

UNIONS OF SETS OF LENGTHS

MICHAEL FREEZE, ALFRED GEROLDINGER

Dedicated to Professor Władysław Narkiewicz
on the occasion of his seventieth birthday

Abstract: Let H be a Krull monoid such that every class contains a prime (this includes the multiplicative monoids of rings of integers of algebraic number fields). For $k \in \mathbb{N}$ let $\mathcal{V}_k(H)$ denote the set of all $m \in \mathbb{N}$ with the following property: There exist atoms (irreducible elements) $u_1, \dots, u_k, v_1, \dots, v_m \in H$ with $u_1 \cdots u_k = v_1 \cdots v_m$. We show that the sets $\mathcal{V}_k(H)$ are intervals for all $k \in \mathbb{N}$. This solves Problem 37 in [4].

Keywords: non-unique factorizations, sets of lengths, Krull monoids

1. Introduction

The theory of non-unique factorizations has its origin in the theory of algebraic numbers, and it was W. Narkiewicz, starting in the 1960s, who did pioneering work. The main objective of factorization theory is to describe and classify the various phenomena of non-unique factorizations in (non-factorial) domains and monoids by arithmetical invariants. The reader may want to consult recent survey articles [11], [15], [18] or the monographs [17, Chapter 9], [12].

Let H be a monoid. If an element $a \in H$ has a factorization of the form $a = u_1 \cdots u_k$, where $k \in \mathbb{N}$ and $u_1, \dots, u_k \in H$ are atoms, then k is called the length of the factorization, and the set $\mathsf{L}(a)$ of all possible lengths is called the set of lengths of a . Sets of lengths (and all invariants derived from them, as the elasticity or the set of distances) are among the most investigated invariants in factorization theory. Suppose that H is v -noetherian. Then all sets of lengths are finite, and it is easy to observe that either all sets of lengths are singletons or that for every $N \in \mathbb{N}$ there is an element $a \in H$ such that $|\mathsf{L}(a)| \geq N$. The Structure Theorem for Sets of Lengths states that all sets of lengths in a given monoid are almost arithmetical multiprogressions with universal bounds for all parameters (roughly speaking, these are finite unions of arithmetical progressions having the same difference). This Structure Theorem holds true for a great variety of monoids satisfying suitable finiteness conditions (which, among others, are satisfied for orders in algebraic number fields, see [12, Section 4.7] for an overview).

Suppose that H is a Krull monoid with finite class group G such that every class contains a prime. It is easy to see that if $|G| > 3$ then there are sets of lengths which are not arithmetical progressions. Moreover, W.A. Schmid recently proved a realization theorem showing that the Structure Theorem is sharp for Krull monoids with finite class group (see [19]).

In 1990 S. T. Chapman and W. W. Smith ([5]) introduced, for every $k \in \mathbb{N}$, the unions $\mathcal{V}_k(H)$ of all sets of lengths containing k (see Definition 3.1), and these unions were further investigated, among others in [6], [7], [3], [2]. Clearly, unions of sets of lengths should have a simpler structure than sets of lengths themselves, and in [4, Problem 37] it was asked whether the sets $\mathcal{V}_k(H)$, for Krull monoids H as above, are all intervals. Theorem 4.1 gives a positive answer to this question. In Section 3 we study unions of sets of lengths in atomic monoids with finite accepted elasticity. We derive a condition implying that all unions of sets of lengths are arithmetical progressions and give a formula for their asymptotic behavior.

2. Preliminaries

Our notation and terminology is consistent with [12]. We briefly gather some key notions. Let \mathbb{N} denote the set of positive integers, and put $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. For integers $a, b \in \mathbb{Z}$ we set $[a, b] = \{x \in \mathbb{Z} \mid a \leq x \leq b\}$. Let $A, B \subset \mathbb{Z}$ be non-empty subsets. Then $A + B = \{a + b \mid a \in A, b \in B\}$ is their *sumset*. We denote by $\Delta(A)$ the *set of (successive) distances* of A , that is the set of all $d \in \mathbb{N}$ for which there exists $l \in A$ such that $A \cap [l, l + d] = \{l, l + d\}$. Clearly, $\Delta(A) \subset \{d\}$ if and only if A is an arithmetical progression with difference d . The set A is called an *interval* if it is an arithmetical progression with difference 1. If $A \subset \mathbb{N}$, we call

$$\rho(A) = \sup \left\{ \frac{m}{n} \mid m, n \in L \right\} = \frac{\sup A}{\min A} \in \mathbb{Q}_{\geq 1} \cup \{\infty\}$$

the *elasticity* of A , and we set $\rho(\{0\}) = 1$.

By a *monoid* we mean a commutative cancellative semigroup with unit element which satisfies the cancellation laws. Let H be a monoid. We denote by $\mathcal{A}(H)$ the set of atoms (irreducible elements) of H , by H^\times the group of invertible elements and by $H_{\text{red}} = \{aH^\times \mid a \in H\}$ the associated reduced monoid of H . We say that H is reduced if $H^\times = \{1\}$. We denote by $\mathfrak{q}(H)$ a quotient group of H , and for a prime element $p \in H$ let $\mathfrak{v}_p: \mathfrak{q}(H) \rightarrow \mathbb{Z}$ be the p -adic valuation.

For a set P we denote by $\mathcal{F}(P)$ the *free (abelian) monoid* with basis P . Then every $a \in \mathcal{F}(P)$ has a unique representation in the form

$$a = \prod_{p \in P} p^{\mathfrak{v}_p(a)} \quad \text{with } \mathfrak{v}_p(a) \in \mathbb{N}_0 \text{ and } \mathfrak{v}_p(a) = 0 \text{ for almost all } p \in P,$$

and we call

$$|a| = \sum_{p \in P} \mathfrak{v}_p(a) \quad \text{the length of } a.$$

The free monoid $Z(H) = \mathcal{F}(\mathcal{A}(H_{\text{red}}))$ is called the *factorization monoid* of H , and the unique homomorphism

$$\pi: Z(H) \rightarrow H_{\text{red}} \quad \text{satisfying} \quad \pi(u) = u \quad \text{for all} \quad u \in \mathcal{A}(H_{\text{red}})$$

is called the *factorization homomorphism* of H . For $a \in H$, the set

$$Z(a) = \pi^{-1}(aH^\times) \subset Z(H) \quad \text{is the set of factorizations of } a, \text{ and}$$

$$\mathbf{L}(a) = \{|z| \mid z \in Z(a)\} \subset \mathbb{N}_0 \quad \text{the set of lengths of } a.$$

By definition, we have $Z(a) = \{1\}$ for all $a \in H^\times$. The monoid H is *atomic* if and only if $Z(a) \neq \emptyset$ for all $a \in H$, and H is *half-factorial* if and only if $|\mathbf{L}(a)| = 1$ for all $a \in H$.

