ACTA ARITHMETICA
148.4 (2011)

Two conjectures on an addition theorem

by

XIANGNENG ZENG and PINGZHI YUAN (Guangzhou)

1. Introduction. In this paper, we follow the notation of [10]; we recall some key notation in the next section.

In 1961, Erdős–Ginzburg–Ziv [4] proved the following theorem.

THEOREM 1.1 (EGZ Theorem). *Let G denote a cyclic group of order n and $S \in \mathcal{F}(G)$ be a sequence of length $2n-1$ over G. Then $0 \in \sum_n(S)$.*

The length $2n-1$ is sharp in view of the example $S = 0^{n-1}g^{n-1}$, where g is a generator of G.

The inverse problem to the EGZ Theorem is to investigate the structure of S satisfying $0 \notin \sum_n(S)$. Let $k = |S| - n$. Peterson and Yuster [17] solved the case of $k = n-2$. Bialostocki and Dierker [1] and Flores and Ordaz [5] solved the case of $k = n-3$. Gao [6] solved the case of $n - \lfloor (n+1)/4 \rfloor - 1 \le k \le n-2$. Gao et al. [7] solved the case when n is a prime and $n - \lfloor (n+1)/3 \rfloor - 1 \le k \le n-2$. Finally, Savchev and Chen [18] gave a structural description of sequences S of length $n+k$ with $\lfloor (n-1)/2 \rfloor \le k \le n-2$; this description does not carry over to smaller values of k (see [9, 5.1.16 and 5.1.17]). Therefore Gao, Thangadurai and Zhuang considered in [8] the maximal multiplicity of sequences S with $0 \notin \sum_n(S)$ and stated the following two conjectures.

CONJECTURE 1.2 ([8]). *Let G be a cyclic group of order $n > 2$, $k \in [1, n-2]$ and $S \in \mathcal{F}(G)$ a sequence of length $|S| = n+k$. If $\mathsf{h}(S) \le k$, then $0 \in \sum_n(S)$.*

CONJECTURE 1.3 ([8]). *Let G be a cyclic group and $S \in \mathcal{F}(G \setminus \{0\})$ a sequence of length $|S| = |G|$. Then $\sum(S) = \sum_{\le \mathsf{h}(S)}(S)$.*

Many authors verified both conjectures for large k and $\mathsf{h}(S)$ respectively. In [8], the proposers proved both conjectures when $n = p^l$ is a prime power

2010 *Mathematics Subject Classification*: Primary 11B50; Secondary 11B75.
Key words and phrases: zero-sum problems, EGZ theorem, Kneser's theorem, zero-sum free sequences.

DOI: 10.4064/aa148-4-5

and $k \geq n/p - 1$ ($\mathsf{h}(S) \geq n/p - 1$, respectively). Cao [2] verified Conjecture 1.2 when $n = p^\alpha q^\beta$ and $k \geq n/p-1$, where p, q are primes and $p < q$. DeVos, Goddyn and Mohar [3] proved the conjectures for any abelian group G when $k \geq |G|/p-1$ ($\mathsf{h}(S) \geq |G|/p-1$, respectively), where p is the smallest prime divisor of $|G|$.

In this paper, we obtain the following result on Conjecture 1.2.

Theorem 1.4. *Let $n > 2$. Conjecture 1.2 holds for $k \geq n/q - 1$, where q is the smallest divisor of n with $q > 2$.*

Theorem 1.4 improves the related result of DeVos, Goddyn and Mohar [3] for cyclic groups of even order n. We present the proof in Section 4. Also we will show that the bound on k is sharp (see the remark after the proof).

For Conjecture 1.3, we have the following result.

Theorem 1.5. *Let G be a cyclic group of order $n > 2$, $H \leq G$ a subgroup of G, and B_H the set of all sequences $S \in \mathcal{F}(G \setminus \{0\})$ with $|S| = |G|$ and $\mathrm{Stab}(\sum_{\leq \mathsf{h}(S)}(S)) = H$.*

(i) *If $S \in B_H$ with $\mathsf{h}(S) \geq |G/H| - 1$, then $\sum_{\leq \mathsf{h}(S)}(S) = \sum(S)$.*
(ii) *If $S \in B_H$ with $\mathsf{h}(S) \in [2, |G/H|]$ and $|G/H| = \mathsf{h}(S)t + r$ with $r \in [0, \mathsf{h}(S) - 1]$, then*

$$2 \leq r \leq \mathsf{h}(S) - \frac{2}{|H| - 1}.$$

(iii) *Let $k \in [2, |G/H|]$ and set $|G/H| = kt + r$ where $r \in [0, k-1]$ is the remainder of $|G/H|$ divided by k. Suppose $2 \leq r \leq k - 2/(|H|-1)$. Then there exists a sequence $S \in B_H$ such that $\mathsf{h}(S) = k$ and $\sum_{\leq \mathsf{h}(S)}(S) \neq \sum(S)$.*

In Theorem 1.5, part (i) implies that if $\mathsf{h}(S)$ is sufficiently large compared with $|G/H|$, then $\sum_{\leq \mathsf{h}(S)}(S) = \sum(S)$, while (ii) and (iii) imply that if $S \in B_H$ and $\mathsf{h}(S)$ is small, then it is possible that $\sum_{\leq \mathsf{h}(S)}(S) \neq \sum(S)$. Also, the theorem shows that $\sum_{\leq \mathsf{h}(S)}(S) = \sum(S)$ holds for special n and $\mathsf{h}(S)$ without any assumptions on the structure of S. For example, let $n = p^l$ be a prime power and $\mathsf{h}(S) = p$. Then the remainder of $|G/H|$ divided by $\mathsf{h}(S)$ is always 0, which implies that $\mathsf{h}(S) \geq |G/H| - 1$ and $\sum_{\leq \mathsf{h}(S)}(S) = \sum(S)$ by the theorem.

Since Conjecture 1.3 is not always true, the length $|S|$ or the restricted length $\mathsf{h}(S)$ may not be large enough. This suggests investigating how large $|S|$ or $\mathsf{h}(S)$ should be to have $\sum_{\leq \mathsf{h}(S)}(S) = \sum(S)$. We define $\mathsf{L}(G)$ to be the smallest integer $l \in \mathbb{N}_0$ such that every sequence $S \in \mathcal{F}(G \setminus \{0\})$ of length $|S| \geq l$ satisfies $\sum_{\leq \mathsf{h}(S)}(S) = \sum(S)$. We have

THEOREM 1.6. *Let $n \geq 16$ and G be a cyclic group of order n.*

(i) *If n is a prime, then $\mathsf{L}(G) = n$.*
(ii) *If n is a composite number, then $\mathsf{L}(G) = 2n - 4a - b + 3 \geq n + 1$, where the pair $(a, b) \in \mathbb{N}^2$ satisfies $n = ab$ and $|4a + b|$ is minimal.*

THEOREM 1.7. *Let $n \geq 16$ and G be a cyclic group of order n. Let $S \in \mathcal{F}(G \setminus \{0\})$ be a sequence of length $|S| = n$.*

(i) *If n is a prime, then $\sum_{\leq \mathsf{h}(S)}(S) = \sum(S)$ and the restricted length $\mathsf{h}(S)$ is the best possible.*
(ii) *If n is a composite number, then $\sum_{\leq 2\mathsf{h}(S)-2}(S) = \sum(S)$.*

2. Notation. Let $a \in \mathbb{R}$. Then $\lfloor a \rfloor$ denotes the maximal integer not exceeding a, and $\lceil a \rceil$ denotes the minimal integer not less than a. Let $a, b \in \mathbb{R}$. Then $[a, b] = \{x \in \mathbb{Z} : a \leq x \leq b\}$ denotes the integers between a and b.

