INTEGERS: ELECTRONIC JOURNAL OF COMBINATORIAL NUMBER THEORY 8 (2008), #A22

ON RESTRICTED SUMSETS IN ABELIAN GROUPS OF ODD ORDER

Guoqing Wang
Institute of Mathematics, Dalian University of Technology, Dalian, 116024, P.R. China
gqwang1979@yahoo.com.cn

Received: 12/28/07, Revised: 1/17/08, Accepted: 4/8/08, Published: 4/17/08

Abstract

Let G be an abelian group of odd order, and let $\mathcal{A}$ be a subset of G. For any integer h such that $2 \leq h \leq |\mathcal{A}| - 2$, we prove that $|h^\wedge\mathcal{A}| \geq |\mathcal{A}|$ and equality holds if and only if $\mathcal{A}$ is a coset of some subgroup of G, where $h^\wedge\mathcal{A}$ is the set of all sums of h distinct elements of $\mathcal{A}$.

1. Introduction

Let $\mathcal{A}$ be a subset of an abelian group. For any integer $h \in \mathbb{N}_0$, we denote by $h^\wedge\mathcal{A}$ the set consisting of all sums of h distinct elements of $\mathcal{A}$, that is, all sums of the form $a_1 + \cdots + a_h$, where $a_1, \ldots, a_h \in \mathcal{A}$ and $a_i \neq a_j$ for $i \neq j$. Throughout this paper, let $\mathbb{Z}_n$ be the cyclic group of n elements, and let p be a prime number.

Over 40 years ago, Erdős and Heilbronn conjectured that $|2^\wedge\mathcal{A}| \geq \min\{p, 2|\mathcal{A}| - 3\}$, where $\mathcal{A}$ is a subset of the group $\mathbb{Z}_p$. Dias da Silva and Hamidoune [4] proved the generalization of this Erdős-Heilbronn conjecture for h-fold sums: $|h^\wedge\mathcal{A}| \geq \min\{p, h|\mathcal{A}| - h^2 + 1\}$.

Another proof was given by Alon, Nathanson and Ruzsa [1, 2] by using the polynomial method. L. Gallardo, G. Grekos, L. Habsieger, et al [5] made a study of $2^\wedge\mathcal{A}$ and $3^\wedge\mathcal{A}$, where $\mathcal{A}$ is a subset of the group $\mathbb{Z}_n$. They obtained that $|2^\wedge\mathcal{A}| \geq n - 2$ in the case when $|\mathcal{A}| \geq \lfloor n/2 \rfloor + 1$. They also proved that $|3^\wedge\mathcal{A}| = n$ in the case when $|\mathcal{A}| \geq \lfloor n/2 \rfloor + 1$ and $n \geq 16$. Hamidoune, Lladó and Serra [6] investigated restricted sumsets for general finite abelian groups. They proved that, for an abelian group G of odd order (respectively, cyclic group), $|2^\wedge\mathcal{A}| \geq \min\{|G|, 3|\mathcal{A}|/2\}$ holds when $\mathcal{A}$ is a generating set of G, $0 \in \mathcal{A}$ and $|\mathcal{A}| \geq 21$ (respectively, $|\mathcal{A}| \geq 33$). The structure of a set for which equality holds was also determined.

For general finite abelian groups and an arbitrary positive integer h, very little is known about $|h^\wedge\mathcal{A}|$.

Our main result in this paper is the following.

Theorem 1.1 *Let G be an abelian group of odd order, and let $\mathcal{A}$ be a subset of G with $0 \in \mathcal{A}$. Let $2 \leq h \leq |\mathcal{A}| - 2$. Then $|h^\wedge\mathcal{A}| \geq |\mathcal{A}|$. Moreover, equality holds if and only if $\mathcal{A}$ is a subgroup of G.*

2. Proof of Theorem 1.1

We begin by introducing some notation.

Let G be an abelian group. Let $S = g_1 \cdot \ldots \cdot g_l$ be a sequence of elements in G. We call $|S| = l$ the length of S; $\sigma(S) = \sum_{i=1}^{l} g_i$ the sum of S; $supp(S) = \{g : g \text{ is contained in } S\}$ the support of S; and $\sum_h(S) = \{\sum_{i \in I} g_i : I \subseteq [1, l] \text{ with } |I| = h\}$ the set of h-term subsums of S. Also, for T a subsequence of S, we let $S \cdot T^{-1}$ denote the sequence after removing the elements of T from S.

Let $\mathcal{A}$ be a subset of the group G with $|\mathcal{A}| = l$. If $h > l$, then $h^\wedge\mathcal{A} = \emptyset$. We define $0^\wedge\mathcal{A} = \{0\}$. Note that $|h^\wedge\mathcal{A}| = |(l-h)^\wedge\mathcal{A}|$ for $h = 0, 1, \ldots, l$. In particular, $|(l-1)^\wedge\mathcal{A}| = |1^\wedge\mathcal{A}| = |\mathcal{A}|$. Moreover, we have $h^\wedge(\mathcal{A} + g) = h^\wedge\mathcal{A} + hg$ for any $g \in G$. This means that the function $|h^\wedge\mathcal{A}|$ is invariant under the translation of the set $\mathcal{A}$.

