A CHARACTERIZATION OF KRULL MONOIDS FOR WHICH SETS OF LENGTHS ARE (ALMOST) ARITHMETICAL PROGRESSIONS

Alfred Geroldinger, Wolfgang Schmid

A CHARACTERIZATION OF KRULL MONOIDS FOR WHICH SETS OF LENGTHS ARE (ALMOST) ARITHMETICAL PROGRESSIONS

ALFRED GEROLDINGER AND WOLFGANG A. SCHMID

Abstract. Let H be a Krull monoid with finite class group G and suppose that every class contains a prime divisor. Then sets of lengths in H have a well-defined structure which just depends on the class group G. With methods from additive combinatorics we establish a characterization of those class groups G guaranteeing that all sets of lengths are (almost) arithmetical progressions.

1. Introduction

Let H be a Krull monoid with class group G and suppose that every class contains a prime divisor. Then every element has a factorization into irreducibles. If $a = u_1 \cdot \ldots \cdot u_k$ with irreducibles $u_1, \ldots, u_k \in H$, then k is called the factorization length. The set $\mathsf{L}(a) \subset \mathbb{N}_0$ of all possible factorization lengths is finite and called the set of lengths of a. The system $\mathcal{L}(H) = \{\mathsf{L}(a) \mid a \in H\}$ is a well-studied means for describing the arithmetic of H. It is classic that $|L| = 1$ for all $L \in \mathcal{L}(H)$ if and only if $|G| \le 2$ and if $|G| \ge 3$, then there are arbitrarily large $L \in \mathcal{L}(H)$.

Sets of lengths in H can be studied in the associated monoid of zero-sum sequences $\mathcal{B}(G)$. The latter is a Krull monoid again and it is well-known that $\mathcal{L}(H) = \mathcal{L}\big(\mathcal{B}(G)\big)$ (as usual we write $\mathcal{L}(G)$ for $\mathcal{L}\big(\mathcal{B}(G)\big)$. A transfer Krull monoid over G is a monoid having a transfer homomorphism to $\mathcal{B}(G)$ which implies that their systems of sets of lengths coincide. Transfer Krull monoids include various classes of non-commutative Dedekind domains (see Section 2).

If the group G is infinite, then, by a theorem of Kainrath, every finite set $L \subset \mathbb{N}_{\ge 2}$ lies in $\mathcal{L}(H)$ ([23], [14, Theorem 7.4.1]; for further rings and monoids with this property see [8] or [22, Corollary 4.7]). Now suppose that the group G is finite. In this case sets of lengths have a well-defined structure. Indeed, by the Structure Theorem for Sets of Lengths (Proposition 2.2.1), the sets in $\mathcal{L}(G)$ are AAMPs (almost arithmetical multiprogressions) with difference in $\Delta^*(G)$ and some universal bound. By a realization result of the second author, this description is best possible (Proposition 2.2.2). By definition, the concept of an AAMP comprises arithmetical progressions, AAPs (almost arithmetical progressions), and AMPs (arithmetical multiprogressions); definitions are gathered in Definition 2.1. The goal of this paper is to characterize those groups where all sets of lengths are not only AAMPs, but have one of these more special forms. We formulate the main result of this paper.

Theorem 1.1. *Let G be a finite abelian group.*

1. *The following statements are equivalent*:
   (a) *All sets of lengths in $\mathcal{L}(G)$ are arithmetical progressions with difference in $\Delta^*(G)$.*
   (b) *All sets of lengths in $\mathcal{L}(G)$ are arithmetical progressions.*
   (c) *The system of sets of lengths $\mathcal{L}(G)$ is additively closed, that is, $L_1 + L_2 \in \mathcal{L}(G)$ for all $L_1, L_2 \in \mathcal{L}(G)$.*
   (d) *G is cyclic of order $|G| \le 4$ or isomorphic to a subgroup of C_2^3 or isomorphic to a subgroup of C_3^2.*

2010 *Mathematics Subject Classification.* 11B30, 13A05, 13F05, 20M13.

Key words and phrases. Krull monoids, transfer Krull monoids, sets of lengths, zero-sum sequences.

This work was supported by the Austrian Science Fund FWF, Project Number P28864-N35.

2. *The following statements are equivalent*:
   (a) *There is a constant $M \in \mathbb{N}$ such that all sets of lengths in $\mathcal{L}(G)$ are* AAP*s with bound M.*
   (b) *G is isomorphic to a subgroup of C_3^3 or isomorphic to a subgroup of C_4^3.*
3. *The following statements are equivalent*:
   (a) *All sets of lengths in $\mathcal{L}(G)$ are* AMP*s with difference in $\Delta^*(G)$.*
   (b) *G is cyclic with $|G| \le 5$ or isomorphic to a subgroup of C_2^3 or isomorphic to a subgroup of C_3^2.*

A central topic in the study of sets of lengths is the Characterization Problem (for recent progress see [4, 15, 20, 31, 30]) which reads as follows:

> *Let G be a finite abelian group with $\mathsf{D}(G) \ge 4$, and let G' be an abelian group with $\mathcal{L}(G) = \mathcal{L}(G')$. Does it follow that $G \cong G'$?*

A finite abelian group G has Davenport constant $\mathsf{D}(G) \le 3$ if and only if either $|G| \le 3$ or $G \cong C_2 \oplus C_2$. Since $\mathcal{L}(C_1) = \mathcal{L}(C_2)$ and $\mathcal{L}(C_3) = \mathcal{L}(C_2 \oplus C_2)$ (Proposition 3.1), small groups require special attention in the study of the Characterization Problem. As a consequence of Theorem 1.1 we obtain an affirmative answer to the Characterization Problem for all involved small groups.

Corollary 1.2. *Let G be a finite abelian group with Davenport constant $\mathsf{D}(G) \ge 4$ and suppose that $\mathcal{L}(G)$ satisfies one of the properties characterized in Theorem 1.1. If G' is any abelian group such that $\mathcal{L}(G) = \mathcal{L}(G')$, then $G \cong G'$.*

In Section 2 we gather the required tools for studying sets of lengths (Propositions 2.2, 2.3, and 2.4). The proof of Theorem 1.1 requires methods from additive combinatorics and is given in Section 3. Several properties occurring in Theorem 1.1 can be characterized by further arithmetical invariants. We briefly outline this in Remark 3.8 where we also discuss the property of being additively closed occurring in Theorem 1.1.1.(c).

2. Background on sets of lengths

Let $\mathbb{N}$ denote the set of positive integers, $\mathbb{P} \subset \mathbb{N}$ the set of prime numbers and put $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. For real numbers $a, b \in \mathbb{R}$, we set $[a, b] = \{x \in \mathbb{Z} \mid a \le x \le b\}$. Let $A, B \subset \mathbb{Z}$ be subsets of the integers. We denote by $A + B = \{a + b \mid a \in A, b \in B\}$ their *sumset*, and by $\Delta(A)$ the *set of* (*successive*) *distances* of A (that is, $d \in \Delta(A)$ if and only if $d = b - a$ with $a, b \in A$ distinct and $[a, b] \cap A = \{a, b\}$). For $k \in \mathbb{N}$, we denote by $k \cdot A = \{ka \mid a \in A\}$ the dilation of A by k. If $A \subset \mathbb{N}$, then

$$\rho(A) = \sup\Big\{\frac{m}{n} \mid m, n \in A\Big\} = \frac{\sup A}{\min A} \in \mathbb{Q}_{\ge 1} \cup \{\infty\}$$

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

Monoids. By a *monoid*, we always mean a cancellative semigroup with identity. Let H be a monoid. If an element $a \in H$ is a product of k irreducible elements, say $a = u_1 \cdot \ldots \cdot u_k$, then k is a factorization length and the set $\mathsf{L}(a) \subset \mathbb{N}$ of all possible factorization lengths is the *set of lengths* of a. If a is invertible in H, then we set $\mathsf{L}(a) = \{0\}$. We denote by

$$\mathcal{L}(H) = \{\mathsf{L}(a) \mid a \in H\} \qquad \text{the } \textit{system of sets of lengths} \text{ of } H\,, \quad \text{and by}$$

$$\Delta(H) = \bigcup_{L \in \mathcal{L}(H)} \Delta(L) \ \subset \mathbb{N} \qquad \text{the } \textit{set of distances} \text{ of } H\,.$$

For $k \in \mathbb{N}$, we set $\rho_k(H) = k$ if H is a group, and

$$\rho_k(H) = \sup\{\sup L \mid L \in \mathcal{L}(H), k \in L\} \in \mathbb{N} \cup \{\infty\}, \quad \text{otherwise}\,.$$

Then

$$\rho(H) = \sup\{\rho(L) \mid L \in \mathcal{L}(H)\} = \lim_{k \to \infty} \frac{\rho_k(H)}{k} \in \mathbb{R}_{\ge 1} \cup \{\infty\}$$

is the *elasticity* of H.

