A characterization of Krull monoids for which sets of lengths are (almost) arithmetical progressions
Alfred Geroldinger, Wolfgang Schmid

To cite this version:
Alfred Geroldinger, Wolfgang Schmid. A characterization of Krull monoids for which sets of lengths are (almost) arithmetical progressions. Revista Matemática Iberoamericana, 2021, 37 (1), pp.293-316. 10.4171/RMI/1207. hal-01976941v2

HAL Id: hal-01976941
https://hal.science/hal-01976941v2
Submitted on 6 May 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
A CHARACTERIZATION OF KRULL MONOIDS FOR WHICH
SETS OF LENGTHS ARE (ALMOST) ARITHMETICAL
PROGRESSIONS

ALFRED GEROLDINGER AND WOLFGANG ALEXANDER 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 depends only 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 $a = u_1 \cdots u_k$ with irreducibles $u_1, \ldots, u_k \in H$, then $k$ is called the factorization
length. The set $L(a) \subset \mathbb{N}_0$ of all possible factorization lengths is finite and called
the set of lengths of $a$. The system $\mathcal{L}(H) = \{ L(a) \mid a \in H \}$ 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 $|G| \leq 2$ and if $|G| \geq 3$, 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 se-
quences $B(G)$. The latter is a Krull monoid again and it is well-known that
$\mathcal{L}(H) = \mathcal{L}(B(G))$ (as usual we write $\mathcal{L}(G)$ for $\mathcal{L}(B(G))$). Our results on $\mathcal{L}(G)$ also
apply to the larger class of transfer Krull monoids over $G$. This will be outlined in
Section 2.

If the group $G$ is infinite, then, by a Theorem of Kainrath, every finite set
$L \subset \mathbb{N}_{\geq 2}$ lies in $\mathcal{L}(H)$ (15, 16 Theorem 7.4.1); for further rings and monoids
with this property see 10 or 24 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 2.1), the sets in $\mathcal{L}(G)$ are
AiMPs (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). By definition, the concept of an AAMP comprises APs
(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 APs with difference in $\Delta^*(G)$.
   (b) All sets of lengths in $\mathcal{L}(G)$ are APs.
   (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 $|G| \leq 4$ or isomorphic to a subgroup of $C_2^3$ or isomorphic to a subgroup of $C_3^2$.

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 AAPs with bound $M$.
   (b) $G$ is isomorphic to a subgroup of $C_3^2$ or isomorphic to a subgroup of $C_2^3$.

3. For all finite sets $\Delta$ with $\Delta \supset \Delta^*(G)$ the following statements are equivalent:
   (a) All sets of lengths in $\mathcal{L}(G)$ are AMPs with difference in $\Delta$.
   (b) $G$ is cyclic of order $|G| \leq 6$ 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, 17, 23, 31, 30]) which reads as follows:

Let $G$ be a finite abelian group with $D(G) \geq 4$, 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 $D(G) \leq 3$ if and only if either $|G| \leq 3$ 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 5.1), 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 $D(G) \geq 4$ 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 3.13 where we also discuss the property of being additively closed occurring in Theorem 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 $[a, b] = \{x \in \mathbb{Z} \mid a \leq x \leq b\}$. 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

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

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

**Monoids.** By a monoid, we mean a commutative cancellative semigroup with identity. Let $H$ be a monoid. Then $H^\times$ denotes the group of invertible elements
of \( H \), \( \mathcal{A}(H) \) the set of atoms of \( H \), and \( H_{\text{red}} = H/H^\times \) the associated reduced monoid. The factorization monoid \( \mathbb{Z}(H) = \mathcal{F}(\mathcal{A}(H_{\text{red}})) \) is the free abelian monoid with basis \( \mathcal{A}(H_{\text{red}}) \) and \( \pi: \mathbb{Z}(H) \to H_{\text{red}} \) denotes the canonical epimorphism. For an element \( a \in H \), \( \mathbb{Z}(a) = \pi^{-1}(aH^\times) \) is the set of factorizations of \( a \) and \( L(a) = \{ |z| = \sum_{u \in \mathcal{A}(H_{\text{red}})} v_u(z); z = \prod_{u \in \mathcal{A}(H_{\text{red}})} u^{v_u(z)} \in \mathbb{Z}(a) \} \subset \mathbb{N} \) is the set of lengths of \( a \) (note that \( L(a) = \{ 0 \} \) if and only if \( a \in H^\times \)). We denote by

\[
\mathcal{L}(H) = \{ L(a) \mid a \in H \}
\]

the system of sets of lengths of \( H \), and by

\[
\Delta(H) = \bigcup_{L \in \mathcal{L}(H)} \Delta(L) \subset \mathbb{N}
\]

the set of distances of \( H \).

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

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

Then

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

is the \textit{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 \textit{sequences over} \( G_0 \). For a sequence

\[
S = g_1 \cdot \ldots \cdot g_l = \prod_{g \in G_0} g^{v_g(S)} \in \mathcal{F}(G_0),
\]

we set \(-S = (-g_1) \cdot \ldots \cdot (-g_l)\), and we call \( |S| = l = \sum_{g \in G} v_g(S) \in \mathbb{N}_0 \) the \textit{length} of \( S \), \( \text{supp}(S) = \{ g \in G \mid v_g(S) > 0 \} \subset G \) the \textit{support} of \( S \), \( v_g(S) \) the \textit{multiplicity} of \( g \) in \( S \),

\[
\sigma(S) = \sum_{i=1}^l g_i \text{ the sum of } S, \text{ and } \Sigma(S) = \left\{ \sum_{i \in I} g_i \mid \emptyset \neq I \subset [1, l] \right\}
\]

the \textit{set of subsequence sums} of \( S \). The sequence \( S \) is said to be

- \textbf{zero-sum free} if \( 0 \notin \Sigma(S) \),
- \textbf{a zero-sum sequence} if \( \sigma(S) = 0 \),
- \textbf{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 \textit{monoid of zero-sum sequences} over \( G_0 \). As usual we set, for all \( k \in \mathbb{N} \), \( \rho_k(G_0) = \rho_k(\mathcal{B}(G_0)) \), \( \rho(G_0) = \rho(\mathcal{B}(G_0)) \), \( \mathcal{L}(G_0) = \mathcal{L}(\mathcal{B}(G_0)) \), \( \mathbb{Z}(G_0) = \mathbb{Z}(\mathcal{B}(G_0)) \), and \( \Delta(G_0) = \Delta(\mathcal{B}(G_0)) \). 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 \textit{Davenport constant} \( D(G_0) \) of \( G_0 \) is the maximal length of an atom whence

\[
D(G_0) = \sup \{ |U| \mid U \in \mathcal{A}(G_0) \} \in \mathbb{N}_0 \cup \{ \infty \}.
\]

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

\[
\Delta^*(G) = \{ \min \Delta(G_0) \mid G_0 \subset G \text{ with } \Delta(G_0) \neq 0 \} \subset \Delta(G).
\]
A tuple \((e_i)_{i \in I}\) is called a basis of \(G\) if all elements are nonzero and \(G = \oplus_{i \in I}(e_i)\). For \(p \in \mathbb{P}\), let \(r_p(G)\) denote the \(p\)-rank of \(G\), \(r(G) = \sup\{r_p(G) \mid p \in \mathbb{P}\}\) denote the rank of \(G\).

**Transfer Krull monoids.** A 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 whenever 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 ([16, Section 2.11]). Monoid domains and monoids of modules that are Krull are discussed in [5, 3, 1, 8]. Let \(A = BC\) with \(B, C \in \mathcal{B}(G_0)\), then

\[ \mathcal{L}(B) + \mathcal{L}(C) \subseteq \mathcal{L}(A). \]

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

\[ ld \leq \sum_{\nu=1}^{l} |V_{\nu}| = |A| = \sum_{\nu=1}^{k} |U_{\nu}| \leq kD(G_0) \text{ whence } \frac{|A|}{D(G_0)} \leq \min L(A) \leq \max L(A) \leq \frac{|A|}{d}. \]

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 \(\operatorname{ord}(g) = n \geq 2\). For a sequence \(S = (n_1 g) \cdots (n_l g) \in \mathcal{F}(g)\), 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, \(\| \cdot \|_g : \mathcal{B}(g) \to \mathbb{N}_0\) 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 \(S = \mathcal{A}(G_0)\). Arguing as above we obtain that

\[ \frac{|A|}{n - 1} \leq \min L(A) \leq \max L(A) \leq \|A\|_g. \]

Now we recall the concept of almost arithmetical multiprogressions (AAMPs) as given in [16, 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 and 2.3). 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
The first statement gives the Structure Theorem for Sets of Lengths \([16, \text{ Theorem } 4.4.11]\), which is sharp by the second statement proved in \([27]\). The third and the fourth statements show that sets of lengths are extremely smooth.

**Proposition 2.2** (Structural results on \(L(G)\)).

Let \(G\) be a finite abelian group with \(|G| \geq 3\).

