ON ERDÖS-GINZBURG-ZIV INVERSE THEOREMS

D. J. GRYNKIEWICZ 1, O. ORDAZ 2, M. T. VARELA 3, AND F. VILLARROEL 4

Abstract. Let $G$ be an abelian group of order $m \geq 2$, let $p$ be the smallest prime divisor of $m$, and let $q$ be the smallest prime divisor of $\frac{m}{p}$ (if $m$ is composite). For a sequence $S$, let $\Sigma_n(S)$ be the set of all elements that can be represented as the sum of terms from some $n$-term subsequence of $S$, and let $\Sigma(S)$ be the set of all elements that can be represented as the sum of terms from some nonempty subsequence of $S$. We prove the following two results.

- Let $S$ be a sequence in $G \setminus \{0\}$ of length at least $m + t \geq m$ with the multiplicity of each element in $S$ at most $h$. If $h + t \geq \frac{m}{p} - 1$, or $\Sigma(S) \neq G$ and $m = pq$, or $\Sigma(S) \neq G$ and $h + t \geq \frac{m}{pq} + q - 3$, then $\bigcup_{n=t+1}^{h+t} \Sigma_n(S) = \Sigma(S)$ and $\Sigma(S)$ is periodic.

- Let $S$ be a sequence in $G$ of length $m + k \geq m + \frac{m}{p} - 1$. If either $0 \notin \Sigma_m(S)$ or $\Sigma_m(S)$ is aperiodic, then there exists an element in $S$ with multiplicity at least $k + 1$.

This confirms and generalizes two conjectures of Gao, Thangadurai and Zhuang.

Key words: abelian group, Erdős-Ginzburg-Ziv theorem, zero-sum sequence. MSC: 11B75.

1. Introduction

Let $\mathcal{F}(G)$ denote the free abelian monoid over the set $G$ with monoid operation written multiplicatively and given by concatenation, i.e., $\mathcal{F}(G)$ consists of all finite subsequences over $G$ under the equivalence relation given by allowing terms to be permuted. Despite possible confusion, the elements of $\mathcal{F}(G)$ will be referred to simply as sequences, and if indeed order or infiniteness were needed in a sequence, it would be explicitly stated when the sequence was first introduced.

Now let $G$ be an abelian group of order $m \geq 2$. The Erdős-Ginzburg-Ziv theorem established that every sequence in $G$ of length $2m - 1$ contains an $m$-term subsequence with zero-sum [6]. There have been many related inverse theorems describing the structure of the sequences $S$ in $G$ with length $|S| = m + k$, $1 \leq k \leq m - 2$, not having any $m$-term subsequence with zero-sum. For cyclic groups of order $m$, the structure of $S$ has been described by several authors: when $k = m - 2$, by Yuster and Peterson in [15], and by Bialostocki and
Dierker in [1]; when \( k = m - 3 \), by Flores and Ordaz in [5]; when \( m - \left\lfloor \frac{m}{2} \right\rfloor - 2 \leq k \leq m - 2 \), by Bialostocki, Dierker, Grynkiewicz, and Lotspeich in [2] (using a related result of Gao from [8]); and when \( k \geq \left\lceil \frac{m-1}{2} \right\rceil \), by Chen in [3].

1.1. **Terminology.** For \( S \in \mathcal{F}(G) \), we let \(|S|\) be the length of \( S \), and employ standard multiplicative monoid notation; in particular, \( ST \) denotes the concatenation of \( S \) and \( T \), and \( S'|S \) denotes that \( S' \) is a subsequence of \( S \), in which case \( SS'^{-1} \) denotes the subsequence of \( S \) obtained by deleting all terms from \( S' \). Let \( \sigma(S) \) denote the sum of terms of \( S \), unless \( S \) is the empty sequence, in which case \( \sigma(S) := 0 \). Let

\[
\Sigma_n(S) = \{ \sigma(S') : S'|S \text{ and } |S'| = n \},
\]

let

\[
\Sigma_{\leq t}(S) = \bigcup_{n=1}^{t} \Sigma_n(S) \quad \text{and} \quad \Sigma_{\geq t}(S) = \bigcup_{n=t}^{\lfloor|S|\rfloor} \Sigma_n(S),
\]

and let

\[
\Sigma(S) = \Sigma_{\leq |S|}(S).
\]

For \( x \in G \), let \( \nu_x(S) \) be the multiplicity of \( x \) in \( S \), and let \( h(S) = \max_{x \in G} \nu_x(S) \).

A subset \( A \) of the abelian group \( G \) is periodic if \( A \) is a union of \( H_a \)-cosets for some nontrivial subgroup \( H_a \leq G \). We will often associate the index of \( H_a \) in \( G \) with \( a \). If \( B \) is another subset of \( G \), then the sumset \( A + B \) is the set of all pairwise sums between \( A \) and \( B \), i.e.,

\[
A + B = \{ a + b : a \in A, b \in B \}.
\]

Note we will often associate a singleton set with its element for the purpose of notational simplicity.

