Extremal incomplete sets in finite abelian groups *

Dan Guo[a], Yongke Qu[a,†], Guoqing Wang[b], Qinghong Wang[c]

[a]Center for Combinatorics, LPMC-TJKLC
Nankai University, Tianjin 300071, P. R. China

[b]Department of Mathematics
Tianjin Polytechnic University, Tianjin 300160, P. R. China

[c]College of Science
Tianjin University of Technology, Tianjin 300384, P. R. China

Abstract

Let G be a finite abelian group. The critical number $\mathrm{cr}(G)$ of G is the least positive integer ℓ such that every subset $A \subseteq G \setminus \{0\}$ of cardinality at least ℓ spans G, i.e., every element of G can be written as a nonempty sum of distinct elements of A. The exact values of the critical number have been completely determined recently for all finite abelian groups. The structure of these sets of cardinality $\mathrm{cr}(G)-1$ which fail to span G has also been characterized except for the case that $|G|$ is an even number and the case that $|G| = pq$ with p, q are primes. In this paper, we characterize these extremal subsets for $|G| \geq 36$ is an even number, or $|G| = pq$ with p, q are primes and $q \geq 2p + 3$.

*The research is supported by NSFC (11001035)
†corresponding email: quyongke@mail.nankai.edu.cn

1 Introduction

Let G be a finite abelian group, and let A be a subset of G. Let $\langle A\rangle$ denote the subgroup of G generated by A. Let

$$\sum(A) = \{\sum_{g\in B} g : \emptyset \neq B \subseteq A\}.$$

The nonempty set A is said to be *complete* if $\sum(A) = \langle A\rangle$. We say A spans G if $\sum(A) = G$, equivalently, if $\langle A\rangle = G$ and A is complete. The critical number $\mathrm{cr}(G)$ of G is the least positive integer ℓ such that every subset $A \subseteq G\setminus\{0\}$ of cardinality at least ℓ spans G. The critical number was first studied by P. Erdős and H. Heilbronn [3] for cyclic groups of prime order in 1964. Since then, due to contributions by H.B. Mann, J.E. Olson, G.T. Dierrich, Y.F. Wou, J.A. Dias da Silva, Y.O. Hamidoune, A.S. Lladó, O. Serra, M. Freeze, W.D. Gao, and A. Geroldinger, et al., the critical numbers of all finite abelian groups have been completely determined. Also, there has been some work generalizing the critical number to non-commutative groups, one can refer to [5, 19]. The values of critical number of finite abelian groups are summarized as follows.

Theorem A. ([1], [2], [4], [6], [11]) *Let G be a finite abelian group of order $|G| \geq 3$, and let p denote the smallest prime divisor of $|G|$.*

1. If $|G| = p$, then $\mathrm{cr}(G) = \lfloor 2\sqrt{p-2}\rfloor$.

2. In each of the following cases we have $\mathrm{cr}(G) = \frac{|G|}{p} + p - 1$;

. G is isomorphic to one of the following groups: $Z_2 \oplus Z_2$, $Z_3 \oplus Z_3$, Z_4, Z_6, $Z_2 \oplus Z_4$, Z_8.

. $\frac{|G|}{p}$ is an odd prime with $2 < p < \frac{|G|}{p} \leq p + \lfloor 2\sqrt{p-2}\rfloor + 1$.

3. In all other cases we have $\mathrm{cr}(G) = \frac{|G|}{p} + p - 2$.

So, a natural question is

What is the structure of the extremal subsets which fail to span G?

With respect to this question, Nguyen, Szemedédi, and Vu [16] characterized the set of Z_p of cardinality at least $\sqrt{2p}$ which fails to span the group Z_p. Recently, Vu [18] also showed that for general finite abelian group G meeting certain conditions, if A is a comparatively large subset of G and A fails to span G, then A contains a complete subset. Before then, Gao, Hamidoune, Lladó and Serra [7] obtained the following result:

Theorem B. *Let G be a finite abelian group of odd order. Let p be the smallest prime divisor of $|G|$. Assume $\frac{|G|}{p}$ is composite and*

$$\frac{|G|}{p} \geq \begin{cases} 62, & \text{if} \quad p = 3; \\ 7p + 3, & \text{if} \quad p \geq 5. \end{cases}$$

Let A be a subset of $G \setminus \{0\}$ of cardinality $\mathrm{cr}(G) - 1$ such that $\sum(A) \neq G$. Then there exists a subgroup H of order $\frac{|G|}{p}$ and an element $g \in G \setminus H$ such that $H \setminus \{0\} \subseteq A$ and $A \subseteq H \cup (g + H) \cup (-g + H)$.

In general, the structure of the extremal set remains unknown only for the following two types of group G:

1. $|G|$ is even.
2. $|G|$ is a product of two odd prime numbers.

In this paper, we characterize the structure of the extremal set for the group G when $|G|$ is an even number with $|G| \geq 36$, or $|G|$ is a product of two odd prime numbers p, q with $q \geq 2p + 3$. Our main result is as follows.

