

Accepted Manuscript

Power monoids: A bridge between factorization theory and arithmetic combinatorics

Yushuang Fan, Salvatore Tringali

PII: S0021-8693(18)30418-6

DOI: <https://doi.org/10.1016/j.jalgebra.2018.07.010>

Reference: YJABR 16784

To appear in: *Journal of Algebra*

Received date: 15 April 2018

Please cite this article in press as: Y. Fan, S. Tringali, Power monoids: A bridge between factorization theory and arithmetic combinatorics, *J. Algebra* (2018), <https://doi.org/10.1016/j.jalgebra.2018.07.010>

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.



POWER MONOIDS: A BRIDGE BETWEEN FACTORIZATION THEORY AND ARITHMETIC COMBINATORICS

YUSHUANG FAN AND SALVATORE TRINGALI

ABSTRACT. We extend a few fundamental aspects of the classical theory of non-unique factorization, as presented in Geroldinger and Halter-Koch's 2006 monograph on the subject, to a non-commutative and non-cancellative setting, in the same spirit of Baeth and Smertnig's work on the factorization theory of non-commutative, but cancellative monoids [J. Algebra **441** (2015), 475–551]. Then, we bring in power monoids and, applying the abstract machinery developed in the first part, we undertake the study of their arithmetic.

More in particular, let H be a multiplicatively written monoid. The set $\mathcal{P}_{\text{fin}}(H)$ of all non-empty finite subsets of H is naturally made into a monoid, which we call the power monoid of H and is non-cancellative unless H is trivial, by endowing it with the operation $(X, Y) \mapsto \{xy : (x, y) \in X \times Y\}$. Power monoids are, in disguise, one of the primary objects of interest in arithmetic combinatorics, and here for the first time we tackle them from the perspective of factorization theory. Proofs lead to consider various properties of finite subsets of \mathbf{N} that can or cannot be split into a sumset in a non-trivial way, giving rise to a rich interplay with additive number theory.

1. INTRODUCTION

From the classical point of view, factorization theory is all about the study of phenomena arising from the non-uniqueness of factorization in atomic monoids and rings, and the classification of these phenomena by a variety of algebraic, arithmetic, or combinatorial invariants.

The theory grew up out of algebraic number theory and has so far been centered on rings and monoids, where the structures in play are cancellative. The subject has become more and more popular since the publication of Geroldinger and Halter-Koch's 2006 monograph [26], which is entirely devoted to the commutative and cancellative case: A more accurate overview of the field is beyond the scope here, but further information and background can be found in the conference proceedings [3, 11, 8, 9], in the surveys [7, 6, 24], or in the volumes [42, 18].

It is, indeed, the main objective of the present work to extend fundamental aspects of factorization theory to *arbitrary* monoids (in a more systematic way than done in the past) and, as an application, to inquire into the arithmetic properties of a new class of “highly non-cancellative” structures we refer to as power monoids (notations and terminology will be explained later, see, in particular, §§ 2 and 3).

2010 *Mathematics Subject Classification.* Primary 11B13, 11B30, 20M13. Secondary 11P70, 16U30, 20M25.

Key words and phrases. Atoms; catenary degree; equimorphisms; irreducible sets; monoids; non-unique factorization; power monoids; sets of lengths; set of distances; sumsets; transfer techniques.

Y.F. was supported by the National Natural Science Foundation of China (NSFC), Project No. 11401542, and the China Scholarship Council (CSC). S.T. was supported by the Austrian Science Fund (FWF), Project No. M 1900-N39.

Our motivation is twofold. On the one hand, there has been a mounting interest for possible generalizations of factorization theory to monoid-like structures that need no longer be commutative or cancellative [5, 13, 17, 24, 25, 29, 52]. On the other, power monoids are both an effective test bed for these generalizations and, in disguise, one of the primary objects of study in arithmetic combinatorics, a very active area of research, which has undergone tremendous developments in recent years, rapidly expanding from the classical bases of additive number theory [43, 44] (where the focus is on the integers) to much more abstract settings involving non-commutative groups or semigroups [32, 49, 53]: In particular, power monoids can serve as a medium for arithmetic combinatorics to benefit, in the long run, from the interaction with factorization theory, much in the same way as the latter has, in its own right, drawn enormous benefits from the former, see [27, 54] and references therein.

For a basic example of the kind of connections alluded to in the previous paragraph, assume that G is an additively written, finite group. A set $X \subseteq G$ is called *irreducible* if there do not exist $A, B \subseteq G$ with $|A|, |B| \geq 2$ such that X is the sumset of A and B , namely, $X = \{a + b : (a, b) \in X \times Y\}$. This notion is related to deep questions in arithmetic combinatorics, see, e.g., [1, 2, 50, 33, 34]; and it follows from the definitions in § 2.1.1 and points (ii) and (iv) of Proposition 3.2 that a subset of G is irreducible if and only if it is an atom in the power monoid of G .

1.1. Plan of the paper and background. With these ideas in mind, we organize the paper as follows. In § 2, we first extend a few fundamental aspects of the classical theory of non-unique factorization to a non-commutative and non-cancellative setting, in the same spirit of Baeth and Smertnig’s work on the factorization theory of non-commutative, cancellative monoids [5] (see Remarks 2.3–2.20, 2.24, 2.8, and 2.13 for a critical comparison). More specifically, we introduce notions of factorization, distance, and catenary degree, along with a generalization of weak transfer homomorphisms we refer to as equimorphisms, and we prove a number of properties related to these notions: In particular, we establish that equimorphisms preserve factorization lengths and do not increase the catenary degree (Theorem 2.22). Moreover, we give conditions for a unit-cancellative monoid to be atomic (Theorem 2.28) and obtain a characterization of BF-monoids in terms of the existence of a length function (Corollary 2.29), thus improving on analogous results of Smertnig in the cancellative setting [52, Proposition 3.1], and Geroldinger, Kainrath, and the authors in the commutative setting [17, Lemma 3.1(1)].

Then we bring in power monoids (Definition 3.1) and, applying the abstract machinery developed in the former part, undertake the study of their arithmetic. More in detail, let H be a monoid. We denote the power monoid of H by $\mathcal{P}_{\text{fin}}(H)$, and show that $\mathcal{P}_{\text{fin}}(H)$ is a BF-monoid if H is linearly orderable and BF (Proposition 3.5). In addition, we obtain that, if H is a Dedekind-finite, non-torsion monoid, then $\mathcal{P}_{\text{fin}}(H)$ is not equimorphic to a cancellative monoid (in particular, is not a transfer Krull monoid), and that the union of the sets of lengths of $\mathcal{P}_{\text{fin}}(H)$ containing k is $\mathbb{N}_{\geq 2}$ for every integer $k \geq 2$; the set of distances (or delta set) is \mathbb{N}^+ ; and the set of catenary degrees is either $\mathbb{N}^+ \cup \{\infty\}$ or \mathbb{N}^+ , the latter being the case if H is a linearly orderable BF-monoid (Proposition 4.12 and Theorem 4.11, respectively).

It is probably worth stressing that we are talking here of several *different* results, insofar as unions of sets of lengths, sets of distances, and sets of catenary degrees are, in principle, “independent objects”, in the sense that, even in the commutative cancellative setting, none of them can be determined from the knowledge of the other two.

As for the proofs, we use transfer principles (see Remark 2.20 and Theorems 2.22 and 3.8) to reduce the kind of arithmetic properties we are considering to corresponding properties of finite subsets of \mathbf{N} than can or cannot be written as a sumset in a non-trivial way.

Analogous contributions have been made by many authors in the cancellative setting. In particular, it follows by work of Kainrath [38, Theorem 1] that the delta set of a commutative Krull monoid with infinite class group in which every class contains a prime divisor, is equal to \mathbf{N}^+ , see also [24, Theorem 17]. The same is true, by [21, Theorem 9], for the monoid (under multiplication) of integer-valued polynomials with rational coefficients; and more generally, by [22, Corollary 4.1], for the monoid of D -valued polynomials with coefficients in the fraction field of a Dedekind domain D with infinitely many maximal ideals, all of which have finite index.

In a similar vein, Hassler has established that the set of distances of certain commutative Krull monoids with infinite class group (where every class is a sum of a bounded number of classes containing prime divisors) is infinite, see [36, Theorem 1], while Smertnig has proved in [52, Theorem 1.2] that, if H is the multiplicative monoid of the non-zero elements of certain maximal orders in a simple central algebra over a number field, then H is not necessarily a transfer Krull monoid, but the delta set of H is still equal to \mathbf{N}^+ and the union of sets of lengths of H containing k is either $\mathbf{N}_{\geq 2}$ or $\mathbf{N}_{\geq 3}$ for every $k \geq 3$.

On a related note, Geroldinger and Schmid have obtained in [28] that for every non-empty finite set $\Delta \subseteq \mathbf{N}^+$ with $\min \Delta = \gcd \Delta$ there is a finitely generated, commutative Krull monoid whose set of distances is Δ , while Geroldinger and Yuan had previously shown [30, Theorem 1.1] that the delta set of a commutative Krull monoid having prime divisors in all classes is either empty or a (discrete) interval whose minimum is equal to 1. The latter result has been subsequently generalized by Geroldinger and Zhong to certain commutative, seminormal, weakly Krull monoids [31, Theorem 1.1], while a non-commutative analogue was established by Smertnig in [52, Theorem 1.1]. Further contributions to this line of research have been made, among others, by Chapman, Gotti, and Pelayo [12], García-García, Moreno-Frías, and Vigneron-Tenorio [23], and Chapman, García-Sánchez, Llena, Ponomarenko, and Rosales [10].

As for the set of catenary degrees, this was also considered in a couple of recent papers by Fan and Geroldinger [16] and O'Neill, Ponomarenko, Tate, and Webb [46], with the former focused on commutative Krull monoids and the latter on finitely generated, cancellative, commutative monoids.

We conclude the paper with a probably challenging problem that will stimulate, it is our hope, further research in the topic (see § 5 for details).

1.2. Generalities. Unless noted otherwise, we reserve the letters ℓ , m , n , and r (with or without subscripts) for positive integers, and the letters i , j , and k for non-negative integers. We use \mathbf{R} for the reals, \mathbf{Z} for the integers, and \mathbf{N} for the non-negative integers.

A *monoid* is a pair (H, \otimes) consisting of a set H (called the *ground set* of the monoid and systematically identified with it if there is no risk of ambiguity) and an associative (binary) operation $\otimes : H \times H \rightarrow H$ for which there exists a (provably unique) element $e \in H$ (the *identity* of the monoid) such that $e \otimes x = x \otimes e = x$ for all $x \in H$. We assume that monoid homomorphisms preserve the identity, and for $X, Y \subseteq H$ we set $X \otimes Y := \{x \otimes y : (x, y) \in X \times Y\}$. Note also that, if not stated otherwise, we will systematically use multiplicative notation for arbitrary monoids.

Given a set \mathcal{U} , we denote by $\mathcal{F}^*(\mathcal{U})$ the *free monoid with basis \mathcal{U}* . We write $\mathcal{F}^*(\mathcal{U})$ multiplicatively, and we adopt the symbol $*$ for its operation (so, for instance, if $\mathfrak{z} \in \mathcal{F}^*(\mathcal{U})$, then $\mathfrak{z}^2 := \mathfrak{z} * \mathfrak{z}$). We refer to the elements of $\mathcal{F}^*(\mathcal{U})$ as \mathcal{U} -words, and to the identity, $1_{\mathcal{F}^*(\mathcal{U})}$, of $\mathcal{F}^*(\mathcal{U})$ as the empty word.

Let \mathfrak{z} be a \mathcal{U} -word. We set $\|\mathfrak{z}\|_{\mathcal{U}} := 0$ if $\mathfrak{z} = 1_{\mathcal{F}^*(\mathcal{U})}$. Otherwise, there are determined $z_1, \dots, z_n \in \mathcal{U}$ such that $\mathfrak{z} = z_1 * \dots * z_n$. So we take $\|\mathfrak{z}\|_{\mathcal{U}} := n$, and we define $\mathfrak{z}z_n^{-1} := z_1^{-1}\mathfrak{z} := 1_{\mathcal{F}^*(\mathcal{U})}$ if $n = 1$, and $\mathfrak{z}z_n^{-1} := z_1 * \dots * z_{n-1}$ and $z_1^{-1}\mathfrak{z} := z_2 * \dots * z_n$ if $n \geq 2$. In both cases, we call $\|\mathfrak{z}\|_{\mathcal{U}}$ the (word) length of \mathfrak{z} (relative to \mathcal{U}). It is clear that $\|\mathfrak{z}_1 * \mathfrak{z}_2\|_{\mathcal{U}} = \|\mathfrak{z}_1\|_{\mathcal{U}} + \|\mathfrak{z}_2\|_{\mathcal{U}}$ for all $\mathfrak{z}_1, \mathfrak{z}_2 \in \mathcal{F}^*(\mathcal{U})$.

If $a, b \in \mathbf{R} \cup \{\pm\infty\}$, we let $\llbracket a, b \rrbracket := \{x \in \mathbf{Z} : a \leq x \leq b\}$ stand for the (discrete) interval between a and b . If $\lambda \in \mathbf{R}$ and $X, Y \subseteq \mathbf{R}$, we denote by X^+ the positive part of X (so, \mathbf{N}^+ is the set of positive integers), and we define the sumset of X and Y by $X + Y := \{x + y : (x, y) \in X \times Y\}$, the n -fold sumset of X by $nX := \{x_1 + \dots + x_n : x_1, \dots, x_n \in X\}$, and the λ -dilation of X by $\lambda \cdot X := \{\lambda x : x \in X\}$.

If X, Y , and Z are sets and \mathcal{C} is an equivalence (relation) on X , we denote by $\mathcal{P}(X)$ the power set of X and by $\llbracket x \rrbracket_{\mathcal{C}}$ the (equivalence) class of a fixed element $x \in X$ in the quotient X/\mathcal{C} , and we write $X = Y \uplus Z$ to mean that $Y \cap Z = \emptyset$ and $X = Y \cup Z$.

We say that a finite sequence x_1, \dots, x_n is the natural enumeration of a non-empty set $X \subseteq \mathbf{R}$ if $X = \{x_1, \dots, x_n\}$ and $x_i < x_{i+1}$ for every $i \in \llbracket 1, n-1 \rrbracket$. Lastly, we assume $\sup(\emptyset) := 0$ and $\inf(\emptyset) := \infty$, and we let \mathfrak{S}_n be the group of permutations of $\llbracket 1, n \rrbracket$.

Further notations and terminology, if not explained, are standard or should be clear from the context.

2. FACTORIZATION THEORY

In this section, we fix some definitions that are at the center of our interest, and we prove some fundamental results that will be used later (in §§ 3 and 4) to investigate the structure of power monoids.

2.1. Basic definitions and arithmetic invariants. Throughout, we let H be a (multiplicatively written) monoid with identity 1_H , and we denote by H^\times the *set of units* (or *invertible elements*) of H .

Note that H need not have any special property (e.g., commutativity), unless a statement to the contrary is made. Also, we will systematically drop the subscript ‘ H ’ from the notations we are going to introduce whenever H is implied from the context and there is no risk of ambiguity.

We say that H is *reduced* if $H^\times = \{1_H\}$; *cancellative* if $xz = yz$ or $zx = zy$, for some $x, y, z \in H$, implies $x = y$; *Dedekind-finite* if $xy = 1_H$ yields $yx = 1_H$; *unit-cancellative* (respectively, *strongly unit-cancellative*) provided that $xy = x$ or $yx = x$ only if $y \in H^\times$ (respectively, $y = 1_H$); *divisible* if, for all $n \in \mathbf{N}^+$ and $x \in H$, there exists $y \in H$ with $x = y^n$; and *non-torsion* if $\text{ord}_H(x) = \infty$ for some $x \in H$, where $\text{ord}_H(x)$ is the *order* of x (in H), i.e., the cardinality of the set $\{x^n : n \in \mathbf{N}^+\}$.

Remark 2.1. Factorization in unit-cancellative monoids is the subject of recent work by Geroldinger, Kainrath, and the authors in the commutative and finitely generated case [17], and by Geroldinger and Schwab in the finitely presented case [29]. In turn, Dedekind-finite monoids, sometimes also referred to as directly finite, weakly 1-finite, inverse symmetric, or von Neumann-finite monoids, form a fairly large class, which includes, among many others, the multiplicative monoid of Artinian or Noetherian rings [14, Proposition 4.6.6 and Theorem 4.6.7(iii)], algebraic algebras over a field [39, Exercise 1.13], right and left self-injective rings [15, Corollary 1.1], and the group ring of a (possibly non-abelian or infinite) group

over a field of characteristic zero [15, Theorem 2.3], not to mention trivial examples such as commutative or cancellative monoids (and submonoids, direct products, and direct limits of Dedekind-finite monoids).

Both unit-cancellative and Dedekind-finite monoids play a central role in the present paper, though most of the basic definitions and results are worked out in greater generality at no additional cost. Of course, all cancellative monoids are strongly unit-cancellative, and the latter are unit-cancellative: What is slightly less obvious is that unit-cancellative monoids are Dedekind-finite (Proposition 2.30).

Given $x, y \in H$, we write $x \mid_H y$ if $uxv = y$ for some $u, v \in H$, cf. [5, Definition 5.2(1)]. Moreover, we use $x \simeq_H y$, and we say that x is *associate* to y , if $y \in H^\times x H^\times$. Lastly, we take a submonoid M of H to be *divisor-closed* if $x \in M$ whenever $x \mid_H y$ and $y \in M$.

2.1.1. Atoms and lengths. We let $\mathcal{A}(H)$ stand for the *set of atoms* (or *irreducible elements*) of H , where $a \in H$ is an atom if $a \notin H^\times$ and there do not exist $x, y \in H \setminus H^\times$ such that $a = xy$ (note that, in general, the product of two non-units can be a unit, so the first condition does not follow from the second, cf. Lemma 2.27(i) and Proposition 2.30).

We set, for every $x \in H$, $\mathsf{L}_H(x) := \{k \in \mathbb{N}^+ : x = a_1 \cdots a_k \text{ for some } a_1, \dots, a_k \in \mathcal{A}(H)\}$ if $x \neq 1_H$, and $\mathsf{L}_H(x) := \{0\} \subseteq \mathbb{N}$ otherwise: We call an element of $\mathsf{L}_H(x)$ a (*factorization*) *length* of x , and $\mathsf{L}_H(x)$ the *set of lengths* of x . Consequently, we say that H is *atomic* (respectively, a *BF-monoid*) if $\mathsf{L}_H(x)$ is non-empty (respectively, non-empty and finite) for all $x \in H \setminus H^\times$.

Lemma 2.2. *Let H be a monoid. The following hold:*

- (i) *If $u, v \in H^\times$, then $uv \in H^\times$. Moreover, the converse is true if $H = H^\times$ or $\mathcal{A}(H) \neq \emptyset$.*
- (ii) *If $a \in \mathcal{A}(H)$ and $u \in H^\times$, then $ua, au \in \mathcal{A}(H)$.*
- (iii) *$\mathsf{L}_H(u) = \emptyset$ for every $u \in H^\times \setminus \{1_H\}$.*
- (iv) *$\mathsf{L}_H(x) = \mathsf{L}_H(uxv)$ for all $x \in H \setminus H^\times$ and $u, v \in H^\times$.*

Proof. (i) The first part is trivial and well known; in particular, if $u, v \in H^\times$, then uv is invertible and $(uv)^{-1} = v^{-1}u^{-1}$. As for the converse, the claim is obvious if $H = H^\times$. Otherwise, pick $a \in \mathcal{A}(H)$ and suppose for a contradiction that there are $x, y \in H$ such that $xy \in H^\times$, but $x \notin H^\times$ or $y \notin H^\times$. We can assume (by symmetry) that $x \notin H^\times$. Then $xyz = 1_H$ for some $z \in H$, which yields $a = x(yza)$. So yza must be a unit, since x is not and a is an atom. In particular, $yzav = 1_H$ for some $v \in H$. This shows that yz is both left- and right-invertible, hence is invertible. It follows $x = (yz)^{-1} \in H^\times$, a contradiction.

(ii) Let $a \in \mathcal{A}(H)$ and $u \in H^\times$. We will prove that au is an atom (the other case is similar). Indeed, au is not a unit: Otherwise, $a = vu^{-1}$ for some $v \in H^\times$, which would imply, say, by point (i) that $a \in H^\times$, a contradiction. Moreover, if $au = xy$ for some $x, y \in H$, then $a = x(yu^{-1})$. So, using that a is an atom, we have $x \in H^\times$, or $yu^{-1} = v$ for some $v \in H^\times$ (and hence $y = vu \in H^\times$). To wit, $au \in \mathcal{A}(H)$.

(iii) It is evident that, if $\mathcal{A}(H)$ is empty, then so is $\mathsf{L}_H(x)$ for every $x \in H \setminus \{1_H\}$, and we are done. Otherwise, we get from point (i) that the units of H cannot be factored into a non-empty product of atoms of H , and consequently $\mathsf{L}_H(u) = \emptyset$ for every $u \in H^\times \setminus \{1_H\}$.

(iv) Let $x \in H \setminus H^\times$ and $u, v \in H^\times$. Since $x = u^{-1}(uxv)v^{-1}$, it is sufficient to prove that $\mathsf{L}_H(x) \subseteq \mathsf{L}_H(uxv)$. If $\mathsf{L}_H(x)$ is empty, this is obvious. Otherwise, pick $k \in \mathsf{L}_H(x)$. Then $k \geq 1$ (because $x \neq 1_H$), and there exist $a_1, \dots, a_k \in \mathcal{A}(H)$ such that $x = a_1 \cdots a_k$. It follows $uxv = b_1 \cdots b_k$, with $b_i := ua_iu^{-1}$ for $i \in [1, k-1]$ and $b_k := ua_kv$. So we conclude from (ii) that $k \in \mathsf{L}_H(uxv)$, and we are done. ■

Remark 2.3. It is perhaps worth noting that $0 \in \mathsf{L}_H(x)$ for some $x \in H$ only if $x = 1_H$, in contrast to the standard convention that the set of lengths of *any* unit of H is equal to $\{0\}$. As a matter of fact, we disagree with this convention, since it looks no longer fit for the non-commutative setting (cf. Remark 2.6), and all the more in the light of Lemma 2.2(iii).

