Journal de Théorie des Nombres
de Bordeaux **14** (2002), 221–239

Zero-sumfree sequences in cyclic groups and some arithmetical application

par Alfred GEROLDINGER et Yahya Ould HAMIDOUNE

Résumé. Nous montrons que dans un groupe cyclique d'ordre n, toute suite S de longueur $|S| \geq \frac{n+1}{2}$ sans sous-suite non vide de somme nulle contient un élément d'ordre n ayant une grande multiplicité.

Abstract. We show that in a cyclic group with n elements every zero-sumfree sequence S with length $|S| \geq \frac{n+1}{2}$ contains some element of order n with high multiplicity.

1. Introduction

Let G be a finite cyclic group with $|G| = n$ and let S be a sequence in G. We say that S is zero-sumfree, if no non-empty subsequence of S sums to zero. An easy observation shows that $n - 1$ is the maximal length of a zero-sumfree sequence and if S is a zero-sumfree sequence with length $|S| = n - 1$, then S consists of one element $g \in G$ with order n which is repeated $n - 1$ times. Investigations of the structure of long zero-sumfree sequences were started in the seventies by P. Erdös et al. In [BEN75] it is proved that a zero-sumfree sequence with length $|S| \geq \frac{n+1}{2}$ contains some element with multiplicity $2|S| - n + 1$. In a recent paper by W. Gao and the first author it is proved that a zero-sumfree sequence S with $|S| \geq \frac{n+3}{2}$ contains some element of order n (see [GG98]). Using a new approach we can sharpen this result and show that a zero-sumfree sequence S with length $|S| \geq \frac{n+1}{2}$ contains some element of order n with high multiplicity. It is easy to verify that this result is best possible (see Theorem 3.12 and Remark 3.13).

Besides of being of interest for its own right, any information about the structure of zero-sumfree sequences in a finite abelian group G gives information about the non-uniqueness of factorizations in a Krull monoid having divisor class group G. For this connnection and some general information on factorization theory we refer to the survey articles in [And97]. Let H

Manuscrit reçu le 18 janvier 2001.

be a Krull monoid with cyclic divisor class G such that every class contains a prime divisor and set $|G| = n$. Then the sets of lengths are almost arithmetical multiprogressions and let $\Delta^*(G)$ denote the set of possible differences. It is easy to see that $\max \Delta^*(G) = n - 2$ and having the sharp result of Theorem 3.12 at our disposal we can show that the second largest value in $\Delta^*(G)$ equals $\lfloor \frac{n}{2} \rfloor - 1$ (Theorem 4.4).

2. Preliminaries

Let $\mathbb{N}$ denote the positive integers and let $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. For some real number $x \in \mathbb{R}$ let $\lfloor x \rfloor \in \mathbb{Z}$ denote the largest integer with $\lfloor x \rfloor \le x$ and $\lceil x \rceil \in \mathbb{Z}$ the smallest integer with $x \le \lceil x \rceil$. For $a, b \in \mathbb{Z}$ we set $[a, b] = \{x \in \mathbb{Z} \mid a \le x \le b\}$.

Throughout, all abelian groups will be written additively. Let G be an abelian group, $\emptyset \ne G_0 \subset G$ a finite subset, $\mathcal{F}(G_0)$ the free abelian monoid with basis G_0 and

$$S = \prod_{i=1}^{l} g_i = \prod_{g \in G_0} g^{v_g(S)} \in \mathcal{F}(G_0)$$

a *sequence* in G_0 where $g_1, \ldots, g_l \in G_0$ and $v_g(S) \in \mathbb{N}_0$ for all $g \in G_0$. We use the same notations as in [GG99]. In particular, $|S| = l = \sum_{g \in G_0} v_g(S)$ denotes the *length* of S, $\mathrm{supp}(S) = \{g_1, \ldots, g_l\} = \{g \in G_0 \mid v_g(S) > 0\} \subset G_0$ the *support* of S, $\sigma(S) = \sum_{i=1}^{l} g_i \in G$ the *sum* of S and

$$\Sigma(S) = \{\sum_{i \in I} g_i \mid \emptyset \ne I \subset [1, l]\} \subset G.$$

The sequence S is called

- *zero-sumfree* if $0 \notin \Sigma(S)$,
- *squarefree* if $v_g(S) = 1$ for all $g \in \mathrm{supp}(S)$,
- *a zero-sum sequence*, if $\sigma(S) = 0$,
- *a minimal zero-sum sequence*, if S is a zero-sum sequence and every proper subsequence is zero-sumfree.

If $G = \mathbb{Z}/n\mathbb{Z}$ for some $n \in \mathbb{N}$ and $S = \prod_{i=1}^{l} (a_i + n\mathbb{Z}) \in \mathcal{F}(\mathbb{Z}/n\mathbb{Z})$ where $a_1, \ldots, a_l \in [1, n]$, we set

$$\sigma_{\mathbb{Z}}(S) = \sum_{i=1}^{l} a_i \in \mathbb{N}.$$

Clearly, $\sigma_{\mathbb{Z}}(S) + n\mathbb{Z} = \sigma(S)$, S is a zero-sum sequence if and only if $\sigma_{\mathbb{Z}}(S) \equiv 0 \mod n$, and if $\sigma_{\mathbb{Z}}(S) < n$, then S is zero-sumfree.

We denote by $\mathcal{A}(G_0)$ the set of all minimal zero-sum sequences in G_0. This is a finite set and

$$\mathsf{D}(G_0) = \max\{|S| \mid S \in \mathcal{A}(G_0)\}$$

denotes *Davenport's constant* of G_0. If G is cyclic, then $\mathsf{D}(G) = |G|$ and $|G| - 1$ is the maximal length of a zero-sumfree sequence in G.

3. Zero-sumfree sequences

We shall use the following two well-known addition theorems. The first one is a special case of Chowla's Addition Theorem (we give a simple proof) and the second one follows from a result of L. Moser and P. Scherk (cf. [MS55]).

Proposition 3.1. *Let G be a finite cyclic group, $a \in G$ with* $\mathrm{ord}(a) = |G|$ *and let B be a subset of G. Then $|\{0, a\} + B| \ge \min\{|G|, |B| + 1\}$.*

Proof. Suppose that $|\{0, a\} + B| \le |B|$. Since $B \subset \{0, a\} + B$, it follows that $B = \{0, a\} + B$ whence $a + B \subset B$. Therefore $ja + B \subset B$ for every $j \in \mathbb{N}$ and thus

$$G = G + B = \{ja \mid j \in \mathbb{N}\} + B \subset B$$

whence $|\{0, a\} + B| \ge |B| \ge |G|$. □

Proposition 3.2. *Let G be a finite abelian group and $S \in \mathcal{F}(G)$ a zero-sumfree sequence. If $S = \prod_{i=1}^{l} S_i$ with $S_1, \ldots, S_l \in \mathcal{F}(G)$, then $|\Sigma(S)| \ge \sum_{i=1}^{l} |\Sigma(S_i)|$.*

Lemma 3.3. *Let G be a finite cyclic group with $|G| = n \ge 4$ and $S \in \mathcal{F}(G)$ a zero-sumfree sequence such that $v_g(S) > 0$ for some $g \in G$ with* $\mathrm{ord}(g) = n$. *Then*

$$|\Sigma(S)| \ge \min\{2|S| - v_g(S), |S| + v_g(S) - 1\}.$$

Proof. Without restriction we may suppose that

$$S = (1 + n\mathbb{Z})^k \prod_{i=1}^{l} (a_i + n\mathbb{Z})$$

where $k = v_{1+n\mathbb{Z}}(S) \in \mathbb{N}$, $l \in \mathbb{N}_0$ and $a_1, \ldots, a_l \in [2, n-1]$.