Let G be an abelian group and H a subgroup of G. Let $\Phi_H : G \to G/H$ be the natural homomorphism. Let A, B be subsets of G. $A + B = \{a + b : a \in A, b \in B\}$ denotes the *sum set* of A and B and $\Phi_H(A)$ denotes the image of A, that is, $\Phi_H(A) = \{\Phi_H(g) : g \in A\}$.

We say A is *H-periodic* if A is a union of H-cosets (i.e. $A + H = A$), where H is a subgroup of G, referred to as the *period*. Note that the trivial subgroup $\{0\}$ is a period of every A. If A is H-periodic for some non-trivial subgroup H, then A is *periodic*, and otherwise A is *aperiodic*. Let $\mathrm{Stab}(A) = \{g \in G : A + g = A\}$ denote the *stabilizer* of A. By the definition, any period of A is a subgroup of $\mathrm{Stab}(A)$ and thus $\mathrm{Stab}(A)$ is the maximal period of A.

A *quasi-periodic decomposition* of A with *quasi-period* H, where H is a non-trivial subgroup of G, is a partition $A = A_1 \cup A_0$ such that $A_1 \cap A_0 = \emptyset$, $A_1 + H = A_1$ and $A_0 \subset a_0 + H$ for some $a_0 \in G$. Here A_1 or A_0 may be empty. Note that every A has a quasi-periodic decomposition with $H = G$ and $A_1 = \emptyset$. The set A is *quasi-periodic* if A_1 is not empty in some quasi-periodic decomposition $A = A_1 \cup A_0$.

Let A be a set. Then the free abelian monoid with basis A, written multiplicatively, is denoted by $\mathcal{F}(A)$.

Let G be an additive finite abelian group, $G_0 \subset G$ a subset and $\mathcal{F}(G_0)$ the free abelian monoid over G_0. An element $S = a_1 \cdot \ldots \cdot a_l = \prod_{g \in G_0} g^{\mathsf{v}_g(S)} \in \mathcal{F}(G_0)$ is called a *sequence* over G_0, where $\mathsf{v}_g(S)$ is the *multiplicity* of g in S. Let $|S| = l = \sum_{g \in G_0} \mathsf{v}_g(S)$ denote the *length* of S, $\mathsf{h}(S) = \max\{\mathsf{v}_g(S) : g \in G_0\}$ the *maximal multiplicity* of S and $\mathrm{supp}(S) = \{g : \mathsf{v}_g(S) > 0\}$ the *support* of S. We say that T is a *subsequence* of S if $T \mid S$ in $\mathcal{F}(G_0)$.

We write

$$\sigma(S) = \sum_{i=1}^{|S|} a_i, \text{ the sum of } S,$$

$$\textstyle\sum_k(S) = \{\sigma(T) : T \mid S \text{ with } |T| = k\}, \text{ the set of } k\text{-term subsums of } S,$$

$$\textstyle\sum_{\le k}(S) = \bigcup_{j\in[1,k]} \sum_j(S),$$

$$\textstyle\sum(S) = \sum_{\le |S|}(S), \text{ the set of all subsums of } S.$$

Any map $\phi : A \to B$ can be naturally extended to $\phi : \mathcal{F}(A) \to \mathcal{F}(B)$. For example, $\Phi_H(S) = \Phi_H(a_1)\cdots\Phi_H(a_{|S|})$.

We denote by $\mathsf{D}(G)$ the *Davenport constant* of G, defined as the smallest integer $l \in \mathbb{N}$ such that every sequence $S \in \mathcal{F}(G)$ of length $|S| \ge l$ satisfies $0 \in \sum(S)$ (see Chapter 5 in [10] for some of its main properties).

Let G be an additive abelian group. We need the concept of setpartitions introduced by D. Grynkiewicz in [11] (see also [15, p. 562]). Let P denote the set of non-empty finite subsets of G. The elements of $\mathcal{F}(P)$ will be called *setpartitions* (over G), and an *n-setpartition* $\mathcal{A}$ (over G) is an element of $\mathcal{F}(P)$ of length n (in other words, $\mathcal{A}$ is a formal product of n non-empty subsets of G). In particular, a sequence over G can be viewed as a setpartition. We denote by $|\mathcal{A}|$ the *length* of $\mathcal{A}$. We call $\mathcal{B}$ a *sub-setpartition* of $\mathcal{A}$ if $\mathcal{B} \mid \mathcal{A}$ in $\mathcal{F}(P)$.

Let $\mathcal{A} = A_1 \cdots A_n \in \mathcal{F}(P)$ be an n-setpartition over G. We set

$$\sigma(\mathcal{A}) = \sum_{i=1}^{n} A_i, \qquad \textstyle\sum_k^{\cup}(\mathcal{A}) = \{x \in \sigma(\mathcal{B}) : \mathcal{B} \mid \mathcal{A} \text{ with } |\mathcal{B}| = k\}.$$

3. Preliminary results. For the proofs, we need the following results.

THEOREM 3.1 (Kneser's Theorem [16]). *Let G be an abelian group, and let $A_1, \ldots, A_n$ be a collection of finite subsets of G. If $H = \mathrm{Stab}(\sum_{i=1}^n A_i)$, then*

$$\Big|\sum_{i=1}^{n} \Phi_H(A_i)\Big| \ge \sum_{i=1}^{n} |\Phi_H(A_i)| - n + 1.$$

THEOREM 3.2 (DeVos–Goddyn–Mohar Theorem (DGM Theorem) [3]). *Let G be an abelian group, $\mathcal{A} = A_1 \cdots A_m$ a setpartition over G, and $n \in \mathbb{N}$ with $n \le m$. Set $H = \mathrm{Stab}(\sum_n^{\cup}(\mathcal{A}))$. Then*

$$\textstyle|\sum_n^{\cup}(\mathcal{A})| \ge |H|\Big(\displaystyle\sum_{Q\in G/H} \min\{n, |\{i \in [1,m] : A_i \cap Q \ne \emptyset\}|\} - n + 1\Big).$$

Also we need the Kemperman Structure Theorem which was first proved in [16]. We will use the notation from [14], where substantial progress was made on this classical result.

Definition 3.3. The pair (A, B) of non-empty finite subsets of the abelian group G is said to be a *critical pair* if $|A + B| = |A| + |B| - 1$.

Let G be an abelian group, $A, B \subseteq G$ finite non-empty subsets of G, and $g \in G$. We denote the number of expressions of g in $A + B$ by $\mathsf{r}_{A,B}(g) = |A \cap (g - B)| = |\{(a, b) : a \in A,\, b \in B,\, a + b = g\}|$. We say that g is the *unique expression element* if $\mathsf{r}_{A,B}(g) = 1$.

Definition 3.4. We call a pair (A, B) of non-empty, finite subsets of an abelian group G an *elementary pair* if one of the following conditions (I)–(IV) holds true.

(I) $|A| = 1$ or $|B| = 1$.
(II) $|A| \geq 2$, $|B| \geq 2$ and A and B are arithmetic progressions with common difference d, where the order of d is at least $|A| + |B| - 1$.
(III) $A \subset a + H$, $B \subset b + H$ (for some $a \in A$, $b \in B$ and $H \leq G$), $|A| + |B| = |H| + 1$ (thus $A + B = a + b + H$), and $a + b$ is the only unique expression element in $A + B$.
(IV) $A \subset a + H$, $B \subset b + H$ (for some $a \in A$, $b \in B$ and $H \leq G$), $A + B$ contains no unique expression elements, A and B are aperiodic, and $A = g - (b + H) \setminus B$ (for some $g \in G$).

