ACTA ARITHMETICA
129.4 (2007)

On Erdős–Ginzburg–Ziv inverse theorems

by

D. J. Grynkiewicz (Barcelona), O. Ordaz (Caracas),
M. T. Varela (Caracas), and F. Villarroel (Cumaná)

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 sequences over G modulo the equivalence relation 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 being infinite are needed in a sequence, it will be explicitly stated when the sequence is first introduced.

Now let G be an abelian group of order $m \geq 2$. The Erdős–Ginzburg–Ziv theorem states that every sequence in G of length $2m-1$ contains an m-term subsequence with zero sum [5]. 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 [7]; when $m - \lfloor m/4 \rfloor - 2 \leq k \leq m-2$, by Bialostocki, Dierker, Grynkiewicz, and Lotspeich in [2] (using a related result of Gao from [8]); and when $k \geq \lceil (m-1)/2 \rceil$, by Chen and Savchev 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 $S' \mid S$ indicates 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 the terms of S, unless S is

2000 *Mathematics Subject Classification*: Primary 11B75.

Key words and phrases: abelian group, Erdős–Ginzburg–Ziv theorem, zero-sum sequence.

Research of D. J. Grynkiewicz supported in part by the National Science Foundation, as an MPS-DRF postdoctoral fellow, under grant DMS-0502193.

Research of O. Ordaz supported in part by CRIPTOSUM CDCH project.

the empty sequence, in which case $\sigma(S) := 0$. Let

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

$$\Sigma_{\le t}(S) = \bigcup_{n=1}^{t} \Sigma_n(S), \quad \Sigma_{\ge t}(S) = \bigcup_{n=t}^{|S|} \Sigma_n(S), \quad \Sigma(S) = \Sigma_{\le |S|}(S).$$

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-cosets for some nontrivial subgroup $H \le G$. We will often write H_a for H if the index of H in G is a. If B is another subset of G, then the *sumset* $A + B$ is $\{a+b : a \in A,\, b \in B\}$. We will often identify a singleton set with its element for notational simplicity.

A sequence S is *squarefree* if $h(S) \le 1$, 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 that 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 [6]) shows that $D(G) \le |G|$.

1.2. *Results.* We have the following open problem:

Problem 1 ([10, 12]). *For an abelian group G of order $m \ge 2$ and a positive integer k, determine the exact value or a bound of*

$$h(G,k) = \min\{h(S) : S \in \mathcal{F}(G) \text{ with } |S| = |G| + k \text{ and } 0 \notin \Sigma_{|G|}(S)\}.$$

There are a few results pertaining to this problem. When G is cyclic of order m, we have $h(G,k) \ge k+1$ provided $m - \lfloor m/4 \rfloor - 2 \le k \le m-2$ (see [8]); $h(G,k) \ge k+1$ provided m is prime with $1 \le k \le m-2$ (see [11]); $h(G, m-2) = m-1$ (see [1] or [15]); and $h(G, m-3) = m-1$ (see [7]).

The main results in this paper confirm the following two conjectures.

Conjecture 1.1 ([9, Conjecture 6.9], [12]). *Let G be a cyclic group of order $m \ge 2$, and p the smallest prime divisor of m. Let $S \in \mathcal{F}(G \setminus 0)$ with $|S| = m$. If $h = h(S) \ge m/p - 1$, then $\Sigma_{\le h}(S) = \Sigma(S)$.*

Conjecture 1.1 was verified for cyclic groups of prime power order in [12]. The following example shows that we cannot hope, in general, for the equality of the conjecture to hold for smaller h. Indeed, the equality fails for $h \le m/p - 2$ and m composite when $m/p \ne 0,\ 1 \bmod h$, and, if $p = 2$,

$m/p \neq -1 \bmod h$. In particular, it does not hold when $h = m/p - 2$ 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 m/p. Let $h \leq m/p - 2$ be a positive integer such that $m/p \neq 0, 1 \bmod h$, and, if $p = 2$, such that $m/p \neq -1 \bmod h$ as well. Hence, in particular, $h > 1$. Let

$$t = \left\lceil \frac{m+h}{ph} \right\rceil = \frac{m+h+ph-\alpha}{ph}, \qquad \text{where } 0 < \alpha \leq ph.$$

Thus

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

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

$$\frac{m}{p} = (t-1)h - \frac{h-\alpha}{p}. \tag{2}$$

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

Suppose first that $\alpha < h$. Then $h - \alpha \equiv 0 \bmod p$ implies that $\alpha \leq h - p$. Hence (1) yields $m/p \leq (t-1)h - 1$, whence $h \leq m/p - 2$ forces $t \geq 3$. Thus let $x \in 1 + H$ and $x' \in (t-2) + H$ be distinct elements. Note that

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

Thus if $(t-2)h + \alpha + 1 < m/p$, 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 by (2) we can assume 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 yield $p < 2$), whence $m/p = (t-1)h - 1$ in view of (2). Consequently, $m/p \equiv -1 \bmod h$ and $p = 2$, contradicting the assumptions on h.