A sequence \( S \) is squarefree if \( h(S) \leq 1 \), in which case \( S \) can be considered as a set. An \( n \)-setpartition of a sequence \( S \) is a sequence of \( n \) nonempty, squarefree subsequences, say \( A = A_1, \ldots, A_n \), such that \( S = A_1 \cdots A_n \). Note we do not use multiplicative notation for the terms of a setpartition in order to distinguish the setpartition, \( A_1, \ldots, A_n \), from the sequence it partitions/factorizes, \( A_1 \cdots A_n \).

Finally, the Davenport constant of \( G \), denoted \( D(G) \), is the least integer \( n \) such that every sequence from \( G \) of length \( n \) contains a nonempty subsequence whose terms sum to zero. A simple argument (see [7]) shows that \( D(G) \leq |G| \).
1.2. Results. We have the following open problem:

**Problem 1** ([11, 12]). For an abelian group $G$ of order $m \geq 2$ and positive integer $k$, determine the exact value or bound of

$$h(G, k) = \min \{ h(S) : S \in \mathcal{F}(G) \text{ with } |S| = |G| + k \text{ and } 0 \not\in \Sigma_G(S) \}.$$

There are few results about the exact value or bound of $h(G, k)$. When $G$ is cyclic of order $m$, we have $h(G, k) \geq k + 1$, provided $m - \lfloor \frac{m}{4} \rfloor - 2 \leq k \leq m - 2$, see [8]; $h(G, k) \geq k + 1$, provided $m$ is prime with $1 \leq k \leq m - 2$, see [9]; $h(G, m - 2) = m - 1$, see [1] or [15]; and $h(G, m - 3) = m - 1$, see [5].

The main results in this paper are the confirmations of the following two conjectures.

**Conjecture 1.1** (Conjecture 6.9 [10], [11]). Let $G$ be a cyclic group of order $m \geq 2$, with $p$ the smallest prime divisor of $m$. Let $S \in \mathcal{F}(G \setminus 0)$ with $|S| = m$. If $h = h(S) \geq \frac{m}{p} - 1$, then $\Sigma_{\leq h}(S) = \Sigma(S)$.

Conjecture 1.1 was verified for cyclic groups of prime power order in [11]. The following example shows that we cannot hope, in general, for Conjecture 1.1 to hold for smaller $h$. Indeed, the Conjecture fails for $h \leq \frac{m}{p} - 2$ and composite $m$ when both $\frac{m}{p} \neq 0$ or 1 mod $h$, and, if $p = 2$, $\frac{m}{p} \neq -1$ mod $h$ as well. In particular, the conjecture does not hold when $h = \frac{m}{p} - 2$ for composite $m > 10$.

Let $G = \mathbb{Z}/m\mathbb{Z}$ with $m$ composite, let $p$ be the smallest prime divisor of $m$, and let $H \leq G$ be the subgroup of index $\frac{m}{p}$. Let $h \leq \frac{m}{p} - 2$ be a positive integer such that $\frac{m}{p} \neq 0$ or 1 mod $h$, and, if $p = 2$, such that $\frac{m}{p} \neq -1$ mod $h$ as well. Hence, in particular, $h > 1$. Let $t = \lceil \frac{m+h}{ph} \rceil = \frac{m+h+ph-\alpha}{ph}$, where $0 < \alpha \leq ph$. Thus

$$((t-1)p-1)h < m = ((t-1)p-1)h + \alpha \leq (tp-1)h,$$

whence $1 < h \leq \frac{m}{p} - 2$ implies that $2 \leq t \leq \frac{m}{p}$. Let $A = H \cup 1 + H \cup \ldots \cup (t - 1) + H$, and let $W$ be the subsequence consisting of every element of $A \setminus 0$ with multiplicity $h$. Note, in view of (1) and $2 \leq t \leq \frac{m}{p}$, that $|W| = (tp-1)h \geq m$. Hence let $S$ be a subsequence of $W$ such that $|S| = m$, and such that $S$ contains some element $y \in (t - 1) + H$ with multiplicity $\min \{ \alpha, h \}$, as well as all $(t - 1)p - 1$ elements from $H \setminus 0 \cup 1 + H \cup \ldots \cup (t - 2) + H$, each with multiplicity $h$, which is possible since $m = ((t - 1)p - 1)h + \alpha$. Note that $S$ contains
exactly \(\alpha\) elements from \((t-1)+H\). Since \(t \geq 2\), it follows that \(h(S) = h\). Note (1) implies that

\[
(2) \quad \frac{m}{p} = (t-1)h - \frac{h-\alpha}{p}.
\]

Hence \(h - \alpha \equiv 0 \mod p\). We proceed to show, in two cases based on the value of \(\alpha\), that \(\Sigma_{\leq h}(S) \neq \Sigma(S)\), which will show that \(S\) does not satisfy the conclusion of Conjecture 1.1 for \(h \leq \frac{m}{p} - 2\), under the assumed restrictions on \(\frac{m}{p}\) modulo \(h\).