1. There exists some \(M \in \mathbb{N}_0\) such that every set of lengths \(L \in L(G)\) 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
   \[
   y + L \in L(G^*) \quad \text{for all} \quad y \geq y_L.
   \]
3. Let \(G_0 \subset G\) be a subset. Then there exist a bound \(M \in \mathbb{N}_0\) and some \(A^* \in B(G_0)\) such that for all \(A \in A^* B(G_0)\) the set of lengths \(L(A)\) is an AAP with difference \(\min \Delta(G_0)\) and bound \(M\).
4. If \(A \in B(G)\) such that \(\text{supp}(A) \cup \{0\}\) is a subgroup of \(G\), then \(L(A)\) is an AP with difference 1.

**Proof.** The first statement gives the Structure Theorem for Sets of Lengths \([16, \text{ Theorem } 4.4.11]\), 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 \([16, \text{ Theorems } 4.3.6 \text{ and } 7.6.8]\). \(\square\)

**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 \(r = r(G), 1 < n_1 | \ldots | n_r, \text{ and } |G| \geq 3\).

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

**Proof.** The statement on max \(\Delta^*(G)\) follows from \([22]\). For all remaining statements see \([16, \text{ Section } 6.8]\). A more detailed analysis of \(\Delta^*(G)\) in case of cyclic groups can be found in \([26]\). \(\square\)
Proposition 2.4 (Results on \(\rho_k(G)\) and on \(\rho(G)\)).

Let \(G\) be a finite abelian group with \(|G| \geq 3\), and let \(k \in \mathbb{N}\).

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

Proof. See [16] Chapter 6.3], [12] Theorem 5.3.1], and [15]. □

We need the following technical lemma which follows from [9] Lemma 6.1.

Lemma 2.5. Let \(G\) be a finite abelian group, \(A \in \mathcal{B}(G)\), \(x = U_1 \cdots U_r \in \mathbb{Z}(G)\), with \(U_1, \ldots, U_r \in \mathcal{A}(G)\) and \(|U_1| = \ldots = |U_r| = 2\), such that \(U_1 \cdots U_r \mid A\) in \(\mathcal{B}(G)\). Then there exists a factorization \(z \in \mathbb{Z}(A)\) with \(|z| = \max L(A)\) and \(x \mid z\) in \(\mathbb{Z}(G)\).

3. A characterization of extremal cases

The goal of this section is to prove Theorem 1.3. First we recall some cases where the systems of sets of lengths are completely determined.

Proposition 3.1.

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

Proof. 1. This is well-known. A proof of 2., 3., and 4. can be found in [16] Theorem 7.3.2]. For 5. we refer to [13] Proposition 3.12]. □

Let \(G\) be a finite abelian group, \(g \in G\) with \(\text{ord}(g) = n \geq 2\), \(r \in [0, n - 1]\), \(k, \ell \in \mathbb{N}_0\), and \(A = g^{nk+r}(-g)^{rn+r}\). We often use that

\[
Z(A) = \{U^{r+\nu}V^{k-\nu}(-V)^{\ell-\nu} \mid \nu \in [0, \min\{k, \ell\}]\},
\]

where \(U = g(-g), V = g^n\), and that

\[
L(A) = \{r + k + \ell + \nu(n - 2) \mid \nu \in [0, \min\{k, \ell\}]\}
= r + k + \ell + (n - 2) \cdot [0, \min\{k, \ell\}]\}.
\]

Proposition 3.2. Let \(G\) be a cyclic group of order \(|G| = n \geq 7\), \(g \in G\) with \(\text{ord}(g) = n, k \in \mathbb{N}\), and

\[
A_k = \begin{cases} 
g^{nk}(-g)^{nk}(2g)^{n} & \text{if } n \text{ is even}, 
g^{nk}(-g)^{nk}((2g)^{(n-1)/2})^{2} & \text{if } n \text{ is odd}. 
\end{cases}
\]

Then there is a bound \(M \in \mathbb{N}\) such that, for all \(k \geq n - 1\), the sets \(L(A_k)\) are AAPs with difference 1 and bound \(M\), but they are not APs 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

$$\|W_0\|_g = n - 1, \|U_2\|_g = \|V_1\|_g = 2, \text{ and } \|U_1\|_g = \|W_j\|_g = 1 \text{ for all } j \in [0, n/2].$$

It is sufficient to prove the following two assertions.

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

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

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

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

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

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

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

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

$$W_0W_{n/2} = W_jW_{n/2-j} \text{ for each } j \in [0, n/2],$$

and similarly, for odd $n$ we have

$$W_0W_{(n-1)/2} = W_jW_{(n-1)/2-j} \text{ for each } j \in [0, (n-1)/2].$$

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 $|z'| - |z| \geq n - 2 > 1$.

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 $n - 1$, $s \geq 1$ 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

$$|z'| - |z| = r + s + t - (2k + 2)$$

$$= r + s + k(n - 1) + (k + 2) - r(n - 1) - 2s - (2k + 2)$$

$$= (k - r)(n - 2) - s.$$ Note that $s \leq v_2g(A_k) \leq n$. Thus, if $k - r \geq 2$, then

$$(k - r)(n - 2) - s \geq 2n - 4 - s \geq n - 4 > 1.$$ 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 $v_2g(U_2) = 2$, it follows that $s \leq v_2g(-W_0)/2 = n/2$ whence

$$(k - r)(n - 2) - s \geq n - 2 - n/2 = n/2 - 2 > 1.$$
Suppose that $V_1$ occurs among the $s$ atoms with $g$-norm 2. Then $n$ is odd, $V_1$ occurs precisely once, and
$$s - 1 \leq v_{2g}(A_k) - \frac{n + 1}{2} = (n - 1) - \frac{n + 1}{2} = \frac{n - 3}{2},$$
whence
$$(k - r)(n - 2) - s \geq (n - 2) - \frac{n - 1}{2} = \frac{n + 1}{2} - 2 > 1. \quad \Box$$

In order to handle the cyclic group with six elements (done in Proposition 5.8), we need five lemmas.

**Lemma 3.3.** Let $G$ be a cyclic group of order $|G| = 6$, $g \in G$ with $\text{ord}(g) = 6$, and $A \in \mathcal{B}(G)$ with $\text{supp}(A) = \{g, 2g, 3g, -g\}$. Then $L(A)$ is an AP with difference 1.

**Proof.** We set $G_0 = \{g, 2g, 3g, -g\}$ and list all atoms of $\mathcal{B}(G_0)$:
\[
\begin{align*}
\| : \|_0 &= 1 : g^6, g^4(2g), g^3(3g), g^2(2g)^2, g(2g)(3g), g(-g), (2g)^3, (3g)^2, \\
\| : \|_2 &= 2 : U_1 = (2g)^2(3g)(-g), U_2 = (2g)(-g)^2, \\
\| : \|_3 &= 3 : U_3 = (3g)(-g)^3, \\
\| : \|_5 &= 5 : U_4 = (-g)^6.
\end{align*}
\]

We choose a factorization $z \in Z(A)$ and we show that either $|z| = \max L(A)$ or that $|z| + 1 \in L(A)$. In each of the following cases it easily follows that $|z| + 1 \in L(A)$.

- $U_2^2 \mid z$ in $Z(G)$, because $3 \in L(U_2^2)$.
- $U_1U_3 \mid z$ in $Z(G)$, because $3 \in L(U_1U_3)$.
- $U_1U_4 \mid z$ in $Z(G)$, because $3 \in L(U_1U_4)$.

From now on we suppose that none of the above cases occurs. If $z$ is divisible only by atoms with $g$-norm one and by at most one atom having $g$-norm two, then we are done. Thus it is sufficient to handle the following four cases.

**CASE 1:** $U_1 \mid z$.

If $z$ is divisible by an atom $W$ with $v_g(W) \geq 1$ and $W \neq (-g)g$, then $3 \in L(U_1W)$ and we are done. Suppose this does not hold. Thus
$$z = U_1U_2^{k_2}(2g)^{k_3}(3g)^{k_4}(-g)^{k_5},$$
with $k_2 \in \mathbb{N}$ and $k_3, k_4, k_5 \in \mathbb{N}_0$. Then $|z| = 1 + k_2 + \ldots + k_5$ and we assert that $|z| = \max L(A)$. By Lemma 2.5 it is sufficient to show that
$$1 + k_2 + k_3 = \max L(U_1U_2^{k_2}(2g)^{k_3}).$$

Each atom $X \in \mathcal{B}(G_0)$ with $X \mid U_1U_2^{k_2}(2g)^{k_3}$ and $(2g) \mid X$ has length $|X| \geq 3$ whence the claim follows.

**CASE 2:** $U_3 \mid z$ and $U_1 \nmid z$.

If $z$ is divisible by an atom $W$ with $v_g(W) \geq 1$. If $W \in \{g^4(2g), g^2(2g)^2, (2g)^3, g(2g)(3g)\}$, then $3 \in L(U_3W)$ and we are done. If this is not the case, then all atoms $W$ are equal to $U_2$. Thus $U_2U_3$ divides $z$. Thus $z$ is divisible by an atom $W$ with $v_g(W) \geq 1$. If $W \in \{g^6, g^3(3g)\}$, then $3 \in L(U_2W)$ and we are done. Thus we may assume that any atom $W$ with $v_g(W) \geq 1$ is equal to $V = (-g)g$. This implies that $v_g(A) = v_V(z)$. We set
$$z = U_2^{k_2}U_3^{k_3}U_4^{k_4}V^{k_5}(3g)^{k_5}.$$
and assert that $|z| = \max L(A)$. By Lemma 2.5 it is sufficient to show that

$$k_2 + k_3 + k_4 = \max L\left(\left(U_2^k U_3^k U_4^k\right)^2\right),$$

and this holds true.