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

$$(t-1)h + 1 < \frac{m}{p}, \tag{3}$$

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 $m/p \equiv 0$ or $1 \bmod h$, contradicting the assumptions on h, and completing the example.

Conjecture 1.2 ([9, Conjecture 7.6], [12]). *Let G be a cyclic group of order $m \geq 2$, and p the smallest prime divisor of m. Let k be an integer such that $k \geq m/p - 1$, and let $S \in \mathcal{F}(G)$ with $|S| = m + k$. If $0 \notin \Sigma_m(S)$, then $h(S) \geq k + 1$.*

Conjecture 1.2 was verified for cyclic groups of prime power order in [12]. The following example shows we cannot hope, in general, for the bound $h(S) \geq k + 1$ of Conjecture 1.2 to be true for smaller k. Indeed, the bound fails whenever

$$\frac{m-d}{(t-1)d} > k \geq \frac{m+1}{td-2} \tag{4}$$

for integers $t, d \geq 2$ with $d \mid m$. In particular, taking $d = p$ and $t = 2$, we see that for $k = m/p - 2$ and $m \geq 27$ composite and odd, the bound of Conjecture 1.2 does not hold. Thus, though it appears the bound on k for $p = 2$ could be improved, in all other cases it is tight.

Let $G = \mathbb{Z}/m\mathbb{Z}$, let $H \leq G$ be the subgroup of index m/d, let W be the sequence consisting of all elements of $H \cup (1 + H) \cup \cdots \cup ((t-1) + H)$, each with multiplicity k, and let W' be the subsequence consisting of all elements of $(1 + H) \cup \cdots \cup ((t-1) + H)$, each with multiplicity k. Assume (4) holds. Hence $t \leq m/d - 1$ and

$$|W| = tdk \geq m + 2k + 1, \tag{5}$$

$$|W'| = (t-1)dk < m - d. \tag{6}$$

Note that $\Sigma_{\leq k}(W) \subseteq \{0, 1, \ldots, k(t-1)\} + H$. Furthermore, (4) implies that $k(t-1) < m/d - 1$. We proceed to define a subsequence $S \mid W$ with

$|S| = m + k$ and $\sigma(S) \in \{k(t-1)+1, k(t-1)+2, \dots, m/d-1\} + H$, which is disjoint from $\Sigma_{\le k}(W)$ and thus also from $\Sigma_k(S)$. Note that such a subsequence will have $h(S) \le h(W) \le k$ and $\sigma(S) \notin \Sigma_k(S) = \Sigma_{|S|-m}(S)$. 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 $\sigma(W) \equiv \alpha \bmod (m/d)$ with $0 \le \alpha \le m/d - 1$. If $\alpha \ge k(t-1)+1$, then in view of (5) and (6) we can find a subsequence $S \mid W$ of length $m+k$ obtained by removing an appropriate number of terms all contained in H; hence $\sigma(S)+H = \sigma(W)+H = \alpha+H \subseteq \{k(t-1)+1, \dots, m/d-1\}+H$ and $|S| = m+k$, yielding a subsequence with the desired properties. Therefore we may assume $\alpha \le k(t-1)$. Hence $\lceil(\alpha+1)/(t-1)\rceil \le k+1 \le kd$. In this case, we can remove $\lceil(\alpha+1)/(t-1)\rceil - 1$ terms from W contained in $(t-1)+H$, and one appropriately chosen additional term contained in $(1+H) \cup \cdots \cup ((t-1)+H)$, to obtain a subsequence $S' \mid W$ with $\sigma(S') \in m/d - 1 + H$. In view of (5) and $\lceil(\alpha+1)/(t-1)\rceil \le k+1$, it follows that $|S'| \ge m+k$. Thus, as in the previous case, we can remove an appropriate number of terms from S' all contained in H to get a subsequence $S \mid S'$ with $|S| = m+k$ and $\sigma(S) + H = \sigma(S') + H' = m/d - 1 + H$, yielding a subsequence with the desired properties.

