# NOTE ON A CONJECTURE OF GRAHAM

DAVID J. GRYNKIEWICZ

Abstract. An old conjecture of Graham stated that if $n$ is a prime and $S$ is a sequence of $n$ terms from the cyclic group $C_n$ such that all (nontrivial) zero-sum subsequences have the same length, then $S$ must contain at most two distinct terms. In 1976, Erdős and Szemeredi gave a proof of the conjecture for sufficiently large primes $n$. However, the proof was complicated enough that the details for small primes were never worked out. Both in the paper of Erdős and Szemeredi and in a later survey by Erdős and Graham, the complexity of the proof was lamented. Recently, a new proof, valid even for non-primes $n$, was given by Gao, Hamidoune and Wang, using Savchev and Chen's recently proved structure theorem for zero-sum free sequences of long length in $C_n$. However, as this is a fairly involved result, they did not believe it to be the simple proof sought by Erdős, Graham and Szemeredi. In this paper, we give a short proof of the original conjecture that uses only the Cauchy-Davenport Theorem and pigeonhole principle, thus perhaps qualifying as a simple proof. Replacing the use of the Cauchy-Davenport Theorem with the Devos-Goddyn-Mohar Theorem, we obtain an alternate proof, albeit not as simple, of the non-prime case. Additionally, our method yields an exhaustive list detailing the precise structure of $S$ and works for an arbitrary finite abelian group, though the only non-cyclic group for which the hypotheses are non-void is $C_2 \oplus C_{2m}$.

## 1. Introduction

The following was an old conjecture of Graham [6].

**Conjecture 1.1.** *Let $C_p$ be the cyclic group of order $p$ prime and let $S$ a sequence over $C_p$ of length $p$. If all (nontrivial) zero-sum subsequences of $S$ are of the same length, then the number of distinct terms in $S$ is at most 2.*

In 1976, Erdős and Szemeredi gave a proof of the conjecture for sufficiently large primes $p$ [6]. However, the proof was complicated enough that the details for small primes were never worked out. Both in the paper of Erdős and Szemeredi and in a later survey by Erdős and Graham [5], the complexity of the proof was lamented. Recently, a new proof, valid even for non-primes, was given by Gao, Hamidoune and Wang [8], using Savchev and Chen's recently proved structure theorem for zero-sum free sequences of long length in the cyclic group $C_n$ [15].

2000 *Mathematics Subject Classification.* 11B50, 11B75.

Supported by FWF project number M1014-N13.

However, as Savchev and Chen's result is fairly involved, they did not believe it to be the simple proof sought by Erdős, Graham and Szemeredi.

In this paper, we give a short proof to the original conjecture of Graham that uses only the Cauchy-Davenport Theorem and pigeonhole principle [14] [16]. Since the proof of the Cauchy-Davenport Theorem (known since 1813 [2]) is elementary and requires only a paragraph, our proof may perhaps qualify as simple. Replacing the use of the Cauchy-Davenport Theorem with the Devos-Goddyn-Mohar Theorem [4] (alternatively, the partition theorem from [11] [12] could be used instead of Devos-Goddyn-Mohar), we obtain an alternate proof, albeit not as simple, of the non-prime case. With only a little added effort, our method naturally yields an exhaustive list detailing the precise structure of $S$ and shows that the result holds in an arbitrary finite abelian group, though the only additional group for which the hypotheses are non-void is $C_2 \oplus C_{2m}$. We state the main theorem in Section 3, after introducing modern notation for sumsets, sequences and subsequence sums.

## 2. Notation and Preliminaries

We follow the notation of [7], [9], [10] and [13] concerning sumsets, sequences and subsequence sums. For the convenience of the reader less familiar with this notation, we give self-contained definitions for all relevant concepts in this section.

2.1. **Sumsets.** Let $G$ be an abelian group, and let $A, B \subseteq G$ be nonempty subsets. Then

$$A + B = \{a + b \mid a \in A,\, b \in B\}$$

denotes their *sumset*. For $g \in G$, we let $g + A = \{g + a \mid a \in A\}$ and let $r_{A,B}(g)$ denote the number of representations of $g = a + b$ as a sum with $a \in A$ and $b \in B$. The *stabilizer* of $A$ is

$$\mathsf{H}(A) := \{g \in G \mid g + A = A\}.$$

The order of an element $g \in G$ is denoted $\mathrm{ord}(g)$, and we use $\phi_H : G \to G/H$ to denote the natural homomorphism modulo $H$. We use $C_n$ to denote the cyclic group of order $n$.

