Monatsh Math (2008)
DOI 10.1007/s00605-008-0547-z
Printed in The Netherlands

Monatshefte für
Mathematik

On products of k atoms

By

Weidong Gao[1] and **Alfred Geroldinger**[2]

[1] Nankai University, Tianjin, P.R. China
[2] Karl-Franzens-Universität Graz, Graz, Austria

Communicated by J. Schoißengeier

Received October 4, 2007; accepted in final form November 13, 2007
Published online May 21, 2008

Abstract. Let H be an atomic monoid. For $k \in \mathbb{N}$ let $\mathscr{V}_k(H)$ denote the set of all $m \in \mathbb{N}$ with the following property: There exist atoms (irreducible elements) $u_1, \ldots, u_k, v_1, \ldots, v_m \in H$ with $u_1 \cdot \ldots \cdot u_k = v_1 \cdot \ldots \cdot v_m$. We show that for a large class of noetherian domains satisfying some natural finiteness conditions, the sets $\mathscr{V}_k(H)$ are almost arithmetical progressions. Suppose that H is a Krull monoid with finite cyclic class group G such that every class contains a prime (this includes the multiplicative monoids of rings of integers of algebraic number fields). We show that, for every $k \in \mathbb{N}$, $\max \mathscr{V}_{2k+1}(H) = k|G| + 1$ which settles Problem 38 in [4].

2000 Mathematics Subject Classification: 11R27, 13F05, 13A05, 20M14
Key words: Non-unique factorizations, sets of lengths, Krull monoids

1. Introduction

Let H be an atomic monoid. This means a commutative cancellative semigroup with unit element such that every non-unit may be written as a finite product of atoms (irreducible elements) of H. The main examples we have in mind are the multiplicative monoids of non-zero elements of noetherian domains. If an element $a \in H$ has a factorization of the form $a = u_1 \cdot \ldots \cdot u_k$, where $k \in \mathbb{N}$ and $u_1, \ldots, u_k \in H$ 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 the most investigated invariants in factorization theory.

In many natural settings (so for example if H is the multiplicative monoid of non-zero elements of a noetherian domain) all sets of lengths are finite, and a straightforward argument shows 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 $|\mathsf{L}(a)| \geqslant N$. 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). In the meantime it is well known that 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 [13, Section 4.7] for an overview).

In 1990, Chapman and Smith [5] introduced, for every $k \in \mathbb{N}$, the unions $\mathscr{V}_k(H)$ of all sets of lengths containing k (see Definition 3.1), and let $\rho_k(H) \in \mathbb{N} \cup \{\infty\}$ denote the supremum of $\mathscr{V}_k(H)$. Obviously, unions of sets of lengths have a simpler structure than sets of lengths themselves. If H is a Krull monoid such that every class contains a prime, then all sets $\mathscr{V}_k(H)$ are intervals (see [10, Theorem 4.2]). Such a result cannot be expected in general, not even for finitely generated monoids. In Theorem 4.2 we present a structure theorem for unions of sets of lengths under very mild finiteness assumptions: these unions are arithmetical progressions apart from possible gaps in their beginning and end part, provided that either, $\rho_k(H) = \infty$ for some $k \in \mathbb{N}$, or that there is an $M \in \mathbb{N}$ such that $\rho_k(H) - \rho_{k-1}(H) \leqslant M$ for all $k \geqslant 2$. In Section 3 we verify this assumption among others for Krull monoids with finite Davenport constant (Corollary 3.6) and for C-monoids (Theorem 3.10).

In Section 4 we study Krull monoids H with finite cyclic class group G such that every class contains a prime (this setting includes rings of integers in algebraic number fields, and more generally holomorphy rings in global fields). The problem to determine $\rho_3(H)$ was first tackled in [7, Section 5] where the bound $\rho_3(H) \leqslant (4|G| - 1)/3$ was established. Furthermore, it was observed that $\rho_3(H) = |G| + 1$ for $|G| \in [3, 8]$. Theorem 5.3 shows that $\rho_{2k+1}(H) = k|G| + 1$ for all $k \in \mathbb{N}$ which settles Problem 38 in [4]. The proof is based on recent results by Savchev and Chen [21, Proposition 10] and by Pingzhi Yuan [23, Theorem 3.1].

2. Preliminaries

Our notation and terminology is consistent with [13]. 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 $[a, b] = \{x \in \mathbb{Z} \mid a \leqslant x \leqslant b\}$. Let $A, B \subset \mathbb{Z}$ be 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 $A \cap [l, l + d] = \{l, l + d\}$. The set A is called an *arithmetical progression with difference* d if $\Delta(A) \subset \{d\}$. Note that $\Delta(\emptyset) = \emptyset$ and that an arithmetical progression may be empty, finite or infinite. If $A \subset \mathbb{N}$, we call

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

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

By a monoid we mean a commutative semigroup with unit element which satisfies the cancellation laws. Let H be a monoid. We denote by $H^\times$ the set of invertible elements of H, by $H_{\text{red}} = H/H^\times = \{aH^\times \mid a \in H\}$ the associated reduced monoid, and by $\mathsf{q}(H)$ a quotient group of H.

A monoid F is called *free* (*with basis* $P \subset F$) if every $a \in F$ has a unique representation in the form

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

In this case, F is (up to canonical isomorphism) uniquely determined by P (and conversely P is uniquely determined by F). We set $F = \mathscr{F}(P)$, and if a is as above, then we call

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

The monoid H is called a *Krull monoid* if it is v-noetherian and completely integrally closed (equivalently, H_{red} is a saturated submonoid of a free monoid F, that is $H_{\text{red}} = F \cap \mathsf{q}(H_{\text{red}})$). If H is a Krull monoid, then its class group is denoted by $\mathscr{C}(H)$ (see [13, Definition 2.4.9]). For all the terminology used in the theory of Krull monoids we refer to one of the monographs [13], [17], [18].

Next we recall some basic arithmetical notions from factorization theory. We denote by $\mathscr{A}(H)$ the *set of atoms* of H, and we call $\mathsf{Z}(H) = \mathscr{F}(\mathscr{A}(H_{\text{red}}))$ the *factorization monoid* of H. Further, $\pi : \mathsf{Z}(H) \to H_{\text{red}}$ denotes the natural homomorphism. For $a \in H$ the set $\mathsf{Z}(a) = \mathsf{Z}_H(a) = \pi^{-1}(aH^\times) \subset \mathsf{Z}(H)$ is called the *set of factorizations* of a, $\mathsf{L}(a) = \mathsf{L}_H(a) = \{|z| \,|\, z \in \mathsf{Z}(a)\} \subset \mathbb{N}_0$ is called the *set of lengths* of a and $\mathscr{L}(H) = \{\mathsf{L}(a) | a \in H\}$ is called the *system of sets of lengths* of H.

H is said to be *atomic* if $\mathsf{Z}(a) \neq \emptyset$ for all $a \in H$ (equivalently, every non-unit of H may be written as a finite product of atoms of H). H is said to be *factorial* if one of the following equivalent statements is satisfied:

- $|\mathsf{Z}(a)| = 1$ for all $a \in H$.
- Every non-unit of H may be written as a finite product of primes of H.
- H_{red} is a free monoid.
- H is a Krull monoid with trivial class group.

