

On Some Developments of the Erdős-Ginzburg-Ziv Theorem II (personal/extended copy)

Arie Bialostocki, Paul Dierker, David Gryniewicz and Mark Lotspeich

August 19, 2001

Abstract. Let S be a sequence of elements from the cyclic group \mathbb{Z}_m . We say S is zsf (zero-sum free) if there does not exist an m -term subsequence of S whose sum is zero. Denote by $g(m, k)$ the least integer such that every sequence S with at least k distinct elements and length $g(m, k)$ must contain an m -term subsequence whose sum is zero. Furthermore, denote by $E(m, s)$ the set of all equivalence classes of zsf sequences with length s , up to order and affine transformation, that are not a proper subsequence of another zsf sequence. In this paper, we first find for a sequence S of sufficient length, $|S| \geq 2m - \lfloor \frac{m}{4} \rfloor - 2$, necessary and sufficient conditions in terms of a system of inequalities over the integers for S to be zsf. Among the consequences, we determine $g(m, k)$ for large m , namely $g(m, k) = 2m - \lfloor \frac{k^2 - 2k + 5}{4} \rfloor$ provided $m \geq k^2 - 2k - 3$, which in turn resolves two conjectures of the first and fourth authors. Next, using independent methods, we evaluate $g(m, 5)$ for every $m \geq 5$. We conclude with the list of $E(m, s)$ for every m and s satisfying $2m - 2 \geq s \geq \max\{2m - 8, 2m - \lfloor \frac{m}{4} \rfloor - 2\}$.

1 Introduction

Let S be a sequence of elements from the cyclic group \mathbb{Z}_m . We say S is zsf (zero-sum free) if there does not exist an m -term subsequence of S whose sum is zero. Let $g(m, k)$ ($g^*(m, k)$) denote the least integer such that every sequence S with at least (with exactly) k distinct elements and length $g(m, k)$ ($g^*(m, k)$) must contain an m -term subsequence whose sum is zero. By an affine transformation in \mathbb{Z}_m , we mean a map of the form $x \mapsto ax + b$, with $a, b \in \mathbb{Z}_m$ and $\gcd(a, m) = 1$. Furthermore, let $E(m, s)$ denote the set of all equivalence classes of zsf sequences S of length s , up to order and affine transformation, that are not a proper subsequence of another zsf sequence. Using the above notation, the renowned Erdős-Ginzburg-Ziv theorem, [1], [11], states that $g(m, 1) = g(m, 2) = 2m - 1$ for $m \geq 2$.

The function $g(m, k)$ was introduced in [4], where it was shown that $g(m, 4) = 2m - 3$ for $m \geq 4$. Furthermore, based on a lower bound construction the authors conjectured the value of $g(m, k)$ for fixed k and sufficiently large m . Concerning the upper bound, they established an upper bound for m prime modulo the affirmation of the Erdős-Heilbronn conjecture (EHC). Since then, the EHC has been affirmed [9], [2], moreover, the bound given in [4] was extended for nonprimes in [17]. As it will later be seen, it is worthwhile to mention that the affirmation of the EHC has resulted in several attempted generalizations and related results [6], [14], [23], [25]. Other relevant developments concerning $g(m, k)$ appear in [3], [5], [7], [13], [15], [16], [23]. For example, the value $g(m, 3) = 2m - 2$ was determined in [3], and the closely related function $g^*(m, k)$, introduced in [5] and further investigated in [4], [15], [16], was determined for all m and k satisfying $k > \frac{m}{2} + 1$.

This paper started under the authorship of the first, second and fourth authors, and was cited in [4] as in preparation. Actually, a rough draft was ready determining $g(m, 5)$ using the methods of [4]. The motivation for the current paper is twofold. First, the third author was able to determine exactly $g(m, k)$ for fixed k and large m by improving the known lower bound construction and adapting the proof used by Gao and Hamidoune [17] to obtain a better upper bound than the one conjectured in [4]. Consequently, the following conjecture of [4] has been affirmed.

Conjecture 1.1. *For every k , $k \geq 2$, there exists an integer $m_0 = m_0(k)$ such that if $m > m_0$, then*

- (a) $g(m, k) = 2m - c$, where $c = c(k)$ is independent of m
- (b) $g^*(m, k) = g(m, k)$.

Thus, the $g(m, k)$ problem for fixed k and large m has been put to rest. Second, as several recent works, e.g. [21], [27], use the known values of $g(m, k)$ and $E(m, s)$ for $k \leq 4$ and $s \geq 2m - 3$, and as it is likely that $g(m, 5)$ will be needed for further zero-sum applications, we determine $g(m, 5)$ for every $m \geq 5$.

The paper is organized as follows. In section 2, definitions and notation are introduced and known results needed later in the paper are listed. In Section 3, first the upper bound proof of [17] is adapted to find for a sequence S with $|S| \geq 2m - \lfloor \frac{m}{4} \rfloor - 2$, necessary and sufficient conditions in terms of a system of inequalities over the integers for S to be zsf. This result and a lower bound construction imply the value of $g(m, k)$ for fixed k and large m . Following is the affirmation of Conjecture 1.1. Section 4 contains the evaluation of $g(m, 5)$ for every $m \geq 5$. The paper concludes with an appendix listing the elements of $E(m, s)$ for every m and s satisfying $2m - 2 \geq s \geq \max\{2m - 8, 2m - \lfloor \frac{m}{4} \rfloor - 2\}$.

2 Preliminaries

Let G denote an abelian group of order m . As we work simultaneously with the cyclic group \mathbb{Z}_m of residue classes modulo m and the additive group of the integers \mathbb{Z} , for $\alpha \in \mathbb{Z}_m$ we denote by $\bar{\alpha}$ the least positive integer that is congruent to α modulo m . A sequence S of elements from G is abbreviated as a string using exponential notation (e.g. the sequence $1, 1, 1, 2, 2, 2, 2$ is abbreviated by $1^3 2^4$). Furthermore, the length of S is denoted by $|S|$. Let t be a nonnegative integer. Denote by $\sum S$ the set of all sums over nonempty subsequences of S , and by $\sum_t S$ ($\sum_{\geq t} S$) the set of all sums over subsequences of S of length exactly (at least) t . If $A, B \subseteq G$, then their sumset, $A + B$, is the set of all possible pairwise sums, i.e. $\{a + b \mid a \in A, b \in B\}$.