The *system of sets of lengths* and the *set of distances* of H are defined by

$$\mathcal{L}(H) = \{\mathbf{L}(a) \mid a \in H\} \quad \text{and} \quad \Delta(H) = \bigcup_{a \in H} \Delta(\mathbf{L}(a)) \subset \mathbb{N}.$$

By definition, H is half-factorial if and only if $\Delta(H) = \emptyset$, and $|\Delta(H)| = 1$ if and only if all sets of lengths are arithmetical progressions with the same difference. Moreover, we have $\min \Delta(H) = \gcd \Delta(H)$ (see [12, Proposition 1.4.5]).

For $a \in H$, $\rho(a) = \rho(\mathbf{L}(a))$ is called the *elasticity* of a , and

$$\rho(H) = \sup\{\rho(a) \mid a \in H\} = \sup\{\rho(L) \mid L \in \mathcal{L}(H)\} \in \mathbb{R}_{\geq 1} \cup \{\infty\}$$

the *elasticity* of H . We say that H has *accepted elasticity* if $\rho(H) = \rho(a)$ for some $a \in H$.

We recall the definition of the block monoid over an abelian group which was introduced by W. Narkiewicz in [16]. The block monoid establishes the relationship between arithmetical problems in a Krull monoid and combinatorial problems on zero-sum sequences over its class group. In modern language this was the first application of a transfer principle (for more information on transfer principles the reader is referred to [12, Section 3.2]). It connects the theory of non-unique factorizations with additive group theory and combinatorial number theory.

Let G be an additive abelian group, $G_0 \subset G$ a subset and $\mathcal{F}(G_0)$ the free monoid with basis G_0 . According to the tradition of combinatorial number theory, the elements of $\mathcal{F}(G_0)$ are called *sequences over* G_0 . If $S \in \mathcal{F}(G_0)$, then

$$S = g_1 \cdot \dots \cdot g_l = \prod_{g \in G_0} g^{\mathbf{v}_g(S)},$$

where $\mathbf{v}_g(S)$ is the g -adic value of S (also called the *multiplicity of g in S*), and $\mathbf{v}_g(S) = 0$ for all $g \in G_0 \setminus \{g_1, \dots, g_l\}$. Then $|S| = l$ is the *length of S* , and we set $-S = (-g_1) \cdot \dots \cdot (-g_l)$. We call $\text{supp}(S) = \{g_1, \dots, g_l\}$ the *support* and $\sigma(S) = g_1 + \dots + g_l$ the *sum* of S . The monoid

$$\mathcal{B}(G_0) = \{S \in \mathcal{F}(G_0) \mid \sigma(S) = 0\} = \mathcal{B}(G) \cap \mathcal{F}(G_0)$$

is called the *block monoid* over G_0 . It is a Krull monoid, its elements are called *zero-sum sequences* over G_0 , and its atoms are the minimal zero-sum sequences (that is, zero-sum sequences without a proper zero-sum subsequence).

For every arithmetical invariant $*(H)$ defined for a monoid H , we write $*(G_0)$ instead of $*(\mathcal{B}(G_0))$. In particular, we set $\mathcal{A}(G_0) = \mathcal{A}(\mathcal{B}(G_0))$, $\rho(G_0) = \rho(\mathcal{B}(G_0))$ and $\Delta(G_0) = \Delta(\mathcal{B}(G_0))$. We define the *Davenport constant* of G_0 by

$$D(G_0) = \sup\{|U| \mid U \in \mathcal{A}(G_0)\} \in \mathbb{N} \cup \{\infty\},$$

which is a central invariant in zero-sum theory (see [9]). If G_0 is finite, then $\mathcal{A}(G_0)$ is finite, and hence $D(G_0) < \infty$. We shall tacitly use that for a non-trivial group G we have $\rho(G) = D(G)/2$ (see [12, Theorem 3.4.11]).

3. The $\mathcal{V}_k(H)$ sets in monoids with accepted elasticity

The main result in this section is Theorem 3.1. It provides a sufficient condition which forces unions of sets of lengths to be arithmetical progressions, and it gives a formula for their asymptotic behavior. Under much milder finiteness assumptions unions of sets of lengths are almost arithmetical progressions ([8, Theorem 4.2]), and in Example 3.1 we discuss a simple monoid, which fails the condition in 3.1, and whose $\mathcal{V}_k(H)$ sets are not arithmetical progressions.

Definition 3.1. *Let H be an atomic monoid and $k \in \mathbb{N}$.*

1. *Let $\mathcal{V}_k(H)$ denote the set of all $m \in \mathbb{N}$ for which there exist $u_1, \dots, u_k, v_1, \dots, v_m \in \mathcal{A}(H)$ with $u_1 \cdot \dots \cdot u_k = v_1 \cdot \dots \cdot v_m$.*
2. *If $H = H^\times$, we set $\rho_k(H) = \lambda_k(H) = k$, and if $H \neq H^\times$, then we define*

$$\rho_k(H) = \sup \mathcal{V}_k(H) \in \mathbb{N} \cup \{\infty\} \quad \text{and} \quad \lambda_k(H) = \min \mathcal{V}_k(H) \in [1, k].$$

The sets $\mathcal{V}_k(H)$ were first studied in [5]. The invariants $\rho_k(H)$ were introduced in [14], and, for Krull monoids with finite class group, the state of knowledge is presented in [12, Section 6.3]. It was proved only recently that a v -noetherian monoid with $\rho_k(H) < \infty$ for all $k \in \mathbb{N}$ is locally tame (see [13, Corollary 4.3]). Apart from the case of Krull monoids with cyclic class group (see Corollary 4.1), little is known about the invariants $\lambda_k(H)$, and only in very special cases have the sets $\mathcal{V}_k(H)$ been written down explicitly. In [1, Theorem 2.6] this is done for numerical monoids generated by an arithmetical progression. In [12, Section 7.3], the systems of sets of lengths $\mathcal{L}(G)$ are explicitly determined for some small groups G , from which it is easy to obtain the $\mathcal{V}_k(G)$ sets.