For the rest of this section we suppose that H is atomic. If H is v-noetherian, then all sets of lengths are finite (see [13, Theorem 2.2.9]), and arithmetical invariants describing sets of lengths are well investigated. We need the following two notions. For an element $a \in H$ we call $\rho(a) = \rho(\mathsf{L}(a))$ the *elasticity* of a. Furthermore,

$$\rho(H) = \sup\{\rho(L) | L \in \mathscr{L}(H)\} \in \mathbb{R}_{\geqslant 1} \cup \{\infty\}$$

is the *elasticity* of H, and the *set of distances* of H is defined by

$$\Delta(H) = \bigcup_{L \in \mathscr{L}(H)} \Delta(L).$$

We recall the concept of the *distance* of two factorizations and the concept of *local tameness*, which is a basic finiteness property in factorization theory. Let $z, z' \in \mathsf{Z}(H)$. Then we can write

$$z = u_1 \cdot \ldots \cdot u_l v_1 \cdot \ldots \cdot v_m \quad \text{and} \quad z' = u_1 \cdot \ldots \cdot u_l w_1 \cdot \ldots \cdot w_n,$$

where $l, m, n \in \mathbb{N}_0$, $u_1, \ldots, u_l, v_1, \ldots, v_m, w_1, \ldots, w_n \in \mathscr{A}(H_{\text{red}})$ such that

$$\{v_1, \ldots, v_m\} \cap \{w_1, \ldots, w_n\} = \emptyset.$$

We call $\mathsf d(z,z') = \max\{m,\, n\} \in \mathbb N_0$ the *distance* of z and z'. For a factorization $x \in \mathsf Z(H)$ and $a \in H$ we define the *tame degree* $\mathsf t(a,x)$ to be the smallest $N \in \mathbb N_0 \cup \{\infty\}$ with the following property:

If $\mathsf Z(a) \cap x\mathsf Z(H) \neq \emptyset$ and $z \in \mathsf Z(a)$, then there exists some factorization $z' \in \mathsf Z(a) \cap x\mathsf Z(H)$ such that $\mathsf d(z,z') \leqslant N$.

We set $\mathsf t(H,x) = \sup\{\mathsf t(a,x) \,|\, a \in H\}$. The monoid H is called *locally tame* if $\mathsf t(H,u) < \infty$ for all $u \in \mathscr A(H_{\red})$, and it is called *tame* if

$$\mathsf t(H) = \sup\{\mathsf t(H,u) \,|\, u \in \mathscr A(H_{\red})\} < \infty.$$

Block monoids over subsets of abelian groups are a crucial tool for the investigation of Krull monoids. Let G be an additive, abelian group, $G_0 \subset G$ a subset and $\mathscr F(G_0)$ the free monoid with basis G_0. According to the tradition of combinatorial number theory, the elements of $\mathscr F(G_0)$ are called *sequences over* G_0. If $S \in \mathscr F(G_0)$, then

$$S = g_1 \cdot \ldots \cdot g_l = \prod_{g \in G_0} g^{\mathsf v_g(S)},$$

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

$$\mathscr B(G_0) = \{S \in \mathscr F(G_0) \,|\, \sigma(S) = 0\}$$

is called the *block monoid* over G_0, and we have $\mathscr B(G_0) = \mathscr B(G) \cap \mathscr F(G_0)$. 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 $*(\mathscr B(G_0))$. In particular, we set $\mathscr A(G_0) = \mathscr A(\mathscr B(G_0))$, $\rho(G_0) = \rho(\mathscr B(G_0))$ and $\Delta(G_0) = \Delta(\mathscr B(G_0))$. We define the *Davenport constant* of G_0 by

$$\mathsf D(G_0) = \sup\{|U| \,|\, U \in \mathscr A(G_0)\} \in \mathbb N_0 \cup \{\infty\},$$

which is a central invariant in zero-sum theory (see [12]).

3. On the difference $\rho_k(H) - \rho_{k-1}(H)$

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

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

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

The invariants $\rho_k(H)$ were introduced in [16], and the sets $\mathscr V_k(H)$ were first studied in [5]. 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 [15, Corollary 4.3]). In this section

we study the growth rate (in k) of the invariants $\rho_k(H)$. We prove that tame monoids, products of finitely primary monoids and C-monoids satisfy the following property:

Either, $\rho_k(H) = \infty$ for some $k \in \mathbb{N}$ (and then clearly $\rho_l(H) = \infty$ for all $l \geqslant k$), or there is an $M \in \mathbb{N}$ such that $\rho_k(H) - \rho_{k-1}(H) \leqslant M$ for all $k \geqslant 2$.

This is the crucial assumption in the structure theorem for unions of sets of lengths in Section 4.

We start with a lemma which gathers some elementary properties of the $\mathscr{V}_k(H)$ sets and of $\rho_k(H)$ and $\lambda_k(H)$ which will be used throughout without further mentioning.

Lemma 3.2. *Let H be an atomic monoid with $H \neq H^\times$ and $k, l \in \mathbb{N}$.*

1. $\mathscr{V}_1(H) = \{1\}$, $k \in \mathscr{V}_k(H)$ *and*
$$\mathscr{V}_k(H) = \bigcup_{k \in L, L \in \mathscr{L}(H)} L.$$
2. $\rho_k(H) = \sup\{\sup L \mid L \in \mathscr{L}(H),\ k \in L\} = \sup\{\sup L \mid L \in \mathscr{L}(H),\ \min L \leqslant k\}$.
3. $\lambda_k(H) = \min\{\min L \mid L \in \mathscr{L}(H),\ k \in L\}$.
4. $\mathscr{V}_k(H) + \mathscr{V}_l(H) \subset \mathscr{V}_{k+l}(H)$ *and*
$$\lambda_{k+l}(H) \leqslant \lambda_k(H) + \lambda_l(H) \leqslant k + l \leqslant \rho_k(H) + \rho_l(H) \leqslant \rho_{k+l}(H).$$
5. *We have $l \in \mathscr{V}_k(H)$ if and only if $k \in \mathscr{V}_l(H)$.*

Proof. The second equality in 2. follows from [13, Proposition 1.4.2.2], and all remaining statements are straightforward. □

We would like to thank Guy Barat for the crucial argument in the proof of the following limit assertion.

Lemma 3.3. *Let H be an atomic monoid with $H \neq H^\times$.*

1. *We have*
$$\rho(H) = \sup\left\{ \frac{\rho_k(H)}{k} \,\middle|\, k \in \mathbb{N} \right\} = \lim_{k \to \infty} \frac{\rho_k(H)}{k}$$
and
$$\frac{1}{\rho(H)} = \inf\left\{ \frac{\lambda_k(H)}{k} \,\middle|\, k \in \mathbb{N} \right\} = \lim_{k \to \infty} \frac{\lambda_k(H)}{k},$$
with the usual convention that $1/\rho(H) = 0$ if $\rho(H) = \infty$.

2. *Let $\rho(H) < \infty$ and $M \in \mathbb{N}$ such that $k\rho(H) - \rho_k(H) \leqslant M$ for all $k \in \mathbb{N}$. Then $\rho_k(H) - \rho_{k-1}(H) \leqslant M + \rho(H)$ for all $k \geqslant 2$.*

3. *If there is some $a \in H$ such that $\rho(a) = \rho(H) < \infty$, then there is an $M \in \mathbb{N}$ such that $k\rho(H) - \rho_k(H) \leqslant M$ for all $k \in \mathbb{N}$.*

Proof. 1. The first assertion follows from [13, Proposition 1.4.2].

To verify the second one, let $k \in \mathbb{N}$ be given. By definition of $\rho(H)$, we have $k \leqslant \lambda_k(H)\rho(H)$, and hence it suffices to verify the limit assertion. We distinguish two cases.

Case 1. $\rho_m(H) < \infty$ for all $m \in \mathbb{N}$. Let $l \in \mathbb{N}$ be maximal such that $\rho_l(H) \leqslant k$. Then $k = \rho_l(H) + j$ with $j \in [0, \rho_{l+1}(H) - \rho_l(H))$, and we obtain that

$$\begin{aligned}\frac{1}{\rho(H)} &\leqslant \frac{\lambda_k(H)}{k} \leqslant \frac{\lambda_{\rho_l(H)}(H) + \lambda_j(H)}{\rho_l(H) + j} \leqslant \frac{l + j}{\rho_l(H) + j} \\ &\leqslant \frac{l + (\rho_{l+1}(H) - \rho_l(H))}{\rho_l(H) + (\rho_{l+1}(H) - \rho_l(H))} = \frac{l}{\rho_{l+1}(H)} + 1 - \frac{\rho_l(H)}{l}\frac{l}{\rho_{l+1}(H)}.\end{aligned}$$

Since the right hand side tends to $1/\rho(H)$ if l tends to infinity, the assertion follows.