Remark 2.4. By Lemma 2.2(iii), 1_H cannot be expressed as a non-empty product of atoms of H . This yields that, for all $x, y \in H$, $\mathsf{L}_H(x) + \mathsf{L}_H(y) \subseteq \mathsf{L}_H(xy)$ and $\sup \mathsf{L}_H(x) + \sup \mathsf{L}_H(y) \leq \sup \mathsf{L}_H(xy)$.

We let $\mathcal{L}(H) := \{\mathsf{L}_H(x) : x \in H\} \setminus \{\emptyset\} \subseteq \mathcal{P}(\mathbf{N})$. We refer to $\mathcal{L}(H)$ as the *system of sets of lengths* of H . Then, for each $k \in \mathbf{N}$ we denote by $\mathcal{U}_k(H)$ the union of all $L \in \mathcal{L}(H)$ with $k \in L$. It is clear that $\mathcal{U}_0(H) = \{0\}$; and if $\mathcal{A}(H)$ is non-empty then $\mathcal{U}_1(H) = \{1\}$ and $k \in \mathcal{U}_k(H)$ for all $k \in \mathbf{N}$, otherwise $\mathcal{U}_1(H) = \mathcal{U}_2(H) = \dots = \emptyset$.

We take $\Delta(H) := \bigcup_{L \in \mathcal{L}(H)} \Delta(L)$, where for $L \subseteq \mathbf{Z}$ we let $\Delta(L)$ be the set of all $d \in \mathbf{N}^+$ such that $L \cap \llbracket l, l+d \rrbracket = \{l, l+d\}$ for some $l \in L$. We call $\Delta(H)$ the *set of distances* (or *delta set*) of H .

Sets of lengths, along with a number of invariants derived from them (e.g., unions of sets of lengths and sets of distances), are by and large the best tools so far available to describe the arithmetic of BF-monoids, see [24] for further discussion on this point.

2.1.2. Factorizations. We let π_H be the unique monoid homomorphism $\mathcal{F}^*(H) \rightarrow H$ such that $\pi_H(x) = x$ for all $x \in H$, and \mathcal{C}_H the smallest monoid congruence on $\mathcal{F}^*(\mathcal{A}(H))$ for which the following holds:

- If $\mathbf{a} = a_1 * \dots * a_m$ and $\mathbf{b} = b_1 * \dots * b_n$ are, respectively, non-empty $\mathcal{A}(H)$ -words of length m and n , then $(\mathbf{a}, \mathbf{b}) \in \mathcal{C}_H$ if and only if $\pi_H(\mathbf{a}) = \pi_H(\mathbf{b})$, $m = n$, and $a_1 \simeq_H b_{\sigma(1)}, \dots, a_n \simeq_H b_{\sigma(n)}$ for some permutation $\sigma \in \mathfrak{S}_n$.

We call π_H the *factorization homomorphism* of H , and the quotient $\mathsf{Z}(H) := \mathcal{F}^*(\mathcal{A}(H)) / \mathcal{C}_H$ the *factorization monoid* of H . We continue denoting the operation of $\mathsf{Z}(H)$ by the same symbol as the operation of $\mathcal{F}^*(\mathcal{A}(H))$, and we observe that, if H is a reduced commutative monoid and $\mathbf{a} = a_1 * \dots * a_n$ is a non-empty $\mathcal{A}(H)$ -word of length n , then

$$\llbracket \mathbf{a} \rrbracket_{\mathcal{C}_H} = \{a_{\sigma(1)} * \dots * a_{\sigma(n)} : \sigma \in \mathfrak{S}_n\}.$$

Accordingly, we abuse notation and identify $\llbracket \mathbf{a} \rrbracket_{\mathcal{C}_H}$ with \mathbf{a} whenever H is commutative and $H^\times = \{1_H\}$.

Also, we notice that $\pi_H(\mathcal{A}) = \{\pi_H(\mathbf{a})\}$ for all $\mathcal{A} \in \mathsf{Z}(H)$ and $\mathbf{a} \in \mathcal{A}$, and we define, for every $x \in H$,

$$\mathsf{Z}_H(x) := \{\llbracket \mathbf{a} \rrbracket_{\mathcal{C}_H} : \mathbf{a} \in \mathcal{F}^*(\mathcal{A}(H)) \text{ and } \pi_H(\mathbf{a}) = x\} \subseteq \mathsf{Z}(H)$$

and

$$\mathsf{Z}_H(x) := \pi_H^{-1}(x) \cap \mathcal{F}^*(\mathcal{A}(H)) = \bigcup \mathsf{Z}_H(x) \subseteq \mathcal{F}^*(\mathcal{A}(H)).$$

From here it is easy to see that

$$\mathsf{L}_H(x) = \{\llbracket \mathbf{a} \rrbracket_H : \mathbf{a} \in \mathsf{Z}_H(x)\}, \text{ for all } x \in H. \quad (1)$$

We refer to the elements of $\mathsf{Z}_H(x)$ as the *factorization classes* of x , and to the $\mathcal{A}(H)$ -words in $\mathsf{Z}_H(x)$ as the *factorizations* of x . Then we have the following:

Lemma 2.5. *Let H be a monoid, and pick $x \in H \setminus \mathcal{A}(H)$ such that $x \neq 1_H$. Then*

$$\mathcal{Z}_H(x) = \bigcup_{y,z \in H \setminus H^\times : x=yz} \{\mathbf{a} * \mathbf{b} : (\mathbf{a}, \mathbf{b}) \in \mathcal{Z}_H(y) \times \mathcal{Z}_H(z)\}. \quad (2)$$

Proof. Let $\mathcal{Z}'_H(x)$ denote the set on the right-hand side of equation (2). It is clear that $\mathcal{Z}'_H(x) \subseteq \mathcal{Z}_H(x)$. As for the opposite inclusion, this is obvious if $\mathcal{Z}_H(x) = \emptyset$. Otherwise, $\mathcal{Z}_H(x)$ is a non-empty subset of $\mathcal{F}^*(\mathcal{A}(H)) \setminus \{1_{\mathcal{F}^*(\mathcal{A}(H))}\}$. Accordingly, let $\mathbf{a} := a_1 * \cdots * a_n \in \mathcal{Z}_H(x)$. Then $n \geq 2$ (since x is not an atom), and hence $\mathbf{a} = \mathbf{b} * \mathbf{c}$, where $\mathbf{b} := a_1 * \cdots * a_{n-1}$ and $\mathbf{c} := a_n$ are non-empty $\mathcal{A}(H)$ -words. But this implies $\mathbf{a} \in \mathcal{Z}'_H(x)$, because it is evident from the above that $\mathcal{A}(H)$ is non-empty, and therefore $y := \pi_H(\mathbf{b})$ and $z := \pi_H(\mathbf{c})$ are non-units of H , by Lemma 2.2(i). ■

Now we take a break for some highlights, to put things in perspective and contrast our approach to the study of the arithmetic of monoids with what has been done so far in the existing body of literature.

Remark 2.6. Our definition of the factorization monoid $\mathcal{Z}(H)$ is, in general, inconsistent with analogous definitions from the literature on factorization theory, and it is probably useful to explain why this inconsistency is not necessarily bad.

Our terms for comparison will be the classical definition of the factorization monoid (for the case when H is commutative and cancellative) and Smertnig's definition of the monoid of rigid factorizations (for cancellative monoids), for which we use, respectively, the notation $\mathcal{Z}_{\text{GeH}}(H)$ and $\mathcal{Z}_{\text{Sm}}(H)$, and we refer, respectively, to [26, Definition 1.2.6] and [52, § 3] (see also Remarks 2.7 and § 2.1.3).

To start with, it is worth stressing that a “full comparison” between $\mathcal{Z}_{\text{GeH}}(H)$ and $\mathcal{Z}(H)$, whatever it may mean, is just impossible. Not only because $\mathcal{Z}_{\text{GeH}}(H)$ is not defined for non-commutative monoids (cancellativity has no active role in this regard, see [17, § 3]), but also, and more importantly, because there seems to be no meaningful way to carry over the definition of $\mathcal{Z}_{\text{GeH}}(H)$ to a non-commutative setting: $\mathcal{Z}_{\text{GeH}}(H)$ is the free *abelian* monoid with basis $\mathcal{A}(H_{\text{red}})$, where H_{red} is the quotient H/H^\times . Thus, a naive attempt to generalize the classical definition to the case when H may not be commutative, would be to take the quotient of H by the monoid congruence \mathcal{C}_{red} generated by the relation \simeq_H and to let the factorization monoid of H equal to $\mathcal{F}^*(\mathcal{A}(H/\mathcal{C}_{\text{red}}))$. But this approach has a major drawback: If H is commutative, then \mathcal{C}_{red} and \simeq_H coincide. Otherwise, \simeq_H need not be a congruence and \mathcal{C}_{red} can be “much larger” than \simeq_H , with the result that $H/\mathcal{C}_{\text{red}}$ is “too small” for carrying any interesting information about the arithmetic of H (cf. [52, Remarks 3.3.1]).

In a similar vein, a full comparison between $\mathcal{Z}_{\text{Sm}}(H)$ and $\mathcal{Z}(H)$ is also unfeasible, since the definition of $\mathcal{Z}_{\text{Sm}}(H)$ is phrased in the language of categories, while the present paper is entirely focused on monoids (though a large part of this section can be abstracted to the level of categories without much trouble).

So, we have no choice but to restrict the comparison between $\mathcal{Z}_{\text{GeH}}(H)$ and $\mathcal{Z}(H)$ to the commutative setting, and the comparison between $\mathcal{Z}_{\text{Sm}}(H)$ and $\mathcal{Z}(H)$ to the case when the former is specialized to monoids (no further comment will be made on this point in the sequel).

Round 1: $\mathcal{Z}_{\text{GeH}}(H)$ vs $\mathcal{Z}(H)$. Assume that H is commutative, and denote by \mathcal{C}'_H the smallest monoid congruence on $\mathcal{F}^*(\mathcal{A}(H))$ for which the following holds:

- If $\mathbf{a} = a_1 * \cdots * a_m$ and $\mathbf{b} = b_1 * \cdots * b_n$ are, respectively, non-empty $\mathcal{A}(H)$ -words of length m and n , then $(\mathbf{a}, \mathbf{b}) \in \mathcal{C}'_H$ if and only if $m = n$ and $a_1 \simeq_H b_{\sigma(1)}, \dots, a_n \simeq_H b_{\sigma(n)}$ for some $\sigma \in \mathfrak{S}_n$.

It is readily checked that $Z_{\text{GeH}}(H)$ is isomorphic (as a monoid) to the quotient $Z'_{\text{GeH}}(H) := \mathcal{F}^*(\mathcal{A}(H))/\mathcal{C}'_H$. Therefore, rather than comparing $Z(H)$ with $Z_{\text{GeH}}(H)$, we may compare the former with $Z'_{\text{GeH}}(H)$, which has practical advantages.

In particular, there is a unique homomorphism $\pi_{\text{GeH}} : Z'_{\text{GeH}}(H) \rightarrow H_{\text{red}}$ such that $\pi_{\text{GeH}}(\llbracket a \rrbracket_{\mathcal{C}'_H}) = aH^\times$ for all $a \in \mathcal{A}(H)$, and for every $x \in H$ we can identify the elements of the set

$$Z'_{\text{GeH}}(x) := \pi_{\text{GeH}}^{-1}(xH^\times) \subseteq Z'_{\text{GeH}}(H)$$

with the factorizations of x in the sense of [26, Definition 1.2.6]. So, taking

$$Z'_{\text{GeH}}(x) := \bigcup Z_{\text{GeH}}(x) \subseteq \mathcal{F}^*(\mathcal{A}(H))$$

and calling the $\mathcal{A}(H)$ -words in $Z'_{\text{GeH}}(x)$ the *classical factorizations* of x , we end up with the conclusion that, in the multiplicative monoid of the ring of integers, the $\mathcal{A}(\mathbf{P})$ -words $2 * (-3)$ and $2 * 3$, where \mathbf{P} is the set of rational primes, are both classical factorizations of 6. Of course, there is nothing wrong or paradoxical with this inference (it is just the consequence of some definitions), though we do not find it very natural and nothing similar happens with our definitions.

Indeed, $Z_H(1_H) = Z'_{\text{GeH}}(x) = \{1_{\mathcal{F}^*(\mathcal{A}(H))}\}$ for $x \in H^\times$, and $Z_H(x) = \emptyset$ for $x \in H^\times \setminus \{1_H\}$. Also, if $\mathbf{a} = a_1 * \dots * a_n$ is a non-empty $\mathcal{A}(H)$ -word of length n and $x = \pi_H(\mathbf{a})$, then

$$\llbracket \mathbf{a} \rrbracket_{\mathcal{C}_H} = \{(a_{\sigma(1)}u_1) * \dots * (a_{\sigma(n)}u_n) : \sigma \in \mathfrak{S}_n, u_1, \dots, u_n \in H^\times, \text{ and } u_1 \dots u_n x = x\} \quad (3)$$

and

$$\llbracket \mathbf{a} \rrbracket_{\mathcal{C}'_H} = \{(a_{\sigma(1)}u_1) * \dots * (a_{\sigma(n)}u_n) : \sigma \in \mathfrak{S}_n \text{ and } u_1, \dots, u_n \in H^\times\}.$$

It follows that $\llbracket \mathbf{a} \rrbracket_{\mathcal{C}_H} \subseteq \llbracket \mathbf{a} \rrbracket_{\mathcal{C}'_H}$, and the inclusion is strict if, for instance, H is strongly unit-cancellative, but not reduced. The point is simply that $\mathcal{C}_H \subseteq \mathcal{C}'_H$, and in general we do not have equality.

In other terms, $Z'_{\text{GeH}}(H)$ is “coarser” than $Z(H)$, in the sense that the former embeds (as a monoid) into the latter, but the embedding is an isomorphism if and only if H is reduced.

Round 2: $Z_{\text{Sm}}(H)$ vs $Z(H)$. In the case of monoids, Smertnig’s definition of $Z_{\text{Sm}}(H)$ comes down to the following: Denote by \circ the binary operation on the set $\mathcal{F}_{\text{Sm}}(H) := H^\times \times \mathcal{F}^*(\mathcal{A}(H))$ given by

$$((u, \mathbf{a}), (v, \mathbf{b})) \mapsto \begin{cases} (u, \mathbf{a}a_n^{-1} * (a_n v) * \mathbf{b}) & \text{if } n := \|\mathbf{a}\|_H \geq 1 \text{ and } \mathbf{a} = a_1 * \dots * a_n, \\ (uv, \mathbf{b}) & \text{otherwise} \end{cases},$$

which is well defined by Lemma 2.2(ii) (Smertnig’s original definition is restricted to the cancellative setting, where the well-definedness of \circ is trivial). Note that the pair $(\mathcal{F}_{\text{Sm}}(H), \circ)$ is a monoid. Accordingly, let \mathcal{C}_{Sm} be the smallest monoid congruence on $(\mathcal{F}_{\text{Sm}}(H), \circ)$ determined by the following:

- If $u, v \in H^\times$, and $\mathbf{a} = a_1 * \dots * a_m$ and $\mathbf{b} = b_1 * \dots * b_n$ are, respectively, non-empty $\mathcal{A}(H)$ -words of length m and n , then $((u, \mathbf{a}), (v, \mathbf{b})) \in \mathcal{C}_{\text{Sm}}$ if and only if $u\pi_H(\mathbf{a}) = v\pi_H(\mathbf{b})$, $m = n$, and there exist $\varepsilon_1, \dots, \varepsilon_n \in H^\times$ with $\varepsilon_n = 1_H$, $ua_1 = vb_1\varepsilon_1^{-1}$, and $a_i = \varepsilon_{i-1}b_i\varepsilon_i^{-1}$ for $i \in \llbracket 2, n \rrbracket$.

In fact, $Z_{\text{Sm}}(H)$ is the quotient of $(\mathcal{F}_{\text{Sm}}(H), \circ)$ by the congruence \mathcal{C}_{Sm} . In particular, if H is reduced, then $Z_{\text{Sm}}(H) \cong \mathcal{F}^*(\mathcal{A}(H))$. So, contrary to what happens with $Z(H)$, $Z_{\text{Sm}}(H)$ is not even isomorphic to $Z_{\text{GeH}}(H)$ when H is reduced and commutative, cf. [5, p. 492]. Nevertheless, there are strong similarities between the constructions of $Z_{\text{Sm}}(H)$ and $Z(H)$, which will be further clarified by Remark 2.7.

First, both constructions involve, through the definition of the congruences \mathcal{C}_{Sm} and \mathcal{C}_H , a condition (in terms of the homomorphism π_H) that rules out the “issues” pointed out in the above in reference to the classical factorizations in the commutative setting.

Secondly, both agree on the role of $\mathcal{F}^*(\mathcal{A}(H))$ and the idea that factorizations, whatever they may be, are related to the quotient of $\mathcal{F}^*(\mathcal{A}(H))$, or something as close to $\mathcal{F}^*(\mathcal{A}(H))$ as $\mathcal{F}_{\text{Sm}}(H)$, by a suitable congruence. But while $\mathbf{Z}_{\text{Sm}}(H)$ brings in “the H^\times factor (...) to represent trivial factorizations of units” (to quote Smertnig’s own words from [52, Remark 3.3.1]), we brush off the trivial factorizations of a unit $u \neq 1_H$ from our approach: This leads to a simplification of the theory, without causing any significant loss (cf. Remarks 2.3 and 2.4).

Remark 2.7. The factorization monoid $\mathbf{Z}(H)$ is *essentially* the same as Baeth and Smertnig’s monoid, $\mathbf{Z}_p(H)$, of permutable factorizations: This may not be immediately apparent, but it follows from Lemma 2.2(ii) and a careful reading of [5, Construction 3.3(2), Definitions 3.4(2) and 3.8(2), and Remark 3.9(2)]. In the notations and terminology of Remark 2.6, $\mathbf{Z}_p(H)$ is, in fact, the quotient of $\mathbf{Z}_{\text{Sm}}(H)$ by the smallest monoid congruence \sim_p on $\mathbf{Z}_{\text{Sm}}(H)$ for which the following holds:

- If $u, v \in H^\times$, and $\mathbf{a} = a_1 * \dots * a_m$ and $\mathbf{b} = b_1 * \dots * b_n$ are non-empty $\mathcal{A}(H)$ -words of length m and n , respectively, then $\llbracket (u, \mathbf{a}) \rrbracket_{\mathcal{C}_{\text{Sm}}} \sim_p \llbracket (v, \mathbf{b}) \rrbracket_{\mathcal{C}_{\text{Sm}}}$ if and only if $u\pi_H(\mathbf{a}) = v\pi_H(\mathbf{b})$, $m = n$, and there exists $\sigma \in \mathfrak{S}_n$ such that $a_i \simeq_H b_{\sigma(i)}$ for all $i \in \llbracket 1, n \rrbracket$.

Consequently, $\mathbf{Z}(H)$ is monoid isomorphic to $\mathbf{Z}_p(H) \setminus \mathcal{C}$, where \mathcal{C} is the set of all congruence classes in $\mathbf{Z}_p(H)$ corresponding to a rigid factorization of the form $\llbracket (u, 1_{\mathcal{F}^*(\mathcal{A}(H))}) \rrbracket_{\mathcal{C}_{\text{Sm}}}$ with $u \in H^\times \setminus \{1_H\}$. In particular, we have a monoid isomorphism between $\mathbf{Z}(H)$ and $\mathbf{Z}_p(H)$ if and only if H is reduced.

2.1.3. Distances and catenary degree. Let \mathbf{d} be a function $\mathcal{F}^*(\mathcal{A}(H)) \times \mathcal{F}^*(\mathcal{A}(H)) \rightarrow \mathbf{R}$. We say that \mathbf{d} is a (*global*) *distance* (on H) if, for all $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathcal{F}^*(\mathcal{A}(H))$, the following hold:

- (D1) $\mathbf{d}(\mathbf{a}, \mathbf{b}) = 0$ whenever $(\mathbf{a}, \mathbf{b}) \in \mathcal{C}_H$.
- (D2) $\mathbf{d}(\mathbf{a}, \mathbf{b}) = \mathbf{d}(\mathbf{b}, \mathbf{a})$.
- (D3) $\mathbf{d}(\mathbf{a}, \mathbf{b}) \leq \mathbf{d}(\mathbf{a}, \mathbf{c}) + \mathbf{d}(\mathbf{c}, \mathbf{b})$.
- (D4) $|\|\mathbf{a}\|_H - \|\mathbf{b}\|_H| \leq \mathbf{d}(\mathbf{a}, \mathbf{b}) \leq \max(\|\mathbf{a}\|_H, \|\mathbf{b}\|_H)$.

We refer to \mathbf{d} as a \mathcal{C}_H -*metric* if it is a distance and, in addition, $\mathbf{d}(\mathbf{a}, \mathbf{b}) = 0$ for some $\mathbf{a}, \mathbf{b} \in \mathcal{F}^*(\mathcal{A}(H))$ implies $(\mathbf{a}, \mathbf{b}) \in \mathcal{C}_H$. Moreover, we call \mathbf{d} *subinvariant* (on H) if we have:

- (D5) $\mathbf{d}(\mathbf{c} * \mathbf{a} * \mathbf{d}, \mathbf{c} * \mathbf{b} * \mathbf{d}) \leq \mathbf{d}(\mathbf{a}, \mathbf{b})$ for all $\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d} \in \mathcal{F}^*(\mathcal{A}(H))$.

In a similar vein, we say that \mathbf{d} is *invariant* (on H) if (D5) holds with equality, namely:

- (D6) $\mathbf{d}(\mathbf{c} * \mathbf{a} * \mathbf{d}, \mathbf{c} * \mathbf{b} * \mathbf{d}) = \mathbf{d}(\mathbf{a}, \mathbf{b})$ for all $\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d} \in \mathcal{F}^*(\mathcal{A}(H))$.

Lastly, we take \mathbf{d} to be *locally invariant* (on H) if it is subinvariant and

- (D7) $\mathbf{d}(\mathbf{c} * \mathbf{a} * \mathbf{d}, \mathbf{c} * \mathbf{b} * \mathbf{d}) = \mathbf{d}(\mathbf{a}, \mathbf{b})$ for all $\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d} \in \mathcal{F}^*(\mathcal{A}(H))$ with $\pi_H(\mathbf{a}) = \pi_H(\mathbf{b})$.

Remark 2.8. The above definitions are all modeled after [5, Definition 3.2], where $\mathcal{F}^*(\mathcal{A}(H))$ is replaced by the category of rigid factorizations $\mathbf{Z}_{\text{Sm}}(H)$, distances are all \mathbf{N} -valued and invariant, and the right-most inequality in (D4) has a slightly different form, for the fact that $\mathbf{Z}_{\text{Sm}}(H)$ is designed to include the trivial factorizations of the units of H (see Remark 2.6 for notations and further details).

