ADDITIVE BASES OF FINITE ABELIAN GROUPS OF RANK 2

Weidong Gao
Center for Applied Mathematics, Tianjin University, Tianjin, P.R. China
wdgao@nankai.edu.cn, weidong.gao@tju.edu.cn

Yuanlin Li
Department of Mathematics and Statistics, Brock University, St. Catharines, Canada
yli@brocku.ca

Yongke Qu
Department of Mathematics, Luoyang Normal University, LuoYang, P.R. China
yongke1239@163.com

Qinghong Wang
School of Science, Tianjin University of Technology, Tianjin, P.R. China
wqh1208@aliyun.com

Received: 12/10/21, Accepted: 3/5/22, Published: 3/14/22

Abstract

Let G be a finite abelian group and p be the smallest prime dividing $|G|$. Let S be a sequence over G. We say that S is regular if for every proper subgroup $H \subsetneq G$, S contains at most $|H|-1$ terms from H. Let $\mathsf{c}_0(G)$ be the smallest integer t such that every regular sequence S over G of length $|S| \geq t$ forms an additive basis of G, i.e., $\sum(S) = G$. The invariant $\mathsf{c}_0(G)$ was first studied by Olson and Peng in the 1980s, and since then it has been determined for all finite abelian groups except for the groups with rank 2 and a few groups of rank 3 or 4 with order less than 10^8. In this paper, we focus on the remaining case concerning groups of rank 2. It was conjectured by Gao et al. (Acta Arith. 168 (2015) 247-267) that $\mathsf{c}_0(G) = m(G)$. We confirm the conjecture for the case when $G = C_{n_1} \oplus C_{n_2}$ with $n_1 | n_2$, $n_1 \geq 2p$, $p \geq 3$ and $n_1 n_2 \geq 72p^6$.

1. Introduction and Main Results

Let G be a finite abelian group, written additively, p be the smallest prime dividing $|G|$ and $\mathsf{r}(G)$ denote the rank of G. Let S be a sequence over G. We say that S is an *additive basis* of G if every element of G can be expressed as the sum over a nonempty subsequence of S.

Let $\mathsf{cr}(G)$ denote the smallest integer t such that every subset of G of cardinality at least t is an additive basis of G. In 1964, Erdős and Heilbronn [1] proposed the problem of determining $\mathsf{cr}(G)$, and it was completely determined by 2009 through many authors' efforts (see [2, 3] and their references).

For every subgroup H of G, let S_H denote the subsequence of S consisting of all terms of S contained in H. We say that S is a *regular sequence* over G if $|S_H| \leq |H| - 1$ holds for every proper subgroup $H \subsetneq G$. With this definition, we can generalize the above problem by considering regular sequences instead of subsets forming an additive basis. Actually, a similar generalization for sumsets can be found in [10, 11]. It is reasonable to study regular sequences, as it can be easily proved that if S is not a regular sequence, then there exists a proper regular subsequence T of S such that $\sum_0(S) = \sum_0(T)$ (see [8, Lemma 2.2]). Let $\mathsf{c}_0(G)$ denote the smallest integer t such that every regular sequence over G of length at least t is an additive basis of G. The problem of determining $\mathsf{c}_0(G)$ was first proposed by Olson and it was conjectured that $\mathsf{c}_0(C_p \oplus C_p) = 2p-1$. In 1987, Peng proved this conjecture and further determined $\mathsf{c}_0(G)$ for all finite elementary abelian p-groups ([13, 14]). Those results and techniques used for determining $\mathsf{c}_0(G)$ have been successfully applied to the study of nonunique factorization ([7]). Recently, the problem related to the additive basis of a finite abelian group has been investigated by several authors ([4, 8, 15, 16, 17]). Let

$$m(G) = \begin{cases} |G|, \text{ if } G \text{ is cyclic}, \\ 2p-1, \text{ if } G = C_p \oplus C_p, \\ kp + 2p - 3, \text{ if } G = C_p \oplus C_{pk} \text{ and } k \geq 2, \\ \frac{|G|}{p} + p - 2, \text{ otherwise}. \end{cases}$$

It has been proved that $\mathsf{c}_0(G) = m(G)$ for any of the following finite abelian groups:

(1) G is cyclic ([4, Theorem 1.1(1)]);

(2) $|G|$ is even ([4, Theorem 1.1(2)]);

(3) $\mathsf{r}(G) \geq 4$ and $G \neq C_3^3 \oplus C_{3n}$ where $n > 3$ is odd and is not a power of 3 with $|G| < 3.72 \times 10^7$ ([15, Theorem 1.2(1)] and [8, Theorem 1.2]);

(4) $\mathsf{r}(G) = 3$ and either $p \geq 11$ or $3 \leq p \leq 7$ with $|G| \geq 3.72 \times 10^7$ ([15, Theorem 1.2(2)] and [8, Theorem 1.2]);

(5) $\mathsf{r}(G) \geq 2$ and G is a p-group ([4, Theorem 1.1(5)] and [16, Theorem 1]);

(6) $G = C_3 \oplus C_{3q}$, where q is a prime ([4, Theorem 1.1(2)], [16, Theorem 1] and [17, Theorem 1.1]).

Clearly, by their definitions, $\mathsf{c}_0(G) \geq \mathsf{cr}(G)$. Moreover, $\mathsf{c}_0(G) = \mathsf{cr}(G)$ for all finite abelian groups with $\mathsf{r}(G) \geq 3$ whose $\mathsf{c}_0(G)$ has been determined. However, $\mathsf{c}_0(G)$

and $\mathsf{cr}(G)$ differ significantly when $\mathsf{r}(G) = 1$. For $\mathsf{r}(G) = 2$, the exact value of $\mathsf{c}_0(G)$ seems mysterious and has only been determined for all finite abelian p-groups and abelian groups of even order.

In this paper, we focus our investigation on the remaining case when G is of rank 2. It was conjectured in [4] that $\mathsf{c}_0(G) = m(G)$. We confirm this conjecture for the case when $G = C_{n_1} \oplus C_{n_2}$ with $n_1|n_2$, $n_1 \geq 2p$, $p \geq 3$ and $n_1 n_2 \geq 72p^6$.

Theorem 1. *Let $G = C_{n_1} \oplus C_{n_2}$ with $n_1|n_2$, and $p \geq 3$ be the smallest prime divisor of $|G|$. If $n_1 \geq 2p$ and $|G| \geq 72p^6$, then $\mathsf{c}_0(G) = |G|/p + p - 2$.*

2. Notation and Preliminaries

Suppose that $G_0 \subseteq G$ is a subset of G and $\mathcal{F}(G_0)$ is the multiplicatively written, free abelian monoid with basis G_0. The elements of $\mathcal{F}(G_0)$ are called *sequences* over G_0. We denote multiplication in $\mathcal{F}(G_0)$ by the bold symbol $\boldsymbol{\cdot}$ rather than by juxtaposition, and use brackets for all exponentiation in $\mathcal{F}(G_0)$.