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

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

$$\Sigma_{\ge t+1}(S) \cap \Sigma_{\le h+t}(S) = \Sigma(S).$$

(i) $h + t \ge m/p - 1$,
(ii) $\Sigma(S) \ne G$ *and* $m = pq$,
(iii) $\Sigma(S) \ne G$ *and* $h + t \ge m/pq + q - 3$.

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 $|S| \ge m + \max\{h(S), m/p-1\}$, 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 $h(G,k) \ge k+1$ for every G with $|G| = m$ and $k \ge m/p - 1$.

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 the 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 $A = A_1, \dots, A_n$ if and only if $|S| \ge n$ and $h(S) \le n$. Furthermore, if S has an n-setpartition, then S has an n-setpartition $B = B_1, \dots, B_n$ with $\big| |B_i| - |B_j| \big| \le 1$ 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 $A_1, \dots, A_n \subseteq \mathbb{Z}/p\mathbb{Z}$ are nonempty with p prime, then*

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

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 $m \ge 2$, let $S \in \mathcal{F}(G)$, let $S' \mid S$, let $P = P_1, \dots, P_n$ be an n-setpartition of S', and let p be the smallest prime divisor of m. If $n \ge \min\{m/p - 1,\ (|S'| - n + 1)/p - 1\}$, then either:*

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

$$\Big|\sum_{i=1}^{n} A_i\Big| \ge \min\{m,\ |S'| - n + 1\},$$

(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*

$$e \le \min\Big\{a - 2,\ \Big\lfloor \frac{|S'| - n}{|H_a|} \Big\rfloor - 1\Big\},$$

and an n-setpartition $B = B_1, \dots, B_n$ of a subsequence $S_0'' \in \mathcal{F}(\alpha + H_a)$ with $S_0'' \mid S$, $|S_0''| \le n + |H_a| - 1$, 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 $f(a) = M/a + a$ for $M,\ a > 0$ (and usually M will be of the form m or m/x) is maximized at a boundary value of a. Thus for example, if $a \mid m$, then $m/a + a \le m/p + p$. We begin by showing all three cases imply the following claim. Note this completes the case of $|G|$ 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* $e \le a-2$ *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 $\Sigma_{h+t}(S0^{h-1}) = \Sigma_{\ge t+1}(S) \cap \Sigma_{\le h+t}(S)$. Since $h \ge h(S)$ and $|S| \ge m+t \ge t+1$, Proposition 1.3 yields an $(h+t)$-setpartition P of $S0^{h-1}$. Since $h+t \ge m/p-1$, we can apply Theorem 1.4 to P. If (i) of Theorem 1.4 holds, then

$$|\Sigma_{h+t}(S0^{h-1})| \ge \min\{m, (|S|+h-1)-(h+t)+1\} = m = |G|.$$

Hence $\Sigma(S) \subseteq G = \Sigma_{h+t}(S0^{h-1}) = \Sigma_{\ge t+1}(S) \cap \Sigma_{\le h+t}(S) \subseteq \Sigma(S)$ holds trivially. So we may assume that (ii) of Theorem 1.4 holds. Consequently, all but $e \le a-2$ terms of $S0^{h-1}$ are from $\alpha + H_a$, where H_a is a proper, nontrivial subgroup of index a.

Suppose that $0 \notin \alpha + H_a$. As there are only $e \le a-2$ terms of $S0^{h-1}$ outside $\alpha + H_a$, it follows that $h-1 \le a-2$. Since $h \ge h(S)$, $|S| \ge m+t$, and $e \le a-2$, it follows that

$$\begin{aligned} m+t+h-1 &\le |S0^{h-1}| \le |H_a|h + e \\ &\le \frac{m}{a}\,h + a - 2 \le \frac{m}{a}\,(a-1) + a - 2. \end{aligned}$$

Thus $h+t \le a - m/a - 1 \le m/p - 3$, contradicting (i). So we may assume $0 \in \alpha + H_a$, whence without loss of generality $\alpha = 0$. Furthermore, since (ii) of Theorem 1.4 holds for $S0^{h-1}$, it follows that $\Sigma_{h+t}(S_a 0^{h-1}) = H_a$, where S_a is the subsequence of terms of S from H_a. As $\nu_0(S_a 0^{h-1}) = h-1 < h+t$ and all terms of $S_a 0^{h-1}$ 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 $\Sigma(S) \ne G$.

