

Restricted sumsets in finite nilpotent groups

by

SHANSHAN DU and HAO PAN (Nanjing)

1. Introduction. Suppose that p is a prime number and A, B are two non-empty subsets of $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$. The classical Cauchy–Davenport theorem (see [17, Theorem 2.2]) says that the sumset

$$A + B = \{a + b : a \in A, b \in B\}$$

contains at least

$$\min\{p, |A| + |B| - 1\}$$

elements. In the 1960's, Erdős and Heilbronn [6, 7, 8] considered the cardinality of the restricted sumset

$$A \dot{+} B = \{a + b : a \in A, b \in B, a \neq b\}.$$

They conjectured that for non-empty $A \subseteq \mathbb{Z}_p$,

$$|A \dot{+} A| \geq \min\{p, 2|A| - 3\}.$$

This conjecture was confirmed by Dias da Silva and Hamidoune [5], with the help of exterior algebra. In 1996, using the polynomial method, Alon, Nathanson and Ruzsa [2, 3] gave a simple proof of the Erdős–Heilbronn conjecture. In fact, they obtained a stronger result:

$$(1.1) \quad |A \dot{+} B| \geq \min\{p, |A| + |B| - 2\}$$

provided $|A| \neq |B|$. Obviously, arbitrarily choosing $B \subseteq A$ with $|B| = |A| - 1$, we have

$$|A \dot{+} A| \geq |A \dot{+} B| \geq \min\{p, |A| + |B| - 2\} = \min\{p, 2|A| - 3\}.$$

Recently, Károlyi [16] considered the exceptional case that $|A| = |B|$ and $A \neq B$. He proved that (1.1) always holds as long as $A \neq B$.

On the other hand, Olson [18] proved that for any finite subsets A, B of a group G , there exists a non-empty subset $C \subseteq A + B$ and a subgroup H

2010 *Mathematics Subject Classification*: Primary 11P70; Secondary 11B13.

Key words and phrases: restricted sumsets.

Received 7 May 2013; revised 18 August 2016.

Published online 23 March 2017.

of G with $H + C = C$ or $C + H = C$ such that

$$|C| \geq |A| + |B| - |H|.$$

Here for convenience, we still use “+”, rather than “ \times ”, to represent the binary operation over G . It easily follows from Olson’s result that

$$(1.2) \quad |A + B| \geq \min\{p(G), |A| + |B| - 1\},$$

where $p(G)$ denotes the smallest prime factor of $|G|$. This is an extension of the Cauchy–Davenport theorem to finite groups. Károlyi [14] gave a new proof of (1.2) and obtained the related inverse result, under the condition that $|A + B| = |A| + |B| - 1 < p(G)$. One key to Károlyi’s proof is a well-known result of Feit and Thompson on finite groups of odd order.

In [12, 13], Károlyi established the following generalization of the Erdős–Heilbronn problem for finite abelian groups:

$$(1.3) \quad |A \dot{+} A| \geq \min\{p(G), 2|A| - 3\},$$

where A is a non-empty subset of the finite abelian group G . Subsequently, motivated by the work of Károlyi [14], Balister and Wheeler [4] removed the restriction that G is abelian. In fact, they showed that

$$(1.4) \quad |A \dot{+} B| \geq \min\{p(G), |A| + |B| - 3\}$$

for any non-empty subsets A, B of a finite group G .

In this paper, we shall consider the extension of (1.1) to finite nilpotent groups.

THEOREM 1.1. *Suppose that G is a finite nilpotent group. Let A, B be non-empty subsets of G . If $A \neq B$, then*

$$(1.5) \quad |A \dot{+} B| \geq \min\{p(G), |A| + |B| - 2\}.$$

We mention that (1.5) may fail for non-nilpotent groups: an example has been given in [11, Example 4.11].

As we shall see later, in order to complete the proof of Theorem 1.1, we need to discuss the structure of A when $|A \dot{+} A| = 2|A| - 3$. For $A \subseteq \mathbb{Z}_p$ with $|A| < (p + 1)/2$, if $|A + A| = 2|A| - 1$, Vosper’s inverse theorem [20] implies that A must be an arithmetic progression. Károlyi [15] proved that if A is a subset of the finite abelian group G satisfying $5 \leq |A| < (p(G) + 3)/2$, then $|A \dot{+} A| = 2|A| - 3$ if and only if A is an arithmetic progression.

We shall prove that

THEOREM 1.2. *Let G be a finite group and let A be a non-empty subset of G with $|A| < (p(G) + 3)/2$. Suppose that*

$$|A \dot{+} A| = 2|A| - 3.$$

Then the elements of A commute, i.e., $a_1 + a_2 = a_2 + a_1$ for any $a_1, a_2 \in A$.

In view of Theorem 1.2, we know that if $|A \dot{+} A| = 2|A| - 3$, then the subgroup generated by A is actually abelian. Thus

COROLLARY 1.1. *Under the assumptions of Theorem 1.2, if $|A| = n \geq 5$, then $A = \{a, a + d, a + 2d, \dots, a + (n - 1)d\}$ where $a, d \in G$ and $a + d = d + a$.*

For further results on inverse Erdős–Heilbronn problem in finite groups, the reader may refer to [10, 11].

2. Proof of Theorem 1.1. In this section, we shall give the most part of the proof of Theorem 1.1, except for one subcase which requires Theorem 1.2.

LEMMA 2.1. *Suppose that G is a finite group. Let $A = \{a_1, \dots, a_n\}$ and $B = \{b_1, \dots, b_m\}$ be non-empty subsets of G with $n + m - 1 \leq p(G)$. Then there exist $1 \leq i_2, \dots, i_n \leq m$ such that*

$$a_1 + b_1, \dots, a_1 + b_m, a_2 + b_{i_2}, \dots, a_n + b_{i_n}$$

are all distinct.

Proof. For $2 \leq j \leq n$, let

$$X_j = (\{a_1, a_j\} + B) \setminus (a_1 + B).$$

In view of (1.2), for any non-empty $J \subseteq \{2, \dots, n\}$,

$$\left| \bigcup_{j \in J} X_j \right| = |((\{a_1\} \cup \{a_j\}_{j \in J}) + B) \setminus (a_1 + B)| \geq |J|.$$

Applying the Hall marriage theorem (see [19, Theorem 5.1]), we may choose distinct $c_2 \in X_2, c_3 \in X_3, \dots, c_n \in X_n$. Letting $b_{i_j} = -a_j + c_j$, we are done. ■

Now suppose that the order of G is not prime. Let $p = p(G)$. Without loss of generality, assume that $|A| + |B| - 2 \leq p$. In fact, if $|A| + |B| - 2 > p$, then we may choose non-empty $A' \subseteq A$ and $B' \subseteq B$ such that $|A'| + |B'| - 2 = p$. Clearly $A' \dot{+} B' \subseteq A \dot{+} B$. If $p = 2$, then it is easy to check directly that $|A \dot{+} B| \geq |A| + |B| - 2$ provided $A \neq B$ and $|A| + |B| \leq 4$. So we only need to consider those odd p .

We will prove Theorem 1.1 by induction on $|G|$. There is nothing to do when G is a group of prime order. So we may assume $|G|$ is composite and Theorem 1.1 holds for any nilpotent group H with $|H|$ a proper divisor of $|G|$. If G is abelian, let H be a subgroup of G such that $[G : H] = p$. Otherwise, let H be the center of G . Since G is nilpotent, G/H is also a non-trivial nilpotent group. Obviously, $p(H), p(G/H) \geq p(G)$. By the induction hypothesis, Theorem 1.1 holds for both H and G/H .

For convenience, let \bar{a} denote the coset $a + H$. Suppose that

$$A = \bigcup_{j=1}^n (a_j + S_j), \quad B = \bigcup_{j=1}^m (b_j + T_j),$$

where S_j, T_j are non-empty subsets of H and $\bar{a}_i \neq \bar{a}_j, \bar{b}_i \neq \bar{b}_j$ for any $i \neq j$. Without loss of generality, we may assume that $\bar{a}_i = \bar{b}_j$ implies $a_i = b_j$. Since either G is abelian or H is the center of G , we have $S + b = b + S$ for any $b \in G$ and $S \subseteq H$. Therefore

$$A \dot{+} B = \left(\bigcup_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m \\ a_i = b_j}} (a_i + b_j + (S_i \dot{+} T_j)) \right) \cup \left(\bigcup_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m \\ a_i \neq b_j}} (a_i + b_j + (S_i + T_j)) \right).$$

Let $\bar{A} = \{\bar{a}_1, \dots, \bar{a}_n\}$ and $\bar{B} = \{\bar{b}_1, \dots, \bar{b}_m\}$. It trivially follows that

$$(2.1) \quad |A \dot{+} B| \geq |\bar{A} \dot{+} \bar{B}| - 1 + \max_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m \\ a_i \neq b_j}} |S_i + T_j|.$$

For $S \subseteq H$ and $a \in G$, clearly

$$-(a + S) = (-S) + (-a) = (-a) + (-S).$$

So we can “exchange” A and B in the sense that

$$|A \dot{+} B| = |-(A \dot{+} B)| = |(-B) \dot{+} (-A)|.$$

That is, we may assume $m \geq n$. Furthermore, when $m = n$, assume that

$$\max\{|S_1|, \dots, |S_n|\} \geq \max\{|T_1|, \dots, |T_m|\}.$$

If $n + m - 1 > p$, then $|\bar{A}| + |\bar{B}| = |A| + |B| = p + 2$ by recalling $|A| + |B| - 2 \leq p$. Since p is odd, we must have $\bar{A} \neq \bar{B}$. In view of (2.1), by the induction hypothesis we get

$$|A \dot{+} B| \geq |\bar{A} \dot{+} \bar{B}| \geq |\bar{A}| + |\bar{B}| - 2.$$

Below we always assume that $n + m - 1 \leq p$. Suppose that $|S_1| \geq \dots \geq |S_n|$. We consider several cases:

(i) $m > n$ and $|S_1| \geq 2$, or $m = n$ and $|S_1| \geq 3$. Applying Lemma 2.1 to G/H , we know there exist $1 \leq i_2, \dots, i_n \leq m$ such that

$$\bar{a}_1 + \bar{b}_1, \dots, \bar{a}_1 + \bar{b}_m, \bar{a}_2 + \bar{b}_{i_2}, \dots, \bar{a}_n + \bar{b}_{i_n}$$

are distinct elements of $\bar{A} + \bar{B}$. Without loss of generality, assume that $a_1 \notin \{b_2, \dots, b_m\}$. Then

$$\begin{aligned}
 (2.2) \quad |A \dot{+} B| &\geq \left| \bigcup_{j=1}^m ((a_1 + S_1) \dot{+} (b_j + T_j)) \cup \bigcup_{j=2}^n ((a_j + S_j) \dot{+} (b_{i_j} + T_{i_j})) \right| \\
 &\geq |a_1 + b_1 + (S_1 \dot{+} T_1)| \\
 &\quad + \sum_{j=2}^m |a_1 + b_j + (S_1 + T_j)| + \sum_{j=2}^n |a_j + b_{i_j} + (S_j \dot{+} T_{i_j})| \\
 &\geq |S_1| + |T_1| - 3 + \sum_{j=2}^m (|S_1| + |T_j| - 1) + \sum_{j=2}^n |S_j \dot{+} T_{i_j}| \\
 &= |B| - 2 + m(|S_1| - 1) + \sum_{j=2}^n |S_j \dot{+} T_{i_j}|.
 \end{aligned}$$

It is easy to see that $|S \dot{+} T| \geq |S| - 1$. Hence for $2 \leq j \leq n$,

$$|S_1| - 1 + |S_j \dot{+} T_{i_j}| \geq |S_1| + |S_j| - 2 \geq |S_j|.$$

First if $m > n$, then

$$\begin{aligned}
 |A \dot{+} B| &\geq |B| - 3 + (m - n) + |S_1| + \sum_{j=2}^n (|S_1| - 1 + |S_j \dot{+} T_{i_j}|) \\
 &\geq |A| + |B| - 2.
 \end{aligned}$$

Next suppose $m = n = 1$. Then either $S_1 \neq T_1$ or $a_1 \neq b_1$. If $S_1 \neq T_1$, then

$$|A \dot{+} B| = |S_1 \dot{+} T_1| \geq |S_1| + |T_1| - 2 = |A| + |B| - 2;$$

and if $a_1 \neq b_1$, then

$$|A \dot{+} B| = |S_1 + T_1| \geq \min\{p, |A| + |B| - 1\} \geq |A| + |B| - 2.$$

Suppose finally that $m = n \geq 2$. Then since $|S_1| \geq 3$, we have

$$|S_1| - 1 + |S_j \dot{+} T_{i_j}| \geq |S_j| + 1.$$

In view of (2.2),

$$|A \dot{+} B| \geq |B| - 3 + |S_1| + \sum_{j=2}^n (|S_j| + 1) \geq |A| + |B| - 2.$$

(ii) $m > n$ and $|S_1| = 1$. Clearly now $\bar{A} \neq \bar{B}$. Hence $|\bar{A} \dot{+} \bar{B}| \geq n + m - 2$. We need to consider three subcases:

(1) Suppose that $\bar{A} \not\subseteq \bar{B}$. Without loss of generality, we may assume that $\bar{a}_1 \notin \bar{B}$. Then for some $2 \leq i_2, \dots, i_{n-1} \leq n$ and $1 \leq k_2, \dots, k_{n-1} \leq m$,

$$\bar{a}_1 + \bar{b}_1, \bar{a}_1 + \bar{b}_2, \dots, \bar{a}_1 + \bar{b}_m, \bar{a}_{i_2} + \bar{b}_{k_2}, \dots, \bar{a}_{i_{n-1}} + \bar{b}_{k_{n-1}}$$

are distinct elements of $\bar{A} \dot{+} \bar{B}$, where $\bar{a}_{i_j} \neq \bar{b}_{k_j}$ for $2 \leq j \leq n-1$. Thus

$$|A \dot{+} B| \geq \sum_{j=1}^m |S_1 + T_j| + \sum_{j=2}^{n-1} |S_{i_j} + T_{k_j}| \geq \sum_{j=1}^m |T_j| + n - 2 = |A| + |B| - 2.$$

(2) Suppose that $\bar{A} \subseteq \bar{B}$ and $\bar{a}_j + \bar{a}_j \in \bar{A} \dot{+} \bar{B}$ for all $1 \leq j \leq n$. Without loss of generality, assume that $a_1 = b_1$. Clearly now $\bar{A} \dot{+} \bar{B} = \bar{A} + \bar{B}$, i.e., $|\bar{A} \dot{+} \bar{B}| \geq n + m - 1$. Hence

$$\bar{a}_1 + \bar{b}_1, \bar{a}_1 + \bar{b}_2, \dots, \bar{a}_1 + \bar{b}_m, \bar{a}_{i_2} + \bar{b}_{k_2}, \dots, \bar{a}_{i_n} + \bar{b}_{k_n}$$

are distinct elements of $\bar{A} \dot{+} \bar{B}$, where $\bar{a}_{i_j} \neq \bar{b}_{k_j}$. It follows that

$$\begin{aligned} |A \dot{+} B| &\geq |S_1 \dot{+} T_1| + \sum_{j=2}^m |S_1 + T_j| + \sum_{j=2}^n |S_{i_j} + T_{k_j}| \\ &\geq (|T_1| - 1) + \sum_{j=2}^m |T_j| + n - 1 = |A| + |B| - 2. \end{aligned}$$

(3) Suppose that $\bar{A} \subseteq \bar{B}$ but $\bar{a}_{j_0} + \bar{a}_{j_0} \notin \bar{A} \dot{+} \bar{B}$ for some $1 \leq j_0 \leq n$. Without loss of generality, assume that $\bar{a}_1 + \bar{a}_1 \notin \bar{A} \dot{+} \bar{B}$ and $a_1 = b_1$. Since $|\bar{A} \dot{+} \bar{B}| \geq n + m - 2$, we may assume that

$$\bar{a}_1 + \bar{b}_2, \dots, \bar{a}_1 + \bar{b}_m, \bar{a}_{i_2} + \bar{b}_{k_2}, \dots, \bar{a}_{i_n} + \bar{b}_{k_n}$$

are distinct elements of $\bar{A} \dot{+} \bar{B}$. We still have

$$|A \dot{+} B| \geq |S_1 \dot{+} T_1| + \sum_{j=2}^m |S_1 + T_j| + \sum_{j=2}^n |S_{i_j} + T_{k_j}| \geq |A| + |B| - 2.$$

(iii) $m = n$ and $|S_1| = 2$. The case $m = n = 1$ is trivial. Suppose $m = n \geq 2$. If $\bar{a}_1 \notin \bar{B}$, then assuming that $\bar{a}_1 + \bar{b}_1, \dots, \bar{a}_1 + \bar{b}_m, \bar{a}_{i_2} + \bar{b}_{k_2}, \dots, \bar{a}_{i_{n-1}} + \bar{b}_{k_{n-1}}$ are distinct elements of $\bar{A} \dot{+} \bar{B}$, we get

$$\begin{aligned} |A \dot{+} B| &\geq \sum_{j=1}^m |S_1 + T_j| + \sum_{j=2}^{n-1} |S_{i_j} + T_{k_j}| \geq \sum_{j=1}^m (|S_1| + |T_j| - 1) + (n - 2) \\ &\geq |A| + |B| - 2. \end{aligned}$$

Suppose that $\bar{a}_1 \in \bar{B}$ and $a_1 = b_1$. In view of Lemma 2.1, we may assume that

$$\bar{a}_1 + \bar{b}_1, \bar{a}_1 + \bar{b}_2, \dots, \bar{a}_1 + \bar{b}_n, \bar{a}_2 + \bar{b}_{i_2}, \dots, \bar{a}_n + \bar{b}_{i_n}$$

are distinct elements of $\bar{A} + \bar{B}$. Suppose that $S_1 \neq T_1$. Then

$$\begin{aligned} |A \dot{+} B| &\geq |S_1 \dot{+} T_1| + \sum_{j=2}^n |S_1 + T_j| + \sum_{j=2}^n |S_j \dot{+} T_{i_j}| \\ &\geq |S_1| + |T_1| - 2 + \sum_{j=2}^n (|S_1| + |T_j| - 1) + \sum_{j=2}^n (|S_j| - 1) \\ &= |A| + |B| + (n-1)|S_1| - 2n = |A| + |B| - 2. \end{aligned}$$

Now suppose that $S_1 = T_1$. Since $A \neq B$, there exists some $2 \leq j_0 \leq n$ such that either $a_{j_0} \neq b_{i_{j_0}}$ or $S_{j_0} \neq T_{i_{j_0}}$.

