1

The critical number of finite abelian groups

Michael Freeze

The University of North Carolina at Wilmington
Department of Mathematics and Statistics
Wilmington, North Carolina 28403-5970, USA

Weidong Gao

Center for Combinatorics, Nankai University, Tianjin 300071, P.R. China

Alfred Geroldinger

Institut für Mathematik und Wissenschaftliches Rechnen
Karl–Franzens–Universität Graz
Heinrichstraße 36
8010 Graz, Austria

Abstract

Let G be an additive, finite abelian group. The critical number $\mathsf{cr}(G)$ of G is the smallest positive integer ℓ such that for every subset $S \subset G \setminus \{0\}$ with $|S| \ge \ell$ the following holds: Every element of G can be written as a nonempty sum of distinct elements from S. The critical number was first studied by P. Erdős and H. Heilbronn in 1964, and due to the contributions of many authors the value of $\mathsf{cr}(G)$ is known for all finite abelian groups G except for $G \cong \mathbb{Z}/pq\mathbb{Z}$ where p, q are primes such that $p + \lfloor 2\sqrt{p-2} \rfloor + 1 < q < 2p$. We determine that $\mathsf{cr}(G) = p + q - 2$ for such groups.

Key words: critical number, finite abelian groups, sumsets
2000 MSC: 11P70, 11B50, 11B75

1. Introduction and Main Results

Let G be an additive, finite abelian group. The critical number $\mathsf{cr}(G)$ of G is the smallest positive integer ℓ such that every subset $S \subset G \setminus \{0\}$ with $|S| \ge \ell$ has the following property: every element of G can be written as a nonempty sum of distinct elements from S.

Email addresses: `freezem@uncw.edu` (Michael Freeze), `wdgao_1963@yahoo.com.cn` (Weidong Gao), `alfred.geroldinger@uni-graz.at` (Alfred Geroldinger)

The critical number was first studied by P. Erdős and H. Heilbronn (see [4]) for cyclic groups of prime order in 1964. After main contributions by H.B. Mann, J.E. Olson, G.T. Diderrich, Y.F. Wou, J.A. Dias da Silva, Y. ould Hamidoune and W. Gao, the precise value of $\mathsf{cr}(G)$ (in terms of the group invariants of G) was determined, apart from cyclic groups of order pq where p and q are primes with $p + \lfloor 2\sqrt{p-2} \rfloor + 1 < q < 2p$. We settle this remaining case in the following Theorem 1.1. Its proof is based on ideas of G.T. Diderrich (developed in his work on cyclic groups of order pq) and on the solution of the Erdős-Heilbronn Conjecture by J.A. Dias da Silva and Y. ould Hamidoune.

Theorem 1.1. *Let G be a cyclic group of order pq where p, q are primes with $p + \lfloor 2\sqrt{p-2} \rfloor + 1 < q < 2p$. Then $\mathsf{cr}(G) = p + q - 2$.*

We consequently have the following determination of the value of the critical number for all finite abelian groups. Apart from Theorem 1.1, it is based on the fundamental work of many authors, and at the end of Section 2 we will provide detailed references to all contributions. Note that, by definition, $|G| \le 2$ implies that $\mathsf{cr}(G) = |G|$.

Theorem 1.2. *Let G be a finite abelian group of order $|G| \ge 3$, and let p denote the smallest prime divisor of $|G|$.*

1. *If $|G| = p$, then $\mathsf{cr}(G) = \lfloor 2\sqrt{p-2} \rfloor$.*
2. *In each of the following cases we have $\mathsf{cr}(G) = \frac{|G|}{p} + p - 1$:*
   - *G is isomorphic to one of the following groups: $C_3 \oplus C_3$, $C_2 \oplus C_2$, C_4, C_6, $C_2 \oplus C_4$, C_8.*
   - *$|G|/p$ is an odd prime with $2 < p < \frac{|G|}{p} \le p + \lfloor 2\sqrt{p-2} \rfloor + 1$.*
3. *In all other cases we have $\mathsf{cr}(G) = \frac{|G|}{p} + p - 2$.*

The work on the precise value of the critical number is complemented by investigations on the structure of sets $S \subset G \setminus \{0\}$ with $|S| \le \mathsf{cr}(G)$ and which have the property that every group element can be written as a nonempty sum of distinct elements from S. We refer to recent work of Y. ould Hamidoune, A.S. Lladó and O. Serra, see [6] and [11].

Throughout this article, let G be an additively written, finite abelian group.

2. Notation and tools from Additive Group Theory

Let $\mathbb{N}$ denote the set of positive integers, $\mathbb{P} \subset \mathbb{N}$ the set of prime numbers, and let $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. For real numbers $a, b \in \mathbb{R}$, we set $[a, b] = \{x \in \mathbb{Z} \mid a \le x \le b\}$.