Suppose first that \(\alpha < h\). Thus \(h - \alpha \equiv 0 \mod p\) implies that \(\alpha \leq h - p\). Hence (1) implies that \(\frac{m}{p} \leq (t-1)h - 1\), whence \(h \leq \frac{m}{p} - 2\) implies that \(t \geq 3\). Thus let \(x \in 1 + H\) and \(x' \in (t-2) + H\) be distinct elements. Note

\[
\alpha y + (h - \alpha)x' + x \in \Sigma(S) \cap ((t-2)h + \alpha + 1 + H).
\]

Thus if \((t-2)h + \alpha + 1 < \frac{m}{p}\), then

\[
\alpha y + (h - \alpha)x' + x \notin \Sigma_{\leq h}(S) \subseteq \{0, 1, \ldots, \alpha(t-1) + (h-\alpha)(t-2)\} + H,
\]

whence \(\Sigma(S) \neq \Sigma_{\leq h}(S)\), as desired. Therefore we can instead assume by (2) that

\[
(t-2)h + \alpha + 1 \geq \frac{m}{p} = (t-1)h - \frac{h-\alpha}{p},
\]

whence \(\alpha \leq h - p\) implies that \(p \leq 2\). Thus \(p = 2\) and \(\alpha = h - p = h - 2\) (else the previous arguments will yield \(p < 2\)), whence in view of (2) it follows that \(\frac{m}{p} = (t-1)h - 1\). Consequently, \(\frac{m}{p} \equiv -1 \mod h\) and \(p = 2\), contradicting the conditions assumed on \(h\).

Next suppose that \(\alpha \geq h\). If \(\alpha = h\), then (2) implies that \(\frac{m}{p} \equiv 0 \mod h\), which is not the case. Hence \(\alpha > h\). Since \(t \geq 2\) and since \(\alpha > h\), let \(x \in 1 + H\) with \(x|S\) and \(x \neq y\). Observe that \(hy + x \in \Sigma(S) \cap ((t-1)h + 1 + H)\). Thus if

\[
(3) \quad (t-1)h + 1 < \frac{m}{p},
\]

then \(hy + x \notin \Sigma_{\leq h}(S)\), whence \(\Sigma(S) \neq \Sigma_{\leq h}(S)\), as desired. However, if \(\alpha > h + p\), then (2) implies

\[
(t-1)h + 1 = \frac{m + h - \alpha}{p} + 1 < \frac{m}{p},
\]
whence (3) holds and \( \Sigma(S) \neq \Sigma_{\leq h}(S) \). Therefore we may instead assume \( \alpha \leq h + p \) and that (3) does not hold. Thus (2) and \( \alpha \geq h \) imply that
\[
(t - 1)h \leq \frac{m}{p} \leq (t - 1)h + 1,
\]
whence \( \frac{m}{p} \equiv 0 \) or \( 1 \mod h \), contradicting the conditions assumed on \( h \), and completing the example.

**Conjecture 1.2** (Conjecture 7.6 [10], [11]). Let \( G \) be a cyclic group of order \( m \geq 2 \), with \( p \) the smallest prime divisor of \( m \). Let \( k \) be an integer such that \( k \geq \frac{m}{p} - 1 \), and let \( S \in \mathcal{F}(G) \) with \( |S| = m + k \). If \( 0 \not\in \Sigma_{\leq h}(S) \), then \( h(S) \geq k + 1 \).

Conjecture 1.2 was verified for cyclic groups of prime power order in [11]. The following example shows we cannot hope, in general, for Conjecture 1.2 to be true for smaller \( k \). Indeed, Conjecture 1.2 fails whenever
\[
|W| = tdk \geq m + 2k + 1,
\]
and
\[
|W'| = (t - 1)dk < m - d.
\]
Note that \( \Sigma_{\leq k}(W) \subseteq \{0, 1, \ldots, k(t - 1)\} + H \). Furthermore, in view of (4) it follows that \( k(t - 1) < \frac{m}{d} - 1 \). We proceed to define a subsequence \( S|W \) with \( |S| = m + k \) and \( \sigma(S) \in \{k(t - 1) + 1, k(t - 1) + 2, \ldots, \frac{m}{d} - 1\} + H \), which is disjoint from \( \Sigma_{\leq k}(W) \) and thus also from \( \Sigma_k(S) \). Note such a subsequence will have \( h(S) \leq h(W) \leq k \) and \( \sigma(S) \notin \Sigma_k(S) =
Σ|S|−m(S). Moreover, in view of the basic correspondence \( \sigma(S) - \Sigma|S| - m(S) = \Sigma_m(S) \), the latter conclusion will imply \( 0 \notin \Sigma_m(S) \), as desired. Thus it remains to construct \( S \).

Let \( \sigma(W) \equiv \alpha \mod \frac{m}{d} \) with \( 0 \leq \alpha \leq \frac{m}{d} - 1 \). If \( \alpha \geq k(t - 1) + 1 \), then in view of (5) and (6) it follows that we can find a subsequence \( S|W \) with length \( m + k \) obtained by removing an appropriate number of terms all contained in \( H \); hence \( \sigma(S) + H = \sigma(W) + H = \alpha + H \subseteq \{k(t - 1) + 1, \ldots, \frac{m}{d} - 1\} + H \) and \( |S| = m + k \), yielding a subsequence with the prescribed properties. Therefore we may assume \( \alpha \leq k(t - 1) \). Hence \( \lceil \frac{\alpha + 1}{t - 1} \rceil \leq k + 1 \leq kd \). In this case, we can remove \( \lceil \frac{\alpha + 1}{t - 1} \rceil - 1 \) terms from \( W \) contained in \( (t - 1) + H \), and one appropriately chosen additional term contained in \( 1 + H \cup \ldots \cup (t - 1) + H \), to yield a subsequence \( S'|W \) with \( \sigma(S') \in \frac{m}{d} - 1 + H \). In view of (5) and \( \lceil \frac{\alpha + 1}{t - 1} \rceil \leq k + 1 \), it follows that \( |S'| \geq m + k \). Thus, as in the previous case, we can remove an appropriate number of terms from \( S' \) all contained in \( H \) to yield a subsequence \( S|S' \) with \( |S| = m + k \) and \( \sigma(S) + H = \sigma(S') + H' = \frac{m}{d} - 1 + H \), yielding a subsequence with the desired properties.