(1) Suppose that $a_{j_0} \neq b_{i_{j_0}}$ for some $2 \leq j_0 \leq n$. Then

$$\begin{aligned} (2.3) \quad |A \dot{+} B| &\geq |S_1 \dot{+} T_1| + \sum_{j=2}^n |S_1 + T_j| + |S_{j_0} + T_{i_{j_0}}| + \sum_{\substack{2 \leq j \leq n \\ j \neq j_0}} |S_j \dot{+} T_{i_j}| \\ &\geq n|S_1| + |B| - (n+2) + |S_{j_0}| + |T_{i_{j_0}}| - 1 + \sum_{\substack{2 \leq j \leq n \\ j \neq j_0}} (|S_j| - 1) \\ &\geq |A| + |B| - 2. \end{aligned}$$

(2) Suppose that $a_j = b_{i_j}$ for all $2 \leq j \leq n$ and $S_{j_0} \neq T_{i_{j_0}}$ for some $2 \leq j_0 \leq n$. If $|S_{j_0}| = 2$, then we may exchange a_1 and a_{j_0} . Thus the desired result follows from our discussion of the case $S_1 \neq T_1$. Assume that $|S_{j_0}| = 1$. Since $S_{j_0} \neq T_{i_{j_0}}$, $S_{j_0} \dot{+} T_{i_{j_0}}$ is non-empty. Then

$$\begin{aligned} |A \dot{+} B| &\geq |S_1 \dot{+} T_1| + \sum_{j=2}^n |S_1 + T_j| + |S_{j_0} \dot{+} T_{i_{j_0}}| + \sum_{\substack{2 \leq j \leq n \\ j \neq j_0}} |S_j \dot{+} T_{i_j}| \\ &\geq n|S_1| + |B| - (n+2) + |S_{j_0}| + \sum_{\substack{2 \leq j \leq n \\ j \neq j_0}} (|S_j| - 1) \geq |A| + |B| - 2. \end{aligned}$$

(iv) $m = n$ and $|S_1| = 1$. Recalling (2.1), we have

$$|A \dot{+} B| \geq |\bar{A} \dot{+} \bar{B}| \geq |A| + |B| - 2$$

provided that $\bar{A} \neq \bar{B}$ or $\bar{A} \dot{+} \bar{B} = \bar{A} + \bar{B}$. So we may assume that $a_j = b_j$ for $1 \leq j \leq n$ and $\bar{a}_1 + \bar{a}_1 \notin \bar{A} \dot{+} \bar{B}$. If $S_1 \neq T_1$, then in view of (1.4),

$$(2.4) \quad |A \dot{+} B| \geq |S_1 \dot{+} T_1| + |\bar{A} \dot{+} \bar{B}| \geq 1 + (|\bar{A}| + |\bar{B}| - 3) = |A| + |B| - 2.$$

However, the final case $S_1 = T_1$ is most annoying. In fact, its proof needs Theorem 1.2 and Corollary 1.1. So we shall first prove Theorem 1.2 for nilpotent groups in Section 3, before completing the proof of Theorem 1.1.

3. Proof of Theorem 1.2 for finite nilpotent groups. In this section, we shall only prove Theorem 1.2 for finite nilpotent groups, which is sufficient to complete the proof of Theorem 1.1.

Let G be a finite non-abelian nilpotent group and let H denote its (non-trivial) center. Assume that Theorem 1.2 holds for G/H . Let A be a non-empty subset of G satisfying

$$|A \dot{+} A| = 2|A| - 3.$$

We shall prove that the elements of A commute. Assume that

$$A = \bigcup_{i=1}^n (a_i + S_i),$$

where $\emptyset \neq S_i \subseteq H$ and $\bar{a}_i \neq \bar{a}_j$ for $i \neq j$. There is nothing to do when $n = 1$. Below we assume that $n \geq 2$. Furthermore, if $p(G) = 2$ and $A = \{a_1, a_2\}$, then $|A \dot{+} A| = 1$ if and only if $a_1 + a_2 = a_2 + a_1$. So we may assume that $p(G)$ is odd.

Suppose that $|S_1| \geq \dots \geq |S_n|$. By (2.2), it is impossible that $|S_1| \geq 3$. Assume that $|S_1| = 2$ and

$$\bar{a}_1 + \bar{a}_1, \bar{a}_1 + \bar{a}_2, \dots, \bar{a}_1 + \bar{a}_n, \bar{a}_2 + \bar{a}_2, \dots, \bar{a}_n + \bar{a}_n$$

are distinct elements of $\bar{A} + \bar{A}$. If $a_{j_0} \neq a_{i_{j_0}}$ for some $2 \leq j_0 \leq n$, then in view of (2.3),

$$\begin{aligned} |A \dot{+} A| &\geq |S_1 \dot{+} S_1| + \sum_{j=2}^n |S_1 + S_j| + |S_{j_0} + S_{i_{j_0}}| + \sum_{\substack{2 \leq j \leq n \\ j \neq j_0}} |S_j \dot{+} S_j| \\ &\geq 2|A| - 2. \end{aligned}$$

So we must have $j = i_j$ for all $2 \leq j \leq n$. Now the set

$$\begin{aligned} (3.1) \quad &(a_1 + a_1 + (S_1 \dot{+} S_1)) \cup \bigcup_{j=2}^n (a_1 + a_j + (S_1 + S_j)) \\ &\cup \bigcup_{j=2}^n (a_j + a_j + (S_j \dot{+} S_j)) \end{aligned}$$

contains at least

$$\begin{aligned} &|S_1 \dot{+} S_1| + \sum_{j=2}^n |S_1 + S_j| + \sum_{j=2}^n |S_j \dot{+} S_j| \\ &\geq \sum_{j=1}^n (|S_1| + |S_j| - 1) - 2 + \sum_{j=2}^n (|S_j| - 1) \geq 2|A| - 3 \end{aligned}$$

elements. That is, the set (3.1) should coincide with $A \dot{+} A$. If there exists an element of $A \dot{+} A$ not lying in (3.1), then we get a contradiction.

Assume that there exist distinct $1 \leq j_1, j_2 \leq n$ satisfying

$$\bar{a}_{j_1} + \bar{a}_{j_2} \notin \{\bar{a}_1 + \bar{a}_1, \bar{a}_1 + \bar{a}_2, \dots, \bar{a}_1 + \bar{a}_n, \bar{a}_2 + \bar{a}_2, \dots, \bar{a}_n + \bar{a}_n\}.$$

Then $a_{j_1} + a_{j_2} + (S_{j_1} + S_{j_2})$ is a non-empty subset of $A \dot{+} A$. But it is evidently not included in (3.1). Therefore we may assume that

$$\bar{A} \dot{+} \bar{A} \subseteq \{\bar{a}_1 + \bar{a}_1, \bar{a}_1 + \bar{a}_2, \dots, \bar{a}_1 + \bar{a}_n, \bar{a}_2 + \bar{a}_2, \dots, \bar{a}_n + \bar{a}_n\}.$$

Let

$$J_1 = \{1 \leq j \leq n : \bar{a}_j + \bar{a}_j \in (\bar{A} \dot{+} \bar{A}) \setminus \{\bar{a}_1 + \bar{a}_2, \dots, \bar{a}_1 + \bar{a}_n\}\},$$

and let $J_2 = \{2, \dots, n\} \setminus J_1$. For $n \geq 4$, we need to find distinct $2 \leq j_1, j_2 \leq n$ such that $a_{j_1} + a_{j_2} + (S_{j_1} + S_{j_2})$ is not contained in (3.1). There are two cases:

(a) Suppose there exists $j_0 \in J_1$ satisfying $|S_{j_0}| = 1$. Since $\bar{a}_{j_0} + \bar{a}_{j_0} \in \bar{A} \dot{+} \bar{A}$, we can find distinct $2 \leq j_1, j_2 \leq n$ such that $\bar{a}_{j_1} + \bar{a}_{j_2} = \bar{a}_{j_0} + \bar{a}_{j_0}$. But now $S_{j_0} \dot{+} S_{j_0} = \emptyset$ and $S_{j_1} + S_{j_2} \neq \emptyset$. Hence $a_{j_1} + a_{j_2} + (S_{j_1} + S_{j_2}) \subseteq A \dot{+} A$ is not included in (3.1).

(b) Assume that $|S_j| = 2$ for each $j \in J_1$. Clearly $|J_1| \geq |\bar{A} \dot{+} \bar{A}| - (n - 1)$. Note that for any $j_0 \in J_1$, there exist distinct $2 \leq j_1, j_2 \leq n$ such that $\bar{a}_{j_1} + \bar{a}_{j_2} = \bar{a}_{j_0} + \bar{a}_{j_0}$. If $|\bar{A} \dot{+} \bar{A}| > 2n - 3$, then $|J_1| \geq n - 1$ and $|J_2| \leq 1$. It is impossible that both j_1 and j_2 belong to J_2 . If $|\bar{A} \dot{+} \bar{A}| = 2n - 3$, then by the induction hypothesis, we get $|J_1| = n - 2$, $|J_2| \leq 2$ and the elements of \bar{A} commute. Since the elements of \bar{A} commute, for distinct $j_1, j_2 \in J_2$, we have $\bar{a}_{j_1} + \bar{a}_{j_2} = \bar{a}_{j_2} + \bar{a}_{j_1}$. So there exists at most one $j_0 \in J_1$ such that $\bar{a}_{j_1} + \bar{a}_{j_2} = \bar{a}_{j_0} + \bar{a}_{j_0}$ and $j_1, j_2 \in J_2$.