Theorem 3.5 (Kemperman Structure Theorem (KST)). *Let A and B be finite, non-empty subsets of an abelian group G. Then*

- $|A + B| = |A| + |B| - 1$, *and either $A + B$ is aperiodic or contains a unique expression element*

if and only if there exist quasi-periodic decompositions $A = A_1 \cup A_0$ and $B = B_1 \cup B_0$ with common quasi-period H, and A_0 and B_0 non-empty, such that:

(i) $\mathsf{r}_{\Phi_H(A),\Phi_H(B)}(c) = 1$, *where* $c = \Phi_H(A_0) + \Phi_H(B_0)$,
(ii) $|\Phi_H(A) + \Phi_H(B)| = |\Phi_H(A)| + |\Phi_H(B)| - 1$,
(iii) $A_1 + H = A_1$, $B_1 + H = B_1$,
(iv) (A_0, B_0) *is an elementary pair,*
(v) *if* $\mathsf{r}_{A,B}(a + b) = 1$ *where* $a \in A$ *and* $b \in B$, *then* $a \in A_0$ *and* $b \in B_0$.

Condition (v) was not stated in Kemperman's original paper, but can be derived from KST as shown in [12] and [13].

4. Proof of Theorem 1.4.

For the proof of Theorem 1.4, we need some lemmas.

Lemma 4.1. *Let G be an abelian group of order n and $S \in \mathcal{F}(G)$ with $|S| = n + k$. If $\mathsf{h}(S) \leq k$, then $\sum_n(S)$ is periodic.*

Proof. Since $\sum_n(S) = \sigma(S) - \sum_k(S)$, $\sum_n(S)$ and $\sum_k(S)$ have the same stabilizer. If $\mathsf{h}(S) \le k$ and $\sum_n(S)$ is aperiodic, then by DGM Theorem, $|\sum_k(S)| \ge |S| - k + 1 \ge |G| + 1$, which is a contradiction. ∎

LEMMA 4.2. *Let G be an abelian group of order n and $S \in \mathcal{F}(G)$ with $|S| = n + k$. Suppose $H = \mathrm{Stab}(\sum_n(S))$ and $k \ge |G/H| - 1$. Then $0 \in \sum_n(S)$.*

Proof. By the EGZ Theorem and the hypothesis, we get the decomposition $S = S_1 \cdots S_{|H|}T$ such that $|S_i| = |G/H|$ and $\sigma(S_i) \in H$ for all $i \in [1, |H|]$, and $|T| = k$. It follows that $\sigma(S_1 \cdots S_{|H|}) \in H \cap \sum_n(S)$. Since $H = \mathrm{Stab}(\sum_n(S))$, we have $0 \in \sum_n(S)$. ∎

DEFINITION 4.3. Let G be a cyclic group of order n and $S, S' \in \mathcal{F}(G)$. We say S is *equivalent* to S' (written $S \cong S'$) if there exists an integer t with $\gcd(t, n) = 1$ and $b \in G$ such that $S = tS' + b$, where $S' = a_0'a_1' \cdots a_m'$ and $tS' + b = (ta_0' + b)(ta_1' + b) \cdots (ta_m' + b)$.

It is easy to see that $0 \in \sum_{ln}(S)$ if and only if $0 \in \sum_{ln}(S')$ for all $l \in \mathbb{N}$, thus we may consider equivalent forms of S in some cases.

LEMMA 4.4. *Let k, m be positive integers with $2 \le k \le m - 2$ and K a cyclic group of order m. Let $S' \in \mathcal{F}(K)$ with $|S'| = 2m + k$, $\mathsf{h}(S') \le 2k$ and $\sum_k(S')$ aperiodic. Suppose that $k \ge 2m/q - 1$ where q is the minimal divisor of $2m$ with $q > 2$. Then $\sigma(S') \in \sum_k(S')$.*

Before we give the proof of Lemma 4.4, we show how to deduce Theorem 1.4 from the above lemmas.

Proof of Theorem 1.4. By Lemma 4.1, $\mathsf{h}(S) \le k$ implies that $\sum_n(S)$ is periodic with the maximal period, say H. If $k \ge |G/H| - 1$, then $0 \in \sum_n(S)$ by Lemma 4.2. Thus we may assume $k < |G/H| - 1$. Since $k \ge n/q - 1$, we have $1 < |H| < q$. Since q is the minimal divisor of n with $q > 2$, we have $|H| = 2$ and $2 \mid n$.

Consider the quotient group G/H which is a cyclic group of order $n/2$ and the image sequence $\varPhi_H(S) \in \mathcal{F}(G/H)$. It is easy to see that $\mathsf{h}(\varPhi_H(S)) \le k|H| = 2k$ and $\sum_k(\varPhi_H(S)) = \sigma(\varPhi_H(S)) - \sum_n(\varPhi_H(S))$ is aperiodic. Applying Lemma 4.4 to $\varPhi_H(S)$, we have $\sigma(\varPhi_H(S)) \in \sum_k(\varPhi_H(S))$ and $0 \in \sum_n(\varPhi_H(S)) = \sigma(\varPhi_H(S)) - \sum_k(\varPhi_H(S))$. Since $\sum_n(S)$ is H-periodic, we have $0 \in \sum_n(S)$. ∎

REMARK. It follows that Conjecture 1.2 holds for the cyclic group of order p or $2p$ with all k when p is a prime. However, Conjecture 1.2 is not always true. The following examples show that the bound for k in Theorem 1.4 is sharp for large n:

Let n be a sufficiently large integer not of the form p or $2p$, G the cyclic group of order n and $g \in G$ with $\mathrm{ord}(g) = n$. Let q be the least divisor of n with $q > 2$, $k = n/q - 2 \geq 2$ and $H = (n/q)G < G$ the subgroup of G of order q. Let $S = UV$ be a sequence with $\mathsf{h}(S) = k$, $|S| = n + k$, $U \in \mathcal{F}(H)$, $V \in \mathcal{F}(g + H)$, and $|V| = an/q - 1$ for some $a \geq 1$. Since $2kq - (n/q - 1) - (n + k) = n - 2n/q - 4q + 3 \geq 0$ for sufficiently large n, such a structure of S is possible. Note that $\sigma(S) \in (n/q - 1)g + H$ and $\sum_k(S) \cap ((n/q - 1)g + H) = \emptyset$, so $\sigma(S) \notin \sum_k(S)$ and $0 \notin \sum_n(S)$.

For example, let $n = 60$ and $k = 18$. Let $S = 0^k \cdot (20g)^k \cdot (40g)^3 \cdot g^k \cdot (21g)^k \cdot (41g)^3$ be the sequence of length $n + k = 78$. An easy calculation shows that $\sum_n(S) = G \setminus \{0, 20g, 40g\}$.

Proof of Lemma 4.4. We divide the proof into some claims and then deduce the result.

Let $I_1 = \{g \in K : \mathsf{v}_g(S') \geq k\}$ and $I_2 = \{g \in K : \mathsf{v}_g(S') < k\}$. Let

$$U = \prod_{g_2 \in I_2} g_2^{\mathsf{v}_{g_2}(S')} \quad \text{and} \quad T = \prod_{g_1 \in I_1} g_1^k \cdot U.$$

Then

$$\textstyle\sum_k(S') = \sum_k(T). \tag{4.1}$$

Hence it remains to consider the construction of T. Since $\sum_k(S')$ is aperiodic, it follows that $|T| < m+k-1$, otherwise the DGM Theorem would imply that $|\sum_k(T)| \geq |T| - k + 1 \geq m$ and $\sum_k(T) = K$. Let $m = tk + r$ where $r \in [0, k-1]$.

Claim 4.1. *$|I_1| = t + 1 \geq 2$ and $\max\{0, 2r - k\} \leq |U| \leq r - 2$.*

Proof of Claim 4.1. If $|I_1| \geq t + 2$, then $|T| \geq k(t + 2) \geq m + k$, a contradiction. If $|I_1| \leq t$, then $|U| \geq |S'| - 2k|I_1|$ and $|T| = k|I_1| + |U| \geq |S'| - k|I_1| \geq |S'| - tk = tk + 2r + k \geq m + k$, a contradiction. Therefore $|I_1| = t + 1$.