For groups G and H, we use $H \leq G$ to mean that H is a subgroup of G.

Lemma 2.1 *[3] Let $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_h$ be nonempty subsets of the group $\mathbb{Z}_p$. Then*

$$|\mathcal{A}_1 + \mathcal{A}_2 + \ldots + \mathcal{A}_h| \geq \min\left\{p, \sum_{i=1}^{h} |\mathcal{A}_i| - h + 1\right\}.$$

Lemma 2.2 *[4] Let $\mathcal{A}$ be a nonempty subset of the group $\mathbb{Z}_p$, and let $1 \leq h \leq |\mathcal{A}|$. Then*

$$|h^\wedge\mathcal{A}| \geq \min\{p, h(|\mathcal{A}| - h) + 1\}.$$

Lemma 2.3 *Let $h \geq 2$, and let $\mathcal{A}$ be a subset of the group $\mathbb{Z}_p$ such that $|\mathcal{A}| \geq 2h$. Then $|h^\wedge\mathcal{A}| \geq |\mathcal{A}|$. Moreover, equality holds if and only if $\mathcal{A} = \mathbb{Z}_p$.*

Proof. It follows from Lemma 2.2 that $|h^\wedge\mathcal{A}| \geq \min\{p, h(|\mathcal{A}| - h) + 1\} \geq |\mathcal{A}|$. Since $h(|\mathcal{A}| - h) + 1 > |\mathcal{A}|$, it follows that if $|h^\wedge\mathcal{A}| = |\mathcal{A}|$ then $|\mathcal{A}| = p$. □

Lemma 2.4 *Let G be a finite abelian group, and let X and Y be two subsets of G such that $|X| = |Y| \geq 2$. Then $|X + Y| \geq |X|$. Moreover, equality holds if and only if there exists a subgroup H of G such that, $X = H + g_x$ and $Y = H + g_y$ where $g_x \in X$ and $g_y \in Y$.*

Proof. $|X+Y| \geq |X|$ holds trivially. Now suppose $|X+Y| = |X| = |Y|$. Choose $g_x \in X$ and $g_y \in Y$. Put $X' = X - g_x$ and $Y' = Y - g_y$. Since $0 \in X' \bigcap Y'$, we have $X' \cup Y' \subseteq X' + Y'$. Also, we see that $|X'| = |X|$, $|Y'| = |Y|$ and $|X'+Y'| = |X+Y|$. It follows that $|X'+Y'| = |X'| = |Y'|$, and so $X' = Y' = X'+Y' = X'+X'$. Therefore, X' is a subgroup of G and we are done. □

Lemma 2.5 *Let G, $G^{'}$ be finite abelian groups and φ a homomorphism of G to $G^{'}$. Let $\mathcal{A}$ be a subset of G of cardinality l, and let $1 \leq h \leq l$. Then $\varphi(h^\wedge \mathcal{A}) = \sum_h(S)$, where $S = \prod_{g\in\mathcal{A}} \varphi(g)$ is a sequence of elements in $G^{'}$.*

Proof. The conclusion follows from the definition of a group homomorphism. □

Lemma 2.6 *Let $h \geq 1$, and let S be a sequence of elements in the group $\mathbb{Z}_p$ with $|S| \geq h+1$. Then $|\sum_h(S)| \geq |supp(S)|$.*

Proof. Let $k = |supp(S)|$. The lemma is trivial if $h = 1$ or $k = 1$. Therefore, we may assume that $h \geq 2$ and $k \geq 2$. Let $S = S_0 \cdot S_1$, where $S_0 = supp(S)$ and $S_1 = S \cdot S_0^{-1}$. Let $h_0 = \min\{k-1, h\}$ and $h_1 = h - h_0$. Then $1 \leq h_0 \leq k-1 = |S_0| - 1$ and $0 \leq h_1 \leq |S_1|$. It follows that $\sum_{h_0}(S_0) + \sum_{h_1}(S_1) \subseteq \sum_h(S)$. By Lemma 2.2, we have $|\sum_{h_0}(S_0)| \geq \min\{p, h_0(k-h_0)+1\} \geq k$. It follows from Lemma 2.1 that $|\sum_h(S)| \geq |\sum_{h_0}(S_0) + \sum_{h_1}(S_1)| \geq \min\{p, |\sum_{h_0}(S_0)| + |\sum_{h_1}(S_1)| - 1\} \geq \min\{p, k\} = k$. □

Lemma 2.7 *Let $h \geq 2$, and let $S = g_1^{\alpha_1} g_2^{\alpha_2} \cdot \ldots \cdot g_r^{\alpha_r}$ be a sequence of elements in the group $\mathbb{Z}_p$ with $|S| \geq h+2$, where $r \geq 2$ and $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_r \geq 1$. If $\alpha_2 \geq 2$ or $r \geq 4$ then $|\sum_h(S)| \geq \min\{p, r+1\}$.*

Proof. Let $S = S_0 \cdot S_1$, where $S_0 = supp(S) = \{g_1, g_2, \ldots, g_r\}$ and $S_1 = S \cdot S_0^{-1}$. If $\alpha_2 \geq 2$, let $h_0 = \min\{r-1, h-1\}$ and $h_1 = h - h_0$. Then $1 \leq h_0 \leq r-1$ and $1 \leq h_1 \leq |S_1| - 1$. By Lemma 2.6, we have $|\sum_{h_0}(S_0)| \geq |supp(S_0)| = r$ and $|\sum_{h_1}(S_1)| \geq |supp(S_1)| \geq 2$. Note that $\sum_{h_0}(S_0) + \sum_{h_1}(S_1) \subseteq \sum_h(S)$. It follows from Lemma 2.1 that $|\sum_h(S)| \geq |\sum_{h_0}(S_0) + \sum_{h_1}(S_1)| \geq \min\{p, |\sum_{h_0}(S_0)| + |\sum_{h_1}(S_1)| - 1\} \geq \min\{p, r+1\}$.