The interest for subinvariant distances stems in part from the next lemma, which the reader may want to compare with points (1) and (2) of [5, Lemma 3.7].

Lemma 2.9. *Let H be a monoid and d a subinvariant distance on H . Then:*

- (i) $d(a, b) = d(c, d)$ for all $a, b, c, d \in \mathcal{F}^*(\mathcal{A}(H))$ with $(a, c), (b, d) \in \mathcal{C}_H$.
- (ii) $d(a * c, b * d) \leq d(a, b) + d(c, d)$ for all $a, b, c, d \in \mathcal{F}^*(\mathcal{A}(H))$.
- (iii) *The binary relation \sim_d on $\mathcal{F}^*(\mathcal{A}(H))$, defined by taking $a \sim_d b$, for some $a, b \in \mathcal{F}^*(\mathcal{A}(H))$, if and only if $\pi_H(a) = \pi_H(b)$ and $d(a, b) = 0$, is a monoid congruence, with $\llbracket c \rrbracket_{\mathcal{C}_H} \subseteq \llbracket c \rrbracket_{\sim_d}$ for every $c \in \mathcal{F}^*(\mathcal{A}(H))$.*

Proof. (i) Let $a, b, c \in \mathcal{F}^*(\mathcal{A}(H))$ with $(a, c) \in \mathcal{C}_H$. By (D2), it is sufficient to show that $d(a, b) \leq d(c, b)$, which is straightforward, because $d(a, b) \leq d(a, c) + d(c, b)$ by (D3) and $d(a, c) = 0$ by (D1).

(ii) Recall from the above that d is non-negative. Then, consider that, for all $a, b, c, d \in \mathcal{F}^*(\mathcal{A}(H))$,

$$d(a * c, b * d) \stackrel{(D3)}{\leq} d(a * c, b * c) + d(b * c, b * d) \stackrel{(D5)}{\leq} d(a, b) + d(c, d),$$

(iii) Let $a, b, c, d \in \mathcal{F}^*(\mathcal{A}(H))$. If $a \sim_d b$ and $b \sim_d c$, then $d(a, c) \leq d(a, b) + d(b, c) = 0$ by (D3), whence it is easy to check that \sim_d is an equivalence relation. To show that \sim_d is actually a congruence, assume $a \sim_d b$ and $c \sim_d d$, i.e., $\pi_H(a) = \pi_H(b)$, $\pi_H(c) = \pi_H(d)$, and $d(a, b) = d(c, d) = 0$. We need to prove that $a * c \sim_d b * d$, which is immediate, since, on the one hand, π_H being a homomorphism $\mathcal{F}^*(H) \rightarrow H$ yields

$$\pi_H(a * c) = \pi_H(a) * \pi_H(c) = \pi_H(b) * \pi_H(d) = \pi_H(b * d),$$

and on the other, we obtain from (ii) that $d(a * c, b * d) \leq d(a, b) + d(c, d) = 0$. So \sim_d is a congruence, and the rest is trivial by (D1). \blacksquare

By Lemma 2.9(iii), every subinvariant distance d on H yields a corresponding notion of factorization class, by looking at the quotient $Z_d(H)$ of $\mathcal{F}^*(\mathcal{A}(H))$ by the congruence \sim_d , i.e., by identifying two words $a, b \in \mathcal{F}^*(\mathcal{A}(H))$ if and only if $d(a, b) = 0$, cf. [5, Definition 3.8(1)]. However, we will not pursue this direction here, as it would take us too far from our main goals. Instead, we note that, by Lemma 2.9(iii), $Z_d(H) = Z(H)$ whenever d is a \mathcal{C}_H -metric, and we proceed to introduce *the* distance we are going to use in the sequel of the paper and to show that it is, in fact, a \mathcal{C}_H -metric, cf. [26, Proposition 1.2.5].

Definition 2.10. We set $\mathcal{A}^*(H) := \{H^\times a H^\times : a \in \mathcal{A}(H)\}$, and given $\mathfrak{A} \in \mathcal{A}^*(H)$ and $\mathfrak{z} \in \mathcal{F}^*(H)$, we let

$$v_H(\mathfrak{z}; \mathfrak{A}) := \begin{cases} |\{i \in \llbracket 1, n \rrbracket : z_i \in \mathfrak{A}\}| & \text{if } n := \|\mathfrak{z}\|_H \geq 1 \text{ and } \mathfrak{z} = z_1 * \dots * z_n, \\ 0 & \text{otherwise} \end{cases},$$

cf. [26, Definition 1.1.9.1]. Then, for all $a, b \in \mathcal{F}^*(\mathcal{A}(H))$ we take

$$\delta_H(a, b) := \begin{cases} 0 & \text{if } \pi_H(a) = \pi_H(b) \\ \frac{1}{2} & \text{otherwise} \end{cases}$$

and

$$a \wedge_H b := \max(\|a\|_H, \|b\|_H) - \sum_{\mathfrak{A} \in \mathcal{A}^*(H)} \min(v_H(a; \mathfrak{A}), v_H(b; \mathfrak{A})). \quad (4)$$

Lastly, we let the *matching distance* of H be the function

$$d_H : \mathcal{F}^*(\mathcal{A}(H)) \times \mathcal{F}^*(\mathcal{A}(H)) \rightarrow \mathbf{R} : (a, b) \mapsto \max(\delta_H(a, b), a \wedge_H b).$$

It turns out that d_H provides a natural way to measure how different two factorizations of a fixed element are from each other, especially when related to our definition of the factorization monoid $Z(H)$.

Lemma 2.11. *Let H be a monoid and pick $\mathbf{a}, \mathbf{b} \in \mathcal{F}^*(\mathcal{A}(H))$. Then*

$$\mathbf{a} \wedge_H \mathbf{b} = \frac{1}{2} \sum_{\mathfrak{A} \in \mathcal{A}^*(H)} |\nu_H(\mathbf{a}; \mathfrak{A}) - \nu_H(\mathbf{b}; \mathfrak{A})| + \frac{1}{2} \left| \|\mathbf{a}\|_H - \|\mathbf{b}\|_H \right|. \quad (5)$$

In particular, if $(\mathbf{a}, \mathbf{c}), (\mathbf{b}, \mathbf{d}) \in \mathcal{C}_H$, then $\mathbf{a} \wedge_H \mathbf{b} = \mathbf{c} \wedge_H \mathbf{d}$.

Proof. It is not difficult to see that

$$\|\mathfrak{z}\|_H = \sum_{\mathfrak{A} \in \mathcal{A}^*(H)} \nu_H(\mathfrak{z}; \mathfrak{A}) = \sum'_{\mathfrak{A} \in \mathcal{A}^*(H)} \nu_H(\mathfrak{z}; \mathfrak{A}), \quad \text{for every } \mathfrak{z} \in \mathcal{F}^*(\mathcal{A}(H)). \quad (6)$$

Here, the prime in the sum means that the summation is over all $\mathfrak{A} \in \mathcal{A}^*(H)$ such that $\nu_H(\mathfrak{z}; \mathfrak{A}) \neq 0$.

As a consequence, the claim is trivial if \mathbf{a} or \mathbf{b} is the empty word. Otherwise, write $\mathbf{a} = a_1 * \cdots * a_m$ and $\mathbf{b} = b_1 * \cdots * b_n$, where $a_1, \dots, a_m, b_1, \dots, b_n \in \mathcal{A}(H)$. Because

$$\mathbf{a} \wedge_H \mathbf{b} = (a_{\sigma(1)} * \cdots * a_{\sigma(m)}) \wedge_H (b_{\tau(1)} * \cdots * b_{\tau(n)}),$$

for all $\sigma \in \mathfrak{S}_m$ and $\tau \in \mathfrak{S}_n$, there is no loss of generality in assuming that there exists $k \in \llbracket 0, \min(m, n) \rrbracket$ with $a_i \simeq_H b_i$ for $i \in \llbracket 1, k \rrbracket$, but $a_i \not\simeq_H b_j$ for every $i \in \llbracket k+1, m \rrbracket$ and $j \in \llbracket k+1, n \rrbracket$. Accordingly, set $\mathbf{a}_0 := \mathbf{a}$ and $\mathbf{b}_0 := \mathbf{b}$, and for each $i \in \llbracket 1, k \rrbracket$ define $\mathbf{a}_i := a_i^{-1} \mathbf{a}_{i-1}$ and $\mathbf{b}_i := b_i^{-1} \mathbf{b}_{i-1}$. Then

$$\mathbf{a} \wedge_H \mathbf{b} = \max(\|\mathbf{a}_k\|_H, \|\mathbf{b}_k\|_H) = \frac{1}{2} \left(\|\mathbf{a}_k\|_H + \|\mathbf{b}_k\|_H \right) + \frac{1}{2} \left| \|\mathbf{a}_k\|_H - \|\mathbf{b}_k\|_H \right|, \quad (7)$$

where for the second equality we have used that $2 \max(x, y) = x + y + |x - y|$ for all $x, y \in \mathbf{R}$. On the other hand, it is clear from our definitions that

$$\|\mathbf{a}_k\|_H - \|\mathbf{b}_k\|_H = \|\mathbf{a}\|_H - \|\mathbf{b}\|_H, \quad (8)$$

and it is easily checked that, for each $\mathfrak{A} \in \mathcal{A}^*(H)$, we have

$$\|\mathbf{a}_k\|_H + \|\mathbf{b}_k\|_H \stackrel{(6)}{=} \sum'_{\mathfrak{A} \in \mathcal{A}^*(H)} \nu_H(\mathbf{a}_k; \mathfrak{A}) + \sum'_{\mathfrak{A} \in \mathcal{A}^*(H)} \nu_H(\mathbf{b}_k; \mathfrak{A}) = \sum_{\mathfrak{A} \in \mathcal{A}^*(H)} |\nu_H(\mathbf{a}_k; \mathfrak{A}) - \nu_H(\mathbf{b}_k; \mathfrak{A})|, \quad (9)$$

where the last equality follows from considering that $\nu_H(\mathbf{a}_k; \mathfrak{A}) \neq 0$, for some $\mathfrak{A} \in \mathcal{A}^*(H)$, if and only if $\nu_H(\mathbf{b}_k; \mathfrak{A}) = 0$ (by construction of \mathbf{a}_k and \mathbf{b}_k). Then (9), together with (7) and (8), leads to (5), because

$$\nu_H(\mathbf{a}_k; \mathfrak{A}) - \nu_H(\mathbf{b}_k; \mathfrak{A}) = \nu_H(\mathbf{a}; \mathfrak{A}) - \nu_H(\mathbf{b}; \mathfrak{A}), \quad \text{for all } \mathfrak{A} \in \mathcal{A}^*(H).$$

The ‘‘In particular’’ part of the statement is now immediate, since $\|\mathbf{c}\|_H = \|\mathbf{d}\|_H$ and $\nu_H(\mathbf{c}; \mathfrak{A}) = \nu_H(\mathbf{d}; \mathfrak{A})$ for all $(\mathbf{c}, \mathbf{d}) \in \mathcal{C}_H$ and $\mathfrak{A} \in \mathcal{A}^*(H)$. \blacksquare

Proposition 2.12. d_H is a locally invariant \mathcal{C}_H -metric and has the additional property that:

- (i) $d_H(\mathbf{a}, \mathbf{b})$ is a non-negative integer for every $(\mathbf{a}, \mathbf{b}) \in \mathcal{C}_H$;
- (ii) $d_H(\mathbf{a}^k, \mathbf{b}^k) = k d_H(\mathbf{a}, \mathbf{b})$ for all $\mathbf{a}, \mathbf{b} \in \mathcal{F}^*(\mathcal{A}(H))$ and $k \in \mathbf{N}$.

Moreover, $d_H(\mathbf{a}, \mathbf{b}) = \frac{1}{2}$ for some non-empty $\mathcal{A}(H)$ -words $\mathbf{a} = a_1 * \cdots * a_m$ and $\mathbf{b} = b_1 * \cdots * b_n$ of length m and n , respectively, if and only if $\pi_H(\mathbf{a}) \neq \pi_H(\mathbf{b})$, $m = n$, and there exists a permutation $\sigma \in \mathfrak{S}_n$ such that $a_i \simeq_H b_{\sigma(i)}$ for every $i \in \llbracket 1, m \rrbracket$.

Proof. (D1) and (D2) are trivial, the rest is a consequence of (6), Lemma 2.11, the triangle inequality for the absolute value, and the fact that $\delta_H(\mathbf{a}, \mathbf{b}) \leq \delta_H(\mathbf{a}, \mathbf{c}) + \delta_H(\mathbf{c}, \mathbf{b})$ for all $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathcal{F}^*(\mathcal{A}(H))$, with equality if and only if $(\mathbf{a}, \mathbf{c}) \in \mathcal{C}_H$ or $(\mathbf{c}, \mathbf{b}) \in \mathcal{C}_H$ (we encourage the reader to fill in the details). ■

Remark 2.13. Up to the technical details highlighted in Remarks 2.7 and 2.8, \mathbf{d}_H is no different from the *permutable distance* introduced by Baeth and Smertnig in the cancellative setting, cf. [5, Definition 3.4(2) and Construction 3.3(2)]. In particular, it follows from Remark 2.7 and [5, Remark 3.5(1)] that \mathbf{d}_H is essentially the same as the distance of [26, Definition 1.2.4 and p. 14] on the level of reduced, cancellative, commutative monoids.

We conclude the section with the definition of another arithmetic invariant that has played a prominent role in recent developments of factorization theory, as it provides more accurate information about factorizations than just their lengths.

Definition 2.14. Let H be a monoid. We take the *catenary degree* of an element $x \in H$, denoted by $\mathbf{c}_H(x)$, to be the infimum of the set of all $d \in \mathbb{N}$ for which the following condition is verified:

- For all $\mathbf{a}, \mathbf{b} \in \mathcal{Z}_H(x)$ there are factorizations $\mathbf{c}_0, \dots, \mathbf{c}_n \in \mathcal{Z}_H(x)$ with $\mathbf{c}_0 = \mathbf{a}$ and $\mathbf{c}_n = \mathbf{b}$ such that $\mathbf{d}_H(\mathbf{c}_{i-1}, \mathbf{c}_i) \leq d$ for every $i \in \llbracket 1, n \rrbracket$.

It is seen that $\mathbf{c}_H(x) = 0$, for a given $x \in H$, if and only if $|\mathcal{Z}_H(x)| \leq 1$. Consequently, we take

$$\mathbf{Ca}(H) := \{\mathbf{c}_H(x) : x \in H\} \setminus \{0\} \subseteq \mathbb{N}^+ \cup \{\infty\},$$

and we call $\mathbf{Ca}(H)$ the *set of catenary degrees* (or *catenary set*) of H .

It is clear that $\mathbf{Ca}(H) \subseteq \mathbb{N}^+$ if H is a BF-monoid, but this need not be true in general.

Remark 2.15. Let $x \in H \setminus H^\times$. It follows by Remark 2.13 that, if H is atomic and cancellative, $\mathbf{c}_H(x)$ coincides with the catenary degree of x associated, according to [5, Definition 4.1(3)], to the permutable distance of Baeth and Smertnig. In particular, if H is atomic, cancellative, and commutative, $\mathbf{c}_H(x)$ has the same value as the catenary degree of x in the classical theory, cf. [26, Definition 1.6.1.2].

Note that, in the same spirit of [5, § 4], every subinvariant distance \mathbf{d} on H gives rise to a corresponding notion of catenary degree. However, this is something beyond the scope of the present work.

2.1.4. Equimorphisms. The kind of arithmetic properties we consider in this paper, are often studied by reduction to suitable families of atomic monoids that are, in a certain way, less problematic than others. This is achieved by means of transfer techniques (cf. Remark 2.20), as per Halter-Koch's notion of transfer homomorphism in the commutative and cancellative setting, see [35, Lemma 5.4]; or Baeth and Smertnig's notion of weak transfer homomorphism, see [5, Definition 2.1] and [24, § 4].

Definition 2.16. Let H and K be multiplicatively written monoids, and let φ a homomorphism $H \rightarrow K$. We denote by φ^* the unique (monoid) homomorphism $\mathcal{F}^*(H) \rightarrow \mathcal{F}^*(K)$ such that $\varphi^*(x) = \varphi(x)$ for all $x \in H$, and we refer to φ as a (*monoid*) *equimorphism* (from H to K) if:

- (E1) $\varphi^{-1}(K^\times) \subseteq H^\times$ (or equivalently $\varphi^{-1}(K^\times) = H^\times$).
- (E2) φ is *atom-preserving*, i.e., $\varphi(a) \in \mathcal{A}(K)$ for all $a \in \mathcal{A}(H)$.
- (E3) If $x \in H$, $\mathbf{b} \in \mathcal{Z}_K(\varphi(x)) \neq \emptyset$, and $\|\mathbf{b}\|_K \neq 0$, then $\varphi^*(\mathbf{a}) \in \llbracket \mathbf{b} \rrbracket_{\mathcal{C}_K}$ for some $\mathbf{a} \in \mathcal{Z}_H(x)$.

Moreover, we call φ a *weak transfer homomorphism* if it is an equimorphism and $K = K^\times \varphi(H) K^\times$.

Then, we say that H is *equimorphic* to K if there exists an equimorphism from H to K ; and that H is a *transfer Krull monoid* if there is a weak transfer homomorphism from H to a monoid of zero-sum sequences over an abelian group G with support in a subset $G_0 \subseteq G$ (see [26, Definition 2.5.5] for further details and terminology).

Remark 2.17. In (E3), the K -word $\varphi^*(\mathbf{a})$ is actually an $\mathcal{A}(K)$ -word by condition (E2). In addition, the $\mathcal{A}(H)$ -word \mathbf{a} is non-empty, since $\|\mathbf{a}\|_H = \|\varphi^*(\mathbf{a})\|_K$ and, on the other hand, $\varphi^*(\mathbf{a}) \in \llbracket \mathbf{b} \rrbracket_{\mathcal{C}_K}$ implies $\|\varphi^*(\mathbf{a})\|_K = \|\mathbf{b}\|_K \neq 0$. Accordingly, write $\mathbf{a} = a_1 * \dots * a_m$ and $\mathbf{b} = b_1 * \dots * b_n$, with $a_1, \dots, a_m \in \mathcal{A}(H)$ and $b_1, \dots, b_n \in \mathcal{A}(K)$. Then $\varphi^*(\mathbf{a}) \in \llbracket \mathbf{b} \rrbracket_{\mathcal{C}_K}$ is equivalent to having that $\pi_K(\mathbf{b}) = \pi_K(\varphi^*(\mathbf{a}))$, $m = n$, and there exists a permutation $\sigma \in \mathfrak{S}_n$ such that $b_{\sigma(i)} \simeq_K \varphi(a_i)$ for every $i \in \llbracket 1, n \rrbracket$.

Remark 2.18. Condition (E2) cannot be proved from (E1) and (E3). Indeed, let H (respectively, K) be the monoid of non-negative integers (respectively, non-negative real numbers) under addition, and let φ be the canonical embedding. Clearly, φ satisfies (E1) and (E3), because $H^\times = K^\times = \{0\}$ and $\mathcal{A}(K) = \emptyset$. But $1 \in \mathcal{A}(H)$, so φ cannot satisfy (E2).

Remark 2.19. In Baeth and Smertnig's original definition of a weak transfer homomorphism $\varphi : H \rightarrow K$, it is assumed that H is cancellative and K is atomic, which implies that φ is atom-preserving. By Remark 2.18, this need not hold for an arbitrary equimorphism, which is the reason for having included condition (E2) in the above definitions. In particular, it follows from here and Remark 2.17 that every weak transfer homomorphism in the sense of Baeth and Smertnig is also a weak transfer homomorphism in our sense, and hence an equimorphism.

Remark 2.20. The rationale behind the introduction of transfer techniques in factorization theory is as follows: We have some kind of monoid homomorphism $\varphi : H \rightarrow K$, and we want to understand properties of one of H or K by looking at corresponding properties of the other. To this end, we use φ to shift information from H to K (as we do here with equimorphisms, see Theorems 2.22 and 3.8), if H is, in a sense, easier to study than K ; or to pull it back from K to H (as is commonly the case with transfer and weak transfer homomorphisms), if it is the other way around.

2.2. Abstract arithmetic results. Now that we have introduced most of the basic notions we need and clarified, we hope, some subtle aspects of the theory, we are ready to prove a couple of results extending some pieces of [26, Proposition 1.2.11.1] and [24, Lemma 11], respectively, to the general setting of this work: As is true for the largest number of results from the present section, they will be used later, in §§ 3 and 4, to study the arithmetic of power monoids.

Proposition 2.21. *Let H be a monoid, and assume that M is a divisor-closed submonoid of H . Then $M^\times = H^\times$ and $\mathcal{A}(M) = \mathcal{A}(H) \cap M$. In addition, $\mathsf{L}_M(x) = \mathsf{L}_H(x)$, $\mathsf{Z}_M(x) = \mathsf{Z}_H(x)$, and $\mathsf{c}_M(x) = \mathsf{c}_H(x)$ for all $x \in M$, and consequently $\mathcal{L}(M) \subseteq \mathcal{L}(H)$, $\Delta(M) \subseteq \Delta(H)$, and $\mathsf{Ca}(M) \subseteq \mathsf{Ca}(H)$.*

Proof. Of course, $M^\times \subseteq H^\times$. On the other hand, $u \in H^\times$ only if $u \mid_H 1_H$, and since $1_H = 1_M$ and M is a divisor-closed submonoid of H , this implies $H^\times \subseteq M^\times$. To wit, $M^\times = H^\times$.