Zero-Sum Theory. Let G be an additive abelian group, $G_0 \subset G$ a subset, and let $\mathcal{F}(G_0)$ be the free abelian monoid with basis G_0. In Combinatorial Number Theory, the elements of $\mathcal{F}(G_0)$ are called *sequences* over G_0. For a sequence

$$S = g_1 \cdot \ldots \cdot g_l = \prod_{g \in G_0} g^{\mathsf{v}_g(S)} \in \mathcal{F}(G_0)\,,$$

we set $-S = (-g_1) \cdot \ldots \cdot (-g_l)$, and we call $|S| = l = \sum_{g \in G} \mathsf{v}_g(S) \in \mathbb{N}_0$ the *length* of S,

$\mathrm{supp}(S) = \{g \in G \mid \mathsf{v}_g(S) > 0\} \subset G$ the *support* of S, $\mathsf{v}_g(S)$ the *multiplicity* of g in S,

$$\sigma(S) = \sum_{i=1}^{l} g_i \text{ the } \textit{sum} \text{ of } S\,, \text{ and } \Sigma(S) = \Big\{ \sum_{i \in I} g_i \mid \emptyset \neq I \subset [1,l] \Big\} \text{ the } \textit{set of subsequence sums} \text{ of } S\,.$$

The sequence S is said to be

- *zero-sum free* if $0 \notin \Sigma(S)$,
- a *zero-sum sequence* if $\sigma(S) = 0$,
- a *minimal zero-sum sequence* if it is a nontrivial zero-sum sequence and every proper subsequence is zero-sum free.

The monoid

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

is called the *monoid of zero-sum sequences* over G_0. As usual we set, for all $k \in \mathbb{N}$,

$$\rho_k(G_0) = \rho_k\big(\mathcal{B}(G_0)\big),\ \rho(G_0) = \rho\big(\mathcal{B}(G_0)\big),\ \mathcal{L}(G_0) = \mathcal{L}(\mathcal{B}(G_0)),\ \text{ and } \Delta(G_0) = \Delta\big(\mathcal{B}(G_0)\big)\,.$$

The atoms (irreducible elements) of the monoid $\mathcal{B}(G_0)$ are precisely the minimal zero-sum sequences over G_0, and they will be denoted by $\mathcal{A}(G_0)$. If G_0 is finite, then $\mathcal{A}(G_0)$ is finite. The *Davenport constant* $\mathsf{D}(G_0)$ of G_0 is the maximal length of an atom whence

$$\mathsf{D}(G_0) = \sup\big\{|U| \ \big|\ U \in \mathcal{A}(G_0)\big\} \in \mathbb{N}_0 \cup \{\infty\}\,.$$

The *set of minimal distances* $\Delta^*(G) \subset \Delta(G)$ is defined as

$$\Delta^*(G) = \{\min \Delta(G_0) \mid G_0 \subset G \text{ with } \Delta(G_0) \neq \emptyset\} \subset \Delta(G)\,.$$

A tuple $(e_i)_{i \in I}$ is called a *basis* of G if all elements are nonzero and $G = \oplus_{i \in I} \langle e_i \rangle$. For $p \in \mathbb{P}$, let $\mathsf{r}_p(G)$ denote the p-rank of G, $\mathsf{r}(G) = \sup\{\mathsf{r}_p(G) \mid p \in \mathbb{P}\}$ denote the *rank* of G, and let $\mathsf{r}^*(G) = \sum_{p \in \mathbb{P}} \mathsf{r}_p(G)$ be the *total rank* of G.

Transfer Krull monoids. A commutative monoid is a *Krull monoid* if it is completely integrally closed and satisfies the ascending chain condition on divisorial ideals. An integral domain R is a Krull domain if and only if its multiplicative monoid $R \setminus \{0\}$ is a Krull monoid whence every integrally closed noetherian domain is Krull. Rings of integers, holomorphy rings in algebraic function fields, and regular congruence monoids in these domains are Krull monoids with finite class group such that every class contains a prime divisor ([14, Section 2.11]). Monoid domains, power series, and monoids of modules that are Krull are discussed in [21, 24, 25, 3, 1, 7]. Let H be a Krull monoid with class group G such that every class contains a prime divisor. Then there is a transfer homomorphism $\theta\colon H \to \mathcal{B}(G)$ which implies that $\mathcal{L}(H) = \mathcal{L}(G)$ ([14, Theorem 3.4.10]). A *transfer Krull monoid* H over G is a monoid allowing such a transfer homomorphism to $\mathcal{B}(G)$ whence $\mathcal{L}(H) = \mathcal{L}(G)$. Thus Theorem 1.1 applies to transfer Krull monoids over finite abelian groups. Recent deep work, mainly by Baeth and Smertnig, revealed that wide classes of non-commutative Dedekind domains are transfer Krull ([29, 2, 28]). We refer to the survey [11] for a detailed discussion of these and further examples.

Sets of Lengths. Let $A \in \mathcal{B}(G_0)$ and $d = \min\{|U| \mid U \in \mathcal{A}(G_0)\}$. If $A = BC$ with $B, C \in \mathcal{B}(G_0)$, then

$$\mathsf{L}(B) + \mathsf{L}(C) \subset \mathsf{L}(A)\,.$$

If $A = U_1 \cdot \ldots \cdot U_k = V_1 \cdot \ldots \cdot V_l$ with $U_1, \ldots, U_k, V_1, \ldots, V_l \in \mathcal{A}(G_0)$ and $k < l$, then

$$ld \le \sum_{\nu=1}^{l} |V_\nu| = |A| = \sum_{\nu=1}^{k} |U_\nu| \le k\mathsf{D}(G_0) \text{ whence } \frac{|A|}{\mathsf{D}(G_0)} \le \min \mathsf{L}(A) \le \max \mathsf{L}(A) \le \frac{|A|}{d}\,.$$

For sequences over cyclic groups the g-norm plays a similar role as the length does for sequences over arbitrary groups. Let $g \in G$ with $\mathrm{ord}(g) = n \ge 2$. For a sequence $S = (n_1 g) \cdot \ldots \cdot (n_l g) \in \mathcal{F}(\langle g \rangle)$, where $l \in \mathbb{N}_0$ and $n_1, \ldots, n_l \in [1, n]$, we define

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

Note that $\sigma(S) = 0$ implies that $n_1 + \ldots + n_l \equiv 0 \mod n$ whence $\|S\|_g \in \mathbb{N}_0$. Thus, $\|\cdot\|_g \colon \mathcal{B}(\langle g \rangle) \to \mathbb{N}_0$ is a homomorphism, and $\|S\|_g = 0$ if and only if $S = 1$. If $S \in \mathcal{A}(G_0)$, then $\|S\|_g \in [1, n-1]$, and if $\|S\|_g = 1$, then $S \in \mathcal{A}(G_0)$. Arguing as above we obtain that

$$\frac{\|A\|_g}{n-1} \le \min \mathsf{L}(A) \le \max \mathsf{L}(A) \le \|A\|_g\,.$$

Now we recall the concept of almost arithmetical multiprogressions (AAMPs) as given in [14, Chapter 4]. Then we gather results on sets of lengths and on invariants controlling their structure such as the set of distances and the elasticities (Propositions 2.2, 2.3, and 2.4). These results form the basis for the proof of Theorem 1.1 given in the next section.