2.2. **Sequences.** We let $\mathcal{F}(G)$ denote the free abelian monoid with basis $G$ written multiplicatively. The elements of $\mathcal{F}(G)$ are then just multi-sets over $G$, but following long standing tradition, we refer to the $S \in \mathcal{F}(G)$ as *sequences*. We write sequences $S \in \mathcal{F}(G)$ in the form

$$S = s_1 \cdot \ldots \cdot s_r = \prod_{g \in G} g^{\mathsf{v}_g(S)}, \quad \text{where} \quad \mathsf{v}_g(S) \geq 0 \text{ and } s_i \in G.$$

We call $|S| := r = \sum_{g \in G} \mathsf{v}_g(S)$ the *length* of $S$, and $\mathsf{v}_g(S) \in \mathbb{N}_0$ the *multiplicity* of $g$ in $S$. The *support* of $S$ is

$$\mathrm{supp}(S) := \{g \in G \mid \mathsf{v}_g(S) > 0\}.$$

A sequence $S_1$ is called a *subsequence* of $S$ if $S_1|S$ in $\mathcal{F}(G)$ (equivalently, $\mathsf{v}_g(S_1) \le \mathsf{v}_g(S)$ for all $g \in G$), and in such case, $S{S_1}^{-1}$ or ${S_1}^{-1}S$ denotes the subsequence of $S$ obtained by removing all terms from $S_1$. We let

$$\mathsf{h}(S) := \max\{\mathsf{v}_g(S) \mid g \in G\}$$

denote the maximum multiplicity of a term of $S$. Given any map $\varphi : G \to G'$, we extend $\varphi$ to a map of sequences, $\varphi : \mathcal{F}(G) \to \mathcal{F}(G')$, by letting $\varphi(S) := \varphi(s_1) \cdots \varphi(s_r)$.

2.3. **Subsequence Sums.** If $S = s_1 \cdots s_r \in \mathcal{F}(G)$, with $s_i \in G$, then the *sum* of $S$ is

$$\sigma(S) := \sum_{i=1}^{r} s_i = \sum_{g \in G} \mathsf{v}_g(S) g.$$

We say $S$ is *zero-sum* if $\sigma(S) = 0$. We adapt the convention that the sum of the trivial/empty sequence is zero. We follow the usual notation for the set of subsequence sums:

$$\Sigma_n(S) \quad = \quad \{\sigma(T) \mid \ T|S \text{ and } |T| = n\}$$

$$\Sigma_{\le n}(S) = \bigcup_{i=1}^{n} \Sigma_i(S) \quad \text{and} \quad \Sigma_{\ge n}(S) = \bigcup_{i=n}^{|S|} \Sigma_i(S) \quad \text{and} \quad \Sigma(S) = \Sigma_{\le |S|}(S).$$

2.4. **Preliminary Results.** For a finite abelian group $G$, we define the Davenport constant $\mathsf{D}(G)$ to be the minimal integer such that any $S \in \mathcal{F}(G)$ with $|S| \ge \mathsf{D}(G)$ has $0 \in \Sigma(S)$. A basic argument shows $\mathsf{D}(G) \le |G|$ (see [9, Propositions 5.1.4]).

We need the following result (see [9, Theorem 5.2.10; Lemma 5.2.9] and also [14, Lemma 2.1]). Proposition 2.1(ii) is a simple consequence of the pigeonhole principle, and we will only use Proposition 2.1(i) in the trivial case $|B| = k = 2$.

**Proposition 2.1.** *Let $G$ be an abelian group with $A, B \subseteq G$ finite and nonempty:*
*(i) if $|A + B| \le |A| + |B| - k$, then $r_{A,B}(x) \ge k$ for all $x \in A + B$;*
*(ii) if $G$ is finite and $|A| + |B| \ge |G| + k$, then $r_{A,B}(x) \ge k$ for all $x \in G$.*

Next, we state a special case of the Devos-Goddyn-Mohar Theorem [4].

**Theorem 2.2.** *Let $G$ be an abelian group, let $S \in \mathcal{F}(G)$ be a sequence, and let $n \in \mathbb{Z}^+$ with $n \le |S|$. If $H = \mathsf{H}(\Sigma_n(S))$, then*

$$|\Sigma_n(S)| \ge \Big( \sum_{g \in G/H} \min\{n, \mathsf{v}_g(\phi_H(S))\} - n + 1 \Big)|H|. \tag{1}$$

A particular case of the (general) Devos-Goddyn-Mohar Theorem is the much simpler Cauchy-Davenport Theorem [2] [3] [14] [16].

**Cauchy-Davenport Theorem.** *Let $p$ be prime and let $A_i \subseteq C_p$, for $i = 1, \ldots, n$, be nonempty. Then*

$$\Big|\sum_{i=1}^{n} A_i\Big| \ge \min\Big\{\sum_{i=1}^{n} |A_i| - n + 1,\ p\Big\}.$$

## 3. When the Length of a Zero-Sum is Unique

We begin with the following simple lemma.

**Lemma 3.1.** *Let $G$ be an abelian group, let $g \in G$, and let $R \in \mathcal{F}(G)$ be nontrivial with*

$$\Sigma(R) \subseteq \{g, 2g, \ldots, |R|g\}. \tag{2}$$

*If $|R| \le \mathrm{ord}(g) - 1$ and $\sigma(R) = |R|g$, then $R = g^{|R|}$.*

*Proof.* The result is clear when $|R| \le 2$, so we may assume $|R| \ge 3$. In view of (2) and $|R| \le \mathrm{ord}(g) - 1$, we have $0 \notin \Sigma(R)$. Suppose to the contrary that there is

$$h \in \mathrm{supp}(R) \subseteq \Sigma(R) \subseteq \{g, 2g, \ldots, |R|g\} \tag{3}$$

with $h \neq g$. Note, since $|R| \le \mathrm{ord}(g) - 1$, that (3) shows $h \neq 0$ as well. From $0 \notin \Sigma(R)$ and (2) (note if $R'|Rh^{-1}$ with $\sigma(R') = \sigma(R)$, then $\sigma(RR'^{-1}) = 0$), we have

$$\Sigma(Rh^{-1}) \subseteq (\{g, 2g, \ldots, |R|g\} \setminus \{\sigma(R)\}) \cap (\{g, 2g, \ldots, |R|g\} - h).$$