The following lemma gathers some straightforward properties of the $\mathcal{V}_k(H)$ sets which will be used throughout the paper without further mentioning.

Lemma 3.1. *Let H be an atomic monoid with $H \neq H^\times$ and $k, l \in \mathbb{N}$.*

1. $\mathcal{V}_1(H) = \{1\}$, $k \in \mathcal{V}_k(H)$ and

$$\mathcal{V}_k(H) = \bigcup_{k \in L, L \in \mathcal{L}(H)} L.$$

2. $\mathcal{V}_k(H) + \mathcal{V}_l(H) \subset \mathcal{V}_{k+l}(H)$ and

$$\lambda_{k+l}(H) \leq \lambda_k(H) + \lambda_l(H) \leq k + l \leq \rho_k(H) + \rho_l(H) \leq \rho_{k+l}(H).$$

3. We have $l \in \mathcal{V}_k(H)$ if and only if $k \in \mathcal{V}_l(H)$.

Proof. Obvious. ■

Lemma 3.2. *Let H be an atomic monoid with $H \neq H^\times$ and finite accepted elasticity.*

1. We have $\rho_k(H) \leq k\rho(H)$ for all $k \in \mathbb{N}$.
2. We have

$$\rho(H) = \sup\left\{\frac{\rho_k(H)}{k} \mid k \in \mathbb{N}\right\} = \lim_{k \rightarrow \infty} \frac{\rho_k(H)}{k},$$

and there is some $N \in \mathbb{N}$ such that

$$\rho(H) = \frac{\rho_{kN}(H)}{kN} \quad \text{for all } k \in \mathbb{N}.$$

Proof. See [12, Proposition 1.4.2]. ■

Lemma 3.3. *Let H be an atomic monoid with $H \neq H^\times$ and finite accepted elasticity. Suppose that $N \in \mathbb{N}$ has the property of Lemma 3.2.2.*

1. Let $j \in [0, N - 1]$ and $k \in \mathbb{N}$. Then

$$0 \leq \rho_{kN+j}(H) - kN\rho(H) \leq (N - 1)\rho(H).$$

2. Let $j \in [0, N - 1]$ and $m \in \mathbb{N}$ with

$$\rho_{mN+j}(H) - mN\rho(H) = \max\{\rho_{kN+j}(H) - kN\rho(H) \mid k \in \mathbb{N}\}.$$

Then $\rho_{(m+i)N+j}(H) = \rho_{mN+j}(H) + iN\rho(H)$ for all $i \in \mathbb{N}_0$.

Proof. 1. By Lemma 3.2.1 we have

$$\rho_{kN+j}(H) \leq (kN + j)\rho(H) \leq kN\rho(H) + (N - 1)\rho(H).$$

2. If $i \in \mathbb{N}_0$, then

$$\begin{aligned} \rho_{(m+i)N+j}(H) - (m+i)N\rho(H) &\leq \rho_{mN+j}(H) - mN\rho(H) \\ &= \rho_{mN+j}(H) + \rho_{iN}(H) - (m+i)N\rho(H) \\ &\leq \rho_{(m+i)N+j}(H) - (m+i)N\rho(H). \end{aligned} \quad \blacksquare$$

Lemma 3.4. *Let H be an atomic monoid with $H \neq H^\times$ and finite accepted elasticity. Suppose that $N \in \mathbb{N}$ has the property of Lemma 3.2.2.*

1. *For all $k \in \mathbb{N}$ we have $\lambda_k(H) \geq \rho(H)^{-1}k$, and if k is a multiple of $N\rho(H)$, then equality holds.*
2. *Let $j \in [0, N\rho(H) - 1]$ and $k \in \mathbb{N}$. Then*

$$0 \leq \lambda_{kN\rho(H)+j}(H) - kN \leq N\rho(H) - 1.$$

Moreover, we have

$$\lim_{l \rightarrow \infty} \frac{\lambda_l(H)}{l} = \frac{1}{\rho(H)}.$$

3. *Let $j \in [0, N\rho(H) - 1]$ and $m \in \mathbb{N}$ with $\lambda_{mN\rho(H)+j}(H) - mN = \min\{\lambda_{kN\rho(H)+j}(H) - kN \mid k \in \mathbb{N}\}$. Then*

$$\lambda_{(m+i)N\rho(H)+j}(H) = \lambda_{mN\rho(H)+j}(H) + iN \quad \text{for all } i \in \mathbb{N}_0.$$

Proof. 1. Let $k \in \mathbb{N}$. There is some $L \in \mathcal{L}(H)$ with $k, \lambda_k(H) \in L$, and hence it follows that

$$k \leq \max L \leq \rho(H) \min L = \rho(H)\lambda_k(H).$$

Let $i \in \mathbb{N}$ and $k = iN\rho(H)$. Since there is some $L \in \mathcal{L}(H)$ with $\{iN, \rho_{iN}(H)\} \subset L$ and $\rho_{iN}(H) = iN\rho(H)$, it follows that

$$\lambda_{iN\rho(H)}(H) \leq iN = \frac{iN\rho(H)}{\rho(H)}.$$

2. By 1. we have $\lambda_{kN\rho(H)+j}(H) \geq kN$. Since $\mathcal{V}_j(H) + \mathcal{V}_{kN\rho(H)}(H) \subset \mathcal{V}_{kN\rho(H)+j}(H)$, it follows that

$$\lambda_{kN\rho(H)+j}(H) \leq \lambda_j(H) + \lambda_{kN\rho(H)}(H) \leq j + kN \leq N\rho(H) - 1 + kN.$$

Since, for every $m \in \mathbb{N}$,

$$0 \leq \frac{\lambda_{mN\rho(H)+j}(H)}{mN\rho(H)+j} - \frac{mN}{mN\rho(H)+j} \leq \frac{N\rho(H) - 1}{mN\rho(H)+j},$$

we infer that

$$\lim_{m \rightarrow \infty} \frac{\lambda_{mN\rho(H)+j}(H)}{mN\rho(H)+j} = \frac{1}{\rho(H)},$$

and hence the assertion follows.

