathscr{A}(H)$.

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

The **factorization monoid** of H is the free monoid $\mathscr{F}^*(\mathscr{A}(H))$ 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

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

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 $\mathfrak{a} \in \mathscr{Z}_H(x)$, 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 $\mathfrak{a}, \mathfrak{b} \in \mathscr{F}^*(\mathscr{A}(H))$. 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 $\mathscr{F}^*(\mathscr{A}(H))$.

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

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

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:

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

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, $\mathcal{P}_{\mathrm{fin},1}(H)$ is indeed a reduced monoid; i.e., its only unit is $\{1_H\}$.

(iii) Unless H is trivial, $\mathcal{P}_{\mathrm{fin}}(H)$ 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 may often use without comment.

Proposition 2.1.1. Let H be a monoid and let $u, v \in H^\times$. The following hold:

(i) If $a \in \mathscr{A}(H)$ then $uav \in \mathscr{A}(H)$.

(ii) If $x \in H \setminus H^\times$ then $\mathsf{L}_H(uxv) = \mathsf{L}_H(x)$.

Proof. These are no different from points (ii) and (iv) of [8, Lemma 2.2]. □

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

(i) If $X_1, \ldots, X_n \in \mathcal{P}_{\mathrm{fin},\times}(H)$ then $|X_1 \cdots X_n| \geq \max_{1 \leq i \leq n} |X_i|$, and if $X_1, \ldots, X_n \in \mathcal{P}_{\mathrm{fin},1}(H)$ then $X_1 \cup \cdots \cup X_n \subseteq X_1 \cdots X_n$.

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

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

(iv) $\mathscr{A}(\mathcal{P}_{\mathrm{fin},\times}(H)) \subseteq H^\times \mathscr{A}(\mathcal{P}_{\mathrm{fin},1}(H)) H^\times$.

Proof. (ii) and (iii) are both straightforward from (i); for the latter it suffices to note that $|uXv| = |X|$ for all $u, v \in H^\times$ and $X \in \mathcal{P}_{\mathrm{fin},\times}(H)$, and that $(X \cdot 1) \cup (1 \cdot Y) \subseteq XY$ for all $X, Y \in \mathcal{P}_{\mathrm{fin},1}(H)$.

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

Our ultimate goal is to investigate factorizations in $\mathcal{P}_{\mathrm{fin}}(H)$ for an arbitrary monoid H. However, this is a difficult task in general, due to a variety of "pathological phenomena" that arise; see, for example, [8, Remark 3.6]. It is in practice more convenient to start with $\mathcal{P}_{\mathrm{fin},1}(H)$ and then lift arithmetic results from $\mathcal{P}_{\mathrm{fin},1}(H)$ to $\mathcal{P}_{\mathrm{fin},\times}(H)$, a point of view which is corroborated by the simple consideration that $\mathcal{P}_{\mathrm{fin}}(H) = \mathcal{P}_{\mathrm{fin},\times}(H)$

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 [19, 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 let $\varphi : H \to K$ be a monoid homomorphism. We say φ is an *equimorphism* if

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

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

(E3) If $x \in H$ and $\mathfrak{b} \in \mathcal{Z}_K(\varphi(x))$ is a non-empty word, there is $\mathfrak{a} \in \mathcal{Z}_H(x)$ with $\varphi^*(\mathfrak{a}) \in [\![\mathfrak{b}]\!]_{\mathscr{C}_K}$,

where $\varphi^* : \mathscr{F}^*(H) \to \mathscr{F}^*(K)$ is the (unique) monoid homomorphism induced by φ. 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. These statements and their proofs can be found in [8, Theorem 2.22] and [19, Theorem 3.3]. □

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

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

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

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

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

Proof. To ease notation, we will write $P_\times$ in place of $\mathcal{P}_{\text{fin},\times}(H)$ and P_1 in place of $\mathcal{P}_{\text{fin},1}(H)$.

In view of Proposition 2.1.4, points (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(iv), and the other inclusion will follow from (i). As such, we focus on (i) for the remainder of the proof.

Clearly, the embedding $P_1 \hookrightarrow P_\times$ satisfies 1. We also see that it is essentially surjective, as any $X \in P_\times$ contains a unit $u \in H$, so $u^{-1}X \in P_1$ and thus $X = u(u^{-1}X)$ is associate to an element of P_1.

To prove 2, let $A \in \mathscr{A}(P_1)$. We aim to show that A is an atom of $P_\times$. For, suppose that $A = XY$ for some $X, Y \in P_\times$. Then $xy = 1$ for some $x \in X$ and $y \in Y$. So, using that H is Dedekind-finite, we get from [8, Lemma 2.2(i)] that $x, y \in H^\times$, and hence $y = x^{-1}$. It follows that $A = XY = (Xx^{-1})(xY)$ and $Xx^{-1}, xY \in P_\times$. But then $Xx^{-1} = \{1\}$ or $xY = \{1\}$, since P_1 is a reduced monoid and A is an atom of P_1. That is, X or Y is a one-element subset of $H^\times$, whence A is an atom of $P_\times$.