Following Kemperman [24], a set $A \subseteq G$ is H -periodic if it is the union of H -cosets for some nontrivial subgroup $H \leq G$. 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. Finally let φ be the map that takes a sequence to its underlying set (e.g. $\varphi(1, 1, 1, 2, 2, 4) = \{1, 2, 4\}$).

First, we state three well know theorems, the first one is a generalized version of what is known as the Caveman Theorem [12], followed by a generalized form of the Erdős-Ginzburg-Ziv Theorem

(EGZ) [1], [11], and the affirmed EHC [2], [9]. The original EGZ Theorem is Theorem 2.2 with $r = 1$; and Theorem 2.2 is obtained by r applications of the EGZ Theorem. Theorem 2.1 is similarly obtained, where the original Caveman Theorem is the case $|S| = m$.

Theorem 2.1. *Let S be a sequence of elements from an abelian group G of order m . If $|S| \geq m$, then there exists a subsequence of S of length r whose terms sum to zero, where r satisfies $|S| - (m - 1) \leq r \leq |S|$.*

Theorem 2.2. *Let r be a positive integer. If S is a sequence of $(r + 1)m - 1$ elements from an abelian group G of order m , then S contains an rm -term subsequence which sums to zero.*

Theorem 2.3. *Let S be a sequence of k distinct elements from \mathbb{Z}_m . If m is prime, then $|\sum_h S| \geq \min\{m, hk - h^2 + 1\}$.*

The following two theorems of Gao [18], [19], respectively, are central to the proof of Theorem 3.1.

Theorem 2.4. *Let l and m be positive integers satisfying $2 \leq l \leq \lfloor \frac{m}{4} \rfloor + 2$, and let S be a sequence of elements from \mathbb{Z}_m satisfying $|S| = 2m - l$. If $0 \notin \sum_m S$, then up to order and affine transformation $S = 0^u 1^v c_1 \dots c_w$, where $m - 2l + 3 \leq v \leq u \leq m - 1$ and $w \leq l - 2$.*

Theorem 2.5. *Let m , n and h be positive integers. Suppose G is a finite abelian group of order m , and $g \in G$. Furthermore, let $S = 0^h a_1 \dots a_n$ be a sequence of elements from G such that the multiplicity of every element in the subsequence $T = a_1 \dots a_n$ is at most h . If $g \in \sum_{\geq m-h} T$, then $g \in \sum_m S$.*

Next, we state the Cauchy-Davenport Theorem [8], [26], and a recently proved composite analog of it [20].

Theorem 2.6. *For positive integers n and m , let $A, \dots, A_n \subseteq \mathbb{Z}_p$. If m is prime, then*

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

Theorem 2.7. *Let n be an integer and let S be a sequence of elements from an abelian group G of order m such that $|S| \geq n$ and every element of S appears at most n times in S . Furthermore, let p be the smallest prime divisor of m . Then either:*

(i) there exists an n -set partition, A_1, \dots, A_n , of S , such that

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

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

When using the above theorem, the following two basic propositions about n -set partitions and sumsets are often used, and for the sake of clarity, we provide their proofs.

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 $A' = A_1, \dots, A_n$ such that $||A_i| - |A_j|| \leq 1$ for all i and j satisfying $1 \leq i \leq j \leq n$.*

Proof. Suppose S has an n -set partition, then from the definition the multiplicity of each element in S is at most n , and since empty sets are not allowed in the n -set partition, it follows that $|S| \geq n$. Next suppose that the multiplicity of each element in S is at most n and $|S| \geq n$. Let $\varphi(S) = \{s_1, \dots, s_u\}$, and rearrange the terms of S so that all the terms that are equal to s_1 come first, followed by all the terms that are equal to s_2 , and so forth, terminating with the terms equal to s_u . Let us denote this new sequence by $S' = x_1 x_2 \dots x_{kn+r}$, where $|S| = |S'| = kn + r$ and $0 \leq r < n$. Consider the following sequence A of n subsequences of S' written vertically.

$$A = \begin{pmatrix} x_1 \\ x_{n+1} \\ \vdots \\ x_{(k-1)n+1} \\ x_{kn+1} \end{pmatrix} \cdots \begin{pmatrix} x_r \\ x_{n+r} \\ \vdots \\ x_{(k-1)n+r} \\ x_{kn+r} \end{pmatrix} \begin{pmatrix} x_{r+1} \\ x_{n+r+1} \\ \vdots \\ x_{(k-1)n+r+1} \\ \cdot \end{pmatrix} \cdots \begin{pmatrix} x_n \\ x_{2n} \\ \vdots \\ x_{kn} \\ \cdot \end{pmatrix}$$

We will show that A is an n -set partition of S' and hence of S . Indeed, since $|S| \geq n$, it follows that none of the sets in A are empty. Furthermore, in view of the definition of S' and the fact that the maximum multiplicity of a term in S' does not exceed n , it follows that $x_{j_1 n+i} \neq x_{j_2 n+i}$, for every i and every $j_1 \neq j_2$. Thus A is an n -set partition of S . The furthermore more part is clear from the definition of A . \square

Proposition 2.2. *Let S be a sequence of elements from a finite abelian group G , and let $A = A_1 \dots A_n$ be an n -set partition of S , where $|\sum_{i=1}^n A_i| = r$, and s is the cardinality of the largest set in A . Furthermore, let $a_1 \dots a_n$ be a subsequence of S such that $a_i \in A_i$ for $i = 1, \dots, n$.*

(i) There exists a subsequence S' of S and an n' -set partition $A' = A'_1 \dots A'_{n'}$ of S' , which is a subsequence of the n -set partition $A = A_1 \dots A_n$, such that $n' \leq r - s + 1$ and $|\sum_{i=1}^{n'} A'_i| = r$.