Note that $\Sigma_{|S|}(S0^{|S|-1}) = \Sigma(S)$. In view of Proposition 1.3, $S0^{|S|-1}$ has an $|S|$-setpartition P. Since $|S| \ge m+t \ge m$, we can apply Theorem 1.4 to P. If (i) of Theorem 1.4 holds, then $|\Sigma(S)| = |\Sigma_{|S|}(S0^{|S|-1})| \ge \min\{m, 2|S| - 1 - |S| + 1\} = m$, whence $\Sigma(S) = G$, a contradiction. Therefore we can assume that (ii) of Theorem 1.4 holds. Thus there exists a proper, nontrivial subgroup H_a of index a, and $\alpha \in G$, such that all but $e \le a-2$ terms of $S0^{|S|-1}$ are from $\alpha + H_a$. Since $\nu_0(S0^{|S|-1}) = |S| - 1 \ge m-1 > a-2$, it follows that $0 \in \alpha + H_a$, whence we can assume $\alpha = 0$. Furthermore, $\Sigma(S_a) = H_a$ as before, completing the proof of the claim. ∎

Assume H_a is chosen to satisfy Claim 1 with minimal cardinality. Note that $|S_a| = |S| - e \ge m - e$. 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 $\Sigma_{\ge t+1}(S) \cap \Sigma_{\le h+t}(S) = \Sigma(S)$.

If $h \le a$, then

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

a contradiction. Therefore we can assume $h \ge a+1$.

Note that $|S| \ge m+t \ge m/2+t \ge m/a+a-2+t \ge m/a+t+e$. Hence $|S_a| \ge m/a+t$. As $\Sigma(S_a) = H_a$, it follows by a simple greedy algorithm that there exists a subsequence R of S_a with $|R| = m/a$ and $\Sigma(R) = H_a$. Since $|S_a| \ge m/a+t$, there exists a subsequence $T_a \mid S_a R^{-1}$ 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 m/a terms of R (and at least one), and at most $e \le a-2$ terms not in H_a, whence $\Sigma(S) = \Sigma_{\ge t+1}(S) \cap \Sigma_{\le m/a+t+a-2}(S)$. Consequently, we may assume

$$h \le \frac{m}{a}+a-3, \tag{7}$$

else the proof is complete.

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

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

a contradiction. Therefore we can assume $|S'_a| \ge h$. As $h(S) \le h$, Proposition 1.3 yields an h-setpartition $A = A_1, \ldots, A_h$ of S'_a with $||A_i|-|A_j|| \le 1$ for all i and j. Assume without loss of generality that $|A_1| \ge \cdots \ge |A_h|$. Let $\lfloor (m-a+2)/h \rfloor = (m-a+2-\epsilon)/h$. Then, since $|S'_a| = |S|-e-t \ge m-a+2$, it follows that

$$|A_i| \ge \frac{m-a+2-\epsilon}{h} \quad \text{for all } i, \tag{8}$$

$$|A_i| \ge \frac{m-a+2-\epsilon}{h}+1 > \frac{m-a+2}{h} \quad \text{for all } i \le \epsilon. \tag{9}$$

Let x be minimal such that $\sum_{i=1}^{x} |A_i| \ge m/a$ (it exists since $|S'_a| = |S_a|-t \ge m/a$). We proceed to show that

$$x \le \frac{mh/a}{m-a+2}+1. \tag{10}$$

If $x \le \epsilon$, then (9) implies that

$$x \le \left\lceil \frac{mh/a}{m-a+2} \right\rceil \le \frac{mh/a}{m-a+2}+1,$$

yielding (10). If $x > \epsilon$ then by (8) and (9),

$$x \le \left\lceil \frac{(m/a-\epsilon)h}{m-a+2-\epsilon} \right\rceil \le \frac{(m/a-\epsilon)h}{m-a+2-\epsilon}+1. \tag{11}$$

If (10) is false, then comparing with (11) yields $m < m/a + a - 2 \le m - 1$, a contradiction. Consequently, (10) always holds.

Suppose $h - e < x$. It follows from (10) and $e \le a - 2$ that

$$\left(1 - \frac{m/a}{m-a+2}\right)h \le a - 2. \tag{12}$$

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

$$a - 2 \ge \frac{1}{2}\, h. \tag{13}$$

In view of $h - e < x$, $e \le a - 2$, and $h \ge a + 1$, it follows that

$$a + 1 \le h \le x - 1 + e \le x + a - 3,$$

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

$$3m - 3a + 6 = 3(m - a + 2) \le \frac{m}{a}\,(2a - 4) = 2m - 4\,\frac{m}{a},$$

so that

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

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

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

Hence $h \ge m/2 + 2 = m/a + a$, contradicting (7). So we may assume $h - e \ge x$.