Case 1: For every $i \in [1, l]$ we have $a_i \in [2, k]$. Then

$$\Sigma(1^k \prod_{i=1}^{l} a_i) = [1, k] + \{0, a_1\} + \cdots + \{0, a_l\} = [1, k + a_1 + \cdots + a_l].$$

Since S is zero-sumfree, it follows that $k + \sum_{i=1}^{l} a_i < n$ whence

$$|\Sigma(S)| \ge k + 2l = 2(k + l) - k = 2|S| - v_{1+n\mathbb{Z}}(S).$$

Case 2: There exists some $i \in [1, l]$ such that $a_i \notin [2, k]$. Since S is zero-sumfree, it follows that $a_i \notin [n - k, n - 1]$. This implies that

$$\Sigma(1^k a_i) = [1, k] \cup (a_i + [1, k])$$

and

$$|\Sigma\big((1+n\mathbb{Z})^k(a_i+n\mathbb{Z})\big)| \ge 2k.$$

Applying Proposition 3.2 we infer that

$$\begin{aligned}|\Sigma(S)| &\ge |\Sigma\big((1+n\mathbb{Z})^k(a_i+n\mathbb{Z})\big)| + |\Sigma\big(\prod_{\nu\in[1,l]\setminus\{i\}}(a_\nu+n\mathbb{Z})\big)| \\ &\ge 2k+(l-1) = |S| + v_{1+n\mathbb{Z}}(S) - 1.\end{aligned}$$

□

Definition 3.4. For a finite abelian group G, a non-empty subset $G_0 \subset G$ and some $k \in \mathbb{N}$ we set

$$f(G_0,k) = \min\{|\Sigma(S)| \,:\, S \in \mathcal{F}(G_0) \text{ zero-sumfree, squarefree and } |S| = k\}$$

The above invariant was introduced by Eggleton and Erdös in [EE72]. For information around it and some recent results we refer to [GG98], section three. Here we only need the following lemma which is well-known. For convenience we provide its simple proof.

Lemma 3.5. *Let G be a finite abelian group and $G_0 \subset G$ a subset which contains a squarefree zero-sumfree sequence of length three but no elements of order two. Then $f(G_0,1)=1, f(G_0,2)=3$ and $f(G_0,3)\ge 6$.*

Proof. Clearly, $f(G_0,1)=1$ and if $S=a\cdot b\in\mathcal{F}(G_0)$ with $a\ne b$, then $\Sigma(S)=\{a,b,a+b\}$, $|\Sigma(S)|=3$ and thus $f(G_0,2)=3$.

Let $S=a_1\cdot a_2\cdot a_3\in\mathcal{F}(G_0)$ be a squarefree, zero-sumfree sequence. Clearly, $M=\{a_1+a_2, a_1+a_3, a_2+a_3, a_1+a_2+a_3\}\subset\Sigma(S)$ and $|M|=4$. We assert that at most one of the elements a_1,a_2,a_3 lies in M. This implies that $|\Sigma(S)|\ge 6$ and we are done. Assume to the contrary, that there are $i,j\in[1,3]=\{i,j,k\}$ such that $a_i,a_j\in M$. Then $a_i=a_j+a_k$ and $a_j=a_i+a_k$ whence $2a_k=0$, a contradiction. □

Next we introduce a key notion of this paper.

Definition 3.6. Let G be a finite abelian group, $S\in\mathcal{F}(G)$ a non-empty sequence, $k\in\mathbb{N}$ and $|S|=kq-r$ with $q\in\mathbb{N}$ and $r\in[0,k-1]$. An *optimal k-partition* of S is a product decompositon $S=\prod_{i=1}^q S_i$ where $S_1,\ldots,S_q\in\mathcal{F}(G)$ are squarefree and $|S_1|=\cdots=|S_{q-1}|=k$ (then clearly $q=\left\lceil\frac{|S|}{k}\right\rceil$ and $|S_q|=k-r\in[1,k]$).

The reason why we are interested in optimal k-partitions lies in the fact, that an optimal k-partition of a zero-sumfree sequence S gives a large lower bound for $|\Sigma(S)|$. This will be done in the next lemma.

Lemma 3.7. *Let G be a finite abelian group, $S \in \mathcal{F}(G)$ and $k \in \mathbb{N}$. If S is zero-sumfree and has an optimal k-partition, then for $G_0 = \mathrm{supp}(S)$ we have*

$$|G| - 1 \geq |\Sigma(S)| \geq f(G_0, k)(q-1) + f(G_0, |S| - k(q-1)).$$

Proof. Let $S = \prod_{i=1}^{q} S_i$ be an optimal k-partition of S. Using Proposition 3.2 we infer that

$$\begin{aligned} |G| - 1 \geq |\Sigma(S)| &\geq \sum_{i=1}^{q-1} |\Sigma(S_i)| + |\Sigma(S_q)| \\ &\geq f(G_0, k)(q-1) + f(G_0, |S| - k(q-1)). \end{aligned}$$

□

Proposition 3.8. *Let G be a finite abelian group, $S \in \mathcal{F}(G)$ a non-empty sequence, $k \in \mathbb{N}$ and $|S| = kq - r$ where $r \in [0, k-1]$. Then the following conditions are equivalent:*

1. *S has an optimal k-partition.*
2. *$\max\{v_g(S) \mid g \in G\} \leq q$ and $|\{g \in G \mid v_g(S) = q\}| \leq k - r$.*

Proof. 1. $\Longrightarrow$ 2. Suppose that S has an optimal k-partition, say $S = \prod_{i=1}^{q} S_i$ where all $S_i \in \mathcal{F}(G) \setminus \{1\}$ are squarefree and $|S_1| = \cdots = |S_{q-1}| = k$.

If S is a product of t squarefree subsequences for any $t \in \mathbb{N}$, then clearly $\max\{v_g(S) \mid g \in G\} \leq t$ whence $\max\{v_g(S) \mid g \in G\} \leq q$.

Let $\{g \in G \mid v_g(S) = q\} = \{g_1, \ldots, g_l\}$. If $l = 0$, then clearly $l = 0 \leq k - r$. Suppose $l > 0$ and set $S_0 = \prod_{i=1}^{l} g_i$. Since $S_0^q \mid S$ and $S_1, \ldots, S_q$ are squarefree, it follows that $S_0 \mid S_i$ for every $i \in [1, q]$ whence $T = S S_0^{-q} = \prod_{i=1}^{q} (S_i S_0^{-1})$. Thus it follows that

$$q(k - |S_0|) - r = |S| - q|S_0| = |T| \geq |\prod_{i=1}^{q-1} (S_i S_0^{-1})| = (q-1)(k - |S_0|)$$

whence $l = |S_0| \leq k - r$.