Case 2. There is an $m \in \mathbb{N}$ such that $\rho_m(H) = \infty$. We set $\mathscr{V}_m(H) \cap \mathbb{N}_{\geqslant m} = \{G_1, G_2, \ldots\}$ where $m = G_1 < G_2 < \ldots$, and let $G_0 = 1$. Let $N \in \mathbb{N}_0$ be maximal with $G_N \leqslant k$. Then k has a unique representation in the form

$$k = \sum_{i=0}^{N} a_i G_i, \quad \text{and we set } S(k) = \sum_{i=0}^{N} a_i,$$

where $a_0, \ldots, a_N \in \mathbb{N}_0$, $a_N > 0$, and starting with a_N, the elements $a_N, a_{N-1}, \ldots$ are chosen to be maximal possible. This implies that, for all $l \in [1, N+1]$, $\sum_{i=0}^{l-1} a_i G_i < G_l$ and hence

$$S(k) = \sum_{i<l} a_i + \sum_{i \geqslant l} a_i \leqslant \sum_{i<l} a_i G_i + \frac{1}{G_l}\sum_{i \geqslant l} a_i G_i \leqslant G_l + \frac{k}{G_l}.$$

Therefore for every $\varepsilon > 0$ there is an $l \in \mathbb{N}$ such that $1/G_l < \varepsilon/2$, and thus for all $n > 2G_l/\varepsilon$ we have

$$\frac{S(n)}{n} \leqslant \frac{G_l}{n} + \frac{1}{G_l} < \varepsilon,$$

hence

$$\lim_{n\to\infty} \frac{S(n)}{n} = 0.$$

Since $\mathscr{V}_m(H) \cap \mathbb{N}_{\geqslant m} = \{G_1, G_2, \ldots\}$ and $k = \sum_{i=0}^{N} a_i G_i$, there is a product of k atoms which has a factorization of length

$$a_0 + m\sum_{i=1}^{N} a_i \leqslant mS(k),$$

hence

$$\lambda_k(H) \leqslant mS(k) \quad \text{and} \quad 0 \leqslant \lim_{n\to\infty} \frac{\lambda_n(H)}{n} \leqslant \lim_{n\to\infty} \frac{mS(n)}{n} = 0.$$

2. If $k \geqslant 2$, then 1. implies that $\rho_k(H) \leqslant k\rho(H)$ and since $(k-1)\rho(H) - \rho_{k-1}(H) \leqslant M$, we obtain the assertion.

3. By [13, Proposition 1.4.2.3], there exists some $N \in \mathbb{N}$ such that $\rho_{iN}(H) = iN\rho(H)$ for all $i \in \mathbb{N}$. Let $k = iN + j$ with $i \in \mathbb{N}_0$ and $j \in [1, N]$. Then

$$iN\rho(H) + j \leqslant \rho_{iN}(H) + \rho_j(H) \leqslant \rho_{iN+j}(H)$$

and hence

$$(iN + j)\rho(H) - N(\rho(H) - 1) \leqslant (iN + j)\rho(H) - j(\rho(H) - 1) \leqslant \rho_{iN+j}(H).$$

Thus the assertion holds with $M = N(\rho(H) - 1)$. □

A subset $U \subset H$ is called an *almost generating set* of H if $U \cap H^\times = \emptyset$ and if there exists some $n \in \mathbb{N}$ such that $(H \setminus H^\times)^n \subset UH$. We denote by $\mathscr{M}(U)$ the smallest $n \in \mathbb{N}$ with this property. Let $U \subset H$ be an almost generating set. We shall need the following simple fact. If $a \in H \setminus UH$ and $k = \max \mathsf{L}(a)$, then $(H \setminus H^\times)^{\mathscr{M}(U)} \subset UH$ implies that $k < \mathscr{M}(U)$.

Lemma 3.4. *Let H be an atomic monoid such that $\rho_k(H) < \infty$ for all $k \in \mathbb{N}$. Suppose that there exist an almost generating set $U \subset H \setminus H^\times$ and constants $M_1, M_2 \in \mathbb{N}$ such that the following two properties are satisfied*:

(a) $\sup\{\sup \mathsf{L}(u) | u \in U\} \leqslant M_1$.

(b) *For all $a \in UH$ and all $z \in \mathsf{Z}(a)$ there are $u \in U$, $\mathsf{u} \in \mathsf{Z}(u)$ and $z' \in \mathsf{u}\mathsf{Z}(H) \cap \mathsf{Z}(a)$ such that $\mathsf{d}(z, z') \leqslant M_2$ and $\min \mathsf{L}(u^{-1}a) < \min \mathsf{L}(a)$.*

Then $\rho_k(H) - \rho_{k-1}(H) \leqslant \max\{\mathscr{M}(U) - 2, M_1 + M_2\}$ for all $k \geqslant 2$.

Proof. Let $k \geqslant 2$. If $\rho_k(H) \leqslant \mathscr{M}(U) - 1$, then $\rho_k(H) - \rho_{k-1}(H) \leqslant \rho_k(H) - 1 \leqslant \mathscr{M}(U) - 2$. Suppose that $\rho_k(H) \geqslant \mathscr{M}(U)$. We choose an element $a \in H$ with $\min \mathsf{L}(a) \leqslant k$, $\max \mathsf{L}(a) = \rho_k(H)$ and a factorization $z \in \mathsf{Z}(a)$ with $|z| = \max \mathsf{L}(a)$. Since $\max \mathsf{L}(a) \geqslant \mathscr{M}(U)$, there exist $u \in U$, $\mathsf{u} \in \mathsf{Z}(u)$, $y \in \mathsf{Z}(H)$ and $z' = \mathsf{u}y \in \mathsf{Z}(a)$ such that $\mathsf{d}(z, z') \leqslant M_2$ and $\min \mathsf{L}(u^{-1}a) < \min \mathsf{L}(a)$. Therefore we obtain that

$$\rho_k(H) - \rho_{k-1}(H) \leqslant |z| - |y| = |z| - |\mathsf{u}y| + |\mathsf{u}| \leqslant \mathsf{d}(z, z') + |\mathsf{u}| \leqslant M_1 + M_2.$$

□

Theorem 3.5. *Let H be a tame monoid. Then $\Delta(H)$ is finite, $\rho(H) \leqslant \max\{1, \mathsf{t}(H)\}$ and $\rho_k(H) - \rho_{k-1}(H) \leqslant 1 + \mathsf{t}(H)$ for all $k \geqslant 2$. If, in particular,*

(a) *H is factorial, then $\rho(H) = 1$ and $1 = \rho_k(H) - \rho_{k-1}(H) = 1 + \mathsf{t}(H) = 1$ for all $k \geqslant 2$.*

(b) *H_{red} is finitely generated, then there is an $M \in \mathbb{N}$ such that $k\rho(H) - \rho_k(H) \leqslant M$ for all $k \in \mathbb{N}$.*

Proof. We may suppose that H is reduced. Then $\Delta(H)$ is finite by [13, Theorems 1.6.3 and 1.6.7]. We set $U = \mathscr{A}(H)$. Then U is an almost generating set of H with $\mathscr{M}(U) = 1$. We verify the two properties of Lemma 3.4. Clearly, Property (a) holds with $M_1 = 1$. Let $a \in H \setminus H^\times$ and $a = u_1 \cdot \ldots \cdot u_s$ with $s = \min \mathsf{L}(a)$ and $u_1, \ldots, u_s \in U$. Then $\min \mathsf{L}(u_2 \cdot \ldots \cdot u_s) = s - 1$, and there is some $z' \in u_1\mathsf{Z}(H) \cap \mathsf{Z}(a)$ such that $\mathsf{d}(z, z') \leqslant \mathsf{t}(H, u_1) \leqslant \mathsf{t}(H)$. Thus Property (b) holds with $M_2 = \mathsf{t}(H)$.