Let $S_a'' = A_1 \cdots A_x \cdots A_{h-e}$. In view of the definition of x, and since $h - e \ge x$, it follows that $|S_a''| \ge m/a$. Let B be the $(h-e+t)$-setpartition of $S_a'' T_a 0^{h-e-1}$ 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. Applying CDT to B, it follows that there are at least

$$|S_a''| + t + (h - e - 1) - (h - e + t) + 1 = |S_a''| \ge m/a$$

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

$$h - e + t - \nu_0(S_a'' T_a 0^{h-e-1}) = t + 1,$$

terms from $S_a'' T_a$, and at most e terms not in H_a. Hence $\Sigma_{\ge t+1}(S) \cap \Sigma_{\le h+t}(S) = \Sigma(S)$, as desired. So we can assume $|H_a| = m/a$ is not prime. Since

$0 < H_a < G$, it follows that m has at least three prime factors, which completes the proof of (ii). Consequently, since

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

both (i) and (iii) imply

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

Suppose $h - e + t \leq m/ap' - 2$, where p' is the smallest prime divisor of m/a. Then $e \leq a - 2$ implies that

$$h + t \leq \frac{m}{ap'} + a - 4. \tag{16}$$

If $a = p$, then $p' = q$, whence (16) implies that $h + t \leq m/pq + p - 4 \leq m/pq + q - 4$. Otherwise, since $|H_a|$ is composite, it follows that $q \leq a \leq m/pq$, whence, in view of $p \leq p'$ and (16),

$$h + t \leq \frac{m}{ap'} + a - 4 \leq \frac{m}{ap} + a - 4 \leq \frac{m}{qp} + q - 4.$$

In both cases we contradict (15). So we may assume that

$$h - e + t \geq \frac{m}{ap'} - 1. \tag{17}$$

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 (i) of Theorem 1.4 holds. Then there exists $S'' \mid S_a 0^{h-e-1}$ of length $|S''_a| + t + h - e - 1$ with an $(h - e + t)$-setpartition whose sumset has cardinality at least

$$\min\left\{\frac{m}{a}, |S''_a| + t + (h - e - 1) - (h - e + t) + 1\right\} = \min\left\{\frac{m}{a}, |S''_a|\right\} = \frac{m}{a}.$$

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, $h - e + t - t' \geq t + 1$. 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 in H_a. Hence $\Sigma(S) = \Sigma_{\geq t+1}(S) \cap \Sigma_{\leq h+t}(S)$, as desired. So we can assume (ii) of Theorem 1.4 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 $0 \notin \beta + H_{ka}$. 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) and $e \leq a - 2$, and $2 \leq a$, $k \leq m/2$, it follows that

$$\begin{aligned} m - 1 \leq m + \frac{m}{ap'} - 2 \leq m + t + h - e - 1 \leq |S0^{h-e-1}| \\ \leq |H_{ka}|h + e' + e \leq \frac{m}{ka}(k + e - 1) + k - 2 + e \end{aligned} \tag{18}$$

$$\leq \frac{m}{ka}(k+a-3)+k+a-4=\left(\frac{m}{a}+a\right)+\left(\frac{m}{k}+k\right)-3\,\frac{m}{ka}-4$$
$$\leq \left(\frac{m}{2}+2\right)+\left(\frac{m}{2}+2\right)-3\,\frac{m}{ka}-4=m-3\,\frac{m}{ka}\leq m-3,$$

a contradiction. So we may assume $0 \in \beta + H_{ka}$, whence without loss of generality $\beta = 0$.

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 (ii) of Theorem 1.4 holds for $S_a 0^{h-e-1}$, it follows that $\Sigma_{h-e+t}(S_{ka}0^{h-e-1}) = H_{ka}$, where S_{ka} is the subsequence of terms of S_a from H_{ka}. Hence, as $\nu_0(S_a 0^{h-e-1}) = h-e-1 < h-e+t$, 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). ■

3. Proof of Theorem 1.2. Since $|S| \geq m + m/p - 1$, let $|S| = m+k$ with $k \geq m/p - 1$. 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.