Now assume that $r \geq 4$. Let $h_0 = \min\{r-2, h\}$ and $h_1 = h - h_0$. Then $2 \leq h_0 \leq r-2$ and $0 \leq h_1 \leq |S_1|$. By Lemma 2.2, we have $|\sum_{h_0}(S_0)| \geq \min\{p, h_0(r-h_0)+1\} \geq \min\{p, r+1\}$. Note that $\sum_{h_0}(S_0) + \sum_{h_1}(S_1) \subseteq \sum_h(S)$. It follows from Lemma 2.1 that $|\sum_h(S)| \geq |\sum_{h_0}(S_0) + \sum_{h_1}(S_1)| \geq \min\{p, |\sum_{h_0}(S_0)| + |\sum_{h_1}(S_1)| - 1\} \geq \min\{p, r+1\}$. □

Proof of Theorem 1.1. Let $\mathcal{A} = \{a_0, a_1, \ldots, a_{l-1}\}$, where $a_0 = 0$. Since $|h^\wedge\mathcal{A}| = |(l-h)^\wedge\mathcal{A}|$, we need only to consider the case that $h \le \lfloor |\mathcal{A}|/2 \rfloor$.

Let m be the number of prime factors of $|G|$ (counted with multiplicity). We proceed by induction on m. If $m = 1$, the theorem follows from Lemma 2.3. Now assume $|G|$ is composite. Let p be the smallest prime factor of $|G|$, and let H be a subgroup of G of index p. Let ϕ_H be the canonical epimorphism of G onto G/H. Then $\bar{S} = \prod_{i=0}^{l-1} \phi_H(a_i)$ is a sequence of elements in G/H. Let $G/H = \{H, H+g, \ldots, H+(p-1)g\}$. For convenience, we also let G/H denote $\{\bar{g}, 2\bar{g}, \ldots, p\bar{g}\}$. Define $\mathcal{A}_i = \mathcal{A} \bigcap (H + ig)$ for $i = 0, 1, \ldots, p-1$. Then $\mathcal{A} = \bigcup_{i=0}^{p-1} \mathcal{A}_i$. Let $M = \max\{|\mathcal{A}_i| : 0 \le i \le p-1\}$. Since $|h^\wedge\mathcal{A}|$ is invariant under the translation of A, we can assume without loss of generality that $M = |\mathcal{A}_0|$. Note that, if $|\mathcal{A}| = 4$, then $h = 2$, and so $|2^\wedge\mathcal{A}| > |\mathcal{A}|$ follows by straightforward calculations. So, we may assume that $|\mathcal{A}| \ge 5$.

If $M = 1$, then $\bar{S}$ is squarefree, that is, $\bar{S}$ is a subset of G/H with $|\bar{S}| = |\mathcal{A}|$. By Lemma 2.3, we have $|\sum_h(\bar{S})| \ge |\bar{S}|$. It follows from Lemma 2.5 that $|\phi_H(h^\wedge\mathcal{A})| = |\sum_h(\bar{S})|$, and so $|h^\wedge\mathcal{A}| \ge |\phi_H(h^\wedge\mathcal{A})| = |\sum_h(\bar{S})| \ge |\bar{S}| = |\mathcal{A}|$. Now suppose $|h^\wedge\mathcal{A}| = |\mathcal{A}|$. Then $|\sum_h(\bar{S})| = |\bar{S}|$. It follows from Lemma 2.3 that $\bar{S} = G/H$, and so $\mathcal{A} = \{a_0, a_1, \ldots, a_{p-1}\}$, where $\phi_H(a_i) = i\bar{g}$ for each $i \in [0, p-1]$. Moreover, since $\phi_H(h^\wedge\mathcal{A}) = \sum_h(\bar{S}) = G/H$, we conclude that $h^\wedge\mathcal{A} = \{c_0, c_1, \ldots, c_{p-1}\}$, where $\phi_H(c_j) = j\bar{g}$ for each $j \in [0, p-1]$.