Definition 2.1. Let $d \in \mathbb{N}$, $l, M \in \mathbb{N}_0$ and $\{0, d\} \subset \mathcal{D} \subset [0, d]$. A subset $L \subset \mathbb{Z}$ is called an

- *arithmetical multiprogression* (AMP for short) with *difference* d, *period* $\mathcal{D}$ and *length* l, if L is an interval of $\min L + \mathcal{D} + d\mathbb{Z}$ (this means that L is finite nonempty and $L = (\min L + \mathcal{D} + d\mathbb{Z}) \cap [\min L, \max L]$), and l is maximal such that $\min L + ld \in L$.
- *almost arithmetical multiprogression* (AAMP for short) with *difference* d, *period* $\mathcal{D}$, *length* l and *bound* M, if
$$L = y + (L' \cup L^* \cup L'') \subset y + \mathcal{D} + d\mathbb{Z}$$
where L^* is an AMP with difference d (whence $L^* \neq \emptyset$), period $\mathcal{D}$ and length l such that $\min L^* = 0$, $L' \subset [-M, -1]$, $L'' \subset \max L^* + [1, M]$ and $y \in \mathbb{Z}$.
- *almost arithmetical progression* (AAP for short) with *difference* d, *bound* M and *length* l, if it is an AAMP with difference d, period $\{0, d\}$, bound M and length l.

Proposition 2.2 (Structural results on $\mathcal{L}(G)$)**.**
Let G be a finite abelian group with $|G| \ge 3$.

1. *There exists some $M \in \mathbb{N}_0$ such that every set of lengths $L \in \mathcal{L}(G)$ is an* AAMP *with some difference $d \in \Delta^*(G)$ and bound M.*
2. *For every $M \in \mathbb{N}_0$ and every finite nonempty set $\Delta^* \subset \mathbb{N}$, there is a finite abelian group G^* such that the following holds: for every* AAMP *L with difference $d \in \Delta^*$ and bound M there is some $y_L \in \mathbb{N}$ such that*
$$y + L \in \mathcal{L}(G^*) \quad \text{for all} \quad y \ge y_L\,.$$
3. *Let $G_0 \subset G$ be a subset. Then there exist a bound $M \in \mathbb{N}_0$ and some $A^* \in \mathcal{B}(G_0)$ such that for all $A \in A^*\mathcal{B}(G_0)$ the set of lengths $\mathsf{L}(A)$ is an* AAP *with difference $\min \Delta(G_0)$ and bound M.*
4. *If $A \in \mathcal{B}(G)$ such that $\mathrm{supp}(A) \cup \{0\}$ is a subgroup of G, then $\mathsf{L}(A)$ is an arithmetical progression with difference* 1.

Proof. The first statement gives the Structure Theorem for Sets of Lengths ([14, Theorem 4.4.11]), which is sharp by the second statement proved in [27]. The third and the fourth statements show that sets of lengths are extremely smooth provided that the associated zero-sum sequence contains all elements of its support sufficiently often ([14, Theorems 4.3.6 and 7.6.8]). □

Proposition 2.3 (Structural results on $\Delta(G)$ and on $\Delta^*(G)$)**.**
Let $G = C_{n_1} \oplus \ldots \oplus C_{n_r}$ where $r, n_1, \ldots, n_r \in \mathbb{N}$ with $r = \mathsf{r}(G)$, $1 < n_1 \mid \ldots \mid n_r$, and $|G| \ge 3$.

1. *$\Delta(G)$ is an interval with*
$$\big[1, \max\{\exp(G) - 2, k - 1\}\big] \subset \Delta(G) \subset \big[1, \mathsf{D}(G) - 2\big] \quad \text{where} \quad k = \sum_{i=1}^{\mathsf{r}(G)} \Big\lfloor \frac{n_i}{2} \Big\rfloor .$$
2. *$1 \in \Delta^*(G) \subset \Delta(G)$, $[1, \mathsf{r}(G) - 1] \subset \Delta^*(G)$, and $\max \Delta^*(G) = \max\{\exp(G) - 2, \mathsf{r}(G) - 1\}$.*
3. *If G is cyclic of order $|G| = n \ge 4$, then $\max\big(\Delta^*(G) \setminus \{n-2\}\big) = \lfloor \frac{n}{2} \rfloor - 1$.*

Proof. The statement on $\max \Delta^*(G)$ follows from [19]. For all remaining statements see [14, Section 6.8]. A more detailed analysis of $\Delta^*(G)$ in case of cyclic groups can be found in [26]. □

Proposition 2.4 (Results on $\rho_k(G)$ and on $\rho(G)$)**.**
Let G be a finite abelian group with $|G| \ge 3$, and let $k \in \mathbb{N}$.

1. *$\rho(G) = \mathsf{D}(G)/2$ and $\rho_{2k}(G) = k\mathsf{D}(G)$.*
2. *$1 + k\mathsf{D}(G) \le \rho_{2k+1}(G) \le k\mathsf{D}(G) + \mathsf{D}(G)/2$. If G is cyclic, then equality holds on the left side.*

Proof. See [14, Chapter 6.3], [10, Theorem 5.3.1], and [13]. □

3. A characterization of extremal cases

The goal of this section is to prove Theorem 1.1 and to do so we proceed in a series of auxiliary results. We first recall some cases where the systems of sets of lengths are completely determined. Then, we proceed to treat the various remaining cases.

Proposition 3.1.

1. $\mathcal{L}(C_1) = \mathcal{L}(C_2) = \big\{\{m\} \mid m \in \mathbb{N}_0\big\}$.
2. $\mathcal{L}(C_3) = \mathcal{L}(C_2 \oplus C_2) = \big\{y + 2k + [0,k] \bigm| y,\, k \in \mathbb{N}_0\big\}$.
3. $\mathcal{L}(C_4) = \big\{y + k + 1 + [0,k] \bigm| y,\, k \in \mathbb{N}_0\big\} \cup \big\{y + 2k + 2 \cdot [0,k] \bigm| y,\, k \in \mathbb{N}_0\big\}$.
4. $\mathcal{L}(C_2^3) = \big\{y + (k+1) + [0,k] \bigm| y \in \mathbb{N}_0,\ k \in [0,2]\big\}$
$\quad \cup \big\{y + k + [0,k] \bigm| y \in \mathbb{N}_0,\ k \ge 3\big\} \cup \big\{y + 2k + 2 \cdot [0,k] \bigm| y,\, k \in \mathbb{N}_0\big\}$.
5. $\mathcal{L}(C_3^2) = \{[2k, l] \mid k \in \mathbb{N}_0, l \in [2k, 5k]\}$
$\quad \cup \{[2k+1, l] \mid k \in \mathbb{N}, l \in [2k+1, 5k+2]\} \cup \{\{1\}\}$.

Proof. 1. This is straightforward and well-known. A proof of 2.,3., and 4. can be found in [14, Theorem 7.3.2]. For 5. we refer to [16, Proposition 3.12]. □

Lemma 3.2. *Let G be a cyclic group of order $|G| = n \ge 7$, $g \in G$ with $\mathrm{ord}(g) = n$, $k \in \mathbb{N}$, and*
$$A_k = \begin{cases} g^{nk}(-g)^{nk}(2g)^n & \text{if } n \text{ is even,} \\ g^{nk}(-g)^{nk}\big((2g)^{(n-1)/2}g\big)^2 & \text{if } n \text{ is odd.} \end{cases}$$
Then there is a bound $M \in \mathbb{N}$ such that, for all $k \ge n-1$, the sets $\mathsf{L}(A_k)$ are AAPs *with difference* 1 *and bound M, but they are not arithmetical progressions with difference* 1.

Proof. We set $G_0 = \{g, -g, 2g\}$, $U_1 = (-g)g$, $U_2 = (-g)^2(2g)$ and, if n is odd, then $V_1 = (2g)^{(n+1)/2}(-g)$. Furthermore, for $j \in [0, n/2]$, we define $W_j = (2g)^j g^{n-2j}$. Then, together with $-W_0 = (-g)^n$, these are all minimal zero-sum sequences which divide A_k for $k \in \mathbb{N}$. Note that
$$\| - W_0\|_g = n - 1,\ \|U_2\|_g = \|V_1\|_g = 2, \quad \text{and} \quad \|U_1\|_g = \|W_j\|_g = 1 \quad \text{for all } j \in [0, n/2]\,.$$
It is sufficient to prove the following two assertions.