Consequently, $h \notin \{g, 0\}$, $0 \notin \{g, 2g, \ldots, |R|g\}$ and $\sigma(R) = |R|g$ imply that $|\Sigma(Rh^{-1})| < |Rh^{-1}| = |R| - 1$. As a result, $|\Sigma(Rh^{-1}) \cup \{0\}| = |\sum_{i=1}^{|R|-1} \{0, g_i\}| \le |R| - 1$, where $Rh^{-1} = g_1 \cdots g_{|R|-1}$ with $g_i \in \mathrm{supp}(R) \subseteq \Sigma(R) \subseteq G \setminus \{0\}$. Hence Proposition 2.1(i) (applied to the partial sums $\sum_{i=1}^{j-1} \{0, g_i\} + \{0, g_j\}$) implies every element of $\sum_{i=1}^{|R|-1} \{0, g_i\}$ has at least two representations, contradicting that $0 \notin \Sigma(R)$. □

The next two lemmas will help with the detailed characterization of $S$.

**Lemma 3.2.** *Let $g, h \in C_n$ and let $S \in \mathcal{F}(C_n)$ with $S = g^l h^{n-l}$ and $l \ge n - l \ge 1$. Suppose $g$ is a generator and*

$$\Sigma(h^{n-l}) = \{g, 2g, \ldots, (n - l - 1)g\} \cup \{b_0\}, \tag{4}$$

*for some $b_0 \in C_n$. If there is a unique $r \in [1, n]$ such that $0 \in \Sigma_r(S)$, then either $S = g^{n-1}h$ or else $n$ is odd, $h = \frac{n+1}{2}g$ and $S = g^{n-2}h^2$.*

*Proof.* The cases $n - l \le 2$ and $l \le 1$ are easily verified, so we may assume $3 \le n - l \le n - 2$ and thus $h \neq \pm g$ (else either there are two disjoint zero-sums of length 2 or $S = g^{n-1}h = g^n$). Now (4) implies

$$\Sigma(h^{n-l}) = \{h, 2h, \ldots, (n - l)h\} = \{g, 2g, \ldots, (n - l - 1)g\} \cup \{b_0\},$$

for some $b_0 \in C_n$. Thus $\{h, 2h, \ldots, (n - l)h\}$ contains an arithmetic progression of difference $g \neq \pm h$ and length $n - l - 1 \ge 2$. Consequently, $h$ must also be a generator. Hence, if $n - l \ge 4$, then it is easily seen, in view of the hypothesis $n - l \le \frac{n}{2}$, that $\{h, 2h, \ldots, (n - l)h\}$ cannot contain an arithmetic progression of length $n - l - 1$ and difference $g \neq \pm h$. On the other hand,

if $n-l=3$, then this could only be possible if $g=\pm 2h$, and this final case can be eliminated by individual consideration, completing the proof. □

**Lemma 3.3.** *Let $G$ be an abelian group of order $n$ even, let $g, h \in G$ with $\mathrm{ord}(g)=\frac{n}{2}$ and $h \neq g$, and let $S \in \mathcal{F}(G)$ with $S=g^l h^{n-l}$, $n-l \geq 2$ and $l \geq \frac{n}{2}$. If $\frac{n}{2} \in [1,n]$ is the unique integer $r$ such that $0 \in \Sigma_r(S)$, then $n-l$ is odd, $h \notin \langle g \rangle$ and $2h=2g$.*

*Proof.* Since $h \neq g$, $l \geq \frac{n}{2}$ and $\mathrm{ord}(g)=\frac{n}{2} \in [1,n]$ is the unique integer $r$ such that $0 \in \Sigma_r(S)$, we conclude that $h \notin \langle g \rangle$. However, noting that $2h \in \langle g \rangle$ (since $\langle g \rangle$ has index 2), we likewise see that we must have $2h=2g$ (in view of $n-l \geq 2$), else the uniqueness of $\frac{n}{2}=\mathrm{ord}(g)$ is again contradicted. Consequently, the sum of any $\frac{n}{2}$-terms of $S$ using an even number of terms from $h^{n-l}$ has sum zero. As a result, if $n-l$ is even, then there are two disjoint zero-sum subsequences of length $\frac{n}{2}$, contradicting the uniqueness of $\frac{n}{2}$, and completing the proof. □

Next, we state and prove the main result. In the remark that follows the proof of Theorem 3.4, we explain how the proof can be simplified in the case $G=C_p$ with $p$ prime, including the use of the Cauchy-Davenport Theorem in place of Devos-Goddyn-Mohar. Also, though we state the theorem for an arbitrary finite abelian group, most non-cyclic cases have no sequences satisfying the hypotheses (since $2\mathsf{D}(G) \leq |G|$ holds for most non-cyclic groups [9, Theorem 5.5.5].) The proof is divided into four main sections labeled steps.