All in all, when $n \geq 4$, one can find $j_0 \in J_1$ and $2 \leq j_1, j_2 \leq n$ such that $\bar{a}_{j_1} + \bar{a}_{j_2} = \bar{a}_{j_0} + \bar{a}_{j_0}$ and at least one of j_1, j_2 does not lie in J_2 . Since $|S_{j_0}| = 2$ and H is abelian, we have $|S_{j_0} \dot{+} S_{j_0}| = 1$. But now $\max\{|S_{j_1}|, |S_{j_2}|\} = 2$ and $|S_{j_1} + S_{j_2}| \geq 2$. So $a_{j_1} + a_{j_2} + (S_{j_1} + S_{j_2})$ is not a subset of (3.1). The case (b) is concluded.

Thus in view of (a) and (b), for $n \geq 4$, it is also impossible that $|S_1| = 2$.

Now consider the case $n = 3$. Suppose that $|\bar{A} \dot{+} \bar{A}| \geq 4$. Then there exist distinct

$$\bar{a}_1 + \bar{a}_2, \bar{a}_1 + \bar{a}_3, \bar{a}_{i_1} + \bar{a}_{k_1}, \bar{a}_{i_2} + \bar{a}_{k_2} \in \bar{A} \dot{+} \bar{A}$$

with $i_1 \neq k_1, i_2 \neq k_2$. Then

$$\begin{aligned} |A \dot{+} A| &\geq (|S_1| + |S_2| - 1) + (|S_1| + |S_3| - 1) + 2((|S_2| + |S_3| - 1)) \\ &\geq 2|A| - 2. \end{aligned}$$

So we must have $|\bar{A} \dot{+} \bar{A}| = 3$. By the induction hypothesis, the elements of \bar{A} commute, i.e., $\bar{a}_i + \bar{a}_j = \bar{a}_j + \bar{a}_i$ for $1 \leq i \leq j \leq 3$. Hence

$$\bar{A} \dot{+} \bar{A} = \{\bar{a}_1 + \bar{a}_2, \bar{a}_1 + \bar{a}_3, \bar{a}_2 + \bar{a}_3\}.$$

Below we shall show that a_1, a_2, a_3 actually commute in G , which evidently implies that the elements of A also commute. Assume $a_2 + a_1 = a_1 + a_2 + h$ where $h \in H$. Note that

$$(a_1 + a_2 + (S_1 + S_2)) \cup (a_1 + a_3 + (S_1 + S_3)) \cup (a_2 + a_3 + (S_2 + S_3))$$

contains exactly

$$(3.2) \quad (|S_1| + |S_2| - 1) + (|S_1| + |S_3| - 1) + (|S_2| + |S_3| - 1) = 2|A| - 3$$

elements. So we must have

$$a_1 + a_2 + (S_1 + S_2) = a_2 + a_1 + (S_2 + S_1) = a_1 + a_2 + h + (S_1 + S_2),$$

i.e., $h + (S_1 + S_2) = S_1 + S_2$. Hence $S_1 + S_2$ includes a coset of the subgroup generated by h . However, since $|S_1 + S_2| < p(G)$, this is impossible unless $h = 0$. Similarly, we can get $a_1 + a_3 = a_3 + a_1$ and $a_2 + a_3 = a_3 + a_2$.

The case $n = 2$ is similar. Suppose that $\bar{a}_1 + \bar{a}_2 \neq \bar{a}_2 + \bar{a}_1$, i.e.,

$$(a_1 + a_2 + S_1 + S_2) \cap (a_2 + a_1 + S_2 + S_1) = \emptyset.$$

Then

$$|A \dot{+} A| \geq 2|S_1 + S_2| \geq 2(|S_1| + |S_2| - 1) = 2|A| - 2.$$

So the elements of \bar{A} must commute. Furthermore, note that

$$\begin{aligned} |A \dot{+} A| &\geq |S_1 + S_2| + \sum_{j=1}^2 |S_j \dot{+} S_j| \geq (|S_1| + |S_2| - 1) + \sum_{j=1}^2 (|S_j| - 1) \\ &= 2|A| - 3. \end{aligned}$$

We can deduce that $a_2 + a_1 + (S_2 + S_1) = a_1 + a_2 + (S_1 + S_2)$, i.e., $a_1 + a_2 = a_2 + a_1$. Hence the elements of A commute.

Finally, suppose that $|S_1| = \cdots = |S_n| = 1$. From $|A \dot{+} A| = 2|A| - 3$, it follows that $|\bar{A} \dot{+} \bar{A}| = 2|\bar{A}| - 3$. By the induction hypothesis, the elements of \bar{A} commute. If $a_i + a_j \neq a_j + a_i$ for some $i \neq j$, then by the above discussion, we know that

$$a_i + a_j + (S_i + S_j) \neq a_j + a_i + (S_i + S_j),$$

i.e., the coset $a_i + a_j + H$ contains two elements of $A \dot{+} A$. Hence

$$|A \dot{+} A| \geq |\bar{A} \dot{+} \bar{A}| + 1 = 2|A| - 2.$$

This leads to a contradiction. Thus a_1, \dots, a_n commute, as also do the elements of A .

The proof of Theorem 1.2 for finite nilpotent groups is concluded. ■

Let us return to the proof of the final case of Theorem 1.1. Suppose that

$$A = \bigcup_{j=1}^n (a_j + S_j), \quad B = \bigcup_{j=1}^n (a_j + T_j),$$

where $|S_1| = \cdots = |S_n| = |T_1| = \cdots = |T_n| = 1$ and $S_j = T_j$ if $\bar{a}_j + \bar{a}_j \notin$

$\bar{A} \dot{+} \bar{B}$. We need to show that $|A \dot{+} B| \geq |A| + |B| - 2$ if $S_{j_0} \neq T_{j_0}$ for some $1 \leq j_0 \leq n$.

Assume on the contrary that $|A \dot{+} B| = |A| + |B| - 3$. Then $|\bar{A} \dot{+} \bar{B}| = |\bar{A} \dot{+} \bar{A}| = 2|\bar{A}| - 3$. If $n \geq 5$, then by Corollary 1.1, \bar{A} is an arithmetic progression. Suppose that $n = 4$, i.e., $\bar{A} = \{\bar{a}_1, \bar{a}_2, \bar{a}_3, \bar{a}_4\}$. Clearly

$$\bar{A} \dot{+} \bar{A} \supseteq \{\bar{a}_1 + \bar{a}_2, \bar{a}_1 + \bar{a}_3, \bar{a}_1 + \bar{a}_4, \bar{a}_2 + \bar{a}_3, \bar{a}_2 + \bar{a}_4, \bar{a}_3 + \bar{a}_4\}.$$

Noting that $|\bar{A} \dot{+} \bar{A}| = 5$, we may assume that $\bar{a}_1 + \bar{a}_4 = \bar{a}_2 + \bar{a}_3$. Since $S_{j_0} \neq T_{j_0}$ for some $1 \leq j_0 \leq n$, in view of (2.4) we have $\bar{a}_{j_0} + \bar{a}_{j_0} \in \bar{A} \dot{+} \bar{A}$, i.e., there exist distinct $1 \leq j_1, j_2 \leq 4$ such that $\bar{a}_{j_0} + \bar{a}_{j_0} = \bar{a}_{j_1} + \bar{a}_{j_2}$. Hence $\{\bar{a}_{j_1}, \bar{a}_{j_0}, \bar{a}_{j_2}\}$ forms an arithmetic progression, as also does \bar{A} . Similarly, when $n = 3$, we also find that \bar{A} is an arithmetic progression.

Now we have proved that $\bar{A} = \{\bar{a}, \bar{a} + \bar{d}, \dots, \bar{a} + (n - 1)\bar{d}\}$. Since the elements of \bar{A} commute, $\bar{a} + \bar{d} = \bar{d} + \bar{a}$. Suppose that $d + a = a + d + h$ where $h \in H$. Without loss of generality, assume that $a_i = a + (i - 1)d$. Clearly now

$$\bar{A} \dot{+} \bar{A} = \{\bar{a} + \bar{a} + \bar{d}, \bar{a} + \bar{a} + 2\bar{d}, \dots, \bar{a} + \bar{a} + (2n - 3)\bar{d}\}.$$

Since $2n - 3 < p(G)$, we have $\bar{a} + \bar{a} \notin \bar{A} \dot{+} \bar{A}$. It follows from our assumption that $S_1 = T_1$. Suppose that $S_j = \{s_j\}$ and $T_j = \{t_j\}$ for $1 \leq j \leq n$. From $\bar{a}_i + \bar{a}_j = \bar{a}_j + \bar{a}_i$, it follows that $(a_j + s_j) + (a_1 + t_1) = (a_j + a_1) + (s_j + t_1)$ must be equal to $(a_1 + s_1) + (a_j + t_j) = (a_1 + a_j) + (s_1 + t_j)$. Therefore $(j - 1)h + (s_j + t_1) = s_1 + t_j$ for $2 \leq j \leq n$. Since $s_1 = t_1$ and $s_{j_0} \neq t_{j_0}$ for some $2 \leq j_0 \leq n$, we must have $h \neq 0$. Thus $s_j \neq t_j$ for each $2 \leq j \leq n$. On the other hand, since $|\bar{A} \dot{+} \bar{A}| = 2n - 3 \leq |\bar{A} \dot{+} \bar{A}| - 2$, there exists $2 \leq j_1 \leq n$ such that $\bar{a}_{j_1} + \bar{a}_{j_1} \notin \bar{A} \dot{+} \bar{A}$. By our assumption, we should have $s_{j_1} = t_{j_1}$, which leads to an evident contradiction. ■

4. Proof of Theorem 1.2: Generalized restricted sumsets. In the next two sections, we shall complete the proof of Theorem 1.2 for general finite groups. Let $\text{Aut } G$ denote the automorphism group of G . For $\sigma \in \text{Aut } G$ and $A, B \subseteq G$, define

$$A \overset{\sigma}{+} B = \{a + b : a \in A, b \in B, a \neq \sigma(b)\}.$$

Balister and Wheeler [4] proved

$$(4.1) \quad |A \overset{\sigma}{+} B| \geq \min\{p(G) - \delta, |A| + |B| - 3\},$$

where $\delta = 1$ or 0 according to whether the order of σ is even or not. (Notice that although our notation is a little different from [4], (4.1) is evidently equivalent to the result stated in [4].) For $A \subseteq G$, define

$$\sigma(A) = \{\sigma(a) : a \in A\}.$$

Here we give a generalization of Theorem 1.2.