Theorem 1.1. *Let G be a finite abelian group, and let p be the smallest prime divisor of $|G|$. Assume that $p = 2$ and $|G| \geq 36$, or $\frac{|G|}{p}$ is a prime number with $\frac{|G|}{p} \geq 2p + 3$. Let $A \subseteq G \setminus \{0\}$ be a subset of cardinality $\mathrm{cr}(G) - 1$ such that $\sum(A) \neq G$. Then there exists a subgroup H of G of cardinality $\frac{|G|}{p}$ such that*

(i) if $p = 2$, then $A = H \setminus \{0\}$;

(ii) if $p \geq 3$, then $A \subseteq H \cup (g + H) \cup (-g + H)$ and $H \setminus \{0\} \subseteq A$, where $g \in G \setminus H$.

The rest of this paper is organized as follows. In Section 2 we introduce some technical notations and tools. The proof of Theorem 1.1 is presented in Section 3. The Final Section 4 contains some concluding remarks, together with two conjectures on the structure of the extremal set for the group $G = Z_{pq}$ with $p < q < 2p + 3$.

2 Notations and tools

Let G be a finite abelian group, and let A and B be nonempty subsets of G. The sumset $A+B$ is the set of all elements of G that can be written in the form $a+b$, where $a \in A$ and $b \in B$. We call A an *arithmetic progression with difference* $d \in G$ if there is some $a \in G$ such that $A = \{a + id : i \in [0, |A|-1]\}$. Let $T = a_1 a_2 \cdot \ldots \cdot a_\ell$ be a sequence of elements in G. Define

$$\sum(T) = \{\sum_{i \in I} a_i : \emptyset \neq I \subseteq [1, \ell]\}$$

and

$$\sum^{\circ}(T) = \sum(T) \cup \{0\}.$$

For notational convenience, we let $\sum(T) = \{0\}$ if T is an empty sequence. For any integer $h \in [1, \ell]$, let

$$\sum_h(T) = \{\sum_{i \in I} a_i : I \subseteq [1, \ell], |I| = h\}.$$

We adopt the convention that $\sum_0(T) = \{0\}$. Let $\mathrm{supp}(T)$ be the set consisting of all distinct elements in T. In this paper, we shall view a set A to be a squarefree sequence, i.e., $\mathrm{supp}(A) = A$. Then all the notations that are valid for sequences automatically apply to sets too.

We present below some tools:

Lemma 2.1 ([9], Lemma 5.2.9)**.** *Let A_1 and A_2 be nonempty subsets of a finite abelian group G. If $|A_1| + |A_2| \geq |G| + 1$ then $A_1 + A_2 = G$.*

Lemma 2.2 ([13])**.** *Let A be a subset of a finite abelian group G such that $0 \notin A$ and $|A| \geq 14$. Then one of the following conditions holds.*

(i). $|\sum^{\circ}(A)| \geq \min(|G| - 3, 3|A| - 3)$;

(ii). There is a subgroup $H \neq G$ such that $|A \cap H| \geq |A| - 1$.

Lemma 2.3 ([15], Theorem 2.3)**.** *Let p be a prime number, and let $A_1, A_2, \ldots, A_h$ be nonempty subsets of Z_p. Then*

$$|A_1 + A_2 + \cdots + A_h| \geq \min(p, \sum_{i=1}^{h} |A_i| - h + 1).$$

Lemma 2.4 ([2])**.** *Let p be a prime number, and let $A_1, A_2, \ldots, A_h$ be nonempty subsets of Z_p, apart from one possible exception, are arithmetic progressions with pairwise distinct nonzero differences. Then*

$$|A_1 + A_2 + \cdots + A_h| \geq \min(p, \sum_{i=1}^{h} |A_i| - 1).$$

Remark. Note that an arithmetic progression $A = \{a, a + d, \ldots, a + (|A| - 1)d\}$ of difference d can also be viewed as an arithmetic progression of difference $-d$. Let $A_1, A_2, \ldots, A_h$ be h arithmetic progressions with $A_i = \{a_i, a_i + d_i, \ldots, a_i + (|A_i| - 1)d_i\}$. If one can find some $h-$tuple $(\theta_1, \theta_2, \ldots, \theta_h) \in \{d_1, -d_1\} \times \{d_2, -d_2\} \times \cdots \times \{d_h, -d_h\}$ such that $\theta_1, \theta_2, \ldots, \theta_h$ are pairwise distinct, then $A_1, A_2, \ldots, A_h$ would be regarded as progressions with pairwise distinct differences.

Lemma 2.5 ([15], Theorem 2.7)**.** *Let p be an odd prime number, and let B_1 and B_2 be nonempty subsets of the group Z_p with $2 \leq |B_i| \leq p - 2$ for $i = 1, 2$. If $|B_1 + B_2| < \min(p, |B_1| + |B_2|)$, then B_1 and B_2 are arithmetic progressions with differences d_1 and d_2, respectively, such that $d_1 \in \{d_2, -d_2\}$.*

Lemma 2.6. *Let p be a prime number, and let A be a nonempty subset of Z_p. Then*

(i). $|\sum_h(A)| \geq \min(p, h|A| - h^2 + 1)$ *for all* $1 \leq h \leq |A|$ *(see [1], [15, Theorem 3.4]);*

(ii). If $|A| = \lfloor\sqrt{4p - 7}\rfloor$ *and* $h = \lfloor|A|/2\rfloor$, *then* $|\sum_h(A)| = p$ *(see [1]);*

(iii). If $|A| \geq \lfloor 2\sqrt{p - 2}\rfloor$ *then* $|\sum(A)| = p$ *(see [4]).*

The following lemma is a corollary of Theorem 1.3 in [8].