3. Let $i \in \mathbb{N}_0$. Since $\mathcal{V}_{mN\rho(H)+j}(H) + \mathcal{V}_{iN\rho(H)}(H) \subset \mathcal{V}_{(m+i)N\rho(H)+j}(H)$, it follows that

$$\lambda_{(m+i)N\rho(H)+j}(H) \leq \lambda_{mN\rho(H)+j}(H) + \lambda_{iN\rho(H)}(H).$$

Thus by definition of m , we infer that

$$\begin{aligned} \lambda_{(m+i)N\rho(H)+j}(H) - (m+i)N &\geq \lambda_{mN\rho(H)+j}(H) - mN \\ &= \lambda_{mN\rho(H)+j}(H) + \lambda_{iN\rho(H)}(H) - (m+i)N \\ &\geq \lambda_{(m+i)N\rho(H)+j}(H) - (m+i)N. \end{aligned} \quad \blacksquare$$

Lemma 3.5. *Let H be an atomic monoid with $\Delta(H) \neq \emptyset$ and $d = \min \Delta(H)$.*

1. $\Delta(\mathcal{V}_k(H)) \subset d\mathbb{N}$, and there exists $k^* \in \mathbb{N}$ such that $\min \Delta(\mathcal{V}_k(H)) = d$ for all $k \geq k^*$.
2. $\sup \Delta(\mathcal{V}_k(H)) \leq \sup \Delta(H)$ for all $k \in \mathbb{N}$.
3. If $k \in \mathbb{N}$ and $\mathcal{V}_m(H) \cap \mathbb{N}_{\geq m}$ is an arithmetical progression with difference d for all $m \in [\lambda_k(H), k]$, then $\mathcal{V}_k(H) \cap [0, k]$ is an arithmetical progression with difference d .
4. The following statements are equivalent:
 - (a) $\mathcal{V}_k(H) \cap \mathbb{N}_{\geq k}$ is an arithmetical progression with difference d for all $k \in \mathbb{N}$.
 - (b) $\mathcal{V}_k(H)$ is an arithmetical progression with difference d for all $k \in \mathbb{N}$.

Proof. 1. Since $d = \gcd \Delta(H)$ (see [13, Proposition 1.4.5]), it follows that

$$\mathcal{V}_k(H) = \bigcup_{k \in L, L \in \mathcal{L}(H)} L \subset k + d\mathbb{Z},$$

whence $\Delta(\mathcal{V}_k(H)) \subset d\mathbb{N}$. Let $k^* \in \mathbb{N}$ and $u_1, \dots, u_{k^*}, v_1, \dots, v_{k^*+d} \in \mathcal{A}(H)$ such that $u_1 \cdots u_{k^*} = v_1 \cdots v_{k^*+d}$, and let $k \in \mathbb{N}$ with $k \geq k^*$. Since $u_1^{k-k^*} u_1 \cdots u_{k^*} = u_1^{k-k^*} v_1 \cdots v_{k^*+d}$, it follows that $d \in \Delta(\mathcal{V}_k(H))$, and thus $d = \min \Delta(\mathcal{V}_k(H))$.

2. If $\Delta(H)$ is infinite, then the assertion is obvious. Suppose that $\Delta(H)$ is finite. Let $k \in \mathbb{N}$ and $d \in \Delta(\mathcal{V}_k(H))$ be given. Then there are $l, m \in \mathbb{N}$ such that $d = m - l$ and $[l, m] \cap \mathcal{V}_k(H) = \{l, m\}$. By Lemma 3.1 there are $a, b \in H$ with $k, l \in \mathbb{L}(a)$ and $k, m \in \mathbb{L}(b)$. We distinguish two cases.

CASE 1: $\min \mathbb{L}(b) < m$.

Then there is $m' \in \mathbb{L}(b)$ with $m' < m$ and $[m', m] \cap \mathbb{L}(b) = \{m', m\}$. Since $\mathbb{L}(b) \subset \mathcal{V}_k(H)$, we get $m' \leq l$ and hence $d = m - l \leq m - m' \in \Delta(\mathbb{L}(b)) \subset \Delta(H)$.

CASE 2: $\min \mathbb{L}(b) = m$.

Then we have $l < m \leq k$. Since $l, k \in \mathbb{L}(a)$, there is some $l' \in \mathbb{L}(a)$ with $l < l'$ and $[l, l'] \cap \mathbb{L}(a) = \{l, l'\}$. Since $\mathbb{L}(a) \subset \mathcal{V}_k(H)$, we get $m \leq l'$ and hence $d = m - l \leq l' - l \in \Delta(\mathbb{L}(a)) \subset \Delta(H)$.

3. Let $k \in \mathbb{N}$ and $l = \lambda_k(H)$. We have to show that $\mathcal{V}_k(H) \cap [l, k]$ is an arithmetical progression with difference d . Let $m \in [l, k]$ such that $k - m$ is a multiple of d . In order to show that $m \in \mathcal{V}_k(H)$, we verify that $k \in \mathcal{V}_m(H)$. We have $m \leq k \leq \rho_l(H) \leq \rho_m(H)$. Since $k \in m + d\mathbb{N}_0$ with $k \leq \rho_m(H)$ and $\mathcal{V}_m(H) \cap \mathbb{N}_{\geq m}$ is an arithmetical progression with difference d , it follows that $k \in \mathcal{V}_m(H)$.

4. This follows immediately from 3. ■

Theorem 3.1. *Let H be an atomic monoid with finite non-empty set of distances $\Delta(H)$ and $d = \min \Delta(H)$. Suppose that there is some $a^* \in H$ with $\rho(a^*) = \rho(H) < \infty$ and $\mathbb{L}(a^*)$ is an arithmetical progression with difference d .*

1. There exists $k^* \in \mathbb{N}$ such that $\mathcal{V}_k(H)$ is an arithmetical progression with difference d for all $k \geq k^*$.