(ii) There exists a subsequence S' of S of length at most $n + r - 1$, and an n -set partition $A' = A'_1 \dots A'_n$ of S' , where $A'_i \subseteq A_i$ for $i = 1, \dots, n$, such that $\sum_{i=1}^n A'_i = \sum_{i=1}^n A_i$. Furthermore, $a_i \in A'_i$ for $i = 1, \dots, n$.

Proof. We first prove (i). Assume w.l.o.g. that $|A_1| = s$. We will construct the n' -set partition A' in n steps as follows; and S' will be implied implicitly. Denote by $A^{(k)} = A'_1 \dots A'_{a_k}$ the constructed sequence after k steps, and hence $A' = A^{(n)}$ and $n' = a_n$. Let $A^{(1)} = A_1$, and for $k = 1, 2, \dots, n - 1$, let

$$A^{(k+1)} = \begin{cases} A^{(k)} & \text{if } |\sum_{i=1}^{a_k} A'_i + A_{k+1}| = |\sum_{i=1}^{a_k} A'_i| \\ A^{(k)} A_{k+1} & \text{if } |\sum_{i=1}^{a_k} A'_i + A_{k+1}| > |\sum_{i=1}^{a_k} A'_i|. \end{cases}$$

It is easily seen by the above algorithm that $|\sum_{i=1}^{a_n} A'_i| = |\sum_{i=1}^n A_i| = r$. Furthermore, since each kept term increases the cardinality of the sumset of the previous terms of A' by at least one, and since $|A_1| = s$, it follows that at most $r - s$ terms, excluding A_1 , were kept, and thus $a_n = n' \leq 1 + r - s$.

The proof of (ii) is similar to that of (i). First, for $i = 1, \dots, n$, let the elements of A_i be $\{a_1^{(i)} \dots a_{|A_i|}^{(i)}\}$, where $a_1^{(i)} = a_i$. We will construct the n -set partition A' in a two loop algorithm. The outer loop has n steps, where at the i th step the set A'_i is constructed using the inner loop. In turn, the inner loop, at the i th step of the outer loop, constructs A'_i in $|A_i|$ steps. For a given i , where $1 \leq i \leq n$, let $A_i^{(k)}$ denote the set constructed after k steps of the inner loop at the i th step of the outer loop, and hence $A' = A_1^{(|A_1|)} \dots A_n^{(|A_n|)}$ with S' implied implicitly. For a given j , where $1 \leq j \leq n$, let $A_j^{(1)} = \{a_j\}$, and for $k = 1, \dots, |A_j| - 1$, let

$$A_j^{(k+1)} = \begin{cases} A_j^{(k)} & \text{if } |\sum_{i=1}^{j-1} A_i^{(|A_i|)} + A_j^{(k)}| = |\sum_{i=1}^{j-1} A_i^{(|A_i|)} + (A_j^{(k)} \cup \{a_{k+1}^{(j)}\})| \\ A_j^{(k)} \cup \{a_{k+1}^{(j)}\} & \text{if } |\sum_{i=1}^{j-1} A_i^{(|A_i|)} + A_j^{(k)}| < |\sum_{i=1}^{j-1} A_i^{(|A_i|)} + (A_j^{(k)} \cup \{a_{k+1}^{(j)}\})|. \end{cases}$$

It is easily seen by the above algorithm that $A_i^{(|A_i|)} \subseteq A_i$ and $a_i \in A_i^{(|A_i|)}$ for $i = 1, \dots, n$, and that $|\sum_{i=1}^n A_i^{(|A_i|)}| = |\sum_{i=1}^n A_i| = r$; and since $\sum_{i=1}^n A_i^{(|A_i|)} \subseteq \sum_{i=1}^n A_i$, it follows that $\sum_{i=1}^n A_i^{(|A_i|)} = \sum_{i=1}^n A_i$. Furthermore, since each kept element $a_k^{(j)}$, where $k \neq 1$ if $j \neq 1$, increases the cardinality of the sumset by at least one, it follows that at most $r - 1$ terms, excluding the a_i 's, were kept, and hence $|S'| \leq n + r - 1$. \square

We will also need the following theorem of [16].

Theorem 2.8. *Let m and k be integers with $m \geq k \geq 2$ and $m \geq 5$.*

(a) *If $\frac{m}{2} + 1 < k \leq m - 1$, then $g(m, k) = m + 2$.*

(b) *If $k = m$, then $g(m, k) = \begin{cases} m & m \text{ odd} \\ m + 1 & m \text{ even.} \end{cases}$*

We conclude the preliminaries with a theorem of Eggleton and Erdős [10].

Theorem 2.9. *Let S be a sequence of k distinct elements from a finite abelian group. If $0 \notin \sum S$ and $k \geq 4$, then $|\sum S| \geq 2k$.*

3 A Theorem of Gao and Hamidoune Revisited

Theorem 3.1 gives necessary and sufficient conditions for a sequence S of sufficient length to be zsf. More precisely, it reduces the problem of determining extremal zsf sequences of sufficient length to the problem of finding integer partitions with a fixed number of parts and all parts greater than 1. Its proof is an adaption of a proof of Gao and Hamidoune [17].

Theorem 3.1. *For integers m and l , let S be a sequence of elements from \mathbb{Z}_m , satisfying $|S| = 2m - l \geq 2m - \lfloor \frac{m}{4} \rfloor - 2$. The sequence S does not contain an m -term zero-sum subsequence if and only if there exists a sequence $S' = 0^u 1^v a_1 \dots a_{w_1} b_1 \dots b_{w_2}$, where $1 < \bar{a}_i \leq \frac{m}{2}$ and $1 \leq \bar{b}_i < \frac{m}{2}$, that is equivalent to S up to order and affine transformation, and for which the following four inequalities are satisfied,*

$$\sum_{i=1}^{w_1} \bar{a}_i \leq m - v - 1 \quad \text{and} \quad \sum_{i=1}^{w_2} \bar{b}_i \leq m - u - 1 - w_2, \quad (1)$$

$$m - 2l + 3 \leq v \leq u \leq m - 1 \quad \text{and} \quad w_1 + w_2 \leq l - 2. \quad (2)$$

Moreover, equality holds in both inequalities of (1) if and only if S belongs to an equivalence class of $E(m, 2m - l)$.