Lemma 2.7. *Let A be a nonempty, finite subset of an abelian group with $0 \notin A$. Then*

$$|\sum(A)| \geq \min(|\langle A\rangle|, 2|A| - 1).$$

By Lemma 2.7, we immediately have the following

Lemma 2.8. *Let p be a prime number, and let A be a subset of $Z_p \setminus \{0\}$ with $|A| = \ell$. Then*

$$|\sum^{\circ}(A)| \geq \min(p, 2\ell - 1 + \epsilon(\ell)),$$

where

$$\epsilon(\ell) = \begin{cases} 2, & \text{if} \quad \ell = 0; \\ 1, & \text{if} \quad \ell = 1; \\ 0, & \text{if} \quad \ell \geq 2. \end{cases}$$

Lemma 2.9. *Let p be a prime number, and let T be a sequence of elements in $Z_p \setminus \{0\}$ and of length $|T| \geq 2$. Then $|\sum^{\circ}(T)| \geq \min(p, |T| + 1)$, and moreover, equality holds only for one of the following two conditions.*

(i). $|T| \geq p - 1$;

(ii). There exists some $g \in Z_p \setminus \{0\}$ such that $\mathrm{supp}(T) \subseteq \{g, -g\}$.

Proof. Let $T = a_1 \cdot \ldots \cdot a_\ell$. Let $A_i = \{0, a_i\}$ for $i \in [1, \ell]$. By Lemma 2.3, we have

$$|\sum^{\circ}(T)| = |\sum_{i=1}^{\ell} A_i| \geq \min(p, \sum_{i=1}^{\ell} |A_i| - \ell + 1) = \min(p, \ell + 1).$$

Now assume that neither (i) nor (ii) holds, i.e.,

$$\ell \leq p - 2$$

and there exist two elements, say

$$a_{\ell-1} \neq a_\ell$$

and

$$a_{\ell-1} + a_\ell \neq 0.$$

Let $A_0 = \{0, a_{\ell-1}, a_\ell, a_{\ell-1} + a_\ell\}$. It follows from Lemma 2.3 that

$$|\sum^{\circ}(T)| = |A_0 + A_1 + \cdots + A_{\ell-2}| \geq \min(p, \sum_{i=0}^{\ell-2} |A_i| - (\ell - 2)) = \ell + 2.$$

Then the lemma follows. ∎

3 Proof of Theorem 1.1

We begin this section with the following observation.

Observation 3.1. *Let G be a finite abelian group, and let A be a subset of $G \setminus \{0\}$ of cardinality $\mathrm{cr}(G) - 1$ such that $\sum(A) \neq G$. If $A^{'}$ is a complete subset of A, then $A \cap \langle A^{'} \rangle = \langle A^{'} \rangle \setminus \{0\}$.*

We shall prove Theorem 1.1 by two cases according to $|G|$ is an even number or $|G|$ is a product of two distinct prime numbers.

Proof of Theorem 1.1 for the case that $|G| \equiv 0 \pmod 2$ *with* $|G| \geq 36$.

By Theorem A, we have

$$|A| = \mathrm{cr}(G) - 1 = \frac{|G|}{2} - 1 \geq 17. \tag{1}$$

Take a subset A_1 of A with

$$|A_1| = 3. \tag{2}$$

Let $A_2 = A \setminus A_1$. Obviously, $|\sum(A_1)| \geq 4$. Since $\sum(A_1) + \sum^{\circ}(A_2) \subseteq \sum(A) \neq G$, it follows from Lemma 2.1 that $|\sum^{\circ}(A_2)| < |G| - 3$. By Lemma 2.2, we conclude that there is a subgroup $K \neq G$ such that $|A_2 \cap K| \geq |A_2| - 1$. It follows from (1) and (2) that $|A_2 \cap K| \geq |A_2| - 1 = \frac{|G|}{2} - 4 > \frac{|G|}{3} - 1$, and so

$$|K| = \frac{|G|}{2}.$$

By (1), we have $|A_2 \cap K| \geq |K| - 4 \geq \frac{|K|+1}{2}$. It follows from Lemma 2.7 that $\sum(A_2 \cap K) = \langle A_2 \cap K \rangle = K$. Then the conclusion follows from Observation 3.1. ∎

Therefore, it remains to prove Theorem 1.1 for the case that

$$G = Z_{pq}$$

where p, q are odd prime number such that

$$q \geq 2p + 3.$$

Before proceeding with our arguments, we need to formulate some more technical notations and definitions which will be used in the rest part of this paper.