Conjecture 1.1 will follow from the case (i) with \( t = 0 \) of the following theorem, which is our first main result.

**Theorem 1.1.** Let \( G \) be an abelian group of order \( m \geq 2 \), let \( p \) be the smallest prime divisor of \( m \), let \( q \) be the smallest prime divisor of \( \frac{m}{p} \) (if \( m \) is composite), let \( S \in \mathcal{F}(G \setminus 0) \), and let \( h \geq h(S) \) and \( t \geq 0 \) be integers. If \( |S| \geq m + t \), then any one of the following conditions implies that \( \Sigma(S) \) is periodic with

\[
\Sigma_{\geq t+1}(S) \cap \Sigma_{\leq h+t}(S) = \Sigma(S)
\]

(i) \( h + t \geq \frac{m}{p} - 1 \), or
(ii) \( \Sigma(S) \neq G \) and \( m = pq \), or
(iii) \( \Sigma(S) \neq G \) and \( h + t \geq \frac{m}{pq} + q - 3 \).

We will then use Theorem 1.1 to derive the following theorem, which provides a mild generalization of Conjecture 1.2.

**Theorem 1.2.** Let \( G \) be an abelian group \( G \) of order \( m \), let \( S \in \mathcal{F}(G) \), and let \( p \) be the smallest prime divisor of \( m \). If \( |S| \geq m + \max\{h(S), \frac{m}{p} - 1\} \), then \( 0 \in \Sigma_m(S) \) and \( \Sigma_m(S) \) is periodic.
Let $G$ be an abelian group of order $m$, and let $p$ be the smallest prime divisor of $m$. From Theorem 1.2 it follows that $h(G, k) \geq k + 1$ for every $G$ with $|G| = m$ and $k \geq \frac{m}{p} - 1$.

1.3. Tools. We will need the following result that gives simple necessary and sufficient conditions for the existence of an $n$-setpartition, and in case of existence, shows that an $n$-setpartition may always be found with constituent cardinalities of as near equal a size as possible [2] [14].

**Proposition 1.3.** Let $n$ be a positive integer. A sequence $S$ has an $n$-setpartition $A = A_1, \ldots, A_n$ if and only if $|S| \geq n$ and $h(S) \leq n$. Furthermore, if $S$ has an $n$-setpartition, then $S$ has an $n$-setpartition $B = B_1, \ldots, B_n$ with $||B_i| - |B_j|| \leq 1$ for all $i$ and $j$.

We will also make use of the following classical lower bound for sumsets in a prime order group [4].

**Cauchy-Davenport Theorem (CDT).** If $A_1, \ldots, A_n \subseteq \mathbb{Z}/p\mathbb{Z}$ are nonempty with $p$ prime, then

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

Finally, we will need the following partition analog of CDT, which will be our main tool for proving Theorem 1.1 [13] [14].

**Theorem 1.4.** Let $G$ be an abelian group of order $m \geq 2$, let $S \in \mathcal{F}(G)$, let $S'|S$, let $P = P_1, \ldots, P_n$ be an $n$-setpartition of $S'$, and let $p$ be the smallest prime divisor of $m$. If $n \geq \min\{\frac{m}{p} - 1, \frac{|S'|-n+1}{p} - 1\}$, then either:

(i) there is an $n$-setpartition $A = A_1, \ldots, A_n$ of a subsequence $S''$ of $S$ with $|S'| = |S''|$, $\sum_{i=1}^{n} P_i \subseteq \sum_{i=1}^{n} A_i$, and

$$\left|\sum_{i=1}^{n} A_i\right| \geq \min\{m, |S'| - n + 1\},$$

(ii) there is a proper, nontrivial subgroup $H_a$ of index $a$, a coset $\alpha + H_a$ such that all but $e$ terms of $S$ are from $\alpha + H_a$, where

$$e \leq \min\{a - 2, \left\lfloor \frac{|S'| - n}{|H_a|} \right\rfloor - 1\},$$
and an \( n \)-setpartition \( B = B_1, \ldots, B_n \) of a subsequence \( S''_0 \in \mathcal{F}(\alpha + H_a) \), with \( S''_0 \mid S \), \( |S''_0| \leq n + |H_a| - 1 \), and \( \sum_{i=1}^{n} B_i = n\alpha + H_a \).