A1. There is a bound $M \in \mathbb{N}_0$ such that $\mathsf L(A_k)$ is an AAP with difference 1 and bound M for all $k \ge n-1$.

A2. For each $k \in \mathbb{N}$, $\mathsf L(A_k)$ is not an arithmetical progression with difference 1.

Proof of **A1**. By Proposition 2.2.1 there is a bound $M' \in \mathbb{N}_0$ such that, for each $k \in \mathbb{N}$, $\mathsf L(A_k)$ is an AAMP with difference $d_k \in \Delta^*(G) \subset [1, n-2]$ and bound M'. Suppose that $k \ge n-1$. Then $(W_0U_2)^{n-1}$ divides A_k. Since $W_0U_2 = W_1U_1^2$, it follows that

$$(W_0U_2)^{n-1} = (W_0U_2)^{n-1-\nu}(W_1U_1^2)^\nu \quad \text{for all} \quad \nu \in [0, n-1]$$

and hence $\mathsf L\big((W_0U_2)^{n-1}\big) \supset [2n-2, 3n-3]$. Thus $\mathsf L(A_k)$ contains an arithmetical progression of difference 1 and length $n-1$. Therefore there is a bound $M \in \mathbb{N}_0$ such that $\mathsf L(A_k)$ is an AAP with difference 1 and bound M for all $k \ge n-1$.

Proof of **A2**. Let $k \in \mathbb{N}$. Observe that

$$A_k = \begin{cases} W_0^k(-W_0)^k W_{n/2}^2 & \text{if } n \text{ is even,} \\ W_0^k(-W_0)^k \big(W_{(n-1)/2}\big)^2 & \text{if } n \text{ is odd,} \end{cases}$$

and it can be seen that $\min \mathsf L(A_k) = 2k+2$. We assert that $2k+3 \notin \mathsf L(A_k)$. If n is even, then

$$W_0 W_{n/2} = W_j W_{n/2-j} \quad \text{for each} \quad j \in [0, n/2]\,,$$

and similarly, for odd n we have

$$W_0 W_{(n-1)/2} = W_j W_{(n-1)/2-j} \quad \text{for each} \quad j \in [0, (n-1)/2]\,.$$

In both cases, all factorizations of A_k of length $2k+2$ contain only atoms with g-norm 1 and with g-norm $n-1$. Let z' be any factorization of A_k containing only atoms with g-norm 1 and with g-norm $n-1$. Then $|z'| - |z|$ is a multiple of $n-2$ whence if $|z'| > |z|$, then $|z'| - |z| \ge n-2 > 1$.

Next we consider a factorization z' of A_k containing at least one atom with g-norm 2, say z' has r atoms with g-norm $n-1$, $s \ge 1$ atoms with g-norm 2, and t atoms with g-norm 1. Then $k > r$,

$$\|A_k\|_g = k(n-1) + (k+2) = r(n-1) + 2s + t\,,$$

and we study

$$\begin{aligned} |z'| - |z| &= r + s + t - (2k+2) \\ &= r + s + k(n-1) + (k+2) - r(n-1) - 2s - (2k+2) \\ &= (k-r)(n-2) - s\,. \end{aligned}$$

Note that $s \le \mathsf v_{2g}(A_k) \le n$. Thus, if $k - r \ge 2$, then

$$(k-r)(n-2) - s \ge 2n - 4 - s \ge n - 4 > 1\,.$$

Suppose that $k - r = 1$. Then we cancel $(-W_0)^{k-1}$, and consider a relation where $-W_0$ occurs precisely once. Suppose that all s atoms of g-norm 2 are equal to U_2. Since $\mathsf v_{-g}(U_2) = 2$, it follows that $s \le \mathsf v_{-g}(-W_0)/2 = n/2$ whence

$$(k-r)(n-2) - s \ge n - 2 - n/2 = n/2 - 2 > 1\,.$$

Suppose that V_1 occurs among the s atoms with g-norm 2. Then n is odd, V_1 occurs precisely once, and

$$s - 1 \le \mathsf v_{2g}(A_k) - \frac{n+1}{2} = (n-1) - \frac{n+1}{2} = \frac{n-3}{2}\,,$$

whence

$$(k-r)(n-2) - s \ge (n-2) - \frac{n-1}{2} = \frac{n+1}{2} - 2 > 1\,. \qquad \square$$

Lemma 3.3. *Let G be a cyclic group of order $|G| = 6$, $g \in G$ with $\mathrm{ord}(g) = 6$ and, for each $k \in \mathbb{N}$, $A_k = g^{6k}(-g)^{6k}(4g)(-g)^4(3g)g^3$. Then there is a bound $M \in \mathbb{N}$ such that, for all $k \in \mathbb{N}$, the sets $\mathsf L(A_k)$ are* AAPs *with difference 1 and bound M, but they are not arithmetical progressions with difference 1.*

Proof. We set $U = g^6$, $W_1 = (4g)(-g)^4$, and $W_2 = (3g)g^3$. Then, for each $k \in \mathbb{N}$, we have $A_k = U^k(-U)^k W_1 W_2$. By Proposition 2.3, we obtain that $\Delta^*(G) = \{1, 2, 4\}$. By Proposition 2.2.1, there is a bound $M' \in \mathbb{N}$ such that, for every $k \in \mathbb{N}$, $\mathsf{L}(A_k)$ is an AAMP with difference $d_k \in \Delta^*(G)$ and bound M'. We show that $2k+4, 2k+5, 2k+6, 2k+7 \in \mathsf{L}(A_k)$ which implies that there is a bound $M \in \mathbb{N}$ such that, for every $k \in \mathbb{N}$, $\mathsf{L}(A_k)$ is an AAP with difference 1 and bound M.

Let $k \in \mathbb{N}$. We set $V = (-g)g$, $W_3 = (4g)(3g)(-g)$, $W_4 = (4g)g^2$, and obtain that

$$\begin{aligned} A_k &= U^k(-U)^k W_1 W_2 = U^k(-U)^k W_3 V^3 \\ &= U^{k-1}(-U)^k W_4 W_2 V^4 = U^{k-1}(-U)^{k-1} W_1 W_2 V^6 = U^{k-1}(-U)^{k-1} W_4 (-W_2) V^7 \,, \end{aligned}$$

and hence $\{2k+2, 2k+4, 2k+5, 2k+6, 2k+7\} \subset \mathsf{L}(A_k)$. Furthermore, $\min \mathsf{L}(A_k) = 2k+2$, and $z = U^k(-U)^k W_1 W_2$ is the only factorization of A_k of length $2k+2$. From this we see that there is no factorization of length $2k+3$, and hence $\mathsf{L}(A_k)$ is not an arithmetical progression with difference 1. □

Lemma 3.4. *Let G be a cyclic group of order $|G| = 5$. Then every $L \in \mathcal{L}(G)$ has one of the following forms*:

- *L is an arithmetical progression with difference* 1.
- *L is an arithmetical progression with difference* 3.
- *L is an* AMP *with period $\{0, 2, 3\}$ or with period $\{0, 1, 3\}$.*

Proof. By Proposition 2.3 we obtain that $\Delta^*(G) = \{1, 3\}$. Let $A' \in \mathcal{B}(G)$. If $A' = 0^m A$ with $m \in \mathbb{N}_0$ and $A \in \mathcal{B}(G \setminus \{0\})$, then $\mathsf{L}(A') = m + \mathsf{L}(A)$. Thus it is sufficient to prove the assertion for $\mathsf{L}(A)$. If $|\operatorname{supp}(A)| = 1$, then $|\mathsf{L}(A)| = 1$. If $|\operatorname{supp}(A)| = 4$, then $\mathsf{L}(A)$ is an arithmetical progression with difference 1 by Proposition 2.2.4. Suppose that $|\operatorname{supp}(A)| = 2$. Then there is a nonzero $g \in G$ such that $\operatorname{supp}(A) = \{g, 2g\}$ or $\operatorname{supp}(A) = \{g, 4g\}$. If $\operatorname{supp}(A) = \{g, 2g\}$, then $\mathsf{L}(A)$ is an arithmetical progression with difference 1 (this can be checked directly by arguing with the g-norm). If $\operatorname{supp}(A) = \{g, 4g\}$, then $\mathsf{L}(A)$ is an arithmetical progression with difference 3.