We are left with 3. So, pick $X \in P_1$. If $X = \{1\}$, the conclusion holds vacuously. Otherwise, let $\mathfrak{b} := B_1 * \cdots * B_k \in \mathscr{Z}_{P_\times}(X)$. Since $X \in P_1$, there are $u_1 \in B_1, \dots, u_k \in B_k$ such that $1 = u_1 \cdots u_k$. Hence, as in the proof of 2, it must be that $u_1, \dots, u_k \in H^\times$. Accordingly, we take, for every $i \in [\![1, k]\!]$, $A_i := u_0 \cdots u_{i-1} B_i u_i^{-1} \cdots u_1^{-1}$, where $u_0 := 1$. Then $1 \in A_i$, and we see from Proposition 2.1.2(iv) and [8, Proposition 2.2(ii)] that A_i is an atom of P_1, and consequently $\mathfrak{a} := A_1 * \cdots * A_k \in \mathscr{Z}_{P_1}(X)$. But each A_i is associate to B_i (by construction). So we have $\mathfrak{a} \in [\![\mathfrak{b}]\!]_{\mathscr{C}_{\mathscr{P}_\times}}$, 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 B be the set of all binary sequences $\mathfrak{s} : \mathbf{N}^+ \to \{0, 1\}$, and let H denote the monoid of all functions $\mathsf{B} \to \mathsf{B}$ under composition; we will write B multiplicatively, so that, if $f, g \in \mathsf{B}$ then fg is the map $\mathsf{B} \to \mathsf{B} : \mathfrak{s} \mapsto f(g(\mathfrak{s}))$. Further, let $n \geq 5$ and consider the functions $L, R, P : \mathsf{B} \to \mathsf{B}$ given by

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

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

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

In particular, observe that $LR = \mathrm{id}_\mathsf{B}$ but $RL \neq \mathrm{id}_\mathsf{B}$, whence H is not Dedekind-finite.

We will prove that $A := \{L, P\} \cdot \{R, P\} = \{\mathrm{id}_\mathsf{B}, LP, PR, P^2\}$ 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 must belong to X or Y (since P^2 must be a product of units), but not both (which is the reason for choosing $n \geq 5$). Without loss of generality, let $P^2 \in X \setminus Y$. Then $Y = \{\mathrm{id}_\mathsf{B}\}$, since one can easily check that $P^2LP, P^3R \notin A$, by noting that the action of P^2LP and P^3R differ from that of A on the sequences $(1, 1, \dots)$ and $(1, 0, 1, 1, \dots)$. This makes A an atom of $\mathcal{P}_{\mathrm{fin},1}(H)$.

We see 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 $\mathscr{A}(\mathcal{P}_{\text{fin},1}(H))$ in full generality.

Lemma 2.1.7. Let H be a monoid and $x \in H \setminus \{1\}$. The following hold:

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

(ii) If $x^2 = 1_H$ or $x^2 = x$, then $\{1_H, x\}$ is not a product of atoms in $\mathcal{P}_{\text{fin},1}(H)$ or in $\mathcal{P}_{\text{fin},\times}(H)$.

Proof. (i) It is clear that, if $x^2 = 1$ or $x^2 = x$, then $\{1, x\} = \{1, x\}^2$, and therefore $\{1, x\}$ is not an atom of $\mathcal{P}_{\text{fin},1}(H)$. As for the converse, assume that $\{1, x\} = YZ$ for some non-units $Y, Z \in \mathcal{P}_{\text{fin},1}(H)$. Then we get from Proposition 2.1.2 that X and Y are two-elements sets, namely, $Y = \{1, y\}$ and $Z = \{1, z\}$ with $y, z \in H \setminus \{1\}$. Hence $\{1, x\} = YZ = \{1, y, z, yz\}$, and immediately this implies $x = y = z$. Therefore, $\{1, x\} = \{1, x, x^2\}$, which is only possible if $x^2 = 1$ or $x^2 = x$.

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

It remains to prove the analogous statement for $\mathcal{P}_{\text{fin},\times}(H)$. For, assume to the contrary that $\{1_H, x\}$ factors into a product of, say, n atoms of $\mathcal{P}_{\text{fin},\times}(H)$. Then $n \geq 2$, since $\{1_H, x\}$ is a non-trivial idempotent (and hence not an atom itself). Consequently, we can write $\{1_H, x\} = YZ$, where Y is an atom and Z a non-unit of $\mathcal{P}_{\text{fin},\times}(H)$. In particular, we get from points (i) and (iii) of Proposition 2.1.2 that both X and Y are 2-element sets, say, $Y = \{u, y\}$ and $Z = \{v, z\}$. It is then immediate to see that there are only two possibilities: 1_H is the product of two units from Y and Z, or 1_H is the product of two non-units from Y and Z. Without loss of generality, we are thus reduced to considering the following cases.

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

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

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

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

We have just seen that, to even *hope* for $\mathcal{P}_{\text{fin},1}(H)$ to be atomic, we must have that the "bottom layer" of two-element subsets of H consists only of atoms, and it will turn out that this is also a sufficient condition.

Before proving this, it seems appropriate to point out some structural implications of the condition that every non-identity element of H is neither an idempotent nor a square root of 1.

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

(i) H is Dedekind-finite.

(ii) If $x \in H$ and $\langle x \rangle = \{x^k : k \geq 1\}$ is finite, then $x \in H^\times$ and $\langle x \rangle$ is a cyclic group.

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

(ii) This follows from [20, 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 $\langle x \rangle$ is finite, there exist $n, k \in \mathbf{N}^+$ such that $x^n = x^{n+k}$, and by induction $x^n = x^{n+hk}$ for all $h \in \mathbf{N}$. It follows that

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

and hence $\langle x \rangle$ has an idempotent. But H has no non-trivial idempotents, thus it must be the case that $x^{nk} = 1$. That is, x is invertible with $x^{-1} = x^{nk-1} \in \langle x \rangle$, and $\langle x \rangle$ is a (finite) cyclic group. □

Theorem 2.1.9. Let H be a monoid. Then $\mathcal{P}_{\text{fin},1}(H)$ is an atomic monoid if and only if $1 \neq x^2 \neq x$ for all $x \in H \setminus \{1\}$.