2. $\Longrightarrow$ 1. Let $\{g \in G \mid v_g(S) = q\} = \{g_1, \ldots, g_l\}$ and $S_0 = \prod_{i=1}^{l} g_i$ (clearly, $S_0 = 1$ is the empty sequence if and only if $l = 0$). Then $S = S_0^q \cdot T$ for some $T \in \mathcal{F}(G)$ with $\gcd(S_0, T) = 1$ (i.e., S_0 and T have no elements in common) and $\max\{v_g(T) \mid g \in T\} \leq q - 1$. We show that T may be written in the form

$$T = \prod_{i=1}^{q} T_i \qquad (*)$$

where $T_1, \dots T_q$ are squarefree, $|T_1| = \dots = |T_{q-1}| = k - l$ and $|T_q| = k - l - r \geq 0$. Then obviously

$$S = \prod_{i=1}^{q} (T_i S_0)$$

is an optimal k-partition of S and we are done.

In order to show $(*)$ we write T in the form

$$T = \prod_{\nu=1}^{u} a_\nu^{m_\nu} = \prod_{\nu=1}^{|T|} g_\nu$$

where $a_1, \dots, a_u$ are pairwise distinct, $q - 1 \geq m_1 \geq \dots \geq m_u \geq 1$ and $g_1, \dots, g_{|T|}$ are numbered in the following way: $a_1 = g_1 = \dots = g_{m_1}, a_2 = g_{m_1+1} = \dots = g_{m_1+m_2}$ and so on.

We describe how to build subsequences $T_1, \dots, T_q$. We give the first element g_1 to T_1, the second element g_2 to T_2 and finally g_q to T_q. Then we give g_{q+1} to T_1, ..., g_{2q} to T_q. We do this $k - l - r$ times. After this we have spent $(k - l - r)q$ elements of T. From now on we only give elements to $T_1, \dots, T_{q-1}$. We give $g_{(k-l-r)q+1}$ to T_1, and $g_{(k-l-r)q+q-1}$ to T_{q-1}. We repeat this procedure r times. Hence for every $i \in [1, q-1]$ the sequence T_i consists of $(k - l - r) + r$ elements and T_q consists of $(k - l - r)$ elements. Since $\max\{v_g(T) \mid g \in G\} \leq q-1$ and T is suitably numbered, all sequences T_i are squarefree. Thus $T = \prod_{i=1}^{q} T_i$ and $(*)$ holds. $\square$

Corollary 3.9. *Let G be a finite abelian group and $S \in \mathcal{F}(G) \setminus \{1\}$.*

1. *S has an optimal 2-partition if and only if* $\max\{v_g(S) \mid g \in G\} \leq \left\lceil \frac{|S|}{2} \right\rceil$.
2. *If S has no optimal 3-partition, then one of the following conditions holds:*
   (a) $\max\{v_g(S) \mid g \in G\} \geq \left\lceil \frac{|S|}{3} \right\rceil + 1$.
   (b) *There are two elements $h \neq g \in$* $\mathrm{supp}(S)$ *such that* $v_g(S) = v_h(S) = \frac{|S|+2}{3}$.

Proof. 1. Let $|S| = 2q - r$ with $r \in [0, 1]$ whence $q = \left\lceil \frac{|S|}{2} \right\rceil$. If S has an optimal 2-partition, then $\max\{v_g(S) \mid g \in G\} \leq q$ by Proposition 3.8. Conversely, suppose that $\max\{v_g(S) \mid g \in G\} \leq q$,

$$S_0 = \prod_{\substack{g \in G \\ v_g(S) = q}} g \quad \text{and} \quad S = S_0^q \cdot T.$$

We have to show that $2 - |S_0| - r \geq 0$. Then the assertion follows from Proposition 3.8. For $|S_0| \leq 1$ this is clear. If $|S_0| \geq 2$, then

$$2q - r = |S| = q|S_0| + |T|$$

implies $r = |T| = 0$ and $2 = |S_0|$ whence $2 - |S_0| - r \ge 0$.

2. Let $|S| = 3q - r$ with $r \in [0,2]$ whence $q = \left\lceil \frac{|S|}{3} \right\rceil$. Suppose that S has no optimal 3-partition and that $\max\{v_g(S) \mid g \in G\} \le q$. We have to show that condition b) holds. As above we set

$$S_0 = \prod_{\substack{g \in G \\ v_g(S) = q}} g \quad \text{and} \quad S = S_0^q \cdot T.$$

Then Proposition 3.8 implies that $|S_0| > 3 - r$ whence $|S_0| \ge 2$. Since $3q - r = |S| = q|S_0| + |T|$, it follows that $|S_0| = 2$ whence $r = 2$ and $q = \frac{|S|+2}{3}$. $\square$

Lemma 3.10. *Let G be a cyclic group with even order n, $g \in G$ with* $\mathrm{ord}(g) = \frac{n}{2}$, *and $S \in \mathcal{F}(G \setminus \{g\})$ a sequence such that $v_h(S) \le 2$ for all $h \in G$ with $2h = g$. Then S may be written in the form*

$$S = U \cdot \prod_{i=1}^{t} T_i$$

where $|T_i| \in [1,2]$, $\sigma(T_i) \in \langle g \rangle \setminus \{g\}$ for all $i \in [1,t]$, $|U| \le 2$ and $|U| = 2$ implies that $\sigma(U) = g$.

Proof. We proceed by induction on $|S|$. The assertion is clear for $|S| \le 2$. Suppose $|S| \ge 3$. We construct a subsequence T_0 of S with $|T_0| \in [1,2]$ and $\sigma(T_0) \in \langle g \rangle \setminus \{g\}$. Then the assertion follows by induction hypothesis.

If there exists some $b \in \mathrm{supp}(S) \cap \langle g \rangle$, then we set $T_0 = b$. Suppose that $\mathrm{supp}(S) \subset G \setminus \{g\}$. We decide two cases.

Case 1: S is squarefree. Then there are pairwise distinct elements $a, b, c \in \mathrm{supp}(S)$ and clearly we have $a+b, a+c \in \langle g \rangle$. If $a+b \ne g$, we set $T_0 = a \cdot b$. If $a + b = g$, then $a + c \ne g$ and we set $T_0 = a \cdot c$.

Case 2: S not squarefree. Then there is some $a \in \mathrm{supp}(S)$ with $a^2 \mid S$. If $2a \ne g$, then we set $T_0 = a^2$. Suppose $2a = g$. Then $v_a(S) = 2$ whence there is some $b \ne a$ such that $a^2 \cdot b \mid S$. Thus $a + b \in \langle g \rangle \setminus \{g\}$ and we set $T_0 = a \cdot b$. $\square$

Proposition 3.11. *Let G be a finite cyclic group with $|G| = n \ge 4$, $S \in \mathcal{F}(G)$ a zero-sumfree sequence with $|S| \ge \frac{n+1}{2}$ and $g \in G$ with $v_g(S) \ge \frac{|S|+2}{3}$. Then* $\mathrm{ord}(g) \in \{n, \frac{n}{2}, \frac{n}{3}\}$ *and, if* $\mathrm{ord}(g) = \frac{n}{2}$, *then there is some* $h \in \mathrm{supp}(S)$ *with* $\mathrm{ord}(h) = n$ *and* $v_h(S) \ge 3$.