We denote by $|i|$ the least nonnegative residue of i modulo p. Let $d_i = a_{|i+1|} - a_{|i|}$ for $i = 0, 1, \ldots, p-1$. We shall prove that $d_i = d_0$ for $i = 0, 1, \ldots, p-1$. Let i be an arbitrary integer of $[0, p-1]$. Choose a subset U of $\mathcal{A}$ of cardinality h such that $\{a_{|i|}, a_{|i+1|}\} \subseteq U$ and $\{a_{|i-1|}, a_{|i+2|}\} \bigcap U = \emptyset$. Let $U' = (U \setminus \{a_{|i|}, a_{|i+1|}\}) \bigcup \{a_{|i-1|}, a_{|i+2|}\}$. It follows that $\phi_H(\sigma(U)) = \sigma(\phi_H(U)) = \sigma(\phi_H(U')) = \phi_H(\sigma(U')) = x\bar{g}$ for some $x \in [0, p-1]$, and so $\sigma(U) = c_x = \sigma(U')$. It follows that $d_{|i+1|} = (a_{|i+2|} - a_{|i+1|}) = (a_{|i|} - a_{|i-1|}) = d_{|i-1|}$. Since $\gcd(2, p) = 1$, it follows that $d_i = d_0$ for $i = 0, 1, \ldots, p-1$. Therefore, we have $\mathcal{A} = \{a_0, a_0 + d_0, a_0 + 2d_0, \ldots, a_0 + (p-1)d_0\} =< d_0 >\le G$, and we are done.

Now we assume $M \ge 2$. We split the proof into two steps.

<u>Step 1.</u> We shall show $|h^\wedge\mathcal{A}| \ge |\mathcal{A}|$, and find some necessary conditions for $|h^\wedge\mathcal{A}| = |\mathcal{A}|$.

Let $\bar{T} = \prod_{a_i \in \mathcal{A} \setminus \mathcal{A}_0} \phi_H(a_i)$. Then $\bar{T}$ is a subsequence of $\bar{S}$.

Case 1. $|supp(\bar{S})| = 1$. This implies that $\mathcal{A} \subseteq H$. It follows from the induction hypothesis that $|h^\wedge\mathcal{A}| \ge |\mathcal{A}|$.

Case 2. $|supp(\bar{S})| = 2$. This implies that $\mathcal{A} = \mathcal{A}_0 \bigcup \mathcal{A}_{i_1}$, where $i_1 \in [1, p-1]$.

Subcase 2.1 $|\mathcal{A}_{i_1}| = 1$. We have $|\mathcal{A}_0| = |\mathcal{A}| - 1 \ge 2h - 1 \ge h + 1$. Let $W_0 =$

$h^\wedge\mathcal{A}_0$ and $W_1 = (h-1)^\wedge\mathcal{A}_0 + \mathcal{A}_{i_1}$. Observe $W_0 \bigcup W_1 \subseteq h^\wedge\mathcal{A}$. Since $\phi_H(W_0) = \bar{0}$ and $\phi_H(W_1) = i_1\bar{g}$, we have $W_0 \bigcap W_1 = \emptyset$. By the induction hypothesis, we have $|h^\wedge\mathcal{A}_0| \geq |\mathcal{A}_0|$ and $|(h-1)^\wedge\mathcal{A}_0| \geq |\mathcal{A}_0|$. Thus, $|W_j| \geq |\mathcal{A}_0|$ for both $j=0$ and $j=1$. Therefore, it follows that $|h^\wedge\mathcal{A}| \geq |W_0 \bigcup W_1| = |W_0| + |W_1| \geq 2|\mathcal{A}_0| > |\mathcal{A}|$.

Subcase 2.2 $|\mathcal{A}_{i_1}| \geq 2$. Since $|\mathcal{A}| \geq \max\{2h, 5\}$ and $|\mathcal{A}_0| \geq |\mathcal{A}|/2$, we have $|\mathcal{A}_0| \geq \max\{h, 3\}$. Let $h_0 = \min\{|\mathcal{A}_0| - 1, h\}$ and $h_1 = h - h_0$. Then $2 \leq h_0 \leq |\mathcal{A}_0| - 1$, and $h_1 \in \{0, 1\}$ since $h \leq \lfloor |\mathcal{A}|/2 \rfloor \leq |\mathcal{A}_0|$. Moreover, we have $h_1 + 2 \leq |\mathcal{A}_{i_1}|$, since if $|\mathcal{A}_{i_1}| = 2$ then $h_0 = h \leq \lfloor |\mathcal{A}|/2 \rfloor \leq |\mathcal{A}_0| - 1$, and since if $|\mathcal{A}_{i_1}| > 2$ then it is trivial.

Let $W_0 = h_0^\wedge\mathcal{A}_0 + h_1^\wedge\mathcal{A}_{i_1}$, $W_1 = (h_0-1)^\wedge\mathcal{A}_0 + (h_1+1)^\wedge\mathcal{A}_{i_1}$ and $W_2 = (h_0-2)^\wedge\mathcal{A}_0 + (h_1+2)^\wedge\mathcal{A}_{i_1}$. Note that W_0, W_1, W_2 are pairwise disjoint nonempty subsets of $h^\wedge\mathcal{A}$. By the induction hypothesis, we have that $|W_0| \geq |h_0^\wedge\mathcal{A}_0| \geq |\mathcal{A}_0|$ and $|W_1| \geq |(h_0-1)^\wedge\mathcal{A}_0| \geq |\mathcal{A}_0|$. Therefore, $|h^\wedge\mathcal{A}| \geq |W_0| + |W_1| + |W_2| \geq 2|\mathcal{A}_0| + 1 > |\mathcal{A}|$.