A sequence $S \in \mathcal{F}(G)$ will be written in the form $S = g_1 \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g_\ell$, where $|S| = \ell$ is the *length* of S. For $g \in G$, let $\mathsf{v}_g(S) = |\{i \in [1, \ell]\colon\, g_i = g\}|$ denote the *multiplicity* of g in S. We call $\operatorname{supp}(S) = \{g \in G\colon \mathsf{v}_g(S) > 0\}$ the *support* of S. Let $\mathsf{h}(S) = \max\{\mathsf{v}_g(S)\colon g \in G\}$. A sequence $T \in \mathcal{F}(G)$ is called a *subsequence* of S and is denoted by $T \mid S$ if $\mathsf{v}_g(T) \leq \mathsf{v}_g(S)$ for all $g \in G$. Denote by $S \boldsymbol{\cdot} T^{[-1]}$ the subsequence of S obtained by removing the terms of T from S.

If $S_1, S_2 \in \mathcal{F}(G)$, then $S_1 \boldsymbol{\cdot} S_2 \in \mathcal{F}(G)$ denotes the sequence satisfying that $\mathsf{v}_g(S_1 \boldsymbol{\cdot} S_2) = \mathsf{v}_g(S_1) + \mathsf{v}_g(S_2)$ for all $g \in G$. For convenience we write

$$g^{[k]} = \underbrace{g \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} g}_{k} \in \mathcal{F}(G)$$

for $g \in G$ and k a nonnegative integer.

Let $\sigma(S) = \sum_{g \in G} \mathsf{v}_g(S) g \in G$ be the sum of S. Define

$$\sum(S) = \{\sigma(T)\colon\ 1 \neq T \mid S\},$$

where 1 is the empty sequence, and

$$\sum\nolimits_0(S) = \sum(S) \cup \{0\} = \{\sigma(T)\colon T \mid S\}.$$

We call a sequence S a *zero-sum* sequence if $\sigma(S) = 0$, and a *zero-sum free* sequence if $0 \notin \sum(S)$. We note that a subset of G can be regarded as a sequence, so all above-mentioned concepts and notations regarding a sequence of G are valid for a subset of G. We say that a subset $A \subset G \setminus \{0\}$ is 2-*zero-sum free* if A contains no two distinct elements with sum zero.

Let $\mathsf{D}(G)$ denote the Davenport constant of G, which is defined as the smallest integer t such that every sequence S over G of length $|S| \geq t$ contains a nonempty zero-sum subsequence. Note that $\mathsf{D}(C_{n_1} \oplus C_{n_2}) = n_1 + n_2 - 1$, where $1 \leq n_1 | n_2$ ([9, Theorem 5.8.3]).

For each subset A of G, denote by $\langle A \rangle$ the subgroup generated by A. Let $\mathrm{st}(A) = \{g \in G \colon g + A = A\}$. Then $\mathrm{st}(A)$ is the maximal subgroup H of G such that $H + A = A$. The following is the well known Kneser's theorem and a proof of it can be found in [12].

Lemma 1 (Kneser, [12, Theorem 4.4]). *Let $A_1, \ldots, A_r$ be nonempty finite subsets of an abelian group G, and let $H = \mathrm{st}(A_1 + \cdots + A_r)$. Then,*

$$|A_1 + \cdots + A_r| \geq |A_1 + H| + \cdots + |A_r + H| - (r-1)|H|.$$

Lemma 2 ([4, Lemma 2.2]). *The inequality $\mathsf{c}_0(G) \geq m(G)$ holds for every finite abelian group G.*

Lemma 3 ([4, Lemma 2.3]). *Let G be a finite abelian group and p be the smallest prime divisor of $|G|$. Let S be a regular sequence over G of length $|S| \geq max\{|G|/p + p - 2, \mathsf{D}(G)\}$. Let T be a nonempty subsequence of S. If $\sum(S) \neq G$, then*

(1) $\mathrm{st}(\sum_0(T)) = \{0\}$*;*

(2) $|\sum_0(T))| \geq |T| + 1$.

We remark that since $|S| \geq \mathsf{D}(G)$, we have $0 \in \sum(S)$. Thus $\sum(S) = \sum_0(S)$, and the above lemma follows immediately from [4, Lemma 2.3].

For a finite abelian group G and a positive integer k, let $f(G,k) = \min\{|\sum(S)|\colon S$ is a subset of G with $|S| = k$ and $0 \notin \sum(S)\}$. If $0 \in \sum(S)$ for every $S \subseteq G$ of $|S| = k$, we set $f(G,k) = \infty$. Let $f(k) = \min\{f(G,k)\colon G$ is a finite abelian group$\}$.

Lemma 4 ([5, Theorem 1.1]). *The inequality $f(k) \geq \frac{k^2}{6}$ holds for every positive integer k.*

3. Proof of Theorem 1

We first prove a few technical results.

Lemma 5. *Let G be a finite abelian group and $A \subseteq G \setminus \{0\}$. If $|A| \geq 6p(p+1)+1$, then there is a zero-sum free subset $B \subseteq A$ such that $|\sum_0(B)| \geq p|B| + 2$ with $|B| \leq 6p + 1$, where p is a nonnegative integer.*

Proof. It is sufficient to prove that there is a zero-sum free subset $B \subseteq A$ such that $|\sum(B)| \geq p|B|+1$ with $|B| \leq 6p+1$. We first prove that for every $k \leq 6p+1$ there is a zero-sum free subset $B \subseteq A$ such that either $|B| = k$ or $|B| < k$ and $|\sum(B)| \geq p|B|+1$.

We proceed by induction on k. If $k=1$, then the result holds trivially. Assume that the result is true for each k ($k < 6p+1$). We next prove it is also true for $k+1$. By the induction hypothesis, there is a zero-sum free subset $B_0 \subseteq A$ such that either $|B_0| = k$ or $|B_0| < k$ and $|\sum(B_0)| \geq p|B_0|+1$. If $|\sum(B_0)| \geq p|B_0|+1$, then let $B = B_0$. Hence $|B| < k+1$ and $|\sum(B)| \geq p|B|+1$, so we are done. Thus we may assume that $|B_0| = k$ and $|\sum(B_0)| \leq p|B_0|$. It follows that $|-\sum(B_0)| = |\sum(B_0)| \leq pk \leq 6p^2 \leq |A| - (6p+1) < |A| - |B_0| = |A \setminus B_0|$. Hence, there is an element $g \in A \setminus B_0$ such that $g \notin -\sum(B_0)$. So, $B_0 \cup \{g\}$ is a zero-sum free subset of A. Set $B = B_0 \cup \{g\}$, and then the result holds for $k+1$.