It is easy to see that $|U| = |T| - (t + 1)k < r - 1$. If $0 \geq 2r - k$, then it is trivial that $|U| \geq 0$. If $2r - k > 0$, then $|U| \geq |S'| - 2k|I_1| = 2r - k$. This completes the proof of Claim 4.1.

Let

$$U = b_1 \cdots b_{|U|} = \prod_{g_2 \in I_2} g_2^{\mathsf{v}_g(S')}.$$

Consider the setpartition $\mathcal{A} = A_1 \cdots A_k$, where $A_i = I_1 \cup \{b_i\}$ for $i \in [1, |U|]$ and $A_j = I_1$ for $j > |U|$. Since $|U| \leq r - 2 < k$, the structure of $\mathcal{A}$ is as desired. We have

$$\textstyle\sum_k(T) = \sigma(\mathcal{A}) = \displaystyle\sum_{i=1}^k A_i. \tag{4.2}$$

Claim 4.2. *$I_1 + I_1$ is aperiodic and $|I_1 + I_1| = 2|I_1| - 1$.*

Proof of Claim 4.2. By the definition of $\mathcal{A}$, $A_j = I_1$ for $j > |U|$. By Claim 4.1, $k \geq r+1 \geq |U|+3$, which implies $A_{k-2} = A_{k-1} = A_k = I_1$. Since $\sum_k(T) = \sum_{i=1}^k A_i$ is aperiodic, $I_1 + I_1 = A_{k-1} + A_k$ is aperiodic. Thus Kneser's Theorem implies that $|I_1 + I_1| \geq 2|I_1| - 1$.

Suppose to the contrary that $|I_1 + I_1| \geq 2|I_1|$. Let $\delta = 0$ when $k - |U|$ is even and $\delta = 1$ when $k - |U|$ is odd. Then

$$\sum_{i=1}^{k} A_i = \sum_{i=1}^{|U|+\delta} A_i + \underbrace{(I_1 + I_1) + \cdots + (I_1 + I_1)}_{(k-|U|-\delta)/2}.$$

Since $\sum_{i=1}^k A_i$ is aperiodic, we have

$$\begin{aligned}
\Big|\sum_{i=1}^{k} A_i\Big| &\geq \sum_{i=1}^{|U|+\delta} |A_i| + \frac{k-|U|-\delta}{2}|I_1 + I_1| - \left(|U| + \delta + \frac{k-|U|-\delta}{2} - 1\right) \\
&\geq |U|(|I_1|+1) + \delta|I_1| + (k-|U|-\delta)|I_1| - \left(\frac{k+|U|+\delta}{2} - 1\right) \\
&= k|I_1| + \frac{|U|-k-\delta}{2} + 1 \geq tk + \frac{|U|+k-1}{2} + 1 \\
&> tk + r = m,
\end{aligned}$$

by Kneser's Theorem and Claim 4.1, a contradiction. This completes the proof of Claim 4.2.

Let q_m be the minimal divisor of m with $q_m > 1$. Since $k \geq 2m/q - 1$ and q is the minimal divisor of $2m$ with $q > 2$, we have $k \geq m/q_m - 1$ and equality holds if and only if $q_m = 2$, $q = 4$ and $k = m/2 - 1$. By Claim 4.1, we have $r \geq 2$ and $|I_1| = t + 1$. Thus if $q \neq 4$ or $k \neq m/2 - 1$, then $t = (m-r)/k$ implies that $t \leq q_m - 1$ and $|I_1| = t + 1 \leq q_m$. Since (I_1, I_1) is a critical pair such that $I_1 + I_1$ is aperiodic, we can use KST to deduce the structure of I_1.

Claim 4.3. *I_1 is one of the following forms:*

(i) *I_1 is an arithmetic progression.*
(ii) *$q = 4$, $k = m/2 - 1$ and $I_1 = g_0 + \{0, g_1, g_2\}$ for some g_0, g_1, $g_2 \in K$ with* $\mathrm{ord}(g_2) = 2$. *In this case, $|U| = 0$ and $A_i = I_1$ for all $i \in [1, k]$.*

Proof of Claim 4.3. Since (I_1, I_1) is a critical pair such that $I_1 + I_1$ is aperiodic, the KST implies that there is a quasi-periodic decomposition $I_1 = I' \cup I''$ with quasi-period $L \leq K$ such that $I' + L = I'$, $I'' \subset g + L$ for some $g \in K$ and $(I''$, $I'')$ is an elementary pair.

First, we consider the case when $I' = \emptyset$, that is, $(I_1, I_1) = (I'', I'')$ is an elementary pair. By Claim 4.1, $|I_1| = t + 1 \geq 2$, so (I_1, I_1) is not of the form (I) of the elementary pair (Definition 3.4). By Claim 4.1, $k \geq r+1 \geq |U|+3$, which implies $A_{k-2} = A_{k-1} = A_k = I_1$. Since $\sum_{i=1}^{k} A_i$ is aperiodic, $I_1 + I_1$ and $I_1 + I_1 + I_1$ are both aperiodic, and so (I_1, I_1) is not of the form (III) or (IV) of the elementary pair. Therefore (I_1, I_1) is of the form (II), so I_1 is an arithmetic progression.

Next, we assume $I' \neq \emptyset$. Since $I_1 = I' \cup I''$, we have $t + 1 = |I_1| \geq |L| + 1 \geq q_m + 1$. By the discussion before the claim, we have $q = 4$ and $k = m/2 - 1$. Thus $m = 2k+2$, which implies that $t = 2$ and $r = 2$. Moreover $|I'| = |L| = q_m = t = 2$ and $|I''| = 1$. Thus $L = \{0, g_2\}$ with $\mathrm{ord}(g_2) = 2$, $I' = g_0 + L$ and $I_1 = g_0 + \{0, g_1, g_2\}$ for some g_0, $g_1 \in K$. In this case, $|U| \leq r - 2 = 0$ by Claim 4.1, so $A_i = I_1$ for all $i \in [1, k]$. This completes the proof of Claim 4.3.

Now that we have more information about the structure of I_1, we are going to get the conclusion of the lemma.

For the case of Claim 4.3(ii), we have

Claim 4.4. *Let $q = 4$, $k = m/2 - 1$ and $I_1 = g_0 + \{0, g_1, g_2\}$ for some $g_0, g_1, g_2 \in K$ with $\mathrm{ord}(g_2) = 2$. Then $0 \in \sum_{2m}(S')$, so $\sigma(S') \in \sum_k(S')$.*

Proof of Claim 4.4. Let S'' be another sequence such that $S'' \cong S'$. Then $0 \in \sum_{2m}(S')$ if and only if $0 \in \sum_{2m}(S'')$ and $\sigma(S') \in \sum_k(S')$ if and only if $\sigma(S'') \in \sum_k(S'')$. Thus it is sufficient to prove the claim for some equivalent form of S'.

Without loss of generality, we may assume $g_0 = 0$. By Claim 4.3, we have $A_i = I_1 = \{0, g_1, g_2\}$ for all $i \in [1, k]$ and $|U| = 0$.

We first show that $\mathsf{v}_g(S') \geq m/2 + 1$ for all $g \in I_1$. Suppose to the contrary that $\mathsf{v}_g(S') \leq m/2$ for some $g \in I_1$. Then

$$5m/2 - 1 = 2m + k = |S'| \leq 2k \cdot 2 + \mathsf{v}_g(S') \leq 4k + m/2 = 5m/2 - 4,$$

a contradiction. Thus $\mathsf{v}_g(S') \geq m/2 + 1$ for all $g \in I_1$.

If $(m/2)g_1 = 0$ in K, we choose a subsequence

$$S_0 = g_1^{m/2} g_2^l 0^{3m/2-l} \mid S',$$

where

$$l = 2\lfloor \mathsf{v}_{g_2}(S')/2 \rfloor.$$

It is easy to see that the above structure of S_0 is possible. Also we have $|S_0| = 2m$ and $\sigma(S_0) = 0$.