Proof. We have

$$\mathrm{ord}(g) \ge v_g(S) + 1 \ge \frac{\frac{n+1}{2} + 2}{3} + 1 = \frac{n+11}{6}$$

whence

$$\operatorname{ord}(g) = \frac{n}{j} \quad \text{with} \quad j \in [1, 5].$$

Let H denote the subgroup generated by g whence $|H| = \operatorname{ord}(g)$.

Suppose that $|H| = \frac{n}{2}$ and assume to the contrary that $v_h(S) \le 2$ for all $h \in G$ with $\operatorname{ord}(h) = n$. Applying Lemma 3.10 to $g^{-v_g(S)} \cdot S$ we see that S may be written in the form

$$S = g^{v_g(S)} \prod_{i=1}^{t} T_i \cdot U$$

where $|T_i| \in [1, 2]$, $\sigma(T_i) \in \langle g \rangle \setminus \{g\}$ for all $i \in [1, t]$, $|U| \le 2$ and $|U| = 2$ implies that $\sigma(U) = g$.

First we consider the case $|U| < 2$. Then

$$S' = g^{v_g(S)} \prod_{i=1}^{t} \sigma(T_i) \in \mathcal{F}(H)$$

is a zero-sumfree sequence with $v_g(S') = v_g(S)$. Thus Lemma 3.3 implies that

$$\begin{aligned}
\frac{n}{2} - 1 = |H| - 1 &\ge |\Sigma(S')| \\
&\ge \min\{2|S'| - v_g(S'), |S'| + v_g(S') - 1\} \\
&= \min\{2t + v_g(S), t + 2v_g(S) - 1\} \\
&\ge \min\{(|S| - 1, (|S| - 1 - v_g(S))/2 + 2v_g(S) - 1\} \\
&= \min\{(|S| - 1, (|S| - 1)/2 + 3v_g(S)/2 - 1\} \\
&\ge \min\{(|S| - 1, (|S| - 1)/2 + (|S| + 2)/2 - 1\} \\
&= \min\{|S| - 1, |S| - 1/2\} \\
&= |S| - 1 \ge \frac{n-1}{2},
\end{aligned}$$

a contradiction.

Suppose now that $|U| = 2$. Then

$$S' = g^{v_g(S)+1} \prod_{i=1}^{t} \sigma(T_i) \in \mathcal{F}(H)$$

is a zero-sumfree sequence with $v_g(S') = v_g(S)+1$. Thus Lemma 3.3 implies that

$$\begin{aligned}\frac{n}{2} - 1 = |H| - 1 &\geq |\Sigma(S')| \\ &\geq \min\{2|S'| - v_g(S'), |S'| + v_g(S') - 1\} \\ &= \min\{v_g(S) + 2t + 1, 2v_g(S) + t + 1\} \\ &\geq \min\{v_g(S) + (|S| - 2 - v_g(S)) + 1, \\ &\qquad\qquad 2v_g(S) + (|S| - 2 - v_g(S))/2 + 1\} \\ &= \min\{|S| - 1, 3v_g(S)/2 + |S|/2\} \\ &\geq \min\{|S| - 1, 3((|S| + 2)/3)/2 + |S|/2\} \\ &= \min\{|S| - 1, |S| + 1\} \\ &= |S| - 1 \geq \frac{n-1}{2},\end{aligned}$$

a contradiction.

Assume now that $|H| \in \left\{\frac{n}{4}, \frac{n}{5}\right\}$ and write S in the form

$$S = S_0 S_1 \quad \text{where} \quad S_0 \in \mathcal{F}(H) \quad \text{and} \quad S_1 \in \mathcal{F}(G \setminus H).$$

Since $n \geq 4$ and

$$|S_1| = |S| - |S_0| \geq \frac{n+1}{2} - (|H| - 1) \geq \frac{n+1}{2} - \frac{n}{4} + 1,$$

it follows that $|S_1| \geq 3$.

We assert that there are elements $a, b \in G$ such that $ab \mid S_1$ and $a + H, b + H$ are generators of G/H. Since $S_1 \in \mathcal{F}(G \setminus H)$ and $|S_1| \geq 3$, there exist two elements a, b such that $ab \mid S_1$ and $a + H, b + H \in G/H \setminus \{H\}$. If $|G/H| = 5$, then $a + H, b + H$ are generating elements. Assume to the contrary, that $|G/H| = 4$ and the assertion does not hold. Then $S_1 = a \cdot S_2$ where $S_2 \in \mathcal{F}(H')$ for a subgroup H' with $H \subsetneq H' \subsetneq G$. Then $S_1 S_2$ is a zero-sumfree sequence in H' with

$$|S_0 S_2| = |S| - 1 \geq \frac{n}{2} = |H'|,$$

a contradiction.

Hence there are $a, b \in G$ having the above properties, and we choose some $c \in G$ such that $abc \mid S_1$. By Proposition 3.1 we infer that

$$|\{0, a + H\} + \{0, c + H\}| \geq \min\{G/H, 2 + 2 - 1\} \geq 3$$

and

$$|\left(\{0, a + H\} + \{0, c + H\}\right) + \{0, b + H\}| \geq \min\{G/H, 3 + 2 - 1\} \geq 4.$$

This implies that $|\Sigma(S_0abc)| \ge 4|S_0|$. Thus we may infer that

$$\begin{aligned} n-1 \ge |\Sigma(S)| &\ge |\Sigma(S_0abc)| + |\Sigma(S_1(abc)^{-1})| \\ &\ge 4|S_0| + |S_1(abc)^{-1}| \\ &= 4|S_0| + |S| - |S_0| - 3 \\ &\ge 3|S_0| + |S| - 3 \\ &\ge 3\frac{|S|+2}{3} + |S| - 3 = 2|S| - 1, \end{aligned}$$

a contradiction. □

Theorem 3.12. *Let G be a cyclic group with $|G| = n \ge 3$ and $S \in \mathcal{F}(G)$ a zero-sumfree sequence. If $|S| \ge \frac{n+1}{2}$, then there exists some $g \in \mathrm{supp}(S)$ with*

$$\mathrm{ord}(g) = n \qquad \textit{and} \qquad v_g(S) \ge \begin{cases} \lceil \frac{n+5}{6} \rceil & \textit{if} \quad n \quad \textit{is odd} \\ 3 & \textit{if} \quad n \quad \textit{is even} \end{cases}$$

Proof. The assertion is obvious, if $n = 3$. Hence suppose that $n \ge 4$ and let S be a zero-sumfree sequence with $|S| \ge \frac{n+1}{2}$.