Case 3. $|supp(\bar{S})| = r \geq 3$. We rewrite $\mathcal{A} = \bigcup_{j=0}^{r-1} \mathcal{A}_{i_j}$, where $i_0 = 0$, $\{i_1, \ldots, i_{r-1}\} \subseteq [1, p-1]$, and $|\mathcal{A}_0| \geq |\mathcal{A}_{i_1}| \geq \cdots \geq |\mathcal{A}_{i_{r-1}}| > 0$.

If $h = 2$, let $W_j = \mathcal{A}_0 + \mathcal{A}_{i_j}$ for $j = 1, \ldots, r-1$. It follows that $\phi_H(W_j) = i_j\bar{g}$. Since $r \geq 3$, it follows from Lemma 2.2 that $|2^\wedge supp(\bar{S})| \geq \min\{p, 2(r-2)+1\} \geq r$, and so there exists a 2-subset $\{x, y\} \subseteq [1, r-1]$ such that $i_x\bar{g} + i_y\bar{g} \notin \{i_1\bar{g}, i_2\bar{g}, \ldots, i_{r-1}\bar{g}\}$. Let $W_0 = \mathcal{A}_{i_x} + \mathcal{A}_{i_y}$. Since $\phi_H(W_0) = i_x\bar{g} + i_y\bar{g}$, it follows that $W_0, W_1, \ldots, W_{r-1}$ are pairwise disjoint. It is easy to see that $|W_0| \geq \max\{|\mathcal{A}_{i_x}|, |\mathcal{A}_{i_y}|\} \geq |\mathcal{A}_{i_{r-2}}|$ and $|W_j| \geq |\mathcal{A}_0|$ for $j = 1, \ldots, r-1$. Therefore, $|2^\wedge\mathcal{A}| \geq \sum_{j=0}^{r-1} |W_j| \geq |\mathcal{A}_{i_{r-2}}| + (r-1)|\mathcal{A}_0| \geq |\mathcal{A}_0| + |\mathcal{A}_{i_1}| + \cdots + |\mathcal{A}_{i_{r-1}}| = |\mathcal{A}|$.

Moreover, if $|2^\wedge\mathcal{A}| = |\mathcal{A}|$, then,

$$2^\wedge\mathcal{A} = \bigcup_{j=0}^{r-1} W_j, \text{ and } |W_j| = |\mathcal{A}_{i_j}| = |\mathcal{A}_0| \text{ for } j = 0, 1, \ldots, r-1. \tag{2.1}$$

Now we suppose $h \geq 3$ and distinguish several subcases.

Subcase 3.1 $|supp(\bar{S})| = 3$. This implies that $\mathcal{A} = \mathcal{A}_0 \bigcup \mathcal{A}_{i_1} \bigcup \mathcal{A}_{i_2}$, where $\{i_1, i_2\} \subseteq [1, p-1]$ and $|\mathcal{A}_0| \geq |\mathcal{A}_{i_1}| \geq |\mathcal{A}_{i_2}| > 0$.

Subsubcase 3.1.1 $|\mathcal{A}_0| \geq h$. Let $W_0 = (h-1)^\wedge\mathcal{A}_0 + \mathcal{A}_{i_1}$, $W_1 = (h-1)^\wedge\mathcal{A}_0 + \mathcal{A}_{i_2}$ and $W_2 = (h-2)^\wedge\mathcal{A}_0 + \mathcal{A}_{i_1} + \mathcal{A}_{i_2}$. Note that W_0, W_1, W_2 are pairwise disjoint subsets of $h^\wedge\mathcal{A}$. By the induction hypothesis, we have that $|(h-1)^\wedge\mathcal{A}_0| \geq |\mathcal{A}_0|$ and $|(h-2)^\wedge\mathcal{A}_0| \geq |\mathcal{A}_0|$. Thus, $|W_j| \geq |\mathcal{A}_0|$ for $j = 0, 1, 2$. It follows that $|h^\wedge\mathcal{A}| \geq |W_0| + |W_1| + |W_2| \geq 3|\mathcal{A}_0| \geq |\mathcal{A}|$.

Moreover, if $|h^\wedge\mathcal{A}| = |\mathcal{A}|$, then

$$h^\wedge\mathcal{A} = \bigcup_{j=0}^{2} W_j \text{ and } |W_j| = |\mathcal{A}_{i_j}| = |\mathcal{A}_0| \text{ for } j = 0, 1, 2. \tag{2.2}$$

Subsubcase 3.1.2 $|\mathcal{A}_0| < h$. Note that since $h \leq \lfloor |\mathcal{A}|/2 \rfloor$ we have $|\mathcal{A}_{i_j}| \geq 2$ for both $j = 1$ and $j = 2$. Let $h_0 = |\mathcal{A}_0| - 1$ and $h_1 = h - h_0$. Then $h_0 \geq 1$, and $2 \leq h_1 \leq |\mathcal{A} \setminus \mathcal{A}_0| - 2$, since $|\mathcal{A}_0| - 1 \leq h - 2$ and $|\mathcal{A} \setminus \mathcal{A}_0| - h_1 + |\mathcal{A}_0| - h_0 = |\mathcal{A}| - h \geq h \geq 3$.