Next, let $k = 6p+1$. We have just proved that there is a zero-sum free subset B of A such that either $|B| = 6p+1$ or $|\sum(B)| \geq p|B|+1$ and $|B| < 6p+1$. If the latter is true, then we are done. So, we may assume that $|B| = 6p+1$. By Lemma 4, $|\sum(B)| \geq f(6p+1) \geq (6p+1)^2/6 \geq p(6p+1)+1$ and again we are done. □

Lemma 6. *Let G be a finite abelian group and p be the smallest prime divisor of $|G|$. Let T be a sequence over $G \setminus \{0\}$ and $H = \langle supp(T) \rangle$. Then $|\sum_0(T)| \geq |T|+1$ if one of the following holds*

(1) $|T| \leq p-1$*;*

(2) $|T| \leq 2p-1$ *and* $|H| \geq 2p$*.*

Proof. Let $T = g_1 \cdot \ldots \cdot g_k$. Then,

$$\sum\nolimits_0(T) = \{g_1, 0\} + \cdots + \{g_k, 0\}.$$

Let $M = \mathrm{st}(\{g_1, 0\} + \cdots + \{g_k, 0\})$. If $M = \{0\}$, then by Lemma 1, $|\sum_0(T)| = |\{g_1, 0\} + \cdots + \{g_k, 0\}| \geq k+1 = |T|+1$ as desired.

Next we assume $M \neq \{0\}$, so $|M| \geq p$.

(1) Since $k = |T| \leq p-1$, we have $|\sum_0(T)| = |\{g_1, 0\} + \cdots + \{g_k, 0\}| = |\{g_1, 0\} + \cdots + \{g_k, 0\} + M| \geq |M| \geq p \geq k+1 = |T|+1$.

(2) If $M \supseteq H$, then as above $|\sum_0(T)| \geq |M| \geq |H|$. Since $|H| \geq 2p$ and $|T| \leq 2p-1$, we have $|\sum_0(T)| \geq 2p \geq |T|+1$. Next we assume that $\{0\} \neq M \not\supseteq H$. Clearly, $\sum_0(T) = \{g_1, 0\} + \cdots + \{g_k, 0\} \subsetneq M$. Thus $g_i \notin M$ for some $1 \leq i \leq k$, and so $|\{g_i, 0\} + M| = 2|M|$. By Lemma 1, $|\sum_0(T)| = |\{g_1, 0\} + \cdots + \{g_k, 0\}| \geq 2|M| \geq 2p \geq |T|+1$ as desired. □

As a consequence, we obtain the following corollary, which will be used in the proof of Lemma 7.

Corollary 1. *Let G be a finite abelian group and p be the smallest prime divisor of $|G|$. Let S and T be sequences over G. Suppose $g \notin \langle supp(S)\rangle$ for every $g \mid T$. Then $|\sum_0(T \cdot S)| \geq (|T|+1)|\sum_0(S)|$ if one of the following holds*

(1) $|T| \leq p-1$;

(2) $|T| \leq 2p-1$ *and* $|\langle supp(T \cdot S)\rangle/\langle supp(S)\rangle| \geq 2p$.

Proof. Let $\varphi : \langle \mathrm{supp}(T \cdot S)\rangle \to \langle \mathrm{supp}(T \cdot S)\rangle/\langle \mathrm{supp}(S)\rangle$ be the canonical epimorphism. Let $T = g_1 \cdot \ldots \cdot g_k$ and $\varphi(T) = \varphi(g_1) \cdot \ldots \cdot \varphi(g_k)$. Since $g_i \notin \langle \mathrm{supp}(S)\rangle$ for every $i \in [1,k]$, we have $\varphi(g_i) \neq 0$ for $i \in [1,k]$. Thus $\varphi(T)$ is a sequence over $\varphi(G)\setminus\{\varphi(0)\}$. By Lemma 6, we have $|\sum_0(\varphi(T))| \geq |\varphi(T)|+1 = |T|+1$. Therefore, $|\sum_0(T \cdot S)| \geq |\sum_0(\varphi(T))| \cdot |\sum_0(S)| \geq (|T|+1)|\sum_0(S)|$. □

Lemma 7. *Let G be a finite abelian group and p be the smallest prime divisor of $|G|$. Let $R = R_1 \cdot R_2$ be a sequence over G. If R satisfies the following three conditions:*

(1) $|R_1| \geq 2p-1$;

(2) $g \notin \langle supp(R_2)\rangle$ *for all* $g \mid R_1$;

(3) $|\langle supp(R)\rangle/\langle supp(R_2)\rangle| \geq 2p$;

then there exists a subsequence $R_1' \mid R_1$ such that $|R_1'| = 2p-1$ and $|\sum_0(R_1' \cdot R_2')| \geq 2p(|R_2'|+1)$ for every subsequence $R_2' \mid R_2$.

Proof. If $\langle \mathrm{supp}(R)\rangle/\langle \mathrm{supp}(R_2)\rangle$ is a group of prime order, then by (1) let R_1' be an arbitrary subsequence of R_1 with length $|R_1'| = 2p-1$. By (2), $\langle \mathrm{supp}(R_1' \cdot R_2)\rangle/\langle \mathrm{supp}(R_2)\rangle$ is not trivial, and thus we must have $\langle \mathrm{supp}(R_1' \cdot R_2)\rangle/\langle \mathrm{supp}(R_2)\rangle = \langle \mathrm{supp}(R)\rangle/\langle \mathrm{supp}(R_2)\rangle$. Therefore, by (3),

$$|\langle \mathrm{supp}(R_1' \cdot R_2)\rangle/\langle \mathrm{supp}(R_2)\rangle| = |\langle \mathrm{supp}(R)\rangle/\langle \mathrm{supp}(R_2)\rangle| \geq 2p.$$

Next we assume that $|\langle \mathrm{supp}(R)\rangle/\langle \mathrm{supp}(R_2)\rangle|$ is a composite number. Since $\langle \mathrm{supp}(R_1 \cdot R_2)\rangle/\langle \mathrm{supp}(R_2)\rangle = \langle \mathrm{supp}(R)\rangle/\langle \mathrm{supp}(R_2)\rangle$, by (1) and (2), there exists a subsequence $R_1' \mid R_1$ with $|R_1'| = 2p-1$ such that $|\langle \mathrm{supp}(R_1' \cdot R_2)\rangle/\langle \mathrm{supp}(R_2)\rangle|$ is a composite number. Since p is the smallest prime divisor of $|G|$, we have $|\langle \mathrm{supp}(R_1' \cdot R_2)\rangle/\langle \mathrm{supp}(R_2)\rangle| \geq p^2 \geq 2p$. So we can always choose a subsequence $R_1' \mid R_1$ such that

$$|R_1'| = 2p-1 \quad \text{and} \quad |\langle \mathrm{supp}(R_1' \cdot R_2)\rangle/\langle \mathrm{supp}(R_2)\rangle| \geq 2p.$$