**Theorem 3.4.** *Let $G$ be a finite abelian group of order $n$ and let $S \in \mathcal{F}(G)$ with $|S|=n$. Suppose there is a unique $r \in [1,n]$ such that $0 \in \Sigma_r(S)$. Then $|\mathrm{supp}(S)| \leq 2$.*

*If $G$ is non-cyclic, then $G=\langle h \rangle \oplus \langle g \rangle \cong C_2 \oplus C_{2m}$, $r=\frac{n}{2}=2m$ and*

$$S=g^{n-1}g' \quad \text{or} \quad S=g^{n/2+x}(h+g)^{n/2-x} \quad \text{or} \quad S=g^{n/2+x}(h+\frac{n+4}{4}g)^{n/2-x},$$

*where $g \in G$, $h, g' \in G \setminus \langle g \rangle$, $\mathrm{ord}(g)=\frac{n}{2}$, $\mathrm{ord}(h)=2$ and $x \in [1, \frac{n}{2}-1]$ is odd.*

*If $G$ is cyclic, then there exists a generator $g \in G \cong C_n$ such that either*

$$S=g^{n-1}g' \quad \text{or} \quad S=(2g)^{n-1}g'',$$

*for some $g' \in G$ or $g'' \in G \setminus \langle 2g \rangle$; or $n$ is odd, $r=\frac{n+1}{2}$ and*

$$S=g^{n-2}(\frac{n+1}{2}g)^2;$$

*or $n \equiv 2 \mod 4$, $r=\frac{n}{2}$ and*

$$S=(2g)^{n/2+x}(\frac{n+4}{2}g)^{n/2-x},$$

*where $x \in [0, \frac{n}{2}-1]$ is even; or $n$ is even, $r=\frac{n}{2}$ and*

$$S=g^{n/2+x}(\frac{n+2}{2}g)^{n/2-x},$$

*where $x \in [0, \frac{n}{2}-1]$ with $\frac{n}{2}-x$ odd.*

*Proof.* Recalling the well-known fact that a zero-sum free subsequence of length $|G|-1$ must be of the form $g^{|G|-1}$ for a generator $g \in G$ (this can be proved in a few lines using the trivial case $|B| = k = 2$ in Proposition 2.1(i); see also [9, Lemma 5.4.2] for a slightly more involved proof), we see that the cases $r = 1$ and $r = n$ are trivial. Therefore we assume $1 < r < n$, whence $0 \notin \text{supp}(S)$. Observe that

$$0 \notin \Sigma_{\le r-1}(S) = \Sigma_{r-1}(0^{r-2}S), \tag{5}$$

$$0 \notin \Sigma_{\ge r+1}(S) = \Sigma_n(0^{n-r-1}S) = \sigma(S) - \Sigma_{n-r-1}(0^{n-r-1}S), \tag{6}$$

where we have used for (6) the fact that $\Sigma_m(T) = \sigma(T) - \Sigma_{|T|-m}(T)$ for $T \in \mathcal{F}(G)$, which follows in view of the correspondence between $R|T$ and $TR^{-1}|T$.

**Step 1.** Let $g \in \text{supp}(S)$ be a term with $\mathsf{v}_g(S) = l := \mathsf{h}(S)$. We first show that either

$$\mathsf{h}(S) \ge \max\{r, n-r+1\}, \text{ or} \tag{7}$$

$$\mathsf{h}(S) \ge \max\{r, n-r\} \quad \text{and} \quad S = g^{n/2}g'^{n/2} \text{ with } \text{ord}(g) = \text{ord}(g') = n \text{ even}, \tag{8}$$

where $g' \in G$. We do so in two cases. First suppose

$$n - r - 1 \ge \frac{n}{2} - 1, \tag{9}$$

in which case $n-r+1 > r$. Note that if there are distinct $g$, $g' \in \text{supp}(S)$ each with multiplicity at least $n-r$, then (9) implies $n$ is even with $S = g^{n/2}g'^{n/2}$ and $r = \frac{n}{2}$. If $\text{ord}(g) = \text{ord}(g') = n$, then (8) holds, as desired. On the other hand, if (say) $\text{ord}(g) \le \frac{n}{2}$, then $\text{ord}(g) = r = \frac{n}{2}$, in which case the proof is easily concluded using Lemma 3.3. Therefore we may assume there is at most one term with multiplicity at least $n-r$.