Proof. First, suppose S is a sequence of elements from \mathbb{Z}_m , satisfying $|S| = 2m - l \geq 2m - \lfloor \frac{m}{4} \rfloor - 2$, and $0 \notin \sum_m S$. Hence from Theorem 2.4 it follows that S is equivalent, up to order and affine transformation, to a sequence $S' = 0^u 1^v a_1 \dots a_{w_1} b_1 \dots b_{w_2}$ satisfying the inequalities in (2), where

$1 < \overline{a_i} \leq \frac{m}{2}$ and $1 \leq \overline{-b_i} < \frac{m}{2}$. Since the fact that S is zsf implies the fact that S' is zsf, it follows from Theorem 2.5 that for any given subsequence T of $a_1 \dots a_{w_1} b_1 \dots b_{w_2}$,

$$\text{either } \overline{\sum_{t_i \in T} t_i} \leq m - v - 1 \text{ or } \overline{\sum_{t_i \in T} t_i} \geq u + 1 + |T|, \text{ and} \quad (3)$$

$$\text{either } -\overline{\sum_{t_i \in T} t_i} \leq m - u - 1 - |T| \text{ or } -\overline{\sum_{t_i \in T} t_i} \geq v + 1. \quad (4)$$

Induction on r , in view of (3) and the following three inequalities, (i) $l \leq \lfloor \frac{m}{4} \rfloor + 2$, (ii) $m - v - 1 \leq \lfloor \frac{m}{2} \rfloor$ (follows from (2) and $l \leq \lfloor \frac{m}{4} \rfloor + 2$), (iii) $3m - 4l + 5 \leq u + 2v$ (follows from (2)), implies

$$\sum_{i=1}^r \overline{a_i} = \overline{\sum_{i=1}^r a_i} \leq m - v - 1, \quad (5)$$

for every r satisfying $1 \leq r \leq w_1$.

Similarly, induction on r , in view of (4) and the inequalities (i), (ii) and (iii), and the fact that $u \geq v$, implies

$$\sum_{i=1}^r \overline{-b_i} = -\overline{\sum_{i=1}^r b_i} \leq m - u - 1 - r, \quad (6)$$

for every r satisfying $1 \leq r \leq w_2$. Hence (5) and (6) imply (1).

Next suppose S is an arbitrary sequence of residues from \mathbb{Z}_m that satisfies (1) and (2). Actually, we will use only the fact that (1) is satisfied and $v \leq u \leq m - 1$. It follows from (1) that any m -term zero-sum modulo m subsequence of S must be zero-sum in \mathbb{Z} as well. In addition, it follows from (1) that the longest zero-sum in \mathbb{Z} subsequence of S that does not contain a zero is of length $w_2 + \sum_{i=1}^{w_2} \overline{-b_i} \leq m - u - 1$. Hence any m -term zero-sum subsequence must use at least $u + 1$ zeros, which exceeds the multiplicity of zero in S . Thus S is zsf, and as affine transformations and reordering preserve m -term zero-sum subsequences, the proof of the main part of the theorem is complete. Notice that the two inequalities in (1) are interchanged by the affine transformation which interchanges 0 and 1. Hence, the moreover part of the theorem is easily deduced from the main part of the theorem. \square

Theorem 3.2. *Let $m \geq k \geq 2$ be positive integers. If k is odd and $m \geq \frac{k^2+4k+3}{8} + 1$ or k is even and $m \geq \frac{k^2+2k}{8} + 1$, then $g^*(m, k) \geq 2m - \lfloor \frac{k^2-2k+5}{4} \rfloor$.*

Proof. If k is even, consider the sequence

$$S_0 = \left(-\frac{k-2}{2}\right) \dots (-2)(-1)(0)^{m-\frac{k^2+2k}{8}} (1)^{m-\frac{k^2+2k}{8}} (2)(3) \dots \left(\frac{k}{2}\right),$$

and if k is odd, consider the sequence

$$S_1 = \left(-\frac{k-3}{2}\right) \dots (-2)(-1)(0)^{m-\frac{k^2-1}{8}} (1)^{m-\frac{k^2+4k+3}{8}} (2)(3) \dots \left(\frac{k+1}{2}\right).$$

It follows from the hypotheses that both strings are well defined. Since both S_1 and S_2 satisfy (1), and since $v \leq u \leq m-1$, where u and v are the multiplicities of 0 and 1 respectively, it follows from the proof of the second direction of Theorem 1 that S_1 and S_2 are zsf. \square

We conclude the section with Theorem 3.3, which determines the value of $g(m, k)$ for fixed k and sufficiently large m , disproving Conjecture 5.1 of [4], and proving Conjectures 1.1(a) and 1.1(b) in parts (a) and (b) respectively. Again, its proof is an adaption of the proof in [17].

Theorem 3.3. *Let $m \geq k \geq 2$ be positive integers. If k is even and $m \geq k^2 - 2k - 4$ or k is odd and $m \geq k^2 - 2k - 3$, then*

$$(a) \ g(m, k) = 2m - \lfloor \frac{k^2-2k+5}{4} \rfloor.$$

$$(b) \ g^*(m, k) = g(m, k)$$

Proof. From Theorem 3.2, and from the trivial fact that $g^*(m, k) \leq g(m, k)$, it suffices for both parts (a) and (b) to show $g(m, k) \leq 2m - \lfloor \frac{k^2-2k+5}{4} \rfloor$. Assume to the contrary that there is a sequence S of elements from \mathbb{Z}_m , with $|S| = 2m - \lfloor \frac{k^2-2k+5}{4} \rfloor$, and $0 \notin \sum_m S$. From the hypotheses and the fact that $k^2 \equiv 0$ or $1 \pmod{4}$, it follows that $\lfloor \frac{k^2-2k+5}{4} \rfloor \leq \lfloor \frac{m}{4} \rfloor + 2$. Hence from Theorem 3.1 it follows that w.l.o.g. S satisfies (1) and (2). Let $c_1 = |\{a_1, \dots, a_{w_1}\}|$ and $c_2 = |\{b_1, \dots, b_{w_2}\}|$. It follows from the first inequality in (1), that $2 + 3 + \dots + (c_1 + 1) + 2(w_1 - c_1) \leq m - v - 1$, implying that