Consequently, it is clear that $\mathcal{A}(H) \cap M \subseteq \mathcal{A}(M)$. To prove the opposite inclusion, let $a \in \mathcal{A}(M)$, and write $a = xy$ for some $x, y \in H$. Then $x, y \in M$, using again that M a divisor-closed submonoid of

H . So, x or y is a unit of M , and hence $a \in \mathcal{A}(H)$, because $M^\times = H^\times$. Therefore, given $x, y \in M$, it is immediate that $\mathcal{Z}_M(x) = \mathcal{Z}_H(x)$, and $x \simeq_M y$ if and only if $x \simeq_H y$. This yields $\mathcal{Z}_M(x) = \mathcal{Z}_H(x)$ for every $x \in M$, and the rest is obvious. ■

Theorem 2.22. *Let H and K be monoids, and $\varphi : H \rightarrow K$ an equimorphism. The following hold:*

- (i) $\mathsf{L}_H(x) = \mathsf{L}_K(\varphi(x))$ for each $x \in H \setminus H^\times$.
- (ii) For each $\mathfrak{A} \in \mathcal{A}^*(H)$ there exists a unique $\mathfrak{B} \in \mathcal{A}^*(K)$ with $\varphi(\mathfrak{A}) \subseteq \mathfrak{B}$.
- (iii) $\varphi^*(\mathfrak{a}) \wedge_K \varphi^*(\mathfrak{b}) \leq \mathfrak{a} \wedge_H \mathfrak{b}$ for all $\mathfrak{a}, \mathfrak{b} \in \mathcal{F}^*(\mathcal{A}(H))$ with $\|\mathfrak{a}\|_H = \|\mathfrak{b}\|_H$.
- (iv) $\mathsf{c}_K(\varphi(x)) \leq \mathsf{c}_H(x)$ for all $x \in H$.
- (v) $\varphi(H)$ is a divisor-closed submonoid of K only if $\varphi(H^\times) = K^\times$.
- (vi) If $\varphi(H^\times) = K^\times$ and K is atomic, then φ is surjective.
- (vii) If K is atomic, then so is H .

In particular, $\mathcal{L}(H) \subseteq \mathcal{L}(K)$ and $\Delta(H) \subseteq \Delta(K)$.

Proof. (i) Pick $x \in H \setminus H^\times$, and set $L := \mathsf{L}_H(x)$ and $L' := \mathsf{L}_K(\varphi(x))$. Since x is not a unit, it is clear from condition (E1) of Definition 2.16 that $\varphi(x) \notin K^\times$, which yields $L, L' \subseteq \mathbf{N}^+$ (see Remark 2.3).

Accordingly, assume $L \neq \emptyset$ and let $k \in L$. Then $x = a_1 \cdots a_k$ for some $a_1, \dots, a_k \in \mathcal{A}(H)$. Therefore $\varphi(x) = \varphi(a_1) \cdots \varphi(a_k)$, and hence $k \in L'$, because φ is an atom-preserving homomorphism.

Conversely, assume $L' \neq \emptyset$ and pick $k \in L'$. Then $\varphi(x) = b_1 \cdots b_k$ for some $b_1, \dots, b_k \in \mathcal{A}(K)$, and by Remark 2.17 there are $a_1, \dots, a_k \in \mathcal{A}(H)$ such that $x = a_1 \cdots a_k$, with the result that $k \in L$.

So, putting it all together, we can conclude that $L = L'$. The “In particular” part of the statement (on systems of sets of lengths and delta sets) is then an obvious consequence.

(ii) Given $\mathfrak{A} \in \mathcal{A}^*(H)$, let $a \in \mathfrak{A}$ and define $\mathfrak{B} := K^\times \varphi(a) K^\times$. Then $\mathfrak{A} = H^\times a H^\times$, and since φ is a homomorphism, we have that $\varphi(\mathfrak{A}) = \varphi(H^\times) \varphi(a) \varphi(H^\times) \subseteq K^\times \varphi(a) K^\times = \mathfrak{B}$; in addition, $\mathfrak{B} \in \mathcal{A}^*(K)$, because φ is atom-preserving. The rest is trivial, in that $\mathcal{A}^*(K)$ is the quotient set of $\mathcal{A}(K)$ under the restriction of the (equivalence) relation \simeq_K to the atoms of K ; so each class in $\mathcal{A}^*(K)$ is non-empty, and pairwise distinct classes are disjoint (by the general properties of equivalences).

(iii) Let $\mathfrak{a}, \mathfrak{b} \in \mathcal{F}^*(\mathcal{A}(H))$ with $\|\mathfrak{a}\|_H = \|\mathfrak{b}\|_H$. Then $\|\varphi^*(\mathfrak{a})\|_K = \|\varphi^*(\mathfrak{b})\|_K$, hence it is clear from (4) that $\varphi^*(\mathfrak{a}) \wedge_K \varphi^*(\mathfrak{b}) \leq \mathfrak{a} \wedge_H \mathfrak{b}$ if and only if

$$\sum_{\mathfrak{A} \in \mathcal{A}^*(H)} \min(\mathsf{v}_H(\mathfrak{a}; \mathfrak{A}), \mathsf{v}_H(\mathfrak{b}; \mathfrak{A})) \leq \sum_{\mathfrak{B} \in \mathcal{A}^*(K)} \min(\mathsf{v}_K(\varphi^*(\mathfrak{a}); \mathfrak{B}), \mathsf{v}_K(\varphi^*(\mathfrak{b}); \mathfrak{B})). \quad (10)$$

Denote by \mathfrak{B}^* , for every $\mathfrak{B} \in \mathcal{A}^*(K)$, the set of all $\mathfrak{A} \in \mathcal{A}^*(H)$ such that $\varphi(\mathfrak{A}) \subseteq \mathfrak{B}$. Then we see from (ii) that $\mathcal{A}^*(H) = \bigsqcup \{\mathfrak{B}^* : \mathfrak{B} \in \mathcal{A}^*(K)\}$. Therefore, a sufficient condition for (10) to hold is that

$$\sum_{\mathfrak{A} \in \mathfrak{B}^*} \min(\mathsf{v}_H(\mathfrak{a}; \mathfrak{A}), \mathsf{v}_H(\mathfrak{b}; \mathfrak{A})) \leq \min(\mathsf{v}_K(\varphi^*(\mathfrak{a}); \mathfrak{B}), \mathsf{v}_K(\varphi^*(\mathfrak{b}); \mathfrak{B})), \quad \text{for all } \mathfrak{B} \in \mathcal{A}^*(K). \quad (11)$$

On the other hand, it is easily verified that, for all $a_1, b_1, \dots, a_n, b_n \in \mathbf{R}$,

$$\min(a_1, b_1) + \cdots + \min(a_n, b_n) \leq \min(a_1 + \cdots + a_n, b_1 + \cdots + b_n).$$

So, for (11) to be true it is enough to check that $\sum_{\mathfrak{A} \in \mathfrak{B}^*} \mathsf{v}_H(\mathfrak{c}; \mathfrak{A}) \leq \mathsf{v}_K(\varphi^*(\mathfrak{c}); \mathfrak{B})$ for every $\mathfrak{B} \in \mathcal{A}^*(K)$ and every non-empty $\mathcal{A}(H)$ -word $\mathfrak{c} = c_1 * \cdots * c_n$, which is now trivial, because $c_i \in \mathfrak{A}$ for some $\mathfrak{A} \in \mathfrak{B}^*$ and $i \in [1, n]$ only if $\varphi(c_i) \in \mathfrak{B}$.

(iv) Let $x \in H$. The inequality is obvious if $c_K(\varphi(x)) = 0$. Otherwise, $\mathcal{Z}_K(\varphi(x)) \neq \emptyset$ and $x \neq 1_H$. So, pick $\mathbf{a}', \mathbf{b}' \in \mathcal{Z}_K(\varphi(x))$. By condition (E3), $\varphi^*(\mathbf{a}) \in \llbracket \mathbf{a}' \rrbracket_{\mathcal{C}_K}$ and $\varphi^*(\mathbf{b}) \in \llbracket \mathbf{b}' \rrbracket_{\mathcal{C}_K}$ for some $\mathbf{a}, \mathbf{b} \in \mathcal{Z}_H(x)$. Consequently, there are factorizations $\mathbf{c}_0, \dots, \mathbf{c}_n \in \mathcal{Z}_H(x)$ with $\mathbf{c}_0 = \mathbf{a}$, $\mathbf{c}_n = \mathbf{b}$, and $d_H(\mathbf{c}_{i-1}, \mathbf{c}_i) \leq c_H(x)$ for each $i \in \llbracket 1, n \rrbracket$. Set $\mathbf{c}'_0 := \mathbf{a}'$, $\mathbf{c}'_n := \mathbf{b}'$, and $\mathbf{c}'_i := \varphi^*(\mathbf{c}_i)$ for $i \in \llbracket 1, n-1 \rrbracket$. By Lemma 2.11,

$$\mathbf{c}'_0 \wedge_K \mathbf{c}'_1 = \varphi^*(\mathbf{a}) \wedge_K \mathbf{c}'_1 = \varphi^*(\mathbf{c}_0) \wedge_K \mathbf{c}'_1 \quad \text{and} \quad \mathbf{c}'_{n-1} \wedge_K \mathbf{c}'_n = \mathbf{c}'_{n-1} \wedge_K \varphi^*(\mathbf{b}) = \mathbf{c}'_{n-1} \wedge_K \varphi^*(\mathbf{c}_n).$$

Therefore, we conclude from (iii) that, for every $i \in \llbracket 1, n \rrbracket$,

$$d_K(\mathbf{c}'_{i-1}, \mathbf{c}'_i) = \mathbf{c}'_{i-1} \wedge_K \mathbf{c}'_i = \varphi^*(\mathbf{c}_{i-1}) \wedge_K \varphi^*(\mathbf{c}_i) \leq \mathbf{c}_{i-1} \wedge_H \mathbf{c}_i = d_H(\mathbf{c}_{i-1}, \mathbf{c}_i) \leq c_H(x),$$

which implies that the catenary degree of $\varphi(x)$ in K is bounded above by $c_H(x)$.

(v) It is straightforward from Proposition 2.21, when considering that $\varphi(H^\times) = \varphi(H)^\times$ (again, by the fact that φ is a homomorphism).

(vi) Assume that K is atomic and $\varphi(H^\times) = K^\times$, and pick $y \in K \setminus K^\times$. We have to prove $y \in \varphi(H)$. To this end, it follows from the atomicity of K that $y = b_1 \cdots b_n$ for some $b_1, \dots, b_n \in \mathcal{A}(K)$, and since φ is an equimorphism, we get from Remark 2.17 (and the assumption that every unit of K is the image under φ of some unit of H) that there are $a_1, \dots, a_n \in \mathcal{A}(H)$, $u_1, v_1, \dots, u_n, v_n \in H^\times$, and $\sigma \in \mathfrak{S}_n$ such that $b_i = \varphi(u_i) \varphi(a_{\sigma(i)}) \varphi(v_i)$ for every $i \in \llbracket 1, n \rrbracket$. So $y = \varphi(x)$, where $x := u_1 a_{\sigma(1)} v_1 \cdots u_n a_{\sigma(n)} v_n$.

(vii) Suppose that K is atomic, and let $x \in H \setminus H^\times$. Then $\varphi(x) \notin K^\times$ (by condition (E1) of Definition 2.16). Hence $\mathcal{L}_H(x) = \mathcal{L}_K(\varphi(x)) \neq \emptyset$, by Theorem 2.22(i) and the atomicity of K . Viz., H is atomic. ■

Remark 2.23. The conclusion of Theorem 2.22(vi) need not be true if K is not atomic. Indeed, let K be the monoid of non-negative real numbers under addition, and H the submonoid of K consisting of the rational numbers. Both H and K are reduced, divisible, cancellative, commutative monoids, and hence $\mathcal{A}(H) = \mathcal{A}(K) = \emptyset$, since every non-unit of H (respectively, of K) is the square of a non-unit. It follows that the canonical embedding $H \rightarrow K$ is an injective equimorphism. Yet, H is not a divisor-closed submonoid of K .

Remark 2.24. It follows from [5, p. 506] and Remark 2.13 that, if $\varphi : H \rightarrow K$ is a transfer homomorphism in the sense of [5, Definition 2.1(1)] and K is atomic, then $c_K(\varphi(x)) \leq c_H(x)$ for all $x \in H \setminus H^\times$, which is a special case of Theorem 2.22(iv), because φ is a weak transfer homomorphism by [5, p. 483], and hence an equimorphism by Remark 2.19.

Sharper results are available in the literature under stronger assumptions or for particular classes of monoids; see, e.g., [26, Theorem 3.2.5.4] for the case when H and K are commutative, cancellative, atomic monoids and φ is a transfer homomorphism, or [5, Proposition 4.8] for the case of an *isoatomic* weak transfer homomorphism from an atomic cancellative monoid to another (φ is *isoatomic* if $\varphi(a) \simeq_K \varphi(b)$, for some $a, b \in \mathcal{A}(H)$, implies $a \simeq_H b$).

Our next step is to have some convenient criteria for a unit-cancellative monoid to be atomic or BF. We start with a couple of definitions, the second of which extends [26, Definition 1.1.3.2] from the case when H is cancellative and commutative, but is more restrictive than analogous definitions given by Geroldinger [25, p. 533] and Smertnig [51, p. 364] in the cancellative setting.

Definition 2.25. A monoid H satisfies the *ascending chain condition* (shortly, ACC) on principal right ideals (respectively, on principal left ideals) if, for every sequence $(a_n)_{n \geq 1}$ of elements of H such that $a_n H \subseteq a_{n+1} H$ (respectively, $H a_n \subseteq H a_{n+1}$) for all n , there is an index $v \in \mathbf{N}^+$ for which $a_n H = a_v H$ (respectively, $H a_v = H a_n$) when $n \geq v$. In addition, we say that H satisfies the ACCP if it satisfies the ACC on both principal right and principal left ideals.

Definition 2.26. Let H be a monoid and λ a function $H \rightarrow \mathbf{N}$. We say that λ is a *length function* (on H) if $\lambda(x) < \lambda(y)$ for all $x, y \in H$ such that $y = uxv$ for some $u, v \in H$ with $u \notin H^\times$ or $v \notin H^\times$.

Then, we proceed to our first theorem, which is an all-embracing generalization of [26, Proposition 1.1.4 and Corollary 1.3.3] and [17, Lemma 3.1(1)].

Lemma 2.27. *Let H be a unit-cancellative monoid, and let $x, y \in H$. We have that:*

- (i) $xy \in H^\times$ if and only if $x, y \in H^\times$.
- (ii) If $xy = xu$ (respectively, $yx = ux$) for some $u \in H^\times$, then $y \in H^\times$.
- (iii) $xH = yH$ (respectively, $Hx = Hy$) if and only if $x \in yH^\times$ (respectively, $x \in H^\times y$).
- (iv) If H satisfies the ACC on principal right (respectively, principal left) ideals and $x \in H \setminus H^\times$, then $x \in \mathcal{A}(H) \cdot H$ (respectively, $x \in H \cdot \mathcal{A}(H)$).

Proof. (i) The “if” part is trivial, see also Lemma 2.2(i). As for the other direction, assume xy is a unit, and let $u \in H$ such that $xyu = uxy = 1_H$. This means that x is right-invertible and y is left-invertible (a right inverse of x being given by yu , and a left inverse of y by ux). Moreover, we have $xyux = x$, which implies, by the unit-cancellativity of H , that $v := yux$ is a unit, and hence $(v^{-1}yu)x = y(uxv^{-1}) = 1_H$. So, in conclusion, we see that both x and y are right- and left-invertible, hence are invertible.

(ii) Suppose that $xy = xu$ for some $u \in H^\times$ (the other case is similar). Then $x = xyu^{-1}$, so we get by the unit-cancellativity of H and point (i) that $y \in H^\times$.

(iii) It is obvious that, if $x \in yH^\times$, then $xH = yH$. So assume $xH = yH$. Then $x = ya$ and $y = xb$ for some $a, b \in H$, with the result that $y = yab$. Because H is unit-cancellative, it follows that $ab \in H^\times$, and hence $a, b \in H^\times$ by point (i) above. This yields $x \in yH^\times$ and finishes the proof, since the analogous statement for principal left ideals can be established in a similar way (we omit details).

(iv) We prove the statement only for principal right ideals, as the other case is similar. To this end, assume for a contradiction that the claim is false. Then the set

$$\Omega := \{zH : z \in H \setminus H^\times \text{ and } z \notin \mathcal{A}(H) \cdot H\}$$

is non-empty. So, using that H satisfies the ACC on principal right ideals, Ω has a \subseteq -maximal element, say $\bar{z}H$. Clearly, \bar{z} is neither a unit nor an atom (of H), because $\bar{z}H \in \Omega$. Therefore, $\bar{z} = ab$ for some $a, b \in H \setminus H^\times$, and it is clear that $a \notin \mathcal{A}(H) \cdot H$, otherwise we would have $\bar{z} \in \mathcal{A}(H) \cdot H$. Thus, $aH \in \Omega$ and $\bar{z}H \subseteq aH$. But $\bar{z}H$ is a \subseteq -maximal element of Ω , so necessarily $\bar{z}H = aH$.

It then follows from point (iii) and the above that $ab = \bar{z} = au$ for some $u \in H^\times$, which is however a contradiction, as it implies $b \in H^\times$ by point (ii). ■

Theorem 2.28. *Let H be a monoid and M a submonoid of H with $M^\times = M \cap H^\times$. The following hold:*

- (i) *Suppose that H is unit-cancellative and satisfies the ACCP. Then H is atomic.*

- (ii) If H is unit-cancellative, then so is M .
- (iii) Assume that H has a length function. Then H is unit-cancellative and satisfies the ACCP.
- (iv) If H has a length function λ , then M is a BF-monoid and $\sup L_M(x) \leq \lambda(x)$ for all $x \in M$.

Proof. (i) We proceed along the lines of the proof of [52, Proposition 3.1]. To start with, suppose for a contradiction that the set

$$\Omega := \{Hx : x \in H \setminus H^\times \text{ and } x \text{ is not a (finite) product of atoms of } H\}$$

is non-empty. Then, using that H satisfies the ACC on principal *left* ideals, Ω must have a maximal element, say $H\tilde{x}$. Of course, \tilde{x} is neither a unit nor an atom (of H), so we get from Lemma 2.27(iv) that $\tilde{x} = ax$ for some $a \in \mathcal{A}(H)$ and $x \in H$, where we have used that H also satisfies the ACC on principal *right* ideals. This shows that $H\tilde{x} \subseteq Hx$, and we claim that $H\tilde{x} \subsetneq Hx$.

Indeed, assume to the contrary that $H\tilde{x} = Hx$. Then we infer from Lemma 2.27(iii) that $H^\times \tilde{x} = H^\times x$, and hence $ax = \tilde{x} = ux$ for some $u \in H^\times$. Yet this is impossible, as it implies by Lemma 2.27(ii) that a is a unit, and hence not an atom, of H . Consequently, we see that $H\tilde{x} \subsetneq Hx$ (as was claimed).

It follows that $Hx \notin \Omega$, because $H\tilde{x}$ is a \subseteq -maximal element of Ω . But we derive from Lemma 2.2(ii) that x is not a unit of H , as $H\tilde{x}$ means, in particular, that \tilde{x} is not an atom. Therefore, $Hx \notin \Omega$ only if $x = a_1 \cdots a_n$ for some $a_1, \dots, a_n \in \mathcal{A}(H)$, which, however, is still a contradiction, since it implies that \tilde{x} is a product of atoms of H (recall from the above that $\tilde{x} = ax$).

(ii) Assume H is unit-cancellative, and let $x, y \in M$ such that $xy = x$ or $yx = x$ in M . Then $xy = x$ or $yx = x$ in H (since M is a submonoid of H), and hence $x \in H^\times$. So, using that $M^\times = M \cap H^\times$, it follows that $x \in M^\times$, and we can conclude that M is unit-cancellative.

(iii) Let $\ell : H \rightarrow \mathbb{N}$ be a length function on H , and suppose for a contradiction that H is not unit-cancellative. Then there exist non-units $x, y \in H$ such that $xy = x$ or $yx = x$. But this is impossible, since $xy = x$ implies $\ell(x) = \ell(xy) > \ell(x)$, and the other case is similar.

So, it remains to prove that H satisfies the ACCP. For, suppose to the contrary that there exists a sequence $(a_n)_{n \geq 1}$ of elements of H such that $a_n H \subsetneq a_{n+1} H$ (respectively, $Ha_n \subsetneq Ha_{n+1}$) for all $n \in \mathbb{N}^+$. Then, for each $n \in \mathbb{N}^+$ we have that $a_n = a_{n+1} v_n$ (respectively, $a_n = v_n a_{n+1}$) for some $v_n \in H \setminus H^\times$, with the result that $\ell(a_{n+1}) < \ell(a_n)$. But this is impossible.

(iv) Because $u \in M \setminus M^\times$ only if $u \notin H^\times$ (by hypothesis), it is obvious that the restriction of λ to M is a length function on M . So we have by point (iii) that M is unit-cancellative and satisfies the ACCP. Consequently, we obtain from (i) that M is atomic, and we are left to show that it is actually BF.

To this end, let $x \in M \setminus M^\times$, and pick $k \in \mathbb{N}^+$ and $a_1, \dots, a_k \in \mathcal{A}(M)$ such that $x = a_1 \cdots a_k$. Since it is immediate from the definition of a length function that $\lambda(a) \geq 1$ for every $a \in M \setminus M^\times$, it is seen by induction that $\lambda(x) \geq k$. Thus $\sup L_M(x) \leq \lambda(x)$, and we are done. ■

We conclude the section with a corollary generalizing [26, Proposition 1.3.2] from cancellative, commutative monoids to arbitrary monoids, cf. [25, Lemma 6.1] and [51, Lemma 3.6] for some analogues in the cancellative setting; and with an elementary proposition showing that unit-cancellative monoids are Dedekind-finite.

Corollary 2.29. *Let H be a monoid. The following are equivalent:*

- (a) H is a BF-monoid.
- (b) $\bigcap_{n \geq 1} (H \setminus H^\times)^n = \emptyset$.
- (c) H has a length function.

In particular, if any of these conditions is satisfied, then H is unit-cancellative.

Proof. To ease notation, set $\mathfrak{m} := H \setminus H^\times$ and $\mathfrak{j} := \bigcap_{n \geq 1} \mathfrak{m}^n$. It is sufficient to prove that (a) \Rightarrow (b) and (b) \Rightarrow (c), since (c) \Rightarrow (a) is straightforward from Theorem 2.28(iv), while the “In particular” part is a consequence of (c) and Theorem 2.28(iii).

(a) \Rightarrow (b): Pick $x \in H$. If $x \in \mathfrak{m}^n$, then $x = x_1 \cdots x_n$ for some $x_1, \dots, x_n \in H \setminus H^\times$, which yields $\sup \mathsf{L}_H(x) \geq n$, because H is BF, and hence x_i is a non-empty product of atoms of H for each $i \in \llbracket 1, n \rrbracket$. But H being a BF-monoid also implies that $\mathsf{L}_H(x)$ is finite. Consequently, there must exist $n \in \mathbf{N}^+$ such that $x \notin \mathfrak{m}^n$, with the result that $\mathfrak{j} = \emptyset$.