THEOREM 4.1. *Suppose that G is a finite group and A is a non-empty subset of G . Let σ be an automorphism of G with odd order. If $2|A| - 3 < p(G)$ and*

$$|\sigma(A) \overset{\sigma}{+} A| = 2|A| - 3,$$

then the elements of A σ -commute, i.e.,

$$\sigma(a_1) + a_2 = \sigma(a_2) + a_1 \quad \text{for any } a_1, a_2 \in A.$$

It is easy to verify Theorem 4.1 when $p(G) = 2$. So below we always assume that $|G|$ is odd. From the Feit–Thompson theorem [9], we know that G is solvable.

For $a \in G$, define $\tau_a : G \rightarrow G$ by $\tau_a(x) = -a + x + a$ for any $x \in G$. Clearly $\tau_a \in \text{Aut } G$, and $x \neq \sigma(y)$ if and only if $\tau_a(x) \neq \tau_a\sigma(y)$. Let $\text{Inn } G = \{\tau_a : a \in G\}$ be the inner automorphism group of G . We know that $\text{Inn } G \cong G/Z(G)$ and $\text{Inn } G \trianglelefteq \text{Aut } G$. By the second isomorphism theorem,

$$\langle \sigma \rangle \text{Inn } G / \text{Inn } G \cong \langle \sigma \rangle / (\langle \sigma \rangle \cap \text{Inn } G),$$

where $\langle \sigma \rangle$ is the subgroup generated by σ . Hence if σ is odd, then $\tau_a\sigma$ is also odd for any $a \in G$.

Suppose that H is a normal subgroup of G with $\sigma(H) = H$. Then for any coset $\bar{a} = a + H$, we have

$$\sigma(\bar{a}) = \sigma(a + H) = \sigma(a) + H.$$

So σ can also be viewed as an automorphism of G/H . The following lemma of Balister and Wheeler says that such an H always exists. For a prime power p^α , let \mathbb{F}_{p^α} denote the finite field with p^α elements.

LEMMA 4.1 ([4, Theorem 3.2]). *Suppose that G is a finite solvable group and σ is an automorphism of G . Then there exists a proper normal subgroup H of G satisfying:*

- (i) $\sigma(H) = H$.
- (ii) G/H is isomorphic to the additive group of some finite field \mathbb{F}_{p^α} .
- (iii) Let χ denote the isomorphism from G/H to the additive group of \mathbb{F}_{p^α} . Then there exists some $\gamma \in \mathbb{F}_{p^\alpha} \setminus \{0\}$ such that $\chi(\sigma(\bar{a})) = \gamma \cdot \chi(\bar{a})$ for each $\bar{a} \in G/H$.

The next lemma is a simple application of Alon’s Combinatorial Nullstellensatz.

LEMMA 4.2. *Let A, B be non-empty subsets of \mathbb{F}_{p^α} with $|A| = |B|$. Suppose that $\gamma \in \mathbb{F}_{p^\alpha} \setminus \{0, 1\}$. Then the cardinality of the restricted sumset*

$$A \overset{\gamma}{+} B = \{a + b : a \in A, b \in B, a \neq \gamma b\}$$

is at least

$$\min\{p, |A| + |B| - 2\}.$$

Proof. Without loss of generality, assume that $|A| = |B| \geq 2$ and $|A| + |B| - 2 \leq p$. Assume on the contrary that $|A \overset{\gamma}{+} B| < |A| + |B| - 2$. Define the polynomial

$$F(x, y) = (x - \gamma y)(x + y)^{|A|+|B|-3-|A \overset{\gamma}{+} B|} \prod_{c \in A \overset{\gamma}{+} B} (x + y - c).$$

Clearly $\deg F(x, y) = |A| + |B| - 2$ and $F(x, y)$ vanishes over the Cartesian product $A \times B$. Let $[x^n y^m]F(x, y)$ denote the coefficient of $x^n y^m$ in the expansion of $F(x, y)$. By [1, Theorem 1.2], $[x^{|A|-1} y^{|B|-1}]F(x, y)$ must be zero. On the other hand, clearly

$$\begin{aligned} [x^{|A|-1} y^{|B|-1}]F(x, y) &= [x^{|A|-1} y^{|B|-1}](x - \gamma y)(x + y)^{|A|+|B|-3} \\ &= \binom{|A| + |B| - 3}{|A| - 2} - \gamma \binom{|A| + |B| - 3}{|B| - 2} \\ &= (|A| + |B| - 3) \binom{|A| + |B| - 4}{|A| - 2} \left(\frac{1}{|B| - 1} - \frac{\gamma}{|A| - 1} \right). \end{aligned}$$

Since $|A| = |B|$ and $\gamma \neq 1$, $[x^{|A|-1} y^{|B|-1}]F(x, y)$ does not vanish, a contradiction. ■

Let H be a normal subgroup of G satisfying the requirements of Lemma 4.1. Suppose that $|H| = 1$. Then G is isomorphic to the additive group of some \mathbb{F}_{p^α} . Let χ be the isomorphism from G to \mathbb{F}_{p^α} . In view of Lemma 4.1, there exists $0 \neq \gamma \in \mathbb{F}_{p^\alpha}$ such that $\chi(\sigma(a)) = \gamma \cdot \chi(a)$ for any $a \in G$. Hence applying Lemma 4.2, for $\emptyset \neq A \subseteq G$, we have

$$|\sigma(A) \overset{\sigma}{+} A| = |\gamma \cdot \chi(A) \overset{\gamma}{+} \chi(A)| \geq \min\{p(G), 2|A| - 2\},$$

unless σ is the identity automorphism. Of course, if σ is the identity automorphism, then clearly Theorem 4.1 is true since G is then abelian.

Now assume that $|H| > 1$ and Theorem 4.1 holds for H and G/H . Note that for $a, b \in G$ and $S, T \subseteq H$,

$$(a + S) + (b + T) = a + b + (-b) + S + b + T = a + b + (\tau_b(S) + T),$$

and we have

$$\sigma(a + S) \overset{\sigma}{+} (a + T) = \sigma(a) + a + (\tau_a \sigma(S) \overset{\tau_a \sigma}{+} T).$$

As in Section 3, write

$$A = \bigcup_{j=1}^n (a_j + S_j),$$

where the S_j are non-empty subsets of H . Now $\sigma(A) \overset{\sigma}{+} A$ is equal to

$$\left(\bigcup_{1 \leq i \leq n} (\sigma(a_i) + a_i + (\tau_{a_i} \sigma(S_i) \overset{\tau_{a_i} \sigma}{+} S_i)) \right) \cup \left(\bigcup_{\substack{1 \leq i, j \leq n \\ i \neq j}} (\sigma(a_i) + a_j + (\tau_{a_j} \sigma(S_i) + S_j)) \right).$$

Assume that $n = 1$. Since $|\sigma(A) \overset{\sigma}{+} A| = 2|A| - 3$, we have

$$|\tau_{a_1} \sigma(S_1) \overset{\tau_{a_1} \sigma}{+} S_1| = 2|S_1| - 3.$$

By the induction hypothesis, for $s_1, s_2 \in T_1$ we have $\tau_{a_1} \sigma(s_1) + s_2 = \tau_{a_1} \sigma(s_2) + s_1$, i.e.,

$$-a_1 + \sigma(s_1) + a_1 + s_2 = -a_1 + \sigma(s_2) + a_1 + s_1.$$

It follows that

$$\sigma(a_1 + s_1) + (a_1 + s_2) = \sigma(a_1 + s_2) + (a_1 + s_1).$$

Hence Theorem 4.1 is true when $n = 1$.

Suppose that $n \geq 2$ and $|S_1| \geq \dots \geq |S_n|$. Let $\bar{A} = \{\bar{a}_1, \dots, \bar{a}_n\}$. By Lemma 2.1, assume that

$$\sigma(\bar{a}_1) + \bar{a}_1, \dots, \sigma(\bar{a}_1) + \bar{a}_n, \sigma(\bar{a}_2) + \bar{a}_{i_2}, \dots, \sigma(\bar{a}_n) + \bar{a}_{i_n}$$

are distinct elements of $\sigma(\bar{A}) + \bar{A}$. Then by (4.1),

$$\begin{aligned} |\sigma(A) \overset{\sigma}{+} A| &\geq |\tau_{a_1} \sigma(S_1) \overset{\tau_{a_1} \sigma}{+} S_1| + \sum_{j=2}^n |\tau_{a_1} \sigma(S_1) + S_j| + \sum_{j=2}^n |\tau_{a_{i_j}} \sigma(S_j) \overset{\tau_{a_{i_j}} \sigma}{+} S_{i_j}| \\ &\geq |S_1| + |S_1| - 3 + \sum_{j=2}^n (|S_1| + |S_j| - 1) + \sum_{j=2}^n |\tau_{a_{i_j}} \sigma(S_j) \overset{\tau_{a_{i_j}} \sigma}{+} S_{i_j}| \\ &\geq |A| - 2 + n(|S_1| - 1) + \sum_{j=2}^n (|S_j| - 1) = 2|A| - 3 + (n - 1)(|S_1| - 2), \end{aligned}$$

where in the third inequality we use the inequality $|S \overset{\sigma}{+} T| \geq |S| - 1$. Hence $|\sigma(A) \overset{\sigma}{+} A| \geq 2|A| - 2$ if $|S_1| \geq 3$.