By Lemma 2.5 and Lemma 2.7, we have $|\phi_H(h_1^\wedge(\mathcal{A} \setminus \mathcal{A}_0))| = |\sum_{h_1}(\bar{T})| \geq \min\{p, |supp(\bar{T})| + 1\} = 3$, and so there exists a 3-subset $\{c_0, c_1, c_2\} \subseteq h_1^\wedge(\mathcal{A} \setminus \mathcal{A}_0)$ such that $\phi_H(c_0)$, $\phi_H(c_1)$ and $\phi_H(c_2)$ are pairwise distinct.

Let $W_j = h_0^\wedge \mathcal{A}_0 + c_j$ for $j = 0, 1, 2$. Similar to Subsubcase 3.1.1, we have $|h^\wedge \mathcal{A}| \geq |W_0| + |W_1| + |W_2| \geq 3|\mathcal{A}_0| \geq |\mathcal{A}|$.

Moreover, if $|h^\wedge \mathcal{A}| = |\mathcal{A}|$, then

$$h^\wedge \mathcal{A} = \bigcup_{j=0}^{2} W_j \text{ and } |W_j| = |\mathcal{A}_{i_j}| = |\mathcal{A}_0| \text{ for } j = 0, 1, 2. \tag{2.3}$$

Subcase 3.2 $|supp(\bar{S})| = 4$. This implies that $\mathcal{A} = \mathcal{A}_0 \bigcup \mathcal{A}_{i_1} \bigcup \mathcal{A}_{i_2} \bigcup \mathcal{A}_{i_3}$, where $\{i_1, i_2, i_3\} \subseteq [1, p-1]$ and $|\mathcal{A}_0| \geq |\mathcal{A}_{i_1}| \geq |\mathcal{A}_{i_2}| \geq |\mathcal{A}_{i_3}| > 0$. Let $h_0 = \min\{|\mathcal{A}_0| - 1, h - 2\}$ and $h_1 = h - h_0$. Note that $1 \leq h_0 \leq |\mathcal{A}_0| - 1$ and $2 \leq h_1 \leq |\mathcal{A} \setminus \mathcal{A}_0| - 1$.

Subsubcase 3.2.1 $|\mathcal{A}_{i_2}| = 1$. By Lemma 2.5 and Lemma 2.6, we have $|\phi_H(h_1^\wedge(\mathcal{A} \setminus \mathcal{A}_0))| = |\sum_{h_1}(\bar{T})| \geq |supp(\bar{T})| = 3$, and so there exists a 3-subset $\{c_0, c_1, c_2\} \subseteq h_1^\wedge(\mathcal{A} \setminus \mathcal{A}_0)$ such that $\phi_H(c_0)$, $\phi_H(c_1)$ and $\phi_H(c_2)$ are pairwise distinct.

Let $W_j = h_0^\wedge \mathcal{A}_0 + c_j$ for $j = 0, 1, 2$. Note that W_0, W_1 and W_2 are pairwise disjoint subsets of $h^\wedge \mathcal{A}$. By the induction hypothesis, we have $|W_j| = |h_0^\wedge \mathcal{A}_0| \geq |\mathcal{A}_0|$ for $j = 0, 1, 2$. By Lemma 2.5 and Lemma 2.7, we have $|\phi_H(h^\wedge \mathcal{A})| = |\sum_h(\bar{S})| \geq \min\{p, |supp(\bar{S})| + 1\} = 5$, and so there exist at least two distinct elements c_3, c_4 of $(h^\wedge \mathcal{A}) \setminus (W_0 \bigcup W_1 \bigcup W_2)$. Therefore, $|h^\wedge \mathcal{A}| \geq |W_0| + |W_1| + |W_2| + |\{c_3, c_4\}| \geq 3|\mathcal{A}_0| + 2 > |\mathcal{A}|$.

Subsubcase 3.2.2 $|\mathcal{A}_{i_2}| \geq 2$. We have $h_1 \leq |\mathcal{A} \setminus \mathcal{A}_0| - 2$, since it is trivial if $h_0 = h - 2 \leq |\mathcal{A}_0| - 1$, and since $|\mathcal{A}_0| - h_0 + |\mathcal{A} \setminus \mathcal{A}_0| - h_1 = |\mathcal{A}| - h \geq h \geq 3$ if $h_0 = |\mathcal{A}_0| - 1 \leq h - 2$.

By Lemma 2.5 and Lemma 2.7, we have $|\phi_H(h_1^\wedge(\mathcal{A} \setminus \mathcal{A}_0))| = |\sum_{h_1}(\bar{T})| \geq \min\{p, |supp(\bar{T})| + 1\} = 4$, and so there exists a 4-subset $\{c_0, c_1, c_2, c_3\} \subseteq h_1^\wedge(\mathcal{A} \setminus \mathcal{A}_0)$ such that $\phi_H(c_0)$, $\phi_H(c_1)$, $\phi_H(c_2)$ and $\phi_H(c_3)$are pairwise distinct.

Let $W_j = h_0^\wedge \mathcal{A}_0 + c_j$ for $j = 0, 1, 2, 3$. Note that W_0, W_1, W_2 and W_3 are pairwise disjoint subsets of $h^\wedge \mathcal{A}$. By Lemma 2.7, we have $|\sum_h(\bar{S})| \geq 5$, and so there exists an element $c_4 \in (h^\wedge \mathcal{A}) \setminus (W_0 \bigcup W_1 \bigcup W_2 \bigcup W_3)$. Therefore, $|h^\wedge \mathcal{A}| \geq |W_0| + |W_1| + |W_2| + |W_3| + 1 \geq 4|\mathcal{A}_0| + 1 > |\mathcal{A}|$.