(b) \Rightarrow (c): To start with, we show that H is unit-cancellative. For, assume to the contrary that $x = xy$ (respectively, $x = yx$) for some $x \in H$ and $y \in H \setminus H^\times$. Then x is a non-unit, and $x = xy^k \in \mathfrak{m}^{k+1}$ (respectively, $x = y^k x \in \mathfrak{m}^{k+1}$) for every $k \in \mathbf{N}$. So $x \in \mathfrak{j} \neq \emptyset$, a contradiction.

With this in hand, let $\bar{x} \in H$. Since $\mathfrak{j} = \emptyset$, there exists $v \in \mathbf{N}^+$ such that $\bar{x} \notin \mathfrak{m}^v$, and we claim that $\bar{x} \notin \mathfrak{m}^n$ for every $n \geq v$. Indeed, suppose that $\bar{x} = x_1 \cdots x_n$ for some $n \geq v$ and $x_1, \dots, x_n \in H \setminus H^\times$, and set $y_i := x_i$ for $i \in \llbracket 1, v-1 \rrbracket$ and $y_v := x_v \cdots x_n$. Then, using that H is unit-cancellative, we obtain from Lemma 2.27(i) that $y_1, \dots, y_v \in H \setminus H^\times$, and hence $\bar{x} \in \mathfrak{m}^v$, which is again a contradiction.

It follows that the function $\lambda : H \rightarrow \mathbf{N} : x \mapsto \sup \{n \in \mathbf{N}^+ : x \in \mathfrak{m}^n\}$ is well defined, because the set $\{n \in \mathbf{N}^+ : x \in \mathfrak{m}^n\}$ is finite for all $x \in H$. We want to show that λ is a length function (on H).

In fact, let $u, v, x, y \in H$ with $y = uv$. Again by Lemma 2.27(i), it is clear that $y \in \mathfrak{m}^{\lambda(u) + \lambda(x) + \lambda(v)}$, where $\mathfrak{m}^0 := H^\times$. Therefore $\lambda(u) + \lambda(x) + \lambda(v) \leq \lambda(y)$, and $\lambda(x) = \lambda(y)$ only if $\lambda(u) = \lambda(v) = 0$, which is, in turn, equivalent to $u, v \in H^\times$. This yields that λ is a length function. ■

As a side remark, we get from Corollary 2.29 that a monoid is BF only if it is unit-cancellative: This extends to the non-commutative setting an observation from the introduction of [17, § 3].

Proposition 2.30. *Let H be a monoid. Then H is Dedekind-finite if and only if $x, y \in H^\times$ for all $x, y \in H$ with $xy \in H^\times$. In particular, H is Dedekind-finite if $\mathcal{A}(H) \neq \emptyset$ or H is unit-cancellative.*

Proof. Suppose first that H is Dedekind-finite, and let $x, y \in H$ such that $xy \in H^\times$. Then there exists $z \in H$ for which $xyz = zxy = 1_H$. It follows that $yzx = 1_H$, which shows that x and y are units (since they are both left- and right-invertible).

Conversely, assume that $x, y \in H^\times$ whenever $x, y \in H$ and $xy \in H^\times$. Then $xy = 1_H$ for some $x, y \in H$ yields $x, y \in H^\times$, and hence $y = x^{-1}xy = x^{-1} \cdot 1_H = x^{-1}$, which implies $yx = 1_H$.

The “In particular” part is now straightforward by the above and Lemmas 2.2(i) and 2.27(i). ■

3. POWER MONOIDS

In this and the subsequent section, we apply most of the ideas developed in § 2 to a specific class of structures that are, in a way, “extremely non-cancellative”. To this end, we make the following:

Definition 3.1. Let H be a (multiplicatively written) monoid. We use $\mathcal{P}_{\text{fin}}(H)$ for the set of all *non-empty* finite subsets of H , and we denote by \cdot the binary operation

$$\mathcal{P}_{\text{fin}}(H) \times \mathcal{P}_{\text{fin}}(H) \rightarrow \mathcal{P}_{\text{fin}}(H) : (X, Y) \mapsto XY,$$

where $XY := X \cdot Y := \{xy : (x, y) \in X \times Y\}$. Moreover, we define

$$\mathcal{P}_{\text{fin}, \times}(H) := \{X \in \mathcal{P}_{\text{fin}}(H) : X \cap H^\times \neq \emptyset\}.$$

It is trivial that $\mathcal{P}_{\text{fin}}(H)$, endowed with the above operation, forms a monoid, with the identity given by the singleton $\{1_H\}$, and $\mathcal{P}_{\text{fin}, \times}(H)$ is a submonoid of $\mathcal{P}_{\text{fin}}(H)$. Accordingly, we call $\mathcal{P}_{\text{fin}}(H)$ and $\mathcal{P}_{\text{fin}, \times}(H)$, respectively, the *power monoid* and *restricted power monoid* of H .

Our goal for the remainder of the paper is, in fact, to investigate some of the algebraic and arithmetic properties of power monoids, and to link them to corresponding properties of the restricted power monoid of $(\mathbb{N}, +)$, which we will denote by $\mathcal{P}_{\text{fin}, 0}(\mathbb{N})$ and always write additively. We start with a few basic results.

Proposition 3.2. *Let H be a monoid. The following hold:*

- (i) $\mathcal{P}_{\text{fin}}(H)$ and $\mathcal{P}_{\text{fin}, \times}(H)$ are cancellative if and only if $H = \{1_H\}$.
- (ii) $\mathcal{P}_{\text{fin}}(H)^\times = \mathcal{P}_{\text{fin}, \times}(H)^\times = \{\{u\} : u \in H^\times\}$.
- (iii) Let H be Dedekind-finite. Then $\mathcal{P}_{\text{fin}, \times}(H)$ is a divisor-closed submonoid of $\mathcal{P}_{\text{fin}}(H)$. In particular, $\mathcal{L}(\mathcal{P}_{\text{fin}, \times}(H)) \subseteq \mathcal{L}(\mathcal{P}_{\text{fin}}(H))$ and $\text{Ca}(\mathcal{P}_{\text{fin}, \times}(H)) \subseteq \text{Ca}(\mathcal{P}_{\text{fin}}(H))$.
- (iv) Let $a \in H$. Then $\{a\}$ is an atom of $\mathcal{P}_{\text{fin}}(H)$ only if a is an atom of H , and the converse is also true if H is strongly unit-cancellative.
- (v) Assume H is cancellative. Then $\mathcal{P}_{\text{fin}}(H)$ is atomic (respectively, a BF-monoid) only if so is H .

Proof. (i) The “if” part is obvious, and of course $\mathcal{P}_{\text{fin}}(H)$ is cancellative only if so is $\mathcal{P}_{\text{fin}, \times}(H)$. Therefore, suppose for a contradiction that $\mathcal{P}_{\text{fin}, \times}(H)$ is cancellative, but $H \neq \{1_H\}$. Accordingly, let $x \in H \setminus \{1_H\}$. We have $1_H \neq x^2 \neq x$: Otherwise, $\{1_H, x\} \cdot \{1_H\} = \{1_H, x\} \cdot \{1_H, x\}$, yet $\{1_H, x\} \neq \{1_H\}$, which is not possible, by the cancellativity of $\mathcal{P}_{\text{fin}, \times}(H)$. But this again leads to a contradiction, because it implies $\{1_H, x^2\} \neq \{1_H, x, x^2\}$, though $\{1_H, x^2\} \cdot \{1_H, x\} = \{1_H, x, x^2\} \cdot \{1_H, x\}$.

(ii) It is trivial that $\{\{u\} : u \in H^\times\} \subseteq \mathcal{P}_{\text{fin}, \times}(H)^\times \subseteq \mathcal{P}_{\text{fin}}(H)^\times$, and it only remains to show $\mathcal{P}_{\text{fin}}(H)^\times \subseteq \{\{u\} : u \in H^\times\}$. For, let $U \in \mathcal{P}_{\text{fin}}(H)^\times$. Then $UV = VU = \{1_H\}$ for some $V \in \mathcal{P}_{\text{fin}}(H)$, and hence, for every $u \in U$, there can be found $v, w \in H$ such that $vu = uw = 1_H$. That is, every element of U is left- and right-invertible, and hence invertible. It is thus clear that $UV = \{1_H\}$ only if $1 = |UV| \geq |U|$. So, U is a one-element subset of H^\times , and we are done.

(iii) Let $X \in \mathcal{P}_{\text{fin}, \times}(H)$ and $Y \in \mathcal{P}_{\text{fin}}(H)$ such that $UYV = X$ for some $U, V \in \mathcal{P}_{\text{fin}}(H)$ (namely, $Y \mid X$ in $\mathcal{P}_{\text{fin}}(H)$), and using that $X \in \mathcal{P}_{\text{fin}, \times}(H)$, pick $x \in X \cap H^\times$. Then, $x = u y v$ for some $u \in U$, $y \in Y$, and $v \in V$. So, by Proposition 2.30, y is a unit of H , because H is Dedekind-finite. It follows that $\mathcal{P}_{\text{fin}, \times}(H)$ is a divisor-closed submonoid of $\mathcal{P}_{\text{fin}}(H)$, and the rest is a consequence of Proposition 2.21.

(iv) Let $a = xy$ for some $x, y \in H \setminus H^\times$. Then $\{a\} = \{x\} \cdot \{y\}$ in $\mathcal{P}_{\text{fin}}(H)$, and we have by point (ii) that neither $\{x\}$ nor $\{y\}$ is a unit of $\mathcal{P}_{\text{fin}}(H)$. So, $\{a\}$ is not an atom of $\mathcal{P}_{\text{fin}}(H)$, which proves the “only if” part of the claim.

Now, assume that H is strongly unit-cancellative and $\{a\} = XY$ for some non-unit $X, Y \in \mathcal{P}_{\text{fin}}(H)$. Accordingly, suppose for a contradiction that $Y \subseteq H^\times$ (the case when $X \subseteq H^\times$ is similar). Then $|Y| \geq 2$,

because every one-element subset of H^\times is a unit of $\mathcal{P}_{\text{fin}}(H)$ by point (ii). In particular, there are $x \in H$ and $y_1, y_2 \in H^\times$ such that $y_1 \neq y_2$ and $a = xy_1 = xy_2$, viz., $xy_1y_2^{-1} = x$. This, however, is impossible, since H is strongly unit-cancellative.

So, putting it all together, neither X nor Y is a subset of H^\times , whence $a = xy$ for some $x \in X \setminus H^\times$ and $y \in Y \setminus H^\times$. To wit, a is not an atom of H .

(v) This is straightforward from points (ii) and (iv), together with the fact that, if H is cancellative, then $|XY| = 1$, for some $X, Y \subseteq H$, implies $|X| = |Y| = 1$. ■

Remark 3.3. (i) Proposition 3.2(i) suggests that the basic goal we are pursuing in this section (that is, the study of power monoids from the perspective of factorization theory) is, except for trivial cases, entirely beyond the scope of the factorization theory of *cancellative* monoids.

(ii) The power monoid of a linearly orderable monoid need not be atomic. In fact, let H be a commutative, linearly orderable, divisible monoid such that $H^\times \neq H$ (e.g., the additive monoid of the non-negative rational numbers). Then the set of atoms of H is empty (cf. Remark 2.23), and since $H \setminus H^\times$ is non-empty, we see that H is not atomic: This proves that, to some extent, Proposition 3.2(v) is sharp.

With the above in mind, we look for conditions such that $\mathcal{P}_{\text{fin}}(H)$ and $\mathcal{P}_{\text{fin},\times}(H)$ are BF-monoids, and to this end we make the following:

Definition 3.4. We say that a monoid H is *linearly orderable* if there exists a total order \preceq on H such that $xz \prec yz$ and $zx \prec zy$ for all $x, y, z \in H$ with $x \prec y$, in which case we call the pair (H, \preceq) a *linearly ordered monoid*.

Every submonoid of a linearly orderable monoid is still a linearly orderable monoid, and the same is true of any direct product (either finite or infinite) of linearly orderable monoids. An interesting variety of linearly orderable groups is provided by abelian torsion-free groups, as first proved by Levi in [40]. In a similar vein, Iwasawa [37], Mal'tsev [41], and Neumann [45] established, independently from each other, that torsion-free nilpotent groups are linearly orderable. Moreover, pure braid groups [48] and free groups [37] are linearly orderable, and so are some Baumslag-Solitar groups, which has led to interesting developments in connection to the study of sums of dilates in additive number theory, see [20, 19] and references therein. Further examples are discussed in [55, Appendix A] and [47, §1].

Proposition 3.5. *Let H be a linearly orderable monoid. Then:*

- (i) $|XY| \geq |X| + |Y| - 1$ for all $X, Y \in \mathcal{P}_{\text{fin}}(H)$.
- (ii) $\mathcal{P}_{\text{fin}}(H)$ and $\mathcal{P}_{\text{fin},\times}(H)$ are strongly unit-cancellative monoids.
- (iii) $\lambda_\times : \mathcal{P}_{\text{fin},\times}(H) \rightarrow \mathcal{P}_{\text{fin},\times}(H) : X \mapsto |X| - 1$ is a length function and $\mathcal{P}_{\text{fin},\times}(H)$ is a BF-monoid.
- (iv) $\mathcal{P}_{\text{fin}}(H)$ is a BF-monoid if and only if so is H .

Proof. To begin, let \preceq be a total order turning H into a linearly ordered monoid. Given $S \in \mathcal{P}_{\text{fin}}(H)$, we will denote by $S_\#$ and S^\sharp , respectively, the minimum and the maximum of S relative to \preceq (which are well defined, since every non-empty finite subset of a totally ordered set has a maximum and a minimum, and these are in fact unique).

(i) Fix $X, Y \in \mathcal{P}_{\text{fin}}(H)$. The claim is immediate if X or Y is a singleton, as linearly orderable monoids are cancellative. Otherwise, let x_1, \dots, x_m be the unique enumeration of X with $x_1 \prec \dots \prec x_m$ and, similarly, y_1, \dots, y_n the unique enumeration of Y with $y_1 \prec \dots \prec y_n$. Then it is clear that

$$x_1 y_1 \prec \dots \prec x_m y_1 \prec \dots \prec x_m y_n,$$

with the result that $|XY| \geq m + n - 1 = |X| + |Y| - 1$.

(ii) Let $X, Y \in \mathcal{P}_{\text{fin}}(H)$ such that $XY = X$ (the case when $YX = X$ is similar). Then $X_{\#} = (XY)_{\#} = X_{\#} \cdot Y_{\#}$ and $X^{\#} = X^{\#} \cdot Y^{\#}$, which is possible if and only if $Y_{\#} = Y^{\#} = 1_H$ (recall that H is cancellative). To wit, $XY = X$ only if $Y = \{1_H\}$. This implies that $\mathcal{P}_{\text{fin}}(H)$ is strongly unit-cancellative, and then so is $\mathcal{P}_{\text{fin}, \times}(H)$, since submonoids of strongly unit-cancellative monoids are strongly unit-cancellative.

(iii) Let $X, Y \in \mathcal{P}_{\text{fin}, \times}(H)$ such that $Y = UXV$, where $U, V \in \mathcal{P}_{\text{fin}, \times}(H)$ and at least one of U and V is not a unit. Then it follows from point (i) that

$$\lambda_{\times}(Y) = |Y| - 1 \geq |U| + |X| + |V| - 3 = \lambda_{\times}(U) + \lambda_{\times}(X) + \lambda_{\times}(V) \geq \lambda_{\times}(X),$$

and the last inequality is strict unless $\lambda_{\times}(U) = \lambda_{\times}(V) = 0$, that is, $|U| = |V| = 1$. So, knowing from Proposition 3.2(ii) that $\mathcal{P}_{\text{fin}, \times}(H)^{\times} = \{\{u\} : u \in H^{\times}\}$, we find $\lambda_{\times}(Y) > \lambda_{\times}(X)$.

In other terms, we have shown that λ_{\times} is a length function on $\mathcal{P}_{\text{fin}, \times}(H)$. Therefore, we conclude from Corollary 2.29 that $\mathcal{P}_{\text{fin}, \times}(H)$ is a BF-monoid.

(iv) The “only if” part is a consequence of Proposition 3.2(v), in combination with the cancellativity of H . As for the other direction, assume H is a BF-monoid and let λ be the function

$$\mathcal{P}_{\text{fin}}(H) \rightarrow \mathbf{N} : X \mapsto |X| + \sup \mathbf{L}_H(X^{\#}) - 1.$$

Note that λ is well defined, because $\mathbf{L}_H(x)$ is a finite subset of \mathbf{N} for every $x \in H$ (by the assumption that H is a BF-monoid). We want to prove that λ is a length function on $\mathcal{P}_{\text{fin}}(H)$, which, as in the proof of point (iii), will imply that $\mathcal{P}_{\text{fin}}(H)$ is a BF-monoid.

Indeed, let $X, Y \in \mathcal{P}_{\text{fin}}(H)$, and suppose that $Y = UXV$ for some $U, V \in \mathcal{P}_{\text{fin}}(H)$ with $U \notin \mathcal{P}_{\text{fin}}(H)^{\times}$ or $V \notin \mathcal{P}_{\text{fin}}(H)^{\times}$. In particular, we can assume (by symmetry) that $U \notin \mathcal{P}_{\text{fin}}(H)^{\times}$. By Proposition 3.2(ii), this means that either $|U| \geq 2$ or $U = \{x\}$ for some $x \notin H^{\times}$, and in both cases $|U| + \sup \mathbf{L}_H(U^{\#}) \geq 2$. Moreover, it is clear that $|V| + \sup \mathbf{L}_H(V^{\#}) \geq 1$. Therefore, we get from Remark 2.4 and point (i) that

$$\lambda(Y) \geq |U| + |X| + |V| + \sup \mathbf{L}_H(U^{\#}) + \sup \mathbf{L}_H(X^{\#}) + \sup \mathbf{L}_H(V^{\#}) - 3 > \lambda(X).$$

It follows that λ is a length function on $\mathcal{P}_{\text{fin}}(H)$, and this finishes the proof. ■

Corollary 3.6. $\mathcal{P}_{\text{fin}, 0}(\mathbf{N})$ is a strongly unit-cancellative, reduced, commutative BF-monoid.

Proof. It is a straightforward consequence of Propositions 3.2(ii) and 3.5(ii)-(iii), when considering that $(\mathbf{N}, +)$ is a linearly orderable, reduced, commutative monoid. ■

Remark 3.7. Let H be a monoid. As a complement to Proposition 3.5(iii), Antoniou and the second-named author have recently proved that $\mathcal{P}_{\text{fin}, \times}(H)$ is atomic if and only if $1_H \neq x^2 \neq x$ for every $x \in H \setminus \{1_H\}$, see [4, Theorems 3.9 and 4.9]; and is BF if and only if H is torsion-free, see [4, Theorem 3.11(iii)]. On the other hand, we do not know of any analogous characterization of when $\mathcal{P}_{\text{fin}}(H)$ is atomic, beside the case covered by Proposition 3.5(iv).

To conclude this section, we show that it is possible to understand some properties of $\mathcal{P}_{\text{fin},\times}(H)$, under suitable assumptions on the monoid H , from the study of $\mathcal{P}_{\text{fin},0}(\mathbf{N})$, with the advantage that the latter is, in a sense, easier to deal with than the former (cf. Remark 2.20).

Theorem 3.8. *Let H be a Dedekind-finite, non-torsion monoid. Then there exists a (monoid) homomorphism $\Phi : \mathcal{P}_{\text{fin},0}(\mathbf{N}) \rightarrow \mathcal{P}_{\text{fin},\times}(H)$ for which the following holds:*

- (c) *Given $X \in \mathcal{P}_{\text{fin},0}(\mathbf{N})$ and $Y_1, \dots, Y_n \in \mathcal{P}_{\text{fin},\times}(H)$ with $\Phi(X) = Y_1 \cdots Y_n$, there are $X_1, \dots, X_n \in \mathcal{P}_{\text{fin},0}(\mathbf{N})$ such that $X = X_1 + \cdots + X_n$ and $\Phi(X_i) \simeq_{\mathcal{P}_{\text{fin},\times}(H)} Y_i$ for every $i \in \llbracket 1, n \rrbracket$.*

In particular, Φ is an injective equimorphism, and hence we have that $\mathsf{L}_{\mathcal{P}_{\text{fin},0}(\mathbf{N})}(X) = \mathsf{L}_{\mathcal{P}_{\text{fin},\times}(H)}(\Phi(X))$ and $\mathsf{c}_{\mathcal{P}_{\text{fin},\times}(H)}(\Phi(X)) \leq \mathsf{c}_{\mathcal{P}_{\text{fin},0}(\mathbf{N})}(X)$ for every $X \in \mathcal{P}_{\text{fin},0}(\mathbf{N})$.

Proof. Using that H is non-torsion, fix $x_0 \in H$ with $\text{ord}_H(x_0) = \infty$, and let ϕ be the unique (monoid) homomorphism from $(\mathbf{N}, +)$ to H with $\phi(1) = x_0$. Of course, ϕ is a monomorphism, because $\phi(x) = \phi(y)$ for some $x, y \in \mathbf{N}$ with $x < y$ would imply $\{x_0^k : k \in \mathbf{N}^+\} \subseteq \{x_0^k : k \in \llbracket 0, y-1 \rrbracket\}$, in contradiction to the fact that $\text{ord}_H(x_0) = \infty$. Moreover, we can clearly lift ϕ to a monomorphism $\Phi : \mathcal{P}_{\text{fin},0}(\mathbf{N}) \rightarrow \mathcal{P}_{\text{fin},\times}(H)$ by taking $\Phi(X) := \{\phi(x) : x \in X\}$ for every $X \in \mathcal{P}_{\text{fin},0}(\mathbf{N})$.