We apply Theorem 2.2 to $\Sigma_{n-r-1}(0^{n-r-1}S)$. Let $H = \mathsf{H}(\Sigma_{n-r-1}(0^{n-r-1}S))$. Now assuming $\mathsf{h}(S) \le n-r$, it follows, in view of (1) and (6), and since there is at most one term of multiplicity $n-r$, that $H$ is a proper, nontrivial subgroup. Moreover, in view of

$$\mathsf{v}_0(0^{n-r-1}S) = n - r - 1 \ge \frac{n}{2} - 1 \ge |G/H| - 1,$$

which follows from (9), we see that (1) implies that all but at most $|G/H| - 2$ terms of $S$ are from $H$. Letting $T|S$ be the subsequence of all terms not from $H$, we see that $\sigma(S) \in \sigma(T) + H$. Thus, since $|T| \le |G/H| - 2 \le \frac{n}{2} - 1 \le n - r - 1$ (by (9)), it follows, in view of the definition of $H$, that $\sigma(S) \in \Sigma_{n-r-1}(0^{n-r-1}S)$, in contradiction to (6). Therefore we may instead assume (9) fails, i.e,

$$r - 1 > \frac{n}{2} - 1. \tag{10}$$

In this case, we apply the Theorem 2.2 to $\Sigma_{r-1}(0^{r-2}S)$. However, assuming $\mathsf{h}(S) \le r-1$ and repeating the above arguments using (5) instead of (6) and using (10) instead of (9), we arrive at the same contradiction. Therefore we conclude that $\mathsf{h}(S) \ge r > \frac{n}{2} > n - r$, as claimed. Thus (7) is established in both cases.

Factor $S = g^l T$, where $T \in \mathcal{F}(G)$, and let $R|T$ be a maximal length subsequence (possibly trivial) such that $\sigma(R) = |R|g$. In view of (7), (8) and (5), it follows that

$$\mathsf{v}_g(S) = l = \mathsf{h}(S) \geq \max\{r,\, n-r\} \geq \frac{n}{2} \geq |T| \tag{11}$$

and $0 \notin \Sigma(T)$; in particular, $0 \notin \Sigma(R)$.

**Step 2.** Suppose $\mathrm{ord}(g) < n$. Then it follows in view of (11) that $r = \mathrm{ord}(g)$ and that $g$ is the only element from $H := \langle g \rangle$ in $\mathrm{supp}(S)$ (else we can find a zero-sum of length distinct from $r$). Iteratively applying the definition of $\mathsf{D}(G/H) \leq |G/H|$ to $\phi_H(U^{-1}Sg^{-\mathrm{ord}(g)})$, beginning with $U$ trivial, we find a zero-sum mod $H$ subsequence $U|Sg^{-\mathrm{ord}(g)}$ with $|U| \geq n - |H| - |G/H| + 1$. Adding on an appropriate number of terms from $g^{\mathrm{ord}(g)}$ (note $\Sigma(g^{\mathrm{ord}(g)}) = H$) yields a zero-sum subsequence $U'|S$ with $|U'| \geq n - |H| - |G/H| + 2$. If $|H| < \frac{n}{2}$, then $|U'| > |H| = r$, a contradiction. On the otherhand, if $|H| = \frac{n}{2}$, then we obtain the same contradiction unless $|U| = \frac{n}{2} - 1$, $\sigma(U) = -g$ and $SU^{-1}g^{-n/2} = g_0 \notin H$. Thus, if there is some $g_0' \in \mathrm{supp}(T) \setminus H$ with $g_0' \neq g_0$, then swapping $g_0$ for $g_0'$ in $U$ yields a new $U|Sg^{-\mathrm{ord}(g)}$ with $\sigma(U) \in H$ and $|U| = \frac{n}{2} - 1$ but $\sigma(U) \neq -g$, whence we obtain the contradiction as before. Therefore, we instead see that all terms outside $H$ in $\mathrm{supp}(S)$ are equal to $g_0$. However, since all terms inside $H$ in $\mathrm{supp}(S)$ are equal to $g$, this shows $|\mathrm{supp}(S)| \leq 2$. But now the proof is easily concluded using Lemma 3.3. So we henceforth assume $\mathrm{ord}(g) = n$, in which case $G \cong C_n$ is cyclic.

Since

$$|R| \leq |T| \leq r \leq l \leq n - 2 = \mathrm{ord}(g) - 2$$

(the last inequality holds else the proof is complete, while the other inequalities follow from (11)), and since $\sigma(R) = |R|g$, it follows that

$$0 \notin \{g, 2g, \ldots, rg\} \quad \subseteq \quad \Sigma(g^l), \tag{12}$$

$$0 \notin \{(r+1)g, (r+2)g, \ldots, (l+|R|)g\} \quad \subseteq \quad \Sigma_{\geq r+1}(g^l R). \tag{13}$$

Hence $l + |R| \leq \mathrm{ord}(g) - 1 = n - 1$ and

$$|R| < |T| = n - l \leq r.$$

**Step 3.** Next, we show that, when $R$ is nontrivial, there is some

$$h \in \Sigma_{\geq r+1}(g^l R) \setminus \{g, 2g, \ldots, (l+|R|)g\}. \tag{14}$$