**CASE 3:** $U_2 \mid z$ and $U_1 \nmid z$ and $U_3 \nmid z$.

If $z$ is divisible by an atom $W$ with $\nu_{2g}(W) \geq 2$, then $3 \in L(U_2 W)$ and we are done. If $z$ is divisible by $W = g(2g)(3g)$, then $U_2 W = U_1 (g(-g))$. Thus there is a factorization $z' \in Z(A)$ with $|z| = |z'|$ and $U_1 \mid z'$ and the claim follows from CASE 1.

Suppose that this is the not the case. Then the each atom dividing $z$ and containing $g$ is $V = (-g)g$ whence $\nu_{g}(A) = \nu_{V}(z)$. If $(2g)^3$ and $U_4$ divides $z$, then $|z| + 1 \in L(A)$ because $3 \in L((3g)^2 U_4)$; otherwise $|z| = \max L(A)$.

**CASE 3:** $U_4 \mid z$ and $U_1 \nmid z$ and $U_2 \nmid z$ and $U_3 \nmid z$.

If $W = (2g)^3$ divides $z$, then $3 \in L(U_4 W)$ and we are done. Suppose this is not the case. If $W = g(2g)(3g)$ divides $z$, then $3 \in L(U_4 W)$ and we are done. Suppose this is not the case. Then there are atoms $W_1, W_2$ such that $2g \mid W_1$ and $3g \mid W_2$ such that $W_1 W_2$ divides $z$. Then $W_1 \in \{g^4(2g), g^2(2g)^2\}$ and $W_2 \in \{(3g)^2, g^2(3g)\}$. In each case we obtain that $W_1 W_2 = WW_4$ for some atom $W_4 \in A(G)$. Thus we obtain a factorization $z' \in Z(A)$ with $|z| = |z'|$ with $WU_4 \mid z'$ and we are done.

**Lemma 3.4.** Let $G$ be a cyclic group of order $|G| = 6$, $g \in G$ with $\ord(g) = 6$, and $A \in B(G)$ with $\supp(A) = \{g, 3g, 4g\}$. Then $L(A)$ is an AP with difference 1.

**Proof.** We set $G_0 = \{g, 3g, 4g\}$ and list all atoms of $B(G_0)$:

$\| \cdot \|_g = 1 : g^6, V_3 = g^3(3g), V_5 = g^2(4g), V_4 = (3g)^2,$

$\| \cdot \|_g = 2 : U_1 = (4g)^2(3g)g, U_2 = (4g)^3,$

We choose a factorization $z \in Z(A)$ and we show that either $|z| = \max L(A)$ or that $|z| + 1 \in L(A)$. If $z$ is divisible by at most one atom having $g$-norm two, then the claim holds. Thus from now on we suppose that $z$ is divisible by at least two atoms having $g$-norm two. Since $U_1^2 = (3g)^2 \left((4g)^2\right) \left((4g)^3\right)^2$, we may suppose that $U_1^2 \nmid z$. Thus $U_1 U_2$ divides $z$ or $U_2^2$ divides $z$.

Since $V_3^2 = (g^6) \left((3g)^2\right)^2$, we may suppose that $\nu_{V_3}(z) \leq 1$. If $z$ is divisible by $g^6$, then $3 \in L(U_2 g^6)$ shows that $|z| + 1 \in L(A)$. Suppose that $g^6 \nmid z$. It follows that

$$z = U_1 \ell_1 U_2 \ell_2 V_3^{\ell_3} V_4^{\ell_4} V_5^{\ell_5},$$

where $\ell_1 \leq 1$, $\ell_3 \leq 1$. Since $U_1 V_3 = V_4 V_5^2$ we may suppose that $\ell_1 + \ell_3 \leq 1$. We assert that $|z| = \max L(A)$, and by Lemma 2.5 it suffices to show that

$$\ell_1 + \ell_2 + \ell_3 + \ell_5 = \max L(A'),$$

where $A' = U_1^\ell U_2^{\ell_2} V_3^{\ell_3} V_4^{\ell_4} V_5^{\ell_5}$.

Since $A'$ is not divisible by an atom of length 2, it follows that $\max L(A') \leq |A'|/3$. Since $|U_2| = |V_3| = 3$ and $\ell_1 + \ell_3 \leq 1$, we infer that $\ell_1 + \ell_2 + \ell_3 + \ell_5 = |A'|/3$. \square

**Lemma 3.5.** Let $G$ be a cyclic group of order $|G| = 6$, $g \in G$ with $\ord(g) = 6$, and $A \in B(G)$ with $\supp(A) = \{g, 2g, 3g, 4g\}$. Then $L(A)$ is an AP with difference 1.

**Proof.** We set $G_0 = \{g, 2g, 3g, 4g\}$ and list all atoms of $B(G_0)$:

$\| \cdot \|_g = 1 : g^6, g^4(2g), V_3 = g^2(3g), g^2(2g)^2, V_5 = g^2(4g), V_1 = g(2g)(3g),$

$V_2 = (2g)(4g), (2g)^3, V_4 = (3g)^2,$

$\| \cdot \|_g = 2 : U_1 = (4g)^2(3g)g, U_2 = (4g)^3,$

$\| \cdot \|_g = 3 : U_3 = U_1 U_2 U_3^{\ell_3} U_4^{\ell_4} U_5^{\ell_5},$
We choose a factorization $z \in \mathbb{Z}(A)$ and we show that either $|z| = \max L(A)$ or that $|z| + 1 \in L(A)$. If $z$ is divisible by at most one atom having $g$-norm two, then the claim holds. Thus from now on we suppose that $z$ is divisible by at least two atoms having $g$-norm two. Since $U_1^2 = (3g)^2 \left((4g)g^2\right)\left((4g)^3\right)$, we may suppose that $U_1^2 \nmid z$. Thus $U_1U_2$ divides $z$ or $U_2^2$ divides $z$.

Since $V_3^2 = (g^6)(3g)^2$, we may suppose that $v_{V_3}(z) \leq 1$. Since $V_1^2 = \left(g^2(2g)^2\right)(3g)^2$, we may suppose that $v_{V_1}(z) \leq 1$. Since $V_1V_3 = V_4V_3$, we may suppose that $v_{V_1}(z) + v_{V_3}(z) \leq 1$. If $z$ is divisible by some $W \in \{g^6, g^4(2g), g^2(2g)^2, (2g)^3\}$, then $3 \in L(U_2W)$ shows that $|z| + 1 \in L(A)$. Suppose that none of these four atoms divides $z$.

Since $v_{2g}(A) \geq 1$, it follows that $V_1 = g(2g)(3g)$ or $V_2 = (2g)(4g)$ divides $z$. If $U_1U_2 | z$, then $3 \in L(U_1V_1)$ shows that $|z| + 1 \in L(A)$. Since $U_1V_2 = U_2V_1$, we may suppose that $U_1 \nmid z$ whence $z$ has the form

$$z = V_3^{k_3}V_5^{k_5}V_4^{k_4}U_1^{k_1}U_2^{k_2}U_3^{k_3}U_5^{k_5}U_2^{k_2}U_1^{k_1}.$$  

We assert that $|z| = \max L(A)$. By Lemma 2.5, it is sufficient to show that

$$\max L\left(V_3^{k_3}V_5^{k_5}V_4^{k_4}U_1^{k_1}U_2^{k_2}\right) = k_3 + k_5 + k_1 + \ell.$$  

If $k_1 = 1$, then $k_3 = k_5 = 0$ and $L\left(V_1^4U_2^2\right) = \{\ell + 1\}$. Suppose that $k_1 = 0$, then $V_3^{k_3}V_5^{k_5}U_\ell$ is not divisible by an atom of length two whence (recall that $k_3 \leq 1$)

$$\max L\left(V_3^{k_3}V_5^{k_5}U_\ell\right) \leq \left|V_3^{k_3}V_5^{k_5}U_\ell\right| \leq \left|V_3^{k_3}V_5^{k_5}\right| = k_3 + k_5 + \ell. \tag*{$\square$}$$

**Lemma 3.6.** Let $G$ be a cyclic group of order $|G| = 6$, $g \in G$ with $\text{ord}(g) = 6$, and $A \in B(G)$ with $\text{supp}(A) = \{g, 2g, -g\}$. If $v_{2g}(A) \geq 3$, then $L(A)$ is an AP with difference 1. If $v_{2g}(A) = 2$, then $L(A)$ is an AMP with period $\{0, 1, 2, 4\}, \{0, 1, 3, 4\}$, or $\{2, 3, 4\}$, and if $v_{2g}(A) = 1$, then it is an AMP with period $\{0, 1, 4\}$ or $\{0, 3, 4\}$.