By translation we may assume 0 is the term with greatest multiplicity $h = h(S)$ in S. Since by hypothesis $h = h(S) \leq |S|-m = k$, let $t = k-h \geq 0$ and $S' = S0^{-h}$. Note that $|S'| = m+k-h = m+t$, and $h(S') \leq h(S) = h$. Since $h+t = k \geq m/p-1$, it follows that S' satisfies (i) of Theorem 1.1, 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' with sum z such that

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

Since $|SS'^{-1}| = h$, adding an appropriate number of zeros to T_z yields a k-term subsequence whose sum is z. Consequently, $\Sigma(S') \subseteq \Sigma_k(S)$. Since $S' = S0^{-h}$, it follows that $\Sigma_k(S) \setminus 0 \subseteq \Sigma(S')$. However, as $|S'| = m+t \geq m = |G| \geq D(G)$, it follows that $0 \in \Sigma(S')$ as well. Hence the above implies that

$$\Sigma(S') = \Sigma_k(S).$$

As $\Sigma(S')$ 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. ■

Acknowledgments. We thank the referee for his helpful suggestions, and for pointing out an inaccuracy in the original lower bound examples.

References

[1] A. Bialostocki and P. Dierker, *On the Erdős–Ginzburg–Ziv theorem and the Ramsey numbers for stars and matchings*, Discrete Math. 110 (1992), 1–8.

[2] A. Bialostocki, P. Dierker, D. Grynkiewicz and M. Lotspeich, *On some developments of the Erdős–Ginzburg–Ziv Theorem II*, Acta Arith. 110 (2003), 173–184.

[3] F. Chen and S. Savchev, *Long n-zero-free sequences in finite cyclic groups*, Discrete Math., to appear.

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

[5] P. Erdős, A. Ginzburg and A. Ziv, *Theorem in the additive number theory*, Bull. Res. Council Israel 10F (1961), 41–43.

[6] P. Erdős and R. L. Graham, *Old and New Results in Combinatorial Number Theory*, Monograph. L'Enseign. Math. 28, Univ. de Genève, Geneva, 1980.

[7] C. Flores and O. Ordaz, *On sequences with zero sum in abelian group*, in: Volumen de homenaje al Dr. Rodolfo A. Ricabarra, Vol. Homenaje 1, Univ. Nac. del Sur, Baha Blanca, 1995, 99–106.

[8] W. Gao, *An addition theorem for finite cyclic groups*, Discrete Math. 163 (1997), 257–265.

[9] W. Gao and A. Geroldinger, *Zero-sum problems in finite abelian groups: A survey*, Expo. Math. 24 (2006), 337–369.

[10] W. Gao, A. Panigrahi and R. Thangadurai, *On the structure of p-zero-sum free sequences and its application to a variant of Erdős–Ginzburg–Ziv theorem*, Proc. Indian Acad. Sci. Math. Sci. 115 (2003), 67–77.

[11] W. Gao and R. Thangadurai, *A variant of Kemnitz conjecture*, J. Combin. Theory Ser. A 107 (2004), 69–70.

[12] W. D. Gao, R. Thangadurai and J. Zhuang, *Addition theorems on the cyclic groups of order pl*, Discrete Math., to appear.

[13] D. Grynkiewicz, *On a partition analog of the Cauchy–Davenport theorem*, Acta Math. Hungar. 107 (2005), 161–174.

[14] —, *On a conjecture of Hamidoune for subsequence sums*, Integers 5 (2005), no. 2, A7, 11 pp. (electronic).

[15] T. Yuster and B. Peterson, *A generalization of an addition theorem for solvable groups*, Canad. J. Math. 3 (1984), 529–536.

Departamento de Matemática Aplicada IV
Universitat Politècnica de Catalunya
Campus Nord, Edifici C3
C. Jordi Girona, 1-3
08034 Barcelona, Spain
E-mail: diambri@hotmail.com

Departamento de Matemáticas
y Centro ISYS
Facultad de Ciencias
Universidad Central de Venezuela
Ap. 47567
Caracas 1041-A, Venezuela
E-mail: flosav@cantv.net

Departamento de Matemáticas Puras y Aplicadas
Universidad Simón Bolivar
Ap. 89000
Caracas 1080-A, Venezuela
E-mail: mtvarela@usb.ve

Departamento de Matemáticas
Escuela de Ciencias, Núcleo Sucre
Universidad de Oriente
Cumaná, Venezuela
E-mail: feliciavillarroel@cantv.net

Received on 4.8.2006
and in revised form on 3.7.2007 (5254)