First we show that $\mathrm{supp}(S)$ does not contain an element of order two. Assume to the contrary that $S = gT$ where $2g = 0$. Then n is even, say $n = 2m$, and $|S| \ge m+1$. Let $\varphi : G \to G$ denote the multiplication by 2. Since $\mathsf{D}(\varphi(G)) = m$, the sequence $\varphi(T)$ contains a subsequence with sum zero, say $\sigma(\varphi(T')) = 0$ for some subsequence T' of T. Then either T' or gT' has sum zero in G.

For $k \in [1,3]$ we set $\alpha(k) = f(\mathrm{supp}(S), k)$. Then Lemma 3.5 implies that $\alpha(1) = 1, \alpha(2) = 3$ and $\alpha(3) \ge 6$.

We set

$$|S| = 3\left\lceil \frac{|S|}{3} \right\rceil - r$$

whence

$$\left\lceil \frac{|S|}{3} \right\rceil \ge \frac{n+1}{6} \quad \text{and} \quad r \in [0,2].$$

We show that either there exists some $g \in G$ such that

$$v_g(S) \ge 1 + \left\lceil \frac{|S|}{3} \right\rceil \ge \frac{n+7}{6}.$$

or that there exist two distinct elements $g, h \in G$ such that

$$v_g(S) = v_h(S) = \left\lceil \frac{|S|+2}{3} \right\rceil \ge \frac{n+5}{6}.$$

Assume to the contrary that this does not hold. Then by Corollary 3.9 S has an optimal 3-partition whence Lemma 3.7 implies that

$$\begin{aligned} n-1 &\ge \alpha(3)(\left\lceil \frac{|S|}{3} \right\rceil - 1) + \alpha(3-r) \ge 6(\left\lceil \frac{|S|}{3} \right\rceil - 1) + \alpha(3-r) \\ &\ge 2|S| + 2r - 6 + \alpha(3-r) \ge 2|S| - 1 \ge n. \end{aligned}$$

a contradiction.

Now we first suppose that there exist some $h \ne g \in G$ such that

$$v_h(S) = v_g(S) = \frac{|S|+2}{3} \ge \frac{n+5}{6}$$

and we apply Proposition 3.11.

If one of the two elements has order $\frac{n}{2}$, then n is even and by Proposition 3.11 there exists some $a \in \operatorname{supp}(S)$ with $\operatorname{ord}(a) = n$ and $v_a(S) \ge 3$.

Suppose that $\{\operatorname{ord}(g), \operatorname{ord}(h)\} \subset \{\frac{n}{3}, n\}$. If $\operatorname{ord}(g) = \operatorname{ord}(h) = \frac{n}{3}$, then S would not be zero-sumfree whence either $\operatorname{ord}(g) = n$ or $\operatorname{ord}(h) = n$, and we are done.

Now we suppose that there exists some $g \in G$ such that

$$v_g(S) \ge 1 + \left\lceil \frac{|S|}{3} \right\rceil \ge \frac{n+7}{6}.$$

Then

$$\operatorname{ord}(g) \ge v_g(S) + 1 \ge \frac{n+13}{6}$$

and Proposition 3.11 implies that $\operatorname{ord}(g) \in \{n, \frac{n}{2}, \frac{n}{3}\}$. If $\operatorname{ord}(g) \in \{n, \frac{n}{2}\}$, then the assertion follows.

Assume to the contrary that $\operatorname{ord}(g) = \frac{n}{3}$. We set $H = \langle g \rangle$ and write S in the form

$$S = S_0 S_1 \quad \text{where} \quad S_0 \in \mathcal{F}(H) \quad \text{and} \quad S_1 \in \mathcal{F}(G \setminus H).$$

Since $\frac{n}{3} = \operatorname{ord}(g) > 2$ and

$$|S_1| = |S| - |S_0| \ge \frac{n+1}{2} - (|H| - 1) = \frac{n+1}{2} - \frac{n}{3} + 1,$$

it follows that $|S_1| \ge 3$.

First show that $n \ge 24$. There exist $t \ge \frac{|S_1|-2}{3}$ disjoint subsequences $Q_1, \ldots, Q_t$ of S_1 with length $|Q_i| \le 3$ and sum $\sigma(Q_i) \in H$. Since S is zero-sumfree, the sequence $S_0 \prod_{i=1}^t \sigma(Q_i) \in \mathcal{F}(H)$ is zero-sumfree whence

$$\begin{aligned}\frac{n}{3} - 1 &\geq |S_0 \prod_{i=1}^t \sigma(Q_i)| = |S_0| + t \\ &\geq |S_0| + \frac{|S_1| - 2}{3} = \frac{|S| + 2|S_0| - 2}{3} \\ &\geq \frac{n+1}{6} + \frac{n+7}{9} - \frac{2}{3}\end{aligned}$$

which implies that $n \geq 23$. Since n is a multiple of 3, we obtain that $n \geq 24$.

Case 1: There exists some $b \in G$ such that $v_b(S_1) \geq \left\lceil \frac{|S_1|}{2} \right\rceil + 2$.

If there is some $c \in \operatorname{supp}(S_1)$ with $c \notin \langle b \rangle$, then $S = (b^2 S_0)(b^{\left\lceil \frac{|S_1|}{2} \right\rceil} c) S_3$ for some $S_3 \in \mathcal{F}(G)$ and we infer that

$$\begin{aligned}|\Sigma(S)| &\geq |\Sigma(b^2 S_0)| + |\Sigma(b^{\left\lceil \frac{|S_1|}{2} \right\rceil} c)| + |\Sigma(S_3)| \\ &\geq (3|S_0|) + 2\left\lceil \frac{|S_1|}{2} \right\rceil + |S_3| \\ &= 3|S_0| + 2\left\lceil \frac{|S_1|}{2} \right\rceil + \big(|S| - |S_0| - \left\lceil \frac{|S_1|}{2} \right\rceil - 3\big) \\ &\geq |S| + 2|S_0| + \frac{|S| - |S_0|}{2} - 3 \\ &\geq n - \frac{1}{2},\end{aligned}$$

a contradiction. Thus it follows that $S_1 \in \mathcal{F}(\langle b \rangle)$.

If $g \notin \langle b \rangle$, then we write S in the form $S = (b^2 S_0 g^{-1})(S_1 g b^{-2})$, apply Proposition 3.2 and infer that

$$\begin{aligned}|\Sigma(S)| &\geq |\Sigma((b^2 S_0 g^{-1}))| + |\Sigma((S_1 g b^{-2}))| \\ &\geq (3(|S_0| - 1)) + 2(|S| - |S_0| - 2) \\ &\geq 2|S| + |S_0| - 7 \\ &\geq n + \frac{n-29}{6} \geq n - \frac{5}{6},\end{aligned}$$

a contradiction.

Suppose that $g \in \langle b \rangle$. Then $\frac{n}{3} = \operatorname{ord}(g)$ divides $\operatorname{ord}(b)$ and since $b \in G \setminus H$, it follows that $\langle g \rangle \neq \langle b \rangle$ whence $\langle b \rangle = G$ and $\operatorname{ord}(b) = n$.