**Proof.** We set $G_0 = \{g, 2g, 3g, 4g\}$ and list all atoms of $B(G_0)$:

$$\begin{align*}
\|1\|_g &= 1 : U_1 = g^6, U_2 = g^4(2g), U_3 = g^2(2g)^2, U_4 = (2g)^3, U_5 = (2g)^3, \\
\|2\|_g &= 2 : V_1 = (2g)(-g)^2, \\
\|3\|_g &= 5 : V_2 = (-g)^b.
\end{align*}$$

CASE 1: $v_{2g}(A) = 1$.

Then each factorization $z \in \mathbb{Z}(A)$ is divisible by $U_2$ or $V_1$. If $v_g(A) < 4$ or $v_{-g}(A) < 2$, it is easy to see that $L(A)$ is a singleton. Thus, we assume that neither is the case and write $A = (2g)g^{w+1}(-g)^{w+2}$. Since $A$ is a zero-sum sequence, it follows that $v \equiv w + 2 \pmod{6}$.

We determine the set of lengths of $A$. Let $z$ be a factorization of $A$. If $z$ contains $U_2$, then $z$ is of the form $U_2z'$ where $z'$ is a factorization of $g^w(-g)^{w+2}$. If $z$ contains $V_1$, then $z$ is of the form $V_1z''$ where $z''$ is a factorization of $g^{w+1}(-g)^w$. Conversely, for each factorization $z'$ of $g^w(-g)^{w+2}$ we have that $U_2z'$ is a factorization of $A$, and for each factorization $z''$ of $g^{w+1}(-g)^w$ we have that $V_1z''$ is a factorization of $A$. Consequently $L(A) = 1 + \left(L\left(g^w(-g)^{w+2}\right) \cup L\left(g^{w+1}(-g)^w\right)\right)$.

We determine $L\left(g^w(-g)^{w+2}\right) \cup L\left(g^{w+1}(-g)^w\right)$. If $v$ is odd, then each factorization contains of $g^w(-g)^{w+2}$ and $g^{w+1}(-g)^w$ contains $(-g)g$ and $L\left(g^v(-g)^{w+2}\right) \cup
$L(g^{v+4}(-g)^w) = 1 + (L(g^{v-1}(-g)^{w-1} + 1) \cup L(g^{v+1}(-g)^{w-1})).$ We thus focus on the case that $v$ is even.

If $v \equiv 0 \pmod{6}$, then

$$L(g^v(-g)^{w+2}) = \frac{v + w + 2}{6} + 4 \cdot \left\lfloor \frac{\min\{v, w + 2\}}{6} \right\rfloor$$

and

$$L(g^{v+4}(-g)^w) = 4 + \frac{v + w - 4}{6} + \frac{4}{6} \cdot \left\lfloor \frac{\min\{v, w - 4\}}{6} \right\rfloor = 3 + \frac{v + w + 2}{6} + \frac{4}{6} \cdot \left\lfloor \frac{\min\{v, w - 4\}}{6} \right\rfloor.$$  

Thus, the union is an AMP with difference 4 and period $\{0, 3, 4\}$.

If $v \equiv 2 \pmod{6}$, then

$$L(g^v(-g)^{w+2}) = 2 + \frac{v - 2 + w}{6} + \frac{4}{6} \cdot \left\lfloor \frac{\min\{v - 2, w\}}{6} \right\rfloor = 1 + \frac{v + 4 + w}{6} + \frac{4}{6} \cdot \left\lfloor \frac{\min\{v - 2, w\}}{6} \right\rfloor$$

and

$$L(g^{v+4}(-g)^w) = \frac{v + 4 + w}{6} + 4 \cdot \left\lfloor \frac{\min\{v + 4, w\}}{6} \right\rfloor.$$  

Thus, the union is an AMP with difference 4 and period $\{0, 1, 4\}$.

If $v \equiv 4 \pmod{6}$, then

$$L(g^v(-g)^{w+2}) = 4 + \frac{v - 4 + w - 2}{6} + 4 \cdot \left\lfloor \frac{\min\{v - 4, w - 2\}}{6} \right\rfloor$$

$$= 3 + \frac{v + w}{6} + 4 \cdot \left\lfloor \frac{\min\{v - 4, w - 2\}}{6} \right\rfloor$$

and

$$L(g^{v+4}(-g)^w) = 2 + \frac{v + w}{6} + 4 \cdot \left\lfloor \frac{\min\{v + 2, w - 2\}}{6} \right\rfloor.$$  

Thus, the union is an AMP with difference 4 and period $\{0, 1, 4\}$.

CASE 2: $\nu_g(A) = 2$.

We set $A = (2g)^2 g^{v+8}(-g)^{w+4}$ with $v_g(A) = v + 8 > 0$, $v_{-g}(A) = w + 4 > 0$, and $v, w \in \mathbb{Z}$. Then $v \equiv w + 4 \pmod{6}$. If $w$ is odd, then $Z(A) = U_{1/2}/A'$ with $A' = U_{1/2}^{-1}A$. Thus we may suppose that $w$ is even.

First suppose that $v_{-g}(A) < 4$. Then $v_{-g}(A) = 2$, $A = (g^2)^2 (2g)^2 g^{6m+4}$ for some $m \in \mathbb{N}$, and $L(A) = \{m + 2, m + 3\}$ is an AP with difference 1. Now suppose that $v_{-g}(A) \geq 4$. We discuss the cases where $v_g(A) \in \{2, 4, 6\}$. If $v_g(A) = 2$, then $A = g^2 (2g)^2 (-g)^{6m}$ for some $m \in \mathbb{N}$ whence $L(A) = \{m + 1, m + 2\}$. If $v_g(A) = 4$, then $A = g^2 (2g)^2 (-g)^{6m+2}$ for some $m \in \mathbb{N}$,

$$A = U_2 V_1 (-U_1)^m = U_3 U_2^2 (-U_1)^m = V_1^2 U_4(-U_1)^{m-1}$$

whence $L(A) = \{2 + m, 3 + m, 5 + m\}$ is an AMP with period $\{0, 1, 3, 4\}$. If $v_g(A) = 6$, then $A = g^6 (2g)^2 (-g)^{6m+4}$ for some $m \in \mathbb{N}$,

$$A = U_2 U_3^2 (-U_1)^m = U_4 V_1 U_2^2 (-U_1)^m = V_1^2 U_6(-U_1)^{m-1},$$

where the last equations holds only in case $m \geq 1$. Thus $L(A) = \{3, 4, 5\}$ or $L(A) = \{3 + m, 4 + m, 5 + m, 7 + m\}$ if $m \in \mathbb{N}$.

Now we suppose that $v_{-g}(A) \geq 4$ and $v_g(A) > 8$ whence $A = (2g)^2 g^{v+8}(-g)^{w+4}$ with $v, w \in \mathbb{N}$ even. Then

$$A = U_2^2 V_1^2 (-U_1)^{w+4} = U_2^2 A_1 = U_3 g^{v+6}(-g)^{w+4} = U_3 A_2$$

$$= V_1^2 g^{v+8}(-g)^{w} = V_1^2 A_3 = V_1 U_2 g^{v+4}(-g)^{w+2} = V_1 U_2 A_4$$


whence

\[ L(A) = 2 + \left( L(A_1) \cup (-1 + L(A_2)) \cup L(A_3) \cup L(A_4) \right) \]

\[ = 2 + \left( (-1 + L(A_2)) \cup L(A_3) \cup L(A_4) \right), \]

where the last equation holds because \( 1 + L(A_1) \subseteq L(g^6A_1) \) and \( g^6A_1 = A_2 \). The sets \( L(A_2), L(A_3) \) and \( L(A_4) \) are APs with difference 4. Thus in order to show that \( L(A) \) is an AMP with difference 4, we study the minima and the lengths of \(-1 + L(A_2), L(A_3) \) and \( L(A_4) \). We distinguish three cases depending on the congruence class of \( v \) modulo 6 (recall that \( v \) is even).

Suppose that \( v \equiv 0 \mod 6 \). The set \(-1 + L(A_2)\) has minimum \( a_0 = (v + w + 4)/6 \) and length \( \ell_0 = \min\{v + 6, w + 4\}/6 \). The set \( L(A_3) \) has minimum \( a_0 + 2 \) and length \( \min\{v + 6, w - 2\}/6 \in \{\ell_0, \ell_0 - 1\} \). Finally \( L(A_4) \) has minimum \( a_0 + 3 \) and length \( \ell_0 - 1 \). This implies that \( L(A) \) is an AMP with period \( \{0, 2, 3, 4\} \).

Suppose that \( v \equiv 4 \mod 6 \). The set \( L(A_3) \) has minimum \( a_4 = (v + w + 8)/6 \) and length \( \ell_4 = \min\{v + 8, w\}/6 \). The set \( L(A_4) \) has minimum \( a_4 + 4 \) and length \( \ell_4 \) or \( \ell_4 - 1 \). The set \(-1 + L(A_2)\) has minimum \( a_4 + 2 \) and the same length as \( L(A_4) \). This implies that \( L(A) \) is an AMP with period \( \{0, 1, 2, 4\} \).

CASE 3: \( v_{2g}(A) \geq 3 \).