2. We have

$$\lim_{k \rightarrow \infty} \frac{|\mathcal{V}_k(H)|}{k} = \frac{1}{d} \left(\rho(H) - \frac{1}{\rho(H)} \right),$$

and there is some $N \in \mathbb{N}$ such that

$$\frac{|\mathcal{V}_{rN\rho(H)}(H)| - 1}{rN\rho(H)} = \frac{1}{d} \left(\rho(H) - \frac{1}{\rho(H)} \right) \quad \text{for all sufficiently large } r \in \mathbb{N}.$$

Proof. Since $\rho(H) < \infty$, Lemma 3.2.1 implies that $\rho_k(H) < \infty$ for all $k \in \mathbb{N}$, and all sets of lengths are finite. We proceed in four steps.

i) Let $N = \min \mathsf{L}(a^*)$, $k \in \mathbb{N}$ and $L_k = \mathsf{L}(a^*) + \dots + \mathsf{L}(a^*)$ the k -fold sumset. Then $\min L_k = kN$, $\max L_k = k \max \mathsf{L}(a^*)$ and L_k is an arithmetical progression with difference d . Then $L_k \subset \mathsf{L}(a^{*k})$,

$$\frac{\rho_{kN}(H)}{kN} \geq \frac{\max \mathsf{L}(a^{*k})}{kN} \geq \frac{\max L_k}{\min L_k} \geq \frac{k \max \mathsf{L}(a^*)}{kN} = \rho(a^*) = \rho(H) \geq \frac{\rho_{kN}(H)}{kN},$$

and hence $\rho(H) \geq \rho(a^{*k}) \geq \rho(L_k) = \rho(H)$ and $L_k = \mathsf{L}(a^{*k})$. Moreover, N has the property of Lemma 3.2.2.

ii) Suppose that

$$a^* = u_1 \cdot \dots \cdot u_N = v_1 \cdot \dots \cdot v_{N\rho(H)}$$

with atoms $u_1, \dots, u_N, v_1, \dots, v_{N\rho(H)}$. Let $r \in \mathbb{N}$ such that

$$r\rho(H) \in \mathbb{N} \quad \text{and} \quad rN(\rho(H)^2 - 1) \geq d^{-1} \max \Delta(H). \tag{*}$$

Then

$$a^{*r} = (u_1 \cdot \dots \cdot u_N)^r = (v_1 \cdot \dots \cdot v_{N\rho(H)})^r$$

and

$$(a^*)^{r\rho(H)} = (u_1 \cdot \dots \cdot u_N)^{r\rho(H)} = (v_1 \cdot \dots \cdot v_{N\rho(H)})^{r\rho(H)}.$$

These two equations and i) imply that $\mathcal{V}_{rN\rho(H)}(H)$ is an arithmetical progression with difference d , $\min \mathcal{V}_{rN\rho(H)}(H) = rN$ and $\max \mathcal{V}_{rN\rho(H)}(H) = rN\rho(H)^2$. In particular, it follows that

$$\begin{aligned} \frac{|\mathcal{V}_{rN\rho(H)}(H)| - 1}{rN\rho(H)} &= \frac{1 \max \mathcal{V}_{rN\rho(H)}(H) - \min \mathcal{V}_{rN\rho(H)}(H)}{rN\rho(H)} = \\ &= \frac{1 rN\rho(H)^2 - rN}{rN\rho(H)} = \frac{1}{d} \left(\rho(H) - \frac{1}{\rho(H)} \right). \end{aligned}$$

iii) Let $r \in \mathbb{N}$ minimal such that (*) holds, and let $k^* \in \mathbb{N}$ be minimal such that every $k \geq k^*$ has the following two properties:

- If $k - rN\rho(H) = mN + j$ with $j \in [0, N - 1]$, then m has the property described in Lemma 3.3.2.

- If $k - rN\rho(H) = mN\rho(H) + j$ with $j \in [0, N\rho(H) - 1]$, then m has the property described in Lemma 3.4.3.

Let $k \geq k^*$. We set $V = \mathcal{V}_{rN\rho(H)}(H)$ and have

$$V + \mathcal{V}_{k-rN\rho(H)}(H) \subset \mathcal{V}_k(H).$$

Since by ii), V is an arithmetical progression with difference d , $\max V - \min V \geq d^{-1} \max \Delta(H)$ and since, by Lemma 3.5, $\max \Delta(\mathcal{V}_{k-rN\rho(H)}(H)) \leq \max \Delta(H)$, it follows that the sumset $V + \mathcal{V}_{k-rN\rho(H)}(H)$ is an arithmetical progression with difference d . We show that the minima and maxima of this sumset and of $\mathcal{V}_k(H)$ coincide. Then obviously $\mathcal{V}_k(H)$ is an arithmetical progression with difference d .

Since $k \geq k^*$, Lemma 3.3.2 implies that

$$\max \mathcal{V}_k(H) = \rho_k(H) = \rho_{k-rN\rho(H)}(H) + rN\rho(H)^2 = \max(\mathcal{V}_{k-rN\rho(H)}(H) + V).$$

Similarly, Lemma 3.4.3 implies that

$$\min \mathcal{V}_k(H) = \lambda_k(H) = \lambda_{k-rN\rho(H)}(H) + rN = \min(\mathcal{V}_{k-rN\rho(H)}(H) + V).$$

iv) Let $k \geq k^*$. Since $\mathcal{V}_k(H)$ is an arithmetical progression with difference d , we get

$$\frac{|\mathcal{V}_k(H)|}{k} = \frac{1}{d} \left(\frac{\rho_k(H) - \lambda_k(H) + d}{k} \right).$$

Now the assertion follows from Lemmas 3.2.2 and 3.4.2. ■

The asymptotic formula in Theorem 3.1.2 was first proved for Dedekind domains with finite class group such that every class contains a prime ideal (see [6, Theorem 6]), and then for atomic monoids with $|\Delta(H)| = 1$ (see [2, Corollary 7]).

If H_{red} is a finitely generated monoid or a Krull monoid with finite class group, then there exists some $a^* \in H$ such that $\rho(a^*) = \rho(H) < \infty$ (see [12, Theorems 3.1.4, 3.4.2 and 3.4.10]). Let p be an odd prime, G a cyclic group of order p , $H = \mathcal{B}(G)$ and

$$a^* = \prod_{g \in G \setminus \{0\}} g^p \in \mathcal{B}(G).$$

Then obviously $\rho(a^*) = p/2 = \rho(H)$, and by Example on page 517 in [10], $L(a^*)$ is an arithmetical progression with difference 1. Next we provide an example of a finitely generated monoid for which the statement of Theorem 3.1 fails (this shows that the additional assumption of Theorem 3.1, that $L(a^*)$ is an arithmetical progression with difference d , is crucial). However, in monoids of the above type unions of sets of lengths are almost arithmetical progressions (see [8, Theorem 4.2]).