If $(m/2)g_1 = m/2$ in K, we choose a subsequence

$$S_0 = g_1^{m/2} (g_2)^l 0^{3m/2-l} \mid S',$$

where

$$l = 1 + 2\left\lfloor \frac{\mathsf{v}_{g_2}(S') - 1}{2} \right\rfloor.$$

Similarly, we have $|S_0| = 2m$ and $\sigma(S_0) = 0$.

This completes the proof of Claim 4.4.

For the case of Claim 4.3(i), we have the following claims.

Claim 4.5. *Let I_1 be an arithmetic progression with difference d. Then A_i is an arithmetic progression with difference d for all $i \in [\lfloor k/2 \rfloor + 1, k]$ (reorder if necessary), so at least half the A_i's are arithmetic progressions with common difference.*

Proof of Claim 4.5. Recall that $U = b_1 \cdots b_{|U|}$ and $\mathcal{A} = A_1 \cdots A_k$, where $A_i = I_1 \cup \{b_i\}$ for $i \in [1, |U|]$ and $A_j = I_1$ for $j > |U|$.

If $|U| \le \lfloor k/2 \rfloor$, we are done.

If $|U| > \lfloor k/2 \rfloor$, choose arbitrarily $k - |U|$ terms of $A_1 A_2 \cdots A_{|U|}$, say $A_{j_1} \cdots A_{j_{k-|U|}}$. Let $J = \{j_1, \ldots, j_{k-|U|}\}$. If $|A_{j_i} + I_1| \ge |A_{j_i}| + |I_1|$ for all $i \in [1, k - |U|]$, then

$$\sum_{i=1}^{k} A_i = \sum_{i=1}^{k-|U|} (A_{j_i} + A_{|U|+i}) + \sum_{i \in [1,|U|] \setminus J} A_i$$

and

$$\Big|\sum_{i=1}^{k} A_i\Big| \ge \sum_{i=1}^{k} |A_i| - (k - |U| + |U| - (k - |U|)) + 1 = k(t+1) + 1 > m,$$

a contradiction. Thus $|A_{j_i} + I_1| = |A_{j_i}| + |I_1| - 1$ for some j_i, which implies that A_{j_i} is an arithmetic progression with difference d for such j_i. Since the choice of $A_{j_1} A_{j_2} \cdots A_{j_{k-|U|}}$ is arbitrary, there are at most $k - |U| - 1$ terms of $A_1 A_2 \cdots A_k$ such that A_i is not an arithmetic progression with difference d. Since $|U| > \lfloor k/2 \rfloor$, we have $k - |U| - 1 \le \lfloor k/2 \rfloor$. This completes the proof of Claim 4.5.

Claim 4.6. *Let I_1 be an arithmetic progression with difference d. Then* $\mathrm{ord}(d) = m$.

Proof of Claim 4.6. By Claim 4.5, A_i is an arithmetic progression with difference d for all $i \in [\lfloor k/2 \rfloor + 1, k]$. It follows that $\sum_{i=\lfloor k/2 \rfloor+1}^{k} A_i$ is an arithmetic progression with difference d. Notice that $\sum_{i=1}^{k} A_i$ aperiodic implies that $\sum_{i=\lfloor k/2 \rfloor+1}^{k} A_i$ is aperiodic. Hence

$$\mathrm{ord}(d) > \Big| \sum_{i=\lfloor k/2 \rfloor+1}^{k} A_i \Big| \ge t\lceil k/2 \rceil + 1.$$

If $t \ge 2$, then $\mathrm{ord}(d) > k + 1 \ge m/q_m$, where q_m is the minimal divisor of m with $q_m > 1$. It follows that $\mathrm{ord}(d) = m$.

If $t = 1$, then $|I_1| = t + 1 = 2$, $m = k + r$ and $\mathrm{ord}(d) > \lceil k/2 \rceil + 1 > m/4$. We consider two cases.

If $\mathrm{ord}(d) = m/3$, we may assume that $I_1 = \{0, d\}$ (equivalent form). By Claim 4.1, $k \ge r + 1 \ge |U| + 3 \ge 3$, so $3k - 3 \ge 2k > m$. Thus

$\sum_{i=1}^{k-2} I_1 = \langle d\rangle$, as otherwise $\mathrm{ord}(d) > |\sum_{i=1}^{k-2} I_1| = k-1 > m/3$. If there are at least two terms (say b_1, b_2) of $U = b_1 \cdots b_{|U|}$ such that $b_1, b_2 \notin \langle d\rangle$, then $\sum_{i=1}^{k} A_i \supset \{0, b_1\} + \{0, b_2\} + \sum_{i=1}^{k-2} I_1 = K$, a contradiction. If there is exactly one term (say b_1) of U such that $b_1 \notin \langle d\rangle$, then $\sum_{i=1}^{k} A_i = \langle d\rangle \cup (b_1 + \langle d\rangle)$, a contradiction to $\sum_{i=1}^{k} A_i$ being aperiodic. If $b_i \in \langle d\rangle$ for any term of U, then $\sum_{i=1}^{k} A_i = \langle d\rangle$, a contradiction. This shows that $\mathrm{ord}(d) \neq m/3$.

If $\mathrm{ord}(d) = m/2$, we may assume that $I_1 = \{0, d\}$. It is easy to see that $\sum_{i=1}^{k-1} I_1 = \langle d\rangle$, as otherwise $\mathrm{ord}(d) > k > m/2$. If there is some term (say b_1) of U such that $b_1 \notin \langle d\rangle$, then $\sum_{i=1}^{k} A_i \supset \{0, b_1\} + \sum_{i=1}^{k-1} I_1 = K$, a contradiction. If $b_i \in \langle d\rangle$ for any term of U, then $\sum_{i=1}^{k} A_i = \langle d\rangle$, a contradiction. This shows that $\mathrm{ord}(d) \neq m/2$.

This completes the proof of Claim 4.6.

Now we complete the proof of the lemma by the following claim.

CLAIM 4.7. *Let I_1 be an arithmetic progression with difference d. Then $\sigma(S') \in \sum_k(S')$.*

Proof of Claim 4.7. By Claim 4.6, we have $\mathrm{ord}(d) = m$. We may assume $I_1 = \{0, d, 2d, \ldots, td\}$. For any $g = ld \in K$ where $l \in [0, m-1]$, we say g is *on the left* if $l \in [\lfloor (m+t)/2\rfloor + 1, m-1]$ and *on the right* if $l \in [t+1, \lfloor (m+t)/2\rfloor]$. If $g = ld$ is on the left, we call $m - l$ its *left distance*, and if g is on the right, we call $l - t$ its *right distance*. We call it the distance for short if we do not care about left or right.

If there is one term (say $b_1 = l_1 d$) of U whose distance is greater than $r-1$, so $t+r \le l_1 \le m-r$, then $\sum_{i=1}^{k} A_i \supset \{0, d, \ldots, td, b_1\} + \sum_{i=1}^{k-1} I_1 = K$, a contradiction. Thus the distance of b_i is at most $r-1$ for any term of U.

If there are two terms (say $b_1 = l_1 d$, $b_2 = l_2 d$) of U whose distances are both greater than $r/2$, then $\sum_{i=1}^{k} A_i \supset \{0, d, \ldots, td, b_1\} + \{0, d, \ldots, td, b_2\} + \sum_{i=1}^{k-2} I_1 = K$, a contradiction. Thus, there is at most one term (say b_1 if such a term exists) whose distance is greater than $r/2$.