$$\frac{c_1^2 - c_1}{2} + 2w_1 \leq m - v - 1. \tag{7}$$

Likewise from the second inequality in (1), it follows that

$$\frac{c_2^2 - c_2}{2} + 2w_2 \leq m - u - 1 - w_2. \tag{8}$$

Inequalities (7) and (8) imply

$$\frac{c_1^2 - c_1}{2} + \frac{c_2^2 - c_2}{2} \leq m - v - 1 - w_1 + m - u - 1 - w_2 = l - 2,$$

which, in turn, yields

$$l \geq \frac{(c_1 + c_2)^2}{4} + \frac{c_1 + c_2}{2} + 2 \geq \frac{(k-2)^2}{4} + \frac{k-2}{2} + 2 = \frac{k^2 - 2k + 4}{4} + 1 > l,$$

which is a contradiction; and the proof is complete. \square

4 The Erdős-Heilbronn Conjecture and $g(m, 5)$

In view of Theorem 3.3, $g(m, 5)$ has been determined for $m \geq 12$. In this section, we present an abbreviated proof determining $g(m, 5)$ for all $m \geq 5$. We will make use of the following conjecture, which can be verified for $k \leq 5$ with some effort by considering the equations generated by the 2-sums of a 5-set S with $|\sum_2 S| < 7$.

Conjecture 4.1. *Let S be a sequence of $k \geq 2$ distinct elements from \mathbb{Z}_m . If $|\sum_2 S| < 2k - 3$, then either $\sum_2 S$ is H -periodic, where $|H| > 2$, or there exists a K -periodic subset T such that $S \subseteq T$ and $2(|T| - |S|) \leq |K| - 2$.*

Proof. For $k \leq 3$, the conjecture is easy. Suppose $k = 3$. Let $S = x_1 x_2 x_3 x_4$ be a sequence of four distinct nonzero residue classes from \mathbb{Z}_m such that $0 \notin \sum S$. Define four sets of equations A_i for $i = 1, 2, 3, 4$: $A_4 = \{x_1 = x_2 + x_3, x_2 = x_1 + x_3, x_3 = x_1 + x_2\}$, $A_3 = \{x_1 = x_2 + x_4, x_2 = x_1 + x_4, x_4 = x_1 + x_2\}$, $A_2 = \{x_1 = x_3 + x_4, x_3 = x_1 + x_4, x_4 = x_1 + x_3\}$, and $A_1 = \{x_2 = x_3 + x_4, x_3 = x_2 + x_4, x_4 = x_2 + x_3\}$. Observe that if two equations hold in some A_i , then two of the three x_j 's from A_i must be from the same coset of $\frac{m}{2}\mathbb{Z}_m$, and the third x_j must be equal to $\frac{m}{2}$ (due to the symmetry of the four sets and the equations in each set it suffices to check any two equations from any set). Hence, it is not difficult to deduce that more than one equation can hold in at most one of the A_i 's. Thus we may w.l.o.g. assume that either in A_4 only one equation holds, say $x_1 = x_2 + x_3$, or else w.l.o.g. only equations in A_1 hold. In the former case, it is then easily checked that the only equations that can hold are the following: $x_4 = x_1 + x_3$, $x_4 = x_1 + x_2$, $x_2 = x_3 + x_4$ and $x_3 = x_2 + x_4$. Hence the following elements must all be distinct: $x_1, x_2, x_3, x_1 + x_2, x_1 + x_3, x_1 + x_4, x_1 + x_2 + x_3$ and $x_1 + x_2 + x_3 + x_4$. In the later case, the following elements must all be distinct: $x_1, x_2, x_3, x_4, x_1 + x_2, x_1 + x_3, x_1 + x_4$ and $x_1 + x_2 + x_3 + x_4$. The case $k = 5$ follows from the next lemma. \square

Lemma 4.1. *Let $S = a_1a_2a_3a_4a_5$ be a sequence of five distinct residues from \mathbb{Z}_m . Then $|\sum_2 S| \geq 7$ or there exists a subgroup H of \mathbb{Z}_m of cardinality $h = 5$ or $h = 6$, and in addition there exists an H -periodic set S' , and a subset T of S' with $|T| = h - 5$, such that $S = S' \setminus T$.*

Proof. Let $A = \{a_1 + a_2, a_1 + a_3, a_1 + a_4, a_1 + a_5, a_2 + a_3, a_2 + a_4, a_2 + a_5, a_3 + a_4, a_3 + a_5, a_4 + a_5\}$ be the set of all 2-sums of S . If any three of the 2-sums in A are all equal to one another, then this implies that not all the a_i are distinct, a contradiction. Hence if $|\sum_2 S| \leq 6$, then there must be at least 4 pairwise disjoint equalities among the 2-sums. Since there are four distinct a_i 's in each of the four equalities, it follows by the pigeonhole principle that one a_i must occur in all 4 equalities, say a_1 . Thus, since $a_1 + a_2 \neq a_1 + a_5$, it follows w.l.o.g. that the equalities in (9) and (10) hold. Furthermore, one of the equalities in (11) and one of the equalities in (12) hold as well.

$$a_1 + a_2 = a_3 + a_4 \tag{9}$$

$$a_1 + a_5 = a_2 + a_3 \tag{10}$$

$$a_1 + a_3 = a_2 + a_4, \quad a_1 + a_3 = a_2 + a_5, \quad a_1 + a_3 = a_4 + a_5 \tag{11}$$

$$a_1 + a_4 = a_2 + a_3, \quad a_1 + a_4 = a_2 + a_5, \quad a_1 + a_4 = a_3 + a_5. \tag{12}$$