2. Proof of Theorem 1.1

We proceed with the proof of all three parts simultaneously. In what follows, we will often make use of the fact that the function \( f(a) = \frac{M}{a} + a \), for \( M, a > 0 \) \( (\text{and usually } M \text{ will be of the form } m \text{ or } \frac{m}{x}) \), is maximized at a boundary value of \( a \). Thus for example, if \( a | m \), then \( \frac{m}{a} + a \leq \frac{m}{p} + p \). We begin by showing all three cases imply the following claim. Note this completes the case \( |G| \) prime.

**Claim 1.** Either the conclusion of Theorem 1.1 is true, or there exists a proper, nontrivial subgroup \( H_a \) of index \( a \), such that \( \Sigma(S_a) = H_a \), and all but \( e \leq a - 2 \) terms of \( S \) are from \( H_a \), where \( S_a \) is the subsequence of \( S \) consisting of all terms from \( H_a \).

**Proof.** First suppose (i) holds. Observe that \( \Sigma(S_a) = H_a \), and all but \( e \leq a - 2 \) terms of \( S \) are from \( H_a \), where \( S_a \) is the subsequence of \( S \) consisting of all terms from \( H_a \).

Hence \( \Sigma(S) = \Sigma(S_{0^{h-1}}) = \Sigma_{\geq t+1}(S) \cap \Sigma_{\leq h+t}(S) \). Since \( h \geq h(S) \), and since \( |S| \geq m + t \geq t + 1 \), it follows in view of Proposition 1.3 that there exists an \((h + t)\)-setpartition \( P \) of \( S_{0^{h-1}} \). Since \( h + t \geq \frac{m}{p} - 1 \), it follows that we can apply Theorem 1.4 to \( P \). If Theorem 1.4(i) holds, then

\[
|\Sigma_{h+t}(S_{0^{h-1}})| \geq \min\{m, (|S| + h - 1) - (h + t) + 1\} = m = |G|.
\]

Hence \( \Sigma(S) \subseteq G = \Sigma_{h+t}(S_{0^{h-1}}) = \Sigma_{\geq t+1}(S) \cap \Sigma_{\leq h+t}(S) \subseteq \Sigma(S) \) holds trivially. So we may assume that Theorem 1.4(ii) holds instead. Consequently, all but \( e \leq a - 2 \) terms of \( S_{0^{h-1}} \) are from \( \alpha + H_a \), where \( H_a \) is a proper, nontrivial subgroup of index \( a \).

Suppose that \( 0 \not\in \alpha + H_a \). Hence, since there are only \( e \leq a - 2 \) terms of \( S_{0^{h-1}} \) outside \( \alpha + H_a \), it follows that \( h - 1 \leq a - 2 \). Hence, since \( h \geq h(S) \), since \( |S| \geq m + t \), and since \( e \leq a - 2 \), it follows that

\[
m + t + h - 1 \leq |S_{0^{h-1}}| \leq |H_a|h + e \leq \frac{m}{a}h + a - 2 \leq \frac{m}{a}(a - 1) + a - 2.
\]

Thus it follows that \( h + t \leq a - \frac{m}{a} - 1 \leq \frac{m}{p} - 3 \), contradicting (i). So we may assume \( 0 \in \alpha + H_a \), whence w.l.o.g. \( \alpha = 0 \). Furthermore, since Theorem 1.4(ii) holds for \( S_{0^{h-1}} \), it follows that \( \Sigma_{h+t}(S_a0^{h-1}) = H_a \), where \( S_a \) is the subsequence of terms of \( S \) from \( H_a \). Thus, since \( \nu_0(S_a0^{h-1}) = h - 1 < h + t \), and since all terms of \( S_a0^{h-1} \) are from \( H_a \), it follows
that $\Sigma(S_a) = H_a$, yielding the claim. So we may assume either (ii) or (iii) holds, whence $\Sigma(S) \neq G$.

Note $\Sigma_{|S|}(S^{1|S|^{-1}}) = \Sigma(S)$. In view of Proposition 1.3, it follows that $S^{1|S|^{-1}}$ has an $|S|$-setpartition $P$. Since $|S| \geq m + t \geq m$, it follows that we can apply Theorem 1.4 to $P$. If Theorem 1.4(i) holds, then $|\Sigma(S)| = |\Sigma_{|S|}(S^{1|S|^{-1}})| \geq \min\{m, 2|S| - 1 - |S| + 1\} = m$, whence $\Sigma(S) = G$, a contradiction. Therefore we can assume Theorem 1.4(ii) holds. Thus there exists a proper, nontrivial subgroup $H_a$ of index $a$, and $\alpha \in G$, such that all but $e \leq a - 2$ terms of $S^{1|S|^{-1}}$ are from $\alpha + H_a$. Since $\nu_0(S^{1|S|^{-1}}) = |S| - 1 \geq m - 1 > a - 2$, it follows that $0 \in \alpha + H_a$, whence w.l.o.g. $\alpha = 0$. Furthermore, $\Sigma(S_a) = H_a$ holds as before, completing the proof of the claim.