For $n \in \mathbb{N}$, let C_n denote a cyclic group with n elements. Throughout, all abelian groups will be written additively.

Let $A, B \subset G$ be nonempty subsets. Then $A + B = \{a + b \mid a \in A, b \in B\}$ denotes their *sumset*. The set A is called an *arithmetic progression with difference* $d \in G$ if there is some $a \in G$ such that $A = \{a + \nu d \mid \nu \in [0, |A| - 1]\}$. If $A = \{a_1, \ldots, a_\ell\}$ and $k \in \mathbb{N}$, we denote the restricted sumset by

$$\Sigma_k(A) = \{\sum_{i \in I} a_i \mid I \subset [1, \ell] \text{ with } |I| = k\} \quad \text{and write} \quad \Sigma(A) = \bigcup_{k \geq 1} \Sigma_k(A)\,.$$

In particular, $A = \emptyset$ if and only if $\Sigma(A) = \emptyset$, and for convenience we set $\Sigma_0(A) = \{0\}$. Thus in more technical terms, the *critical number* $\mathsf{cr}(G)$ is the smallest integer $\ell \in \mathbb{N}$ such that every subset $S \subset G \setminus \{0\}$ with $|S| \geq \ell$ satisfies $\Sigma(S) = G$.

Now we provide the background necessary to prove Theorem 1.1. We start with the classical addition theorem of Cauchy-Davenport (see [7, Corollary 5.2.8]).

Theorem 2.1. (*Cauchy-Davenport*) *Let G be prime cyclic of order p, $s \in \mathbb{N}_{\geq 2}$, and $A_1, \ldots, A_s \subset G$ nonempty subsets. Then*

$$|A_1 + \ldots + A_s| \geq \min\Big\{p, \sum_{i=1}^{s} |A_i| - s + 1\Big\}\,.$$

In Theorem 2.1 of [2] and a following remark, G.T. Diderrich improved the Cauchy-Davenport bound under extra structure assumptions on $A_1, \ldots, A_s$.

Theorem 2.2. (*Diderrich*) *Let G be prime cyclic of order p, $s \in \mathbb{N}_{\geq 2}$ and $A_1, \ldots, A_s \subset G$ nonempty subsets such that all subsets, apart from one possible exception, are arithmetic progressions with pairwise distinct nonzero differences. Then*

$$|A_1 + \ldots + A_s| \ \geq \min\Big\{p, \sum_{i=1}^{s} |A_i| - 1\Big\}\,.$$

The Theorem of Dias da Silva and Hamidoune settled the Erdős-Heilbronn Conjecture on restricted sumsets (see [1] for the original paper, and also [10, Theorems 3.4 and 3.8]).

Theorem 2.3. (*Dias da Silva-Hamidoune*) *Let G be prime cyclic of order p, $S \subset G$ a subset and $k \in [1, |S|]$.*

1. $|\Sigma_k(S)| \geq \min\{p, k(|S| - k) + 1\}$.
2. *If $|S| = \lfloor \sqrt{4p - 7} \rfloor$ and $k = \lfloor |S|/2 \rfloor$, then $\Sigma_k(S) = G$.*

Clearly, the second item of 2.3 is a special case of the first item. Simple calculations show that $k \in [2, |S|-1]$, then $k(|S|-k)+1 \ge |S|$ whence $|\Sigma_k(S)| \ge |S|$. We use these observations throughout the paper.

For the convenience of the reader we offer a proof of Theorem 1.2 based on Theorem 1.1 and on the fundamental work of prior authors, which is scattered in the literature and for which we offer precise references. Moreover, we recall the classical example showing that for $|G| > p$ we have

$$\mathsf{cr}(G) \ge \frac{|G|}{p} + p - 2\,, \quad \text{where } p \text{ is the smallest prime divisor of } |G|\,.$$

Let $H \subset G$ be a subgroup with $(G:H) = p$. Then there exist $h_1, \ldots, h_{p-2} \in G \setminus H$ such that $h_1 + H = h_i + H$ for all $i \in [1, p-2]$. Then for $S = (H \setminus \{0\}) \cup \{h_1, \ldots, h_{p-2}\}$ we have $\Sigma(S) \subset H \cup (h_1 + H) \cup \ldots \cup \big((p-2)h_1 + H\big)$. This shows that $|\Sigma(S)| \le (p-1)|H| < |G|$ and thus $\mathsf{cr}(G) \ge |S| + 1 = |G|/p + p - 2$.

Proof of Theorem 1.2, based on 1.1. Let $|G| \ge 3$ and p be the smallest prime divisor of $|G|$.

CASE 1: G is cyclic of order p.

Note, since $p \ge 3$, we have $\sqrt{4p-7} \notin \mathbb{N}$ and thus $\lfloor \sqrt{4p-7} \rfloor = \lfloor \sqrt{4p-8} \rfloor = \lfloor 2\sqrt{p-2} \rfloor$. Thus Theorem 2.3 by Dias da Silva and Hamidoune shows that $\lfloor 2\sqrt{p-2} \rfloor$ is an upper bound (see [1, Corollary 4.2] for details), and simple examples show that the bound is sharp (see [1, Example 4.2] and [8, Theorem 7]).

