On the Intersection of two $m$-sets and the Erdős-Ginzburg-Ziv Theorem

Arie Bialostocki∗ and David J. Grynkiewicz†

December 11, 2008

Abstract

We prove the following extension of the Erdős-Ginzburg-Ziv Theorem. Let $m$ be a positive integer. For every sequence $\{a_i\}_{i \in I}$ of elements from the cyclic group $\mathbb{Z}_m$, where $|I| = 4m - 5$ (where $|I| = 4m - 3$), there exist two subsets $A, B \subseteq I$ such that $|A \cap B| = 2$ (such that $|A \cap B| = 1$), $|A| = |B| = m$, and $\sum_{i \in A} a_i = \sum_{i \in B} b_i = 0$.

1 Introduction

Since the seminal theorem of Erdős-Ginzburg-Ziv (EGZ) [13] [14] [1]—which states that any sequence of $2m - 1$ elements from a finite abelian group of order $m$ contains an $m$-term subsequence whose terms sum to zero—many generalizations, analogs, related problems [17] [15] [1] [2], and what are known as generalizations in the sense of EGZ for edge colorings of graphs [7] [16] as well as for colorings of the integers [12], were published. Two surveys appeared in [3] [5]. In the early 1990’s, the first author posed the following related conjecture.

Conjecture 1.1. Let $m$ be a positive integer. For every sequence $\{a_i\}_{i \in I}$ of elements from the cyclic group $\mathbb{Z}_m$, where $|I| = 4m - 5$ (where $|I| = 4m - 3$), there exist two subsets $A, B \subseteq I$ such that $|A \cap B| = 2$ (such that $|A \cap B| = 1$), $|A| = |B| = m$, and $\sum_{i \in A} a_i = \sum_{i \in B} b_i = 0$.

While the case $|A \cap B| = 1$ follows directly from the Cauchy-Davenport Theorem [6] for $m$ prime, there were no tools to attack the case $|A \cap B| = 2$, until recently. The main tool

∗300 Brink Hall, University of Idaho, P.O. Box 441103, Moscow, ID 83844-1103,
†Mathematics 253-37, Caltech, Pasadena, CA 91125
to handle this kind of problem was developed by the second author [10]. It is stated below as
Theorem 2.1. The aim of this note is to affirm the conjecture above. It is worthwhile to note
that a continuation by the second author along similar lines will appear in [9].

2 Preliminaries

Let $G$ denote an abelian group of order $m$, and let $S$ be a sequence of elements from $G$. The
length of $S$ is denoted by $|S|$. If $A, B \subseteq G$, then their sumset, $A + B$, is the set of all possible
pairwise sums, i.e. $\{a + b \mid a \in A, b \in B\}$. Furthermore, an $n$-set partition of $S$ is a sequence
of $n$ nonempty subsequences of $S$, pairwise disjoint as sequences, such that every term of $S$
belongs to exactly one subsequence, and the terms in each subsequence are distinct. Thus
such subsequences can be considered sets. Let $\varphi$ be the function which takes a sequence to its
underlying set, so that if $S = (0, 0, 1, 2, 0, 2, 2)$, then $\varphi(S) = \{0, 1, 2\}$. For $\alpha \in Z_m$, let $\overline{\alpha}$ denote
the least positive integer representative of $\alpha$. If $S'$ is a subsequence of $S$, then $S \setminus S'$ denotes
the subsequence of $S$ obtained by deleting the terms of $S'$ in $S$.

The following [10] [8] [11] is a recent composite analog of the Cauchy-Davenport Theorem
[6].

Theorem 2.1. Let $S$ be a sequence of elements from an abelian group $G$ of order $m$ with an
$n$-set partition $P = P_1, \ldots, P_n$, and let $p$ be the smallest prime divisor of $m$. Then either:

(i) there exists an $n$-set partition $A = A_1, A_2, \ldots, A_n$ of $S$ such that:

$$|\sum_{i=1}^n A_i| \geq \min \{m, (n + 1)p, |S| - n + 1\};$$

Furthermore, if $n' \geq \frac{m}{p} - 1$ is an integer such that $P$ has at least $n - n'$ cardinality one sets and
if $|S| \geq n + \frac{m}{p} + p - 3$, then we may assume there are at least $n - n'$ cardinality one sets in $A$, or

(ii) (a) there exists $\alpha \in G$ and a nontrivial proper subgroup $H_\alpha$ of index $a$ such that all but
at most $a - 2$ terms of $S$ are from the coset $\alpha + H_\alpha$; and (b) there exists an $n$-set partition
$A_1, A_2, \ldots, A_n$ of the subsequence of $S$ consisting of terms from $\alpha + H_\alpha$ such that $\sum_{i=1}^n A_i =
na + H_\alpha$.

When using the above theorem, the following basic proposition about $n$-set partitions is
useful [2].

Proposition 2.1. A sequence $S$ has an $n$-set partition $A$ if and only if the multiplicity of each
element in $S$ is at most $n$ and $|S| \geq n$. Furthermore, a sequence $S$ with an $n$-set partition
has an \(n\)-set partition \(A' = A_1, \ldots, A_m\) such that \(||A_i| - |A_j|| \leq 1\) for all \(i\) and \(j\) satisfying \(1 \leq i \leq j \leq n\).