Proof. The "only if" part is a consequence of Lemma 2.1.7(ii). As for the other direction, assume that $1 \neq x^2 \neq x$ for each $x \in H \setminus \{1\}$, and fix $X \in \mathcal{P}_{\text{fin},1}(H)$ with $|X| \geq 2$.

We wish to show that X can be factored as a product of atoms. If $|X| = 2$, 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 take $|X| \geq |A| \geq |B| \geq 2$.

If $|A| < |X|$, both A and B factor as a product of atoms (by the inductive hypothesis), and so too does $X = AB$. Therefore, we are only left to consider the case when $|X| = |A|$. This implies $AB = A$ and $B \subseteq A$, as $A = A \cdot 1 \subseteq AB = X$ and $B = 1 \cdot B \subseteq AB = A$.

Since B is a non-unit, we can choose $b \in B \setminus \{1\} \subseteq A$ and set $A_b := A \setminus \{b\}$, so $|A_b| < |A|$. If $|B| < |A|$ then A_b and B are both products of atoms (by induction), thus so is $X = AB = A_b B$. If $|B| = |A|$ then, in fact, $B = A$. By assumption, $|A| = |X| \geq 3$, so choose $a \in A \setminus \{1, b\}$; then $X = AB = A_b(B \setminus \{a\})$. By induction, both sets on the right hand side are products of atoms, making the same true for X and finishing the proof. □

Now that we have established when power monoids are atomic, we can engage in a finer study of their arithmetic. For instance, we may wish to study their (systems of) sets of lengths. However, we are met with a problem immediately: Some sets of lengths in power monoids 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 $X := \{1\} \cup \langle x \rangle_H$. Then it is clear that, for every $n \geq m-1$, X is the setwise product of n copies of $\{1, x\}$. This shows that the set of lengths of X relative to $\mathcal{P}_{\text{fin},1}(H)$ contains the interval $[\![m-1, \infty]\!]$ (and hence is infinite), since we know from Lemma 2.1.7 that $\{1, x\}$ is an atom of $\mathcal{P}_{\text{fin},1}(H)$.

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 $\sup \mathsf{L}(X) \leq |X|^2$.

(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) Let $n := |X|$ and suppose for a contradiction that there is some $\ell > n^2$ with $\ell \in \mathsf{L}(X)$. There are $A_1, \ldots, A_\ell \in \mathscr{A}(\mathcal{P}_{\text{fin},1}(H))$ with $X = A_1 \cdots A_\ell$. By the Pigeonhole Principle, there is some element $x \in X$ and a subset $I \subseteq [\![1, \ell]\!]$ such that $m := |I| > n$ and $a_i = x$ for each $i \in I$. Writing $I = \{i_1, \ldots, i_m\}$, we have that $x^k = \prod_{j=1}^{k} a_{i_j} \in A_1 \cdots A_\ell = X$. However, since H is torsion-free, each power of x is distinct, so $X \subseteq \{1, x, \ldots, x^m\}$, which is a contradiction since $m > n = |X|$.

(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 $x^m = 1$. If m is even then $(x^{m/2})^2 = 1$, 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 $\langle x \rangle$ 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 (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 so, by Theorem 2.1.9, we have $1 \neq x^2 \neq x$ for all $x \in H \setminus \{1\}$. From here, Lemma 2.1.8(ii) implies H is Dedekind finite, so the 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(iii). □

2.2 Minimal Factorizations and Conditions for Minimal Properties

2.3 Subset Arithmetic in Finite Cyclic Groups

Chapter 3

Power Monoids of Natural Lattices

3.1 Passage to Other 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 of passing between the natural power monoid $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ and other monoids while preserving certain aspects of factorization behavior. In particular, we will discuss the way in which information about factorization can be locally transported between $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ and $\mathcal{P}_{\text{fin},0}(\mathbb{N}^d)$ for $d > 1$, in a sense to be made rigorous in the coming pages.

Definition 3.1.1. 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 the map $f^* : \mathcal{Z}_H(x) \to \mathcal{Z}_K(f(x))$ is a (length-preserving) bijection, where f^* is identified with the restriction to $\mathcal{Z}_H(x)$ of the induced map $f^* : \mathscr{F}^*(\mathscr{A}(H)) \to \mathscr{F}^*(\mathscr{A}(K))$.

Natural Lattice Power Monoids

Lemma 3.1.2. Let $\varphi : G \to H$ be a homomorphism of abelian groups. If there is a subset $W \subseteq G$ 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) φ preserves atoms in W; that is, if $A \subseteq W$ is an atom in $\mathcal{P}_{\text{fin},0}(G)$ then $\varphi(A)$ is an atom in $\mathcal{P}_{\text{fin},0}(H)$.

(iii) There is a length-preserving bijection $\mathcal{Z}_{\mathcal{P}_{\text{fin},0}(G)}(W) \to \mathcal{Z}_{\mathcal{P}_{\text{fin},0}(H)}(\varphi(W))$.

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 $\varphi(A)$.

To see (iii), we define the map $\Phi : \mathcal{Z}(W) \to \mathcal{Z}(\varphi(W))$ as follows: for a factorization $\mathfrak{a} = A_1 * \cdots * A_k \in \mathcal{Z}(W)$, let $\Phi(\mathfrak{a}) = \varphi(A_1) * \cdots * \varphi(A_k)$. By (ii), such a $\Phi(\mathfrak{a})$ is indeed a word in atoms. It is also not too difficult to check that $\pi_{\mathcal{P}_{\text{fin},0}(H)}(\Phi(\mathfrak{a})) = \varphi(W)$, so that Φ is a well-defined map.