We assert that \( L(A) \) is an AP with difference 1. We choose a factorization \( z \in Z(A) \) and we show that either \( |z| = \max L(A) \) or that \( |z| + 1 \in L(A) \). Since \( V_2U_5 = V_4^3 \), we may suppose that \( \min \{\nu_{2g}(z), \nu_{U_6}(z)\} = 0 \).

Suppose that \( V_1 \vdash z \). If \( U_1 \vdash z \) for some \( i \in \{1, 3\} \), then \( |z| + 1 \in L(A) \). If \( \nu_{U_6}(z) = 0 \), then \( |z| = \max L(A) \). Suppose that \( \nu_{2g}(z) = 0 \). Then \( z = U_4^{k_4}U_5^{k_5}V_1^{\ell_1} \) with \( k_4, k_5, \ell_1 \in \mathbb{N}_0 \), and we claim that then \( |z| = \max L(A) \). By Lemma 2.5 it suffices to show that \( k_5 + \ell_1 = \max |U_5^{k_5}V_1^{\ell_1}| \). Since \( U_5^{k_5}V_1^{\ell_1} \) is not divisible by an atom of length two, it follows that \( \max |U_5^{k_5}V_1^{\ell_1}| \leq |U_5^{k_5}V_1^{\ell_1}|/3 = k_5 + \ell_1 \).

Suppose that \( V_1 \vdash z \). If \( \nu_{2g}(z) = 0 \), then \( |z| = \max L(A) \) because all remaining atoms have \( g \)-norm one. From now on we suppose that \( V_2 \vdash z \). This implies that \( U_5 \vdash z \). Since \( v_{2g}(A) \geq 3 \), then \( U_5 \vdash U_2^{\nu_{U_2}(z)}U_3^{\nu_{U_3}(z)} \) and we obtain a factorization \( z' \in Z(A) \) with \(|z'| = |z| \) and with \( U_5 \vdash z' \) and we still have that \( V_2 \vdash z' \). Since \( V_2U_5 = V_4^3 \), it follows that \(|z'| + 1 \in L(A) \).

**Lemma 3.7.** Let \( G \) be a cyclic group of order \( |G| = 6 \), \( g \in G \) with \( \text{ord}(g) = 6 \), and \( A \in \mathcal{B}(G) \) with \( \text{supp}(A) = \{g, 2g, 4g, -g\} \). If \( v_{2g}(A) + v_{4g}(A) \geq 3 \), then \( L(A) \) is an AP with difference 1 and otherwise it is an AMP with period \( \{0, 1, 2, 4\} \) or \( \{0, 1, 2, 3, 4\} \) or \( \{0, 2, 3, 4\} \).

**Proof.** We set \( G_0 = \{g, 2g, 4g, -g\} \) and list all atoms of \( \mathcal{B}(G_0) \):

\[
|| : ||_{g} = 1 : U_0 = g^6, U_1 = g^4(2g), U_2 = g^2(2g)^2, U_3 = (2g)^3, V_2 = (2g)(4g), W = (4g)g^2, V_1 = g(-g),
|| : ||_{g} = 2 : -U_3 = (4g)^3, -W = (2g)(-g)^2,
|| : ||_{g} = 3 : -U_2 = (4g)^2(-g)^2,
|| : ||_{g} = 4 : -U_1 = (-g)^2(4g),
|| : ||_{g} = 5 : -U_0 = (-g)^6
\]
First, suppose that $v_{2g}(A) + v_{4g}(A) \geq 3$. We choose a factorization $z \in \mathbb{Z}(A)$ and we show that either $|z| = \max L(A)$ or that $|z| + 1 \in L(A)$. We write $z$ in the form

$$z = z^+ z^0 z^-,$$

where $z^+$ is the product of all atoms from $B(\{g, 2g\})$ (these are $U_0, U_1, U_2, U_3$), $z^-$ is the product of all atoms from $B(\{-g, 4g\})$, and $z^0$ is the product of all remaining atoms. Note that the sets in $L(\{g, 2g\})$ and $L(\{-g, 4g\})$ are singletons. If $U_3 \mid z^+$ and $z^- \neq 1$, then $|z| + 1 \in L(A)$. Similarly, if $-U_3 \mid z^-$ and $z^+ \neq 1$, then $|z| + 1 \in L(A)$.

Suppose that $z^- = 1$. If $-W \nmid z$, then all atoms dividing $z$ have $g$-norm equal to 1 whence $|z| = \max L(A)$. Suppose that $-W \mid z$. If $(-W)Y \mid z$ with $Y \in \{U_0, U_1, U_2, W\}$, then $|z| + 1 \in L(A)$. Otherwise, $z$ is a product of the atoms $-W, U_3, V_2$, and $V_1$ which implies that $|z| = \max L(A)$. The case $z^+ = 1$ follows by symmetry.

Thus we may suppose that $z^+ \neq 1$ and $z^- \neq 1$ and that $U_3 \nmid z^+$ and that $(-U_3) \nmid z^-$. Let $A^+$ resp. $A^-$ denote the zero-sum sequences corresponding to $z^+$ resp. $z^-$. If $v_{2g}(A^+) \geq 3$, then there is a factorization $z'$ of $A^+$ with $|z'| = |z^+|$ and with $U_3 \mid z'$ and we are back to an earlier case. Thus we may suppose that $v_{2g}(A^+)$ is a product of the atoms $U_3, V_2$, and $V_1$ which implies that $|z| = \max L(A)$. The case $z^+ = 1$ follows by symmetry.

We infer that $v_{A^+}(z^+) \leq 1$. Now we distinguish two cases.

CASE 1: $U_2 \mid z^+$ or $(-U_2) \mid z^-$. By symmetry we may suppose that $U_2 \mid z^+$. If $(-U_2) \mid z^-$ or $(-U_1) \mid z^-$, then $|z| + 1 \in L(A)$. Otherwise $z^-$ is a product of $(-U_0)$. Since $v_{4g}(A) \geq 1$, it follows that $V_2 \mid z$ or $W \mid z$. Since $(-U_0)V_2 = (-W)(-U_1)$, we are back to a previous case. Since $(-U_0)W = V_1^2(-U_1)$, it follows that $|z| + 1 \in L(A)$.

CASE 2: $U_2 \mid z^+$ and $(-U_2) \mid z^-$. If $(-W) \mid z_0$, then $|z| + 1 \in L(A)$ because $z^+$ is a nonempty product of $U_0$ and $U_1$. If $W \mid z_0$, then $|z| + 1 \in L(A)$ because $z^-$ is a nonempty product of $-U_0$ and $-U_1$. From now on we suppose that $W \nmid z_0$ and $-W \nmid z_0$. Since $v_{2g}(A) + v_{4g}(A) \geq 3$, it follows that $V_2 \mid z_0$. If $U_0 \mid z$, then $U_0V_2 = WU_1$ leads back to the case just handled. If $U_1 \mid z$, then $U_1V_2 = U_2W$ and we are back to CASE 1.

Now suppose that $v_{2g}(A) = v_{4g}(A) = 1$. Then $v_g(A) \equiv v_{-g}(A) \mod 6$, and we set $v_g(A) = v = 6m + r$ and $v_{-g}(A) = w = 6n + r$ with $v, w \in \mathbb{N}, r \in [0, 5]$, and $m, n \in \mathbb{N}_0$. Then

$$A = V_2g^v(-g)^w = U_1Wg^{v-6}(-g)^w = (-U_1)(-W)g^v(-g)^{w-6} = W(-W)g^{v-2}(-g)^{w-2} = U_1(-U_1)g^{v-4}(-g)^{w-4},$$

where negative exponents are interpreted in the quotient group of $\mathcal{F}(G)$. Since each factorization of $A$ is divisible by exactly one of the following

$$V_2, U_1W, (-U_1)(-W), W(-W), U_1(-U_1),$$
we infer that $L(A) = L_1 \cup L_2 \cup L_3 \cup L_4 \cup L_5$, where

$$L_1 = 1 + r + (m + n) + 4 \cdot [0, \min\{m, n\}]$$

$$L_2 = 2 + r + (m + n - 1) + 4 \cdot [0, \min\{m - 1, n\}]$$

$$L_3 = 2 + r + (m + n - 1) + 4 \cdot [0, \min\{m, n - 1\}]$$

$$L_4 = \begin{cases} 2 + (r - 2) + (m + n) + 4 \cdot [0, \min\{m, n\}] & r \in [2, 5] \\ 2 + (r - 2 + 6) + (m + n - 2) + 4 \cdot [0, \min\{m - 1, n - 1\}] & r \in [0, 1] \end{cases}$$

$$L_5 = \begin{cases} 2 + (r - 4) + (m + n) + 4 \cdot [0, \min\{m, n\}] & r \in [4, 5] \\ 2 + (r - 4 + 6) + (m + n - 2) + 4 \cdot [0, \min\{m - 1, n - 1\}] & r \in [0, 3] \end{cases}$$

Note, if exponents in the above equations are negative, then the associated sets $L_i$ are indeed empty. More precisely, if

- $v < 6$, then $m = 0$, $[0, \min\{m - 1, n\}] = \emptyset$, and hence $L_2 = \emptyset$;
- $w < 6$, then $n = 0$ and $L_3 = \emptyset$;
- $r \in [0, 1]$ and $\min\{m, n\} = 0$, then $L_4 = \emptyset$;
- $r \in [0, 3]$ and $\min\{m, n\} = 0$, then $L_5 = \emptyset$.