CASE 2: $G = C_p \oplus C_p$ with $p \ge 3$.

H.B. Mann and J.E. Olson showed that $\mathsf{cr}(G) \le 2p - 1$ (with equality for $p = 3$), and after that $\mathsf{cr}(G) = 2p - 2$ for all $p \ge 5$ was proved by H.B. Mann and Ying Fou Wou (see [9]).

CASE 3: $G = C_p \oplus C_q$ for a prime q with $3 \le p < q$.

The case $q \le p + \lfloor 2\sqrt{p-2} \rfloor + 1$ was settled by J.R. Griggs (see [8, Theorem 4]).

The case $p + \lfloor 2\sqrt{p-2} \rfloor + 1 < q < 2p$ follows from the present Theorem 1.1.

The case $q \ge 2p + 1$ was settled by G.T. Diderrich (see [2, Theorem 1.0]).

CASE 4: $|G|$ is even.

This case was settled by G.T. Diderrich and H.B. Mann in [3], see also [8, Theorem 5] for a self-contained, simplified proof.

CASE 5: $|G|$ is odd and $|G|/p$ is composite.

Then $\mathsf{cr}(G) = |G|/p + p - 2$ by W. Gao and Y. ould Hamidoune (see [5]). $\square$

3. The setting and the strategy of the proof

First, we fix our notations which remain valid throughout the rest of the paper, and then we outline the strategy of the proof of Theorem 1.1.

Let G be cyclic of order pq where p, q are primes with $p+\lfloor 2\sqrt{p-2}\rfloor+1 < q < 2p$ (which implies that $p \ge 7$) and let $S \subset G\setminus\{0\}$ be a subset with $|S| = p+q-2$.

Let $H, K \subset G$ be the subgroups with $(G : H) = p$ and $(G : K) = q$. Let $s = |\{a + H \in G/H \mid a \in S \setminus H\}|$ and pick $a_1, \ldots, a_s \in S \setminus H$ such that $|\{a_i + H \mid i \in [1, s]\}| = s$. We set $S_0 = H \cap S$ and $S_i = (a_i + H) \cap S$ for all $i \in [1, s]$.

Suppose that $a_1, \ldots, a_s$ and $t, r, n \in \mathbb{N}_0$ are chosen in such a way that

- $|S_1| \ge \ldots \ge |S_t| \ge 3$,
- $|S_{t+1}| = \ldots = |S_{t+r}| = 1$ and
- $|S_{t+r+1}| = \ldots = |S_{t+r+u}| = 2$.

Notice that

$$s = t + r + u \le p - 1 \quad \text{and} \quad |S_0| + \sum_{i=1}^{t} |S_i| + r + 2u = p + q - 2 = |S| \,.$$

For an element $x \in G$ we consider a representation

$$x + H = \sum_{i=1}^{s} f_i(a_i + H) \tag{$*$}$$

with $f_i \in [0, |S_i|]$ for all $i \in [1, s]$ and $f_1 + \ldots + f_s > 0$. If $f_i \in \{0, |S_i|\}$, then f_i is called a *collapsed coefficient* and

$$C(*) = \sum_{i=1, f_i \in \{0,|S_i|\}}^{s} (|S_i| - 1)$$

is called the *collapse* of the representation $(*)$. We say that G/H *has a representation with collapse* $C \in \mathbb{N}_0$ if every $x \in G$ has a representation $(*)$ and C is the maximum of the collapses $C(*)$.

We provide an example to illustrate the definition of the collapse of a representation.

Example 3.1. Following the notation introduced above, consider the cyclic group $G = \mathbb{Z}/91\mathbb{Z}$ and the subgroup H of order 13. Take

$$S = \{\overline{2}, \overline{5}, \overline{7}, \overline{8}, \overline{10}, \overline{13}, \overline{15}, \overline{21}, \overline{24}, \overline{34}, \overline{37}, \overline{40}, \overline{43}, \overline{46}, \overline{63}, \overline{66}, \overline{71}, \overline{72}\},$$

and fix $a_1 = \overline{8}$, $a_2 = \overline{2}$, $a_3 = \overline{10}$, $a_4 = \overline{46}$, $a_5 = \overline{5}$, $a_6 = \overline{13}$.

Note that $|S_0| = 3$, $|S_1| = 4$, $|S_2| = 3$, $|S_3| = 3$, $|S_4| = 1$, $|S_5| = 2$, and $|S_6| = 2$.