To see that Φ satisfies condition (c), let $X \in \mathcal{P}_{\text{fin},0}(\mathbf{N})$ and $Y_1, \dots, Y_n \in \mathcal{P}_{\text{fin},\times}(H)$ such that $\Phi(X) = Y_1 \cdots Y_n$. Since ϕ is a homomorphism and $0 \in X$, there exist $u_1 \in Y_1, \dots, u_n \in Y_n$ for which $u_1 \cdots u_n = \phi(0) = 1_H$, and we get from Proposition 2.30 that $u_1, \dots, u_n \in H^\times$ (recall that, by hypothesis, H is Dedekind-finite). Set, for every $i \in \llbracket 1, n \rrbracket$,

$$Y'_i := u_0 \cdots u_{i-1} Y_i u_i^{-1} \cdots u_1^{-1}, \quad \text{with } u_0 := 1_H.$$

It is straightforward that $\Phi(X) = Y'_1 \cdots Y'_n$, and of course $Y'_i \simeq_{\mathcal{P}_{\text{fin},\times}(H)} Y_i$ for each $i \in \llbracket 1, n \rrbracket$. Further, $1_H \in \bigcap_{i=1}^n Y'_i$, with the result that $Y'_1, \dots, Y'_n \subseteq \Phi(X)$. Thus, since Φ is injective, there exist $X_1, \dots, X_n \subseteq X$ with $0 \in X_i$ and $\Phi(X_i) = Y'_i \simeq_{\mathcal{P}_{\text{fin},\times}(H)} Y_i$ for all $i \in \llbracket 1, n \rrbracket$. So $\Phi(X) = \Phi(X_1 + \cdots + X_n)$, and hence $X = X_1 + \cdots + X_n$ (again by the injectivity of Φ). To wit, Φ satisfies condition (c), as was desired.

We are left to show that Φ is an equimorphism, as all the rest will follow from points (i) and (iv) of Theorem 2.22. For, it is clear from the above that Φ satisfies conditions (E1) and (E3) of Definition 2.16. Therefore, it will be enough to prove that Φ is atom-preserving.

To this end, let $A \in \mathcal{A}(\mathcal{P}_{\text{fin},0}(\mathbf{N}))$, and assume first that $\Phi(A) = X'Y'$ for some $X', Y' \in \mathcal{P}_{\text{fin},\times}(H)$. Then, we derive from condition (c) that there are $X, Y \in \mathcal{P}_{\text{fin},0}(\mathbf{N})$ such that

$$\Phi(X) \simeq_{\mathcal{P}_{\text{fin},\times}(H)} X', \quad \Phi(Y) \simeq_{\mathcal{P}_{\text{fin},\times}(H)} Y', \quad \text{and} \quad A = X + Y,$$

which can only happen if one of X and Y is $\{0\}$, since $\mathcal{P}_{\text{fin},0}(\mathbf{N})$ is a reduced BF-monoid (Corollary 3.6) and A is an atom of $\mathcal{P}_{\text{fin},0}(\mathbf{N})$. Accordingly, $X' \simeq_{\mathcal{P}_{\text{fin},\times}(H)} \{1_H\}$ or $Y' \simeq_{\mathcal{P}_{\text{fin},\times}(H)} \{1_H\}$, and hence one of X' and Y' is a unit of $\mathcal{P}_{\text{fin},\times}(H)$.

On the other hand, suppose for a contradiction that $\Phi(A) \in \mathcal{P}_{\text{fin},\times}(H)^\times$. Then, we have by Proposition 3.2(ii) that $|\Phi(A)| = 1$. So A is a singleton (recall that Φ is injective), and hence $A = \{0\}$. This, however, is impossible, because A is an atom of $\mathcal{P}_{\text{fin},0}(\mathbf{N})$. \blacksquare

4. SOME ADDITIVE COMBINATORICS

We derive from Proposition 3.2 and Theorem 3.8 that, in many relevant cases, the arithmetic of power monoids is “controlled by the combinatorial structure” of the integers, as algebraically encoded by the restricted power monoid of $(\mathbf{N}, +)$, which we continue to denote by $\mathcal{P}_{\text{fin},0}(\mathbf{N})$ and to write additively (as in § 3). As a consequence, we are led here to consider various properties of (finite) subsets of \mathbf{N} that can or cannot be split into a sumset in a non-trivial way. We start by identifying some families of atoms of $\mathcal{P}_{\text{fin},0}(\mathbf{N})$.

Proposition 4.1. *Let $X, Y_1, \dots, Y_n \in \mathcal{P}_{\text{fin},0}(\mathbf{N})$ such that $X = Y_1 + \dots + Y_n$. We have:*

- (i) $Y_i \subseteq X$ for every $i \in \llbracket 1, n \rrbracket$.
- (ii) $L(q \cdot X) = L(X)$ for every $q \in \mathbf{N}^+$.
- (iii) If $X^+ \neq \emptyset$, then $\min X^+ \in Y_i$ for some $i \in \llbracket 1, n \rrbracket$.
- (iv) Every 2-element set in $\mathcal{P}_{\text{fin},0}(\mathbf{N})$ is an atom.
- (v) A 3-element set $A \in \mathcal{P}_{\text{fin},0}(\mathbf{N})$ is not an atom if and only if $A = \{0, x, 2x\}$ for some $x \in \mathbf{N}^+$.

Proof. (i)-(iii) are straightforward (we leave it as an exercise for the reader to fill in the details).

(iv) Let $x \in \mathbf{N}^+$ and assume that $\{0, x\} = X + Y$ for some $X, Y \in \mathcal{P}_{\text{fin},0}(\mathbf{N})$. Since $(\mathbf{N}, +)$ is a linearly orderable monoid, we get from Proposition 3.5(i) that $2 \geq |X| + |Y| - 1$, which is possible only if X or Y is a singleton. Together with Proposition 3.2(ii), this proves that $\{0, x\}$ is an atom of $\mathcal{P}_{\text{fin},0}(\mathbf{N})$.

(v) The “if” clause is trivial. As for the other direction, let $X, Y \in \mathcal{P}_{\text{fin},0}(\mathbf{N})$ such that $A := X + Y$ is a 3-element set, but neither X nor Y is a unit. Then it is easily seen from Propositions 3.2(ii) and 3.5(i) that $|X| = |Y| = 2$, i.e., $X = \{0, x\}$ and $Y = \{0, y\}$ for some $x, y \in \mathbf{N}^+$. It follows $A = \{0, x, y, x + y\}$, which is only possible if $x = y$ (because $|A| = 3$ and $1 \leq x, y < x + y$), so that $A = \{0, x, 2x\}$. ■

Proposition 4.2. *Let $d, \ell, q \in \mathbf{N}^+$ and $A \in \mathcal{P}_{\text{fin}}(\mathbf{N})$ such that $\min(d, \min A) > \ell q$ and $x \equiv y \pmod d$ for all $x, y \in A$. Then $(q \cdot \llbracket 0, \ell \rrbracket) \cup A \notin \mathcal{A}(\mathcal{P}_{\text{fin},0}(\mathbf{N}))$ if and only if $A = \{(\ell + k)q\}$ for some $k \in \llbracket 1, \lceil \ell/2 \rceil \rrbracket$.*

Proof. Set $B := (q \cdot \llbracket 0, \ell \rrbracket) \cup A$, and suppose first that $A = \{(\ell + k)q\}$ for some $k \in \llbracket 1, \lceil \ell/2 \rceil \rrbracket$. Then $k \leq \ell - k + 1$ and $B = \{0, qk\} + C$ with $C := (q \cdot \llbracket 0, \ell - k \rrbracket) \cup \{\ell q\}$. Therefore, B is not an atom of $\mathcal{P}_{\text{fin},0}(\mathbf{N})$, because it is the sum of two elements of $\mathcal{P}_{\text{fin},0}(\mathbf{N})$ both different from $\{0\}$ (recall that $\mathcal{P}_{\text{fin},0}(\mathbf{N})$ is a reduced monoid). So the “if” part of the statement is proved.

As for the other direction, let $B = X + Y$ for some non-zero $X, Y \in \mathcal{P}_{\text{fin},0}(\mathbf{N})$ (so, both X^+ and Y^+ are non-empty), and set $x_M := \max X$ and $y_M := \max Y$. By symmetry, we can assume $1 \leq x_M \leq y_M$.

We claim $y_M \leq \ell q$. Indeed, suppose the contrary, and define $x_m := \min X^+$. Then $y_M, x_m + y_M \in A$, which is only possible if $x_m \geq d \geq \ell q + 1$, since $x_m = (x_m + y_M) - y_M \geq 1$ and $x \equiv y \pmod d$ for all $x, y \in A$ (by hypothesis). In addition, points (i) and (iii) of Proposition 4.1 imply $q \in X \cup Y$ (note that $q = \min B^+$). So $x_m + q$ or $q + y_M$ is in $X + Y = B$, and hence in A (since $x_m + q$ and $q + y_M$ are both $\geq \ell q + 1$). This is however a contradiction, in that $q = (x_m + q) - x_m = (q + y_M) - y_M$ and $1 \leq q < d$, but any two distinct elements in A should have a distance $\geq d$.

It follows $B \subseteq \llbracket 0, x_M + y_M \rrbracket \subseteq \llbracket 0, 2\ell q \rrbracket$, hence $A \subseteq \llbracket \ell q + 1, 2\ell q \rrbracket$. Since $1 \leq 2\ell q - (\ell q + 1) < d$ and A is non-empty, we can therefore conclude $|A| = 1$ (using again that $a \equiv b \pmod d$ for all $a, b \in A$). On the other hand, $y_M \leq \ell q$ yields, along with Proposition 4.1(i), that $X, Y \subseteq q \cdot \llbracket 0, \ell \rrbracket$, hence $A \subseteq X + Y \subseteq q \cdot \mathbf{N}$.

So, putting it all together, we see that $A = \{(\ell + k)q\}$ for some $k \in \llbracket 1, \ell \rrbracket$. Suppose for a contradiction that $\lceil \ell/2 \rceil < k \leq \ell$. Then $k \geq 2$, and of course $x_M \geq kq$, otherwise we would obtain

$$(\ell + k)q = \max B = x_M + y_M < kq + \ell q,$$

which is impossible. Moreover, we claim that

$$X \cap \llbracket x_M - kq + 1, x_M - 1 \rrbracket = Y \cap \llbracket y_M - kq + 1, y_M - 1 \rrbracket = \emptyset. \quad (12)$$

In fact, if $x \in X \cap \llbracket x_M - kq + 1, x_M - 1 \rrbracket \neq \emptyset$ (the other case is similar), then $x + y_M, (\ell + k)q \in B$ (as was already noted, we have $(\ell + k)q = x_M + y_M$), and actually

$$(\ell + k)q > x + y_M \geq (\ell + k)q - kq + 1 = \ell q + 1.$$

We thus get $x + y_M, (\ell + k)q \in A$, which is impossible (since A is a singleton) and leads to (12).

Accordingly, we find that $X \subseteq \llbracket 0, x_M - kq \rrbracket \cup \{x_M\}$ and $Y \subseteq \llbracket 0, y_M - kq \rrbracket \cup \{y_M\}$, whence

$$q \cdot \llbracket 0, \ell \rrbracket = B \setminus \{(\ell + k)q\} = (X + Y) \setminus \{(\ell + k)q\} \subseteq (\llbracket 0, (\ell - k)q \rrbracket \cup \llbracket x_M, \ell q \rrbracket) \cap (q \cdot \mathbf{N}). \quad (13)$$

However, this is still a contradiction, because $x_M - (\ell - k)q \geq kq - (\ell - k)q = (2k - \ell)q \geq 2q$, with the result that at least one multiple of q in the interval $\llbracket 0, \ell q \rrbracket$ is missing from the right-most side of (13). ■

Proposition 4.3. *Let $A \in \mathcal{P}_{\text{fin},0}(\mathbf{N})$ and $b, c \in \mathbf{N}^+$, and assume $b \neq 2c$ and $2 \sup A < c < b - \sup A$. Then $A \cup (A + b) \cup \{c\}$ is an atom of $\mathcal{P}_{\text{fin},0}(\mathbf{N})$.*

Proof. Suppose to the contrary that $B := A \cup (A + b) \cup \{c\}$ is not an atom of $\mathcal{P}_{\text{fin},0}(\mathbf{N})$, i.e., there are $X, Y \in \mathcal{P}_{\text{fin},0}(\mathbf{N})$ such that $B = X + Y$ and $|X|, |Y| \geq 2$. We claim $c \in X \cup Y$.

Otherwise, $c = \bar{x} + \bar{y}$ for some $\bar{x} \in X^+$ and $\bar{y} \in Y^+$, and this can only happen if $\bar{x}, \bar{y} \in A$, because $X, Y \subseteq B$ and $\inf(A + b) = b > c$. It follows that $c = \bar{x} + \bar{y} \leq 2 \sup A$, which is a contradiction, since $2 \sup A < c$ (by hypothesis). Thus $c \in X \cup Y$ (as claimed), and by symmetry we can assume $c \in X$.

Then $Y^+ \subseteq (A + b) \cup \{c\}$, because the assumptions made on A , b , and c imply that $\sup A < c + a \leq c + \sup A < b$ for all $a \in A$. In turn, this yields $Y = \{0, c\}$, since $Y \cap (A + b) \neq \emptyset$ would imply

$$\sup B = \sup X + \sup Y \geq c + b > \sup(A + b) = \sup B,$$

which is, of course, impossible. So $B = X \cup (X + c)$, and therefore $X^+ \neq \emptyset$, because $\{0, b, c\} \subseteq B$ and $0 < c < b$ (whereas $X^+ = \emptyset$ would give $|B| = 2$). Accordingly, set $\bar{z} := \inf X^+$.

Then $\bar{z} + c \in B$, and actually $\bar{z} + c \in A + b$, as we see by considering that $\bar{z} + c > c > \sup A$. But this is only possible if $A^+ = \emptyset$; otherwise, we would get from the above and Proposition 4.1(iii) that $\bar{z} = \inf A^+$, and hence $\bar{z} + c \leq \sup A + c < b$, in contrast to the fact that $\bar{z} + c \in A + b$.

So putting it all together, we obtain that $B = \{0, b, c\}$, which, however, is still a contradiction, because $\{0, b, c\}$ is an atom, by Proposition 4.1(v) and the assumption that $2c \neq b > c$. ■

We will also need a series of lemmas, the last of which (Lemma 4.7) is of crucial importance for the goals that we are pursuing (as summarized in § 1.1).

Lemma 4.4. *Let $\alpha_1, \beta_1, \dots, \alpha_n, \beta_n \in \mathbf{N}$ and $u_1, \dots, u_n \in \mathbf{N}^+$ such that $\sum_{j=1}^i u_j \cdot \max(\alpha_j, \beta_j) < u_{i+1}$ for every $i \in \llbracket 1, n-1 \rrbracket$. Then $\sum_{i=1}^n \alpha_i u_i = \sum_{i=1}^n \beta_i u_i$ if and only if $\alpha_i = \beta_i$ for all $i \in \llbracket 1, n \rrbracket$.*

Proof. The “if” part is obvious. As for the other, assume $\sum_{i=1}^n \alpha_i u_i = \sum_{i=1}^n \beta_i u_i$, set $E := \{i \in \llbracket 1, n \rrbracket : \alpha_i \neq \beta_i\}$, and suppose for a contradiction that $E \neq \emptyset$. Accordingly, let $i_0 := \max E$; by symmetry, we can admit that $\alpha_{i_0} < \beta_{i_0}$. Then $\alpha_i = \beta_i$ for $i \in \llbracket i_0 + 1, n \rrbracket$, and we have $\sum_{i=1}^{i_0} \alpha_i u_i = \sum_{i=1}^{i_0} \beta_i u_i$. This is however impossible, since our assumptions imply that

$$\sum_{i=1}^{i_0} \alpha_i u_i \leq \sum_{i=1}^{i_0-1} \alpha_i u_i + (\beta_{i_0} - 1)u_{i_0} < \beta_{i_0} u_{i_0} \leq \sum_{i=1}^{i_0} \beta_i u_i. \quad \blacksquare$$

Lemma 4.5. *Given $u_1, \dots, u_{n+1} \in \mathbf{N}^+$ such that (a) $u_1 + \dots + u_i < \frac{1}{2}u_{i+1}$ for every $i \in \llbracket 1, n-1 \rrbracket$ and (b) $2u_n < u_{n+1}$, assume that $\sum_{i \in \mathcal{I}} u_i = \sum_{j \in \mathcal{J}} u_j + \sum_{k \in \mathcal{K}} u_k$ for some $\mathcal{I}, \mathcal{J}, \mathcal{K} \subseteq \llbracket 1, n+1 \rrbracket$. Then either $\mathcal{I} = \mathcal{J} \uplus \mathcal{K}$, or $n \in (\mathcal{J} \cap \mathcal{K}) \setminus \mathcal{I}$ and $n+1 \in \mathcal{I} \setminus (\mathcal{J} \cup \mathcal{K})$.*

Proof. Set $x := \sum_{j \in \mathcal{J}} u_j$, $y := \sum_{k \in \mathcal{K}} u_k$, and $z := \sum_{i \in \mathcal{I}} u_i$. We denote by δ_S , for a fixed $S \subseteq \mathbf{N}$, the function $\mathbf{N} \rightarrow \{0, 1\} \subseteq \mathbf{N}$ defined by $\delta_S(i) := 1$ if $i \in S$ and $\delta_S(i) := 0$ otherwise. Accordingly, for each $i \in \llbracket 1, n+1 \rrbracket$ we take $\alpha_i := \delta_{\mathcal{J}}(i)$, $\beta_i := \delta_{\mathcal{K}}(i)$, and $\gamma_i := \delta_{\mathcal{I}}(i)$; and we let $E := \{i \in \llbracket 1, n+1 \rrbracket : \alpha_i + \beta_i \neq \gamma_i\}$. We distinguish two cases:

CASE 1: $E = \emptyset$. We have $\alpha_i + \beta_i = \gamma_i$ for every $i \in \llbracket 1, n+1 \rrbracket$, which is clearly possible if and only if $\mathcal{I} = \mathcal{J} \uplus \mathcal{K}$ (in particular, note that $\gamma_i \leq 1 < 2 = \alpha_i + \beta_i$ for every $i \in \mathcal{J} \cap \mathcal{K}$).

CASE 2: $E \neq \emptyset$. Let $i_0 := \max E$. Since $\alpha_i + \beta_i = \gamma_i$ for $i \in \llbracket i_0 + 1, n+1 \rrbracket$, we have

$$\sum_{i=1}^{i_0} \gamma_i u_i = \sum_{i=1}^{i_0} (\alpha_i + \beta_i) u_i.$$

On the other hand, we derive from (a) and (b) that $u_1 + \dots + u_i < 2u_i < u_{i+1}$ for all $i \in \llbracket 1, n \rrbracket$. Thus, it is immediate that $\alpha_{i_0} + \beta_{i_0} < \gamma_{i_0}$; otherwise,

$$\sum_{i=1}^{i_0} (\alpha_i + \beta_i) u_i \geq (\gamma_{i_0} + 1)u_{i_0} > \gamma_{i_0} u_{i_0} + \sum_{i=1}^{i_0-1} u_i \geq \sum_{i=1}^{i_0} \gamma_i u_i,$$

a contradiction. So $\alpha_{i_0} = \beta_{i_0} = 0$ and $\gamma_{i_0} = 1$; moreover, we must have $i_0 = n+1$, or else

$$\sum_{i=1}^{i_0} (\alpha_i + \beta_i) u_i \leq (\gamma_{i_0} - 1)u_{i_0} + \sum_{i=1}^{i_0-1} (\alpha_i + \beta_i) u_i \leq (\gamma_{i_0} - 1)u_{i_0} + 2 \sum_{i=1}^{i_0-1} u_i \stackrel{(a)}{<} \gamma_{i_0} u_{i_0} \leq \sum_{i=1}^{i_0} \gamma_i u_i,$$

which is still impossible. It follows that $\gamma_n = 0$ and $\alpha_n = \beta_n = 1$, since

$$\begin{aligned} \gamma_n u_n + u_{n+1} &\leq \sum_{i=1}^{n+1} \gamma_i u_i = x + y \leq (\alpha_n + \beta_n)u_n + 2 \sum_{i=1}^{n-1} u_i \\ &\stackrel{(a)}{<} (\alpha_n + \beta_n + 1)u_n \stackrel{(b)}{<} u_n \cdot \min(\alpha_n, \beta_n) + u_{n+1}. \end{aligned}$$

To wit, $n \in (\mathcal{J} \cap \mathcal{K}) \setminus \mathcal{I}$ and $n+1 \in \mathcal{I} \setminus (\mathcal{J} \cup \mathcal{K})$. \blacksquare

Lemma 4.6. *Let $u_1, \dots, u_{n+1} \in \mathbf{N}^+$ such that (a) $u_1 + \dots + u_i < \frac{1}{2}u_{i+1}$ for every $i \in \llbracket 1, n-1 \rrbracket$ and (b) $2u_n < u_{n+1}$. Assume in addition that*

$$\sum_{i=1}^{n+1} \{0, u_i\} = X + Y, \quad \text{for some } X, Y \in \mathcal{P}_{\text{fin},0}(\mathbf{N}); \quad (14)$$

and set $I_X := \{i \in \llbracket 1, n+1 \rrbracket : u_i \in X\}$ and $I_Y := \{i \in \llbracket 1, n+1 \rrbracket : u_i \in Y\}$. The following hold:

- (i) $\llbracket 1, n+1 \rrbracket = I_X \uplus I_Y$.
- (ii) If $\sum_{j \in J} u_j \in X$ for some $J \subseteq \llbracket 1, n+1 \rrbracket$, then $J \setminus \{n\} \subseteq I_X$ (and similarly for Y).
- (iii) If $\sum_{j \in J} u_j \in X$, $\sum_{k \in K} u_k \in Y$, and $\sum_{i \in I} u_i = \sum_{j \in J} u_j + \sum_{k \in K} u_k$ for some $I, J, K \subseteq \llbracket 1, n+1 \rrbracket$, then either $I = J \uplus K$; or $n \notin I$, $J \cap K = \{n\}$, and $n+1 \in I \setminus (J \cup K)$.

Proof. (i) As in the proof of Lemma 4.5, it is easy to derive from conditions (a) and (b) that

$$u_i \leq u_1 + \cdots + u_i < 2u_i < u_{i+1}, \quad \text{for all } i \in \llbracket 1, n \rrbracket. \quad (15)$$

Consequently, we see (from (14)) that $2u_i \notin X + Y$, and hence $u_i \notin X \cap Y$, for all $i \in \llbracket 1, n+1 \rrbracket$.