Subcase 3.3 $|supp(\bar{S})| = r \geq 5$. Let $h_0 = \min\{|\mathcal{A}_0| - 1, h - 2\}$ and $h_1 = h - h_0$.

Similar to Subsubcase 3.1.2, we have $1 \leq h_0 \leq |\mathcal{A}_0| - 1$ and $2 \leq h_1 \leq |\mathcal{A} \setminus \mathcal{A}_0| - 2$.

By Lemma 2.5 and Lemma 2.7, we have $|\phi_H(h_1^\wedge(\mathcal{A}\setminus\mathcal{A}_0))| = |\sum_{h_1}(\bar{T})| \geq \min\{p, |supp(\bar{T})| + 1\} = |supp(\bar{T})| + 1 = r$, and so there exists an r-subset $\{c_0, c_1, \ldots, c_{r-1}\} \subseteq h_1^\wedge(\mathcal{A} \setminus \mathcal{A}_0)$ such that $\phi_H(c_0), \phi_H(c_1), \ldots, \phi_H(c_{r-1})$ are pairwise distinct.

Let $W_j = h_0^\wedge \mathcal{A}_0 + c_j$ for $j = 0, 1, \ldots, r-1$. Note that $W_0, W_1, \ldots, W_{r-1}$ are pairwise disjoint subsets of $h^\wedge \mathcal{A}$. By the induction hypothesis, we have $|W_j| = |h_0^\wedge \mathcal{A}_0| \geq |\mathcal{A}_0|$ for $j = 0, 1, \ldots, r-1$. Therefore, we conclude that $|h^\wedge \mathcal{A}| \geq |\bigcup_{j=0}^{r-1} W_j| = \sum_{j=0}^{r-1} |W_j| \geq r|\mathcal{A}_0| \geq \sum_{j=0}^{r-1} |\mathcal{A}_{i_j}| = |\mathcal{A}|$, and moreover, $|h^\wedge \mathcal{A}| = |\mathcal{A}|$ holds if, and only if, $h^\wedge \mathcal{A} = \bigcup_{j=0}^{r-1} W_j$, $|W_j| = |\mathcal{A}_{i_j}| = |\mathcal{A}_0|$ for $j = 0, 1, \ldots, r-1$. (2.4)

Step 2. Suppose $|h^\wedge \mathcal{A}| = |\mathcal{A}|$. We shall prove $\mathcal{A} \leq G$.

If $|supp(\bar{S})| = 1$, by the induction hypothesis, we have $\mathcal{A} \leq G$. Recall that if $|supp(\bar{S})| = 2$, then $|h^\wedge \mathcal{A}| > |\mathcal{A}|$. So it suffices to consider the case when $|supp(\bar{S})| = r \geq 3$.

From Equations (2.1), (2.2), (2.3) and (2.4), we conclude that $\mathcal{A} = \bigcup_{j=0}^{r-1} \mathcal{A}_{i_j}$, where $i_0 = 0$, $\{i_1, \ldots, i_{r-1}\} \subseteq [1, p-1]$, and $|\mathcal{A}_{i_j}| = |\mathcal{A}_0|$ for $j = 1, \ldots, r-1$; and that $h^\wedge \mathcal{A} = \bigcup_{j=0}^{r-1} W_j$, where $|W_0| = |W_1| = \cdots = |W_{r-1}| = |\mathcal{A}_0|$, and there exist r elements $c_0, c_1, \ldots, c_{r-1}$ of $h^\wedge \mathcal{A}$ such that $\phi_H(W_j) = \phi_H(c_j)$ are pairwise distinct for $j = 0, 1, \ldots, r-1$.

Claim. There exists a subgroup K of H such that $\mathcal{A}_{i_j} = K + b_j$, where $b_j \in \mathcal{A}_{i_j}$, for $j = 0, 1, \ldots, r-1$.

Proof. Choose an arbitrary integer j in $\{1, \ldots, r-1\}$. Let $h_0 = \min\{h-1, |\mathcal{A}_0| - 1\}$, and let $h_1 = h - h_0 - 1$. Then $1 \leq h_0 \leq |\mathcal{A}_0| - 1$, and $0 \leq h_1 \leq |\mathcal{A}| - 2|\mathcal{A}_0| = |\mathcal{A} \setminus (\mathcal{A}_0 \bigcup \mathcal{A}_{i_j})|$ since $|\mathcal{A}| \geq 3|\mathcal{A}_0|$ and $h \leq |\mathcal{A}|/2$. Fix a subset B of $\mathcal{A} \setminus (\mathcal{A}_0 \bigcup \mathcal{A}_{i_j})$ with $|B| = h_1$. Then $h_0^\wedge \mathcal{A}_{i_j} + \mathcal{A}_0 + \sigma(B) \subseteq h^\wedge \mathcal{A} \bigcap H + g_x$ for some $g_x \in G$, and so $h_0^\wedge \mathcal{A}_{i_j} + \mathcal{A}_0 + \sigma(B) \subseteq W_t$ for some $t \in [0, r-1]$. It follows that $|h_0^\wedge \mathcal{A}_{i_j} + \mathcal{A}_0| \leq |W_t| = |\mathcal{A}_0|$. By the induction hypothesis, we have $|h_0^\wedge \mathcal{A}_{i_j}| \geq |\mathcal{A}_{i_j}|$. It follows from Lemma 2.4 that there exists a subgroup K of G, such that $\mathcal{A}_0 = K$. Since $\mathcal{A}_0 \subseteq H$, then K is a subgroup of H. Similarly, by considering $h_0^\wedge \mathcal{A}_0 + \mathcal{A}_{i_j} + \sigma(B)$, since $h_0^\wedge \mathcal{A}_0 = K$, we obtain $\mathcal{A}_{i_j} = K + b_j$, where $b_j \in \mathcal{A}_{i_j}$. This proves the claim. □