Thus assume for the moment that $R$ is nontrivial. Then, in view of Lemma 3.1 and $0 \notin \Sigma(R)$, there is some nontrivial $R_0|R$ with $\sigma(R_0) \notin \{0, g, \ldots, |R|g\}$. Note $\sigma(R_0) \neq |R|g = \sigma(R)$ implies $|R_0| < |R| < |T| \leq r$; thus $1 \leq |R_0| \leq r - 2$. If $\sigma(R_0) \in \{-g, -2g, \ldots, -(r - |R_0| - 1)g\}$, then $0 \in \Sigma_{\leq r-1}(g^l R_0)$, contrary to hypothesis. Therefore

$$\sigma(R_0) \in \{(|R|+1)g, (|R|+2)g, \ldots, (n - r + |R_0|)g\},$$

whence $l+|R| \le \mathrm{ord}(g)-1 = n-1$ and $g^l|S$ with $l \ge r \ge r-|R_0|+1 \ge 0$ show that either $\sigma(R_0) = (n-r+|R_0|)g = (|R_0|-r)g$ or else (14) holds, as desired. However, in the former case, factor $R = R_0R_1$ and note that $\sigma(R_1) = \sigma(R) - \sigma(R_0) = (|R_1|+r)g$. Now

$$|R| < |T| < |R_1| + r \le |T| - 1 + r \le n-1,$$

where the last inequality follows from $|T| = n-l$ with $l \ge r$, whence $\sigma(R_1) \notin \{0, g, \ldots, |R|g\}$ (in view of $\mathrm{ord}(g) = n$) and so $|R_1| < |R| < |T| \le r$. Thus $1 \le |R_1| \le r-2$, and applying the above arguments with $R_1$ instead of $R_0$, we establish (14) unless $(|R_1|+r)g = \sigma(R_1) = (|R_1|-r)g$. However, the latter case implies $2rg = 0$, whence $r = \frac{n}{2}$ with $n$ even.

Furthermore, by the above work for $R_0$ and $R_1$, we see that (14) is established unless

$$\sigma(R') \in \{g, 2g, \ldots, |R|g\} \cup \{(|R'| - \frac{n}{2})g\} \tag{15}$$

for all nontrivial $R'|R$. Applying (15) to each $x \in \mathrm{supp}(R)$, noting that $g \notin \mathrm{supp}(R)$ (in view of $R|T$), and recalling that $|R| < |T| \le r = \frac{n}{2}$, we conclude that

$$\mathrm{supp}(R) \subseteq \{2g, 3g, \ldots, (\frac{n}{2}-1)g\} \cup \{(\frac{n}{2}+1)g\}.$$

If there are $(\frac{n}{2}+1)g$, $x \in \mathrm{supp}(R)$ with $x \in \{2g, 3g, \ldots, (\frac{n}{2}-1)g\}$, then applying (15) to the sequence $x((\frac{n}{2}+1)g)$ yields a contradiction. Therefore we conclude that either

$$\mathrm{supp}(R) = \{(\frac{n}{2}+1)g\} \quad \text{or} \quad \mathrm{supp}(R) \subseteq \{2g, 3g, \ldots, (\frac{n}{2}-1)g\}. \tag{16}$$

Noting that $\frac{n}{2}g = rg = -rg$ and $\sigma(R_1) = (|R_1|+r)g$, we see that

$$\{(|R_1|+r+1)g, (|R_1|+r+2)g, \ldots, (n-2)g\} \subseteq \sigma(R_1) + \Sigma_{\le r-|R_1|-2}(g^l) \subseteq \Sigma_{\le r-2}(g^lR_1).$$

Thus, since $|R_1|+r+1 \le |R|+l+1$, and in view of (13) and $\mathrm{ord}(g) = n$, we have

$$G \setminus \{-g, (r-1)g\} \subseteq \Sigma_{\le r-2}(g^lR) \cup \Sigma_{\ge r}(g^lR).$$

As a result (recall $|R| < |T|$),

$$\mathrm{supp}(TR^{-1}) = \{-(r-1)g\} = \{(\frac{n}{2}+1)g\}, \tag{17}$$

$$(r-1)g \notin \Sigma_{\le r-2}(g^lR) \cup \Sigma_{\ge r}(g^lR), \tag{18}$$

else we find a zero-sum of length distinct from $r$ using precisely one term from $TR^{-1}$ (recall $g \notin \mathrm{supp}(T)$ in view of the definition of $T$), contrary to hypothesis.

By (16) and (17), we discover that $\mathrm{supp}(R) \subseteq \{2g, 3g, \ldots, (\frac{n}{2}-1)g\}$, else $\mathrm{supp}(S) = \{g, \frac{n+2}{2}g\}$ with $r = \frac{n}{2}$, from which the remainder of the proof is easily deduced. Thus, since $r = \frac{n}{2}$ and $R$ is nontrivial, we see that $r \ge 3$ and $(tg)g^{r-1-t}|g^lR$ for some $t \in [2, r-1]$. However $\sigma((tg)g^{r-1-t}) = (r-1)g$ with $|(tg)g^{r-1-t}| = r-t \in [1, r-2]$, contradicting (18). So we see that (14) is finally established.