Subsequently, we will refer to an equation in a numbered line by the number of the line followed by a letter from $abc\dots$ in lexicographic order, e.g. (11) a , (11) b and (11) c correspond to the equations $a_1 + a_3 = a_2 + a_4$, $a_1 + a_3 = a_2 + a_5$ and $a_1 + a_3 = a_4 + a_5$, respectively. From (9) and (10) it follows that

$$2a_2 = a_4 + a_5. \tag{13}$$

Observe that (12) a cannot hold, since if it does, then together with (9) and (13), it will imply that $a_4 = a_5$, a contradiction. Thus either (12) b or (12) c holds. If (12) b holds, then together with (9) and (10), equalities (14) (a) , (14) (b) and (14) (c) are implied; and in turn (14) a and (14) (b) imply (14) (d) .

$$2a_5 = a_3 + a_4, \quad 2a_1 = a_3 + a_5, \quad 2a_2 + a_3 = 2a_1 + a_4, \quad a_4 + 2a_1 = 3a_5 \tag{14}$$

If (12) c holds, then together with (9) and (10), equalities (15) (a) , (15) (b) , (15) (c) and (15) (d) are implied; and in turn (15) a and (15) (b) imply (16).

$$2a_4 = a_2 + a_5, \quad 2a_5 = a_2 + a_4, \quad 2a_3 + a_5 = 2a_1 + a_2, \quad 2a_1 + a_4 = 2a_3 + a_2, \tag{15}$$

$$3a_5 = 3a_4. \quad (16)$$

We proceed by considering three cases, corresponding to each of the three equalities in (11).

Case 1: (11)*a* holds. Then (11)*a* and (9) imply (17)(*a*) and (17)(*b*).

$$2a_1 = 2a_4, \quad 2a_3 = 2a_2 \quad (17)$$

Suppose (12)*c* holds. Then (17)(*a*), (17)(*b*) and (15)*d* imply $3a_4 = 3a_2$, which, along with (16), (17)*a* and (17)*b*, implies the theorem with $h = 6$. Hence we may assume (12)*b* holds. Furthermore, (17)(*a*), (17)(*b*) and (14)*c* imply $3a_3 = 3a_4$; and (17)*a* and (14)*d* imply $3a_4 = 3a_5$. Thus from (17)(*a*), (17)(*b*) and $3a_3 = 3a_4 = 3a_5$, it follows that the theorem holds with $h = 6$.

Case 2: (11)*b* holds. Then (11)*b* and (10) imply $2a_3 = 2a_5$ and $2a_1 = 2a_2$, which, along with (14)*a*, implies $a_3 = a_4$, a contradiction, and which, along with (15)*c*, implies $3a_5 = 3a_2$. In the later case, we obtain the three equalities, $2a_3 = 2a_5$, $2a_1 = 2a_2$, $3a_5 = 3a_2$, which, along with (16), imply the theorem with $h = 6$.

Case 3: (11)*c* holds. Then (11)*c*, (10) and (9) imply (18)*a* and (18)*b*.

$$2a_3 = a_2 + a_5, \quad 2a_1 = a_2 + a_4 \quad (18)$$

Suppose that (12)*c* holds. Then (18)*a* and (15)*a* imply $2a_3 = 2a_4$; and (18)*b* and (15)*b* imply $2a_5 = 2a_1$. Furthermore, (15)*b* and (15)*c* imply $5a_5 + 2a_3 = 2a_1 + 2a_2 + a_4$, which, along with (18)*b* and $2a_3 = 2a_4$, implies $3a_2 = 3a_5$. Thus $2a_3 = 2a_4$, $2a_5 = 2a_1$, $3a_2 = 3a_5$ and (16) imply the theorem with $h = 6$. So we may assume (12)*b* holds. Then (18)*b* and (14)*b* imply $a_2 + a_4 = a_3 + a_5$; and we conclude in this case that there are at most 5 distinct 2-sums. Furthermore, $a_2 + a_4 = a_3 + a_5$ and (9) imply $2a_4 = a_5 + a_1$. Thus (18)*a*, (18)*b*, (14)*a*, (13), and $2a_4 = a_5 + a_1$ imply (19)(*a*), (19)(*b*) and (19)(*c*).

$$3a_4 + a_3 = 3a_5 + a_1, \quad 3a_3 + a_4 = 3a_5 + a_2, \quad 3a_2 = 2a_1 + a_5 \quad (19)$$

We proceed by combining (19)(*a*), (19)(*b*) and (19)(*c*) with (18), (13), and $2a_4 = a_5 + a_1$, yielding (20)*a*, (20)*b* and (20)*c*.

$$5a_4 = 4a_5 + 2a_1 - a_3, \quad 5a_3 = 4a_5 + 2a_2 - a_4, \quad 5a_2 = 2a_1 + 2a_5 + a_4 \quad (20)$$

Next (20)*a*, (20)*b* and (14)*c* imply $5a_4 = 5a_3$; and (20)*c* and (14)*d* imply $5a_2 = 5a_5$. Furthermore, (20)*a*, (14)*a*, and (14)*d* imply $5a_4 = 5a_5$. Therefore it follows that $\{a_2, a_3, a_4, a_5\}$ are four elements

from a coset $\alpha + H$, where H is a subgroup of \mathbb{Z}_m of cardinality 5. Then it can be easily verified that a_1 is the fifth element of $\alpha + H$, as otherwise $|\sum_2 S| > 5$, contradicting the fact that there are at most five distinct 2-sums. Thus the theorem holds with $h = 5$, completing the proof. \square

Theorem 4.1. *Let $m \geq 5$. Then $g(6, 5) = 8$, and if $m \neq 6$, then $g(m, 5) = 2m - 5$.*

Proof. For $m \leq 6$ the result follows from Theorem 2.8. Suppose S is zsf and $|S| = 2m - 5$. We may w.l.o.g. assume that 0 has the greatest multiplicity in S .