Example 3.1. Let $d_1, d_2 \in \mathbb{N}$ and $d = \gcd(d_1, d_2)$ such that $2d < d_2 - d_1$. For $i \in \{1, 2\}$ let H_i be a reduced atomic monoid with $\min \Delta(H_i) = d_i$, $\rho(H_i) = 1 + d_i/2$ and $a_i \in H_i$ with $L(a_i) = \{2, 2 + d_i\}$. Then $H = H_1 \times H_2$ is an atomic monoid with $d = \min \Delta(H)$.

Note, if $i \in \{1, 2\}$, $n_i = 2 + d_i$ and $G_i = \{1 + n_i\mathbb{Z}, -1 + n_i\mathbb{Z}\} \subset \mathbb{Z}/n_i\mathbb{Z}$, then $H_i = \mathcal{B}(G_i)$ has the above properties, and H is a finitely generated Krull monoid.

Let $c = c_1c_2 \in H$ where $c_1 \in H_1$ and $c_2 \in H_2$. Then

$$\rho(c) = \frac{\max \mathsf{L}(c_1) + \max \mathsf{L}(c_2)}{\min \mathsf{L}(c_1) + \min \mathsf{L}(c_2)} \leq \max\{\rho(c_1), \rho(c_2)\} \leq \rho(H_2).$$

This shows that $\rho(H) = \rho(H_2)$.

Let $s \in \mathbb{N}$ and $k = s(2 + d_2)$. Then both $2s$ and k are in $\mathsf{L}(a_2^s)$ whence $k \in \mathcal{V}_{2s}(H)$. Assume to the contrary that $\mathcal{V}_{2s}(H)$ is an arithmetical progression with difference d . Then $k - d \in \mathcal{V}_{2s}(H)$, and hence there are $c_1 \in H_1$, $c_2 \in H_2$ such that for $c = c_1c_2$ we have $2s, k - d \in \mathsf{L}(c)$. Since $k - 2s - d = sd_2 - d$, it follows that $|\mathsf{L}(c_1)| \neq 1$ and $|\mathsf{L}(c_2)| \neq 1$. If $\min \mathsf{L}(c) < 2s$, then $\min \mathsf{L}(c) \leq 2s - d$ and

$$\rho(c) = \frac{\max \mathsf{L}(c)}{\min \mathsf{L}(c)} \geq \frac{k - d}{2s - d} > \frac{k}{2s} = \rho(H_2) = \rho(H),$$

a contradiction. Thus $\min \mathsf{L}(c) = 2s$ and

$$\rho(c) \geq \frac{k - d}{2s} = \frac{2s + sd_2 - d}{2s} = 1 + d_2/2 - d/(2s).$$

If $i \in \mathbb{N}$ such that $\min \mathsf{L}(c_2) = 2s - i$, then $\min \mathsf{L}(c_1) = i$ and

$$\begin{aligned} \rho(c) &\leq \frac{(2s - i)\rho(c_2) + i\rho(c_1)}{2s} \leq \frac{(2s - i)(1 + d_2/2) + i(1 + d_1/2)}{2s} \\ &= 1 + d_2/2 - \frac{i(d_2/2 - d_1/2)}{2s} < 1 + d_2/2 - d/(2s), \end{aligned}$$

a contradiction.

4. The $\mathcal{V}_k(H)$ sets in Krull monoids

In this section we study Krull monoids with class group G such that every class contains a prime. The class of these Krull monoids includes the multiplicative monoids of rings of integers of algebraic number fields and of holomorphy rings in algebraic function fields over finite fields (see [12, Theorems 2.10.14 and 8.9.5] and [12, Examples 7.4.2] for further examples).

We start with a lemma. Its first item was already observed in [6] (in the setting of Dedekind domains). For convenience we provide a short proof. Recall that according to our conventions we set $\mathcal{V}_k(G) = \mathcal{V}_k(\mathcal{B}(G))$ for an abelian group G .

Lemma 4.1. *Let G be a finite abelian group with $|G| \geq 3$ and $k \in \mathbb{N}$.*

1. $\mathcal{V}_{2k}(G) \cap [2k, k\mathsf{D}(G)]$ is an interval.
2. $\mathcal{V}_k(G) \cap [0, k]$ is an interval.
3. $\mathcal{V}_k(G) \cap \mathbb{N}_{\geq k}$ is an interval.

Proof. 1. We first show that $\mathcal{V}_2(G) = [2, D(G)]$.

Let $j \in [2, D(G)]$ and $U = g_1 \cdots g_l \in \mathcal{A}(G)$ with $|U| = l = D(G)$. If $h_j = g_j + \dots + g_l$, then $U_j = g_1 \cdots g_{j-1} h_j \in \mathcal{A}(G)$ and $\{2, j\} \subset L((-U_j)U_j) \subset \mathcal{V}_2(G)$. Thus $[2, D(G)] \subset \mathcal{V}_2(G)$, and since $\rho(G) = D(G)/2$, equality follows.

Now suppose that $k \geq 2$. Then

$$2k \in \mathcal{V}_2(G) + \mathcal{V}_{2(k-1)}(G) \subset \mathcal{V}_{2k}(G).$$

Since $\mathcal{V}_2(G) = [2, D(G)]$ and, by Lemma 3.5.2, $\max \Delta(\mathcal{V}_{2(k-1)}(G)) \leq \max \Delta(G) \leq D(G) - 2$, it follows that $\mathcal{V}_2(G) + \mathcal{V}_{2(k-1)}(G)$ is an interval. Since the maxima of $\mathcal{V}_2(G) + \mathcal{V}_{2(k-1)}(G)$ and of $\mathcal{V}_{2k}(G)$ coincide, it follows that $\mathcal{V}_{2k}(G) \cap [2k, kD(G)]$ is an interval.

2. We set $l = \lambda_k(G)$ and have to show that $\mathcal{V}_k(G) \cap [l, k]$ is an interval. Pick $m \in [l, k]$. In order to show that $m \in \mathcal{V}_k(G)$, we verify that $k \in \mathcal{V}_m(G)$.

CASE 1: m is even.

Since $l \leq m \leq k \leq \rho_l(G) \leq \rho_m(G)$, we get that $k \in [m, \rho_m(G)]$, and thus 1. implies that $k \in \mathcal{V}_m(G)$.

CASE 2: m is odd.