Now 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), $\varphi^{-1}(\varphi(A_i)) = A_i$. Thus the map sending $\mathfrak{b} \mapsto \varphi^{-1}(B_1) * \cdots * \varphi^{-1}(B_k)$ is easily checked to be inverse to Φ, which is all we needed to show. □

Remark 3.1.3. Note that the property $(*)$ in Lemma 3.1.2 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 3.1.4. Let $d \geq 1$ and $W \in \mathcal{P}_{\text{fin},0}(\mathbb{N}^{d+1})$. Let $N > 2\max\{\pi_d(w) : w \in W\}$, where $\pi_d : \mathbb{N}^{d+1} \to \mathbb{N}$ is the projection map from the dth coordinate. Define $\varphi : \mathbb{N}^{d+1} \to \mathbb{N}^d$ by $\varphi(w_1, \ldots, w_{d+1}) = (w_1, \ldots, w_{d-1}, w_d + Nw_{d+1})$. 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) There is a length-preserving bijection $\mathcal{Z}_{\mathcal{P}_{\text{fin},0}(\mathbb{N}^{d+1})}(W) \to \mathcal{Z}_{\mathcal{P}_{\text{fin},0}(\mathbb{N}^d)}(\varphi(W))$.

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 $m = \max\{\pi_d(w) : w \in W\}$). Suppose $x, y, z \in W$, writing $x = (x_1, \ldots, x_{d+1})$ and so on. If $x = y+z$, then it is clear that $\varphi(x) = \varphi(y)+\varphi(z)$ by (i). Conversely, if $\varphi(x) = \varphi(y) + \varphi(z)$, then we immediately have $x_i = y_i + z_i$ for all $i < d$. For the dth component, we have

$$x_d + Nx_{d+1} = y_d + Ny_{d+1} + z_d + Nz_{d+1},$$

meaning that $x_d - y_d - z_d = N(y_{d+1} + z_{d+1} - x_{d+1})$. Since $|x_d - y_d - z_d| \leq 2m < N$, it must be that both sides of this last equation are equal to zero, so that $x_d = y_d + z_d$ and $x_{d+1} = y_{d+1} + z_{d+1}$. Now we have $x = y + z$, as we wished.

Finally, (iii) follows from (i) and (ii) by Lemma 3.1.2. □

Theorem 3.1.5. Let $d > 1$. Then $\mathcal{P}_{\mathrm{fin},0}(\mathbb{N}^d)$ is locally transferrable to $\mathcal{P}_{\mathrm{fin},0}(\mathbb{N})$.

Proof. One can prove this by a straightforward induction on d, using Proposition 3.1.4 to resolve both the base case and the inductive step. □

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

Non-Torsion Monoids

As Fan and Tringali prove in [8, Theorem 3.8, Theorem 4.11], all of the factorization information of $\mathcal{P}_{\mathrm{fin},0}(\mathbb{N})$ embeds into *any* non-torsion monoid H. We briefly recall the basic ideas underpinning this fact below.

Proposition 3.1.6. Let H be a non-torsion monoid. Then there is an equimorphism from $\mathcal{P}_{\mathrm{fin},0}(\mathbb{N}) \to \mathcal{P}_{\mathrm{fin},1}(H)$.

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 $f : \mathcal{P}_{\mathrm{fin},0}(\mathbb{N}) \to \mathcal{P}_{\mathrm{fin},1}(\langle x \rangle)$. In turn, this isomorphism induces an isomorphism $f^* : \mathscr{F}(\mathscr{A}(\mathcal{P}_{\mathrm{fin},0}(\mathbb{N}))) \to \mathscr{F}(\mathscr{A}(\mathcal{P}_{\mathrm{fin},1}(\langle x \rangle)))$. As a consequence, for any $X \in \mathcal{P}_{\mathrm{fin},0}(\mathbb{N})$, we have a bijection $f^* : \mathcal{Z}_{\mathcal{P}_{\mathrm{fin},0}(\mathbb{N})}(X) \to \mathcal{Z}_{\mathcal{P}_{\mathrm{fin},1}(\langle x \rangle)}(f(X)) = \mathcal{Z}_{\mathcal{P}_{\mathrm{fin},1}(H)}(f(X))$, where the last inequality follows from Proposition 2.1.2 (ii) (that is, $\mathcal{P}_{\mathrm{fin},1}(\langle x \rangle)$ is divisor-closed in $\mathcal{P}_{\mathrm{fin},1}(H)$). □

Thus the study of factorizations of $\mathcal{P}_{\mathrm{fin},0}(\mathbb{N})$ actually tells us about the factorization of certain subsets of H. Of course, there is much more to be studied in $\mathcal{P}_{\mathrm{fin},1}(H)$ 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 $\mathcal{P}_{\mathrm{fin},0}(\mathbb{N})$ actually occurs in many more power monoids.

Cyclic Groups

Abelian groups are a classical setting for combinatorial sumset problems [CITE SOME PAPERS]. By the Fundamental Theorem of Finitely Generated Abelian Groups, all finitely-generated abelian groups can be constructed as direct sums of cyclic groups, so studying the power monoid of a cyclic group can be motivated by the hope to fully understand sumset arithmetic in all abelian groups.

For any abelian group G, $\mathcal{P}_{\mathrm{fin}}(G) = \mathcal{P}_{\mathrm{fin},\times}(G)$, and we have by [LEMMA ON PRESERVATION OF MINIMAL FACTORIZATIONS IN COMMUTATIVE CASE] that the embedding $\mathcal{P}_{\mathrm{fin},1}(G) \hookrightarrow \mathcal{P}_{\mathrm{fin},\times}(G)$ is an essentially surjective equimorphism. Thus the study of $\mathcal{P}_{\text{fin},1}(G)$ actually encompasses the full study of $\mathcal{P}_{\text{fin}}(G)$.