We observe that $L_2 \subset L_1$ and $L_3 \subset L_1$.

If $r \in [4, 5]$, then $\min L_5 = r - 2 + m + n$, $\min L_4 = 2 + \min L_5$, and $\min L_1 = 3 + \min L_5$; since $L_5$, $L_4$, and $L_1$ are APs with difference 4 and length $\min\{m, n\}$, $L(A)$ is an AMP with period $\{0, 2, 3, 4\}$.

If $r \in [2, 3]$, then $\min L_4 = r + m + n$, $\min L_1 = 1 + \min L_4$, and $\min L_1 = 2 + \min L_4$; since $L_4$, $L_1$, and $L_5$ are APs with difference 4, $L_4$ and $L_1$ have length $\min\{m, n\}$, and $L_5$ has length $\min\{m, n\} - 1$, $L(A)$ is an AMP with period $\{0, 1, 2, 4\}$.

If $r \in [0, 1]$, then $\min L_1 = 1 + r + m + n$, $\min L_5 = 1 + \min L_1$, and $\min L_4 = 3 + \min L_1$; since $L_1$, $L_5$, and $L_4$ are APs with difference 4, $L_4$ and $L_5$ have length $\min\{m, n\} - 1$, and $L_1$ has length $\min\{m, n\}$, $L(A)$ is an AMP with period $\{0, 1, 3, 4\}$. \hfill \Box

**Proposition 3.8.** Let $G$ be a cyclic group of order $|G| = 6$. Then every $L \in \mathcal{L}(G)$ has one of the following forms:

- $L$ is an AP with difference in $\{1, 2, 4\}$.
- $L$ is an AMP with one of the following periods: $\{0, 1, 4\}$, $\{0, 3, 4\}$, $\{0, 1, 2, 4\}$, $\{0, 1, 3, 4\}$, $\{0, 2, 3, 4\}$.

Each of the mentioned forms is actually attained by arbitrarily large sets of lengths.

**Proof.** Let $A' \in \mathcal{B}(G)$. If $A' = 0^mA$ with $m \in \mathbb{N}_0$ and $A \in \mathcal{B}(G \setminus \{0\})$, then $L(A') = m + L(A)$. Thus it is sufficient to prove the assertion for $L(A)$. Let $g \in G$ with $\text{ord}(g) = 6$.

If $\text{supp}(A) = G \setminus \{0\}$, then $L(A)$ is an AP with difference 1 by Proposition 2.2.4. Suppose that $\text{supp}(A) \subseteq G \setminus \{g, -g\} = \{2g, 3g, 4g\} = G_0$. Since $(3g)^2$ is a prime element in $\mathcal{B}(G_0)$ and $\{2g, 4g\}$ is a cyclic group of order three, it follows that $L(A)$ is an AP with difference 1 by Proposition 3.3. Thus from now on we may suppose that $g \in \text{supp}(A)$. We distinguish two cases.

**CASE 1:** $-g \notin \text{supp}(A)$.

Then $\text{supp}(A) \subseteq \{g, 2g, 3g, 4g\}$ and we assert that $L(A)$ is an AP with difference 1. Since all atoms in $\mathcal{B}\{g, 2g, 3g\}$ have $g$-norm one, the sets in $\mathcal{L}(\{g, 2g, 3g\})$ are singletons. Thus the claim holds if $\text{supp}(A) \subseteq \{g, 2g, 3g\}$. If $\text{supp}(A) = \{g, 2g, 3g, 4g\}$,
then the claim follows from Lemma 3.6. Thus it remains to consider the cases where supp(A) equals one of the following three sets:

\[ \{g, 4g\}, \{g, 2g, 4g\}, \text{ or } \{g, 3g, 4g\}. \]

The multiplicity of g in any zero-sum sequence \( B \in \mathcal{B}\{\{g, 2g, 4g\}\} \) is even, whence \( \mathcal{L}(\{g, 2g, 4g\}) = \mathcal{L}(\{2g, 4g\}) \). Since \( \{0, 2g, 4g\} \) is a cyclic group of order three, all sets of lengths in \( \mathcal{L}(\{0, 2g, 4g\}) \) are APs with difference 1 by Proposition 3.1. If supp(A) = \( \{g, 3g, 4g\} \), then the claim follows from Lemma 3.4.

CASE 2: \(-g \in \text{supp}(A)\).

Then \( \{g, -g\} \subset \text{supp}(A) \) and we distinguish four cases.

CASE 2.1: supp(A) \( \subset G_0 = \{g, 3g, -g\} \).

Since \( \min \Delta(G_0) = 2 \) by \[19\] Lemma 6.8.5 and \( \max \Delta(G_0) = 4 \), it follows that \( \Delta(G_0) = \{2, 4\} \). If \( 4 \in \Delta(\mathcal{L}(A)) \), then \( \mathcal{L}(A) \) is an AP with difference 4 by \[6\] Theorem 3.2, and otherwise \( \mathcal{L}(A) \) is an AP with difference 2.

CASE 2.2: supp(A) = \( \{g, 2g, -g\} \) or supp(A) = \( \{g, 4g, -g\} \).

By symmetry it suffices to consider the first case. Lemma 3.6 shows that \( \mathcal{L}(A) \) has one of the given forms.

CASE 2.3: supp(A) = \( \{g, 2g, 3g, -g\} \) or supp(A) = \( \{g, 3g, 4g, -g\} \).

By symmetry it suffices to consider the first case. Lemma 3.3 shows that \( \mathcal{L}(A) \) is an AP with difference 1.

CASE 2.4: supp(A) = \( \{g, 2g, 4g, -g\} \).

Lemma 3.7 shows that \( \mathcal{L}(A) \) has one of the given forms.

Finally, we note that the preceding lemmas imply that each of the mentioned forms is actually attained by arbitrarily large sets of lengths. \( \square \)

The next proposition is used substantially in \[19\] Subsection 4.1, where the system \( \mathcal{L}(G_5) \) is written down explicitly.

**Proposition 3.9.** 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 AP with difference in \( \{1, 3\} \).
- \( L \) is an AMP with period \( \{0, 2, 3\} \) or with period \( \{0, 1, 3\} \).

Each of the mentioned forms is actually attained by arbitrarily large sets of lengths.

**Proof.** By Proposition 2.3 we obtain that \( \Delta^*(G) = \{1, 3\} \). Let \( A' \in \mathcal{B}(G) \). If \( A' = 0^mA \) with \( m \in \mathbb{N}_0 \) and \( A \in \mathcal{B}(G \setminus \{0\}) \), then \( L(A') = m + L(A) \). Thus it is sufficient to prove the assertion for \( L(A) \). If \( |\text{supp}(A)| = 1 \), then \( |L(A)| = 1 \). If \( |\text{supp}(A)| = 4 \), then \( L(A) \) is an AP with difference 1 by Proposition 2.2. Suppose that \( |\text{supp}(A)| = 2 \). Then there is a nonzero \( g \in G \) such that supp(A) = \( \{g, 2g\} \) or supp(A) = \( \{g, 4g\} \). If supp(A) = \( \{g, 2g\} \), then \( L(A) \) is an AP with difference 1 (this can be checked directly by arguing with the g-norm). If supp(A) = \( \{g, 4g\} \), then \( L(A) \) is an AP with difference 3.

Thus it remains to consider the case \( |\text{supp}(A)| = 3 \). We set \( G_0 = \text{supp}(A) \).

Then there is an element \( g \in G_0 \) such that \(-g \in G_0 \). Thus either \( G_0 = \{g, 2g, -g\} \) or \( G_0 = \{1, 3g, -g\} \). Since \( \{1, 3g, -g\} = \{-g, 2(-g), -(-g)\} \), we may suppose without restriction that \( G_0 = \{g, 2g, -g\} \). We list all atoms of \( \mathcal{B}(G_0) \):

\[
\begin{align*}
\| \cdot \|_1 &= 1: g; g^3(2g), g(2g)^2; g(-g), \\
\| \cdot \|_2 &= 2: (2g)^5; (2g)^3(-g); (2g)(-g)^2, \\
\| \cdot \|_3 &= 4: (-g)^5.
\end{align*}
\]
We set $L$ contradiction. Since $\Delta(L) = \{3\}$ by Theorem 3.2, which means that $L(A)$ is an AP with difference 3. Thus it remains to consider the case where $2 \in \Delta(L(A)) \subset [1, 2]$. We show that $L(A)$ is an AMP with period $\{0, 2\}$ or with period $\{0, 1, 3\}$. Since $2 \in \Delta(L(A))$, there exist $k \in \mathbb{N}, A_1, \ldots, A_k, B_1, \ldots, B_{k+2} \in A(G_0)$ such that

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

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 $k + 1 \in L(A)$, 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 $\max L(A) = k$, 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 $k + 1 \in L(A)$, 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 $\left(g^3(2g)\right)\left((2g)(-g)^2\right) = \left((-g)g\right)^2 \left(g(2g)^2\right)$ and $k + 1 \notin L(A)$, 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 $\left((-h)^5\right)\left(h^2(3h)\right) = \left(h(-h)\right)^2 \left((3h)(-h)^3\right)$, we obtain that $k + 1 \in L(A)$, a contradiction.