Thus we must have $|S_1| \leq 2$. Suppose that $|S_1| = \dots = |S_n| = 1$. Then from $|\sigma(A) \overset{\sigma}{+} A| = 2n - 3$, we know that $|\sigma(\bar{A}) \overset{\sigma}{+} \bar{A}| = 2n - 3$. By the induction hypothesis, $\sigma(\bar{a}_i) + \bar{a}_j = \sigma(\bar{a}_j) + \bar{a}_i$ for any distinct $1 \leq i, j \leq n$. Let $X_i = a_i + S_i = \{x_i\}$. Then for distinct $1 \leq i, j \leq n$, $|(\sigma(X_i) + X_j) \cup (\sigma(X_j) + X_i)| = 1$ implies that $\sigma(x_i) + x_j = \sigma(x_j) + x_i$.

Suppose now that $|S_1| = 2$. Then

$$(4.2) \quad |\sigma(A) \overset{\sigma}{+} A| \geq \sum_{j=1}^n (|S_1| + |S_j| - 1) - 2 + \sum_{j=2}^n |\sigma(a_i + S_i) \overset{\sigma}{+} (a_{i_j} + S_{i_j})| \geq 2|A| - 3.$$

In the first inequality of (4.2), equality holds only if

$$|\tau_{a_1}\sigma(S_1) \overset{\tau_{a_1}\sigma}{+} S_1| = 2|S_1| - 3;$$

and equality holds in the second inequality of (4.2) only if $j = i_j$ for all $2 \leq j \leq n$ and

$$(4.3) \quad |\tau_{a_j}\sigma(S_j) \overset{\tau_{a_j}\sigma}{+} S_j| = |S_j| - 1.$$

Now $\sigma(A) \overset{\sigma}{+} A$ coincides with

$$(4.4) \quad \bigcup_{j=2}^n (\sigma(a_1) + a_j + (\tau_{a_j}\sigma(S_1) + S_j)) \cup \bigcup_{j=1}^n (\sigma(a_j) + a_j + (\tau_{a_j}\sigma(S_j) \overset{\tau_{a_j}\sigma}{+} S_j)).$$

Furthermore, we must have

$$\sigma(\bar{A}) \overset{\sigma}{+} \bar{A} \subseteq \{\sigma(\bar{a}_1) + \bar{a}_1, \sigma(\bar{a}_1) + \bar{a}_2, \dots, \sigma(\bar{a}_1) + \bar{a}_n, \sigma(\bar{a}_2) + \bar{a}_2, \dots, \sigma(\bar{a}_n) + \bar{a}_n\}.$$

Otherwise, there will exist distinct $2 \leq j_1, j_2 \leq n$ such that

$$\sigma(a_{j_1}) + a_{j_2} + (\tau_{a_{j_2}}\sigma(S_{j_1}) + S_{j_2}) \subseteq \sigma(A) \overset{\sigma}{+} A$$

is not included in (4.4).

Let

$$J_1 = \{1 \leq j \leq n : \sigma(\bar{a}_j) + \bar{a}_j \in (\sigma(\bar{A}) \overset{\sigma}{+} \bar{A}) \setminus \{\sigma(\bar{a}_1) + \bar{a}_2, \dots, \sigma(\bar{a}_1) + \bar{a}_n\}\},$$

and let $J_2 = \{2, \dots, n\} \setminus J_1$. We must have $|S_j| = 2$ for all $j \in J_1$. Otherwise, if $|S_{j_0}| = 1$ for some $j_0 \in J_1$, then there exist distinct $2 \leq j_1, j_2 \leq n$ such

that $\sigma(\bar{a}_{j_0}) + \bar{a}_{j_0} = \sigma(\bar{a}_{j_1}) + \bar{a}_{j_2}$. By (4.3), $\tau_{a_{j_0}}\sigma(S_{j_0}) \overset{\tau_{a_{j_0}}\sigma}{+} S_{j_0}$ is empty. But

$$\sigma(a_{j_1} + S_{j_1}) \overset{\sigma}{+} (a_{j_2} + S_{j_2}) = \sigma(a_{j_1} + S_{j_1}) + (a_{j_2} + S_{j_2})$$

is not empty.

We also have $n \leq 3$. Otherwise, for $n \geq 4$, by similar discussion to cases (a) and (b) of Section 3, we may find $j_0 \in J_1$ and distinct $2 \leq j_1, j_2 \leq n$ such that $\sigma(\bar{a}_{j_0}) + \bar{a}_{j_0} = \sigma(\bar{a}_{j_1}) + \bar{a}_{j_2}$ and $\max\{|S_{j_1}|, |S_{j_2}|\} = 2$. Thus in view

of (4.3), we have $|\tau_{a_{j_0}}\sigma(S_{j_0}) \overset{\tau_{a_{j_0}}\sigma}{+} S_{j_0}| = |S_{j_0}| - 1 = 1$, and the set

$$\sigma(a_{j_1} + S_{j_1}) \overset{\sigma}{+} (a_{j_2} + S_{j_2}) = \sigma(a_{j_1}) + a_{j_2} + (\tau_{a_{j_2}}\sigma(S_{j_1}) + S_{j_2})$$

has at least two elements.

Now we have shown that $|\sigma(A) \overset{\sigma}{+} A| = 2|A| - 3$ is impossible provided $|S_1| = 2$ and $n \geq 4$. However, the case $|S_1| = 2$ and $n = 2, 3$ is the most difficult part in the proof of Theorem 1.2. These are handled in the last section.

5. Proof of Theorem 1.2: The case $|S_1| = 2$ and $n = 2, 3$

LEMMA 5.1. *Let σ be an automorphism of G of odd order.*

- (i) *Suppose that $p(G) > 2$ and that $A = \{x_1, x_2\}$ and $B = \{y\}$ are subsets of G . If*

$$|(\sigma(A) + B) \cup (\sigma(B) + A)| = 2,$$

then $\sigma(x_i) + y = \sigma(y) + x_i$ for $i = 1, 2$.

- (ii) *Suppose that $p(G) > 3$ and that $A = \{x_1, x_2\}$ and $B = \{y_1, y_2\}$ are subsets of G . If*

$$|\sigma(A) \overset{\sigma}{+} A| = |\sigma(B) \overset{\sigma}{+} B| = 1, \quad |(\sigma(A) + B) \cup (\sigma(B) + A)| = 3,$$

then $\sigma(x_i) + y_j = \sigma(y_j) + x_i$ for $1 \leq i, j \leq 2$.

Proof. (i) Clearly $|(\sigma(A) + B) \cup (\sigma(B) + A)| = 2$ implies that $\sigma(x_1) + y$ equals either $\sigma(y) + x_1$ or $\sigma(y) + x_2$. Assume that

$$(5.1) \quad \sigma(x_1) + y = \sigma(y) + x_2,$$

or equivalently,

$$(5.2) \quad \sigma(x_2) + y = \sigma(y) + x_1.$$

By (5.2), we have $\sigma(x_2) = \sigma(y) + x_1 - y$. Substituting this into (5.1), we get

$$\sigma^2(x_1) + \sigma(y) = \sigma^2(y) + \sigma(x_2) = \sigma^2(y) + \sigma(y) + x_1 - y,$$

i.e.,

$$\sigma^2(x_1) = \sigma^2(y) + \sigma(y) + x_1 - y - \sigma(y).$$

By an easy induction, we have

$$\sigma^{2k}(x_1) = \sigma^{2k}(y) + \sigma^{2k-1}(y) + \dots + \sigma(y) + x_1 - y - \sigma(y) - \dots - \sigma^{2k-1}(y).$$

Let h be the order of σ and $k = (h|G| + 1)/2$. Then

$$\begin{aligned} \sigma^{2k}(y) + \sigma^{2k-1}(y) + \dots + \sigma^2(y) &= \sigma \left(\sum_{j=0}^{|G|-1} (\sigma^{jh+h}(y) + \dots + \sigma^{jh+1}(y)) \right) \\ &= \sigma(|G|(\sigma^h(y) + \sigma^{h-1}(y) + \dots + \sigma(y))) = 0. \end{aligned}$$

Similarly

$$-\sigma(y) - \dots - \sigma^{2k-1}(y) = |G|(-\sigma(y) - \dots - \sigma^h(y)) = 0.$$

Hence

$$\sigma(x_1) = \sigma^{2k}(x_1) = \sigma(y) + x_1 - y,$$

which clearly contradicts our assumption (5.1).