Let H be the subgroup of G of order q, and let φ be the canonical epimorphism of G onto the quotient group $G \diagup H$. Then $\varphi(A)$ is a sequence of elements in $G \diagup H$ of length $p + q - 3$. Denote

$$k = |\mathrm{supp}(\varphi(A)) \setminus \{0\}|.$$

Fix k elements $a_1, \ldots, a_k \in A \setminus H$ such that $\varphi(a_1), \ldots, \varphi(a_k)$ are pairwise distinct. Let

$$A \setminus H = \bigcup_{i=1}^{k} A_i,$$

where $A_i + H = a_i + H$ for all $i \in [1, k]$, and let

$$A_0 = A \cap H$$

(A_0 is perhaps an empty set). Let

$$\widetilde{A_i} = A_i - a_i \quad \text{for} \quad i \in [1, k].$$

Note that $\widetilde{A_1}, \ldots, \widetilde{A_k}$ are subsets of H. Denote

$$\ell_i = |A_i| \quad \text{for} \quad i \in [0, k].$$

We shall always admit

$$\ell_1 \geq \ell_2 \geq \cdots \geq \ell_k. \tag{3}$$

Let

$$R_1 = \{i \in [1, k] : \ell_i = 1\};$$
$$R_2 = \{i \in [1, k] : \ell_i = 2\};$$

$$R_3 = \{i \in [1,k] : \ell_i = 3\};$$
$$R_4 = \{i \in [1,k] : \ell_i = 4\};$$
$$R_5 = \{i \in [1,k] : \ell_i \geq 5\};$$

and let

$$r_i = |R_i| \quad \text{for } i \in [1,5].$$

For convenience, let

$$m_t = k - \sum_{i=1}^{t-1} r_i \quad \text{for } t \in [1,5].$$

Notice that

$$[1, m_t] = \{i \in [1,k] : \ell_i \geq t\} \quad \text{for } t \in [1,5],$$

and that

$$[m_{u+1}+1, m_u] = \{i \in [1,k] : \ell_i = u\} \quad \text{for } u \in [1,4].$$

Definition 3.2. *For any element $\bar{g} \in G/H$, we say that $\bar{g}$ has a representation with coefficients $f_1, \ldots, f_k$ provided that*

$$\bar{g} = \sum\nolimits_{i=1}^{k} f_i \ \varphi(a_i), \tag{4}$$

where $f_i \in [0, \ell_i]$ and $f_1 + \cdots + f_k > 0$.

Definition 3.3. *Let*

$$\begin{aligned}
X_i^{\Delta} &= \{2\varphi(a_i), 3\varphi(a_i), \ldots, \mu_i\varphi(a_i)\} && \text{if} \quad i \in [1, m_4];\\
X_i &= \{\varphi(a_i), 2\varphi(a_i), \ldots, \lambda_i\varphi(a_i)\} && \text{if} \quad i \in [1, m_2];\\
X_i &= \{0, \varphi(a_i)\} && \text{if} \quad i \in [m_2+1, k];\\
Y &= \varphi(\sum_{i=1}^{r_2} a_{m_3+i}) - \{0, \varphi(a_{m_3+1}), \varphi(a_{m_3+2}), \ldots, \varphi(a_{m_3+r_2})\},
\end{aligned}$$

where $\mu_i = \min(\ell_i - 2, p+1)$ and $\lambda_i = \min(\ell_i - 1, p)$.

Definition 3.4. *For $n \in [0, m_4]$, let*

$$\alpha_n = \min(p, |\sum_{i=1}^{n} X_i^{\Delta} + \sum_{i=n+1}^{m_3} X_i + \sum_{i=m_2+1}^{k} X_i + Y|).$$

For any integer $m \geq 0$, let

$$\delta(m) = \begin{cases} 0, & \text{if} \quad m = 0; \\ 1, & \text{if} \quad m > 0. \end{cases}$$

To make the remainder of the proof clear, we propose the general idea as follows. If $|A_0|$ is large, the conclusion of Theorem 1.1 is easy to prove. Assume $|A_0|$ is small. We shall derive a contradiction by the following process. We first show that there exists some $n \in [0, m_4]$ such that $\alpha_n = p$, i.e., every element $\bar{g} \in G/H$ has a fixed representation with coefficients $f_1 = f_1(n, \bar{g}), \ldots, f_k = f_k(n, \bar{g})$, where

$$f_i \in [2, \ell_i - 2] \qquad \text{for } i \in [1, n], \tag{5}$$

and that

$$f_j \in [1, \ell_j - 1] \qquad \text{for } j \in [n+1, m_2] \tag{6}$$

with at most one exception $u \in R_2$ such that $f_u = 0$,
and that

$$f_w \in [0, 1] \qquad \text{for } w \in [m_2 + 1, k]. \tag{7}$$

Furthermore, we show that

$$|\sum\nolimits^{\circ}(A_0) + \sum\nolimits_{f_1}(\widetilde{A_1}) + \cdots + \sum\nolimits_{f_k}(\widetilde{A_k})| = q$$

for every $\bar{g} \in G/H$, where $f_1 = f_1(n, \bar{g}), \ldots, f_k = f_k(n, \bar{g})$ are given as (5), (6) and (7). This would implies $\sum(A) = G$, which is a contradiction.

Based on the above, we shall require the following two lemmas.

Lemma 3.5. *For $n \in [0, m_4]$, if*

$$q - 3 - \ell_0 - 3n + \delta(r_2) \geq p$$

then $\alpha_n = p$.