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

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

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

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

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

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

$$A = (g^5)^{m_1}((-g)^5)((-g)g)^{m_2}((2g)g^3),$$
where $m_1 \in \mathbb{N}_0$, $m_2 \in \mathbb{N}$, and $m_3 \in [0, 4]$. Suppose that $m_1 \geq 1$. Note that
\[ A' = (g^5)((-g)^5)((2g)^5) = ((-g)^3)(2g)((-g)^2)(g^5) = ((-g)^5)((2g)^5), \]
and hence $L(A') = \{3, 5, 6\}$. 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 $L(A)$ is the subset of $L(A')$ and $L(A'')$ whence
\[ L(A) = L(A') + L(A'') = 3 + \{0, 2, 3\} + L(A''). \]
Since $L(A'')$ is an AP with difference $3$, $L(A)$ is an AP with period $\{0, 2, 3\}$. Suppose that $m_1 = 0$. If $m_3 \in [2, 4]$, then $L(A) = \{m_2 + m_3, m_2 + m_3 + 1, m_2 + m_3 + 3\}$ is an AP with period $\{0, 1, 3\}$. If $m_3 = 1$, then $L(A) = \{m_2 + 2, m_2 + 4\}$. If $m_3 = 0$, then $L(A) = \{m_2 + 1, m_2 + 3\}$. □

**Proposition 3.10.** Let $G$ be a finite abelian group, $e_1, e_2 \in G\setminus\{0\}$ with $\langle e_1 \rangle \cap \langle e_2 \rangle = \{0\}$, $\text{ord}(e_2) = n \geq 4$, and $U = (e_1 + e_2)(-e_1)e_2^{n-1}$. Then, for every $k \in \mathbb{N}$, we have
\[ L(U(-U)(e_2(-e_2))^{kn}) = \{2, n, n + 1\} + 2k + (n - 2) \cdot [0, k]. \]

**Proof.** Let $k \in \mathbb{N}$ and $A_k = U(-U)(e_2(-e_2))^{kn}$. If $X \in \mathcal{A}(G)$ with $X \mid A_k$, then
\[ X \in \{U, U, V = (e_1 + e_2)(-e_1)(-e_2), -V, W_0 = (e_1 + e_2)(-e_1 - e_2), \]
\[ W_1 = e_1(-e_1), W_2 = e_2(-e_2), e_2^2, (-e_2)^n\}. \]
Thus
\[ Z(A_k) = W_0W_1Z(W_2^{kn+n-1}) \cup U(-U)Z(W_2^{kn}) \cup V(-V)Z(W_2^{kn+n-2}) \cup U(-V)Z(W_2^{kn-1}(-e_2)^n) \cup (-U)VZ(W_2^{kn-1}e_2^n), \]
and we obtain the claim by using (3.1). □

**Proposition 3.11.** Let $G = C_4^2$, $(e_1, e_2, e_3, e_4)$ be a basis of $G$, $e_0 = e_1 + \ldots + e_4$, $U_4 = e_0 \ldots e_4$, $U_3 = e_0e_1e_2(e_1 + e_2 + e_3)$, and $U_2 = e_1e_2(e_1 + e_2)$.

1. For each $k \in \mathbb{N}$, $L((U_4U_4)^{2k}) = \{4k\} \cup [4k + 2, 9k]$.  
2. For each $k \in \mathbb{N}$, $L(U_4^{2k}U_2) = (2k + 1) + \{0, 1, 3\} + 3 \cdot [0, k - 1]$.  

**Proof.** 1. Let $k \in \mathbb{N}$ and $A_k = (U_3U_4)^{2k}$. Then  
\[ \{4k\} \cup [4k + 2, 9k - 2] \cup \{9k\} = (2k + 2 \cdot [0, k]) + (2k + 3 \cdot [0, k]) = L(U_3^{2k}) + L(U_4^{2k}) \subseteq L((U_3U_4)^{2k}). \]
Since $\max L(A_k) = \lceil A_k/2 \rceil = 9k$, it follows that $\max L(A_k) = 9k$. We set $z = U_3^{2k}U_4^{2k} \in Z(A_k)$. Since $U_4$ is the only atom of length $D(G) = 5$ dividing $A_k$ and since $2k = \nu_U(A_k) = \nu_U(z) = \max \{\nu_U(z') \mid z' \in Z(A_k)\}$, it follows that $\min L(A_k) = \lceil z \rceil = 4k$.

Next we assert that $4k + 1 \not\in L(A_k)$. For $\nu \in [0, 4]$, we set $V_\nu = e_\nu^2$ and $V_5 = (e_1 + e_2 + e_3)^2$. Since $Z(U_3^2) = \{U_3^2, V_1V_2V_3V_5\}$, $Z(U_4^2) = \{U_4^2, V_1V_2V_3V_4V_6\}$, and $Z(U_3U_4) = \{U_3U_4, V_1V_2V_3W\}$ where $W = (e_1 + e_2 + e_3)e_0$, it follows that $\min (L(A_k) \setminus \{4k\}) = 4k + 2$.

Since $A_k$ has precisely one factorization $z$ of length $\lceil z \rceil = \max L(A_k) = 9k$, and $z$ is a product of atoms of length two with $V_0V_4V_5 \mid z$. Since $V_0V_4V_5 = W^2$, it follows that $A_k$ has a factorization of length $9k - 1$.  

**Sets of lengths are (almost) arithmetical progressions**

17
2. Setting \( W = (e_1 + e_2)e_3e_4e_5 \) we infer that \( U_2^2U_2 = U_3(e_2^2)(e_2^2)W = U_2(e_2^2) \cdot \ldots \cdot (e_2^2) \) and hence \( L(U_2^2U_2) = \{3, 4, 6\} \). Thus for each \( k \in \mathbb{N} \) we obtain that
\[
L(U_2^{2k}U_2) = (\{1\} + L(U_2^{2k})) \cup (L(U_2^{2k-2}) + L(U_2^2U_2)) \\
= (2k + 1 + 3 \cdot [0, k]) \cup (2k - 2 + 3 \cdot [0, k - 1] + \{3, 4, 6\}) \\
= (2k + 1 + 3 \cdot [0, k]) \cup (2k + 2 + 3 \cdot [0, k - 1]) \cup (2k + 4 + 3 \cdot [0, k - 1]) \\
= (2k + 1) + \{0, 1, 3\} + 3 \cdot [0, k - 1]. \quad \square
\]

**Proposition 3.12.** 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 \( U = (e_1 \cdot \ldots \cdot e_r)^2e_0 \).

1. If \( r = 3 \), then for each \( k \in \mathbb{N} \) we have
\[
L(U^{6k+1}(U)) = [6k + 2, 14k + 5] \cup \{14k + 7\}.
\]

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

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

First, consider \( L(U^{6k}) \). We observe that \( Z(U^2) = \{U^2, U_1U_2U_3X, U_0U_1U_2U_3U_4U_5^2\} \) and \( Z(U^3) = \{U^3, UU_1U_2U_3X, U_0U_1U_2U_3U_4U_5^2\} \). Furthermore, \( \min L(U^{6k}) = 6k \), \( \max L(U^{6k}) = 14k \), \( \Delta([e_0, \ldots, e_3]) = \{2\} \), and hence
\[
L(U^{6k}) = 6k + 2 \cdot [0, 4k].
\]

Next, consider \( L((-U)U) \). For subsets \( I, J \subset [1, 3] \) with \( [1, 3] = \emptyset J \), we set
\[
W_I = e_0 \prod_{i \in I} e_i^3 \prod_{j \in J} (-e_j).
\]

Since
\[
Z(U((-U))) = \left\{ V_0V_1^2V_2^2V_3^2 \right\} \cup \left\{ W_I((-W_I) \prod_{j \in J} V_j \mid I, J \subset [1, 3] \text{ with } [1, 3] = I \cup J \right\},
\]

it follows that
\[
L((-U)U) = \left\{ 7 \right\} \cup \left\{ 2 + |J| \mid I, J \subset [1, 3] \text{ with } [1, 3] = I \cup J \right\} = \{2, 3, 4, 5, 7\},
\]

which implies that
\[
[6k + 2, 14k + 5] \cup \{14k + 7\} = L((-U)U) + L(U^{6k}) \subset L(A_k) \subset [6k + 2, 14k + 7].
\]

It remains to show that \( 14k + 6 \notin L_k \). For this, we consider the unique factorization \( z \in Z(A_k) \) of length \( |z| = 14k + 7 \) which has the form
\[
z = (U_0U_1U_2U_3^2V_4^2V_5^2)^{2k}(V_0V_1^2V_2^2V_3^2).
\]

Assume to the contrary that there is a factorization \( z' \in Z(A_k) \) of length \( |z'| = 14k + 6 \). If \( V_0 \parallel z' \), then \( V_0V_1^2V_2^2V_3^2 | z' \) and \( z' = V_0V_1^2V_2^2V_3^2x \) with \( x \in Z(U^{6k}) \). Whence \( |x| \in L(U^{6k}) \) and \( |z'| \in 7 + L(U^{6k}) \), a contradiction. Suppose that \( V_0 \nparallel z' \). Then there are \( I, J \subset [1, 3] \) with \( [1, 3] = I \cup J \) such that \( W_I((-W_I) \prod_{j \in J} V_j) | z' \) and hence \( z' = W_I((-W_I)(\prod_{j \in J} V_j)x \) with \( x \in Z(U^{6k}) \). Thus \( |z'| \in [2, 5] + L(U^{6k}) \), a contradiction.
2. Let \( r = 4 \) and \( k \in \mathbb{N} \). We have \( L(U^2) = \{2,5\} \) and \( L(U^{3k}) = 3k + 3 \cdot [0,2k] \).