Section [SECTION REFERENCE HERE] tells us about the factorization theory of $\mathcal{P}_{\text{fin},0}(\mathbb{Z}/n\mathbb{Z})$, establishing a foothold in the study of subset arithmetic of finite cyclic groups. By analogy, we should study $\mathcal{P}_{\text{fin},0}(\mathbb{Z})$ to complete our understanding of cyclic groups. However, a mild reduction allows us to pass to $\mathcal{P}_{\text{fin},0}(\mathbb{N})$: if $X \subseteq \mathbb{Z}$ is a finite subset, then $X - \min(X) \in \mathcal{P}_{\text{fin},0}(\mathbb{N})$, and there is a bijection (using Proposition 2.1.1 (ii)) between $\mathcal{Z}_{\mathcal{P}_{\text{fin},0}(\mathbb{Z})}(X)$ and $\mathcal{Z}_{\mathcal{P}_{\text{fin},0}(\mathbb{Z})}(X - \min(X))$. By Proposition 2.1.2 (ii) (the divisor-closedness of $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ in $\mathcal{P}_{\text{fin},0}(\mathbb{Z})$), the latter is equal to $\mathcal{Z}_{\mathcal{P}_{\text{fin},0}(\mathbb{N})}(X - \min(X))$.

We have seen just above that studying $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ is sufficient for studying the subset arithmetic of $\mathbb{Z}$. In a similar way, we may also justify the passage between $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ and $\mathcal{P}_{\text{fin},0}(\mathbb{N}^d)$, for $d \geq 2$ (at least in a certain local sense), making $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ an appropriate setting for the study of all torsion-free abelian groups.

We will soon see some advantages of working inside of $\mathbb{N}^d$. First, however, we state a general lemma on finding sumset decompositions in abelian groups. Let G be an abelian group and $X \in \mathcal{P}_{\text{fin},0}(G)$. Often, for a given $A \in \mathcal{P}_{\text{fin},0}(G)$, we need to determine whether A divides X; that is, whether there is Y so that $X = A + Y$. Due to the non-cancellative nature of power monoids, there is not a canonical choice for such a Y. In general, there may be many such Y. To partially make up for this, we have the following definition and proposition.

Definition 3.1.7. Let G be an abelian group and $X, A \in \mathcal{P}_{\text{fin},0}(G)$. We define the **cofactor of A in X** by

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

Proposition 3.1.8. Let $X, A \in \mathcal{P}_{\text{fin},0}(\mathbb{N})$.

(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. □

3.2 Independence Arguments in the Lattice

Throughout the rest of this chapter, we will make reference to $\mathbb{N}^d$, where d is to be thought of simply as a sufficiently high ambient dimension. Unless otherwise specified, all subsets involved will be finite subsets of $\mathbb{N}^d$ containing 0 (i.e. elements of $\mathcal{P}_{\text{fin},0}(\mathbb{N}^d)$).

Theorem 3.1.5 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 formulate and exploit a notion of independence of subsets of the lattice $\mathbb{N}^d$.

Definition 3.2.1. Let $d \geq 1$. For a subset $U \subseteq \mathbb{N}^d$, set $\mathbb{Z}U := \operatorname{span}_{\mathbb{Z}}(U) = \{\sum_{i=1}^n c_i u_i : u_1, \dots, u_n \in U, c_1, \dots, c_n \in \mathbb{Z}\}$

We will 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. (Should this be a stronger notion than regular $\mathbb{Z}$-independence of $n > 2$ sets, or is the regular notion useless?)

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 3.2.2. Let $U, U_1, \dots, U_k$ be totally $\mathbb{Z}$-independent subsets of $\mathbb{N}^d$.

(i) For any elements $u_1, \dots, u_n \in U$, if $\sum_i u_i = 0$ then $u_i = 0$ for all $i = 1, \dots, n$.

(ii) For $u_1, v_1 \in U_1, \dots, u_k, v_k \in U_k$, if $\sum_i u_i = \sum_i v_i$ then $u_i = v_i$ for $i = 1, \dots, k$.

Proof. (i) is actually a simple consequence of $\mathbb{N}^d$ being a reduced monoid, and has nothing to do with $\mathbb{Z}$-independence. We include it among results one $\mathbb{Z}$-independence because of the way in which it will be used in our arguments to come.

For (ii), 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 $u_1 - v - 1 = v_2 - u_2 \in \operatorname{span}_{\mathbb{Z}} U_1 \cap \operatorname{span}_{\mathbb{Z}} U_2 = \{0\}$, 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

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

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 3.2.3. 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 3.2.2(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 3.2.2(ii), $\sum_i v_i = 0$, and each $v_i = 0$ by Proposition 3.2.2(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 3.2.4. Let $U, V_1, \ldots, V_m$ 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 $U_j \subset A_{f(j)}$ 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 3.2.3(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 3.2.3(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 3.2.3 (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 3.2.5. If $V_1, \ldots, V_m$ are totally $\mathbb{Z}$-independent then $V_1 + \cdots + V_m$ factors uniquely.

Proof. Let $V = V_1 + \cdots + V_m$. The result will essentially follow from Lemma 3.2.4, taking $U = \{0\}$.