We set $S_1 = b \cdot b' \cdot S'$. Then

$$v_b(S') \geq v_b(S_1) - 2 \geq \frac{|S_1|}{2} = \frac{|S'| + 2}{2}$$

whence

$$|S'| - v_b(S') \leq v_b(S') - 1$$

and Lemma 3.3 implies that

$$|\Sigma(S')| \geq |S'| + \min\{|S'| - v_b(S'), v_b(S') - 1\} = 2|S'| - v_b(S').$$

Clearly, we have $|\Sigma(S_0 \cdot b \cdot b')| \geq 3|S_0|$ and so we obtain that

$$\begin{aligned} n - 1 \geq |\Sigma(S)| &\geq |\Sigma(S_0 \cdot b \cdot b')| + |\Sigma(S')| \\ &\geq 3|S_0| + 2|S'| - v_b(S') \\ &= 2|S| - 4 + |S_0| - v_b(S') \\ &\geq (n-1) - 2 + |S_0| - v_b(S') \end{aligned}$$

whence

$$v_b(S) \geq v_b(S') + 1 \geq |S_0| - 1.$$

If $|S_0| \geq \frac{n+11}{6}$, then $v_b(S) \geq \frac{n+5}{6}$. If $|S_0| \leq \frac{n+11}{6}$, then

$$\begin{aligned} v_b(S) &\geq \left\lceil \frac{|S_1|}{2} \right\rceil + 2 \\ &\geq \frac{1}{2}(|S| - |S_0| + 4) \\ &\geq \frac{1}{2}(\frac{n+1}{2} - \frac{n+11}{6} + 4) \\ &= \frac{n+8}{6}. \end{aligned}$$

Case 2. For every $c \in G$ we have $v_c(S_1) \leq \left\lceil \frac{|S_1|}{2} \right\rceil + 1$.

We assert that there are elements $a, b \in G$ such that $ab \mid S_1$, such that for every $c \in G$ we have

$$v_c(S_1(ab)^{-1}) \leq \left\lceil \frac{|S_1|}{2} \right\rceil - 1 = \left\lceil \frac{|S_1(ab)^{-1}|}{2} \right\rceil.$$

Such a choice may be done in the following way. Suppose that $S = \prod_{i=1}^{l} h_i^{k_i}$ with pairwise distinct $h_1, \ldots, h_l$ and $k_1 \geq \cdots \geq k_l \geq 1$. If $k_1 = \left\lceil \frac{|S_1|}{2} \right\rceil + 1$, then we set $a = b = h_1$, and obviously the assertion holds. If $k_1 \leq \left\lceil \frac{|S_1|}{2} \right\rceil$, then $1 \leq k_2 \leq \left\lceil \frac{|S_1|}{2} \right\rceil$. We set $a = h_1, b = h_2$, and obviously, the assertion holds again.

Since $a + H$ and $b + H$ are generating elements of G/H, Proposition 3.1 implies that

$$|\{0, a + H\} + \{0, b + H\}| \geq \min\{|G/H|, 2 + 2 - 1\} = 3$$

whence $|\Sigma(abS_0)| \geq 3|S_0|$.

The sequence $S_1(ab)^{-1}$ satisfies the assumptions of Corollary 3.9 with $k = 2$. We have

$$\left\lceil \frac{|S_1(ab)^{-1}|}{2} \right\rceil - 1 = \left\lceil \frac{|S_1|}{2} \right\rceil - 2$$

and

$$|S_1(ab)^{-1}| - 2\left(\left\lceil \frac{|S_1|}{2} \right\rceil - 2\right) = |S_1| - 2 - 2\left\lceil \frac{|S_1|}{2} \right\rceil + 4,$$

and let r' defined by

$$|S_1| - 2\left\lceil \frac{|S_1|}{2} \right\rceil + 2 = 2 - r'.$$

Thus we obtain that

$$\begin{aligned}
|\Sigma(S_1(ab)^{-1})| &\geq \alpha(2)\left(\left\lceil \frac{|S_1|}{2} \right\rceil - 2\right) + \alpha(2 - r') \\
&\geq 3\left\lceil \frac{|S_1|}{2} \right\rceil - 6 + \alpha(2 - r') \\
&\geq \frac{3}{2}(|S_1| + r') + \alpha(2 - r') - 6 \\
&\geq \frac{3}{2}(|S| - |S_0|) + \frac{3}{2}r' + \alpha(2 - r') - 6 \\
&\geq \frac{3}{2}(|S| - |S_0|) - \frac{7}{2}.
\end{aligned}$$

Summing up we infer that

$$\begin{aligned}
n - 1 \geq |\Sigma(S)| &\geq |\Sigma(S_0ab)| + |\Sigma(S_1(ab)^{-1})| \\
&\geq 3|S_0| + \frac{3}{2}(|S| - |S_0|) - \frac{7}{2} \\
&= \frac{3}{2}(|S| + |S_0|) - \frac{7}{2}
\end{aligned}$$

whence

$$\frac{3}{2}(|S| + |S_0|) \leq n + \frac{5}{2}$$

and thus

$$|S_0| \leq \frac{n+7}{6}.$$

The final inequality implies that

$$\frac{n+7}{6} \leq v_g(S) \leq |S_0| \leq \frac{n+7}{6}$$

whence equality holds.

Since $|S_1| \ge 3$, we may set $S_1 = abcT$ with $c \in G$, $T \in \mathcal{F}(G)$ and infer that

$$\begin{aligned}|\Sigma(S)| &\ge |\Sigma(abcS_0)| + |\Sigma(T)| \\ &\ge 4|S_0| + |T| = 4|S_0| + (|S| - |S_0| - 3) \\ &= |S| + 3(|S_0| - 1) = |S| + \frac{n+1}{2} \\ &\ge n+1,\end{aligned}$$

a contradiction. □

Remark 3.13. We discuss some examples which show that the above result is sharp in general.

1. If n is even but not a power of 2, then the assumption "$|S| \ge \frac{n+1}{2}$" cannot be weakened. Suppose $n = 2^k m$ where $1 < m$ is odd. Then
$$S = (2 + n\mathbb{Z})^{\frac{n}{2}-1} \cdot (m + n\mathbb{Z}) \in \mathcal{F}(\mathbb{Z}/n\mathbb{Z})$$
is a sequence with length $|S| = \frac{n}{2}$ which does not contain an element of order n. We assert that S is zero-sumfree. Assume to the contrary, that S contains a zero-sum subsequence T. Then $T = (2 + n\mathbb{Z})^i \cdot (m + n\mathbb{Z})$ with $i \in [1, \frac{n}{2} - 1]$ and $n \le \sigma_{\mathbb{Z}}(T) \le \sigma_{\mathbb{Z}}(S) < 2n$ whence $\sigma_{\mathbb{Z}}(T) = n$, a contradiction.
2. If n is even, then the assertion "$v_g(S) \ge 3$" cannot be enbettered. Suppose $n = 2m$ for some $m \ge 2$ and consider
$$S = (2 + n\mathbb{Z})^{m-2} \cdot (1 + n\mathbb{Z})^3 \in \mathcal{F}(\mathbb{Z}/n\mathbb{Z}).$$
Then $\sigma_{\mathbb{Z}}(S) = 2m - 1 < n$ whence S is zero-sumfree, $|S| = \frac{n}{2} + 1$ and $v_{1+n\mathbb{Z}}(S) = 3$.
3. If n is odd, then the assertion "$v_g(S) \ge \lceil \frac{n+5}{6} \rceil$" cannot be enbettered. Let $n = 6k - r$ be odd with $r \in [0, 5]$ (whence $k = \lceil \frac{n+5}{6} \rceil$) and
$$S = (1 + n\mathbb{Z})^k (2 + n\mathbb{Z})^k (3 + n\mathbb{Z})^{\frac{n+1}{2} - 2k} \in \mathcal{F}(\mathbb{Z}/n\mathbb{Z}).$$
Then $\sigma_{\mathbb{Z}}(S) = k + 2k + 3(\frac{n+1}{2} - 2k) < n$ whence S is zero-sumfree and
$$\max\{v_g(S) \mid g \in G\} = \max\{k, \frac{n+1}{2} - 2k\} = k = \left\lceil \frac{n+5}{6} \right\rceil.$$