Assume $H_a$ is chosen to satisfy Claim 1 with minimal cardinality. Note $|S_a| = |S| - e \geq m - e$. Since $\Sigma(S_a) = H_a$, it follows that $\Sigma(S) = H_a + \Sigma(0SS_a^{-1})$, whence $\Sigma(S)$ is periodic. Consequently, it suffices to show $\Sigma_{\geq t+1}(S) \cap \Sigma_{\leq h+t}(S) = \Sigma(S)$.

If $h \leq a$, then

$$m \leq |S| \leq (\frac{m}{a} - 1)h + e \leq (\frac{m}{a} - 1)h + a - 2 \leq (\frac{m}{a} - 1)a + a - 2 = m - 2,$$

a contraction. Therefore we can assume $h \geq a + 1$.

Note $|S| \geq m + t \geq \frac{m}{2} + t \geq \frac{m}{a} + a - 2 + t \geq \frac{m}{a} + t + e$. Hence $|S_a| \geq \frac{m}{a} + t$. Thus, since $\Sigma(S_a) = H_a$, it follows by a simple greedy algorithm that there exists a subsequence $R$ of $S_a$ with $|R| = \frac{m}{a}$ and $\Sigma(R) = H_a$. Since $|S_a| \geq \frac{m}{a} + t$, there exists a subsequence $T_a|S_aR^{-1}$ with $|T_a| = t$. Thus every term of $\Sigma(S)$ can be expressed as a sum of all $t$ terms from $T_a$, at most $\frac{m}{a}$ terms of $R$ (and at least one), and at most $e \leq a - 2$ terms outside $H_a$, whence $\Sigma(S) = \Sigma_{\geq t+1}(S) \cap \Sigma_{\leq \frac{m}{a} + t + a - 2}(S)$. Consequently, we may assume

$$h \leq \frac{m}{a} + a - 3,$$

else the proof is complete.

Let $S'_a = S_aT_a^{-1}$. If $|S'_a| \leq h - 1$, then $h - 1 \geq |S_aT_a^{-1}| \geq m - e \geq m - a + 2$. Thus (7) implies that

$$m \leq \frac{m}{a} + 2a - 6 \leq 2 + 2\frac{m}{2} - 6 = m - 4,$$

a contradiction. Therefore we can assume $|S'_a| \geq h$. Hence, since $h(S) \leq h$, it follows in view of Proposition 1.3 that there exists an $h$-setpartition $A = A_1, \ldots, A_h$ of $S'_a$ with
\(|A_i| - |A_j| \leq 1\) for all \(i\) and \(j\). Assume w.l.o.g. that \(|A_1| \geq |A_2| \geq \ldots \geq |A_h|\). Let \(\left\lfloor \frac{m-a+2}{h} \right\rfloor = \frac{m-a+2-\epsilon}{h}\). Hence, since \(|S'_a| = |S| - e - t \geq m - a + 2\), it follows that

\[
|A_i| \geq \frac{m-a+2-\epsilon}{h}
\]

for all \(i\), and that

\[
|A_i| \geq \frac{m-a+2-\epsilon}{h} + 1 > \frac{m-a+2}{h}
\]

for all \(i \leq \epsilon\).

Let \(x\) be the minimal number such that \(\sum_{i=1}^{x} |A_i| \geq \frac{m}{a}\) (since \(|S'_a| = |S_a| - t \geq \frac{m}{a}\), it follows that \(x\) exists). We proceed to show that

\[
x \leq \frac{\frac{m}{a}h}{m-a+2} + 1.
\]

If \(x \leq \epsilon\), then it follows in view of (9) that \(x \leq \left\lfloor \frac{\frac{m}{m-a+2}h}{m-a+2} \right\rfloor \leq \frac{\frac{m}{m-a+2}h}{m-a+2} + 1\), yielding (10). Therefore, to establish (10), it remains to handle the case when \(x > \epsilon\). In this case, it follows in view of (8) and (9) that

\[
x \leq \left\lfloor \frac{(\frac{m}{a} - \epsilon)h}{m-a+2-\epsilon} \right\rfloor \leq \frac{(\frac{m}{a} - \epsilon)h}{m-a+2-\epsilon} + 1.
\]

If (10) is false, then comparing with (11) yields \(m < \frac{m}{a} + a - 2 \leq m - 1\), a contradiction. Consequently, we see that (10) holds regardless.

Suppose \(h - e < x\). Hence, it follows in view of (10) and \(e \leq a - 2\) that

\[
(1 - \frac{\frac{m}{m-a+2}}{m-a+2})h \leq a - 2.
\]

If \(\frac{m}{m-a+2} > \frac{1}{2}\), then \(2 \leq a \leq \frac{m}{2}\) would imply that \(m \leq 2\frac{m}{a} + a - 3 \leq m - 1\), a contradiction. Therefore \(\frac{m}{m-a+2} \leq \frac{1}{2}\), which combined with (12) yields

\[
a - 2 \geq \frac{1}{2}h.
\]