Proof. We may assume without loss of generality that $\ell_i \leq p + 2$ for $i \in [1, n]$, and that $\ell_j \leq p$ for $j \in [n+1, m_4]$. This implies that

$$|X_i^{\Delta}| = \ell_i - 3 \quad \text{for} \;\; i \in [1, n], \tag{8}$$

and

$$|X_j| = \ell_j - 1 \quad \text{for} \quad j \in [n+1, m_3]. \tag{9}$$

Denote $t = |[1,n] \cap R_4|$. That is,

$$\ell_{n-t+1} = \ell_{n-t+2} = \cdots = \ell_n = 4 \tag{10}$$

and

$$\ell_i \geq 5 \quad \text{for} \quad i \in [1, n-t].$$

Thus,

$$|X_i^{\Delta}| = 1 \quad \text{for} \quad i \in [n-t+1, n]. \tag{11}$$

It follows from (8), (9), (10), (11) and Lemma 2.4 that

$$\begin{aligned}
\alpha_n &= \min(p, |\sum_{i=1}^{n-t} X_i^{\Delta} + \sum_{i=n-t+1}^{n} X_i^{\Delta} + \sum_{i=n+1}^{m_3} X_i + \sum_{i=m_2+1}^{k} X_i + Y|) \\
&= \min(p, |\sum_{i=1}^{n-t} X_i^{\Delta} + \sum_{i=n+1}^{m_3} X_i + \sum_{i=m_2+1}^{k} X_i + Y|) \\
&= \min(p, \sum_{i=1}^{n-t} |X_i^{\Delta}| + \sum_{i=n+1}^{m_3} |X_i| + \sum_{i=m_2+1}^{k} |X_i| + (r_2 + \delta(r_2)) - 1) \\
&= \min(p, \sum_{i=1}^{n-t} (\ell_i - 3) + \sum_{i=n+1}^{m_3} (\ell_i - 1) + \sum_{i=m_2+1}^{k} (\ell_i + 1) \\
&\quad + (\sum_{i=m_3+1}^{m_2} (\ell_i - 1) + \delta(r_2)) - 1) \\
&= \min(p, \sum_{i=1}^{k} \ell_i - \sum_{i=n-t+1}^{n} \ell_i - 3(n-t) - (m_3 - n) \\
&\quad + (k - m_2) - (m_2 - m_3) + \delta(r_2) - 1) \\
&= \min(p, (p + q - 3 - \ell_0) - 4t - 3(n-t) + n + k \\
&\quad - 2m_2 + \delta(r_2) - 1) \\
&= \min(p, p + q - 3 - \ell_0 - t - 2n + k - 2(k - r_1) + \delta(r_2) - 1) \\
&\geq \min(p, p + q - 3 - \ell_0 - n - 2n + k - 2(k - r_1) + \delta(r_2) - 1) \\
&\geq \min(p, p + q - 3 - \ell_0 - 3n - k + \delta(r_2) - 1) \\
&\geq \min(p, p + q - 3 - \ell_0 - 3n - (p-1) + \delta(r_2) - 1)
\end{aligned}$$

$$= \quad p.$$

Then the lemma follows. ∎

Lemma 3.6. *Assume that there exists some $n \in [0, m_4]$ such that $\alpha_n = p$ and $\sum_{i=0}^{n} \ell_i + \epsilon(\ell_0) - 3n - \delta(r_2) \geq 3$. For every element $\bar{g} \in G/H$,*

$$|\sum\nolimits^{\circ}(A_0) + \sum_{i=1}^{k} \sum\nolimits_{f_i}(\widetilde{A_i})| = q$$

where $f_1 = f_1(n, \bar{g}), \ldots, f_k = f_k(n, \bar{g})$.

Proof. By (5), (6), (7), Lemma 2.3, Lemma 2.6 (i) and Lemma 2.8, we have that

$$\begin{aligned}
& |\sum\nolimits^{\circ}(A_0) + \sum_{i=1}^{k} \sum\nolimits_{f_i}(\widetilde{A_i})| \\
= \quad & |\sum\nolimits^{\circ}(A_0) + \sum_{i=1}^{m_2} \sum\nolimits_{f_i}(\widetilde{A_i})| \\
\geq \quad & \min(q, |\sum\nolimits^{\circ}(A_0)| + \sum_{i=1}^{n} |\sum\nolimits_{f_i}(\widetilde{A_i})| + \sum_{i=n+1}^{m_3} |\sum\nolimits_{f_i}(\widetilde{A_i})| \\
& \quad + \sum_{i=m_3+1}^{m_2} |\sum\nolimits_{f_i}(\widetilde{A_i})| - m_2) \\
\geq \quad & \min(q, (2\ell_0 - 1 + \epsilon(\ell_0)) + \sum_{i=1}^{n}(2\ell_i - 3) + \sum_{i=n+1}^{m_3} \ell_i \\
& \quad + (\sum_{i=m_3+1}^{m_2} \ell_i - \delta(r_2)) - (k - r_1)) \\
\geq \quad & \min(q, (2\ell_0 - 1 + \epsilon(\ell_0)) + \sum_{i=1}^{n}(2\ell_i - 3) + \sum_{i=n+1}^{m_3} \ell_i \\
& \quad + (\sum_{i=m_3+1}^{m_2} \ell_i - \delta(r_2)) - (k - \sum_{i=m_2+1}^{k} \ell_i)) \\
= \quad & \min(q, \sum_{i=0}^{k} \ell_i + \sum_{i=0}^{n} \ell_i + \epsilon(\ell_0) - 3n - \delta(r_2) - (k+1))
\end{aligned}$$

$$\begin{aligned} &\geq \min(q, p+q-3+\sum_{i=0}^{n} \ell_i + \epsilon(\ell_0) - 3n - \delta(r_2) - p) \\ &= q. \end{aligned}$$

Then the lemma follows. ∎

Now we are in a position to prove Theorem 1.1 for the remaining case.