We may represent $\overline{1}$ by

$$\overline{1} = 1(\overline{8}) + 0(\overline{2}) + 0(\overline{10}) + 0(\overline{46}) + 0(\overline{5}) + 0(\overline{13}),$$

noting that each of the five zero-coefficients are collapsed so that the collapse of the representation is $2 + 2 + 0 + 1 + 1 = 6$.

We may also represent $\overline{1}$ by

$$\overline{1} = 2(\overline{8}) + 1(\overline{2}) + 1(\overline{10}) + 1(\overline{46}) + 1(\overline{5}) + 1(\overline{13}),$$

and this representation has only one collapsed coefficient, namely the coefficient 1 of $\overline{46}$ since $|S_4| = 1$. The collapse of this representation is then 0.

As will be seen later, representations with small collapse are advantageous for our approach.

The strategy of the proof is as follows. First we settle the very simple case where $|S_0| \geq \lfloor 2\sqrt{q-2} \rfloor$. After supposing that $|S_0| \leq \lfloor 2\sqrt{q-2} \rfloor - 1$ we follow the ideas of G.T. Diderrich and proceed in two steps:

1. First, we show that G/H has a representation with some collapse $C \in \mathbb{N}_0$ (see Lemmas 4.3, 4.2, 4.7).

2. For $x \in G$ and a representation $(*)$ we show that

$$|(\Sigma(S_0) \cup \{0\}) + \Sigma_{f_1}(S_1) + ... + \Sigma_{f_s}(S_s)| \geq q\,.$$

Suppose that **1.** and **2.** are settled. Notice that

$$\begin{aligned}(\Sigma(S_0) \cup \{0\}) + \Sigma_{f_1}(S_1) + ... + \Sigma_{f_s}(S_s) &\subset H + f_1(a_1 + H) + ... + f_s(a_s + H) \\ &= H + \sum_{i=1}^{s} f_i(a_i + H) = x + H\,.\end{aligned}$$

Thus **2.** implies that we have equality in the above inclusion. Therefore

$$x + H = (\Sigma(S_0) \cup \{0\}) + \Sigma_{f_1}(S_1) + ... + \Sigma_{f_s}(S_s) \subset \Sigma(S)\,,$$

and together with **1.** we obtain $G = \Sigma(S)$.

4. Proof of Theorem 1.1

We start with a simple special case.

Proposition 4.1. *If* $|S_0| \geq \lfloor 2\sqrt{q-2} \rfloor$, *then* $\Sigma(S) = G$.

Proof. Suppose that $|S_0| \ge \lfloor 2\sqrt{q-2} \rfloor$. Since, by Theorem 1.2.1, $\mathsf{cr}(H) = \lfloor 2\sqrt{q-2} \rfloor$, it follows that $\Sigma(S_0) = H$. Since $|S \setminus H| \ge p+q-2-(q-1) = p-1$, we can choose $p-1$ distinct elements $b_1, \cdots, b_{p-1} \in S \setminus H$. For $i \in [1, p-1]$ we set $W_i = \{0 + H, b_i + H\} \subset G/H$, and by Theorem 2.1 we obtain that

$$|\Sigma(W_1 + \ldots + W_{p-1})| \ge \min\{p, 2(p-1) - (p-1) + 1\} = p\,.$$

Thus it follows that

$$\Sigma(S) \supset \Sigma(S_0) + \big(\Sigma(\{b_1, \ldots, b_{p-1}\}) \cup \{0\}\big) = G\,. \qquad \square$$

Hence from now on we may assume that $|S_0| \le \mathsf{cr}(H) - 1$, and we proceed in the two steps described above.

Lemma 4.2. *If $t \ge \lfloor 2\sqrt{p-2} \rfloor$, then G/H has a representation with collapse $C = 0$.*

Proof. By Theorem 1.2.1, we have $t \ge \lfloor 2\sqrt{p-2} \rfloor = \mathsf{cr}(G/H)$ and thus $\Sigma(\{a_1 + H, \ldots, a_t + H\}) = G/H$. Pick some $x \in G$. Then there exists a nonempty subset $I \subset [1, t]$ such that

$$x - (a_1 + \ldots + a_s) + H = \sum_{i \in I} (a_i + H)$$

and hence

$$x + H = \sum_{i \in I} 2(a_i + H) + \sum_{i \in [1,t] \setminus I} (a_i + H) + \sum_{i=t+1}^{s} (a_i + H)\,. \qquad (**)$$

Since $|S_i| \ge 3$ for all $i \in [1, t]$, the representation $(**)$ has collapse $C(**) = 0$. $\square$

Lemma 4.3. *If $|S_0| \le \lfloor 2\sqrt{q-2} \rfloor - 1$, then G/H has a representation with collapse $C \le 1$.*

Proof. Suppose that $|S_0| \le \lfloor 2\sqrt{q-2} \rfloor - 1$. We construct sets $A_1, \ldots, A_{t+r}$ and D as follows:

$$\begin{aligned} A_i &= \{a_i + H, \ldots, (|S_i| - 1)a_i + H\} \subset G/H \quad \text{for } i \in [1, t]; \\ A_i &= \{H, a_i + H\} \subset G/H \quad \text{for} \quad i \in [t+1, t+r]; \\ D &= \{b_0, b_0 - b_1, b_0 - b_2, \ldots, b_0 - b_u\} \subset G/H \end{aligned}$$

where $b_j = a_{t+r+j} + H$ for $j \in [1, u]$, and $b_0 = \sum_{j=1}^{u} b_j + H$. We assert that $D + \sum_{i=1}^{t+r} A_i = G/H$. Clearly, this implies that G/H has a representation with collapse $C \le 1$.