In view of \(h - e < x\), \(e \leq a - 2\), and \(h \geq a + 1\), it follows that

\[
a + 1 \leq h \leq x - 1 + e \leq x + a - 3,
\]

implying that \(x \geq 4\). Thus (10) and (13) imply that

\[
3m - 3a + 6 = 3(m-a+2) \leq \frac{m}{a}(2a-4) = 2m - \frac{4m}{a}.
\]
implying that

$$\tag{14} m \leq 3a - \frac{4m}{a} - 6.$$ 

If \(a \leq \frac{m}{3}\), then (14) implies that \(m \leq 3\frac{m}{3} - 4 \cdot 3 - 6 = m - 18\), a contradiction. Therefore we may assume that \(a = \frac{m}{2}\), whence \(|H_a| = 2\). Thus \(S_a\) has exactly one distinct term equal to the generator of \(H_a\). Consequently, in view of \(h(S) \leq h\) and \(e \leq a - 2\), it follows that

$$m \leq |S| = |S_a| + e \leq |S_a| + a - 2 = |S_a| + \frac{m}{2} - 2 \leq h + \frac{m}{2} - 2.$$ 

Hence \(h \geq \frac{m}{2} + 2 = \frac{m}{a} + a\), contradicting (7). So we may assume \(h - e \geq x\).

Hence, let \(S''_a = A_1 \cdots A_x \cdots A_{h-e}\). In view of the definition of \(x\), and since \(h - e \geq x\), it follows that \(|S''_a| \geq \frac{m}{a}\). Let \(B\) be the \((h-e+t)\)-setpartition of \(S''_aT_a0^{h-e-1}\) defined by adding a zero to each \(A_i\) with \(i > 1\), and including each term of \(T_a\) as a singleton set.

Suppose \(|H_a|\) is prime. Thus applying CDT to \(B\), it follows that there are at least

$$|S''_a| + t + (h - e - 1) - (h - e + t) + 1 = |S''_a| \geq \frac{m}{a}$$

elements in the sumset of \(B\), whence the sumset is \(H_a\). Thus every element of \(\Sigma(S)\) can be expressed as a sum of at most \(h - e + t\), and at least

$$h - e + t - \nu_0(S''_aT_a0^{h-e-1}) = t + 1,$$

terms from \(S''_aT_a\), and at most \(e\) terms not from \(H_a\). Hence \(\Sigma_{\geq t+1}(S) \cap \Sigma_{\leq h+e}(S) = \Sigma(S)\), as desired. So we can assume \(|H_a| = \frac{m}{a}\) is not prime. Hence, since \(0 < H_a < G\), it follows that \(m\) has at least three prime factors, which completes the proof of (ii). Consequently, since

$$\frac{m}{p} - 1 = \frac{m}{2p} + \frac{m}{2p} - 1 \geq \frac{m}{2p} + \frac{m}{pq} + q - 3,$$

it follows that both (i) and (iii) imply

$$\tag{15} h + t \geq \frac{m}{pq} + q - 3.$$ 

Suppose \(h - e + t \leq \frac{m}{ap'} - 2\), where \(p'\) is the smallest prime divisor of \(\frac{m}{a}\). Hence \(e \leq a - 2\) implies that

$$\tag{16} h + t \leq \frac{m}{ap'} + a - 4.$$
If \( a = p \), then \( p' = q \), whence (16) implies that \( h + t \leq \frac{m}{pq} + p - 4 \leq \frac{m}{pq} + q - 4 \). Otherwise, since \(|H_a|\) composite, it follows that \( q \leq a \leq \frac{m}{pq} \), whence, in view of \( p \leq p' \) and (16), it follows that
\[
h + t \leq \frac{m}{ap'} + a - 4 \leq \frac{m}{ap} + a - 4 \leq \frac{m}{qp} + q - 4.
\]
In both cases we contradict (15). So we may assume that
\[
(17) \quad h - e + t \geq \frac{m}{ap'} - 1.
\]
Thus we can apply Theorem 1.4 with \( S' = S''_a T_a 0^{h-e-1} \), \( S = S_a 0^{h-e-1} \), \( n = h - e + t \), \( G = H_a \), and \( P = B \).

Suppose Theorem 1.4(i) holds. Hence there exists \( S''|S_a 0^{h-e-1} \) of length \( |S''_a| + t + h - e - 1 \) with an \((h - e + t)\)-setpartition whose sumset has cardinality at least
\[
\min\{\frac{m}{a} , |S''_a| + t + (h - e - 1) - (h - e + t) + 1\} = \min\{\frac{m}{a} , |S''_a|\} = \frac{m}{a}.
\]
Hence \( \Sigma_{\geq h-e+t-t'}(S'') \cap \Sigma_{\leq h-e+t}(S'') = H_a \), where
\[
t' = \nu_0(S'') \leq \nu_0(S_a 0^{h-e-1}) = h - e - 1.
\]
Consequently, it follows that \( h - e + t - t' \geq t + 1 \). Thus every term of \( \Sigma(S) \) can be expressed as a sum of at most \( h - e + t \) terms from \( S'' \) (and at least \( h - e + t - t' \geq t + 1 \) terms), and at most \( e \) terms not from \( H_a \). Hence \( \Sigma(S) = \Sigma_{\geq t+1}(S) \cap \Sigma_{\leq h+t}(S) \), as desired. So we can assume Theorem 1.4(ii) holds, whence there exists a proper, nontrivial subgroup \( H_{ka} \) of index \( k \) in \( H_a \), and \( \beta \in H_a \), such that all but \( e' \leq k - 2 \) terms of \( S_a 0^{h-e-1} \) are from \( \beta + H_{ka} \).