4. On $\Delta^*(G)$

Let G be a finite abelian group and $\emptyset \ne G_0 \subset G$ a non-empty subset. We briefly recall some basic terminology from factorization theory. To do so, we restrict to block monoids. However, matters are similar for Krull monoids having finite divisor class groups. For details the reader is referrred to the survey articles in [And97].

Let $\mathcal{B}(G_0)$ denote the set of all zero-sum sequences in G_0. Then $\mathcal{B}(G_0) \subset \mathcal{F}(G_0)$ is a submonoid - called the *block monoid over* G_0 - and $\mathcal{A}(G_0)$ is precisely the set of irreducible elements of $\mathcal{B}(G_0)$. Let $B \in \mathcal{B}(G_0)$. Then there are minimal zero-sum sequences $U_1, \ldots, U_k \in \mathcal{A}(G_0)$ such that

$$B = U_1 \cdot \ldots \cdot U_k.$$

Such a product decompostion is called a *factorization* of A and k is called the *length* of this factorization. Then

$$\mathsf{L}(B) = \{l \in \mathbb{N} \mid B \text{ has a factorization of length } l\} \subset \mathbb{N}$$

is a finite subset of the positive integers and is called the *set of lengths* of B. For any finite subset $L = \{x_0, \ldots, x_l\} \subset \mathbb{Z}$ with $x_1 < \cdots < x_l$ let

$$\Delta(L) = \{x_i - x_{i-1} \mid i \in [1, l]\} \subset \mathbb{N}$$

denote the *set of distances* of L. Clearly, $|\Delta(L)| \leq 1$ if and only if L is an arithmetical progression. We define

$$\Delta(G_0) = \bigcup_{B \in \mathcal{B}(G_0)} \Delta(\mathsf{L}(B)) \subset \mathbb{N}$$

and say that G_0 is *half-factorial*, if $\Delta(G_0) = \emptyset$ (equivalently, $|\mathsf{L}(B)| = 1$ for all $B \in \mathcal{B}(G_0)$).

We shall need the following properties of $\Delta(G_0)$.

Lemma 4.1. *Let G be a finite abelian group and $G_0 \subset G$ a subset with $\Delta(G_0) \neq \emptyset$.*

1. $\max \Delta(G_0) \leq \mathsf{D}(G_0) - 2$.
2. $\min \Delta(G_0) = \gcd \Delta(G_0)$.

Proof. See Proposition 3 and Proposition 4 in [Ger88]. □

Lemma 4.2. *Let $G = \mathbb{Z}/n\mathbb{Z}$ with $n \geq 4$ and $G_0 \subset G$ a subset with $\Delta(G_0) \neq \emptyset$ and $1 + n\mathbb{Z} \in G_0$. Then*

$$\min \Delta(G_0) = \gcd\{\frac{1}{n}\sigma_{\mathbb{Z}}(U) - 1 \mid U \in \mathcal{A}(G_0)\}.$$

Proof. See Proposition 7 in [Ger87]. □

Let G be a finite abelian group and $G_0 \subset G$ a subset which is not half-factorial. Then for every $N \in \mathbb{N}$ there exists some $B \in \mathcal{B}(G_0)$ such that $|\mathsf{L}(B)| \geq N$. Moreover, there exists some $M \in \mathbb{N}$ such that for every $B \in \mathcal{B}(G_0)$ the set of lengths $\mathsf{L}(B)$ is an *almost arithmetical multiprogression* with bound M. The set $\Delta^*(G)$ defined below describes the set of possible differences which appear in such multiprogressions (cf. [CG97] and [GG00]).

Definition 4.3. Let G be a finite abelian group. Then

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

Now we can formulate the main result in this section which heavily rests on Theorem 3.12.

Theorem 4.4. *Let G be a cyclic group with $|G| = n \geq 4$. Then*

$$\max \Delta^*(G) = n - 2 \quad \textit{and} \quad \max(\Delta^*(G) \setminus \{n-2\}) = \left\lfloor \frac{n}{2} \right\rfloor - 1.$$

Proof. Lemma 4.1 implies that

$$\max \Delta^*(G) \leq \max \Delta(G) \leq \mathsf{D}(G) - 2 = n - 2.$$

If $G_0 = \{1 + n\mathbb{Z}, n - 1 + n\mathbb{Z}\}$, then

$$\mathcal{A}(G_0) = \{(1 + n\mathbb{Z})^n, (n - 1 + n\mathbb{Z})^n, (1 + n\mathbb{Z}) \cdot (n - 1 + n\mathbb{Z})\}$$

whence by Lemma 4.2 we have $n - 2 = \min \Delta(G_0) \in \Delta^*(G)$.

If $n = 2m + 1$ with $m \geq 2$, we set $G_0 = \{1 + n\mathbb{Z}, m + n\mathbb{Z}\}$ and assert that $\min \Delta(G_0) = m - 1 = \lfloor \frac{n}{2} \rfloor - 1$. Clearly, we have

$$\mathcal{A}(G_0) = \{(1 + n\mathbb{Z})^n, (m + n\mathbb{Z})^n, (1 + n\mathbb{Z}) \cdot (m + n\mathbb{Z})^2, \\ (1 + n\mathbb{Z})^{n-m} \cdot (m + n\mathbb{Z})\}$$

and

$$\{\frac{1}{n}\sigma_{\mathbb{Z}}(U) - 1 \mid U \in \mathcal{A}(G_0)\} = \{0, m - 1\}$$

whence Lemma 4.2 implies that $\min \Delta(G_0) = m - 1$.

If $n = 2m$ for some $m \geq 2$, we set $G_0 = \{1 + n\mathbb{Z}, m + n\mathbb{Z}, (n-1) + n\mathbb{Z}\}$ and assert that $\min \Delta(G_0) = m - 1$. Since

$$\mathcal{A}(G_0) = \{(1 + n\mathbb{Z})^n, (n - 1 + n\mathbb{Z})^n, (m + n\mathbb{Z})^2, \\ (m + n\mathbb{Z}) \cdot (1 + n\mathbb{Z})^{n-m}, (m + n\mathbb{Z}) \cdot (n - 1 + n\mathbb{Z})^m\},$$

the assertion follows from Lemma 4.2.