Case 1: The multiplicity of 0 in S is at most $m - 2$. Applying Conjecture 4.1 with $k = 5$ to all possible 5-sets of $\varphi(S)$ that include 0, we can either find a 5-set $A \subseteq \varphi(S)$ such that $|\sum_2 A| = |\sum_3 A| \geq 7$ and $0 \in A$, or else there exists a subgroup H of cardinality $h = 5$ or $h = 6$ such that $\varphi(S) \subseteq H$. In the latter case, $m \geq 10$, and so from Theorem 2.2 it follows that any subsequence with length $m + h - 1 \leq 2m - 5$ must contain an m -term zero-sum subsequence, a contradiction. So $|\sum_3 A| \geq 7$. In view of the assumption of the case and Proposition 2.1, there exists an $(m - 3)$ -set partition P of $S \setminus A$ with $m - 7$ sets of cardinality two. Applying Theorem 2.7 to $S \setminus A$, and using $|\sum_3 A| \geq 7$, we obtain an m -term zero-sum subsequence of S , provided conclusion (i) of Theorem 2.7 holds. Hence we are done for $m \leq 8$.

So assume that conclusion (ii) of Theorem 2.7 holds with coset $\alpha + H$ of index a , and w.l.o.g. assume $\alpha = 0$. Let P be the $(m - 3)$ -set partition implied by conclusion (ii) of Theorem 2.7. Applying Proposition 2.2(i) followed by Proposition 2.2(ii) to P we obtain an $(\frac{m}{a} - 1)$ -set partition P' of a subsequence Q of $S \setminus A$ of length at most $2\frac{m}{a} - 2$, whose sumset is also H . Then there exists a subsequence R of $S \setminus A$ of length $a - 1$ whose terms are from H and are not used in P' . We can apply Theorem 2.1 to a subsequence of $S \setminus \{Q \cup R\}$ of length $m - \frac{m}{a} + 1$ with its terms considered as elements from \mathbb{Z}_m/H to obtain a subsequence T of $S \setminus \{Q \cup R\}$ whose sum is an element of H and of length r , where r satisfies $m - \frac{m}{a} - a + 2 \leq r \leq m - \frac{m}{a} + 1$. Since the sumset of P' is H , we can find $\frac{m}{a} - 1$ terms from P' which along with T and an appropriate number of terms from R gives an m -term subsequence with sum zero.

Case 2: The multiplicity of 0 in S is $m - 1$. Let T' be a subsequence of S that consists of 4 distinct nonzero residue classes and 3 zeros. In view of Proposition 2.1, it follows that there exists an $(m - 4)$ -set partition P' of $S \setminus T'$ with $m - 8$ cardinality two sets. Applying Theorem 2.7 to P and Theorem 2.9 to $\varphi(T') \setminus \{0\}$, we find an m -term zero-sum subsequence provided conclusion (i) of Theorem 2.7 holds. If conclusion (ii) of Theorem 2.7 holds instead, then since $m - 4 > a - 2$

implies $0 \in \alpha + H$, the arguments from the end of Case 1 complete the proof. \square

References

- [1] N. Alon and M. Dubiner, *Zero-sum sets of prescribed size*, Combinatorics, Paul Erdos is eighty, Vol. 1, Bolyai Soc. Math. Stud., János Bolyai Math. Soc., Budapest, 1993, 33–50.
- [2] N. Alon, M. B. Nathanson and I. Ruzsa, *The polynomial method and restricted sums of congruence classes*, J. Number Theory 56 (1996), no. 2, 404–417.
- [3] A. Bialostocki and P. Dierker, *On the Erdős-Ginzburg-Ziv theorem and the Ramsey numbers for stars and matchings*, Discrete Math. 110 (1992), no. 1–3, 1–8.
- [4] A. Bialostocki and M. Lotspeich, *Developments of the Erdős-Ginzburg-Ziv Theorem I*, Sets, graphs and numbers, Budapest, 1991, 97–117.
- [5] W. Brakemeier, *Eine Anzahlformel von zahlen modulo n* , Monatsh. Math. **85** (1978), no. 4, 277–282.
- [6] H. Cao and Z. Sun, *On sums of distinct representatives*, Acta Arith. 87 (1998), no. 2, 159–169.
- [7] Y. Caro, *Remarks on a zero-sum theorem*, J. Combin. Theory Ser. A 76 (1996), no. 2, 315–322.
- [8] H. Davenport, *On the addition of residue classes*, J. London Math. Society 10 (1935), 30–32.
- [9] J. A. Dias da Silva and Y. O. Hamidoune, *A note on the minimal polynomial of the Kronecker sum of two linear operators*, Linear Algebra Appl. 141 (1990), 283–287.
- [10] R. B. Eggleton and P. Erdős, *Two combinatorial problems in group theory*, Acta Arithmetica 21 (1972), 111–116.
- [11] P. Erdős, A. Ginzburg and A. Ziv, *Theorem in additive number theory*, Bull. Research Council Israel 10 F (1961), 41–43.
- [12] P. Erdős and R. L. Graham, *Old and new results in combinatorial number theory*, Monographie 28 de L’Enseignement Mathématique, Geneve, 1980.

- [13] C. Flores and O. Ordaz, *On the Erdős-Ginzburg-Ziv theorem*, Discrete Math. 152 (1996), no. 1-3, 321-324.
- [14] L. Gallardo, G. Grekos, L. Habsieger, F. Hennecart, B. Landreau and A. Plagne, *Restricted addition in \mathbb{Z}/n and an application to the Erdős-Ginzburg-Ziv problem*, J. London Math. Soc. (2) 65 (2002), no. 3, 513–523.
- [15] L. Gallardo and G. Grekos, *On Brakemeier’s variant of the Erdős-Ginzburg-Ziv problem*, Number theory (Liptovský Ján, 1999), Tatra Mt. Math. Publ. 20 (2000), 91-98.
- [16] L. Gallardo, G. Grekos and J. Pihko, *On a variant of the Erdős-Ginzburg-Ziv problem*, Acta Arith. 89 (1999), no. 4, 331–336.
- [17] W. D. Gao and Y. O. Hamidoune, *Zero sums in abelian groups*, Combin. Probab. Comput. 7 (1998), no. 3, 261-263.
- [18] W. D. Gao, *An addition theorem for finite cyclic groups*, Discrete Math. 163 (1997), no. 1-3, 257–265.
- [19] W. D. Gao, *Addition theorems for finite abelian groups*, J. Number Theory 53 (1995), no. 2, 241–246.
- [20] D. Grynkiewicz, *On a partition analog of the Cauchy-Davenport Theorem*. Preprint.
- [21] D. Grynkiewicz and R. Sabar, *Monochromatic and zero-sum sets of nondecreasing modified-diameter*. Preprint.
- [22] Y. O. Hamidoune, A. S. Lladó and O. Serra, *On restricted sums*, Combin. Probab. Comput. 9 (2000), no. 6, 513–518.
- [23] Y. O. Hamidoune, O. Ordaz and A. Ortuño, *On a combinatorial theorem of Erdős, Ginzburg and Ziv*, Combin. Probab. Comput. 7 (1998), no. 4, 403-412.
- [24] J. H. B. Kemperman, *On small sumsets in an abelian group*, Acta Math. 103 (1960), 63–88.
- [25] V. F. Lev, *Restricted set addition in groups. I. The classical setting*, J. London Math. Soc. (2) 62 (2000), no. 1, 27–40.