Assume to the contrary, that $D + \sum_{i=1}^{t+r} A_i \subsetneq G/H$. Applying the Cauchy-Davenport Theorem and Theorem 2.2, we have

$$\begin{aligned} |D + \sum_{i=1}^{t+r} A_i| &\geq |D| + |\sum_{i=1}^{t+r} A_i| - 1 \\ &\geq |D| + \sum_{i=1}^{t+r} |A_i| - 2 \\ &= u + \sum_{i=1}^{t} |S_i| - t + 2r - 1\,, \end{aligned}$$

and hence

$$u + \sum_{i=1}^{t} |S_i| - t + 2r - 1 \leq p - 1\,. \qquad (***)$$

Since by our constructions,

$$p + q - 2 = |S_0| + \sum_{i=1}^{t} |S_i| + r + 2u\,,$$

we can solve this equation for $\sum_{i=1}^{t} |S_i|$, yielding

$$\begin{aligned} u + (p + q - 2 - |S_0| - r - 2u) - t + 2r - 1 &\leq p - 1 \\ q - u - t + r &\leq |S_0| + 2 \\ q - (u + t + r) + 2r &\leq |S_0| + 2. \end{aligned}$$

Therefore we have

$$q - (u + t + r) + (2r - 1) \leq |S_0| + 1\,.$$

We distinguish two cases.

CASE 1: $|S_0| \leq \lfloor 2\sqrt{q-2} \rfloor - 2$ or $s \leq p - 2$ or $r \geq 1$.

Using $u + t + r = s \leq p - 1$ and the assumption of CASE 1 we obtain

$$q - p + 1 \leq \lfloor 2\sqrt{q-2} \rfloor\,.$$

Here, since $q - p + 1$ is positive, squaring both sides preserves the inequality, giving us

$$\begin{aligned} (q-p)^2 + 2(q-p) + 1 &\leq 4(q-2) \\ q^2 - 2pq + p^2 + 2q - 2p + 1 &\leq 4q - 8 \\ q^2 - 2pq - 2q + p^2 - 2p + 9 &\leq 0 \\ q^2 - (2p+2)q + (p^2 - 2p + 9) &\leq 0. \end{aligned}$$

By considering this as a quadratic in terms of q, we can apply the quadratic formula to find that

$$q \le p + 1 + 2\sqrt{p-2}\,.$$

Since q and $p+1$ are integers, we then have

$$q \le p + 1 + \lfloor 2\sqrt{p-2} \rfloor\,,$$

which is a contradiction to the original restrictions of $p + \lfloor 2\sqrt{p-2} \rfloor + 1 < q < 2p$.

CASE 2: $|S_0| = \lfloor 2\sqrt{q-2} \rfloor - 1$, $s = p-1$ and $r = 0$.

Using $p - 1 = s = t + r + u = t + u$ and $(***)$ we obtain that

$$p - 1 + (t-1) = u + 2t - 1 \le u + \sum_{i=1}^{t} |S_i| - t - 1 \le p - 1\,,$$

whence $t \le 1$.

If $t = 0$, then $p = u + 1 = |D|$ and hence $D = G/H$, a contradiction.

If $t = 1$, then $u = p - 2$ and (looking back at the beginning of the proof) we get

$$p-1 \ge |D + \sum_{i=1}^{t+r} A_i| = |D + A_1| \ge |D| + |A_1| - 1 = (u+1) + (|S_1| - 1) - 1 = u + |S_1| - 1\,,$$

and hence $|S_1| \le 2$, a contradiction. □

We require the following technical Lemma.

Lemma 4.4. *Suppose that G/H has a representation with collapse $C \in \mathbb{N}_0$. If $(p+q-2) + \max\{1, |S_0| - 1\} - C - s \ge q$, then for every $x \in G$ with $C(*) \le C$ we have $|\,(\Sigma(S_0) \cup \{0\}) + \sum_{i=1}^{s} \Sigma_{f_i}(S_i)| \ge q$.*

Proof. For any subset $A \subset G$ we set $\bar{A} = \{a + K \mid a \in A\} \subset G/K$ where $K \subset G$ is the subgroup with $(G\colon K) = q$. Clearly we have $\overline{\Sigma_k(A)} = \Sigma_k(\overline{A})$ for all $k \in \mathbb{N}_0$, $|A| \ge |\overline{A}|$ and if $x \in G$ and $A \subset x + H$, then $|A| = |\overline{A}|$. If $|\Sigma(\overline{S_0}) \cup \{\overline{0}\}| \ge q$, then the statement of the Lemma follows. Suppose that $|\Sigma(\overline{S_0} \cup \{\overline{0}\})| < q$.