Thus it remains to consider the case $|\operatorname{supp}(A)| = 3$. We set $G_0 = \operatorname{supp}(A)$. Then there is an element $g \in G_0$ such that $-g \in G_0$. Thus either $G_0 = \{g, 2g, -g\}$ or $G_0 = \{g, 3g, -g\}$. Since $\{g, 3g, -g\} = \{-g, 2(-g), -(-g)\}$, we may suppose without restriction that $G_0 = \{g, 2g, -g\}$.

If $\Delta(\mathsf{L}(A)) \subset \{1\}$, then $\mathsf{L}(A)$ is an arithmetical progression with difference 1. If $3 \in \Delta(\mathsf{L}(A))$, then $\Delta(\mathsf{L}(A)) = \{3\}$ by [5, Theorem 3.2], which means that $\mathsf{L}(A)$ is an arithmetical progression with difference 3. Thus it remains to consider the case where $2 \in \Delta(\mathsf{L}(A)) \subset [1, 2]$. We show that $\mathsf{L}(A)$ is an AMP with period $\{0, 2, 3\}$ or with period $\{0, 1, 3\}$. Since $2 \in \Delta(\mathsf{L}(A))$, there exist $k \in \mathbb{N}$, $A_1, \ldots, A_k, B_1, \ldots, B_{k+2} \in \mathcal{A}(G_0)$ such that

$$A = A_1 \cdot \ldots \cdot A_k = B_1 \cdot \ldots \cdot B_{k+2}, \quad \text{and} \quad k+1 \notin \mathsf{L}(A) \,.$$

For convenience we list the elements of $\mathcal{A}(G_0)$, and we order them by their lengths:

- g^5, $(-g)^5$, $(2g)^5$,
- $g^3(2g)$, $(2g)^3(-g)$,
- $g(2g)^2$, $(2g)(-g)^2$,
- $g(-g)$.

Clearly, $\{\|S\|_g \mid S \in \mathcal{A}(G_0)\} = \{1, 2, 4\}$, and $(-g)^5$ is the only atom having g-norm 4. We distinguish two cases.

CASE 1: $(-g)^5 \notin \{A_1, \ldots, A_k\}$.

Then $\{A_1, \ldots, A_k\}$ must contain atoms with g-norm 2. These are the atoms $(2g)^5, (2g)(-g)^2, (2g)^3(-g)$. If g^5 or $g^3(2g)$ occurs in $\{A_1, \ldots, A_k\}$, then $k+1 \in \mathsf{L}(A)$, a contradiction. Thus none of the elements $(-g)^5, g^5$, and $g^3(2g)$ lies in $\{A_1, \ldots, A_k\}$, and hence

$$\{A_1, \ldots, A_k\} \subset \{(2g)^5, (2g)^3(-g), g(2g)^2, (2g)(-g)^2, g(-g)\} \,.$$

Now we set $h = 2g$ and obtain that

$$\{A_1, \ldots, A_k\} \subset \{(2g)^5, (2g)^3(-g), g(2g)^2, (2g)(-g)^2, g(-g)\} = \{h^5, h^3(2h), h^2(3h), h(2h)^2, (2h)(3h)\}\,.$$

Since the h-norm of all these elements equals 1, it follows that $\max \mathsf L(A) = k$, a contradiction.

CASE 2: $(-g)^5 \in \{A_1, \ldots, A_k\}$.

If $(2g)^5$, or $g(2g)^2$, or $(2g)^3(-g)$ occurs in $\{A_1, \ldots, A_k\}$, then $k+1 \in \mathsf L(A)$, a contradiction. Since $\Delta(\{-g, g\}) = \{3\}$, it follows that

$$\Omega = \{A_1, \ldots, A_k\} \cap \{g^3(2g), (2g)(-g)^2\} \neq \emptyset\,.$$

Since $\Big(g^3(2g)\Big)\Big((2g)(-g)^2\Big) = \Big((-g)g\Big)^2\Big(g(2g)^2\Big)$ and $k+1 \notin \mathsf L(A)$, it follows that $|\Omega| = 1$. We distinguish two cases.

CASE 2.1: $\{A_1, \ldots, A_k\} \subset \{g^5, (-g)^5, g(-g), (2g)(-g)^2\}$.

We set $h = -g$, and observe that

$$\{A_1, \ldots, A_k\} \subset \{g^5, (-g)^5, g(-g), (2g)(-g)^2\} = \{h^5, (-h)^5, h(-h), h^2(3h)\}\,.$$

Since $(-h)^5$ is the only element with h-norm greater than 1, it follows that $(-h)^5 \in \{A_1, \ldots, A_k\}$. Since $\Delta(\{h, -h\}) = \{3\}$, it follows that $h^2(3h) \in \{A_1, \ldots, A_k\}$. Since $\Big((-h)^5\Big)\Big(h^2(3h)\Big) = \Big(h(-h)\Big)^2\Big((3h)(-h)^3\Big)$, we obtain that $k+1 \in \mathsf L(A)$, a contradiction.

CASE 2.2: $\{A_1, \ldots, A_k\} \subset \{g^5, (-g)^5, g(-g), g^3(2g)\}$.

Since $\Big(g^3(2g)\Big)^2\Big((-g)^5\Big) = \Big(g^5\Big)\Big(g(-g)\Big)\Big((2g)(-g)^2\Big)^2$ and $k+1 \notin \mathsf L(A)$, it follows that

$$|\{i \in [1,k] \mid A_i = g^3(2g)\}| = 1\,,$$

and hence $\mathsf v_{2g}(A) = 1$. Thus every factorization z of A has the form

$$z = \big((2g)g^3\big)z_1 \quad \text{or} \quad z = \big((2g)(-g)^2\big)z_2\,,$$

where z_1, z_2 are factorizations of elements $B_1, B_2 \in \mathcal B(\{-g, g\})$. Since $\mathsf L(B_1)$ and $\mathsf L(B_2)$ are arithmetical progressions of difference 3, $\mathsf L(A)$ is a union of two shifted arithmetical progression of difference 3. We set

$$A = \big(g^5\big)^{m_1}\big((-g)^5\big)\big((-g)g\big)^{m_3}\big((2g)g^3\big)\,,$$

where $m_1 \in \mathbb N_0$, $m_2 \in \mathbb N$, and $m_3 \in [0,4]$. Suppose that $m_1 \ge 1$. Note that

$$A' = \big(g^5\big)\big((-g)^5\big)\big((2g)g^3\big) = \big((-g)g\big)^3\big((2g)(-g)^2\big)\big(g^5\big) = \big((-g)g\big)^5\big((2g)g^3\big)\,,$$

and hence $\mathsf L(A') = \{3, 5, 6\}$. We set $A = A'A''$ with $A'' \in \mathcal B(\{g, -g\})$. The above argument on the structure of the factorizations of A implies that $\mathsf L(A)$ is the sumset of $\mathsf L(A')$ and $\mathsf L(A'')$ whence

$$\mathsf L(A) = \mathsf L(A') + \mathsf L(A'') = 3 + \{0, 2, 3\} + \mathsf L(A'')\,.$$

Since $\mathsf L(A'')$ is an arithmetical progression with difference 3, $\mathsf L(A)$ is an AMP with period $\{0, 2, 3\}$. Suppose that $m_1 = 0$. If $m_3 \in [2, 4]$, then $\mathsf L(A) = \{m_2 + m_3, m_2 + m_3 + 1, m_2 + m_3 + 3\}$ is an AMP with period $\{0, 1, 3\}$. If $m_3 = 1$, then $\mathsf L(A) = \{m_2 + 2, m_2 + 4\}$. If $m_3 = 0$, then $\mathsf L(A) = \{m_2 + 1, m_2 + 3\}$. □

Lemma 3.5. *Let $G = C_{n_1} \oplus C_{n_2}$ where $n_1, n_2 \in \mathbb N$ with $4 \le n_1 \,|\, n_2$, (e_1, e_2) be a basis of G with $\mathrm{ord}(e_i) = n_i$ for $i \in [1,2]$, and set $W = e_1^{n_1-1}e_2^{n_2-1}(e_1 + e_2)$. Then there is a bound $M \in \mathbb N$ such that, for all sufficiently large k, the sets $\mathsf L\big(W^k(-W)^k\big)$ are* AAPs *with difference* 1 *and bound M, but they are not arithmetical progressions with difference* 1.