(ii) Assume that our assertion is not true. Clearly $|\sigma(A) \overset{\sigma}{+} A| = 1$ implies that

$$(5.3) \quad \sigma(x_1) + x_2 = \sigma(x_2) + x_1.$$

Similarly, it follows from $|\sigma(B) \overset{\sigma}{+} B| = 1$ that

$$(5.4) \quad \sigma(y_1) + y_2 = \sigma(y_2) + y_1.$$

In view of (i), either $|(\sigma(A) + y_1) \cup (\sigma(y_1) + A)| = 3$ or $|(\sigma(A) + y_2) \cup (\sigma(y_2) + A)| = 3$. By symmetry, we may assume that the first case holds, that is,

$$(5.5) \quad (\sigma(A) + B) \cup (\sigma(B) + A) = \{\sigma(x_1) + y_1, \sigma(x_2) + y_1, \sigma(y_1) + x_1\}$$

or

$$(5.6) \quad (\sigma(A) + B) \cup (\sigma(B) + A) = \{\sigma(x_1) + y_1, \sigma(x_2) + y_1, \sigma(y_1) + x_2\}.$$

On the other hand,

$$\sigma(A) + B = \{\sigma(x_1) + y_1, \sigma(x_2) + y_1, \sigma(x_1) + y_2, \sigma(x_2) + y_2\}.$$

So without loss of generality, we may assume that

$$(5.7) \quad \sigma(x_1) + y_1 = \sigma(x_2) + y_2.$$

Thus

$$\sigma(A) + B = \{\sigma(x_1) + y_1, \sigma(x_2) + y_1, \sigma(x_1) + y_2\}.$$

Now we have either

$$\sigma(y_1) + x_1 = \sigma(x_1) + y_2$$

or

$$\sigma(y_1) + x_2 = \sigma(x_1) + y_2,$$

according to whether (5.5) or (5.6) holds. Assume that $\sigma(y_1) + x_1 = \sigma(x_1) + y_2$.

There are the following six subcases:

$$(a) \begin{cases} \sigma(x_2) + y_2 = \sigma(x_1) + y_1, \\ \sigma(y_1) + x_2 = \sigma(x_1) + y_1, \\ \sigma(y_2) + x_1 = \sigma(x_2) + y_1, \\ \sigma(y_2) + x_2 = \sigma(x_1) + y_2, \\ \sigma(y_1) + x_1 = \sigma(x_1) + y_2, \end{cases} \quad (b) \begin{cases} \sigma(x_2) + y_2 = \sigma(x_1) + y_1, \\ \sigma(y_1) + x_2 = \sigma(x_2) + y_1, \\ \sigma(y_2) + x_1 = \sigma(x_2) + y_1, \\ \sigma(y_2) + x_2 = \sigma(x_1) + y_2, \\ \sigma(y_1) + x_1 = \sigma(x_1) + y_2, \end{cases}$$

$$\begin{array}{cc}
\text{(c)} \left\{ \begin{array}{l} \sigma(x_2) + y_2 = \sigma(x_1) + y_1, \\ \sigma(y_2) + x_1 = \sigma(x_1) + y_1, \\ \sigma(y_1) + x_2 = \sigma(x_2) + y_1, \\ \sigma(y_2) + x_2 = \sigma(x_1) + y_2, \\ \sigma(y_1) + x_1 = \sigma(x_1) + y_2, \end{array} \right. &
\text{(d)} \left\{ \begin{array}{l} \sigma(x_2) + y_2 = \sigma(x_1) + y_1, \\ \sigma(y_1) + x_2 = \sigma(x_1) + y_1, \\ \sigma(y_2) + x_1 = \sigma(x_1) + y_1, \\ \sigma(y_2) + x_2 = \sigma(x_1) + y_2, \\ \sigma(y_1) + x_1 = \sigma(x_1) + y_2, \end{array} \right. \\
\text{(e)} \left\{ \begin{array}{l} \sigma(x_2) + y_2 = \sigma(x_1) + y_1, \\ \sigma(y_1) + x_2 = \sigma(x_1) + y_1, \\ \sigma(y_2) + x_1 = \sigma(x_1) + y_1, \\ \sigma(y_2) + x_2 = \sigma(x_2) + y_1, \\ \sigma(y_1) + x_1 = \sigma(x_1) + y_2, \end{array} \right. &
\text{(f)} \left\{ \begin{array}{l} \sigma(x_2) + y_2 = \sigma(x_1) + y_1, \\ \sigma(y_2) + x_2 = \sigma(x_1) + y_1, \\ \sigma(y_1) + x_2 = \sigma(x_2) + y_1, \\ \sigma(y_2) + x_1 = \sigma(x_2) + y_1, \\ \sigma(y_1) + x_1 = \sigma(x_1) + y_2. \end{array} \right.
\end{array}$$

First, it is impossible that $\sigma(y_2) + x_1 = \sigma(x_1) + y_1$ and $\sigma(y_1) + x_1 = \sigma(x_1) + y_2$ simultaneously. In fact, if it is true, then we have

$$\sigma(x_1) + y_1 - x_1 = \sigma(y_2) = \sigma(-\sigma(x_1) + \sigma(y_1) + x_1),$$

i.e.,

$$\sigma^2(y_1) = \sigma^2(x_1) + \sigma(x_1) + y_1 - x_1 - \sigma(x_1).$$

By the discussion in the proof of (i), we get $\sigma(y_1) = \sigma(x_1) + y_1 - x_1$. Thus (c), (d) and (e) can be omitted.

Second, $\sigma(y_2) + x_2 = \sigma(x_1) + y_2$ and $\sigma(y_1) + x_2 = \sigma(x_2) + y_1$ cannot simultaneously hold. In fact, $x_2 = -\sigma(y_2) + \sigma(x_1) + y_2$ implies that

$$\sigma(x_2) = \sigma(-\sigma(y_2) + \sigma(x_1) + y_2) = -\sigma^2(y_2) + \sigma^2(x_1) + \sigma(y_2).$$

If $\sigma(y_1) + x_2 = \sigma(x_2) + y_1$, then

$$\begin{aligned}
\sigma(y_1) + (-\sigma(y_2) + \sigma(x_1) + y_2) &= (-\sigma^2(y_2) + \sigma^2(x_1) + \sigma(y_2)) + y_1 \\
&= -\sigma^2(y_2) + \sigma^2(x_1) + \sigma(y_1) + y_2,
\end{aligned}$$

where in the second equality we use (5.4). Thus we get

$$y_1 - y_2 + x_1 = -\sigma(y_2) + \sigma(x_1) + y_1.$$

It follows that

$$\sigma(x_1) + y_1 = \sigma(y_2) + y_1 - y_2 + x_1 = \sigma(y_1) + y_2 - y_2 + x_1 = \sigma(y_1) + x_1.$$

Hence (b) is impossible.

Similarly, $\sigma(y_2) + x_2 = \sigma(x_1) + y_1$ and $\sigma(y_1) + x_2 = \sigma(x_2) + y_1$ cannot hold simultaneously. Otherwise we would have

$$x_2 = -\sigma(y_2) + \sigma(x_1) + y_1$$

and

$$\sigma(y_1) + (-\sigma(y_2) + \sigma(x_1) + y_1) = -\sigma^2(y_2) + \sigma^2(x_1) + \sigma(y_1) + y_1.$$

That is,

$$\sigma(y_1) - \sigma(y_2) + \sigma(x_1) = -\sigma^2(y_2) + \sigma^2(x_1) + \sigma(y_1),$$

i.e.,

$$y_1 - y_2 + x_1 = -\sigma(y_2) + \sigma(x_1) + y_1.$$

However, from (5.4), we have

$$\sigma(x_1) + y_1 = \sigma(y_2) + y_1 - y_2 + x_1 = \sigma(y_1) + y_2 - y_2 + x_1 = \sigma(y_1) + x_1,$$

which contradicts the last equation of (f). So (f) is impossible.

Finally, let us turn to (a). In view of the fifth equation of (a), we have

$$(5.8) \quad \begin{aligned} \sigma^2(x_1) &= \sigma(\sigma(y_1) + x_1 - y_2) = \sigma^2(y_1) + \sigma(x_1) - \sigma(y_2) \\ &= \sigma^2(y_1) + \sigma(y_1) + x_1 - y_2 - \sigma(y_2). \end{aligned}$$

By the fourth equation of (a), we have

$$\sigma(x_2) = \sigma(-\sigma(y_2) + \sigma(x_1) + y_2) = -\sigma^2(y_2) + \sigma^2(x_1) + \sigma(y_2).$$

So from (5.8), we get

$$\sigma(x_2) + y_2 = -\sigma^2(y_2) + \sigma^2(x_1) + \sigma(y_2) + y_2 = -\sigma^2(y_2) + \sigma^2(y_1) + \sigma(y_1) + x_1.$$

It follows from the first equation of (a) that

$$\sigma(x_1) = -\sigma^2(y_2) + \sigma^2(y_1) + \sigma(y_1) + x_1 - y_1,$$

i.e.,

$$(5.9) \quad \begin{aligned} \sigma^2(x_1) &= -\sigma^3(y_2) + \sigma^3(y_1) \\ &\quad + \sigma^2(y_1) + (-\sigma^2(y_2) + \sigma^2(y_1) + \sigma(y_1) + x_1 - y_1) - \sigma(y_1). \end{aligned}$$

On the other hand, by the third equation of (a), we have $\sigma(x_2) = \sigma(y_2) + x_1 - y_1$, and by the second equation of (a), we get

$$\sigma^2(x_1) + \sigma(y_1) = \sigma(\sigma(y_1) + x_2) = \sigma^2(y_1) + (\sigma(y_2) + x_1 - y_1),$$

i.e.,

$$(5.10) \quad \sigma^2(x_1) = \sigma^2(y_1) + \sigma(y_2) + x_1 - y_1 - \sigma(y_1).$$

Combining (5.9) and (5.10) and recalling $\sigma^3(y_2) + \sigma^2(y_1) = \sigma^3(y_1) + \sigma^2(y_2)$ by (5.4), we obtain

$$\sigma^2(y_1) - \sigma^2(y_2) + \sigma^2(y_1) + \sigma(y_1) = \sigma^2(y_2) + \sigma(y_2),$$

i.e.,

$$2\sigma(-y_2 + y_1) = y_2 - y_1.$$

However, $\sigma(y_1) + y_2 = \sigma(y_2) + y_1$ implies that $\sigma(-y_2 + y_1) = y_1 - y_2$. So we get

$$3(y_1 - y_2) = 0.$$

Hence (a) is also impossible.