Suppose that H is factorial. Then by definition we have $\rho(H) = 1$ and $\mathsf{t}(H) = 0$, and thus the assertion follows.

Suppose that $H_{\red}$ is finitely generated. Then by [13, Theorem 3.1.4] there is some $a \in H$ such that $\rho(a) = \rho(H) < \infty$. Thus the assertion follows from Lemma 3.3.3. □

In the following corollary we deal with Krull monoids. Recall that an integral domain R is a Krull domain if and only if its multiplicative monoid $R\setminus\{0\}$ is a Krull monoid. Furthermore, for every finite subset G_0 of any abelian group G the Davenport constant $\mathsf{D}(G_0)$ is finite, but the converse does not hold (see [13, Theorem 3.4.2 and Example 3.4.3]).

Corollary 3.6. *Let H be a Krull monoid with class group G and let $G_P \subset G$ denote the set of classes containing primes. If $\mathsf{D}(G_P) < \infty$, then $\Delta(H)$ is finite and*

$$\rho_k(H) - \rho_{k-1}(H) \leqslant 2 + \frac{\mathsf{D}(G_P)(\mathsf{D}(G_P) - 1)}{2} \quad \text{for all } k \geqslant 2.$$

Proof. Suppose that $\mathsf{D}(G_P) < \infty$. Then [13, Theorem 3.4.10.6] implies that

$$\mathsf{t}(H) \leqslant 1 + \frac{\mathsf{D}(G_P)(\mathsf{D}(G_P) - 1)}{2}.$$

Thus H is a tame monoid, and the assertion follows from Theorem 3.5. □

We recall the concepts of finitely primary monoids and of weakly Krull domains. Details may be found in [13, Sections 2.9 and 2.10]. The monoid H is called *finitely primary* if there exist $s, \alpha \in \mathbb{N}$ such that H is a submonoid of a factorial monoid $F = F^\times \times [p_1, \ldots, p_s]$ with s pairwise non-associated prime elements $p_1, \ldots, p_s$ satisfying

$$H\setminus H^\times \subset p_1 \cdot \ldots \cdot p_s F \quad \text{and} \quad (p_1 \cdot \ldots \cdot p_s)^\alpha F \subset H.$$

If this is the case, then we say that H is finitely primary of *rank* s and *exponent* α. The significance of finitely primary monoids stems from their appearance in ring theory.

A domain R is called a *weakly Krull domain* if it is v-noetherian and v-$\max(R) = \mathfrak{X}(R)$ (see [13, Definition 2.10.11], and [18, Chapters 22 and 24.5] for a more general notion of weakly Krull domains). Let R be a one-dimensional noetherian domain. Then R is a weakly Krull domain and the monoid of v-invertible v-ideals with v-multiplication coincides with the monoid of invertible ideals with usual ideal multiplication. If moreover its integral closure $\overline{R}$ is a finitely generated R-module, then $(R : \widehat{R}) \neq \{0\}$ and, for every non-zero prime ideal $\mathfrak{p} \subset R$, the multiplicative monoid $H = R_{\mathfrak{p}}\setminus\{0\}$ is finitely primary.

Theorem 3.7. *Let H be a finite product of finitely primary monoids. Then $\Delta(H)$ is finite, and either, $\rho_k(H) = \infty$ for some $k \in \mathbb{N}$, or there is an $M \in \mathbb{N}$ such that $\rho_k(H) - \rho_{k-1}(H) \leqslant M$ for all $k \geqslant 2$.*

Proof. Suppose that $H = D_1 \times D_2$ with submonoids D_1, D_2 of H. By [13, Proposition 1.4.5], the set $\Delta(H)$ is finite if and only if $\Delta(D_1)$ and $\Delta(D_2)$

are both finite, and $\mathscr{L}(H) = \{L_1 + L_2 \mid L_1 \in \mathscr{L}(D_1), L_2 \in \mathscr{L}(D_2)\}$. Therefore, setting $\rho_0(D_1) = \rho_0(D_2) = 0$, we obtain that

$$\rho_k(H) = \sup\{\rho_{k-i}(D_1) + \rho_i(D_2) | i \in [0,k]\}$$

for all $k \in \mathbb{N}$. Thus it suffices to show the assertion for finitely primary monoids.

Let D be a finitely primary monoid of rank s and exponent α. If $s = 1$, then D is tame by [13, Theorem 3.1.5], and hence the assertion follows from Theorem 3.5. If $s \geqslant 2$, then $\Delta(D)$ is finite and $\min \mathsf{L}(a) \leqslant 2\alpha$ for all $a \in D$ (again by [13, Theorem 3.1.5]), which implies that $\rho_{2\alpha}(D) = \infty$. □

Corollary 3.8. *Let R be a weakly Krull domain, $\mathfrak{f} = (R : \widehat{R}) \neq \{0\}$ and $H = (\mathscr{I}_v^*(R), \cdot_v)$ the monoid of v-invertible v-ideals with v-multiplication. Then $\Delta(H)$ is finite, and either, $\rho_k(H) = \infty$ for some $k \in \mathbb{N}$, or there is an $M \in \mathbb{N}$ such that $\rho_k(H) - \rho_{k-1}(H) \leqslant M$ for all $k \geqslant 2$.*

Proof. By [13, Theorem 3.7.1], $\Delta(H)$ is finite, and $H \cong \mathscr{F}(P) \times T$ where T is a finite product of finitely primary monoids. Thus the assertion follows from Theorem 3.7. □

We recall the concept of C-monoids (see [13, Sections 2.9 and 2.11] for some background information and [14] for recent progress). The monoid H is called a C-*monoid* if it is a submonoid of a factorial monoid $F = F^\times \times \mathscr{F}(P)$ such that $H \cap F^\times = H^\times$ and the class semigroup $\mathscr{C}^*(H,F)$ is finite. If this is the case, then there exist some $\alpha \in \mathbb{N}$ such that

$$q^{2\alpha}F \cap H = q^\alpha(q^\alpha F \cap H) \quad \text{for all } q \in F \setminus F^\times .$$

We refer to these properties by saying that *H is defined in F with exponent α*. A subset $E \subset P$ is called *H-essential* if there is some $x \in H \setminus F^\times$ such that $E = \{p \in P \mid \mathsf{v}_p(x) > 1\}$. H is called *simple* (in F) if every minimal H-essential subset of P is a singleton. To point out a crucial example for C-monoids, let R be a Mori domain with complete integral closure $\widehat{R}$ such that the conductor $\mathfrak{f} = (R : \widehat{R})$ is non-zero and the ring $R/\mathfrak{f}$ and the v-class group of $\widehat{R}$ are both finite. Then the multiplicative monoid $R \setminus \{0\}$ is a C-monoid (see [13, Theorem 2.11.9]). Note that these finiteness assumptions are satisfied for all orders in algebraic number fields and for a large number of higher-dimensional finitely generated algebras over $\mathbb{Z}$ (see [19], [20] for details).

Proposition 3.9. *Let H be a reduced* C*-monoid defined in a factorial monoid $F = F^\times \times \mathscr{F}(P)$ with exponent $\alpha \in \mathbb{N}$ such that P and $F^\times$ are finite.*

1. *Let $u \in \mathscr{A}(H)$, $p \in P$ and $n \in \mathbb{N}_0$.*
   (a) *If $\mathsf{v}_p(u) - n\alpha \geqslant 2\alpha$, then $up^{-n\alpha} \in \mathscr{A}(H)$.*
   (b) *If $\mathsf{v}_p(u) \geqslant 4\alpha$, then $up^{n\alpha} \in \mathscr{A}(H)$.*

2. *Let $a \in H$ and $z \in \mathsf{Z}(a)$ with $|z| > 2^{|P|}$. Then there exist an $u \in \mathscr{A}(H)$ with $\mathsf{v}_p(u) < 4\alpha$ for all $p \in P$ and some $z' \in u\mathsf{Z}(H) \cap \mathsf{Z}(a)$ such that $\mathsf{d}(z,z') \leqslant 2$.*

Proof. 1. See [9, Lemma 4.3].