By Claim 4.5, A_i is an arithmetic progression with common difference d for all $i \in [\lfloor k/2\rfloor + 1, k]$. Hence $\sum_{i=\lfloor k/2\rfloor+1}^{k} A_i$ is an arithmetic progression of length $|\sum_{i=\lfloor k/2\rfloor+1}^{k} A_i| \ge k/2 + 1 > r/2$. Since the distance of b_i is at most $r/2$ for any $2 \le i \le |U|$, $\sum_{i=2}^{k} A_i$ is an arithmetic progression of length $|\sum_{i=2}^{k} A_i| \ge k > r$. Since the distance of b_1 is at most $r-1$, $\sum_{i=1}^{k} A_i$ is an arithmetic progression.

Let u_l and u_r denote the numbers of terms of U which are on the left and on the right respectively. Let s_l and s_r denote the sums of the distances of the respective terms. Then $u_l \le s_l$, $u_r \le s_r$, $s_l + s_r < r$ and

$$\sum_{i=1}^{k} A_i = \{(m-s_l)d, (m-s_l+1)d, \ldots, (m-1)d, 0, d, \ldots, (kt+s_r)d\}.$$

Let S_0 be such that $S'S_0 = I_1^{2k}U$. Then

$$\sigma(S') + \sigma(S_0) = \sigma(I_1^{2k}U) = (t(t+1)k + (u_r t + s_r) + (u_l m - s_l))d.$$

Since $m = kt + r = (t+1)k - (k-r)$, we have $\sigma(S') + \sigma(S_0) = (kt + s_r - rt + u_r t - s_l)d$. It is easy to see that $-s_l \le kt + s_r - rt + u_r t - s_l \le kt + s_r$, which implies that $\sigma(S') + \sigma(S_0) \in \sum_{i=1}^{k} A_i$. The length of S_0 is $|S_0| = 2k|I_1| + |U| - (2m+k) = |U| + k - 2r = u_l + u_r + k - 2r \ge 0$. It is easy to see that $(u_l + u_r + k - 2r)t \le kt < m$ and $\sigma(S_0) \in \{0, d, 2d, \ldots, (u_l + u_r + k - 2r)td\}$. Since $kt + s_r - rt + u_r t - s_l - (u_l + u_r + k - 2r)t = rt - u_l t + s_r - s_l \ge -s_l$, we have

$$\sigma(I_1^{2k}U) - \{0, d, 2d, \ldots, (u_l + u_r + k - 2r)td\} \subset \sum_{i=1}^{k} A_i$$

and

$$\sigma(S') = \sigma(I_1^{2k}U) - \sigma(S_0) \in \sum_{i=1}^{k} A_i.$$

This completes the proof of Claim 4.7 and of Lemma 4.4. ∎

5. Proofs of other theorems

Lemma 5.1 ([9, Proposition 4.2.6]). *Let G be a finite abelian group and $S \in \mathcal{F}(G)$ with $|S| \ge |G|$. Then $0 \in \sum_{\le \mathsf{h}(S)}(S)$.*

Lemma 5.2. *Let $S \in \mathcal{F}(G)$ with $|S| \ge |G|$. Suppose there exists a decomposition $S = UV$ where $0 \notin \mathrm{supp}(U)$, $\mathrm{supp}(V) = \{0\}$ and $|U| \ge |G| - 1$. Let $k \in \mathbb{N}$ with $k \ge \mathsf{h}(U)$. Then $\sum_{\le k}(S)$ is periodic.*

Proof. Let $T = U \cdot 0^k$. It is easy to see that $\sum_{\le k}(S) = \sum_k(T)$ by Lemma 5.1.

If $\sum_{\le k}(S) = \sum_k(T)$ is not periodic, then we apply the Devos–Goddyn–Mohar Theorem to T, and obtain $\sum_k(T) \ge |T| - k + 1 \ge |G|$, a contradiction. ∎

By the definition of $\mathsf{D}(G)$, we have

Lemma 5.3. *Let $S \in \mathcal{F}(G)$. Then*

$$\textstyle\sum(S) \subset \sum_{\le \mathsf{D}(G)-1}(S) \cup \{0\}.$$

Now we are ready to give the proofs of Theorems 1.5–1.7.

Proof of Theorem 1.5. By Lemma 5.2, H is not trivial, otherwise B_H is empty. Let $\Phi_H : G \to G/H$ be the natural homomorphism. Let $S_H =$

$\Phi_H(S)$. Since H is the maximal period of $\sum_{\le \mathsf{h}(S)}(S)$, $\sum_{\le \mathsf{h}(S)}(S_H)$ is aperiodic.

Let $T_H | S_H$ be the maximal subsequence satisfying $\mathsf{h}(T_H) \le \mathsf{h}(S)$. It is easy to see that

$$T_H = \prod_{g \in G/H} g^{\min(\mathsf{h}(S), \mathsf{v}_g(S_H))} \quad \text{and} \quad \textstyle\sum_{\le \mathsf{h}(S)}(S_H) = \sum_{\le \mathsf{h}(T_H)}(T_H).$$

By the pigeonhole principle, we have $|T_H| \ge |G/H|$. Since $\sum_{\le \mathsf{h}(S)}(S_H) = \sum_{\le \mathsf{h}(T_H)}(T_H)$ is aperiodic, we have $0 \in \operatorname{supp}(T_H)$ by Lemma 5.2.

Let $I_1(S) = \{g \in G/H : \mathsf{v}_g(S_H) \ge \mathsf{h}(S) \text{ and } g \ne 0\}$ and $I_2(S) = \{g \in G/H : \mathsf{v}_g(S_H) < \mathsf{h}(S) \text{ and } g \ne 0\}$. Then

$$T_H = 0^{\min(\mathsf{h}(S), \mathsf{v}_0(S_H))} \prod_{g \in I_1(S)} g^{\mathsf{h}(S)} \prod_{g \in I_2(S)} g^{\mathsf{v}_g(S_H)}.$$

Let

$$U_H = \prod_{g \in I_1(S)} g^{\mathsf{h}(S)} \prod_{g \in I_2(S)} g^{\mathsf{v}_g(S_H)}$$

denote the subsequence of non-zero terms of T_H. Then $|U_H| \le |G/H| - 2$ by Lemma 5.2.

(i) Suppose that $\mathsf{h}(S) \ge |G/H| - 1$.

If $H = G$, then $\sum_{\le \mathsf{h}(S)}(S) = \sum(S) = G$. Thus we may assume that $H < G$ and then $\sum(S_H) \subset \sum_{\le |G/H|-1}(S_H)$ by Lemma 5.3 with $\mathsf{D}(G/H) = |G/H|$ and $0 \in \operatorname{supp}(T_H) \subset \operatorname{supp}(S_H)$. Since $\sum_{\le |G/H|-1}(S_H) \subset \sum_{\le \mathsf{h}(S)}(S_H)$ and $\sum_{\le \mathsf{h}(S)}(S)$ is H-periodic, $\sum(S) \subset \sum_{\le \mathsf{h}(S)}(S)$, which is the result.

(ii) Since $|G/H| = \mathsf{h}(S)t + r$, we have $n = |G| = \mathsf{h}(S)t|H| + r|H|$. It is easy to see that the number of non-zero terms of S_H is at least

$$\begin{aligned} n - (|H|-1)\mathsf{h}(S) &= t|H|\mathsf{h}(S) + r|H| - (|H|-1)\mathsf{h}(S) \\ &\ge (t-1)|H|\mathsf{h}(S) + \mathsf{h}(S). \end{aligned}$$

If $r \le 1$, then by the pigeonhole principle, we have $|U_H| \ge t\mathsf{h}(S) = |G/H| - r \ge |G/H| - 1$, a contradiction. Therefore, $r \ge 2$.

If $r > \mathsf{h}(S) - 2/(|H|-1)$, then $r|H| - (|H|-1)\mathsf{h}(S) \ge r - 1$. Thus by the pigeonhole principle, we have $|U_H| \ge t\mathsf{h}(S) + r - 1 = |G/H| - 1$, a contradiction. Therefore $r \le \mathsf{h}(S) - 2/(|H|-1)$.