We assert that $|\Sigma(S_0) \cup \{0\}| \ge |S_0| + \max\{1, |S_0| - 1\}$. If $|S_0| \le 1$, then this is clear. Suppose that $\overline{S_0} = \{z_1 + K, \ldots, z_\lambda + K\}$ with $z_1, \ldots, z_\lambda \in G$ and $\lambda \ge 2$. Then $\Sigma(\overline{S_0}) \cup \{\overline{0}\} = \{\overline{0}, z_1 + K\} + \ldots + \{\overline{0}, z_\lambda + K\}$, and Theorem 2.2 implies that

$$|\Sigma(S_0) \cup \{0\}| \ge |\Sigma(\overline{S_0}) \cup \{\overline{0}\}| \ge \min\{q, 2\lambda - 1\} = 2|S_0| - 1\,.$$

Let $x \in G$ with representation $(*)$ and let $i \in [1, s]$. If f_i is a collapsed coefficient, then $|\Sigma_{f_i}(S_i)| = |\Sigma_{f_i}(\overline{S_i})| = 1$. If f_i is not a collapsed coefficient, then the observation after Theorem 2.3 gives us

$$|\Sigma_{f_i}(S_i)| \ge |\Sigma_{f_i}(\overline{S_i})| \ge |\overline{S_i}| = |S_i|\,.$$

Thus we obtain

$$|\Sigma(\overline{S_0}) \cup \{\overline{0}\}| + \sum_{i=1}^{s} |\Sigma_{f_i}(\overline{S_i})| \geq \sum_{i=0}^{s} |S_i| + \max\{1, |S_0| - 1\} - C\,,$$

and by Theorem 2.1 we have

$$\begin{aligned} |\,(\Sigma(S_0) \cup \{0\}) + \sum_{i=1}^{s} \Sigma_{f_i}(S_i)| &\geq |\,\big(\Sigma(\overline{S_0}) \cup \{\overline{0}\}\big) + \sum_{i=1}^{s} \Sigma_{f_i}(\overline{S_i})| \\ &\geq \min\{q, |\Sigma(\overline{S_0}) \cup \{\overline{0}\}| + \sum_{i=1}^{s} |\Sigma_{f_i}(\overline{S_i})| - s\} \\ &\geq \min\{q, \sum_{i=0}^{s} |S_i| + \max\{1, |S_0| - 1\} - C - s\} \\ &= \min\{q, p + q - 2 + \max\{1, |S_0| - 1\} - C - s\}\,. \end{aligned}$$

So if $p + q - 2 + \max\{1, |S_0| - 1\} - C - s \geq q$, then the assertion follows. $\square$

Proposition 4.5. *If $3 \leq |S_0| \leq \lfloor 2\sqrt{q-2} \rfloor - 1$, then $\Sigma(S) = G$.*

Proof. Since $|S_0| \leq \lfloor 2\sqrt{q-2} \rfloor - 1$, Lemma 4.3 gives us a representation of G/H with collapse $C \leq 1$. Notice that since $|S_0| \geq 3$, we have $p+q-2+\max\{1, |S_0|-1\} - C - s \geq p + q - 2 + 2 - 1 - (p - 1) = q$. Thus the assertion follows from Lemma 4.4. $\square$

Now consider the case $|S_0| \leq 2$, we contemplate two subcases. First take the case where $|S_1| \leq 3$.

Proposition 4.6. *If $|S_0| \leq 2$ and $|S_1| \leq 3$, then $\Sigma(S) = G$.*

Proof. Since $q \geq 5$, we have $|S_0| \leq 2 < \lfloor 2\sqrt{q-2} \rfloor$. Thus Lemma 4.3 implies that there is a representation of G/H with collapse $C \leq 1$. Thus it remains to verify the assumption of Lemma 4.4, and thus we have to show that

$$(p + q - 2) + \max\{1, |S_0| - 1\} - C - s \geq q\,.$$

Note that $|S_0| \leq 2$ implies that $\max\{1, |S_0| - 1\} = 1$. We have $(p + q - 2) + \max\{1, |S_0| - 1\} - C - s \geq q$ for $s \leq p - 2$. Consider the case $s = p - 1$. Since

$$\begin{aligned} p + q - 2 &= |S_0| + \sum_{i=1}^{t} |S_i| + r + 2u \\ &\leq 2 + 3t + r + 2u \\ &= 2 + s + 2t + u \\ &= p + 1 + 2t + u\,, \end{aligned}$$

it follows that

$$\begin{aligned} q - 2 &\le 1 + 2t + u \\ &= 1 + t + (t + u + r) - r \\ &= 1 + t + (p - 1) - r \\ &= t + p - r. \end{aligned}$$