If $m = l$, then there is nothing to show. Suppose that $l + 1 \leq m$. Since $l \leq m - 1 \leq k - 1 \leq \rho_l(G) \leq \rho_{m-1}(G)$, it follows that $k - 1 \in [m - 1, \rho_{m-1}(G)]$. Since $m - 1$ is even, 1. implies that $k - 1 \in \mathcal{V}_{m-1}(G)$ and hence $k \in \mathcal{V}_m(G)$.

3. For $l \in [k, \rho_k(G)]$ let

$$m_l(G) = \min\{|B| \mid B \in \mathcal{B}(G) \text{ with } k, l \in L(B)\}.$$

We assert that every $l \in [k + 1, \rho_k(G)]$ lies in $\mathcal{V}_k(G)$ and that

$$m_l(G) < m_{l+1}(G) < \dots < m_{\rho_k(G)}(G).$$

We proceed by induction on l . For $l = \rho_k(G)$ the assertion is clear. Suppose that $l \leq \rho_k(G)$ and that the assertions hold for all $s \in [l, \rho_k(G)]$.

Let $B \in \mathcal{B}(G)$ such that $k, l \in L(B)$ and $|B| = m_l(G)$. Then there are $U_1, \dots, U_k, V_1, \dots, V_l \in \mathcal{A}(G)$ such that

$$B = U_1 \cdots U_k = V_1 \cdots V_l.$$

After renumbering if necessary there is some $i \in [0, k - 1]$ such that $U_1 = V_1, \dots, U_i = V_i$ and $\{U_{i+1}, \dots, U_k\} \cap \{V_{i+1}, \dots, V_l\} = \emptyset$. Since $|B| = m_l(G)$, it follows that $|U_1| = \dots = |U_i| = 1$ and that $|U_r| \geq 2$ and $|V_s| \geq 2$ for all $r \in [i + 1, k]$ and all $s \in [i + 1, l]$.

Since $U_k \nmid V_j$ for any $j \in [i + 1, l]$ and $|U_k| \geq 2$ there are $g_1, g_2 \in G$ such that $g_1 g_2 \mid U_k$ and, after renumbering V_{i+1}, \dots, V_l if necessary, $g_1 \mid V_{i-1}$ and $g_2 \mid V_i$. We set

$$\widetilde{U}_k = (g_1 + g_2)(g_1 g_2)^{-1} U_k \quad \text{and} \quad \widetilde{V}_{i-1} = (g_1 + g_2)(g_1 g_2)^{-1} V_{i-1} V_i.$$

Then $\widetilde{U}_k \in \mathcal{A}(G)$, $\widetilde{V}_{i-1} \in \mathcal{B}(G)$ and

$$U_1 \cdots U_{k-1} \widetilde{U}_k = V_1 \cdots V_{i-2} \widetilde{V}_{i-1}.$$

Suppose that \widetilde{V}_{i-1} is a product of t atoms. Then $t \in [1, \rho_k(G) - (l - 2)]$.

Assume to the contrary that $t \geq 2$. Then

$$m_l(G) = |B| > |U_1 \cdots U_{k-1} \widetilde{U}_k| \geq m_{l-2+t}(G) \geq m_l(G),$$

a contradiction.

Thus it follows that $t = 1$, $\widetilde{V}_{l-1} \in \mathcal{A}(G)$, $l - 1 \in \mathcal{V}_k(G)$ and

$$m_{l-1}(G) \leq |U_1 \cdots U_{k-1} \widetilde{U}_k| < |U_1 \cdots U_k| = m_l(G). \quad \blacksquare$$

Theorem 4.1. *Let H be a Krull monoid with class group G such that every class contains a prime. Then for every $k \in \mathbb{N}$ the set $\mathcal{V}_k(H)$ is an interval.*

Proof. By [12, Theorem 3.4.10], we have $\mathcal{V}_k(H) = \mathcal{V}_k(G)$ and hence $\lambda_k(H) = \lambda_k(G)$ and $\rho_k(H) = \rho_k(G)$ for all $k \in \mathbb{N}$. Thus it suffices to prove the assertion for the block monoid $\mathcal{B}(G)$.

Suppose that G is infinite. By Kainrath’s Theorem every set $L \subset \mathbb{N}_{\geq 2}$ is a set of lengths (see [12, Theorem 7.4.1]). This implies that $\mathcal{V}_k(H) = \mathbb{N}_{\geq 2}$ for all $k \geq 2$.

If $|G| \leq 2$, then $\mathcal{B}(G)$ is half-factorial whence the sets $\mathcal{V}_k(G)$ are singletons for all $k \in \mathbb{N}$. If $3 \leq |G| < \infty$, then the assertion follows from Lemma 4.1. \blacksquare

Corollary 4.1. *Let H be a Krull monoid with cyclic class group G of order $n \geq 2$ such that every class contains a prime. Then for every $k \in \mathbb{N}$ we have $\mathcal{V}_k(H) = [\lambda_k(H), \rho_k(H)]$ and*

$$\lambda_{kn+j}(H) = \begin{cases} 2k + j & \text{for } j \in [0, 1] \\ 2k + 2 & \text{for } j \in [2, n - 1] \end{cases} \quad \text{and}$$

$$\rho_{2k+j}(H) = kn + j \quad \text{for } j \in [0, 1].$$

Proof. As in the proof of Theorem 4.1 it suffices to consider the block monoid $\mathcal{B}(G)$. If $n = 2$, then $\mathcal{B}(G)$ is half-factorial whence for all $k \in \mathbb{N}$ we have $\lambda_k(G) = k = \rho_k(G)$. Suppose that $n \geq 3$, and let $k \in \mathbb{N}$. By Theorem 4.1 we obtain that $\mathcal{V}_k(H) = [\lambda_k(G), \rho_k(G)]$. The assertion on $\rho_{2k+j}(G)$ follows from [8, Theorem 5.3], and it remains to verify the assertion concerning $\lambda_{kn+j}(G)$. For every $j \in [0, n - 1]$, Lemma 3.4.1 implies that

$$\lambda_{kn+j}(G) \geq \rho(G)^{-1}(kn + j) = \frac{2}{n}(kn + j) = 2k + \frac{2j}{n}.$$