(iii) We construct S as follows. Let $d \in G$ with $\operatorname{ord}(d) = n$. Let $t_0 = t$ when $r|H| - (|H|-1)k \ge 0$ and $t_0 = t - 1$ when $r|H| - (|H|-1)k < 0$. Set

$$S = \prod_{g \in H \setminus \{0\}} g^k \cdot \prod_{i=1}^{t_0} \Big(\prod_{g \in id + H} g^k \Big) \cdot U,$$

where $U \in \mathcal{F}((t_0+1)d + H)$ is any sequence of length $n + k - (t_0+1)k|H|$ with $\mathsf{h}(U) \le k$. Since $n + k - (t_0+1)k|H| = (t-t_0)k|H| + r|H| - (|H|-1)k$, we have $0 \le n+k-(t_0+1)k|H| \le k|H|$. Thus the structure of S is possible. It is easy to see that $\mathsf{h}(S) = k$ and $\sum_{\le k}(S)$ is H-periodic.

Let S_H, T_H, U_H, $I_1(S)$ and $I_2(S)$ be defined as above. Note that $|U_H| = t_0k+\min\{n+k-(t_0+1)k|H|, k\}$. If $n+k-(t_0+1)k|H| \ge k$, that is, $n/|H| \ge (t_0+1)k$, then $t_0 = t-1$ and $|U_H| = (t_0+1)k = |G/H| - r \le |G/H| - 2$ (here we use $r \ge 2$). If $n+k-(t_0+1)k|H| < k$, so that $n/|H| < (t_0+1)k$, then $t_0 = t$ and

$$\begin{aligned} |U_H| &= tk+n+k-(t+1)k|H| = tk + r|H| + k - k|H| \\ &\le tk + r - 2 = |G/H| - 2 \end{aligned}$$

(here we use $k \ge r + 2/(|H|-1)$). Therefore, $|U_H| \le |G/H| - 2$ in both cases. It is easy to see that

$$\textstyle\sum_{\le k}(S_H) = \sum_{\le k}(T_H) = \{0, \Phi(d), \ldots, |U_H|\Phi(d)\},$$

which implies that $\sum_{\le k}(S_H)$ is aperiodic and $S \in B_H$. As $\Phi((|U_H|+1)d) \in \sum(S_H)$, we have $\sum_{\le \mathsf{h}(S)}(S) \ne \sum(S)$. ∎

Proof of Theorem 1.6. Let $d \in G$ with $\mathrm{ord}(d) = n$.

(i) Assume n is a prime. The sequence $S = d^{n-2}(2d)$ satisfies $\sum_{\le \mathsf{h}(S)}(S) \ne \sum(S)$, since $0 \notin \sum_{\le \mathsf{h}(S)}(S)$. Hence $\mathsf{L}(G) \ge n$. On the other hand, suppose $|S| = n$. By Lemma 5.2, $\sum_{\le \mathsf{h}(S)}(S)$ is periodic, which implies $\sum_{\le \mathsf{h}(S)}(S) = G = \sum(S)$. Therefore, if G is a cyclic group of prime order n, then $\mathsf{L}(G) = n$.

(ii) Assume n is a composite number. Let $p \mid n$ be the minimal divisor of n and let (a,b) be as in the theorem. It is easy to see that $n/p - 4p \le n-4$ and $4p - n/p \le n-4$, so $(a,b) \ne (1,n)$.

Let $H \le G$ be a subgroup of order a. Then $|G/H| = b$. Let $S = UV$, where

$$V = \prod_{g \in H\setminus\{0\}} g^{b-2} \quad \text{and} \quad U = \prod_{g \in d+H} g^{b-2}.$$

Then $|S| = |V| + |U| = (a-1)(b-2) + a(b-2) = 2n - 4a - b + 2$. Also, we can see that $\sum_{\le \mathsf{h}(S)}(S) \ne \sum(S)$, since $(b-1)d + H \subset \sum(S) \setminus \sum_{\le \mathsf{h}(S)}(S)$. Therefore $\mathsf{L}(G) \ge 2n - 4a - b + 3$.

On the other hand, let $S \in \mathcal{F}(G \setminus \{0\})$ with $|S| \ge 2n - 4a - b + 3 \ge n+1$. By Lemma 5.2, $\sum_{\le \mathsf{h}(S)}(S)$ is periodic. Let H be the maximal period of $\sum_{\le \mathsf{h}(S)}(S)$. Let $\Phi_H : G \to G/H$ be the natural homomorphism. Let $S_H = \Phi_H(S)$ and T_H be the maximal subsequence of S_H such that $\mathsf{h}(T_H) \le \mathsf{h}(S)$. Then $|T_H| > n/|H|$ by the pigeonhole principle and $\sum_{\le \mathsf{h}(S)}(S_H) = \sum_{\le \mathsf{h}(S)}(T_H)$.

If $H = G$, we are done. Thus we may assume that $H < G$.

If $0 \notin \mathrm{supp}(T_H)$, then $\sum_{\le \mathsf{h}(S)}(T_H)$ is periodic by Lemma 5.2, which contradicts H being the maximal period. Thus $0 \in \mathrm{supp}(T_H) \subset \mathrm{supp}(S_H)$.

If $\mathsf{h}(S) \geq n/|H| - 1$, then by Lemma 5.3 and $0 \in \operatorname{supp}(S_H)$, we have

$$\sum(S_H) \subset \sum_{\leq n/|H|-1}(S_H) \subset \sum_{\leq \mathsf{h}(S)}(S_H) \subset \sum(S_H),$$

which implies the conclusion of theorem.

If $\mathsf{h}(S) \leq n/|H| - 2$, let $n/|H| = t\mathsf{h}(S) + r$ with $r \in [0, \mathsf{h}(S) - 1]$. Let $S = UV$, where $U \in \mathcal{F}(G \setminus H)$ and $V \in \mathcal{F}(H)$. Since $S \in \mathcal{F}(G \setminus \{0\})$, we have $|V| \leq (|H| - 1)\mathsf{h}(S)$. Hence

$$\begin{aligned}
|U| &= |S| - |V| = 2n - 4a - b + 3 - |V| \\
&\geq (2n - 4|H| - n/|H| + 3) - (|H| - 1)\mathsf{h}(S) \\
&= n + (n/|H| - 4 - \mathsf{h}(S))(|H| - 1) - 1 \\
&= t\mathsf{h}(S)|H| + ((t-1)\mathsf{h}(S) + 2r - 4)(|H| - 1) + (r - 1).
\end{aligned}$$

Let $T_H = U_T V_T$ where $0 \notin \operatorname{supp}(U_T)$ and $\operatorname{supp}(V_T) = \{0\}$. Since $\sum_{\leq \mathsf{h}(S)}(T_H)$ is aperiodic, by Lemma 5.2, we have $|U_T| \leq n/|H| - 2$. If $r \geq 2$, then $|U| \geq t\mathsf{h}(S)|H| + r - 1$. By the pigeonhole principle, $|U_T| \geq t\mathsf{h}(S) + r - 1 = n/|H| - 1$, a contradiction. If $r = 1$, then

$$|U| \geq (t-1)\mathsf{h}(S)|H| + (t\mathsf{h}(S) - 2)(|H| - 1) + \mathsf{h}(S) \geq (t-1)\mathsf{h}(S)|H| + \mathsf{h}(S).$$

Thus $|U_T| \geq (t-1)\mathsf{h}(S) + \mathsf{h}(S) = n/|H| - 1$, a contradiction. If $r = 0$, then

$$|U| \geq (t-1)\mathsf{h}(S)|H| + (t\mathsf{h}(S) - 4)(|H| - 1) + \mathsf{h}(S) - 1.$$

Since $\mathsf{h}(S) \leq n/|H| - 2$, we have $t \geq 2$. Since $t \geq 2$ and $\mathsf{h}(S) \geq 2$, it follows that $|U| \geq (t-1)\mathsf{h}(S)|H| + \mathsf{h}(S) - 1$. Thus $|U_T| \geq (t-1)\mathsf{h}(S) + \mathsf{h}(S) - 1 = n/|H| - 1$, a contradiction.