Let φ_K be the canonical epimorphism of G onto G/K. Let $|K| = k$. By the claim above, we see that $\mathcal{A} = \bigcup_{j=0}^{r-1} \mathcal{A}_{i_j} = \bigcup_{j=0}^{r-1} (K + b_j)$. Note that by the definitions of $W_0, W_1, \ldots, W_{r-1}$, then $h^\wedge \mathcal{A} = \bigcup_{j=0}^{r-1} W_j = \bigcup_{j=0}^{r-1} (K + c_j)$, where $\varphi_K(c_0)$, $\varphi_K(c_1), \ldots, \varphi_K(c_{r-1})$ are pairwise distinct, since $\phi_H(c_0), \phi_H(c_1), \ldots, \phi_H(c_{r-1})$ are pairwise distinct and $K \leq H$. Hence, $|\varphi_K(h^\wedge \mathcal{A})| = r$.

Let $U = \prod_{i=0}^{l-1} \varphi_K(a_i)$. It follows that $U = \bar{0}^k \bar{b}_1^k \cdot \ldots \cdot \bar{b}_{r-1}^k$. If $r = 3$, we write $U = U_0 \cdot U_1$ where $U_0 = \bar{0}^{k-2}\bar{b}_1^{k-2}\bar{b}_2^{k-2}$ and $U_1 = \bar{0}^2\bar{b}_1^2\bar{b}_2^2$. Let $h_0 = h - 2$. Since $k \geq 3$, we have $h_0 = h - 2 \leq |U|/2 - 2 \leq |U| - 6 = |U_0|$. Fix a subsequence V of U_0 with $|V| = h_0$. We have $\sum_2(U_1) + \sigma(V) \subseteq \sum_h(U)$ and $\sum_2(U_1) = supp(U) + supp(U)$. It follows from Lemma 2.5 that $|\varphi_K(h^\wedge\mathcal{A})| = |\sum_h(U)| \geq |\sum_2(U_1)| = |supp(U) + supp(U)| \geq |supp(U)| = r$, and so $|supp(U) + supp(U)| = |supp(U)|$. It follows from Lemma 2.4 that $supp(U) \leq G/K$.

If $r \geq 4$, we write $U = U_0 \cdot U_1$ where $U_0 = \bar{0}^{k-1}\bar{b}_1^{k-1} \cdot \ldots \cdot \bar{b}_{r-1}^{k-1}$ and $U_1 = supp(U) = \{\bar{0}, \bar{b}_1, \ldots, \bar{b}_{r-1}\}$. Let $h_0 = h - 2$. Then $h_0 \leq |U|/2 - 2 < |U_0|$. Fix a subsequence V of U_0 with $|V| = h_0$. We have $2^\wedge U_1 + \sigma(V) \subseteq \sum_h(U)$. It follows from Lemma 2.5 and the induction hypothesis that $|\varphi_K(h^\wedge\mathcal{A})| = |\sum_h(U)| \geq |2^\wedge U_1| \geq |U_1| = r$, and so $|2^\wedge U_1| = |U_1|$, which implies $supp(U) = U_1 \leq G/K$.

Therefore, by the group homomorphism theorem, we have $\mathcal{A} \leq G$. $\square$

Acknowledgement The author is indebted to Professor W.D. Gao and Professor Y.O. Hamidoune for their helpful suggestions.

References

[1] Noga Alon, Melvyn B. Nathanson and Imre Ruzsa, Adding distinct congruence classes modulo a prime, Am. Math. Monthly, 102 (1995) 250-255.

[2] Noga Alon, Melvyn B. Nathanson and Imre Ruzsa, The polynomial method and restricted sums of congruence classes, Journal of Number Theory, 56 (1996) 404-417.

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

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

[5] L. Gallardo, G. Grekos, L. Habsieger, F. Hennecart, B. Landreau and A. Plagne, Restricted addition in $\mathbb{Z}/n\mathbb{Z}$ and an application to the Erdős-Ginzburg-Ziv problem, J. London Math. Soc (2) 65 (2002) 513-523.

[6] Y.O. Hamidoune, A.S. Lladó and O. Serra, On restricted sums, Combinatorics. Probalility and Computing, 9 (2000) 513-518.

[7] Melvyn B. Nathanson, Additive number theory: Inverse problems and the geometry of sumsets, Vol. 165 of Graduate Texts in Mathematics, Springer, New York.