Since $q \ge p + \lfloor 2\sqrt{p-2} \rfloor + 2$, we see that

$$\begin{aligned} t &\ge q - p - 2 \\ &\ge \lfloor 2\sqrt{p-2} \rfloor. \end{aligned}$$

Consequently, Lemma 4.2 implies that we have collapse $C = 0$. Putting all together we obtain

$$(p + q - 2) + \max\{1, |S_0| - 1\} - C - s \ge (p + q - 2) + 1 - 0 - (p - 1) = q\,,$$

and hence the assumption of Lemma 4.4 is satisfied. □

Finally, we address the remaining case where $|S_0| \le 2$ and $|S_1| \ge 4$.

Lemma 4.7. *If $|S_0| \le 2$ and $|S_1| \ge 4$, then for every $x \in G$ there is a representation $(*)$ of $x + H$ with $f_1 \in [2, |S_1| - 2]$.*

Proof. We argue as in Lemma 4.3. Suppose that $|S_0| \le 2$ and $|S_1| \ge 4$. We construct sets $A_1, \ldots, A_{t+r}$ and D as follows:

$$\begin{aligned} A_1 &= \{2a_1 + H, \ldots, (|S_1| - 2)a_1 + H\} \subset G/H\,, \\ A_i &= \{a_i + H, \ldots, (|S_i| - 1)a_i + H\} \subset G/H \quad \text{for } i \in [2, t]; \\ A_i &= \{H, a_i + H\} \subset G/H \quad \text{for } \ i \in [t+1, t+r]; \\ D &= \{b_0, b_0 - b_1, b_0 - b_2, \ldots, b_0 - b_u\} \subset G/H \end{aligned}$$

where $b_j = a_{t+r+j} + H$ for $j \in [1, u]$, and $b_0 = \sum_{j=1}^{u} b_j + H$. It suffices to show that $D + \sum_{i=1}^{t+r} A_i = G/H$. Applying the Cauchy-Davenport Theorem and Theorem 2.2, we have

$$\begin{aligned} |D + \sum_{i=1}^{t+r} A_i| &\ge \min\{p, |D| + |\sum_{i=1}^{t+r} A_i| - 1\} \\ &\ge \min\{p, |D| + \sum_{i=1}^{t+r} |A_i| - 2\} \\ &= \min\{p, u + \sum_{i=1}^{t} |S_i| - t + 2r - 3\}\,. \end{aligned}$$

Recall that $p+q-2 = |S_0| + \sum_{i=1}^t |S_i| + r + 2u$ implies $\sum_{i=1}^t |S_i| = p+q-2-|S_0|-r-2u$. Now we have

$$\begin{aligned} u + \sum_{i=1}^{t} |S_i| - t + 2r - 3 &= u + (p+q-2-|S_0|-r-2u) - t + 2r - 3 \\ &= p+q-5-|S_0|+r-u-t \\ &= p+q-5-|S_0|+r-(s-r) \\ &= p+q-5-|S_0|+2r-s. \end{aligned}$$

Since $s \le p-1$, we see that

$$\begin{aligned} p+q-5-|S_0|+2r-s &\ge p+q-5-|S_0|+2r-p+1 \\ &= q-4-|S_0|+2r \\ &\ge p+\lfloor 2\sqrt{p-2}\rfloor - 2 - |S_0| + 2r \end{aligned}$$

for the given values of primes p, q. This gives us

$$\begin{aligned} u + \sum_{i=1}^{t} |S_i| - t + 2r - 3 &\ge p+\lfloor 2\sqrt{p-2}\rfloor - 2 - |S_0| + 2r \\ &\ge p+\lfloor 2\sqrt{p-2}\rfloor - 4 + 2r \\ &\ge p+\lfloor 2\sqrt{p-2}\rfloor - 4 \\ &\ge p\,. \end{aligned}$$

□

Proposition 4.8. *If $|S_0| \le 2$ and $|S_1| \ge 4$, then $\Sigma(S) = G$.*

Proof. By Lemma 4.7 it remains to show that

$$|\,(\Sigma(S_0)\cup\{0\}) + \sum_{i=1}^{s} \Sigma_{f_i}(S)| \ge q\,.$$

As in the proof of Lemma 4.4, we set, for any subset $A \subset G$, $\bar{A} = \{a+K \mid a \in A\} \subset G/K$, and we use all observations made before. Theorem 2.1 implies that

$$|\,\big(\Sigma(\overline{S_0})\cup\{\overline{0}\}\big) + \sum_{i=1}^{s}\Sigma_{f_i}(\overline{S_i})| \ge \min\{q, |\Sigma(\overline{S_0})\cup\{\overline{0}\}| + |\Sigma_{f_1}(\overline{S_1})| + \sum_{i=2}^{s}|\Sigma_{f_i}(\overline{S_i})| - s\}\,.$$