Proof of Theorem 1.1 for the case that $G = Z_{pq}$ with $q \geq 2p+3$.

Suppose $\ell_0 \geq \lfloor 2\sqrt{q-2} \rfloor$. By Lemma 2.6 (iii), we have $\sum(A_0) = H = \langle A_0 \rangle$. By Observation 3.1, we have $A_0 = H \setminus \{0\}$ and so $|\bigcup_{i=1}^{k} A_i| = |A| - |A_0| = p-2$. It follows from Lemma 2.9 that there exists an element $g \in G \setminus H$ such that $\bigcup_{i=1}^{k} A_i \subseteq (g+H) \cup (-g+H)$, we are done. Therefore, we may assume that

$$\ell_0 \leq \lfloor 2\sqrt{q-2} \rfloor - 1, \tag{12}$$

equivalently,

$$\sum_{i=1}^{k} \ell_i \geq (p+q-3) - (\lfloor 2\sqrt{q-2} \rfloor - 1) \geq p+3. \tag{13}$$

Claim A. $\ell_i \leq p+1$ for all $i \in [1,k]$.

Assume to the contrary that $\ell_1 \geq p+2$. It follows from (13) that (i) $\ell_1 \geq p+3$ or (ii) $\sum_{i=2}^{k} \ell_i \geq 1$. If (i) holds, then $|X_1^{\Delta}| = p$ and so $\alpha_1 = p$. If (ii) holds, it is easy to see $|\sum_{i=2}^{m_3} X_i + \sum_{i=m_2+1}^{k} X_i + Y| \geq 2$, by Lemma 2.1, $\alpha_1 = |X_1^{\Delta} + \sum_{i=2}^{m_3} X_i + \sum_{i=m_2+1}^{k} X_i + Y| = p$. Since $\ell_1 + \ell_0 + \epsilon(\ell_0) \geq p+2+2 \geq 7$, applying Lemma 3.6 with $n=1$, we derive a contradiction. This proves Claim A. ∎

Claim B. $\ell_0 + \epsilon(\ell_0) - \delta(r_2) \leq 2$.

Assume to the contrary that $\ell_0 + \epsilon(\ell_0) - \delta(r_2) \geq 3$. By Lemma 3.6, we have $\alpha_0 < p$, and thus, by (12) and Lemma 3.5,

$$\begin{aligned}
p - 1 &\geq q - \ell_0 - 3 \\
&\geq q - (\lfloor 2\sqrt{q-2} \rfloor - 1) - 3 \\
&\geq \frac{q+1}{2} - 3 \\
&\geq \frac{(2p+3)+1}{2} - 3 \\
&= p - 1,
\end{aligned}$$

which implies

$$q - (\lfloor 2\sqrt{q-2} \rfloor - 1) = \frac{q+1}{2}, \tag{14}$$

and

$$q = 2p + 3. \tag{15}$$

By (15), we have $p \neq 3$ and so $q \geq 13$. Thus, we check that

$$q - (\lfloor 2\sqrt{q-2} \rfloor - 1) > \frac{q+1}{2},$$

a contradiction with (14). This proves Claim B. ∎

By Claim B, we have

$$\ell_0 \leq 3.$$

Observe that

$$\sum_{i=1}^{k} \ell_i = q + p - 3 - \ell_0 \geq (2p+3) + p - 3 - \ell_0 = 3(p-1) + (3 - \ell_0). \tag{16}$$

Suppose $\delta(r_2) = 0$. By Claim B, we have $\ell_0 \leq 2$. By (16), we have $\ell_1 \geq 4$. By Lemma 3.5, we check that $\alpha_1 = p$. By Lemma 3.6, we derive a contradiction. Therefore,

$$\delta(r_2) = 1. \tag{17}$$

Suppose $\ell_0 = 3$. Since $\ell_k \leq 2$, it follows from (16) that $\ell_1 \geq 4$. Applying Lemma 3.5 with $n = 1$ and Lemma 3.6, we derive a contradiction. Hence,

$$\ell_0 \leq 2. \tag{18}$$

Suppose $\ell_1 \geq 5$. By Lemma 3.5, we check that $\alpha_1 = p$. By Lemma 3.6, we derive a contradiction. Therefore,

$$\ell_1 \leq 4. \tag{19}$$

By (16), (17), (18) and (19), we conclude that

$$\ell_1 = \ell_2 = 4$$

and so $p \geq 5$. It follows that

$$q = |A| - p + 3 \leq \ell_0 + \sum_{i=1}^{3} \ell_i + \ell_4 - 2 \leq 2 + 3 \times 4 + 2 - 2 = 14,$$

which implies

$$q = 13$$

and

$$p = 5.$$

Noting that $\ell_0 \leq 2$, $\ell_1 = \ell_2 = 4$, $\ell_4 = 2$ and $\ell_3 = 5 - \ell_0 \geq 3$, we shall close this proof by deriving a contradiction in the following.