Since $R_2' \mid R_2$ is a subsequence of R_2, we have $\langle \mathrm{supp}(R_2')\rangle \le \langle \mathrm{supp}(R_2)\rangle$ and thus

$$\begin{aligned}|\langle \mathrm{supp}(R_1' \cdot R_2')\rangle / \langle \mathrm{supp}(R_2')| &= |\langle \mathrm{supp}(R_1'), \mathrm{supp}(R_2')\rangle / \langle \mathrm{supp}(R_2')\rangle| \\ &\ge |\langle \mathrm{supp}(R_1'), \mathrm{supp}(R_2)\rangle / \langle \mathrm{supp}(R_2)\rangle| \\ &= |\langle \mathrm{supp}(R_1' \cdot R_2)\rangle / \langle \mathrm{supp}(R_2)\rangle| \\ &\ge 2p.\end{aligned}$$

Note that by (2), $g \notin \langle \mathrm{supp}(R_2')\rangle$ for every $g \mid R_1'$. By Corollary 1(2) and Lemma 3(2), we have $|\sum_0(R_1' \cdot R_2')| \ge (|R_1'|+1)|\sum_0(R_2')| \ge 2p(|R_2'|+1)$. □

Lemma 8 ([4, Lemma 3.1]). *If A is a 2-zero-sum free subset of three elements in an arbitrary abelian group, then either $|\sum_0(A)| \ge 7$ or A contains some element of order two.*

We now prove our main result.

Proof of Theorem 1. Let $n = |G|$. By Lemma 2, it suffices to prove $\mathsf{c}_0(G) \le n/p + p-2$. Let S be a regular sequence over G of length $|S| = n/p+p-2$. We only need to show that $\sum(S) = G$. Since $2p \le n_1|n_2$, we have $n/p+p-2 \ge n_1+n_2-1 = \mathsf{D}(G)$. Hence $0 \in \sum(S)$ and thus $\sum(S) = \sum_0(S)$.

Assume to the contrary that $\sum_0(S) \ne G$, that is, $|\sum_0(S)| < n$. Thus, by Lemma 3(1), we have $\mathrm{st}(\sum_0(S)) = \{0\}$.

Suppose that $\mathsf{h}(S) \le 2p-2$. If $|\mathrm{supp}(S)| \le 6p(p+1)$, then $|S| \le |\mathrm{supp}(S)| \cdot \mathsf{h}(S) \le 12p(p^2-1)$. Since $|S| = \frac{n}{p} + p - 2 \ge \frac{72p^6}{p} + p - 2 \ge 72p^5 > 12p(p^2-1)$, we get a contradiction. Hence $|\mathrm{supp}(S)| \ge 6p(p+1)+1$. By Lemma 5, we may choose $A_1 \subseteq \mathrm{supp}(S) \subseteq G$, such that $|A_1| \le 6p+1$ and $|\sum_0(A_1)| \ge p|A_1|+2$. Let $t \ge 1$ be the maximal integer such that S has a factorization

$$S = A_1 \cdot \ldots \cdot A_t \cdot T$$

with $A_i \subseteq G$, $|A_i| \le 6p+1$ and $|\sum_0(A_i)| \ge p|A_i|+2$ for every $i \in [1,t]$.

Note that if $S' \mid S$ is a subsequence of S, then S' has a factorization of $S' = A_1' \cdot \ldots \cdot A_t' \cdot T'$, where $A_i' \mid A_i$ for $i \in [1,t]$ and $T' \mid T$. On the other hand, if $A_i' \mid A_i$ for $i \in [1,t]$ and $T' \mid T$, then $S' = A_1' \cdot \ldots \cdot A_t' \cdot T'$ is a subsequence of S. So, $\sum_0(S) = \{\sigma(S') \colon S' \mid S\} = \{\sigma(A_1') + \cdots + \sigma(A_t') + \sigma(T') \colon A_i' \mid A_i \text{ for } i \in [1,t] \text{ and } T' \mid T\} = \{\sigma(A_1') \colon A_1' \mid A_1\} + \cdots + \{\sigma(A_t') \colon A_t' \mid A_t\} + \{\sigma(T') \colon T' \mid T\} = \sum_0(A_1) + \cdots + \sum_0(A_t) + \sum_0(T)$. Since $\sum(S) = \sum_0(S)$, we have

$$\sum(S) = \sum\nolimits_0(S) = \sum\nolimits_0(A_1) + \cdots + \sum\nolimits_0(A_t) + \sum\nolimits_0(T).$$

By the maximality of t and Lemma 5, we have $|\mathrm{supp}(T)| \le 6p(p+1)$. Thus $|T| \le |\mathrm{supp}(T)| \cdot \mathsf{h}(S) \le 12p(p^2-1)$. Since $|A_i| \le 6p+1$ for each $i \in [1,t]$, we have $t \geq \frac{|S|-|T|}{6p+1}$. By Lemma 3(2), $|\sum_0(T)| \geq |T|+1$. Since $\mathrm{st}(\sum(S)) = \{0\}$, by Lemma 1, we have

$$\begin{aligned}
|\sum\nolimits_0(S)| &= |\sum\nolimits_0(A_1) + \cdots + \sum\nolimits_0(A_t) + \sum\nolimits_0(T)| \\
&\geq (|\sum\nolimits_0(A_1)| - 1) + \cdots + (|\sum\nolimits_0(A_t)| - 1) + |\sum\nolimits_0(T)| \\
&\geq \sum_{i=1}^{t}(p|A_i| + 1) + |T| + 1 \\
&= p(|S| - |T|) + t + |T| + 1 \\
&\geq (p + \frac{1}{6p+1})(|S| - |T|) + |T| + 1 \qquad (3.1)\\
&\geq n + \frac{n}{p(6p+1)} + p^2 - 2p - (p - \frac{6p}{6p+1})|T| + 1 \text{ (as } |S| = \frac{n}{p} + p - 2) \\
&\geq n + \frac{n}{p(6p+1)} + p^2 - 2p - \frac{12p^2(6p-5)(p^2-1)}{6p+1} + 1 \\
&\quad \text{(as } |T| \leq 12p(p^2-1)) \\
&\geq n + \frac{n}{p(6p+1)} - \frac{12p^2 \cdot 6p \cdot p^2}{6p+1} \\
&\geq n \qquad \text{(as } n \geq 72p^6),
\end{aligned}$$

yielding a contradiction. Therefore, we must have $\mathsf{h}(S) \geq 2p-1$. We choose $g_1 \in \mathrm{supp}(S)$ such that

$$|S_{\langle g_1 \rangle}| = \max\{|S_{\langle g \rangle}| \colon g \in \mathrm{supp}(S) \text{ and } \mathsf{v}_g(S) \geq 2p-1\}.$$

Let $S_1 = S_{\langle g_1 \rangle}$ and λ be the maximal integer such that S has a factorization

$$S = (T_1 \cdot S_1) \cdot (T_2 \cdot S_2) \cdot \ldots \cdot (T_\lambda \cdot S_\lambda) \cdot S'$$

with the following properties:

(1) $|T_i| = 2p-1$ for each $i \in [1, \lambda]$;

(2) for each $i \in [1, \lambda]$, $\mathsf{v}_{g_i}(S_i) \geq 2p-1$ for some $g_i \in G$; moreover, S_i contains all terms from $S \cdot ((T_1 \cdot S_1) \cdot (T_2 \cdot S_2) \cdot \ldots \cdot (T_{i-1} \cdot S_{i-1}))^{[-1]}$ contained in $\langle g_i \rangle$;

(3) $|\sum_0(T_i \cdot S_i')| \geq 2p(|S_i'| + 1)$ for all subsequences $S_i' \mid S_i$, where $i \in [1, \lambda]$.