2. Let $z = u_1 \cdot \ldots \cdot u_k$ with $k > 2^{|P|}$ and $u_1, \ldots, u_k \in \mathscr{A}(H)$. Since $k > 2^{|P|}$, there are distinct $i, j \in [1, k]$, say $i = 1$ and $j = 2$, such that

$$\mathsf{v}_p(u_1) \geqslant 4\alpha \quad \text{if and only if} \quad \mathsf{v}_p(u_2) \geqslant 4\alpha \quad \text{for all } p \in P.$$

Let $Q \subset P$ denote the set of all $p \in P$ with $\mathsf{v}_p(u_1) \geqslant 4\alpha$. If $Q = \emptyset$, then $u = u_1$ and $z' = z$ have the required properties.

Suppose that $Q \neq \emptyset$. For $p \in Q$ let $n_p \in \mathbb{N}_0$ be maximal such that $\mathsf{v}_p(u_1) - n_p\alpha \geqslant 2\alpha$. Then $n_p \geqslant 2$ and $\mathsf{v}_p(u_1) - n_p\alpha < 3\alpha \leqslant 4\alpha$. By 1., we infer that

$$u = u_1' = u_1 \prod_{p \in Q} p^{-n_p\alpha} \in \mathscr{A}(H) \quad \text{and} \quad u_2' = u_2 \prod_{p \in Q} p^{n_p\alpha} \in \mathscr{A}(H).$$

Then $u_1'u_2' = u_1u_2$, $z' = u_1'u_2'u_3 \cdot \ldots \cdot u_k \in u\mathsf{Z}(H) \cap \mathsf{Z}(a)$ and $\mathsf{d}(z, z') = 2$. □

Theorem 3.10. *Let H be a* C*-monoid.*

1. *The set $\Delta(H)$ is finite, and the following statements are equivalent*:
   (a) *H is simple.*
   (b) *$\rho(H) < \infty$.*
   (c) *$\rho_k(H) < \infty$ for all $k \in \mathbb{N}$.*

2. *If H is simple, then there exists an $M \in \mathbb{N}$ such that $\rho_k(H) - \rho_{k-1}(H) \leqslant M$ for all $k \geqslant 2$.*

Proof. 1. By [13, Theorems 3.3.4 and 1.6.3] the set of distances $\Delta(H)$ is finite.

(a) $\Rightarrow$ (b) This follows from [13, Theorem 3.3.1.2].
(b) $\Rightarrow$ (c) This follows from Lemma 3.3.1.
(c) $\Rightarrow$ (a) If H is not simple, then the proof of [13, Theorem 3.3.1.2] shows that there is some $k \leqslant (3\alpha - 1)|\mathrm{supp}_P(a)|$ such that $\rho_k(H) = \infty$.

2. Suppose that H is simple. By [13, Theorem 3.3.4], there is a transfer homomorphism to a reduced C-monoid $\widetilde{H}$ defined in a factorial monoid $F = F^\times \times \mathscr{F}(P)$ where P and $F^\times$ are finite. Since $\rho_k(H) = \rho_k(\widetilde{H})$ for all $k \in \mathbb{N}$, it suffices to study $\widetilde{H}$. We write H instead of $\widetilde{H}$. Suppose that H has exponent α and observe that the assumptions of Proposition 3.9 are satisfied.

Since P is finite, H has a finite almost generating set U' (see [13, Proposition 2.9.15.4]), and hence

$$U = U' \cup \{b \in H \setminus H^\times \mid \max \mathsf{L}(b) \leqslant 2^{|P|}\rho(H)\}$$

is an almost generating set of H. We verify the two properties of Lemma 3.4. Then the assertion follows from Lemma 3.4. Clearly, Property (a) of Lemma 3.4 holds.

To verify Property (b), let $a \in UH$ be given. If $\min \mathsf{L}(a) \leqslant 2^{|P|}$, then $\max \mathsf{L}(a) \leqslant 2^{|P|}\rho(H)$ whence $a \in U$. Thus Property (b) holds with $u = a$ and $\mathsf{u} = z$. Suppose that $\min \mathsf{L}(a) > 2^{|P|}$, and let $y \in \mathsf{Z}(a)$ with $|y| = \min \mathsf{L}(a)$. By Proposition 3.9.2 there exists an $u \in \mathscr{A}(H) \subset U$ with $\sum_{p \in P} \mathsf{v}_p(u) < 4\alpha|P|$ and a factorization $y' = uu_2 \cdot \ldots \cdot u_k \in u\mathsf{Z}(H) \cap \mathsf{Z}(a)$ with $\mathsf{d}(y, y') \leqslant 2$ where $k \in \mathbb{N}$ and $u_2, \ldots, u_k \in \mathscr{A}(H)$. Then it follows that $|y'| = |y| = \min \mathsf{L}(a)$

and $\min \mathsf L(u^{-1}a) = k-1 < k = \min \mathsf L(a)$. Since H is locally tame ([13, Theorem 3.3.3]), it follows that for every $z \in \mathsf Z(a)$ there is a factorization $z' \in u\mathsf Z(H) \cap \mathsf Z(a)$ such that $\mathsf d(z,z') \leqslant \mathsf t(H,u)$. By [13, Proposition 3.3.2], it follows that

$$\mathsf t(H,u) \leqslant |P|((2\alpha-1)(4\alpha|P|+d+1)+\alpha) + \max \mathsf L(u),$$

where $d = \mathsf d(\mathscr C^*(H,F))$ is the Davenport constant of the class semigroup. Since $\mathscr C^*(H,F)$ is finite, we get $d < \infty$ by [13, Proposition 2.8.13], and hence Property (b) of Lemma 3.4 holds with

$$M_2 = |P|((2\alpha-1)(4\alpha|P|+d+1)+\alpha)+1. \qquad \square$$

4. The structure of unions of sets of lengths

Definition 4.1. Let $d \in \mathbb N$ and $M \in \mathbb N_0$. A subset $L \subset \mathbb Z$ is called an *almost arithmetical progression* (AAP for short) with *difference* d and *bound* M if

$$L = y + (L' \cup L^* \cup L'') \subset y + d\mathbb Z$$

where L^* is a non-empty arithmetical progression with difference d such that $\min L^* = 0$, $L' \subset [-M,-1]$, $L'' \subset \sup L^* + [1,M]$ (with the convention that $L'' = \emptyset$ if L^* is infinite) and $y \in \mathbb Z$.

By definition, an AAP is a non-empty subset of $\mathbb Z$, and for finite subsets of $\mathbb Z$, Definition 4.1 coincides with [13, Definition 4.2.1]. If a subset $L \subset \mathbb Z$ is an AAP with difference $d \in \mathbb N$ and some bound $M \in \mathbb N$, then it is an AAP with difference d and bound M^* for all $M^* \geqslant M$. Furthermore, a non-empty subset $L \subset \mathbb N_0$ is an arithmetical progression (with difference d) if and only if it is an AAP (with difference d) and bound $M = 0$.

In Theorem 4.2 we show that – under mild assumptions – unions of sets of lengths are AAPs (under much more restrictive assumptions unions of sets of lengths may even turn out to be arithmetical progressions, see [10, Theorems 3.7 and 4.2]). In finitely primary monoids even sets of lengths are AAPs (see [13, Theorem 4.3.6]). However, already in Krull monoids with finite class group, sets of lengths need not be AAPs but have a more general structure (see [13, Section 4.7] and [22]). We point out that only in very special cases the sets $\mathscr V_k(H)$ have been written down explicitly. In [1, Theorem 2.6] this is done for numerical monoids generated by an arithmetical progression. In [13, Section 7.3], the systems of sets of lengths $\mathscr L(G)$ are explicitly determined for some small groups G, from which it is easy to obtain the $\mathscr V_k(G)$ sets.