Suppose \( 0 \notin \beta + H_{ka} \). Hence, since there are only \( e' \leq k - 2 \) terms of \( S_a 0^{h-e-1} \) outside of \( H_{ka} \), it follows that \( h - e - 1 \leq k - 2 \). Thus, in view of (17), \( e \leq a - 2 \), and \( 2 \leq a \), \( k \leq \frac{m}{2} \), it follows that
\[
(18) \quad m - 1 \leq m + \frac{m}{ap'} - 2 \leq m + t + h - e - 1 \leq |S0^{h-e-1}| \leq |H_{ka}|h + e' + e \leq \frac{m}{ka}(k + e - 1) + k - 2 + e \leq \frac{m}{ka}(k + a - 3) + k + a - 4 = \left(\frac{m}{a} + a\right) + \left(\frac{m}{k} + k\right) - 3\frac{m}{ka} - 4 \leq \left(\frac{m}{2} + 2\right) + \left(\frac{m}{2} + 2\right) - 3\frac{m}{ka} - 4 = m - 3\frac{m}{ka} \leq m - 3,
\]
a contradiction. So we may assume \( 0 \in \beta + H_{ka} \), whence w.l.o.g. \( \beta = 0 \).
Consequently, all but at most \( k - 2 + a - 2 \leq ka - 4 \) terms of \( S \) are from the same nontrivial subgroup \( H_{ka} < H_a \). Furthermore, since Theorem 1.4(ii) holds for \( S_0^{h-e-1} \), it follows that \( \Sigma_{h-e+t}(S_0^{h-e-1}) = H_{ka} \), where \( S_{ka} \) is the subsequence of terms of \( S_a \) from \( H_{ka} \). Hence, since \( \nu_0(S_0^{h-e-1}) = h - e - 1 < h - e + t \), it follows that \( \Sigma(S_{ka}) = H_{ka} \). Thus \( H_{ka} \) contradicts the minimality of \( H_a \), completing the proof of both (i) and (iii).

\[ \square \]

3. PROOF OF THEOREM 1.2

Since \( |S| \geq m + \frac{m}{p} - 1 \), let \( |S| = m + k \) with \( k \geq \frac{m}{p} - 1 \). Note that

\[
\Sigma_m(S) = \sigma(S) - \Sigma_{|S|-m}(S) = \sigma(S) - \Sigma_k(S).
\]

Thus it suffices to show that \( \sigma(S) \in \Sigma_k(S) \), and that \( \Sigma_k(S) \) is periodic.

We may w.l.o.g. by translation assume 0 is the term with greatest multiplicity \( h = h(S) \) in \( S \). Since by hypothesis \( h = h(S) \leq |S| - m = k \), then let \( t = k - h \geq 0 \) and \( S' = S_{0-h} \). Note that \( |S'| = m + k - h = m + t \), and that \( h(S') \leq h(S) = h \). Thus, since \( h + t = k \geq \frac{m}{p} - 1 \), it follows that we can apply Theorem 1.1(i) to \( S' \), whence

\[
\Sigma_{\geq t+1}(S') \cap \Sigma_{\leq h+t}(S') = \Sigma_{\geq t+1}(S') \cap \Sigma_{\leq k}(S') = \Sigma(S'),
\]

and \( \Sigma(S') \) is periodic.

Thus for every \( z \in \Sigma(S') = \Sigma_{\geq t+1}(S') \cap \Sigma_{\leq k}(S') \), there exists a subsequence \( T_z \) of \( S' \) whose sum is \( z \), such that

\[
k - h + 1 = t + 1 \leq |T_z| \leq k.
\]

Since \( |SS'^{-1}| = h \), then adding the appropriate number of zeros to \( T_z \) yields a \( k \)-term subsequence whose sum is \( z \). Consequently, \( \Sigma(S') \subseteq \Sigma_k(S) \). Since \( S' = S_{0-h} \), it follows that \( \Sigma_k(S) \setminus 0 \subseteq \Sigma(S') \). However, since \( |S'| = m + t \geq m = |G| \geq D(G) \), it follows that \( 0 \in \Sigma(S') \) as well. Hence the previous sentences imply that

\[
\Sigma(S') = \Sigma_k(S).
\]

Thus, since \( \Sigma(S') \) is periodic, it follows that \( \Sigma_k(S) \) is periodic, and since \( \sigma(S) = \sigma(S') \in \Sigma(S') \), it follows that \( \sigma(S) \in \Sigma_k(S) \), completing the proof as remarked earlier.

\[ \square \]

Acknowledgment: We thank the referee for their helpful suggestions, and for pointing out an inaccuracy in the original lower bound examples.
References


---

1 Departamento de Matemática Aplicada IV; Universitat Politècnica de Catalunya; Campus Nord, Edifici C3; C. Jordi Girona, 1-3; 08034-Barcelona; Barcelona, Espanya. Supported in part by the National Science Foundation, as an MPS-DRF postdoctoral fellow, under grant DMS-0502193.


4 Departamento de Matemáticas, Escuela de Ciencias, Núcleo Sucre, Universidad de Oriente. Cumaná, Venezuela.