By Lemma 4.7 we have $f_1 \in [2, |S_1|-2]$, and by Theorem 2.3 we get

$$|\Sigma_{f_1}(\bar{S_1})| \ge \min\{q,\ f_1|S_1| - f_1^2 + 1\}\,.$$

To find a lower bound on this inequality, we consider the minimum value of the quadratic expression $f_1|S_1| - f_1^2 + 1$ over the interval $[2, |S_1| - 2]$. Since the leading term is negative, the minimum value will occur when $f_1 = 2$ or $f_1 = |S_1| - 2$. Hence $f_1|S_1| - f_1^2 + 1 \geq 2|S_1| - 3 \geq |S_1| + 1$ because $|S_1| \geq 4$. Now we have

$$
\begin{aligned}
|\,(\Sigma(S_0) \cup \{0\}) + \sum_{i=1}^{s} \Sigma_{f_i}(S)| &\geq |\,\big(\Sigma(\overline{S_0}) \cup \{\overline{0}\}\big) + \sum_{i=1}^{s} \Sigma_{f_i}(\overline{S_i})| \\
&\geq \min\{q, |\Sigma(\overline{S_0}) \cup \{\overline{0}\}| + |\Sigma_{f_1}(\overline{S_1})| + \sum_{i=2}^{s} |\Sigma_{f_i}(\overline{S_i})| - s\} \\
&\geq \min\{q, |\Sigma(S_0) \cup \{0\}| + (|S_1| + 1) + \sum_{i=2}^{s} |S_i| - 1 - s\}\,,
\end{aligned}
$$

where we subtract one for a possible collapsed coefficient yielding $\Sigma_{f_i}(S_i) = \{0\}$ for some $i \in [2, s]$. Therefore we obtain that

$$
\begin{aligned}
|\,(\Sigma(S_0) \cup \{0\}) + \sum_{i=1}^{s} \Sigma_{f_i}(S)| &\geq \min\{q, (|S_0| + \max\{1, |S_0| - 1\} + (|S_1| + 1) + \sum_{i=2}^{s} |S_i| - 1 - s\} \\
&= \min\{q, p + q - 2 + \max\{1, |S_0| - 1\} - s\} \\
&\geq \min\{q, p + q - 2 + 1 - (p - 1)\} \\
&= q\,.
\end{aligned}
$$

□

Now the proof of Theorem 1.1 follows by a simple combination of the previous propositions.

Proof of Theorem 1.1. Let G be cyclic of order pq where p, q are primes with $p + \lfloor 2\sqrt{p-2} \rfloor + 1 < q < 2p$, and let $S \subset G \setminus \{0\}$ be a subset with $|S| = p + q - 2$. We use all notations as introduced at the beginning of Section 3.

If $|S_0| \geq \lfloor 2\sqrt{q-2} \rfloor$, then Proposition 4.1 implies that $\Sigma(S) = G$.

If $3 \leq |S_0| \leq \lfloor 2\sqrt{q-2} \rfloor - 1$, then Proposition 4.5 yields that $\Sigma(S) = G$.

Consider now the case $|S_0| \leq 2$. If additionally we have $|S_1| \leq 3$, then Proposition 4.6 yields that $\Sigma(S) = G$. On the other hand, if $|S_1| \geq 4$, then Proposition 4.8 yields that $\Sigma(S) = G$. □

Acknowledgement The authors thank Jenn Eyl for observations leading to Lemma 4.2, and thank the reviewer for suggestions leading to improved clarity in the paper. This work was supported by the Austrian Science Fund FWF, Project No. P18779-N13.

References

[1] J.A. Dias da Silva and Y. ould Hamidoune, *Cyclic spaces for Grassmann derivatives and additive theory*, Bull. Lond. 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] G.T. Diderrich and H.B. Mann, *Combinatorial problems in finite abelian groups*, A Survey of Combinatorial Theory, North-Holland, 1973, pp. 95 – 100.

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

[5] W. Gao and Y. ould Hamidoune, *On additive bases*, Acta Arith. **88** (1999), 233 – 237.

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

[7] A. Geroldinger and F. Halter-Koch, *Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory*, Pure and Applied Mathematics, vol. 278, Chapman & Hall/CRC, 2006.

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

[9] H.B. Mann and Ying Fou Wou, *An addition theorem for the elementary abelian group of type* (p, p), Monatsh. Math. **102** (1986), 273 – 308.

[10] M.B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Springer, 1996.

[11] A.S. Lladó Y. ould Hamidoune and O. Serra, *On complete subsets of the cyclic groups*, J. Comb. Theory, Ser. A **115** (2008), 1279 – 1285.