Suppose that $\ell_3 \geq 4$ or $\varphi(a_3) \neq -\varphi(a_4)$. Let $X_4^{\blacklozenge} = \{0, \varphi(a_4), 2\varphi(a_4)\}$. By Lemma 2.1 and Lemma 2.5, we have $|X_3 + X_4^{\blacklozenge}| = p$, and so $|X_1^{\Delta} + X_2^{\Delta} + X_3 + X_4^{\blacklozenge}| = p$. This implies that for every element $\bar{g} \in G/H$, there exists a representation with coefficient $f_1 = f_1(\bar{g}), \ldots, f_4 = f_4(\bar{g})$, where $f_1 = f_2 = 2$, $f_3 \in [1, \ell_3 - 1]$ and $f_4 \in [0, \ell_4]$. It follows from Lemma 2.3 and Lemma 2.6 (iii) that

$$\begin{aligned}
&|\sum\nolimits^{\circ}(A_0) + \sum_{i=1}^{4} \sum\nolimits_{f_i}(\widetilde{A_i})| \\
&\geq |\sum\nolimits^{\circ}(A_0) + \sum_{i=1}^{3} \sum\nolimits_{f_i}(\widetilde{A_i})| \\
&\geq \min(q, |\sum\nolimits^{\circ}(A_0)| + \sum_{i=1}^{2} |\sum\nolimits_{f_i}(\widetilde{A_i})| + |\sum\nolimits_{f_3}(\widetilde{A_3})| - 3) \\
&\geq \min(q, (2\ell_0 - 1 + \epsilon(\ell_0)) + (\ell_1 + 1) + (\ell_2 + 1) + \ell_3 - 3) \\
&\geq \min(q, (2\ell_0 - 1 + \epsilon(\ell_0)) + 5 + 5 + (5 - \ell_0) - 3)
\end{aligned}$$

$$= \min(q, \ell_0 + \epsilon(\ell_0) + 11)$$
$$= q.$$

This implies that $\sum(A) = G$, a contradiction. Therefore,

$$\ell_3 = 3$$

and

$$\varphi(a_3) = -\varphi(a_4),$$

which implies

$$\varphi(a_2) \notin \{\varphi(a_3), -\varphi(a_3)\}.$$

By Lemma 2.5, we have $|X_2 + X_3| \geq \min(p, |X_2| + |X_3|) = p$, and so $|X_1^{\Delta} + X_2 + X_3 + X_4| = p$. This implies that for every element $\bar{g} \in G/H$, there exists a representation with coefficient $f_1 = f_1(\bar{g}), \ldots, f_4 = f_4(\bar{g})$, where $f_1 = 2$, $f_2 \in [1, \ell_2 - 1]$, $f_3 \in [1, \ell_3 - 1]$ and $f_4 = 1$. It follows Lemma 2.3 and Lemma 2.6 (iii) that

$$\begin{aligned}
&|\sum{}^{\circ}(A_0) + \sum_{i=1}^{4} \sum\nolimits_{f_i}(\widetilde{A_i})| \\
&\geq \min(q, |\sum{}^{\circ}(A_0)| + |\sum\nolimits_{f_1}(\widetilde{A_1})| + \sum_{i=2}^{4} |\sum\nolimits_{f_i}(\widetilde{A_i})| - 4) \\
&\geq \min(q, (2\ell_0 - 1 + \epsilon(\ell_0)) + (\ell_1 + 1) + \ell_2 + \ell_3 + \ell_4 - 4) \\
&\geq \min(q, (2\ell_0 - 1 + \epsilon(\ell_0)) + 5 + 4 + (5 - \ell_0) + 2 - 4) \\
&\geq \min(q, \ell_0 + \epsilon(\ell_0) + 11) \\
&= q.
\end{aligned}$$

This implies that $\sum(A) = G$, a contradiction. ∎

4 Conclusion

We first give examples to show that the conclusion of Theorem 1.1 does not hold true for the group $G = Z_{pq}$ with $q < 2p + 3$.