Now we prove

$$\lambda \geq 1.$$

We first show that $\langle \mathrm{supp}(S) \rangle = G$. For otherwise, if $H = \langle \mathrm{supp}(S) \rangle < G$, then $|H| \leq \frac{n}{p}$ where p is the smallest prime divisor of $|G|$. Since S is regular, we have $|H|-1 \geq |S_H| = |S| = \frac{n}{p}+p-2 \geq |H|$, yielding a contradiction. Thus $\langle \text{supp}(S)\rangle = G$. It follows that $\langle \text{supp}((S\cdot S_1^{[-1]})\cdot S_1)\rangle/\langle \text{supp}(S_1)\rangle = G/\langle \text{supp}(S_1)\rangle$. Since $\langle \text{supp}(S_1)\rangle$ is a cyclic group, we have $|\langle \text{supp}(S_1)\rangle| \leq n_2$ and thus

$$|\langle \text{supp}((S\cdot S_1^{[-1]})\cdot S_1)\rangle/\langle \text{supp}(S_1)\rangle| = |G/\langle \text{supp}(S_1)\rangle| \geq n_1 \geq 2p.$$

Note that

$$|S\cdot S_1^{[-1]}| \geq \frac{n}{p}+p-2-\frac{n}{p^2} \geq 2p-1.$$

By the assumption of S_1, we have $g \notin \langle \text{supp}(S_1)\rangle$ for all $g \mid S\cdot S_1^{[-1]}$. By Lemma 7, there exists a subsequence $T_1 \mid S\cdot S_1^{[-1]}$ such that $|T_1| = 2p-1$ and $|\sum_0(T_1\cdot S_1')| \geq 2p(|S_1'|+1)$ for all subsequences $S_1' \mid S_1$. So, T_1 together with S_1 satisfies all three properties. Thus, $\lambda \geq 1$.

Next we distinguish the remaining proof into the following two cases according to the value of $\mathsf{h}(S')$.

Case 1. $\mathsf{h}(S') \leq 2p-2$.

Let $t \geq 0$ be the maximal integer such that S' has a factorization

$$S' = A_1\cdot \ldots \cdot A_t \cdot T$$

with $A_i \subseteq G$, $|A_i| \leq 6p+1$ and $|\sum_0(A_i)| \geq p|A_i|+2$. By the maximality of t and Lemma 5, we have $|\text{supp}(T)| \leq 6p(p+1)$. Thus $|T| \leq |\text{supp}(T)|\cdot \mathsf{h}(S') \leq 12p(p^2-1)$. Since $|T_i\cdot S_i| \geq 4p-2$ for each $i \in [1,\lambda]$, we have $\lambda \leq \frac{|S|-|S'|}{4p-2}$. Similarly, $t \geq \frac{|S'|-|T|}{6p+1}$. By Lemma 3(2), $|\sum_0(T)| \geq |T|+1$. Since $\text{st}(\sum_0(S)) = \{0\}$, by Lemma 1, we have

$$\begin{aligned}
|\textstyle\sum_0(S)| &= |\sum_{i=1}^{\lambda}\textstyle\sum_0(T_i\cdot S_i) + \sum_{j=1}^{t}\sum_0(A_j) + \sum_0(T)| \\
&\geq \sum_{i=1}^{\lambda}(|\textstyle\sum_0(T_i\cdot S_i)|-1) + \sum_{j=1}^{t}(|\sum_0(A_j)|-1) + |\sum_0(T)| \\
&\geq \sum_{i=1}^{\lambda}(2p|S_i|+2p-1) + \sum_{j=1}^{t}(p|A_j|+1) + |T|+1 \\
&= \sum_{i=1}^{\lambda}(2p|T_i\cdot S_i|-(2p-1)^2) + p(|S'|-|T|) + t + |T| + 1 \\
&\geq 2p(|S|-|S'|) - (2p-1)^2\lambda + (p+\frac{1}{6p+1})(|S'|-|T|) + |T| + 1 \\
&\geq (p+1/2)(|S|-|S'|) + (p+\frac{1}{6p+1})(|S'|-|T|) + |T| + 1 \\
&\geq (p+\frac{1}{6p+1})(|S|-|T|) + |T| + 1 \\
&\geq n \qquad (\text{as } |T| \leq 12p(p^2-1)),
\end{aligned}$$

yielding a contradiction. We note that the last inequality was obtained by using a similar calculation as in (3.1).

Case 2. $\mathsf{h}(S') \ge 2p-1$.

There exists $g_{\lambda+1} \in G$ such that $\mathsf{v}_{g_{\lambda+1}}(S') = \mathsf{h}(S') \ge 2p-1$. Let $S_{\lambda+1} = S'_{\langle g_{\lambda+1}\rangle}$ and $U = S' \boldsymbol{\cdot} S_{\lambda+1}^{[-1]}$. Then

$$S = (T_1 \boldsymbol{\cdot} S_1) \boldsymbol{\cdot} (T_2 \boldsymbol{\cdot} S_2) \boldsymbol{\cdot} \ldots \boldsymbol{\cdot} (T_\lambda \boldsymbol{\cdot} S_\lambda) \boldsymbol{\cdot} S_{\lambda+1} \boldsymbol{\cdot} U.$$

We next distinguish the rest of the proof into the following two subcases.

Subcase 2.1. $|U| \le 2p-2$.