Proof. We set $e_0 = e_1 + e_2$, $G_0 = \{e_\nu, -e_\nu \mid \nu \in [0,2]\}$, $U_\nu = e_\nu^{\mathrm{ord}(e_\nu)}$ and $V_\nu = (-e_\nu)e_\nu$ for $\nu \in [0,2]$. For $k \in \mathbb{N}$ we set $A_k = W^k(-W)^k$ and $L_k = \mathsf{L}(A_k)$. Since $\gcd \Delta(G_0) \mid \gcd(\{n_1 - 2, n_2 - 2, |W| - 2 = n_1 + n_2 - 3\}) = 1$, it follows that $\min \Delta(G_0) = 1$. Thus, by Proposition 2.2.3, there are $M, k_0 \in \mathbb{N}$ such that for all $k \ge k_0$, the set L_k is an AAP with difference 1 and bound M.

Let $k \in \mathbb{N}$. We assert that $1 + \min L_k \notin L_k$. This implies that L_k is not an arithmetical progression with difference 1. Since $|W| = |-W| = \mathsf{D}(G)$, it follows that $\min L_k = 2k$, and clearly $W^k(-W)^k$ is the only factorization of A_k having length $2k$. If $S = (-e_1)e_2^{n_2-1}(e_1 + e_2)$, then $W(-W) = S(-S)V_1^{n_1-2}$, $2k + n_1 - 2 \in L_k$, and this is the second shortest factorization length of A_k. □

Lemma 3.6. *Let $G = C_2^4$, (e_1, e_2, e_3, e_4) be a basis of G, $e_0 = e_1 + \ldots + e_4$, $U_4 = e_0 \cdot \ldots \cdot e_4$, $U_3 = e_1e_2e_3(e_1 + e_2 + e_3)$, and $U_2 = e_1e_2(e_1 + e_2)$.*

1. *There is a bound $M \in \mathbb{N}$ such that, for all sufficiently large k, the sets $\mathsf{L}\big((U_3U_4)^{2k}\big)$ are* AAPs *with difference 1 and bound M, but they are not arithmetical progressions with difference 1.*
2. *For each $k \in \mathbb{N}$, we have*

$$\mathsf{L}(U_4^{2k}U_2) = (2k+1) + \{0,1,3\} + 3 \cdot [0, k-1]\,.$$

Proof. 1. We set $G_0 = \mathrm{supp}(U_3U_4)$, $A_k = U_3^{2k}U_4^{2k}$ and $L_k = \mathsf{L}(A_k)$ for each $k \in \mathbb{N}$. Since $\gcd \Delta(G_0) \mid \gcd\{|U_3| - 2 = 2, |U_4| - 2 = 3\}$, it follows that $\min \Delta(G_0) = 1$. Thus, by Proposition 2.2.3, there are $M, k_0 \in \mathbb{N}$ such that for all $k \ge k_0$, the set L_k is an AAP with difference 1 and bound M.

Let $k \in \mathbb{N}$. Then $\min L_k = 4k$, and we assert that $1 + 4k \notin L_k$. For $\nu \in [0,4]$, we set $V_\nu = e_\nu^2$ and $V_5 = (e_1 + e_2 + e_3)^2$. Since $\mathsf{Z}(U_3^2) = \{U_3^2, V_1V_2V_3V_5\}$, $\mathsf{Z}(U_4^2) = \{U_4^2, V_1V_2V_3V_4V_0\}$, and $\mathsf{Z}(U_3U_4) = \{U_3U_4, V_1V_2V_3W\}$ where $W = (e_1 + e_2 + e_3)e_0e_4$, it follows that $\min(L_k \setminus \{4k\}) = 4k + 2$.

2. Setting $W = (e_1 + e_2)e_3e_4e_0$ we infer that $U_4^2U_2 = U_4(e_1^2)(e_2^2)W = U_2(e_0^2) \cdot \ldots \cdot (e_4^2)$ and hence $\mathsf{L}(U_4^2U_2) = \{3,4,6\}$. Thus for each $k \in \mathbb{N}$ we obtain that

$$\begin{aligned}
\mathsf{L}(U_4^{2k}U_2) &= \big(\{1\} + \mathsf{L}(U_4^{2k})\big) \cup \big(\mathsf{L}(U_4^{2k-2}) + \mathsf{L}(U_4^2U_2)\big) \\
&= \big(2k + 1 + 3 \cdot [0,k]\big) \cup \big(2k - 2 + 3 \cdot [0, k-1] + \{3,4,6\}\big) \\
&= \big(2k + 1 + 3 \cdot [0,k]\big) \cup \big(2k + 2 + 3 \cdot [0, k-1]\big) \cup \big(2k + 4 + 3 \cdot [0, k-1]\big) \\
&= (2k+1) + \{0,1,3\} + 3 \cdot [0, k-1]\,. \quad \square
\end{aligned}$$

Lemma 3.7. *Let $G = C_3^r$ with $r \in [3,4]$, $(e_1, \ldots, e_r)$ a basis of G, $e_0 = e_1 + \ldots + e_r$, and $U = (e_1 \cdot \ldots \cdot e_r)^2 e_0$.*

1. *If $r = 3$, then there is a bound $M \in \mathbb{N}$ such that, for all $k \in \mathbb{N}$, the sets $\mathsf{L}\big(U^{6k+1}(-U)\big)$ are* AAPs *with difference 1 and bound M, but they are not arithmetical progressions with difference 1.*
2. *If $r = 4$ and $V_1 = e_1^2e_2^2(e_1 + e_2)$, then for each $k \in \mathbb{N}$ we have*

$$\mathsf{L}(U^{3k}V_1) = (3k+1) + \{0,1,3\} + 3 \cdot [0, 2k-1]\,.$$

Proof. 1. Let $r = 3$ and $k \in \mathbb{N}$. We set $A_k = U^{6k+1}(-U)$ and $L_k = \mathsf{L}(A_k)$. For $\nu \in [0,3]$, we set $U_\nu = e_\nu^3$, $V_\nu = (-e_\nu)e_\nu$, and we define $X = e_0^2e_1e_2e_3$.

First, consider $\mathsf{L}(U^{6k})$. We observe that $\mathsf{Z}(U^2) = \{U^2, U_1U_2U_3X\}$ and $\mathsf{Z}(U^3) = \{U^3, UU_1U_2U_3X, U_0U_1^2U_2^2U_3^2\}$. Furthermore, $\min \mathsf{L}(U^{6k}) = 6k$, $\max \mathsf{L}(U^{6k}) = 14k$, $\Delta(\{e_0, \ldots, e_3\}) = \{2\}$, and hence

$$\mathsf{L}(U^{6k}) = 6k + 2 \cdot [0, 4k]\,.$$

Next, consider $\mathsf{L}\big((-U)U\big)$. For subsets $I, J \subset [1,3]$ with $[1,3] = I \uplus J$, we set

$$W_I = e_0 \prod_{i \in I} e_i^2 \prod_{j \in J} (-e_j)\,.$$

Since

$$\mathsf Z\big(U(-U)\big) = \Big\{V_0V_1^2V_2^2V_3^2\Big\} \ \uplus\ \Big\{W_I(-W_I)\prod_{j\in J} V_j \mid I, J \subset [1,3] \ \text{ with } [1,3] = I \uplus J\Big\}\,,$$

it follows that

$$\mathsf L\big((-U)U\big) = \Big\{7\Big\} \ \uplus\ \Big\{2 + |J| \mid I, J \subset [1,3] \ \text{ with } [1,3] = I \uplus J\Big\} = \{2,3,4,5,7\}\,.$$

This implies that

$$[6k+2, 14k+5] \cup \{14k+7\} = \mathsf L\big((-U)U\big) + \mathsf L(U^{6k}) \subset \mathsf L(A_k) \subset [6k+2, 14k+7]\,,$$

and we claim that $[6k+2, 14k+5] \cup \{14k+7\} = \mathsf L(A_k)$. Then the assertion of the lemma follows.