Example 4.1. *Let p, q be two odd prime numbers with $p+\lfloor 2\sqrt{p-2}\rfloor+1 < q < 2p+3$, and let $G = Z_{pq}$. Let K be the subgroup of G of order p. Let $A \subseteq K \cup (g+K) \cup (-g+K)$ be a subset of G with $|A| = \mathrm{cr}(G) - 1 = p+q-3 < 3p$ and $A \cap K = K \setminus \{0\}$, where $g \in G \setminus K$.*

Example 4.2. *Let p, q be two odd prime numbers with $p < q \leq p + \lfloor 2\sqrt{p-2}\rfloor + 1$, and let $G = Z_{pq}$. Let $A = \{\pm g, \pm 2g, \ldots, \pm \frac{p+q-2}{2} g\}$ with $|A| = \mathrm{cr}(G) - 1 = p+q-2$, where $g \in G$ and $\mathrm{ord}(g) = pq$.*

It is easy to check that $\sum(A) \neq G$ in both Example 4.1 and Example 4.2. However, we don't observe any other counterexamples. Therefore, we conjecture the following

Conjecture 4.3. *Let p, q be two odd prime numbers with $p+\lfloor 2\sqrt{p-2}\rfloor + 1 < q < 2p+3$, and let A be a subset of $G = Z_{pq}$ with $|A| = \mathrm{cr}(G) - 1 = p+q-3$ and $0 \notin A$. Then A contains a complete subset.*

Conjecture 4.4. *Let p, q be two odd prime numbers with $p < q \leq p + \lfloor 2\sqrt{p-2}\rfloor + 1$, and let A be a subset of $G = Z_{pq}$ with $|A| = \mathrm{cr}(G) - 1 = p+q-2$ and $0 \notin A$. Then there exists an element $g \in G$ of order pq such that $A = \{\pm g, \pm 2g, \ldots, \pm \frac{p+q-2}{2} g\}$*

We remark that, as shown in [18], in most finite abelian groups G, the comparatively large set A fails to span the whole group G just because that most elements of A concentrate in some proper subgroup of G, i.e., A contains a complete subset. Therefore, we formulate the following theorem which is easy to proved to be equivalent to Theorem B and Theorem 1.1 by Observation 3.1 and Lemma 2.9.

Theorem C. *Let G be a finite abelian group, and let p be the smallest prime dividing $|G|$. Let A be a subset of $G \setminus \{0\}$ with $|A| = \mathrm{cr}(G) - 1$. Then A contains a complete subset provided that G is one of the following types:*

1. *$|G|$ is an even number no less than 36.*
2. *$\frac{|G|}{p}$ is composite and*

$$\frac{|G|}{p} \geq \begin{cases} 62, & \text{if } p = 3; \\ 7p+3, & \text{if } p \geq 5. \end{cases}$$

3. $|G|$ is a product of two odd prime numbers p, q with $q \geq 2p + 3$.

Acknowledgement. *The authors are grateful to the the referee for helpful suggestions and comments.*

References

[1] J.A. Dias da Silva, Y.O. Hamidoune, *Cyclic spaces for Grassmann derivatives and additive theory*, Bull. London Math. Soc, **26** (1994) 140–146.

[2] G.T. Diderrich, *An Addition Theorem for Abelian Groups of Order pq*, J. Number Theory, **7** (1975) 33–48.

[3] P. Erdős, H. Heilbronn, *On the addition of residue classes* mod p, Acta Arith., **9** (1964) 149–159.

[4] M. Freeze, W.D. Gao, A. Geroldinger, *The critical number of finite abelian groups*, J. Number Theory, **129** (2009) 2766–2777.

[5] W.D. Gao, *A combinatorial problem on finite groups*, Acta Math. Sinica, **38** (1995) 395-399.

[6] W.D. Gao, Y.O. Hamidoune, *On additive bases*, Acta Arith., **88** (1999) 233–237.

[7] W.D. Gao, Y.O. Hamidoune, A. Lladó, O. Serra, *Covering a finite abelian group by subset sums*, Combinatorica, **23** (2003) 599–611.

[8] W.D. Gao, J.T. Peng, G.Q. Wang, *Behaving sequences*, J. Combin. Theory Ser. A, **118** (2011) 613–622.

[9] A. Geroldinger, F. Halter-Koch, *Non-unique factorizations: Combinatorial and Analytic Theory*, Pure and Applied Mathematics, vol. 278, Chapman & Hall/CRC, 2006.

[10] A. Geroldinger, I. Ruzsa, *Combinatorial Number Theory and Additive Group Theory*, in: Adv. Courses Math. CRM Barcelona, Birkhäuser, 2009.

[11] J.R. Griggs, *Spanning subset sums for finite abelian groups*, Discrete Math., **229** (2001) 89–99.

[12] Y.O. Hamidoune, *Adding distinct congruence classes*, Combin. Probab. Comput., **7** (1998) 81–87.

[13] Y.O. Hamidoune, A.S. Lladó and O. Serra, *On sets with a small subset sum*, Combin. Probab. Comput., **8** (1999) 461–466.

[14] H.B. Mann, *Addition theorems*, John Wiley and Sons, New York, 1965.

[15] M.B. Nathanson, *Additive number theory: Inverse problems and the geometry of sumsets*, Springer, 1996.

[16] Hoi H. Nguyen, Endre Szemerédi, Van H. Vu, *Subset sums modulo a prime*, Acta Arith., **131** (2008) 303–316.

[17] Hoi H. Nguyen, Van H. Vu, *Classification theorems for sumsets modulo a prime*, J. Comb. Theory Ser. A, **116** (2009) 936–959.

[18] Van H. Vu, *Structure of large incomplete sets in abelian groups*, Combinatorica, **30** (2010) 225–237.

[19] Q.H. Wang, Y.K. Qu, *On the critical number of finite groups (II)*, Ars Combin., to appear.