If $j \in \{0, 1\}$, then $\rho_{2k+j}(G) = kn + j$, hence $\lambda_{kn+j}(G) \leq 2k + j$ and thus $\lambda_{kn+j}(G) = 2k + j$. Let $j \in [2, n - 1]$. By [12, Proposition 6.6.1] there is some $L \in \mathcal{L}(G)$ with $\{2, j\} \subset L$. Thus $2k + 2 \in \mathcal{V}_{kn}(G) + \mathcal{V}_j(G) \subset \mathcal{V}_{kn+j}(G)$ and thus $\lambda_{kn+j} \leq 2k + 2$. Since $\rho_{2k+1}(G) = kn + 1$, it follows that $\lambda_{kn+j}(G) = 2k + 2$. \blacksquare

As already pointed out, Theorem 4.1 includes the multiplicative monoids of rings of integers of algebraic number fields. The question arises whether the same result is true for a non-principal order R of an algebraic number field. Since

the Structure Theorem for Sets of Lengths holds for R and since every class of the Picard group $\text{Pic}(R)$ contains a prime ideal (see [12, Corollary 2.11.16]), it is tempting to speculate that the $\mathcal{V}_k(R)$ sets are intervals too. But no work has been done yet into this direction. We end with a simple example showing that unions of sets of lengths in $\mathbb{Z}[\sqrt{-7}]$ are intervals.

Example 4.1. Let K be an algebraic number field, $R \subset K$ a non-principal order of K , $R^\bullet = R \setminus \{0\}$ its multiplicative monoid and \overline{R} the integral closure of R in K . Then $\rho(R) < \infty$ if and only if for every non-zero prime ideal $\mathfrak{p} \subset R$, there is precisely one prime ideal $\overline{\mathfrak{p}} \subset \overline{R}$ such that $\overline{\mathfrak{p}} \cap R = \mathfrak{p}$ (see [12, Corollary 3.7.2]).

Suppose that $R = \mathbb{Z}[\sqrt{-7}]$, $k \in \mathbb{N}_{\geq 2}$ and $B = (\mathbb{N} \times \mathbb{N} \cup \{(0, 0)\}, +) \subset (\mathbb{N}_0^2, +)$. By [12, Example 3.7.3, Special case1], there is a monoid $\mathcal{B}(R)$ such that $\mathcal{L}(R^\bullet) = \mathcal{L}(\mathcal{B}(R))$ and hence $\mathcal{V}_k(R^\bullet) = \mathcal{V}_k(\mathcal{B}(R))$. Furthermore, there is an isomorphism $\Phi: \mathbb{N}_0 \times B \rightarrow \mathcal{B}(R)$. Since every non-zero element of B has a factorization of length 2 (see [12, Example 3.1.8]), it follows that $\mathcal{V}_k(B) = \mathbb{N}_{\geq 2}$ and thus $\mathcal{V}_k(R^\bullet) = \mathbb{N}_{\geq 2}$.

Acknowledgement. We thank the referee for a careful reading. This work was supported by the Austrian Science Fund FWF, Project No. P18779-N13.

References

- [1] J. Amos, S. T. Chapman, N. Hine, J. Paixao, *Sets of lengths do not characterize numerical monoids*, *Integers* **7** (2007), Paper A50, 8p.
- [2] P. Baginski, S. T. Chapman, N. Hine, J. Paixao, *On the asymptotic behavior of unions of sets of lengths in atomic monoids*, *Involve* **1** (2008), 101–110.
- [3] S. T. Chapman, M. Freeze, W. W. Smith, *On generalized lengths of factorizations in Dedekind and Krull domains*, *Non-Noetherian Commutative Ring Theory, Mathematics and Its Applications*, vol. 520, Kluwer Academic Publishers, 2000, pp. 117–137.
- [4] S. T. Chapman, S. Glaz, *One hundred problems in commutative ring theory*, *Non-Noetherian Commutative Ring Theory, Mathematics and Its Applications*, vol. 520, Kluwer Academic Publishers, 2000, pp. 459–476.
- [5] S. T. Chapman, W. W. Smith, *Factorization in Dedekind domains with finite class group*, *Isr. J. Math.* **71** (1990), 65–95.
- [6] ———, *On lengths of factorizations of elements in an algebraic number ring*, *J. Number Theory* **43** (1993), 24–30.
- [7] ———, *Generalized sets of lengths*, *J. Algebra* **200** (1998), 449–471.
- [8] W. Gao, A. Geroldinger, *On products of k atoms*, *Monatsh. Math.*, to appear.
- [9] ———, *Zero-sum problems in finite abelian groups: a survey*, *Expo. Math.* **24** (2006), 337–369.
- [10] A. Geroldinger, *Über nicht-eindeutige Zerlegungen in irreduzible Elemente*, *Math. Z.* **197** (1988), 505–529.
- [11] A. Geroldinger, F. Halter-Koch, *Non-unique factorizations: a survey*, *Multiplicative Ideal Theory in Commutative Algebra* (J.W. Brewer, S. Glaz, W. Heinzer, and B. Olberding, eds.), Springer, 2006, pp. 217–226.

- [12] ———, *Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory*, Pure and Applied Mathematics, vol. 278, Chapman & Hall/CRC, 2006.
- [13] A. Geroldinger, W. Hassler, *Local tameness of v -noetherian monoids*, J. Pure Appl. Algebra **212** (2008), 1509–1524.
- [14] A. Geroldinger, G. Lettl, *Factorization problems in semigroups*, Semigroup Forum **40** (1990), 23–38.
- [15] F. Halter-Koch, *Non-unique factorizations of algebraic integers*, Funct. Approximatio, Comment. Math., **XXXIX.1** (2008), 131–144
- [16] W. Narkiewicz, *Finite abelian groups and factorization problems*, Colloq. Math. **42** (1979), 319–330.
- [17] ———, *Elementary and Analytic Theory of Algebraic Numbers, 3rd ed.*, Springer, 2004.
- [18] W. A. Schmid, *Characterization of class groups of Krull monoids via their systems of sets of lengths: a status report*, HRI Conference Proceedings, ed. by S.D. Adhikari and R. Thangadurai, (2008)
- [19] ———, *A realization theorem for sets of lengths*, manuscript.

Addresses: M. Freeze, The University of North Carolina at Wilmington Department of Mathematics and Statistics Wilmington, North Carolina 28403-2870, USA

A. Geroldinger, Institut für Mathematik und Wissenschaftliches Rechnen Karl–Franzens–Universität Graz Heinrichstraße 36 8010 Graz, Austria

E-mail: freeze@uncw.edu, alfred.geroldinger@uni-graz.at

Received: 1 October 2007; **revised:** 15 January 2008