The asymptotic formula in Theorem 4.2.2 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]).

Theorem 4.2. *Let H be an atomic monoid with finite non-empty set of distances $\Delta(H)$ and $d = \min \Delta(H)$. Suppose that either, $\rho_k(H) = \infty$ for some $k \in \mathbb N$, or that there is an $M \in \mathbb N$ such that $\rho_k(H) - \rho_{k-1}(H) \leqslant M$ for all $k \geqslant 2$.*

1. There exist constants k^* *and* $M^* \in \mathbb{N}$ *such that for all* $k \ge k^*$, $\mathscr{V}_k(H)$ *is an* AAP *with difference* d *and bound* M^*. *Moreover, if* $\rho_k(H) < \infty$ *for all* $k \in \mathbb{N}$, *then the assertion holds for* $k^* = 1$.

2. *We have*

$$\lim_{k\to\infty} \frac{|\mathscr{V}_k(H)|}{k} = \frac{1}{d}\left(\rho(H) - \frac{1}{\rho(H)}\right).$$

Proof. 1. Since $\mathscr{V}_k(H) \subset \lambda_k(H) + d\mathbb{N}_0$ for all $k \in \mathbb{N}$ (see [10, Lemma 3.6.1]), it remains to show that there exist constants $k^*, M^* \in \mathbb{N}$ such that, for all $k \ge k^*$,

$$\mathscr{V}_k(H) \cap [k, \rho_k(H) - M^*] \quad \text{and} \quad \mathscr{V}_k(H) \cap [\lambda_k(H) + M^*, k]$$

are arithmetical progressions with difference d (recall that by our conventions, the empty set is an arithmetical progression, and if $\rho_k(H) = \infty$, then $[k, \rho_k(H) - M^*] = \mathbb{N}_{\ge k}$).

1. (a) Since $d \in \Delta(H)$, there is an element $a \in H$ and $m \in \mathbb{N}$ such that $\{m, m+d\} \subset \mathsf{L}(a)$. Since $\min \Delta(H) = \gcd \Delta(H)$ (see [13, Proposition 1.4.5]), $\psi = \rho(\Delta(H)) - 1 \in \mathbb{N}$. Then $V^* = \{k_0, k_0 + d, \ldots, k_0 + \psi d\} \subset \mathsf{L}(a^\psi)$ where $k_0 = \psi m$. Therefore we have $V^* \subset \mathscr{V}_{k_0}(H)$, say

$$\mathscr{V}_{k_0}(H) = V' \cup V^* \cup V'',$$

where $\min V' = \lambda_{k_0}(H)$, $\max V' < k_0$, $k_0 + \psi d < \min V''$ and $\sup V'' = \rho_{k_0}(H)$.

Now we pick some $k^* \ge 2k_0$, and if there is some $l \in \mathbb{N}$ with $\rho_l(H) = \infty$, let l_0 denote the smallest such $l \in \mathbb{N}$, and we suppose further that $k^* - k_0 \ge l_0$.

Pick $k \ge k^*$. Then

$$\begin{aligned}(V' + \mathscr{V}_{k-k_0}(H)) \cup (V^* + \mathscr{V}_{k-k_0}(H)) \cup (V'' + \mathscr{V}_{k-k_0}(H)) \\ = \mathscr{V}_{k_0}(H) + \mathscr{V}_{k-k_0}(H) \subset \mathscr{V}_k(H).\end{aligned}$$

Clearly, we have $k \in V^* + \mathscr{V}_{k-k_0}(H)$. Since $\max \Delta(\mathscr{V}_{k-k_0}(H)) \leqslant \max \Delta(H)$ and $\Delta(\mathscr{V}_{k-k_0}(H)) \subset d\mathbb{N}$ (see [10, Lemma 3.6]), it follows that $V^* + \mathscr{V}_{k-k_0}(H)$ is an arithmetical progression with difference d. If there is some $l \in \mathbb{N}$ such that $\rho_l(H) = \infty$, then $\rho_{k-k_0}(H) = \rho_k(H) = \infty$ and

$$(V^* + \mathscr{V}_{k-k_0}(H)) \cap \mathbb{N}_{\ge k} = k + d\mathbb{N}_0 = \mathscr{V}_k(H) \cap \mathbb{N}_{\ge k}.$$

Suppose that $\rho_l(H) < \infty$ for all $l \in \mathbb{N}$. Then

$$\max \mathscr{V}_k(H) - \max(V^* + \mathscr{V}_{k-k_0}(H)) = \rho_k(H) - \max V^* - \rho_{k-k_0}(H) \leqslant k_0 M,$$

and hence

$$(V^* + \mathscr{V}_{k-k_0}(H)) \cap [k, \rho_k(H) - k_0 M] = \mathscr{V}_k(H) \cap [k, \rho_k(H) - k_0 M]$$

is an arithmetical progression with difference d. Thus the assertion follows with $M^* = k_0 M$.

1. (b) By 1.(a), there are $k^*, M^* \in \mathbb{N}$ such that for all $k \ge k^*$, the set $\mathscr{V}_k(H) \cap [k, \rho_k(H) - M^*]$ is an arithmetical progression with difference d. Without restriction we may suppose that $M^* \ge k^*$.

Let $k \geqslant k^*$ and $l = \lambda_k(H)$. We show that $\mathscr{V}_k(H) \cap [l + M^*, k]$ is an arithmetical progression with difference d. Let $m \in [l + M^*, k]$ such that $k - m$ is a multiple of d. In order to show that $m \in \mathscr{V}_k(H)$, we verify that $k \in \mathscr{V}_m(H)$. Since

$$k \leqslant \rho_l(H) \quad \text{and} \quad l + M^* \leqslant m,$$

it follows that $k \leqslant \rho_l(H) \leqslant \rho_{m-M^*}(H)$ and hence

$$k + M^* \leqslant \rho_{m-M^*}(H) + M^* \leqslant \rho_{m-M^*}(H) + \rho_{M^*}(H) \leqslant \rho_m(H).$$

Since $k \in m + d\mathbb{N}_0$ with $k \leqslant \rho_m(H) - M^*$ and $\mathscr{V}_m(H) \cap [m, \rho_m(H) - M^*]$ is an arithmetical progression with difference d (because $m \geqslant l + M^* \geqslant k^*$), it follows that $k \in \mathscr{V}_m(H)$.

1. (c) Suppose that $\rho_k(H) < \infty$ for all $k \in \mathbb{N}$, and that the assertion holds with the constants k^* and $M^* \in \mathbb{N}$. Since for all $k \in [1, k^* - 1]$,

$$\mathscr{V}_k(H) = ([\lambda_k(H), k-1] \cap \mathscr{V}_k(H)) \cup \{k\} \cup ([k+1, \rho_k(H)] \cap \mathscr{V}_k(H))$$

is an AAP with bound $M' = \max\{k - \lambda_k(H), \rho_k(H) - k | k \in [1, k^* - 1]\}$, it follows that for all $k \in \mathbb{N}$ the sets $\mathscr{V}_k(H)$ are AAPs with difference d and bound $\widetilde{M} = \max\{M^*, M'\}$.