Therefore, if G is a cyclic group of composite order n, then $\mathsf{L}(G) = 2n - 4a - b + 3$. ■

Proof of Theorem 1.7. Let $d \in G$ with $\operatorname{ord}(d) = n$.

(i) Assume n is a prime. By Lemma 5.2, $\sum_{\leq \mathsf{h}(S)}(S)$ is periodic, which implies that $\sum_{\leq \mathsf{h}(S)}(S) = G = \sum(S)$. On the other hand, the example $S = d^n$ implies that the restricted length $\mathsf{h}(S)$ is the best possible.

(ii) Assume n is a composite number. By Lemma 5.2, $\sum_{\leq 2\mathsf{h}(S)-2}(S)$ is periodic with maximal period, say H. Let $\Phi_H : G \to G/H$ be the natural homomorphism. Let $S_H = \Phi_H(S)$ and T_H be the maximal subsequence of S_H such that $\mathsf{h}(T_H) \leq 2\mathsf{h}(S) - 2$. Then $|T_H| > n/|H|$ and $\sum_{\leq 2\mathsf{h}(S)-2}(S_H) = \sum_{\leq 2\mathsf{h}(S)-2}(T_H)$. It is easy to see that $0 \in \operatorname{supp}(T_H)$, otherwise $\sum_{\leq 2\mathsf{h}(S)-2}(T_H)$ is periodic by Lemma 5.2, which contradicts H being the maximal period.

If $2\mathsf{h}(S) - 2 \geq n/|H| - 1$, then $\sum(S_H) \subset \sum_{\leq n/|H|-1}(S_H) \subset \sum_{\leq 2\mathsf{h}(S)-2}(S_H)$ by Lemma 5.3, which implies $\sum_{\leq 2\mathsf{h}(S)-2}(S) = \sum(S)$.

If $2\mathsf{h}(S)-2 \le n/|H|-2$, then $2\mathsf{h}(S) \le n/|H|$. Let $|G/H| = t\mathsf{h}(S)+r$ where $r \in [0, \mathsf{h}(S)-1]$, then the number of non-zero terms of S_H is at least

$$n-(|H|-1)\mathsf{h}(S) = (t-1)|H|\mathsf{h}(S)+r|H|+\mathsf{h}(S).$$

Since $S \in \mathcal{F}(G \setminus \{0\})$ with $|S| = n$, we have $\mathsf{h}(S) \ge 2$. Let U_T denote the subsequence consisting of the non-zero terms of T_H. We have $|U_T| \le |G/H|-2$ by Lemma 5.2.

If $r = 0$, then $n-(|H|-1)\mathsf{h}(S) = (t-1)|H|\mathsf{h}(S)+\mathsf{h}(S)$ and $|U_T| \ge (t-1)(2\mathsf{h}(S)-2)+\mathsf{h}(S) \ge t\mathsf{h}(S) = |G/H|$, a contradiction.

If $r \ge 1$, then by the pigeonhole principle,

$$|U_T| \ge (t-1)(2\mathsf{h}(S)-2)+\min\{r|H|+\mathsf{h}(S), 2\mathsf{h}(S)-2\}.$$

Since

$$(t-1)(2\mathsf{h}(S)-2)+r|H|+\mathsf{h}(S) \ge t\mathsf{h}(S)+r$$

and

$$(t-1)(2\mathsf{h}(S)-2)+2\mathsf{h}(S)-2 \ge t\mathsf{h}(S)+r-1,$$

we have $|U_T| \ge |G/H|-1$, a contradiction. This completes the proof. ∎

Remark. The second part of Theorem 1.7 is sharp in view of the following example. Let $n = pm$ where $p \ge 7$ is odd and m is large. Let G be a cyclic group of order n and $H < G$ the subgroup of order m. Let $d \in G$ with $\mathrm{ord}(d) = n$. Let $k = (p+1)/2$ and

$$S = \prod_{g \in H\setminus\{0\}} g^k \cdot \prod_{g \in d+H} g^{\mathsf{v}_g(S)},$$

where $\mathsf{v}_g(S)$'s satisfy $\mathsf{v}_g(S) \le k$ for all $g \in d+H$ and $k(|H|-1)+\sum_{g\in d+H}\mathsf{v}_g(S) = n$. Since $(|H|-1)k+|H|k \ge n$ for sufficiently large m, the structure of S is possible. Note that $\mathsf{h}(S) = k = (p+1)/2$. For such S, we have

$$\textstyle\sum_{\le 2\mathsf{h}(S)-3}(S) = \sum_{\le p-2}(S) = \bigcup_{i=0}^{p-2}(id+H)$$

and $\sum(S) = G$, therefore $\sum_{\le 2\mathsf{h}(S)-3}(S) \ne \sum(S)$.

Acknowledgments. This research was supported by a grant from the Guangdong Provincial Natural Science Foundation (No. 8151027501000114) and a grant from NSF of China (No. 10971072).

References

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

[2] H. Q. Cao, *An addition theorem on the cyclic group $\mathbb{Z}_{p^\alpha q^\beta}$*, Electron. J. Combin. 13 (2006), no. 1, note 9, 4 pp.

[3] M. DeVos, L. Goddyn and B. Mohar, *A generalization of Kneser's addition theorem*, Adv. Math. 220 (2009), 1531–1548.

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

[5] C. Flores and O. Ordaz, *On the Erdős–Ginzburg–Ziv theorem*, Discrete Math. 152 (1996), 321–324.

[6] W. D. Gao, *An addition theorem for finite cyclic groups*, ibid. 163 (1996), 257–265.

[7] W. D. 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 (2005), 67–77.

[8] W. D. Gao, R. Thangadurai and J. Zhuang, *Addition theorems on the cyclic groups of order p^l*, Discrete Math. 308 (2008), 2030–2033.

[9] A. Geroldinger, *Additive group theory and non-unique factorizations*, in: Combinatorial Number Theory and Additive Group Theory, A. Geroldinger and I. Ruzsa (eds.), Adv. Courses Math. CRM Barcelona, Birkhäuser, 2009, 1–86.

[10] A. Geroldinger and F. Halter-Koch, *Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory*, Pure Appl. Math. 278, Chapman & Hall/CRC, 2006.

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

[12] —, *Quasi-periodic decompositions and the Kemperman structure theorem*, Eur. J. Combin. 26 (2005), 559–575.

[13] —, *Sumsets, zero-sums and extremal combinatorics*, Ph.D. Dissertation, Caltech, 2006.

[14] —, *A step beyond Kemperman's structure theorem*, Mathematika 55 (2009), 67–114.

[15] D. J. Grynkiewicz, L. E. Marchan and O. Ordaz, *Representation of finite abelian group elements by subsequence sums*, J. Théor. Nombres Bordeaux 21 (2009), 559–587.

[16] J. H. B. Kemperman, *On small sumsets in an abelian group*, Acta Math. 103 (1960), 63–88.

[17] B. Peterson and T. Yuster, *A generalization of an addition theorem for solvable groups*, Canad. J. Math. 36 (1984), 529–536.

[18] S. Savchev and F. Chen, *Long n-zero-free sequences in finite cyclic groups*, Discrete Math. 308 (2008), 1–8.

Xiangneng Zeng
School of Mathematics
Sun Yat-Sen University
Guangzhou 510275, P.R. China
E-mail: junevab@163.com

Pingzhi Yuan
School of Mathematics
South China Normal University
Guangzhou 510631, P.R. China
E-mail: mcsypz@mail.sysu.edu.cn

Received on 8.7.2010
and in revised form on 13.10.2010 (6446)