By the choice of S_1, we have $|S_{\lambda+1}| \le |S_1|$. Since $|T_i \boldsymbol{\cdot} S_i| \ge 4p-2$ for each $i \in [2,\lambda]$, we have $\lambda - 1 \le \frac{|S|-|S_1 \boldsymbol{\cdot} T_1|-|S_{\lambda+1}|-|U|}{4p-2}$. By Lemma 3(2), $|\sum_0(S_{\lambda+1} \boldsymbol{\cdot} U)| \ge |S_{\lambda+1} \boldsymbol{\cdot} U| + 1$. Since $\mathrm{st}(\sum_0(S)) = \{0\}$, by Lemma 1, we have

$$\begin{aligned}
|\textstyle\sum_0(S)| &= |\textstyle\sum_0(T_1 \boldsymbol{\cdot} S_1) + \displaystyle\sum_{i=2}^{\lambda} \textstyle\sum_0(T_i \boldsymbol{\cdot} S_i) + \sum_0(S_{\lambda+1} \boldsymbol{\cdot} U)| \\
&\ge (|\textstyle\sum_0(T_1 \boldsymbol{\cdot} S_1)| - 1) + \displaystyle\sum_{i=2}^{\lambda} (|\textstyle\sum_0(T_i \boldsymbol{\cdot} S_i)| - 1) + |\sum_0(S_{\lambda+1} \boldsymbol{\cdot} U)| \\
&\ge (2p|S_1| + 2p - 1) + \sum_{i=2}^{\lambda}(2p|S_i| + 2p - 1) + |S_{\lambda+1} \boldsymbol{\cdot} U| + 1 \\
&\ge (p+1/2)|S_1| + \sum_{i=2}^{\lambda}(2p|T_i \boldsymbol{\cdot} S_i| - (2p-1)^2) + (p+1/2)|S_{\lambda+1}| + 2p \\
&= (p+1/2)(|S_1| + |S_{\lambda+1}|) + 2p(|S| - |T_1 \boldsymbol{\cdot} S_1| - |S_{\lambda+1}| - |U|) \\
&\quad - (2p-1)^2(\lambda-1) + 2p \\
&\ge (p+1/2)(|S_1| + |S_{\lambda+1}|) + (p+1/2)(|S| - |T_1 \boldsymbol{\cdot} S_1| - |S_{\lambda+1}| - |U|) \\
&\quad + 2p \\
&= (p+1/2)(|S| - |T_1| - |U|) + 2p \\
&\ge (p+1/2)(n/p + p - 2 - (4p-3)) + 2p \\
&\ge n \qquad (\text{as } n \ge 6p^3 - 3p^2 - p),
\end{aligned}$$

yielding a contradiction.

Subcase 2.2. $|U| \ge 2p-1$.

Let $H = \langle \mathrm{supp}(U \boldsymbol{\cdot} S_{\lambda+1})\rangle$. By the choice of $S_{\lambda+1}$, we have $\langle \mathrm{supp}(S_{\lambda+1})\rangle = \langle g_{\lambda+1}\rangle$, and $g \notin \langle g_{\lambda+1}\rangle$ for all $g \mid U$. If $|H/\langle g_{\lambda+1}\rangle| \ge 2p$, then by Lemma 7, we can find a subsequence $T_{\lambda+1} \mid U$ such that $|T_{\lambda+1}| = 2p-1$ and $|\sum_0(T_{\lambda+1} \boldsymbol{\cdot} S'_{\lambda+1})| \ge 2p(|S'_{\lambda+1}| + 1)$ for all subsequence $S'_{\lambda+1} \mid S_{\lambda+1}$. Therefore, $S_{\lambda+1}$ and $T_{\lambda+1}$ satisfy

Properties $(1)-(3)$, yielding a contradiction to the maximality of λ. Therefore, we must have $|H/\langle g_{\lambda+1}\rangle| \leq 2p-1$. Since $\langle g_{\lambda+1}\rangle$ is a cyclic subgroup of G, we have $|G/\langle g_{\lambda+1}\rangle| \geq n_1 \geq 2p$. Thus $H \neq G$. Therefore,

$$|H| \leq n/p \quad \text{and} \quad |S'| \leq |S_H| \leq n/p-1 \text{ (as } S'|S_H \text{ and } S \text{ is regular).}$$

Suppose that $\mathrm{supp}(S_i) \nsubseteq H$ for some $i \in [1,\lambda]$. Then let $S_i' = S_i \cdot g_i^{[-(p-1)]}$. We have

$$S = \left(\prod_{1\leq j\neq i\leq \lambda}(T_j \cdot S_j)\right) \cdot (T_i \cdot S_i') \cdot (g_i^{[p-1]} \cdot S').$$

Let $U' \mid U$ with $|U'| = p-1$. By Corollary 1(1) and Lemma 3(2), $|\sum_0(U' \cdot g_{\lambda+1}^{[2p-1]})| \geq (|U'|+1)|\sum_0(g_{\lambda+1}^{[2p-1]})| = 2p^2$. By Lemma 3(1), $\mathrm{st}(\sum_0(S')) = \{0\}$. Note that

$$\sum\nolimits_0(S') = \sum\nolimits_0(S' \cdot (U' \cdot g_{\lambda+1}^{[2p-1]})^{[-1]}) + \sum\nolimits_0(U' \cdot g_{\lambda+1}^{[2p-1]}).$$

By Lemma 1 and Lemma 3(2), $|\sum_0(S')| \geq |\sum_0(S' \cdot (U' \cdot g_{\lambda+1}^{[2p-1]})^{[-1]})| + |\sum_0(U' \cdot g_{\lambda+1}^{[2p-1]})| - 1 \geq |S' \cdot (U' \cdot g_{\lambda+1}^{[2p-1]})^{[-1]}| + 2p^2 = |S'| + 2p^2 - 3p + 2$. Therefore, by Corollary 1(1),

$$|\sum\nolimits_0(g_i^{[p-1]} \cdot S')| \geq (|g_i^{[p-1]}|+1)|\sum\nolimits_0(S')| \geq p|\sum\nolimits_0(S')| \geq p|S'| + 2p^3 - 3p^2 + 2p.$$

As in Subcase 2.1, we have $\lambda - 1 \leq \frac{|S|-|T_i\cdot S_i|-|S'|}{4p-2}$. Since $\mathrm{st}(\sum_0(S)) = \{0\}$, by Lemma 1,

$$\begin{aligned}
|\sum\nolimits_0(S)| &= |\sum_{1\leq j\neq i\leq\lambda}\sum\nolimits_0(T_j \cdot S_j) + \sum\nolimits_0(T_i \cdot S_i') + \sum\nolimits_0(g_i^{[p-1]} \cdot S')| \\
&\geq \sum_{1\leq j\neq i\leq\lambda}(|\sum\nolimits_0(T_j \cdot S_j)| - 1) + (|\sum\nolimits_0(T_i \cdot S_i')| - 1) \\
&\quad + |\sum\nolimits_0(g_i^{[p-1]} \cdot S')| \\
&\geq \sum_{1\leq j\neq i\leq\lambda}(2p|T_j \cdot S_j| - (2p-1)^2) + (2p|S_i'| + 2p - 1) + p|S'| + 2p^3 \\
&\quad - 3p^2 + 2p \\
&= 2p(|S| - |S_i \cdot T_i| - |S'|) - (2p-1)^2(\lambda-1) + 2p(|S_i| - p + 1) + p|S'| \\
&\quad + 2p^3 - 3p^2 + 4p - 1 \\
&\geq (p+1/2)(|S| - |S_i \cdot T_i| - |S'|) + 2p|S_i| + p|S'| + 2p^3 - 5p^2 + 6p - 1 \\
&= (p+1/2)|S| + (p-1/2)|S_i| - (p+1/2)|T_i| - |S'|/2 + 2p^3 - 5p^2 + 6p \\
&\quad - 1 \\
&\geq (p+1/2)(n/p + p - 2) - (2p-1) - (n/p-1)/2 + 2p^3 - 5p^2 + 6p - 1 \\
&\geq n,
\end{aligned}$$

yielding a contradiction.