2. If there is some $k \in \mathbb{N}$ such that $\rho_k(H) = \infty$, then both the left and the right hand side of the asserted equation are infinite (see Lemma 3.3.1). Suppose that $\rho_k(H) < \infty$ for all $k \in \mathbb{N}$. By 1. there are $k^* \in \mathbb{N}$ and $M^* \in d\mathbb{N}$ such that, for all $k \geqslant k^*$, $\mathscr{V}_k(H) \cap [\lambda_k(H) + M^*, \rho_k(H) - M^*]$ is an arithmetical progression with difference d. Thus for all $k \geqslant k^*$ we obtain that

$$\frac{(\rho_k(H) - M^*) - (\lambda_k(H) + M^*) + d}{dk} \leqslant \frac{|\mathscr{V}_k(H)|}{k} \leqslant \frac{\rho_k(H) - \lambda_k(H) + d}{dk}.$$

Since, by Lemma 3.3.1,

$$\lim_{k \to \infty} \frac{\rho_k(H)}{k} = \rho(H) \quad \text{and} \quad \lim_{k \to \infty} \frac{\lambda_k(H)}{k} = \frac{1}{\rho(H)},$$

the assertion follows. □

5. Krull monoids with cyclic class groups

In Krull monoids with class group G all invariants dealing with lengths of factorizations can be studied in the associated block monoid (this is the monoid of zero-sum sequences) over the set of divisor classes $G_P \subset G$ containing primes. This monoid is the link – which is closest if $G_P = G$ – between factorization theory on the one side and additive group theory and combinatorial number theory on the other side. Results from these areas are fundamental for precise arithmetical results in Krull monoids in contrast to abstract finiteness results for more general noetherian domains.

Let H be a Krull monoid with finite class group G such that every class contains a prime, and let $k \in \mathbb{N}$. Then one easily gets (see [13, Section 6.3]) that

$\rho_k(H) = k$ if $|G| \leqslant 2$, and that in case $|G| \geqslant 3$

$$\rho_{2k}(H) = k\mathsf{D}(G) \quad \text{and} \quad k\mathsf{D}(G) + 1 \leqslant \rho_{2k+1}(H) \leqslant k\mathsf{D}(G) + \left\lfloor \frac{\mathsf{D}(G)}{2} \right\rfloor.$$

The only precise results so far show that – in certain types of groups – $\rho_{2k+1}(H)$ attains the upper bound, and this is always done by explicit constructions. It was first observed by Chapman and Smith that in case of cyclic class groups the situation should be different. They conjecture that $\rho_3(H)$ equals the lower bound, that is $\rho_3(H) = |G| + 1$, and they verify this if $|G| \in [3, 8]$ (see [7], [4]). Theorem 5.3 settles their conjecture. Our approach is based on a recent result on the structure of long minimal zero-sum sequences over cyclic groups, which was achieved independently by Savchev and Chen [21] and by Yuan [23].

We start with the definition of the index of a zero-sum sequence (see [3], [11], [8]), and then we state the crucial structural result.

Definition 5.1. Let G be an abelian group.

1. Let $g \in G$ be a non-zero element with $\mathrm{ord}(g) = n < \infty$. For a sequence

$$S = (n_1 g) \cdot \ldots \cdot (n_l g), \quad \text{where } l \in \mathbb{N}_0 \quad \text{and } n_1, \ldots, n_l \in [1, n],$$

we define

$$\|S\|_g = \frac{n_1 + \cdots + n_l}{n}.$$

2. Let S be a zero-sum sequence for which $\langle \mathrm{supp}(S) \rangle \subset G$ is a finite cyclic group. Then we call

$$\mathrm{index}(S) = \min\{\|S\|_g \,|\, g \in G \text{ with } \langle \mathrm{supp}(S) \rangle = \langle g \rangle\} \in \mathbb{N}_0$$

the *index of* S.

3. If G is finite cyclic, then let $\mathsf{l}(G)$ denote the smallest integer $l \in \mathbb{N}$ such that every minimal zero-sum sequence $S \in \mathscr{F}(G)$ of length $|S| \geqslant l$ satisfies $\mathrm{index}(S) = 1$.

If G is a finite cyclic group and $S \in \mathscr{B}(G)$, then obviously

$$\begin{aligned} \mathrm{index}(S) &= \min\{\|S\|_g \,|\, g \in G \text{ with } \mathrm{supp}(S) \subset \langle g \rangle\} \\ &= \min\{\|S\|_g \,|\, g \in G \text{ with } G = \langle g \rangle\}. \end{aligned}$$

Proposition 5.2. *Let G be a cyclic group of order $n \geqslant 1$. If $n \in \{1, 2, 3, 4, 5, 7\}$, then $\mathsf{l}(G) = 1$, and otherwise we have $\mathsf{l}(G) = \lfloor \frac{n}{2} \rfloor + 2$.*

Proof. See [23, Theorem 3.1] or [21, Proposition 10]. □

Theorem 5.3. *Let H be a Krull monoid with cyclic class group G of order $|G| \geqslant 3$. Then for every $k \in \mathbb{N}$ we have*

$$\rho_{2k}(H) \leqslant k|G| \quad \text{and} \quad \rho_{2k+1}(H) \leqslant k|G| + 1.$$

Moreover, if every class contains a prime, then equality holds.

Proof. Without restriction we may suppose that H is reduced. Then there is a free monoid $F = \mathscr{F}(P)$ such that $H \hookrightarrow F$ is a divisor theory and $G = \mathsf{q}(F)/\mathsf{q}(H)$. Let $G_P \subset G$ denote the set of classes containing primes, and let $k \in \mathbb{N}$. Then [13, Theorem 3.4.10] implies that $\rho_k(H) = \rho_k(G_P) \leqslant \rho_k(G)$. It is straightforward that $\rho_{2k}(G) = k|G|$, and that $\rho_k(G) = \infty$ whenever G is infinite and $k \geqslant 2$ (see [13, Proposition 6.3.1] for details). Suppose G is finite. Since $k|G| + 1 = \rho_{2k}(G) + \rho_1(G) \leqslant \rho_{2k+1}(G)$, it is sufficient to prove that $\rho_{2k+1}(G) \leqslant k|G| + 1$.

We set $n = |G|$ and assume to the contrary that there is some $k \in \mathbb{N}$ such that $\rho_{2k+1}(G) \geqslant kn + 2$. Let $k \in \mathbb{N}$ be minimal with this property whence $\rho_{2k-1}(G) = (k-1)n + 1$ and $\rho_{2k+1}(G) \geqslant kn + 2$. Then there exists a $B \in \mathscr{B}(G)$ and minimal zero-sum sequences $U_1, \ldots, U_{2k+1}, V_1, \ldots, V_\rho$ with $\rho = \rho_{2k+1}(G)$ and

$$B = U_1 \cdot \ldots \cdot U_{2k+1} = V_1 \cdot \ldots \cdot V_\rho. \qquad (*)$$

We may suppose that $|B|$ is maximal such that an equation $(*)$ holds. Furthermore, we may suppose that $|U_1| \geqslant \cdots \geqslant |U_{2k+1}|$, and since $\rho_{2k}(G) = kn$, it follows that $0 \nmid B$ whence $|U_{2k+1}| \geqslant 2$.

Suppose there is some $h \in G$ such that $(-h)h|B$, say $h|V_1$ and $(-h)|V_2$. Then

$$V_1V_2 = ((-h)h)V_2' \quad \text{with } V_2' \in \mathscr{A}(G).$$

Thus we may suppose that there is an $\ell \in \mathbb{N}_0$ such that $|V_1| = \cdots = |V_\ell| = 2$, $3 \leqslant |V_{\ell+1}| \leqslant \cdots \leqslant |V_\rho|$ and there is no $h \in G$ with $(-h)h|V_{\ell+1} \cdot \ldots \cdot V_\rho$. If $\ell = 0$, then

$$\rho \leqslant \frac{|U_1 \cdot \ldots \cdot U_{2k+1}|}{3} \leqslant kn + 1,$$

a contradiction. Thus we have $\ell \geqslant 1$.