Let $A_1, \ldots, A_k$ be atoms with $V = \sum_i A_i$. As in Lemma 3.2.4(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 3.2.4(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 3.2.3(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 is $V_1 * \cdots * V_m$. □

Example 3.2.6. Theorem 3.2.5 allows us to partially recover [8, Proposition 4.9]. We recall here the content of Fan and Tringali's result: Let $a_1, \ldots, a_\ell \in \mathbb{N}$ such that $a_1 + \cdots + a_i < \frac{1}{2} a_{i+1}$ for $i \in [\![1, \ell - 2]\!]$ and (if $\ell \geq 2$) $a_1 + \cdots + a_{\ell-1} < a_\ell - a_{\ell-1}$. Then $\mathcal{Z}(\{0, a_1\} + \cdots + \{0, a_\ell\}) = \{\{0, a_1\} * \cdots * \{0, a_\ell\}\}$.

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

For $i \in [\![1, \ell]\!]$, let $e_i \in \mathbb{N}^\ell$ be the ith standard basis vector (whose entries are all zero, except for a 1 in the ith coordinate). Let $V = \{0, e_1\} + \cdots + \{0, e_\ell\}$; by Theorem 3.2.5, V factors uniquely. We will follow the procedure given in Theorem 3.1.5 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 3.1.4, φ_i is a homomorphism which essentially preserves the set of factorizations of V_{i+1}. Letting $\varphi := \varphi_1 \circ \cdots \circ \varphi_{\ell-1}$, we have that $U := \varphi(V)$ factors uniquely.

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

3.3 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 3.3.1. 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 3.3.3) 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 3.3.2. Let U_{n+1} be as in Definition 3.3.1, 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 $f \notin \operatorname{span}_{\mathbb{Z}}(\{e_1, \dots, e_{n-1}\} \cup V)$ and the e_n coefficient of g is larger than that of f.

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

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

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

Theorem 3.3.3. Let $n \geq 2$ and let $e_1, \dots, e_n \in \mathbb{N}^n$ be $\mathbb{Z}$-linearly independent. Set $f = \sum_{i=1}^n e_i$, $g = f + e_n$. Letting $U = \sum_{i=1}^n \{0, e_i\} + \{0, g\}$, we have

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

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 $K = \llbracket 1, n \rrbracket$, 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 $I \subsetneqq \llbracket 1, n \rrbracket$, $e_I \in X$ 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 $H \subseteq \llbracket 1, n \rrbracket$ then $g + e_I \in X$ for every $I \subseteq I_X$ with $I \subsetneqq \llbracket 1, n \rrbracket$.

Let $I \subseteq I_X$ with $I \subsetneqq \llbracket 1, n \rrbracket$. 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 $I \neq \llbracket 1, n \rrbracket$, $K \subsetneqq \llbracket 1, n \rrbracket$ 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 $I = \llbracket 1, n-1 \rrbracket$ and $J = K = \llbracket 1, n \rrbracket$ (so $e_J = e_K = f$). However, since $\llbracket 1, n-1 \rrbracket \subseteq I_X$, 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 3.2.5, Y factors uniquely and we have $\{0, e_1\} * \cdots \{0, e_n\} * \{0, g\} \in \mathcal{Z}_{\mathcal{P}_{\text{fin},0}(\mathbb{N}^n)}(U)$.

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

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

We can completely determine the structure of Y. First observe that we cannot have $f = e_{\llbracket 1, n \rrbracket} \in Y$ 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 3.1.8, 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 3.2.5) 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 3.2.5) as the sum of $\{0, g\}$ and the $\{0, e_i\}$ for $i \in I_X$. This can only produce – up to reordering, of course – the factorization $\{0, g\} * \{0, e_1\} * \cdots * \{0, e_n\} \in \mathcal{Z}_{\mathcal{P}_{\text{fin},0}(\mathbb{N}^n)}(U)$.

If $f \in X$, then $X = \left[\{0, g\} + \sum_{i \in I_X} \{0, e_i\}\right] \cup \{f\}$ (and $Y = \{0, e_n\}$ per our considerations in (F3′)). By Lemma 3.3.2, X is an atom, producing the factorization $X * \{0, e_n\} \in \mathcal{Z}_{\mathcal{P}_{\text{fin},0}(\mathbb{N}^n)}(U)$ and completing the proof. □

Remark 3.3.4. In the same vein as Example 3.2.6, one may use Theorem 3.3.3 to recover some cases of [8, Proposition 4.8].

Theorem 3.3.5. 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 definitely belong to $\mathsf{L}(U+V)$.

It is easiest to see that $m+n+1 = \max \mathsf{L}(V) + \max \mathsf{L}(U) = \mathsf{L}(U+V)$. For the rest, suppose $0 \leq h \leq m$. Then, by Lemma 3.3.2,

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

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 $\mathsf{L}(U+V)$. Suppose that $k > m+2$ and that there are atoms $A_1, \ldots, A_k$ with $U + V = A_1 + \cdots + A_k$. By Proposition 3.2.3(iv), we know that $k \leq m+n+1$.

By Proposition 3.2.3(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 3.2.4 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 3.2.4(ii),(iii).

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

Proposition 3.2.3(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 $v \in V$, $U + v = \sum\limits_{i<s} U \cap A_i + (U+v) \cap A_s$.

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 $u = \sum_{i \le s} u_i$, $v_s = v$, and $v_i = 0$ for all $i \ne s$. 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 $\sum_{i \le s} u_i + v \in \sum_{i \le s} A_i \subseteq U + V$, so we can find $u' \in U$ and $v' \in V$ with

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

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

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 $t > 3$. If this were not the case and $t \le 2$, then $k = |[\![1, s]\!] \cup [\![t, k]\!]| \le 2 + |[\![t, k]\!]| \le m + 2$, 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 3 atoms, and U has only one factorization consisting of more than 2 atoms. Say $B_1, \ldots, B_{n+1}$ are the atoms with $U = \sum_{i=1}^{n+1} B_i$. 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

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

and we have proved the claim.