Besides that, let $i_0 \in \llbracket 1, n \rrbracket$. Since $u_{i_0} \in X + Y$, there are $\mathcal{J}, \mathcal{K} \subseteq \llbracket 1, n+1 \rrbracket$ with $x := \sum_{j \in \mathcal{J}} u_j \in X$, $y := \sum_{k \in \mathcal{K}} u_k \in Y$, and $x + y = u_{i_0}$. Thus, we obtain from Lemma 4.5 (applied with $\mathcal{I} = \{i_0\}$, $\mathcal{J} = J$, and $\mathcal{K} = K$) that $J \uplus K = \{i_0\}$, which is only possible if $J = \emptyset$ or $K = \emptyset$, namely, $u_{i_0} \in X \cup Y$. This, together with (15), shows that

$$\llbracket 1, n \rrbracket \subseteq I_X \cup I_Y \quad \text{and} \quad I_X \cap I_Y = \emptyset.$$

In particular, we can assume (without loss of generality) that $u_n \in X$, and it only remains to prove that $n+1 \in I_X \cup I_Y$. For, suppose the contrary and set $U := \{\sum_{i \in I} u_i : I \subseteq \llbracket 1, n-1 \rrbracket\}$. We distinguish two cases.

CASE 1: $Y \cap (U + u_n) = \emptyset$. Because $u_{n+1} \in (X + Y) \setminus (X \cup Y)$, we must have that $x + y = u_{n+1}$ for some $x \in X$ and $y \in Y$ with $x, y < u_{n+1}$. So we obtain that

$$u_{n+1} = x + y \stackrel{(15)}{\leq} \sum_{i=1}^n u_i + \sum_{i=1}^{n-1} u_i = u_n + 2 \sum_{i=1}^{n-1} u_i \stackrel{(a)}{<} 2u_n \stackrel{(b)}{<} u_{n+1},$$

which is impossible and completes the analysis of the present case.

CASE 2: $Y \cap (U + u_n) \neq \emptyset$. Since $u_n + u_{n+1} \in X + Y$ and $u_{n+1} \notin X \cup Y$, there exist two index sets $J, K \subseteq \llbracket 1, n+1 \rrbracket$, none of which is equal to $\{n+1\}$, such that $x := \sum_{j \in J} u_j \in X$, $y := \sum_{k \in K} u_k \in Y$, and $x + y = u_n + u_{n+1}$. It follows that $n+1 \in J \cup K$; otherwise,

$$x + y \leq 2 \sum_{i=1}^n u_i = 2u_n + 2 \sum_{i=1}^{n-1} u_i \stackrel{(b)}{<} u_{n+1} + 2 \sum_{i=1}^{n-1} u_i \stackrel{(a)}{<} u_{n+1} + u_n,$$

a contradiction. Therefore, we apply Lemma 4.5 (with $\mathcal{I} = \{n, n+1\}$, $\mathcal{J} = J$, and $\mathcal{K} = K$) to find that $\{n, n+1\} = J \uplus K$. On the other hand, recalling that $u_n \in X$ and $Y \cap (U + u_n) \neq \emptyset$, and taking K_0 to be any subset of $\llbracket 1, n+1 \rrbracket$ such that $n \in K_0$ and $\sum_{k \in K_0} u_k \in Y$, we get again from Lemma 4.5 (applied first with $\mathcal{J} = J$ and $\mathcal{K} = K_0$, then with $\mathcal{J} = \{n\}$ and $\mathcal{K} = K$) that neither J nor K can be equal to $\{n, n+1\}$. But since $\{n, n+1\} = J \uplus K$, this is only possible if $J = \{n+1\}$ or $K = \{n+1\}$, and hence $u_{n+1} \in X \cup Y$, which is still a contradiction.

(ii) Suppose that $x := \sum_{j \in J} u_j \in X$ for some $J \subseteq \llbracket 1, n+1 \rrbracket$, but $J \setminus \{n\} \not\subseteq I_X$, i.e., there exists an index $i \in J \setminus \{n\}$ such that $i \notin I_X$. Then $i \in I_Y$, by point (i). So $x + u_i \in X + Y$, in contradiction to Lemma 4.5 (applied with $\mathcal{J} = J$ and $\mathcal{K} = \{i\}$).

(iii) Set $x := \sum_{j \in J} u_j$ and $y := \sum_{k \in K} u_k$, and assume that $\sum_{i \in I} u_i = x + y$, but $I \neq J \uplus K$. Then Lemma 4.5 (applied with $\mathcal{I} = I$, $\mathcal{J} = J$, and $\mathcal{K} = K$) yields $n \in (J \cap K) \setminus I$ and $n+1 \in I \setminus (J \cup K)$. It

thus follows from (ii) that $J \setminus \{n\} \subseteq I_X$ and $K \setminus \{n\} \subseteq I_Y$. On the other hand, we know from (i) that $I_X \uplus I_Y = \llbracket 1, n+1 \rrbracket$. So, putting it all together, we can conclude that $J \cap K = \{n\}$. ■

Lemma 4.7. *Let $u_1, \dots, u_{n+1} \in \mathbb{N}^+$ be given so that (a) $u_1 + \dots + u_n \leq u_{n+1} - u_n$, (b) $2u_n \neq u_{n+1}$, and (c) $u_1 + \dots + u_i < \frac{1}{2}u_{i+1}$ for all $i \in \llbracket 1, n-1 \rrbracket$. Next, let $X, Y \in \mathcal{P}_{\text{fin},0}(\mathbb{N})$ such that*

$$\{0, u_1\} + \dots + \{0, u_{n+1}\} = X + Y, \quad (16)$$

and set $I_X := \{i \in \llbracket 1, n+1 \rrbracket : u_i \in X\}$ and $I_Y := \{i \in \llbracket 1, n+1 \rrbracket : u_i \in Y\}$. The following hold:

- (i) $X \setminus \{u_1 + \dots + u_n\} = \sum_{i \in I_X} \{0, u_i\}$ and $Y \setminus \{u_1 + \dots + u_n\} = \sum_{i \in I_Y} \{0, u_i\}$.
- (ii) If $X \neq \sum_{i \in I_X} \{0, u_i\}$ or $Y \neq \sum_{i \in I_Y} \{0, u_i\}$, then $n \geq 2$, $u_1 + \dots + u_n = u_{n+1} - u_n$, and one of X and Y is equal to $\{0, u_n\}$.

Proof. To start with, we note for future reference that conditions (a)-(c) yield

$$u_1 + \dots + u_i < 2u_i < u_{i+1} \quad \text{for all } i \in \llbracket 1, n \rrbracket, \quad (17)$$

and for the sake of notation we set

$$U := \sum_{i=1}^{n+1} \{0, u_i\}, \quad U^* := \sum_{i=1}^{n-1} \{0, u_i\}, \quad U' := U^* + \{0, u_n\}, \quad \text{and} \quad U'' := U^* + \{0, u_{n+1}\}.$$

To ease the exposition, we break up the proof into a series of claims. We will often use without comment that $X, Y \subseteq U$, as is implied by Proposition 4.1(i). Moreover, we assume, based on Lemma 4.6(i), that $u_n \in X$ (as the statements to be proved are symmetric with respect to X and Y).

CLAIM A. *Assume that $Y \cap (U'' + u_n) \neq \emptyset$. Then the following hold:*

- (A1) $n \geq 2$, $Y \cap (U'' + u_n) = \{u_1 + \dots + u_n\} = \{u_{n+1} - u_n\}$, and $\llbracket 1, n-1 \rrbracket \subseteq I_Y$.
- (A2) $X = \{0, u_n\}$ and $I_Y = \llbracket 1, n+1 \rrbracket \setminus \{n\}$.

Proof of Claim A. (A1) Let $K \subseteq \llbracket 1, n+1 \rrbracket$ such that $n \in K$ and take $y := \sum_{k \in K} u_k \in Y$. Since $u_n \in X$, we get from Lemma 4.6(iii) (applied with $\mathcal{J} = \{n\}$ and $\mathcal{K} = K$) that $K \subseteq \llbracket 1, n \rrbracket$ and $u_n + y \geq u_{n+1}$. So, it follows from condition (a) that $u_n + y = u_{n+1}$, which is only possible if $n \geq 2$ (recall that $2u_n \neq u_{n+1}$) and $K = \llbracket 1, n \rrbracket$, i.e., $y = u_1 + \dots + u_n$. Then $\llbracket 1, n-1 \rrbracket \subseteq I_Y$, by Lemma 4.6(ii).

(A2) Let $x \in X^+$. Then $x = \sum_{j \in J} u_j \in X$ for some non-empty $J \subseteq \llbracket 1, n+1 \rrbracket$, and we get from Lemma 4.6(iii) (applied with $\mathcal{J} = J$ and $\mathcal{K} = \llbracket 1, n \rrbracket$) that $J \cap \llbracket 1, n \rrbracket = \emptyset$ or $n \in J \subseteq \llbracket 1, n \rrbracket$. In particular, the maximum of X is $\leq u_{n+1}$, and hence $X \setminus \{u_{n+1}\} \subseteq U'$, because $J \cap \llbracket 1, n \rrbracket = \emptyset$ only if $J = \{n+1\}$.

Suppose that $J = \{n+1\}$, namely, $u_{n+1} \in X$. Then Lemma 4.6(iii) yields $Y \cap (U' + u_{n+1}) = \emptyset$, and we find that $X + Y \subseteq (U' + Y) \cup (X + U^*) \cup (u_1 + \dots + u_{n+1})$, for we know from (A1) that $n \geq 2$ and $Y \setminus \{u_1 + \dots + u_n\} \subseteq U^*$. On the other hand, we see that

$$\max(U' + Y) = 2(u_1 + \dots + u_n) \stackrel{(A1)}{=} u_{n+1} + \sum_{i=1}^{n-1} u_i = \max(X + U^*) \stackrel{(17)}{<} u_{n+1} + u_n,$$

and it is clear that $u_n + u_{n+1} < u_1 + \dots + u_{n+1}$ (because $n \geq 2$). Thus $u_n + u_{n+1} \notin X + Y = U$, which is, however, a contradiction. So, putting it all together, we must conclude that $n \in J \subseteq \llbracket 1, n \rrbracket$.

But we have from Lemma 4.6(ii) and (A2) that $J \setminus \{n\} \subseteq I_X$ and $\llbracket 1, n-1 \rrbracket \subseteq I_Y$; and from Lemma 4.6(i) that $I_X \uplus I_Y = \llbracket 1, n+1 \rrbracket$. So $J = \{n\}$, and since x was an arbitrary element in X^+ and we are assuming that $u_n \in X$, it follows that $X = \{0, u_n\}$ and $I_Y = \llbracket 1, n+1 \rrbracket \setminus \{n\}$. ■

CLAIM B. *Let $J, K \subseteq \llbracket 1, n+1 \rrbracket$ such that $\sum_{j \in J} u_j \in X$ and $\sum_{k \in K} u_k \in Y$. Then one (and only one) of the following two cases occurs:*

- (B1) $J \subseteq I_X$, $K \subseteq I_Y$, and $J \cap K = \emptyset$.
- (B2) $J \subseteq I_X = \{n\}$, $K = \llbracket 1, n \rrbracket$, and conditions (A1) and (A2) of Claim A are satisfied.

Proof of Claim B. Set $x := \sum_{j \in J} u_j$ and $y := \sum_{k \in K} u_k$. We distinguish two cases:

CASE 1: $K \subseteq I_Y$. We prove $J \cap I_Y = \emptyset$; this will give $J \subseteq I_X$ and $J \cap K = \emptyset$, since $J \subseteq \llbracket 1, n+1 \rrbracket$ and, by Lemma 4.6(i), $I_X \uplus I_Y = \llbracket 1, n+1 \rrbracket$. For, assume to the contrary that $J \cap I_Y$ is non-empty, and let $i_0 \in J \cap I_Y$. Then we infer from Lemma 4.6(iii) (applied with $\mathcal{J} = J$ and $\mathcal{K} = \{i_0\}$) that $i_0 = n$, and hence $u_n \in Y$, in contradiction to Claim A.

CASE 2: $K \not\subseteq I_Y$. Since $K \subseteq \llbracket 1, n+1 \rrbracket$ and, by Lemma 4.6(i), $I_X \uplus I_Y = \llbracket 1, n+1 \rrbracket$, it is clear that $I_X \cap K \neq \emptyset$. Let $i_0 \in I_X \cap K$. Then Lemma 4.6(iii) (applied with $\mathcal{J} = \{i_0\}$ and $\mathcal{K} = K$) yields $i_0 = n$, which implies by Claim A that $X = \{0, u_n\}$ and $Y \cap (U^* + u_n) = \{u_1 + \dots + u_n\}$. So $J \subseteq I_X = \{n\}$ and $y = u_1 + \dots + u_n$, and by (17) and Lemma 4.4 this is possible only if $K = \llbracket 1, n \rrbracket$. ■

CLAIM C. *Given $I \subseteq \llbracket 1, n+1 \rrbracket$, there exist $J, K \subseteq \llbracket 1, n+1 \rrbracket$ for which $\sum_{j \in J} u_j \in X$, $\sum_{k \in K} u_k \in Y$, and $\sum_{i \in I} u_i = \sum_{j \in J} u_j + \sum_{k \in K} u_k$. Moreover, one (and only one) of the following holds:*

- (C1) $J \uplus K = I$, $J \subseteq I_X$, and $K \subseteq I_Y$.
- (C2) $J \subseteq I_X = \{n\}$ and $K = \llbracket 1, n \rrbracket$.

Proof of Claim C. Set $z := \sum_{i \in I} u_i$. Then $z \in X + Y = U$, and hence there exist $J, K \subseteq \llbracket 1, n+1 \rrbracket$ such that $x := \sum_{j \in J} u_j \in X$, $y := \sum_{k \in K} u_k \in Y$, and $z = x + y$. If $K \subseteq I_Y$, then $J \cap K = \emptyset$ and $J \subseteq I_X$ by point (B1) of Claim B, hence $J \uplus K = I$ by Lemma 4.5 (applied with $\mathcal{I} = I$, $\mathcal{J} = J$, and $\mathcal{K} = K$). Otherwise, point (B2) of Claim B yields $J \subseteq I_X = \{n\}$ and $K = \llbracket 1, n \rrbracket$. ■

CLAIM D. $\sum_{i \in \mathcal{I}_X} u_i \in X$ for every $\mathcal{I}_X \subseteq I_X$, and $\sum_{i \in \mathcal{I}_Y} u_i \in Y$ for every $\mathcal{I}_Y \subseteq I_Y$.

Proof of Claim D. We just prove the statement relative to X , as the other is similar. For, let $I \subseteq I_X$, and set $z := \sum_{i \in I} u_i$. The claim is obvious if $|I| \leq 1$ (by the very definition of I_X), so assume $|I| \geq 2$.

Since $z \in U = X + Y$, there exist $J, K \subseteq \llbracket 1, n+1 \rrbracket$ such that $x := \sum_{j \in J} u_j \in X$, $y := \sum_{k \in K} u_k \in Y$, and $z = x + y$. Because $|I_X| \geq |I| \geq 2$, we thus obtain from Claim C that $J \uplus K = I$ and $K \subseteq I_Y$. But this is possible only if $K = \emptyset$, because $I_X \cap I_Y = \emptyset$ by Lemma 4.6(i) and $K \subseteq I \subseteq I_X$. So $I = J$, and hence $z = x \in X$. ■

With all this in hand, we are ready to conclude. In fact, we get from Claim C that

$$X \subseteq \sum_{i \in I_X} \{0, u_i\} \quad \text{and} \quad Y \setminus \{u_1 + \dots + u_n\} \subseteq \sum_{i \in I_Y} \{0, u_i\},$$

and from Claim D that

$$\sum_{i \in I_X} \{0, u_i\} \subseteq X \quad \text{and} \quad \sum_{i \in I_Y} \{0, u_i\} \subseteq Y \setminus \{u_1 + \dots + u_n\},$$

with the result that $X = \sum_{i \in I_X} \{0, u_i\}$ and $Y \setminus \{u_1 + \cdots + u_n\} = \sum_{i \in I_Y} \{0, u_i\}$. This proves point (i), while (ii) follows from Claim A (recall that we are assuming without loss of generality that $u_n \in X$). ■

The next step is to determine the set of lengths of X for some special choices of the set $X \in \mathcal{P}_{\text{fin},0}(\mathbf{N})$. Consistently with the notation introduced in § 2.1.2 (in the special case of reduced, commutative monoids), we will identify a word $\mathbf{c} \in \mathcal{F}(\mathcal{A}(\mathcal{P}_{\text{fin},0}(\mathbf{N})))$ with the congruence class $[\mathbf{c}]_{\mathcal{C}_{\mathcal{P}_{\text{fin},0}(\mathbf{N})}}$.

Proposition 4.8. $L([0, n]) = [2, n]$ for every $n \geq 2$.

Proof. As was noted before, $\mathcal{P}_{\text{fin},0}(\mathbf{N})$ is a reduced BF-monoid. So the claim is trivial if $n = 2$, because if $[0, 2] = X + Y$ for some $X, Y \subseteq \mathcal{P}_{\text{fin},0}(\mathbf{N}) \setminus \{\{0\}\}$, then it is clear that $X = Y = [0, 1]$.

Accordingly, suppose the claim is true for a fixed $n \geq 2$, and observe that $[0, n+1] = [0, 1] + [0, n]$. Since $L(X) + L(Y) \subseteq L(X + Y)$ for all $X, Y \in \mathcal{P}_{\text{fin},0}(\mathbf{N})$, it follows that

$$L([0, n+1]) \supseteq 1 + L([0, n]) = [3, n+1]. \quad (18)$$

On the other hand, let $A := \{0, 2\}$ if $n = 2$ and $A := \{0, 1\} \cup \{k \in [2, n] : k \equiv n \pmod{2}\}$ otherwise. Then A is an atom by Propositions 4.1(iv) and 4.2 (apply the latter with $d = 2$ and $\ell = q = 1$), and we have $[0, n+1] = \{0, 1\} + A$, which implies, together with (18), that $[2, n+1] \subseteq L([0, n+1])$.

So we are done, since $(\mathbf{N}, +)$ is a linearly orderable monoid, and therefore we get from Theorem 2.28(iv) and Proposition 3.5(iii) that $\sup L([0, n+1]) \leq |[0, n+1]| - 1 = n+1$. ■

Proposition 4.9. Let $v_1, \dots, v_\ell \in \mathbf{N}^+$ such that $v_1 + \cdots + v_i < \frac{1}{2}v_{i+1}$ for every $i \in [1, \ell-2]$ and, if $\ell \geq 2$, $v_1 + \cdots + v_{\ell-1} < v_\ell - v_{\ell-1}$. Then $Z(\{0, v_1\} + \cdots + \{0, v_\ell\}) = \{\{0, v_1\} * \cdots * \{0, v_\ell\}\}$ in $\mathcal{P}_{\text{fin},0}(\mathbf{N})$.

Proof. If $\ell = 1$, the conclusion is trivial, since every two-element set in $\mathcal{P}_{\text{fin},0}(\mathbf{N})$ is an atom by Proposition 4.1(iv). So let $\ell \geq 2$ and assume that the following condition is verified:

- (H) If $t \in [1, \ell-1]$ and $x_1, \dots, x_t \in \mathbf{N}^+$ are such that $x_1 + \cdots + x_i < \frac{1}{2}x_{i+1}$ for all $i \in [1, t-2]$ and, when $t \geq 2$, $x_1 + \cdots + x_{t-1} < x_t - x_{t-1}$, then $Z(\{0, x_1\} + \cdots + \{0, x_t\}) = \{\{0, x_1\} * \cdots * \{0, x_t\}\}$.

Next, suppose that $V := \sum_{i=1}^\ell \{0, v_i\} = X + Y$ for some non-unit $X, Y \in \mathcal{P}_{\text{fin},0}(\mathbf{N})$, and set

$$I_X := \{i \in [1, \ell] : v_i \in X\} \quad \text{and} \quad I_Y := \{i \in [1, \ell] : v_i \in Y\}.$$

By Lemma 4.7 (applied with $n = \ell - 1$ and $u_1 = v_1, \dots, u_{n+1} = v_\ell$), we see that

$$X = \sum_{i \in I_X} \{0, v_i\}, \quad Y = \sum_{i \in I_Y} \{0, v_i\}, \quad \text{and} \quad I_X \uplus I_Y = [1, \ell]. \quad (19)$$

In particular, $\emptyset \neq I_X, I_Y \subsetneq [1, \ell]$, because X and Y are both different from $\{0\}$.

Put $m := |I_X|$, and let i_1, \dots, i_m be the natural enumeration of I_X . Since v_{i_1}, \dots, v_{i_m} is a subsequence of v_1, \dots, v_ℓ , we have $v_{i_1} + \cdots + v_{i_k} < \frac{1}{2}v_{i_{k+1}}$ for all $k \in [1, m-2]$ and, for $m \geq 2$, $v_{i_1} + \cdots + v_{i_{m-1}} < v_{i_m} - v_{i_{m-1}}$. Therefore, we derive from condition (H) that $Z(X) = \{\{0, v_{i_1}\} * \cdots * \{0, v_{i_m}\}\}$. Likewise, if $n := |I_Y|$ and j_1, \dots, j_n is the natural enumeration of I_Y , then $Z(Y) = \{\{0, v_{j_1}\} * \cdots * \{0, v_{j_n}\}\}$.

So, putting it all together and recalling from (19) that $I_X \uplus I_Y = [1, \ell]$, we conclude by Lemma 2.5 that $Z(V) = \{\{0, v_1\} * \cdots * \{0, v_\ell\}\}$. ■

Proposition 4.10. *Let $n \in \mathbb{N}_{\geq 2}$, and let $u_1, \dots, u_{n+1} \in \mathbf{N}^+$ such that (a) $u_1 + \dots + u_n = u_{n+1} - u_n$ and (b) $u_1 + \dots + u_i < \frac{1}{2}u_{i+1}$ for every $i \in \llbracket 1, n-1 \rrbracket$. Set*

$$U := \{0, u_1\} + \dots + \{0, u_{n+1}\} \quad \text{and} \quad A := \left\{ \sum_{i \in I} u_i : I \subseteq \llbracket 1, n-1 \rrbracket \right\}.$$

Then the following hold:

- (i) $B := A \cup (A + u_{n+1}) \cup \{u_1 + \dots + u_n\} \in \mathcal{A}(\mathcal{P}_{\text{fin},0}(\mathbf{N}))$ and $|B| \geq 3$.
- (ii) $Z(U) = \{\{0, u_n\} * B, \{0, u_1\} * \dots * \{0, u_{n+1}\}\}$.

In particular, $\mathbf{L}(U) = \{2, n+1\}$, $\Delta(U) = \{n-1\}$, and $\mathbf{c}(U) = n$.