**Step 4.** Let $A := \{g, 2g, \dots, (l+|R|), h\}$ if $R$ is nontrivial, and otherwise let $A := \{g, 2g, \dots, lg\}$. Let $TR^{-1} = g_1 \cdots g_{n-|R|-l}$, where $g_i \in G$. Recall $|R| < |T|$, so $TR^{-1}$ is nontrivial. Let $T_i := g_1 \cdots g_i$, for $i = 0, 1, \dots, n - |R| - l$. Now $B := \{\sigma(T_0), \sigma(T_1), \sigma(T_2), \dots, \sigma(T_{n-|R|-l})\}$ is a set of cardinality $n - l - |R| + 1$ by the following reasoning: if $\sigma(T_i) = \sigma(T_j)$ with $i < j$, then $\sigma(T_j T_i^{-1}) = 0$, which contradicts $0 \notin \Sigma(T)$. Note that $A + B = G$ in view of Proposition 2.1(ii); moreover, if $|R| > 0$, then every element has at least two representations.

Suppose $0 \in (A + \sigma(T_i)) \cap (A + \sigma(T_j))$ for some $i < j$, i.e., 0 has at least two representations, say $0 = x_i g + \sigma(T_i)$ and $0 = x_j g + \sigma(T_j)$, as a sum in $A + B$, where $x_i$, $x_j \in [1, n]$. Consequently, since (from (13))

$$\{(r+1)g, (r+2)g, \dots, (l+|R|)\} \subseteq \Sigma_{\ge r+1}(g^l R),$$

and since $h \in \Sigma_{\ge r+1}(g^l R)$ if $R$ is nontrivial (from (14)), we see from the definition of $A$ that $x_i$, $x_j \in [1, r]$, else $0 \in \Sigma_{\ge r+1}(S)$, contrary to hypothesis. Thus $g^{x_i} T_i | S$ and $g^{x_j} T_j | S$ are zero-sum subsequences, and so our hypothesis of all zero-sums having length $r$ implies $\sigma(T_i) = (|T_i| - r)g$ and $\sigma(T_j) = (|T_j| - r)g$, whence $\sigma(T_j T_i^{-1}) = |T_j T_i^{-1}|g$. But now $R T_j T_i^{-1}$ contradicts the maximality of $R$. Therefore we may instead assume 0 has a unique representation in $A + B$, in which case $R$ is trivial, as remarked in the previous paragraph.

However, in this case $A = \{g, 2g, \dots, lg\}$ is an arithmetic progression with difference $g$ such that $0 \in A + B = G$ is a unique expression element. Hence it follows that

$$|B \cap \{-lg, -(l-1)g, \dots, -g\}| = 1.$$

Let $b_0 \in B \cap \{-l, -(l-1)g, \dots, -g\}$, so that (in view of $|B| = |G| - |A| + 1 = n - l + 1$)

$$B = \{0, g, 2g, \dots, (n-l-1)g\} \cup \{b_0\}. \tag{19}$$

Observe, in view of (19) and Lemma 3.2, that it now suffices to show $|\mathrm{supp}(S)| \le 2$ to complete the proof. Let $T_k$ be the subsequence such that $\sigma(T_k) = b_0$.

Note that if we swap the index between $g_i$ and $g_{i+1}$, for $i \in [1, k-1]$, and use this ordering to define a new $B$, let us call it $B'$, as above, then $b_0 \in B'$ and only one element of $B'$ differs from $B$, namely that corresponding to $\sigma(T_i)$. However, applying the above argument using $B'$ instead of $B$, we see that we again contradict the maximality of $R$ unless $B = B'$ (in view of $b_0 \in B'$). As $B = B'$ if and only if $g_i = g_{i+1}$, we conclude that $g_1 = g_2 = \ldots = g_k$. Likewise, swapping the index between $g_i$ and $g_{i+1}$, for $i \in [k+1, n-l-1]$, and proceeding as we did for $i \in [1, k-1]$ allows us to conclude $g_{k+1} = g_{k+2} = \ldots = g_{n-l}$. Let $g_1 = ag$ and $g_{n-l} = bg$, with $a$, $b \in [2, n-1]$ (since 0, $g \notin \mathrm{supp}(T)$). If $|T| \ge 3$, then we can find an ordering of the $g_i$ such that $g_1 = g_{n-l}$. Then using this ordering to define $B$ and repeating the above arguments, we either contradict the maximality of $R$ or show $|\mathrm{supp}(S)| = 2$, in which case the proof is complete as remarked before. So it only remains to consider the case $|T| = 2$, as the proof is trivially complete when $|T| = 1$. But in this case, $l = n-2$ and $a$, $b \in [2, n-1]$ imply that $g^{n-a}(ag) | S$ and $g^{n-b}(bg) | S$ are both zero-sum subsequences of respective lengths $n-a+1$ and $n-b+1$, whence

the uniqueness of $r$ as a zero-sum length implies $a = b$. Thus $\mathrm{supp}(S) = \{g, ag\}$, completing the proof as remarked before. □

**Remark.** When $G = C_n$ with $n$ prime, the above proof can be simplified. First remark that $\mathrm{ord}(g) = n$ holds trivially for $|G| = p$ prime, so Step 2 is unnecessary. Next, noting that the case $n = 2$ is trivial, we can assume $n \geq 3$, and thus that $n$ is odd. This eliminates the lengthy extra portion of Step 3 needed to establish (14) when $r = \frac{n}{2}$ with $n$ even. Also, the following argument, using the Cauchy-Davenport Theorem instead of the Devos-Goddyn-Mohar Theorem, can be used to establish (7).