We now come to the proof of

$$\max(\Delta^*(G) \setminus \{n - 2\}) \leq \lfloor \frac{n}{2} \rfloor - 1.$$

Clearly, the assertion holds for $n \in [4, 6]$. Let $n \geq 7$ and $G_1 \subset G$ a non half-factorial subset with $\min \Delta(G_1) < n - 2$. Let $G_0 \subset G_1 \setminus \{0\}$ be a minimal non half-factorial subset with $d = \min \Delta(G_0)$. If $d = n - 2$, then

$$n - 2 \neq \min \Delta(G_1) = \gcd \Delta(G_1) \mid \gcd \Delta(G_0) = n - 2$$

whence $\min \Delta(G_1) \leq \frac{n-2}{2}$. Suppose that $d < n - 2$. It suffices to show that $d \leq \lfloor \frac{n}{2} \rfloor - 1$.

Assume to the contrary that $d \geq \frac{n-1}{2}$. Then

$$\frac{n-1}{2} \leq d = \min \Delta(G_0) \leq \max \Delta(G_0) \leq \mathsf{D}(G_0) - 2$$

implies that $\mathsf{D}(G_0) \ge \frac{n+3}{2}$. Therefore there exists a zero-sumfree sequence $S \in \mathcal{F}(G_0)$ with

$$|S| = \mathsf{D}(G_0) - 1 \ge \frac{n+1}{2}.$$

By Theorem 3.12 there exists some $g \in \operatorname{supp}(S)$ with $\operatorname{ord}(g) = n$. Since $\min \Delta(\{-g, g\}) = n-2$, it follows that $-g \notin G_0$. There exists some group automorphism $\varphi : G \to \mathbb{Z}/n\mathbb{Z}$ with $\varphi(g) = 1 + n\mathbb{Z}$. Since $d = \min \Delta(G_0) = \min \Delta(\varphi(G_0))$, we may suppose without restriction that $g = 1 + n\mathbb{Z}$ and

$$G_0 = \{1 + n\mathbb{Z}, a_2 + n\mathbb{Z}, \ldots, a_s + n\mathbb{Z}\}$$

with $1 = a_1 < a_2 < \cdots < a_s < n-1$. We set

$$\{\frac{1}{n}\sigma_{\mathbb{Z}}(U) - 1 \mid U \in \mathcal{A}(G_0)\} = \{0, d_1, \ldots, d_k\}$$

with $0 < d_1 < \cdots < d_k$. By Lemma 4.2 it follows that $d = \gcd\{d_1, \ldots, d_k\}$. Since

$$\frac{n-1}{2} \le d \le d_k \le \frac{1}{n} a_s n - 1 = a_s - 1 \le n-3,$$

it follows that $k = 1, d_1 = d$ and

$$\sigma_{\mathbb{Z}}(U) \in \{n, n(d+1)\} \qquad \text{for every} \qquad U \in \mathcal{A}(G_0).$$

Case 1: There exists some $a \in \{a_2, \ldots, a_s\}$ with $\gcd\{a, n\} = 1$. Then there exists some $l_1 \in [2, n-1]$ with $al_1 + 1 \equiv 0 \mod n$. Considering the following two irreducible blocks

$$U = (a + n\mathbb{Z})^n \qquad \text{and} \qquad V = (1 + n\mathbb{Z}) \cdot (a + n\mathbb{Z})^{l_1}$$

we infer that $\sigma_{\mathbb{Z}}(U) = na > l_1 a + 1 = \sigma_{\mathbb{Z}}(V)$ and thus $l_1 a + 1 = n$. This implies that

$$\sigma_{\mathbb{Z}}(U) = n\frac{n-1}{l_1} \le n\frac{n-1}{2} < n(d+1),$$

a contradiction.

Case 2: There exists some $a \in \{a_2, \ldots, a_s\}$ with $1 < \gcd\{a, n\} < a$. Then $U = a^{n/\gcd\{a,n\}} \in \mathcal{A}(G_0)$ and

$$n < \sigma_{\mathbb{Z}}(U) = a\frac{n}{\gcd\{a, n\}} \le n\frac{n-2}{2} < n(d+1),$$

a contradiction.

Case 3: For every $i \in [2, s]$ we have $a_i \mid n$. Thus for every $U = \prod_{i=1}^{s}(a_i + n\mathbb{Z})^{k_i} \in \mathcal{A}(G_0)$ with $\sigma_{\mathbb{Z}}(U) > n$ we have $k_i \le \frac{n}{a_i} - 1$ and hence

$$\sigma_{\mathbb{Z}}(U) = \sum_{i=1}^{s} k_i a_i \le \sum_{i=1}^{s}(n - a_i) < s(n-1) \le n\frac{n-1}{2} < n(d+1),$$

a contradiction. $\square$

References

[And97] *Factorization in integral domains.* (Editeur Daniel D. Anderson). Lecture Notes in Pure and Applied Mathematics **189**, Marcel Dekker, Inc., New York, 1997.

[BEN75] J. D. Bovey, P. Erdös, I. Niven, *Conditions for zero sum modulo n.* Canad. Math. Bull. **18** (1975), 27–29.

[CG97] S. Chapman, A. Geroldinger, *Krull domains and monoids, their sets of lengths and associated combinatorial problems.* In *Factorization in integral domains*, 73–112, Lecture Notes in Pure and Appl. Math. **189**, Marcel Dekker, New York, 1997.

[EE72] R. B. Eggleton, P. Erdös, *Two combinatorial problems in group theory.* Acta Arith. **21** (1972), 111–116.

[Ger87] A. Geroldinger, *On non-unique factorizations into irreducible elements* II. Number theory, Vol. II (Budapest, 1987), 723–757, Colloq. Math. Soc. János Bolyai **51**, North-Holland, Amsterdam, 1990.

[Ger88] A. Geroldinger, *Über nicht-eindeutige Zerlegungen in irreduzible Elemente.* Math. Z. **197** (1988), 505–529.

[GG98] W. Gao, A. Geroldinger, *On the structure of zerofree sequences.* Combinatorica **18** (1998), 519–527.

[GG99] W. Gao, A. Geroldinger, *On long minimal zero sequences in finite abelian groups.* Period. Math. Hungar. **38** (1999), 179–211.

[GG00] W. Gao, A. Geroldinger, *Systems of sets of lengths* II. Abh. Math. Sem. Univ. Hamburg **70** (2000), 31–49.

[MS55] L. Moser, P. Scherk, *Distinct elements in a set of sums.* Amer. Math. Monthly **62** (1955), 46–47.

Alfred Geroldinger
Institut für Mathematik
Karl-Franzens Universität
Heinrichstrasse 36
8010 Graz, Austria
E-mail : `alfred.geroldinger@uni-graz.at`

Yahya Ould Hamidoune
E. Combinatoire, Case 189
Universite P. et M. Curie
4, Place Jussieu
75005 Paris, France
E-mail : `yha@ccr.jussieu.fr`