Claim E: A_s is not an atom.

To see this, we compute

$$\begin{aligned}
A_s = (U+V)\cap A_s &= (U+V'+V'')\cap A_s \\
&= (U+V')\cap A_s && \text{(by Claim A and Proposition 3.2.3)} \\
&= \bigcup_{v\in V'} (U+v)\cap A_s \\
&= \bigcup_{v\in V'} (U\cap A_s + v) && \text{(by Claim D)} \\
&= U\cap A_s + V'.
\end{aligned}$$

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 3.2.3(iii). For $i \le s$, since $V\cap A_i = \{0\}$, Proposition 3.2.3(ii) implies that $A_i = (U+V)\cap A_i = U\cap A_i \subseteq U$. Then we have, by Proposition 3.2.3(i), that $U = \sum_{i\le s} U\cap A_i = \sum_{i\le s} A_i$. This means that $s \in \mathsf{L}(U) = \{2, n+1\}$ and, by identical reasoning for V, that $|[\![t,k]\!]| = m$. We conclude that $k \in \{m+2, m+n+1\}$; we assumed that $k > m+2$, so it must be that $k = m+n+1$. □

Chapter 4

Partition Type of Factorizations in the Natural Power Monoid

4.1 Bad Partition Types for Intervals

The length set realization Theorems **??** and 3.3.3 show that some subsets of $\mathbb{N}$ have very well-controlled sets of factorization. On the other hand, there are subsets with comparatively "wild" set of factorizations; the intervals $[\![0, n]\!]$ are a simple class examples which demonstrate this since, for instance, we have $\mathsf{L}([\![0, n]\!]) = [\![2, n]\!]$ [8, Proposition 4.8]. However, observe that any subset X can be obtained by deleting points from the interval $[\![0, \max(X)]\!]$. If X has relatively tame factorization behavior and we imagine this process of deleting points from $[\![0, \max(X)]\!]$, then the subsets between the full interval and X experience a transition between "wild" and "tame" factorization behavior. In what follows, we seek to more rigorously quantify what is meant by "wild" factorization behavior and to investigate the nature of this transition.

Since we will be thinking of elements of $\mathcal{P}_{\text{fin},0}(\mathbb{N})$ as subsets of the intervals $[\![0, n]\!]$, it will be convenient to have some notation to help us filter $\mathbb{N}$.

Definition 4.1.1. For $n \geq 0$, we distinguish the following collections of subsets:

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

In any monoid, we can distinguish different factorizations of an element x by their lengths; that is, we know that if $\mathfrak{a}, \mathfrak{b} \in \mathcal{Z}(x)$ with $|\mathfrak{a}| \neq |\mathfrak{b}|$, then $\mathfrak{a}$ and $\mathfrak{b}$ are not equivalent. In $\mathcal{P}_{\text{fin},0}(\mathbb{N})$, we have some additional leverage which comes from integer partitions; we make some definitions to facilitate this leverage now.

Definition 4.1.2. Let $n \geq 1$. A *partition of* n is $P = (m_1, \dots, m_k)$, where $m_1 \geq \cdots \geq m_k \geq 1$ and $m_1 + \cdots + m_k = n$. Each m_i is said to be a *part* of P, and k is said to be the *length* or number of parts of P. For brevity, we occasionally write $P \vdash n$.

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

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

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 4.1.3. 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.

Proposition 4.1.4. 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 3.1.8. Let $Y = X{:}\{0, c\} = X \cap (X - c)$; we know that $\{0, c\} + Y \subseteq X$, so we just need to show the other inclusion. Suppose $X \supsetneqq \{0, c\} + Y$; then there is $x \in X$ with $x \notin \{0, c\} + Y$.

This means that $x \notin X \cap (X-c)$ and $x \notin X \cap (X-c)$; all together, this means $x+c, x-c \notin X$. However, this contradicts part (i), taking $b = 2c$ and $k = x+c$. Thus we must have $X = \{0,c\} + X{:}\{0,c\}$. □

Proposition 4.1.5. Let $n \geq 1$.

(i) For $n \geq 4$, $\mathscr{Z}^{(n-2,2)}(\llbracket 0,n \rrbracket) = \emptyset$.

(ii) For even $n \geq 4$, $\mathscr{Z}^{(2,\ldots,2)}(\llbracket 0,n \rrbracket) = \emptyset$.

(iii) For odd $n \geq 5$, $\mathscr{Z}^{(3,2,\ldots,2)}(\llbracket 0,n \rrbracket) = \emptyset$.

(iv) For even $n \geq 6$, $\mathscr{Z}^{(4,2,\ldots,2)}(\llbracket 0,n \rrbracket) = \emptyset$.

(v) For odd $n \geq 7$, $\mathscr{Z}^{(5,2,\ldots,2)}(\llbracket 0,n \rrbracket) = \emptyset$.

Proof. For (i), we can use the second part of Lemma 4.1.4 with $c = 1$ to see that there can be no atom A with $A + \{0,2\} = \llbracket 0,n \rrbracket$.