- [26] M. B. Nathanson, *Additive Number Theory. Inverse Problems and the Geometry of Sumsets*, *Graduate Texts in Mathematics*, 165, Springer-Verlag, New York, 1996.
- [27] R. Sabar, *On a family of inequalities and the Erdős-Ginzburg-Ziv Theorem*. Preprint.

Appendix

In the following table, Theorem 3.1 is used to list the values of $E(m, s)$ for all m and s satisfying $2m - 2 \geq s \geq \max\{2m - 8, 2m - \lfloor \frac{m}{4} \rfloor - 2\}$.

Table 1:

m	s	$E(m, s)$			
$m \geq 2$	$2m - 2$	$0^{m-1}1^{m-1}$			
$m \geq 4$	$2m - 3$	$0^{m-1}1^{m-3}2$			
$m \geq 8$	$2m - 4$	$0^{m-1}1^{m-5}2^2$	$(-1)0^{m-3}1^{m-3}2$	$0^{m-1}1^{m-4}3$	
$m \geq 12$	$2m - 5$	$0^{m-1}1^{m-7}2^3$ $0^{m-1}1^{m-5}4$	$(-1)0^{m-3}1^{m-5}2^2$	$0^{m-1}1^{m-6}23$	$(-1)0^{m-3}1^{m-4}3$
$m \geq 16$	$2m - 6$	$0^{m-1}1^{m-9}2^4$ $(-1)0^{m-3}1^{m-6}23$ $(-1)0^{m-3}1^{m-5}4$	$(-1)0^{m-3}1^{m-7}2^3$ $(-2)0^{m-4}1^{m-5}2^2$ $(-2)0^{m-4}1^{m-4}3$	$(-1)^2 0^{m-5}1^{m-5}2^2$ $0^{m-1}1^{m-7}24$ $0^{m-1}1^{m-6}5$	$0^{m-1}1^{m-8}2^33$ $0^{m-1}1^{m-7}3^2$
$m \geq 20$	$2m - 7$	$0^{m-1}1^{m-11}2^5$ $(-1)0^{m-3}1^{m-8}2^33$ $0^{m-1}1^{m-9}2^4$ $(-1)^2 0^{m-5}1^{m-5}4$ $(-2)0^{m-4}1^{m-5}4$	$(-1)0^{m-3}1^{m-9}2^4$ $(-2)0^{m-4}1^{m-7}2^3$ $(-1)0^{m-3}1^{m-7}24$ $0^{m-1}1^{m-8}25$ $0^{m-1}1^{m-7}6$	$(-1)^2 0^{m-5}1^{m-7}2^3$ $(-1)^2 0^{m-5}1^{m-6}23$ $(-1)0^{m-3}1^{m-7}3^2$ $0^{m-1}1^{m-8}34$	$0^{m-1}1^{m-10}2^33$ $0^{m-1}1^{m-9}23^2$ $(-2)0^{m-4}1^{m-6}23$ $(-1)0^{m-3}1^{m-6}5$
$m \geq 24$	$2m - 8$	$0^{m-1}1^{m-13}2^6$ $0^{m-1}1^{m-12}2^43$ $(-2)(-1)0^{m-6}1^{m-7}2^3$ $(-1)0^{m-3}1^{m-9}2^32$ $(-3)0^{m-5}1^{m-7}2^3$ $0^{m-1}1^{m-10}3^3$ $(-2)0^{m-4}1^{m-7}3^2$ $0^{m-1}1^{m-9}35$ $(-3)0^{m-5}16^{m-5}4$	$(-1)0^{m-3}1^{m-11}2^5$ $(-1)0^{m-3}1^{m-10}2^33$ $0^{m-1}1^{m-11}2^34$ $(-2)0^{m-4}1^{m-8}2^33$ $(-2)(-1)0^{m-6}1^{m-6}23$ $(-1)0^{m-3}1^{m-8}25$ $(-1)^2 0^{m-5}1^{m-6}5$ $0^{m-1}1^{m-9}4^2$ $0^{m-1}1^{m-8}7$	$(-1)^2 0^{m-5}1^{m-9}2^4$ $(-2)0^{m-4}1^{m-9}2^4$ $0^{m-1}1^{m-11}2^33^2$ $(-1)^2 0^{m-5}1^{m-7}24$ $0^{m-1}1^{m-10}2^5$ $(-1)0^{m-3}1^{m-8}34$ $(-3)0^{m-5}1^{m-6}23$ $(-1)0^{m-3}1^{m-7}6$	$(-1)^3 0^{m-7}1^{m-7}2^3$ $(-1)^2 0^{m-5}1^{m-8}2^33$ $(-1)0^{m-3}1^{m-9}2^4$ $(-1)^2 0^{m-5}1^{m-7}3^2$ $0^{m-1}1^{m-10}2^34$ $(-2)0^{m-4}1^{m-7}24$ $0^{m-1}1^{m-9}26$ $(-2)0^{m-4}1^{m-6}5$

Arie Bialostocki
Department of Mathematics
University of Idaho
Moscow, ID 83844, USA

Paul Dierker
Department of Mathematics
University of Idaho
Moscow, ID 83844, USA

David Gryniewicz
Mathematics 253-57
Caltech
Pasadena, CA 91125, USA

Mark Lotspeich
Department of Mathematics
Albertson College
Caldwell, ID 83605, USA