To prove this, we consider the unique factorization $z \in \mathsf Z(A_k)$ of length $|z| = 14k+7$ which has the form

$$z = \big(U_0U_1^2U_2^2U_3^2\big)^{2k}\big(V_0V_1^2V_2^2V_3^2\big)\,.$$

Assume to the contrary that there is a factorization $z' \in \mathsf Z(A_k)$ of length $|z'| = 14k+6$. If $V_0 \,|\, z'$, then $V_0V_1^2V_2^2V_3^2 \,|\, z'$ and $z' = V_0V_1^2V_2^2V_3^2x$ with $x \in \mathsf Z(U^{6k})$, whence $|x| \in \mathsf L(U^{6k})$ and $|z'| \in 7 + \mathsf L(U^{6k})$, a contradiction. Suppose that $V_0 \nmid z'$. Then there are $I, J \subset [1,3]$ with $[1,3] = I \uplus J$ such that $W_I(-W_I)\prod_{j\in J} V_j \,|\, z'$ and hence $z' = W_I(-W_I)\big(\prod_{j\in J} V_j\big)x$ with $x \in \mathsf Z(U^{6k})$. Thus $|z'| \in [2,5] + \mathsf L(U^{6k})$, a contradiction.

2. Let $r = 4$ and $k \in \mathbbm N$. We have $\mathsf L(U^2) = \{2,5\}$ and $\mathsf L(U^{3k}) = 3k + 3\cdot[0,2k]$. We define

$$V_2 = (e_1+e_2)e_1e_2e_3^2e_4^2e_0\,,\ V_3 = (e_1+e_2)e_3e_4e_0^2, \quad \text{and} \quad W = e_1\cdot\ldots\cdot e_4e_0^2\,,$$

and observe that

$$U^3V_1 = U^2V_2(e_1^3)(e_2^3) = UV_3(e_1^3)^2(e_2^3)^2(e_3^3)(e_4^3)$$

whence $\mathsf L(U^3V_1) = \{4,5,7,8\}$. Clearly, each factorization of $U^{3k}V_1$ contains exactly one of the atoms V_1, V_2, V_3, and it contains it exactly once. Therefore we obtain that

$$\begin{aligned}
\mathsf L(U^{3k}V_1) &= \big(\{1\} + \mathsf L(U^{3k})\big) \cup \big(\mathsf L(U^3V_1) + \mathsf L(U^{3k-3})\big) \\
&= \big((3k+1) + 3\cdot[0,2k]\big) \cup \big(\{4,5,7,8\} + (3k-3) + 3\cdot[0,2k-2]\big) \\
&= \big((3k+1) + 3\cdot[0,2k]\big) \cup \big((3k+1) + \{0,1,3,4\} + 3\cdot[0,2k-2]\big) \\
&= (3k+1) + \{0,1,3\} + 3\cdot[0,2k-1]\,. \quad \square
\end{aligned}$$

Proof of Theorem 1.1. 1. (d) $\Rightarrow$ (a) Proposition 3.1 shows that, for all groups mentioned, all sets of lengths are arithmetical progressions. Proposition 2.3 shows that all differences lie in $\Delta^*(G)$.

(c) $\Leftrightarrow$ (d) This is the special case of finite groups of [16, Theorem 1.1] (see Remark 3.8.1).

(a) $\Rightarrow$ (b) Obvious.

(b) $\Rightarrow$ (d) Suppose that $\exp(G) = n$, and that G is not isomorphic to any of the groups listed in (d). We have to show that there is an $L \in \mathcal L(G)$ which is not an arithmetical progression. We distinguish four cases.

CASE 1: $n \ge 5$.

Then [15, Proposition 3.6.1] provides examples of sets of lengths which are not arithmetical progressions.

CASE 2: $n = 4$.

Since G is not cyclic, it has a subgroup isomorphic to $C_2 \oplus C_4$. Then [14, Theorem 6.6.5] shows that $\{2,4,5\} \in \mathcal L(C_2 \oplus C_4\} \subset \mathcal L(G)$.

CASE 3: $n = 3$.

Then G is isomorphic to C_3^r with $r \ge 3$, and Lemma 3.7.1 provides examples of sets of lengths which are not arithmetical progressions.

CASE 4: $n = 2$.

Then G is isomorphic to C_2^r with $r \ge 4$, and Lemma 3.6.1 provides examples of sets of lengths which are not arithmetical progressions.

2. (b) $\Rightarrow$ (a) Suppose that G is a subgroup of C_4^3 or a subgroup of C_3^3. Then Proposition 2.3.2 implies that $\Delta^*(G) \subset \{1, 2\}$, and hence Proposition 2.2.1 implies the assertion.

(a) $\Rightarrow$ (b) Suppose that (b) does not hold. Then G has a subgroup isomorphic to a cyclic group of order $n \ge 5$, or isomorphic to C_2^4, or isomorphic to C_3^4. We show that in none of these cases (a) holds.

If G has a subgroup isomorphic to C_n for some $n \ge 5$, then [15, Proposition 3.6.1] shows that (a) does not hold. If G has a subgroup isomorphic to C_2^4, then Lemma 3.6.2 shows that (a) does not hold. If G has a subgroup isomorphic to C_3^4, then Lemma 3.7.2 shows that (a) does not hold.

3. Suppose that G is cyclic. If $|G| \le 4$, then all sets of lengths are arithmetical progressions with difference in $\Delta^*(G)$ by 1. and hence they are AMPs with difference in $\Delta^*(G)$. If $|G| \ge 5$, then the assertion follows from the Lemmas 3.2, 3.3, and 3.4.

Suppose that G has rank $r \ge 2$ and $\exp(G) \in [2, 5]$, say $G = C_{n_1} \oplus \ldots \oplus C_{n_r}$ with $1 < n_1 \mid \ldots \mid n_r$. If $n_1 \ge 4$, then Lemma 3.5 shows that there are sets of lengths which are not AMPs with difference in $\Delta^*(G)$. Thus it suffices to consider the cases where G is isomorphic to one of the following groups: $C_2^r, C_2^{r-1} \oplus C_4, C_3^r$.

If $G = C_2^{r-1} \oplus C_4$, then $\mathcal{L}(G)$ contains (arbitrarily long) AAPs with difference 2 which are not arithmetical progressions and hence no AMPs ([10, Example 3.2.1]).

Suppose that $G = C_2^r$. If $r \le 3$, then the assertion follows from 1. If $r \ge 4$, then the assertion follows from Lemma 3.6.1.

Suppose that $G = C_3^r$. If $r \le 2$, then the assertion follows from 1. If $r \ge 3$, then the assertion follows from Lemma 3.7.1. □

Proof of Corollary 1.2. Let G' be an abelian group such that $\mathcal{L}(G) = \mathcal{L}(G')$. Then G' is finite by Proposition 2.2 and by [14, Theorem 7.4.1]. By Proposition 2.4, we have $\mathsf{D}(G) = \rho_2(G) = \rho_2(G') = \mathsf{D}(G')$, and $\mathcal{L}(G)$ satisfies one of the properties given in Theorem 1.1 if and only if the same is true for $\mathcal{L}(G')$. We distinguish three cases.

CASE 1: $\mathcal{L}(G)$ satisfies the property in Theorem 1.1.1.

By 1., G is cyclic of order $|G| \le 4$ or isomorphic to a subgroup of C_2^3 or isomorphic to a subgroup of C_3^2, and the same is true for G'. Since $\mathsf{D}(G) \ge 4$, the assertion follows from Proposition 3.1.

CASE 2: $\mathcal{L}(G)$ satisfies the property in Theorem 1.1.2.