Next assume that $\text{supp}(S_i) \subseteq H$ for every $i \in [1, \lambda]$. Let

$$S'' = S_1 \cdot \ldots \cdot S_\lambda \cdot S'.$$

Then $S'' \mid S_H$. Let

$$n' = |H| \leq n/p.$$

Since $S'' = S_1 \cdot \ldots \cdot S_\lambda \cdot S'$ with $|S_i| \geq |T_i|$ for $i \in [1, \lambda]$, we have $|S''| \geq (|S| + |S'|)/2 \geq ((n/p + p - 2) + |U| + |S_{\lambda+1}|)/2 \geq (n' + |U| + |S_{\lambda+1}| + 1)/2$.

Let $T = h_1 \cdot h_2 \cdot S_{\lambda+1}$ where $h_1 \cdot h_2 \mid U$. Let $t \geq 0$ be the maximal integer such that S'' has a new factorization

$$S'' = A_1 \cdot \ldots \cdot A_t \cdot W \cdot T$$

where each A_i is a 2-zero-sum free 3-subset of G, and W is a subsequence of S'' which contains no 2-zero-sum free 3-subset of G. Then

$$3t + |W| + |S_{\lambda+1}| + 2 = |S''| \geq (n' + |U| + |S_{\lambda+1}| + 1)/2 \tag{3.2}$$

and

$$\text{supp}(W) \subseteq \{u_1, -u_1, u_2, -u_2\}$$

for some distinct elements $u_1, u_2 \in H$. By Lemma 8, $|\sum_0(A_i)| \geq 7$ for $i \in [1, t]$.

We now show that $|W| > |U|$. Since $S'' \subseteq H$ and $|H| = n'$, we must have

$$\sum\nolimits_0(S'') \subsetneq H, \quad \text{and thus} \quad |\sum\nolimits_0(S'')| \leq n' - 1.$$

For otherwise, $\sum_0(S'') = H$ and thus $\text{st}(\sum_0(S'')) \supseteq H \neq \{0\}$. However, by Lemma 3(1), $\text{st}(\sum_0(S'')) = \{0\}$, yielding a contradiction. By Corollary 1(1) and Lemma 3(2), $|\sum_0(T)| \geq 3(|S_{\lambda+1}| + 1)$. It follows from Lemma 1 and 3(2) that

$$\begin{aligned}
n' - 1 \geq |\sum\nolimits_0(S'')| &= |\sum_{i=1}^{t} \sum\nolimits_0(A_i) + \sum\nolimits_0(W) + \sum\nolimits_0(T)| \\
&\geq \sum_{i=1}^{t} (|\sum\nolimits_0(A_i)| - 1) + (|\sum\nolimits_0(W)| - 1) + |\sum\nolimits_0(T)| \\
&\geq \sum_{i=1}^{t} 6 + |W| + 3(|S_{\lambda+1}| + 1) \\
&= 6t + |W| + 3|S_{\lambda+1}| + 3 \\
&= 2|S''| - |W| + |S_{\lambda+1}| - 1 \\
&\geq n' + |U| + 2|S_{\lambda+1}| - |W| \qquad \text{(by (3.2))}.
\end{aligned}$$

This gives
$$|W| \geq |U| + 2|S_{\lambda+1}| + 1 > |U|.$$
Note that $W \mid S'' \cdot S_{\lambda+1}^{[-1]} = S_1 \cdot \ldots \cdot S_\lambda \cdot U$. In view of Property (2), if u_1 lies in $\mathrm{supp}(S_j)$ for some $j \leq \lambda+1$, then $\mathsf{v}_{\pm u_1}(S'') = \mathsf{v}_{\pm u_1}(S_j)$. Therefore, $u_1 \in \mathrm{supp}(U)$ if and only if $\mathsf{v}_{\pm u_1}(U) = \mathsf{v}_{\pm u_1}(S'')$, meaning all terms equal to u_1 or $-u_1$ in S'' occur in U provided that $u_1 \in \mathrm{supp}(U)$; and likewise for $-u_1$, u_2 and $-u_2$. Since $W \mid S''$ and $\mathrm{supp}(W) \subseteq \{u_1, -u_1, u_2, -u_2\}$, we have $W \mid u_1^{\mathsf{v}_{u_1}(S'')} \cdot (-u_1)^{\mathsf{v}_{-u_1}(S'')} \cdot u_2^{\mathsf{v}_{u_2}(S'')} \cdot (-u_2)^{\mathsf{v}_{-u_2}(S'')}$. If $u_1 \cdot u_2 \mid W$ and $u_1 \cdot u_2 \mid U$, then by what we just proved, $u_1^{\mathsf{v}_{u_1}(S'')} \cdot (-u_1)^{\mathsf{v}_{-u_1}(S'')} \cdot u_2^{\mathsf{v}_{u_2}(S'')} \cdot (-u_2)^{\mathsf{v}_{-u_2}(S'')} \mid U$, so $W \mid U$, implying $|W| \leq |U|$, yielding a contradiction to $|W| > |U|$. Therefore, without loss of generality, we may assume that $u_1 \mid W$ and $u_1 \notin \mathrm{supp}(U)$. Thus $u_1 \in \mathrm{supp}(S_j)$ for some $j \leq \lambda+1$. Since the sequence W is disjoint from $S_{\lambda+1}$ by construction, it follows that $u_1 \in \mathrm{supp}(S_j)$ for some $j \leq \lambda$. In view of Property (2), we conclude that $-u_1 \in \mathrm{supp}(S_j)$ and $v \notin \langle u_1 \rangle \leq \langle g_j \rangle$ for every $v \in \mathrm{supp}(S_{\lambda+1})$. Write $W = W_1 \cdot W_2$ with
$$W_1 \mid u_1^{[\mathsf{v}_{u_1}(S'')]} \cdot (-u_1)^{[\mathsf{v}_{-u_1}(S'')]} \quad \text{and} \quad W_2 \mid u_2^{[\mathsf{v}_{u_2}(S'')]} \cdot (-u_2)^{[\mathsf{v}_{-u_2}(S'')]}.$$
Now fix $v \mid S_{\lambda+1}$. Let $V = W_1 \cdot v$ and $T' = T \cdot v^{[-1]}$. We obtain another factorization
$$S'' = A_1 \cdot \ldots \cdot A_t \cdot V \cdot W_2 \cdot T'.$$
Since $v \notin \langle u_1 \rangle$, by Corollary 1(1) and Lemma 3(2), $|\sum_0(V)| \geq 2(|W_1|+1)$. Note that
$$|S''| = 3t + |V| + |W_2| + |T| - 1 = 3t + |W_1| + |W_2| + |S_{\lambda+1}| + 2. \tag{3.3}$$
As before, we obtain
$$\begin{aligned} n' - 1 &\geq |\textstyle\sum_0(S'')| = |\displaystyle\sum_{i=1}^{t} \textstyle\sum_0(A_i) + \sum_0(V) + \sum_0(W_2) + \sum_0(T')| \\ &\geq \sum_{i=1}^{t} (|\textstyle\sum_0(A_i)| - 1) + (|\sum_0(V)| - 1) + (|\sum_0(W_2)| - 1) + |\sum_0(T')| \\ &\geq \sum_{i=1}^{t} 6 + 2|W_1| + 1 + |W_2| + 3|S_{\lambda+1}| \\ &= 6t + 2|W_1| + |W_2| + 3|S_{\lambda+1}| + 1 \\ &= 2|S''| - |W_2| + |S_{\lambda+1}| - 3 \qquad \text{(by (3.3))} \\ &\geq n' + |U| + 2|S_{\lambda+1}| - |W_2| - 2 \qquad \text{(by (3.2))}, \end{aligned}$$