Suppose there is some $i \in [1, 2k+1]$ such that $\mathrm{index}(U_i) = 1$. Then there is some $g \in G$ with $\mathrm{ord}(g) = n$ such that $U_i = (a_1g) \cdot \ldots \cdot (a_sg)$ with $s = |U_1|$, $a_1, \ldots, a_s \in [1, n]$ and $\|U_i\|_g = 1$. Assume to the contrary that $s < n$. Then there is some $\nu \in [1, s]$, say $\nu = 1$, with $a_1 \geqslant 2$, and there is some $j \in [1, \rho]$ such that $(a_1g)|V_j$. Then

$$U_i' = (a_1g)^{-1}g((a_1 - 1)g)U_i \in \mathscr{B}(G), \quad V_j' = (a_1g)^{-1}g((a_1 - 1)g)V_j \in \mathscr{B}(G)$$

and

$$B' = U_i^{-1}U_i'U_1 \cdot \ldots \cdot U_{2k+1} = V_j^{-1}V_j'V_1 \cdot \ldots \cdot V_\rho.$$

Since $\|U_i\|_g = \|U_i'\|_g = 1$, it follows that $U_i' \in \mathscr{A}(G)$. Since $\rho = \rho_{2k+1}(G)$, it follows that $V_j' \in \mathscr{A}(G)$. But this is a contradiction to the maximality of $|B|$. Thus $s = n$ and $U_i = g^n$.

If $|U_{2k}| \leqslant \lfloor \frac{n}{2} \rfloor + 1$, then

$$\begin{aligned} \rho &\leqslant \frac{|U_1 \cdot \ldots \cdot U_{2k-1}U_{2k}U_{2k+1}|}{2} \\ &\leqslant \frac{1}{2}\left((2k-1)n + \left\lfloor \frac{n}{2} \right\rfloor + 1 + \left\lfloor \frac{n}{2} \right\rfloor + 1\right) \leqslant kn + 1, \end{aligned}$$

a contradiction. Thus $|U_1| \geqslant \cdots \geqslant |U_{2k}| \geqslant \lfloor \frac{n}{2} \rfloor + 2$, and Proposition 5.2 implies that $\mathrm{index}(U_1) = \cdots = \mathrm{index}(U_{2k}) = 1$. Therefore, for all $i \in [1, 2k]$, we have $U_i = g_i^n$ where $g_i \in G$ with $\mathrm{ord}(g_i) = n$.

Suppose there are distinct $i, j \in [1, 2k+1]$ such that $U_i = g^n$ and $U_j = (-g)^n$ for some $g \in G$. Then $\ell \geqslant n$, and after renumbering if necessary we may suppose that $V_1 = \cdots = V_n = (-g)g$. Since $(U_iU_j)^{-1}U_1 \cdot \ldots \cdot U_{2k+1} = V_{n+1} \cdot \ldots \cdot V_\rho$, it follows that $(k-1)n + 1 = \rho_{2k-1}(G) \geqslant (k-1)n + 2$, a contradiction. Thus there are no two U_i, U_j of such a form and hence $\ell \leqslant |U_{2k+1}|$.

Suppose that $\mathrm{index}(U_{2k+1}) = 1$. Then $U_{2k+1} = g_{2k+1}^n$ for some $g_{2k+1} \in G$ with $\mathrm{ord}(g_{2k+1}) = n$. Since $\ell \geqslant 1$, it follows that $g_{2k+1} \in \{-g_1, \ldots, -g_{2k}\}$, a contradiction. Thus $\mathrm{index}(U_{2k+1}) \geqslant 2$. Now Proposition 5.2 implies that

$$|U_{2k+1}| \leqslant \left\lfloor \frac{n}{2} \right\rfloor + 1,$$

and therefore we obtain that

$$\begin{aligned} \rho &\leqslant \ell + \frac{|B| - 2\ell}{3} = \frac{|B| + \ell}{3} = \frac{2kn + |U_{2k+1}| + \ell}{3} \\ &\leqslant \frac{2kn + 2|U_{2k+1}|}{3} \leqslant \frac{2kn + n + 2}{3} \leqslant kn + \frac{2}{3}, \end{aligned}$$

a contradiction. □

Acknowledgement. We thank the referee for a careful reading. This work was supported, partially by NSFC and 973 program, and by the Austrian Science Fund FWF, Project No. P18779-N13. Part of the manuscript was written while the first author was visiting the Fields Institute in Toronto. He is thankful to the Fields Institute for providing excellent atmosphere for research and all their hospitality.

References

[1] Amos J, Chapman ST, Hine N, Paixao J (2007) Sets of lengths do not characterize numerical monoids. Integers **7**: Paper A50, 8 p
[2] Baginski P, Chapman ST, Hine N, Paixao J (2008) On the asymptotic behavior of unions of sets of lengths in atomic monoids. Involve, to appear
[3] Chapman ST, Freeze M, Smith WW (1999) Minimal zero sequences and the strong Davenport constant. Discrete Math **203**: 271–277
[4] Chapman ST, Glaz S (2000) One hundred problems in commutative ring theory. In: Chopman ST et al. (eds) Non-Noetherian Commutative Ring Theory, pp 459–476. Dordrecht: Kluwer
[5] Chapman ST, Smith WW (1990) Factorization in Dedekind domains with finite class group. Israle J Math **71**: 65–95
[6] Chapman ST, Smith WW (1993) On lengths of factorizations of elements in an algebraic number ring. J Number Theory **43**: 24–30
[7] Chapman ST, Smith WW (1998) Generalized sets of lengths. J Algebra **200**: 449–471
[8] Chapman ST, Smith WW (2005) A characterization of minimal zero-sequences of index one in finite cyclic groups. Integers **5**(1): Paper A27, 5p
[9] Foroutan A, Geroldinger A (2005) Monotone chains of factorizations in C-monoids. In: Chapman ST (ed) Arithmetical Properties of Commutative Rings and Monoids, Lect Notes Pure Appl Math 241, pp 99–113. Boca Raton, FL: Chapman & Hall/CRC
[10] Freeze M, Geroldinger A (2008) Unions of sets of lengths. Funct Approximotio, Comment Math, to appear
[11] Gao W (2000) Zero sums in finite cyclic groups. Integers **0**: Paper A14, 9 p
[12] Gao W, Geroldinger A (2006) Zero-sum problems in finite abelian groups: a survey. Expo Math **24**: 337–369
[13] Geroldinger A, Halter-Koch F (2006) Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory. Boca Raton, FL: Chapman & Hall/CRC

[14] Geroldinger A, Hassler W (2008) Arithmetic of Mori domains and monoids. J Algebra **319**: 3419–3463
[15] Geroldinger A, Hassler W (2008) Local tameness of v-noetherian monoids. J Pure Appl Algebra **212**: 1509–1524
[16] Geroldinger A, Lettl G (1990) Factorization problems in semigroups. Semigroup Forum **40**: 23–38
[17] Grillet PA (2001) Commutative Semigroups. Dordrecht: Kluwer
[18] Halter-Koch F (1998) Ideal systems. An Introduction to Multiplicative Ideal Theory. New York: Marcel Dekker
[19] Hassler W (2004) Factorization in finitely generated domains. J Pure Appl Algebra **186**: 151–168
[20] Kainrath F (2005) Elasticity of finitely generated domains. Houston J Math **31**: 43–64
[21] Savchev S, Chen F (2007) Long zero-free sequences in finite cyclic groups. Discrete Math **307**: 2671–2679
[22] Schmid WA (2007) A realization theorem for sets of lengths. Manuscript
[23] Yuan P (2007) On the index of minimal zero-sum sequences over finite cyclic groups. J Comb Theory Ser A **114**: 1545–1551

Authors' addresses: W. Gao, Center for Combinatorics, Nankai University, Tianjin 300071, P.R. China, e-mail: wdgao_1963@yahoo.com.cn; A. Geroldinger, Institut für Mathematik und Wissenschaftliches Rechnen, Karl-Franzens-Universität Graz, Heinrichstraße 36, 8010 Graz, Austria, e-mail: alfred.geroldinger@uni-graz.at