By CASE 1, we may suppose that $\mathcal{L}(G)$ and $\mathcal{L}(G')$ do not satisfy the property in 1. Then by 2., G and G', are isomorphic to one of the following groups: C_3^3, $C_2 \oplus C_4$, $C_2^2 \oplus C_4$, $C_2 \oplus C_4^2$, C_4^2, or C_4^3. Since C_3^3 and C_4^2 are the only non-isomorphic groups having the same Davenport constant, it remains to show that $\mathcal{L}(C_3^3) \ne \mathcal{L}(C_4^2)$. Since $\max \Delta(C_4^2) = 3$ (by [18, Lemma 3.3]) and $\max \Delta(C_3^3) = 2$ (by [12, Proposition 5.5]), the assertion follows.

CASE 3: $\mathcal{L}(G)$ satisfies the property in Theorem 1.1.3.

By CASE 1, we may suppose that G and G' do not satisfy the property in 1. But then 3. implies that G and G' are both cyclic of order five. □

Remark 3.8.

1. Let H be an atomic monoid. The system of sets of lengths $\mathcal{L}(H)$ is said to be additively closed if the sumset $L_1 + L_2 \in \mathcal{L}(H)$ for all $L_1, L_2 \in \mathcal{L}(H)$. Thus $\mathcal{L}(H)$ is additively closed if and only if $(\mathcal{L}(H), +)$ is a commutative reduced semigroup with respect to set addition. If this holds, then $\mathcal{L}(H)$ is an acyclic semigroup in the sense of Cilleruelo, Hamidoune, and Serra ([6]). $\mathcal{L}(H)$ is additively closed in certain Krull monoids stemming from module theory ([1, Section 6.C]). Examples in a non-cancellative setting

can be found in [17, Theorem 4.5] and a more detailed discussion of the property of being additively closed is given in [16].

2. Several properties occurring in Theorem 1.1 can be characterized by further arithmetical invariants such as the catenary degree $\mathsf{c}(G)$ and the tame degree $\mathsf{t}(G)$ (for background see [14, Sections 6.4 and 6.5]). For example, the properties (a) - (d) given in Theorem 1.1.1. are equivalent to each of the following properties (e) and (f):

(e) $\mathsf{c}(G) \le 3$ or $\mathsf{c}(G) = 4$ and $\{2, 4\} \in \mathcal{L}(G)$.

(f) $\mathsf{c}(G) \le 3$ or $\mathsf{t}(G) = 4$.

(use [18, Theorem A], [9, Theorem 4.12], and [14, Theorem 6.6.3]).

References

[1] N.R. Baeth and A. Geroldinger, *Monoids of modules and arithmetic of direct-sum decompositions*, Pacific J. Math. **271** (2014), 257 – 319.

[2] N.R. Baeth and D. Smertnig, *Factorization theory: From commutative to noncommutative settings*, J. Algebra **441** (2015), 475 – 551.

[3] N.R. Baeth and R. Wiegand, *Factorization theory and decomposition of modules*, Am. Math. Mon. **120** (2013), 3 – 34.

[4] P. Baginski, A. Geroldinger, D.J. Grynkiewicz, and A. Philipp, *Products of two atoms in Krull monoids and arithmetical characterizations of class groups*, Eur. J. Comb. **34** (2013), 1244 – 1268.

[5] 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), 137 – 146.

[6] J. Cilleruelo, Y.ould Hamidoune, and O. Serra, *Addition theorems in acyclic semigroups*, Additive Number Theory. Festschrift In Honor of the Sixtieth Birthday of Melvyn B. Nathanson (D. Chudnovsky and G. Chudnovsky, eds.), Springer, 2010, pp. 99 – 104.

[7] A. Facchini, *Krull monoids and their application in module theory*, Algebras, Rings and their Representations (A. Facchini, K. Fuller, C. M. Ringel, and C. Santa-Clara, eds.), World Scientific, 2006, pp. 53 – 71.

[8] S. Frisch, S. Nakato, and R. Rissner, *Sets of lengths of factorizations of integer-valued polynomials on Dedekind domains with finite residue fields*, J. Algebra, to appear, https://arxiv.org/abs/1710.06783.

[9] W. Gao, A. Geroldinger, and W.A. Schmid, *Local and global tameness in Krull monoids*, Commun. Algebra **43** (2015), 262 – 296.

[10] A. Geroldinger, *Additive group theory and non-unique factorizations*, Combinatorial Number Theory and Additive Group Theory, Advanced Courses in Mathematics CRM Barcelona, Birkhäuser, 2009, pp. 1 – 86.

[11] ———, *Sets of lengths*, Amer. Math. Monthly **123** (2016), 960 – 988.

[12] A. Geroldinger, D.J. Grynkiewicz, and W.A. Schmid, *The catenary degree of Krull monoids I*, J. Théor. Nombres Bordx. **23** (2011), 137 – 169.

[13] A. Geroldinger, D.J. Grynkiewicz, and P. Yuan, *On products of k atoms II*, Mosc. J. Comb. Number Theory **5** (2015), 73 – 129.

[14] A. Geroldinger and F. Halter-Koch, *Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory*, Pure and Applied Mathematics, vol. 278, Chapman & Hall/CRC, 2006.

[15] A. Geroldinger and W. A. Schmid, *A characterization of class groups via sets of lengths*, http://arxiv.org/abs/1503.04679.

[16] A. Geroldinger and W.A. Schmid, *The system of sets of lengths in Krull monoids under set addition*, Rev. Mat. Iberoam. **32** (2016), 571 – 588.

[17] A. Geroldinger and E.D. Schwab, *Sets of lengths in atomic unit-cancellative finitely presented monoids*, Colloq. Math. **151** (2018), 171 – 187.

[18] A. Geroldinger and Q. Zhong, *The catenary degree of Krull monoids II*, J. Australian Math. Soc. **98** (2015), 324 – 354.

[19] ———, *The set of minimal distances in Krull monoids*, Acta Arith. **173** (2016), 97 – 120.

[20] ———, *A characterization of class groups via sets of lengths II*, J. Théor. Nombres Bordx. **29** (2017), 327 – 346.

[21] R. Gilmer, *Commutative Semigroup Rings*, The University of Chicago Press, 1984.

[22] F. Gotti, *On the system of sets of lengths and the elasticity of submonoids of* $\mathbb{N}^d$, https://arxiv.org/abs/1806.11273.

[23] F. Kainrath, *Factorization in Krull monoids with infinite class group*, Colloq. Math. **80** (1999), 23 – 30.

[24] H. Kim, *The distribution of prime divisors in Krull monoid domains*, J. Pure Appl. Algebra **155** (2001), 203 – 210.

[25] H. Kim and Y. S. Park, *Krull domains of generalized power series*, J. Algebra **237** (2001), 292 – 301.

[26] A. Plagne and W.A. Schmid, *On congruence half-factorial Krull monoids with cyclic class group*, Journal of Combinatorial Algebra, to appear.

[27] W.A. Schmid, *A realization theorem for sets of lengths*, J. Number Theory **129** (2009), 990 – 999.

[28] D. Smertnig, *Factorizations in bounded hereditary noetherian prime rings*, Proc. Edinburgh Math. Soc., to appear, https://doi.org/10.1017/S0013091518000305.

[29] ———, *Sets of lengths in maximal orders in central simple algebras*, J. Algebra **390** (2013), 1 – 43.
[30] Q. Zhong, *A characterization of finite abelian groups via sets of lengths in transfer Krull monoids*, Commun. Algebra **46** (2018), 4021 – 4041.
[31] ———, *Sets of minimal distances and characterizations of class groups of Krull monoids*, Ramanujan J. **45** (2018), 719 – 737.

Institute for Mathematics and Scientific Computing, University of Graz, NAWI Graz, Heinrichstrasse 36, 8010 Graz, Austria
E-mail address: alfred.geroldinger@uni-graz.at
URL: http://imsc.uni-graz.at/geroldinger

Université Paris 13, Sorbonne Paris Cité, LAGA, CNRS, UMR 7539, Université Paris 8, F-93430, Villetaneuse, France, and, Laboratoire Analyse, Géométrie et Applications (LAGA, UMR 7539), COMUE Université Paris Lumières, Université Paris 8, CNRS, 93526 Saint-Denis cedex, France
E-mail address: schmid@math.univ-paris13.fr