implying

$$|W_2| \geq |U| + 2|S_{\lambda+1}| - 1 > |U|.$$

Next we consider W_2. Since $\mathrm{supp}(W_2) \subseteq \{u_2, -u_2\}$, if $u_2 \in \mathrm{supp}(U)$, then as above, we obtain $W_2 \mid U$, implying $|W_2| \leq |U|$, giving a contradiction. Thus $u_2 \notin \mathrm{supp}(U)$. As above, we conclude that $\{\pm u_2\} \subseteq \mathrm{supp}(S_{j'})$ for some $j' \leq \lambda$ and $z \notin \langle u_2 \rangle \leq \langle g_{j'} \rangle$ for every $z \in \mathrm{supp}(S_{\lambda+1})$. Since $|S_{\lambda+1}| \geq 2p - 1 \geq 5$, we can choose $z \mid S_{\lambda+1} \cdot v^{[-1]}$. Define $V = W_1 \cdot v$, $Z = W_2 \cdot z$ and $T'' = T \cdot v^{[-1]} \cdot z^{[-1]}$. Thus we obtain another factorization

$$S'' = A_1 \cdot \ldots \cdot A_t \cdot V \cdot Z \cdot T''.$$

As before, we obtain

$$\begin{aligned}
n' - 1 &\geq |\textstyle\sum_0(S'')| = |\displaystyle\sum_{i=1}^{t} \textstyle\sum_0(A_i) + \sum_0(V) + \sum_0(Z) + \sum_0(T'')| \\
&\geq \sum_{i=1}^{t}(|\textstyle\sum_0(A_i)| - 1) + (|\sum_0(V)| - 1) + (|\sum_0(Z)| - 1) + |\sum_0(T'')| \\
&\geq \sum_{i=1}^{t} 6 + 2|W_1| + 1 + 2|W_2| + 1 + 3(|S_{\lambda+1}| - 1) \\
&= 6t + 2|W_1| + 2|W_2| + 3|S_{\lambda+1}| - 1 \\
&= 2|S''| + |S_{\lambda+1}| - 5 \qquad \text{(by (3.3))} \\
&\geq n' + |U| + 2|S_{\lambda+1}| - 4 \qquad \text{(by (3.2))} \\
&\geq n' \qquad (\text{as } |U| \geq 2p - 1 \geq 5),
\end{aligned}$$

yielding a contradiction. In all cases we have found contradictions. Thus we must have $\sum(S) = G$. This completes the proof. □

We end this paper with the following remark.

Remark 1. It was proved that $f(6) = 19$ in [6, Theorem 1.2]. Thus Lemma 5 can be improved as follows: if $A \subseteq G \setminus \{0\}$ is a subset with $|A| \geq 21$, then there is a subset $B \subset A$ such that $|\sum_0(B)| \geq 3|B| + 2$ with $|B| \leq 6$. Therefore, when $p = 3$, we may relax the condition $|G| \geq 72p^6 = 52488$ to $|G| \geq 3045$, and the same proof as in Theorem 1 still works.

Acknowledgements. We would like to thank the referee for their valuable suggestions which helped improve the readability and the presentation of the paper. Part of this work was carried out during a visit of the first author to Brock University as an international visiting scholar. He would like to gratefully thank the host institution for its hospitality and for providing an excellent atmosphere for research. This work was supported in part by the National Natural Science Foundation of China (No. 11701256, 11871258, 12071344), the Youth Backbone Teacher Foundation of Henan's University (No. 2019GGJS196), the China Scholarship Council (Grant No. 201908410132), and it was also supported in part by a Discovery Grant from the Natural Sciences and Engineering Research Council of Canada (Grant No. RGPIN 2017-03903).

References

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

[2] M. Freeze, W. Gao and A. Geroldinger, The critical number of finite abelian groups, *J. Number Theory* **129** (2009), 2766-2777; Corrigendum, ibid. **152** (2015), 205-207.

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

[4] W. Gao, D. Han, G. Qian, Y. Qu and H. Zhang, On additive bases II, *Acta Arith.* **168** (2015), 247-267.

[5] W. Gao, M. Huang, W. Hui, Y. Li, C. Liu and J. Peng, Sums of sets of abelian group elements, *J. Number Theory* **208** (2020), 208-229.

[6] W. Gao, Y. Li, J. Peng and F. Sun, Subsums of a zero-sum free subset of an abelian group, *Electron. J. Combin.* **15** (2008), R116.

[7] W. Gao, J. Peng and Q. Zhong, A quantivative aspect of non-unique factorizations: the Narkiewicz constants III, *Acta Arith.* **158** (2013), 271-285.

[8] W. Gao, Y. Qu and H. Zhang, On additive bases III, *Acta Arith.* **193** (2020), 293-308.

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

[10] G. Martin, A. Peilloux and E. Wong, Lower bounds for sumsets of multisets in $\mathbb{Z}_p^2$, *Integers* **13** (2013), art. A72, 17pp.

[11] K. Matomäki, On sumsets of multisets in $\mathbb{Z}_p^m$, *Electron. J. Combin.* **20** (2013), art. 30, 10pp.

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

[13] C. Peng, Addition theorems in elementary abelian groups I, *J. Number Theory* **27** (1987), 46-57.

[14] C. Peng, Addition theorems in elementary abelian groups II, *J. Number Theory* **27** (1987), 58-62.

[15] Y. Qu and D. Han, An inverse theorem for additive bases, *Int. J. Number Theory* **12** (2016), 1509-1518.

[16] Y. Qu and D. Han, Additive bases of $C_p \oplus C_{p^n}$, *Int. J. Number Theory* **13** (2017), 2453-2459.

[17] Y. Qu and Y. Li, Additive bases of $C_3 \oplus C_{3q}$, *Colloq. Math.*, DOI: 10.4064/cm8515-6-2021.