Proof. The “In particular” part of the statement is a straightforward consequence of point (ii), so we can definitely focus on the proof of (i) and (ii).

(i) Clearly $|B| \geq 3$, and hence $B \neq \{0, u_i\}$ for every $i \in \llbracket 1, n+1 \rrbracket$, because $\{0, u_1, u_1 + \dots + u_n\} \in B$ and $0 < u_1 < u_1 + \dots + u_n$ (here we use that $n \geq 2$). Moreover, we have

$$2 \sup A = 2(u_1 + \dots + u_{n-1}) \stackrel{(b)}{<} u_n \leq u_1 + \dots + u_n \stackrel{(a)}{=} u_{n+1} - u_n \stackrel{(b)}{<} u_{n+1} - \sup A.$$

Therefore, we infer from Proposition 4.3 (applied with $b = u_{n+1}$ and $c = u_1 + \dots + u_n$) that B is an atom of $\mathcal{P}_{\text{fin},0}(\mathbf{N})$, since it is clear from (a) that $2(u_1 + \dots + u_n) - u_{n+1} =$

(ii) Observe that U is not an atom of $\mathcal{P}_{\text{fin},0}(\mathbf{N})$, and recall that $\mathcal{P}_{\text{fin},0}(\mathbf{N})$ is a reduced, commutative BF-monoid (by Corollary 3.6). Accordingly, let $U = X + Y$ for some non-unit $X, Y \in \mathcal{P}_{\text{fin},0}(\mathbf{N})$, and set

$$Z(X, Y) := \{\mathbf{a} * \mathbf{b} : (\mathbf{a}, \mathbf{b}) \in Z(X) \times Z(Y)\} \subseteq Z(\mathcal{P}_{\text{fin},0}(\mathbf{N})).$$

Moreover, take $I_X := \{i \in \llbracket 1, n+1 \rrbracket : u_i \in X\}$ and $I_Y := \{i \in \llbracket 1, n+1 \rrbracket : u_i \in Y\}$. By Lemma 4.7, we have $I_X \uplus I_Y = \llbracket 1, n+1 \rrbracket$, and there are only two cases:

CASE 1: $X = \{0, u_n\}$ and $Y = B$ (up to rearrangement). By Proposition 4.1(iv) and point (i), both X and Y are atoms, hence $Z(X, Y) = \{\{0, u_n\} * B\}$.

CASE 2: $X = \sum_{i \in I_X} \{0, u_i\}$ and $Y = \sum_{i \in I_Y} \{0, u_i\}$. Let i_1, \dots, i_h be the natural enumeration of I_X and j_1, \dots, j_k the natural enumeration of I_Y , where $h := |I_X|$ and $k := |I_Y|$ (it is clear that $h, k \in \mathbf{N}^+$, because $X, Y \neq \{0\}$). Since u_{i_1}, \dots, u_{i_h} is a *proper* subsequence of u_1, \dots, u_{n+1} , it holds

$$u_{i_1} + \dots + u_{i_s} < \frac{1}{2}u_{i_{s+1}}, \quad \text{for all } s \in \llbracket 1, h-2 \rrbracket,$$

and

$$u_{i_1} + \dots + u_{i_{h-1}} < u_{i_h} - u_{i_{h-1}}, \quad \text{for } h \geq 2.$$

So, we get from Proposition 4.9 (applied with $\ell = h$ and $v_1 = u_{i_1}, \dots, v_\ell = u_{i_h}$) that $Z(X) = \{\{0, u_{i_1}\} * \dots * \{0, u_{i_h}\}\}$. And in a similar way, we obtain that $Z(Y) = \{\{0, u_{j_1}\} * \dots * \{0, u_{j_k}\}\}$. Hence, using that $\llbracket 1, n+1 \rrbracket = \{i_1, \dots, i_h\} \uplus \{j_1, \dots, j_k\}$, we find $Z(X, Y) = \{\{0, u_1\} * \dots * \{0, u_{n+1}\}\}$.

We are now in the position to finish the proof of point (ii), as we infer from the above and Lemma 2.5 that $Z(U) = \{\{0, u_n\} * B, \{0, u_1\} * \dots * \{0, u_{n+1}\}\}$. ■

Finally, we have all the ingredients we need to prove the main result of this section.

Theorem 4.11. *Let H be a Dedekind-finite, non-torsion monoid. Then:*

- (i) $\mathcal{L}(\mathcal{P}_{\text{fin}}(H)) \supseteq \mathcal{L}(\mathcal{P}_{\text{fin},\times}(H)) \supseteq \mathcal{L}(\mathcal{P}_{\text{fin},0}(\mathbf{N}))$.
- (ii) $\mathcal{U}_k(\mathcal{P}_{\text{fin}}(H)) = \mathcal{U}_k(\mathcal{P}_{\text{fin},\times}(H)) = \mathcal{U}_k(\mathcal{P}_{\text{fin},0}(\mathbf{N})) = \mathbf{N}_{\geq 2}$ for every $k \geq 2$.
- (iii) $\Delta(\mathcal{P}_{\text{fin}}(H)) = \Delta(\mathcal{P}_{\text{fin},\times}(H)) = \Delta(\mathcal{P}_{\text{fin},0}(\mathbf{N})) = \mathbf{N}^+$.
- (iv) $\text{Ca}(\mathcal{P}_{\text{fin}}(H)) \supseteq \text{Ca}(\mathcal{P}_{\text{fin},\times}(H)) \supseteq \text{Ca}(\mathcal{P}_{\text{fin},0}(\mathbf{N})) = \mathbf{N}^+$.

In particular, if H is a linearly orderable BF-monoid, then the inclusions in point (iv) are equalities.

Proof. To ease notation, we will write P in place of $\mathcal{P}_{\text{fin},\times}(H)$ and P_0 in place of $\mathcal{P}_{\text{fin},0}(\mathbf{N})$.

Clearly, (i) follows from Theorem 3.8 and Proposition 3.2(iii); (ii) from (i) and Proposition 4.8; and (iii) from (i) and Proposition 4.10. As for (iv), we need some more work.

To start with, we get from Proposition 4.10 that $\mathbf{N}_{\geq 2} \subseteq \text{Ca}(P_0)$, and since P_0 is a BF-monoid, it is evident that $\text{Ca}(P_0) \subseteq \mathbf{N}^+$. This yields $\text{Ca}(P_0) = \mathbf{N}^+$, as it is easy to check that

$$Z([0, 6] \setminus \{4\}) = \{\{0, 1\} * \{0, 2, 5\}, \{0, 1\} * \{0, 1, 2, 5\}\} \subseteq Z(P_0). \quad (20)$$

On the other hand, Proposition 3.2(iii) yields $\text{Ca}(P) \subseteq \text{Ca}(\mathcal{P}_{\text{fin}}(H))$. So we are left to show that $\text{Ca}(P_0) \subseteq \text{Ca}(P)$, as the “In particular” part of the statement is a consequence of (iv) and Proposition 3.5.

For, pick $n \in \mathbf{N}^+$ and let Φ be the same homomorphism of Theorem 3.8. We set $U_n := [0, 6] \setminus \{4\}$ if $n = 1$; and $U_n := \sum_{i=1}^{n+1} \{0, u_i\}$ otherwise, where $u_1, \dots, u_{n+1} \in \mathbf{N}^+$, $u_1 + \dots + u_n = u_{n+1} - u_n$, and $u_1 + \dots + u_i < \frac{1}{2}u_{i+1}$ for every $i \in [1, n-1]$. Also, we define $c_n := c_{P_0}(U_n)$ and $c_n^* := c_P(\Phi(U_n))$.

By (20) and Proposition 4.10, there exist atoms $A_0, \dots, A_{n+1} \in \mathcal{A}(P_0)$ such that $|A_i| \neq |A_0|$ for all $i \in [1, n+1]$ and $Z_{P_0}(U_n) = \{A_0 * A_1, A_1 * \dots * A_{n+1}\} \subseteq Z(P_0)$. So it is evident that $c_n = n$.

On the other hand, we know from Theorem 3.8 that Φ is actually an injective equimorphism. Consequently, it follows from the above and condition (E3) of Definition 2.16 that

$$Z_P(\Phi(U_n)) = \{\llbracket \Phi(A_0) * \Phi(A_1) \rrbracket_{\mathcal{C}_P}, \llbracket \Phi(A_1) * \dots * \Phi(A_{n+1}) \rrbracket_{\mathcal{C}_P} \} \subseteq Z(P),$$

Besides, the injectivity of Φ implies that $|\Phi(A_i)| = |A_i| \neq |A_0| = |\Phi(A_0)|$ for every $i \in [1, n+1]$, with the result that $(\Phi(A_0) * \Phi(A_1)) \wedge_P (\Phi(A_1) * \dots * \Phi(A_{n+1})) = n$. So, putting it all together, we conclude from Lemma 2.11 that $c_n^* = c_n = n$. This finishes the proof, because $n \in \mathbf{N}^+$ was arbitrary. ■

We close the section by proving that there is little chance that the arithmetic results summarized in Theorem 4.11 can be also obtained via “standard transfer techniques”.

Proposition 4.12. *Let H be a Dedekind-finite, non-torsion monoid. Then neither $\mathcal{P}_{\text{fin}}(H)$ nor $\mathcal{P}_{\text{fin},\times}(H)$ is equimorphic to a cancellative monoid (in particular, neither is a transfer Krull monoid).*

Proof. By Proposition 4.10 (applied with $r = 2$), there are $A, B, C, D \in \mathcal{A}(\mathcal{P}_{\text{fin},0}(\mathbf{N}))$ such that $A + B = A + C + D$. So, if Φ is the equimorphism of Theorem 3.8, then $\bar{A} := \Phi(A)$, $\bar{B} := \Phi(B)$, $\bar{C} := \Phi(C)$, and $\bar{D} := \Phi(D)$ are atoms of $\mathcal{P}_{\text{fin},\times}(H)$. In addition, $\bar{A}\bar{B} = \bar{A}\bar{C}\bar{D}$.

Building on these premises, suppose for a contradiction that there is an equimorphism $\varphi : \mathcal{P}_{\text{fin}}(H) \rightarrow K$ (respectively, $\varphi : \mathcal{P}_{\text{fin},\times}(H) \rightarrow K$) for which K is a cancellative monoid. It follows

$$\varphi(\bar{A})\varphi(\bar{B}) = \varphi(\bar{A})\varphi(\bar{C})\varphi(\bar{D}),$$

which, by cancellativity of K , yields $\varphi(\bar{B}) = \varphi(\bar{C})\varphi(\bar{D})$. However, we know from Proposition 3.2(iii) that $\mathcal{P}_{\text{fin},\times}(H)$ is a divisor-closed submonoid of $\mathcal{P}_{\text{fin}}(H)$, and this implies, by the above and Proposition

2.21, that \bar{B} , \bar{C} , and \bar{D} are also atoms of $\mathcal{P}_{\text{fin}}(H)$. So, using that φ is atom-preserving, we conclude that $\varphi(\bar{B})$, $\varphi(\bar{C})$, and $\varphi(\bar{D})$ are all atoms of K , in contradiction to the fact that $\varphi(\bar{B}) = \varphi(\bar{C})\varphi(\bar{D})$. ■

5. PROSPECTS FOR FUTURE RESEARCH

We conjecture that, if H is a Dedekind-finite, non-torsion monoid, then the systems of sets of lengths of $\mathcal{P}_{\text{fin}}(H)$ and $\mathcal{P}_{\text{fin},\times}(H)$ contain every non-empty finite subset of $\mathbf{N}_{\geq 2}$. Note that, by Theorem 3.8 and Proposition 3.5(iii)-(iv), it is sufficient to show that

$$\mathcal{L}(\mathcal{P}_{\text{fin},0}(\mathbf{N})) = \{\{0\}, \{1\}\} \cup \mathcal{P}_{\text{fin}}(\mathbf{N}_{\geq 2}).$$

The conjecture is probably difficult, and we hope it will stimulate further work in the subject. Analogous conclusions are known to hold for certain cancellative commutative monoids, see, e.g., [38, Theorem 1] or [22, Corollary 4.1].

ACKNOWLEDGEMENTS

The authors are indebted to Alfred Geroldinger for invaluable comments and enlightening conversations; to Daniel Smertnig for useful discussions (in particular, we owe him the observation that a monoid has a length function only if it is unit-cancellative) and his help with a campaign of numerical experiments that have eventually led to the formulation of Lemma 4.7; to Benjamin Steinberg for answering a question related to Lemma 2.2(i) on MathOverflow (see <http://mathoverflow.net/questions/261850/>); and to an anonymous referee for some precious remarks.

REFERENCES

- [1] N. Alon, *Large sets in finite fields are sumsets*, J. Number Theory **126** (2007), No. 1, 110–118.
- [2] N. Alon, A. Granville, and A. Ubis, *The number of sumsets in a finite field*, Bull. Lond. Math. Soc. **42** (2010), No. 5, 784–794.
- [3] D.D. Anderson (ed.), *Factorization in Integral Domains*, Lect. Notes Pure Appl. Math. **189**, Marcel Dekker, 1997.
- [4] A.A. Antoniou and S. Tringali, *On the arithmetic of power monoids and sumsets in cyclic groups*, e-print (arXiv:1804.10913).
- [5] N.R. Baeth and D. Smertnig, *Factorization theory: From commutative to noncommutative settings*, J. Algebra **441** (2015), 475–551.
- [6] N.R. Baeth and R. Wiegand, *Factorization Theory and Decompositions of Modules*, Amer. Math. Monthly **120** (2013), No. 1, 3–34.
- [7] P. Baginski and S.T. Chapman, *Factorizations of algebraic integers, block monoids, and additive number theory*, Amer. Math. Monthly **118** (2011), 901–920.
- [8] S.T. Chapman (ed.), *Arithmetical Properties of Commutative Rings and Monoids*, Lect. Notes Pure Appl. Math. **241**, Chapman & Hall/CRC, 2005.
- [9] S. Chapman, M. Fontana, A. Geroldinger, and B. Olberding (eds.), *Multiplicative Ideal Theory and Factorization Theory: Commutative and Non-Commutative Perspectives*, Springer Proc. Math. Stat. **170**, Springer, 2016.
- [10] S.T. Chapman, P.A. García-Sánchez, D. Llena, V. Ponomarenko, and J.C. Rosales, *The catenary and tame degree in finitely generated commutative cancellative monoids*, Manuscripta Math. **120** (2006), No. 3, 253–264.
- [11] S.T. Chapman and S. Glaz (eds.), *Non-Noetherian Commutative Ring Theory*, Math. Appl. **520**, Springer, 2000.
- [12] S.T. Chapman, F. Gotti, and R. Pelayo, *On delta sets and their realizable subsets in Krull monoids with cyclic class groups*, Colloq. Math. **137** (2014), No. 1, 137–146.

- [13] S. Chun and D.D. Anderson, *Irreducible elements in commutative rings with zero-divisors, II*, Houston J. Math. **39** (2013), No. 3, 741–752.
- [14] P.M. Cohn, *Basic Algebra: Groups, Rings and Fields*, Springer, 2005 (2nd printing).
- [15] C. Faith, *Dedekind Finite Rings and a Theorem of Kaplansky*, Comm. Algebra **31** (2003), No. 9, 4175–4178.
- [16] Y. Fan and A. Geroldinger, *Minimal relations and catenary degrees in Krull monoids*, to appear in J. Commut. Algebra (arXiv:1603.06356).
- [17] Y. Fan, A. Geroldinger, F. Kainrath, and S. Tringali, *Arithmetic of commutative semigroups with a focus on semigroups of ideals and modules*, J. Algebra Appl. **16** (2017), No. 11, 42 pages.
- [18] M. Fontana, E. Houston, and T. Lucas, *Factoring Ideals in Integral Domains*, Lect. Notes Unione Mat. Ital. **14**, Springer, Berlin, 2013.
- [19] G.A. Freiman, M. Herzog, P. Longobardi, M. Maj, A. Plagne, D.J.S. Robinson, and Y.V. Stanchescu, *On the structure of subsets of an orderable group with some small doubling properties*, J. Algebra **445** (2016), 307–326.
- [20] G.A. Freiman, M. Herzog, P. Longobardi, M. Maj, and Y.V. Stanchescu, *A small doubling structure theorem in a Baumslag–Solitar group*, European J. Combin. **44**, Part A (2015), 106–124.
- [21] S. Frisch, *A construction of integer-valued polynomials with prescribed sets of lengths of factorizations*, Monatsh. Math. **171** (2013), Nos. 3–4, 341–350.
- [22] S. Frisch, S. Nakato, and R. Rissner, *Sets of lengths of factorizations of integer-valued polynomials on Dedekind domains with finite residue fields*, e-print (arXiv:1710.06783).
- [23] J.I. García-García, M.A. Moreno-Frías, and A. Vigneron-Tenorio, *Computation of delta sets of numerical monoids*, Monatsh. Math. **178** (2015), No. 3, 457–472.
- [24] A. Geroldinger, *Sets of lengths*, Amer. Math. Monthly **123** (2016), No. 10, 960–988.
- [25] ———, *Non-commutative Krull monoids: A divisor theoretic approach and their arithmetic*, Osaka J. Math. **50** (2013), No. 2, 503–539.
- [26] A. Geroldinger and F. Halter-Koch, *Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory*, Pure Appl. Math. **278**, Chapman & Hall/CRC, Boca Raton (FL), 2006.
- [27] A. Geroldinger and I.Z. Ruzsa (eds.), *Combinatorial Number Theory and Additive Group Theory*, Birkhäuser, Basel, 2009.
- [28] A. Geroldinger and W. Schmid, *A realization theorem for sets of distances*, J. Algebra **481** (2017), 188–198.
- [29] A. Geroldinger and E.D. Schwab, *Sets of lengths in atomic unit-cancellative finitely presented monoids*, Colloq. Math. **151** (2018), No. 1, 171–187.
- [30] A. Geroldinger and P. Yuan, *The set of distances in Krull monoids*, Bull. Lond. Math. Soc. **44** (2012), No. 6, 1203–1208.
- [31] A. Geroldinger and Q. Zhong, *The set of distances in seminormal weakly Krull monoids*, J. Pure Appl. Algebra **220** (2016), No. 11, 3713–3732.
- [32] D.J. Gryniewicz, *Structural Additive Theory*, Dev. Math. **30**, Springer, 2013.
- [33] K. Gyarmati, S. Konyagin, and A. Sárközy, *On the reducibility of large sets of residues modulo p* , J. Number Theory **133** (2013), No. 7, 2374–2397.
- [34] K. Gyarmati and A. Sárközy, *On Reducible and Primitive Subsets of \mathbb{F}_p , II*, Q. J. Math. **68** (2017), No. 1, 59–77.
- [35] F. Halter-Koch, “Finitely Generated Monoids, Finitely Primary Monoids, and Factorization Properties of Integral Domains”, pp. 31–72 in D.D. Anderson (ed.), *Factorization in Integral Domains*, Lect. Notes Pure Appl. Math. **189**, Dekker, New York, 1997.
- [36] W. Hassler, *Factorization properties of Krull monoids with infinite class group*, Colloq. Math. **92** (2002), No. 2, 229–242.
- [37] K. Iwasawa, *On linearly ordered groups*, J. Math. Soc. Japan **1** (1948), No. 1, 1–9.
- [38] F. Kainrath, *Factorization in Krull monoids with infinite class group*, Colloq. Math. **80** (1999), No. 1, 23–30.
- [39] T.Y. Lam, *Exercises in Classical Ring Theory*, Problem Books in Math., Springer, New York, 2003 (2nd edition).
- [40] F.W. Levi, *Arithmetische Gesetze im Gebiete diskreter Gruppen*, Rend. Circ. Mat. Palermo **35** (1913), 225–236.
- [41] A.I. Mal’tsev, *On ordered groups*, Izv. Akad. Nauk. SSSR Ser. Mat. **13** (1949), No. 6, 473–482.

- [42] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Springer Monogr. Math., Springer-Verlag, 2004 (3rd edition).
- [43] M.B. Nathanson, *Additive Number Theory: The Classical Bases*, Grad. Texts in Math. **164**, Springer, New York, 1996.
- [44] ———, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Grad. Texts in Math. **165**, Springer, New York, 1996.
- [45] B.H. Neumann, *On ordered groups*, Amer. J. Math. **71** (1949), 1–18.
- [46] C. O'Neill, V. Ponomarenko, R. Tate, and G. Webb, *On the set of catenary degrees of finitely generated cancellative commutative monoids*, Internat. J. Algebra Comput. **26** (2016), No. 3, 565–576.
- [47] A. Plagne and S. Tringali, *Sums of dilates in ordered groups*, Comm. Algebra **44** (2016), No. 12, 5223–5236.
- [48] D. Rolfsen and J. Zhu, *Braids, orderings and zero divisors*, J. Knot Theory Ramifications **7** (1998), No. 6, 837–841.
- [49] I.Z. Ruzsa, “Sumsets and Structure”, pp. 88–210 in: A. Geroldinger and I.Z. Ruzsa (eds.), *Combinatorial Number Theory and Additive Group Theory*, Birkhäuser, Basel, 2009.
- [50] A. Sárközy, *On additive decompositions of the set of quadratic residues modulo p* , Acta Arith. **155** (2012), No. 1, 41–51.
- [51] D. Smertnig, “Factorizations of Elements in Noncommutative Rings: A survey”, pp. 353–402 in [9].
- [52] ———, *Sets of lengths in maximal orders in central simple algebras*, J. Algebra **390** (2013), 1–43.
- [53] T. Tao and V.H. Vu, *Additive Combinatorics*, Cambridge Stud. Adv. Math. **105**, Cambridge Univ. Press, Cambridge, 2006.
- [54] S. Tringali, *Structural properties of subadditive families with applications to factorization theory*, to appear in Israel J. Math. (arXiv:1706.03525).
- [55] ———, *Small doubling in ordered semigroups*, Semigroup Forum **90** (2015), No. 1, 135–148.

MATHEMATICAL COLLEGE, CHINA UNIVERSITY OF GEOSCIENCES | HAIDIAN DISTRICT, BEIJING, CHINA

E-mail address: fys@cugb.edu.cn

URL: <http://yushuang-fan.weebly.com/>

INSTITUTE FOR MATHEMATICS AND SCIENTIFIC COMPUTING, UNIVERSITY OF GRAZ, NAWI GRAZ | HEINRICHSTR. 36,
8010 GRAZ, AUSTRIA

E-mail address: salvatore.tringali@uni-graz.at

URL: <http://imsc.uni-graz.at/tringali>