We define
\[
V_2 = (e_1 + e_2)e_1 e_2 e_3^2 e_4^2 e_5, \quad V_3 = (e_1 + e_2)e_3 e_4 e_5^2, \quad \text{and} \quad W = e_1 \cdots e_4 e_5^2,
\]
and observe that
\[
U^3 V_1 = U^3 V_2 (e_3^3) = U^3 V_3 (e_2^3)^2 (e_3^3) (e_4^3)
\]
whence \( L(U^3 V_1) = \{4,5,7,8\} \). Clearly, each factorization of \( U^3 V_1 \) contains exactly one of the atoms \( V_1, V_2, V_3 \), and it contains it exactly once. Therefore we obtain that
\[
L(U^{3k} V_1) = (\{1\} + L(U^{3k})) \cup (L(U^3 V_1) + L(U^{3k-3}))
\]
\[
= ((3k+1) + 3 \cdot [0,2k]) \cup (\{4,5,7,8\} + (3k-3) + 3 \cdot [0,2k-2])
\]
\[
= (3k+1) + 3 \cdot [0,2k] \cup ((3k+1) + \{0,1,3\} + 3 \cdot [0,2k-2])
\]
\[
= (3k+1) + \{0,1,3\} + 3 \cdot [0,2k-1]. \quad \square
\]

**Proof of Theorem 1.1.**

1. (a) \( \Rightarrow \) (b) This implication is 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 AP. We distinguish four cases.

(d) \( \Rightarrow \) (a) Proposition 3.1 shows that, for all groups mentioned, all sets of lengths are APs. Proposition 2.3 shows that all differences lie in \( \Delta^*(G) \).

(c) \( \Leftrightarrow \) (d) This is the special case for finite groups of Theorem 1.1 (see Remark 3.13).

**CASE 1:** \( n \geq 5 \).

Then Proposition 3.6 provides examples of sets of lengths which are not APs.

**CASE 2:** \( n = 4 \).

Since \( G \) is not cyclic, it has a subgroup isomorphic to \( C_2 \oplus C_4 \). Then Theorem 6.6 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 \( C_n^r \) with \( r \geq 3 \), and Proposition 3.12 provides examples of sets of lengths which are not APs.

**CASE 4:** \( n = 2 \).

Then \( G \) is isomorphic to \( C_2^r \) with \( r \geq 4 \), and Proposition 3.11 provides examples of sets of lengths which are not APs.

2. (b) \( \Rightarrow \) (a) Suppose that \( G \) is a subgroup of \( C_4^2 \) or a subgroup of \( C_3^3 \). Then Proposition 2.3 implies that \( \Delta^*(G) \subset \{1,2\} \), and hence Proposition 2.2 implies the assertion.

(a) \( \Rightarrow \) (b) Suppose that (b) does not hold. Then \( G \) has a subgroup isomorphic to a cyclic group of order \( n \geq 5 \), or isomorphic to \( C_4^2 \), or isomorphic to \( C_3^3 \). We show that in none of these cases (a) holds.

If \( G \) has a subgroup isomorphic to \( C_n \) for some \( n \geq 5 \), then Proposition 3.6 shows that (a) does not hold. If \( G \) has a subgroup isomorphic to \( C_4^2 \), then Proposition 3.12 shows that (a) does not hold. If \( G \) has a subgroup isomorphic to \( C_3^3 \), then Proposition 3.12 shows that (a) does not hold.

3. Let \( \Delta \) be finite with \( \Delta^*(G) \subset \Delta \subset \mathbb{N} \). If \( G \) is cyclic with \( |G| \leq 6 \), then all sets of lengths are AMPs with difference in \( \Delta^*(G) \) by Propositions 3.1, 3.5, and
3.9 If \( \exp(G) \geq 7 \), then Proposition 3.2 shows that there are arbitrarily large sets of lengths that are not AMPs with difference \( d \in \Delta \).

Suppose that \( G \) has rank \( r \geq 2 \) and \( \exp(G) = n \in [2, 6] \). If \( n \geq 4 \), then Proposition 3.10 shows that there are arbitrarily large sets of lengths that are not AMPs with difference \( d \in \Delta \). Thus it suffices to consider elementary 2-groups and elementary 3-groups.

Suppose that \( G = C_5 \). If \( r \leq 3 \), then the assertion follows from 1. If \( r \geq 4 \), then the assertion follows from Proposition 3.11.1.

Suppose that \( G = C_5 \). If \( r \leq 2 \), then the assertion follows from 1. If \( r \geq 3 \), then the assertion follows from Proposition 3.12.1.

**Proof of Corollary 1.2** Let \( G' \) be an abelian group such that \( L(G) = L(G') \). Then \( G' \) is finite by Proposition 2.2 and by [16, Theorem 7.4.1]. By Proposition 2.3 we have \( D(G) = \rho_2(G) = \rho_2(G') = D(G') \), and \( L(G) \) satisfies one of the properties given in Theorem 1.1 if and only if the same is true for \( L(G') \). We distinguish three cases.

**CASE 1:** \( L(G) \) satisfies the property in Theorem 1.1.1.

Then \( G \) is cyclic of order \( |G| \leq 4 \) or isomorphic to a subgroup of \( C_2^3 \) or isomorphic to a subgroup of \( C_2^2 \). Moreover, the same is true for \( G' \). Since \( D(G) \geq 4 \), the assertion follows from Proposition 3.2.1.

**CASE 2:** \( L(G) \) satisfies the property in Theorem 1.1.2.

By CASE 1, we may suppose that \( L(G) \) and \( L(G') \) do not satisfy the property in Theorem 1.1.1. Thus \( G \) and \( G' \), are isomorphic to one of the following groups: \( C_2^3 \), \( C_2 \oplus C_4 \), \( C_2^2 \oplus C_4 \), \( C_2 \oplus C_4^2 \), \( C_2^2 \oplus C_2^2 \), or \( C_2^3 \). Since \( C_2^3 \) and \( C_2^2 \) are the only non-isomorphic groups having the same Davenport constant, it remains to show that \( L(C_2^3) \neq L(C_2^2) \). Since \( \max \Delta(C_2^3) = 3 \) (by [21, Lemma 3.3]) and \( \max \Delta(C_2^2) = 2 \) (by [14, Proposition 5.5]), the assertion follows.

**CASE 3:** \( L(G) \) satisfies the property in Theorem 1.1.3.

By CASE 1, we may suppose that \( G \) and \( G' \) do not satisfy the property in Theorem 1.1.1. Thus \( G \) and \( G' \) are cyclic of order five or six. Since \( D(C_5) = 5 \) and \( D(C_6) = 6 \), the claim follows.

**Remark 3.13.**

1. Let \( H \) be an atomic monoid. The system of sets of lengths \( L(H) \) is said to be additively closed if the sum set \( L_1 + L_2 \in L(H) \) for all \( L_1, L_2 \in L(H) \). Thus \( L(H) \) is additively closed if and only if \( (L(H), +) \) is a commutative reduced semigroup with respect to set addition. If this holds, then \( L(H) \) is an acyclic semigroup in the sense of Cilleruelo, Hamidoune, and Serra ([7]). \( L(H) \) is additively closed in certain Krull monoids stemming from module theory ([14, Section 6.C]). Examples in a non-cancellative setting can be found in [20, Theorem 4.5] and a more detailed discussion of the property of being additively closed is given in [18].

2. Several properties occurring in Theorem 1.1 can be characterized by further arithmetical invariants such as the catenary degree \( c(G) \) and the tame degree \( t(G) \) (for background see [16] 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) \( c(G) \leq 3 \) or \( c(G) = 4 \) and \( \{2, 4\} \in L(G) \).
- (f) \( c(G) \leq 3 \) or \( t(G) = 4 \).
(use [21, Theorem A], [11, Theorem 4.12], and [16, Theorem 6.6.3]).

References


(A.G.) Institute for Mathematics and Scientific Computing, University of Graz, NAWI Graz, Heinrichstrasse 36, 8010 Graz, Austria

E-mail address: alfred.geroldinger@uni-graz.at

(W.S.) Université Paris 13, Sorbonne Paris Cité, LAGA, CNRS, UMR 7539, Université Paris 8, F-93430, Villetaneuse, France, and, Laboratoire Analyse, Géometrie 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