Finally, we need the following theorem which describes the extremal instances for EGZ [4].

**Theorem 2.2.** Let \(S\) be a sequence of elements from \(\mathbb{Z}_m\). If \(|S| = 2m - 2\) and \(S\) contains no \(m\)-term zero-sum subsequence, then \(S\) contains two distinct residues, whose difference is coprime to \(m\), each with multiplicity \(m - 1\).

## 3 The Proof

Let \(S\) be a sequence of elements from \(\mathbb{Z}_m \overset{\text{def}}{=} G\) with \(|S| = 4m - 5\) (with \(|S| = 4m - 3\)). If there exists \(\alpha \in G\) such that \(|\varphi^{-1}(\alpha)| \geq 2m - 2\) (such that \(|\varphi^{-1}(\alpha)| \geq 2m - 1\), then the proof is complete with both \(m\)-term subsequences monochromatic. Hence we may assume \(|\varphi(S)| \geq 3\), else the proof is complete by the pigeonhole principle.

Suppose there does not exist a subsequence \(S'\) of \(S\) with \(|S'| = 2m - 3\) (with \(|S'| = 2m - 2\), such that there exist an \((m - 2)\)-set partition \(P\) of \(S'\) (such that there exists an \((m - 1)\)-set partition of \(S'\)). Hence, since \(|\varphi(S)| \geq 3\), it follows from Proposition 2.1 that there is \(\alpha \in G\) with \(|\varphi^{-1}(\alpha)| \geq 3m - 3\) (with \(|\varphi^{-1}(\alpha)| \geq 3m - 1\), and the result follows from the arguments from the first paragraph. So we may assume such \(S'\) exists.

Since \(|S \setminus S'| = 2m - 2\) (since \(|S \setminus S'| = 2m - 1\)), it follows from Theorem 2.2 that there is an \(m\)-term zero-sum subsequence of \(S \setminus S'\), unless w.l.o.g. \(\varphi(S \setminus S') = \{0, 1\}\), with both 0 and 1 occurring with multiplicity \(m - 1\) in \(S \setminus S'\) (it follows from EGZ that there is an \(m\)-term zero-sum subsequence of \(S \setminus S'\) regardless). We can avoid this case by swapping a 0 or 1 from \(S \setminus S'\) with a term \(\beta\) from \(S'\) with \(\beta \neq 1\) and \(\beta \neq 0\), unless, up to order, \(S = (0, 0, \ldots, 0, 1, 1, \ldots, 1, \gamma)\), with \(\gamma \neq 0\) and \(\gamma \neq 1\); but it is easily checked, since \((\gamma, 1, \ldots, 1, 0, \ldots, 0)\) is zero-sum, that the sequence \((0, 0, \ldots, 0, 1, 1, \ldots, 1, \gamma)\) satisfies conjecture 1.1. So we may assume that there is a \(m\)-term zero-sum subsequence in \(S \setminus S'\), say \(T\).

Let \(S'' = S \setminus T\), and let \(P'\) be a \((2m - 4)\)-set partition of \(S''\) (let \(P\) be a \((2m - 2)\)-set partition of \(S'\)) obtained by adding the terms of \((S \setminus S') \setminus \emptyset\) to \(P\) as singleton sets. Fix two elements in \(T\), say \(\{t_1, t_2\} = T'\) (fix an element in \(T\), say \(\{t_1\} = T'\)). Applying Theorem 2.1 to \(P'\), it follows that either (i) holds and hence there exist \(m - 2\) elements from \(S''\) (there exist \(m - 1\) elements from \(S''\)) which along with \(T'\) form a \(m\)-term zero-sum sequence, and the proof is complete, or else (ii) holds and hence, w.l.o.g. by translation, there exists a proper nontrivial
subgroup $H \leq G$ with index $a$ such that all but at most $a - 2$ terms of $S''$ are from $H$. Note that this proves the theorem for $m$ prime.

We proceed by induction on the number of primes in the factorization of $m$. Hence, since $4 \frac{m}{a} - 5 \leq 3m - 3 - a$ (since $4 \frac{m}{a} - 3 \leq 3m - 1 - a$), it follows by induction hypothesis that there are two $\frac{m}{a}$-term zero-sum subsequences of $S''$, $A$ and $B$, that share exactly two terms (that share exactly one term). Thus, since $(2a - 3) \frac{m}{a} + 2 \frac{m}{a} - 1 \leq 3m - 3 - a - (2 \frac{m}{a} - 2)$ (since $(2a - 3) \frac{m}{a} + 2 \frac{m}{a} - 1 \leq 3m - 1 - a - (2 \frac{m}{a} - 1)$), it follows by $2a - 2$ applications of the Erdős-Ginzburg-Ziv Theorem with the group $H_a$ that there exist two $m$-term zero-sum subsequences $A'$ and $B'$, with $A$ a subsequence of $A'$, with $B$ a subsequence of $B'$, and with $A'$ and $B'$ sharing exactly two terms (sharing exactly one term), completing the proof.

Acknowledgement The first author would like to thank Professor Zoltan Furedi for a helpful discussion concerning this topic in February 1991.

References