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 $\llbracket 0, 2m+1 \rrbracket$ is to have a factorization of partition type $(3,2,\ldots,2)$, then that factorization must include $\{0,1,3\}$. However, we see that

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

which does not contain $2m = n-1$, so $\llbracket 0, 2m+1 \rrbracket$ 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

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

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

4.2 Good Partition Types for Intervals

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 4.2.1. 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 $h \geq 3$. $\square$

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

Lemma 4.2.2. If $q \geq r \geq 3$ then $[\![0, q + r]\!] \in \mathscr{A}_q + \mathscr{A}_r$; that is, there are atoms $A_q \in \mathscr{A}_q$ and $A'_r \in \mathscr{A}_r$ 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. $\square$

Proposition 4.2.3. 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 4.2.4. For $q \geq 6$ and $t \geq 2$, there is an atom $A \in \mathscr{A}_q$ 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 4.2.5. 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 4.1.5, which says that $D_q + \{0,2\}$ cannot be an interval since D_q is an atom.

Theorem 4.2.6. Let $n \geq 1$ and suppose P is a partition of n with $P \notin \{(n-2,2)\} \cup \{(m,2\dots,2) : 2 \leq m \leq 5\}$. Then $\mathscr{Z}^P(\llbracket 0,n \rrbracket) \neq \emptyset$. In particular, $|\mathsf{T}(\llbracket 0,n \rrbracket)| = p(n)-4$, where $p(n)$ is the number of integer partitions of n.

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

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

Here, Lemma 4.2.4 implies that $\mathscr{Z}^P(\llbracket 0,n \rrbracket) \neq \emptyset$.

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

The content of Lemma 4.2.2 is exactly that $\mathscr{Z}^P(\llbracket 0,n \rrbracket) \neq \emptyset$ for any such partition.

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

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

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

Case 4: P has smallest part equal to 1.

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

If $k=1$, we can see that $C_{n-1} * \{0,1\} \in \mathscr{Z}^P(\llbracket 0,n \rrbracket)$, where C_{n-1} is one of the atoms constructed in Proposition 4.2.1. Similarly, if $k=2$ we have by Lemma 4.2.2 that there are atoms $A \in \mathscr{A}_{m_1}$ and $A' \in \mathscr{A}_{m_2}$ with $A + A' = \llbracket 0, m_1+m_2 \rrbracket$, so $A * A' * \{0,1\} \in \mathscr{Z}^P(\llbracket 0,n \rrbracket)$.

Now assume that $k > 2$ and write $P' = (m_1, \dots, m_k)$. If $m_k = 1$, then there is some $\mathfrak{a}' \in \mathcal{Z}^{P'}(\llbracket 0, n-1 \rrbracket)$ by induction, so that $\mathfrak{a} = \mathfrak{a}' * \{0, 1\} \in \mathcal{Z}^P(\llbracket 0, n \rrbracket)$. However, if $m_k > 1$, set $Q = (m_1, \dots, m_{k-1}, 1)$ (a partition of $n - m_k$). Again, we have by induction that there is some $\mathfrak{b} \in \mathcal{Z}^Q(\llbracket 0, n - m_k \rrbracket)$. 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 $\mathfrak{a} = \mathfrak{b} * \{0, m_k\} \in \mathcal{Z}^P(\llbracket 0, n \rrbracket)$, proving what we wished. □

4.3 Partition Subsums and Near Intervals

We have just seen that intervals of the form $\llbracket 0, n \rrbracket$ 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 4.3.1. Let $m_1, \dots, m_k$ be integers. We will refer to $S = (m_1, \dots, m_k)$ as a *sequence* of integers. Define the **set of subsums of S** to be $\Sigma(S) := \left\{\sum_{i \in I} m_i : I \subseteq \llbracket 1, k \rrbracket\right\}$.

Remark 4.3.2. The notion of "set of subsums" of a sequence can be compared with the similar notion which appears in much of the literature on zero-sum problems in finite abelian groups [CITE SOME PAPERS]. Ours is nearly identical, except for its inclusion of the empty sum. Since we are not focused on the appearance of zero sums, including the empty sum does not put us at any disadvantage in our setting. To the contrary, it is convenient for us as it allows us to express the set of subsums of $S = (m_1, \dots, m_k)$ as a sum in $\mathcal{P}_{\text{fin},0}(\mathbb{Z})$: $\Sigma(S) = \{0, m_1\} + \cdots + \{0, m_k\}$.

Lemma 4.3.3. Let $m_1, \dots, m_k$ 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 $\Sigma(m_1, \dots, m_k) = \llbracket 0, n \rrbracket$.

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 $\ell > \max(\Sigma(T))/2$, $\Sigma(T) = \llbracket 0, \max(\Sigma(T)) \rrbracket$.

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 $T := (m_2, \dots, m_k)$. Now we have $\Sigma(T) = \llbracket 0, n - m_1 \rrbracket$, so $\Sigma(S) = \{0, m_1\} + \llbracket 0, n - m_1 \rrbracket = \llbracket 0, n - m_1 \rrbracket \cup \llbracket m_1, n \rrbracket$. This union of intervals is equal to $\llbracket 0, n \rrbracket$ 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 4.3.4. Let n be even and let P be a partition into $n/2$ parts. Then one of the following holds:

- $\Sigma(P) = [\![0, n]\!]$.
- $\Sigma(P) = [\![0, n]\!]$ 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 4.3.3, $\Sigma(m-2, \ldots, m_k) = [\![0, n - m_1]\!]$.

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 4.3.5. Let $X \in \mathcal{P}_{\mathrm{fin},0}(\mathbb{N})$ 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 $A_i \in \mathscr{A}_{m_i}$ with $\mathfrak{a} = A_1 * \cdots * A_k$. The result is immediate from Lemma 4.3.3, 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 $X \subseteq [\![0, \max(X)]\!] = [\![0, n]\!]$. □

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 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.

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

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

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

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

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

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