To show (7), we proceed in the same two cases. First suppose

$$n - r - 1 \geq \frac{n}{2} - 1, \tag{20}$$

in which case $n - r + 1 > r$. Note that if there are two distinct $g$, $g' \in \mathrm{supp}(S)$ with multiplicity at least $n - r$, then this contradicts (20) in view of $n$ odd, whence we may assume otherwise. Thus, assuming $\mathsf{h}(S) \leq n - r$, it is easily seen that we can find $n - r - 1$ nonempty sets $A_1, \ldots, A_{n-r-1} \subseteq G$ such that $\prod_{i=1}^{n-r-1} \prod_{g \in A_i} g = 0^{n-r-1} S x^{-1} \in \mathcal{F}(G)$, for some $x \in \mathrm{supp}(S)$ (see [1, Proposition 2.1]). Applying the Cauchy-Davenport Theorem to $A_1, \ldots, A_{n-r-1}$, we find that $\Sigma_{n-r-1}(0^{n-r-1} S x^{-1}) = G$, whence $\Sigma_{n-r-1}(0^{n-r-1} S) = G$, contradicting (6). Therefore we may instead assume (20) fails, i.e,

$$r > \frac{n}{2}. \tag{21}$$

In this case, assuming $\mathsf{h}(S) \leq r - 1$, we can (as before) find $r - 1$ nonempty sets $A_1, \ldots, A_{r-1} \subseteq G$ such that $\prod_{i=1}^{r-1} \prod_{g \in A_i} g = 0^{r-2} S \in \mathcal{F}(G)$. Applying the Cauchy-Davenport Theorem to $A_1, \ldots, A_{r-1}$, we find that $\Sigma_{r-1}(0^{r-2} S) = G$, contradicting (5). Therefore we conclude, in view of (21), that $\mathsf{h}(S) \geq r > \frac{n}{2} > n - r$, as claimed. Thus (7) is established in both cases.

## References


[1] A. Bialostocki, P. Dierker, D. J. Grynkiewicz, and M. Lotspeich, On Some Developments of the Erdős-Ginzburg-Ziv Theorem II, *Acta Arith.*, 110 (2003), no. 2, 173–184.

[2] A. L. Cauchy, Recherches sur les nombres, *J. École polytech.*, 9 (1813), 99–116.

[3] H. Davenport, On the addition of residue classes, *J. London Math. Society*, 10 (1935), 30–32.

[4] M. DeVos, L. Goddyn and B. Mohar, A Generalization of Kneser' s Addition Theorem, *Adv. Math.*, 220 (2009), 1531–1548.

[5] P. Erdős and R. L. Graham, Old and new problems and results in combinatorial number theory, *Monographies de L'Enseignement Mathmatique [Monographs of L'Enseignement Mathmatique]*, 28, Université de Genève, L'Enseignement Mathématique, Geneva, 1980, pp. 95.

[6] P. Erdős and E. Szemerédi, On a problem of Graham, *Publ. Math. Debrecen*, 23 (1976), no. 1-2, 123–127.

[7] W. Gao and A. Geroldinger, Zero-sum problems in finite abelian groups: A survey, *Expositiones Mathematicae*, 24 (2006), no. 4, 337–369.

[8] W. Gao, Y. O. Hamidoune and G. Wang, Distinct Lengths Modular Zero-sum Subsequences: A Proof of Graham's Conjecture, preprint (2009).

[9] A. Geroldinger and F. Halter-Koch, *Non-unique factorizations: Algebraic, combinatorial and analytic theory.* Pure and Applied Mathematics (Boca Raton), 278. Chapman & Hall/CRC, Boca Raton, FL, 2006.

[10] A. Geroldinger, Additive group theory and non-unique factorizations, *Combinatorial Number Theory and Additive Group Theory*, Advanced Courses in Mathematics, eds. A. Geroldinger and I. Ruzsa, Birkhäuser, CRM Barcelona, 2009, 1–89.

[11] D. J. Grynkiewicz, On a Partition Analog of the Cauchy-Davenport Theorem, *Acta Math. Hungar.*, 107 (2005), no. 1–2, 161–174.

[12] D. J. Grynkiewicz, On a conjecture of Hamidoune for subsequence sums, *Integers*, 5 (2005), no. 2, A7 (electronic).

[13] D. J. Grynkiewicz, L. E. Marchan and O. Ordaz, Representation of finite abelian group elements by subsequence sums, to appear in *J. Théor. Nombres Bordeaux*.

[14] M. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Graduate Texts in Mathematics 165, Springer-Verlag, New York, 1996.

[15] S. Savchev and F. Chen, Long zero-free sequences in finite cyclic groups, *Discrete Math.*, 307 (2007), 2671–2679.

[16] T. Tao and V. Vu, *Additive Combinatorics*, Cambridge Studies in Advanced Mathematics 105, Cambridge University Press, Cambridge, 2006.

Institut für Mathematik und Wissenschaftliches Rechnen, Karl-Franzens-Universität Graz, Heinrichstrasse 36, 8010 Graz, Austria

*E-mail address*: diambri@hotmail.com