Now we have proved that $\sigma(y_1) + x_1 = \sigma(x_1) + y_2$ is impossible. And the case $\sigma(y_1) + x_2 = \sigma(x_1) + y_2$ is also impossible, as can be seen by considering the following six subcases:

$$\begin{array}{cc}
 \text{(a')} \left\{ \begin{array}{l} \sigma(x_1) + y_1 = \sigma(x_2) + y_2, \\ \sigma(y_1) + x_2 = \sigma(x_1) + y_2, \\ \sigma(y_2) + x_1 = \sigma(x_1) + y_2, \\ \sigma(y_1) + x_1 = \sigma(x_1) + y_1, \\ \sigma(y_2) + x_2 = \sigma(x_2) + y_1, \end{array} \right. & \text{(b')} \left\{ \begin{array}{l} \sigma(x_1) + y_1 = \sigma(x_2) + y_2, \\ \sigma(y_1) + x_2 = \sigma(x_1) + y_2, \\ \sigma(y_2) + x_1 = \sigma(x_1) + y_2, \\ \sigma(y_1) + x_1 = \sigma(x_2) + y_1, \\ \sigma(y_2) + x_2 = \sigma(x_1) + y_1, \end{array} \right. \\
 \\
 \text{(c')} \left\{ \begin{array}{l} \sigma(x_1) + y_1 = \sigma(x_2) + y_2, \\ \sigma(y_1) + x_2 = \sigma(x_1) + y_2, \\ \sigma(y_2) + x_1 = \sigma(x_1) + y_2, \\ \sigma(y_1) + x_1 = \sigma(x_1) + y_1, \\ \sigma(y_2) + x_2 = \sigma(x_1) + y_1, \end{array} \right. & \text{(d')} \left\{ \begin{array}{l} \sigma(x_1) + y_1 = \sigma(x_2) + y_2, \\ \sigma(y_1) + x_2 = \sigma(x_1) + y_2, \\ \sigma(y_2) + x_1 = \sigma(x_1) + y_2, \\ \sigma(y_1) + x_1 = \sigma(x_2) + y_1, \\ \sigma(y_2) + x_2 = \sigma(x_2) + y_1, \end{array} \right. \\
 \\
 \text{(e')} \left\{ \begin{array}{l} \sigma(x_1) + y_1 = \sigma(x_2) + y_2, \\ \sigma(y_1) + x_2 = \sigma(x_1) + y_2, \\ \sigma(y_2) + x_1 = \sigma(x_1) + y_1, \\ \sigma(y_1) + x_1 = \sigma(x_2) + y_1, \\ \sigma(y_2) + x_2 = \sigma(x_2) + y_1, \end{array} \right. & \text{(f')} \left\{ \begin{array}{l} \sigma(x_1) + y_1 = \sigma(x_2) + y_2, \\ \sigma(y_1) + x_2 = \sigma(x_1) + y_2, \\ \sigma(y_2) + x_1 = \sigma(x_2) + y_1, \\ \sigma(y_1) + x_1 = \sigma(x_1) + y_1, \\ \sigma(y_2) + x_2 = \sigma(x_1) + y_1. \end{array} \right.
 \end{array}$$

The discussions for (a')–(f') do not require any new ideas, so we omit the details. ■

Let us return to the proof of Theorem 4.1. Suppose $n = 3$. Note that when $i \neq j$, we have

$$\begin{aligned}
 |\sigma(a_i + S_i) \overset{\sigma}{+} (a_j + S_j)| &= |(\sigma(a_i) + a_j) + (\tau_{a_j} \sigma(S_i) + S_j)| \\
 &\geq |S_i| + |S_j| - 1.
 \end{aligned}$$

Clearly, $\sigma(\bar{a}_1) + \bar{a}_2, \sigma(\bar{a}_1) + \bar{a}_3 \in \sigma(\bar{A}) \overset{\sigma}{+} \bar{A}$; and for other $\sigma(\bar{a}_i) + \bar{a}_j \in \sigma(\bar{A}) \overset{\sigma}{+} \bar{A}$ with $i \neq j$, we have

$$|\sigma(a_i + S_i) \overset{\sigma}{+} (a_j + S_j)| \geq |S_i| + |S_j| - 1 \geq |S_2| + |S_3| - 1$$

by recalling $|S_1| \geq |S_2| \geq |S_3|$. Hence $\sigma(A) \overset{\sigma}{+} A$ contains at least

$$\sum_{j=2}^3 |\sigma(a_1 + S_1) \overset{\sigma}{+} (a_j + S_j)| + \sum_{\substack{\sigma(\bar{a}_i) + \bar{a}_j \in \sigma(\bar{A}) \overset{\sigma}{+} \bar{A} \\ \sigma(\bar{a}_i) + \bar{a}_j \neq \sigma(\bar{a}_1) + \bar{a}_2, \sigma(\bar{a}_1) + \bar{a}_3}} |\sigma(a_i + S_i) \overset{\sigma}{+} (a_j + S_j)|$$

$$\begin{aligned} &\geq \sum_{j=2}^3 (|S_1| + |S_j| - 1) + (|\sigma(\bar{A}) \overset{\sigma}{+} \bar{A}| - 2)(|S_2| + |S_3| - 1) \\ &= 2|A| - 3 + (|\sigma(\bar{A}) \overset{\sigma}{+} \bar{A}| - 3)(|S_2| + |S_3| - 1) \end{aligned}$$

elements. So we must have $|\sigma(\bar{A}) \overset{\sigma}{+} \bar{A}| = 3$, i.e., $\sigma(\bar{a}_i) + \bar{a}_j = \sigma(\bar{a}_j) + \bar{a}_i$ for $1 \leq i, j \leq 3$ by the induction hypothesis. It follows that

$$\sigma(\bar{A}) \overset{\sigma}{+} \bar{A} = \{\sigma(\bar{a}_1) + \bar{a}_2, \sigma(\bar{a}_2) + \bar{a}_3, \sigma(\bar{a}_3) + \bar{a}_1\}.$$

Furthermore, for $1 \leq i \leq 3$, if $\sigma(\bar{a}_i) + \bar{a}_i \notin \sigma(\bar{A}) \overset{\sigma}{+} \bar{A}$, then $\tau_{a_i} \sigma(S_i) \overset{\tau_{a_i} \sigma}{+} S_i$ must be empty, i.e., $|S_i| = 1$. Since $|S_1| = 2$, we have $\sigma(\bar{a}_1) + \bar{a}_1 \in \sigma(\bar{A}) \overset{\sigma}{+} \bar{A}$, i.e., $\sigma(\bar{a}_1) + \bar{a}_1 = \sigma(\bar{a}_2) + \bar{a}_3$. We claim that $\sigma(\bar{a}_2) + \bar{a}_2 \notin \sigma(\bar{A}) \overset{\sigma}{+} \bar{A}$. Assume on the contrary that $\sigma(\bar{a}_2) + \bar{a}_2 \in \sigma(\bar{A}) \overset{\sigma}{+} \bar{A}$. We must have $\sigma(\bar{a}_2) + \bar{a}_2 = \sigma(\bar{a}_1) + \bar{a}_3$. So

$$\sigma(\bar{a}_2) + \bar{a}_3 = \sigma(\bar{a}_1) + \bar{a}_1 = (\sigma(\bar{a}_2) + \bar{a}_2 - \bar{a}_3) + \bar{a}_1,$$

i.e., $\bar{a}_3 - \bar{a}_1 = \bar{a}_2 - \bar{a}_3$. So we have $\bar{a}_3 = \bar{a}_1 + \bar{d}$ and $\bar{a}_2 = \bar{a}_1 + 2\bar{d}$ for some $d \in G$. Recall that G/H is abelian. From $\sigma(\bar{a}_1) + \bar{a}_3 = \sigma(\bar{a}_3) + \bar{a}_1$, it follows that $\sigma(\bar{d}) = \bar{d}$. Since $\sigma(\bar{a}_1) + \bar{a}_1 = \sigma(\bar{a}_2) + \bar{a}_3$, we get $3\bar{d} = 0$. However, since $|A| \geq 4$ and $2|A| - 3 < p(G)$, we have $p(G) > 3$. This evidently leads to a contradiction. Similarly, it is also impossible that $\sigma(\bar{a}_3) + \bar{a}_3 \in \sigma(\bar{A}) \overset{\sigma}{+} \bar{A}$. Thus $|S_2| = |S_3| = 1$.

Let $X_i = a_i + S_i$. Assume that $X_1 = \{x_1, x_2\}$, $X_2 = \{y_1\}$ and $X_3 = \{y_2\}$. Now we have

$$|\sigma(X_1) \overset{\sigma}{+} X_1| = |(\sigma(X_2) + X_3) \cup (\sigma(X_3) + X_2)| = 1$$

and

$$|(\sigma(X_1) + X_2) \cup (\sigma(X_2) + X_1)| = |(\sigma(X_1) + X_3) \cup (\sigma(X_3) + X_1)| = 2.$$

Evidently $|\sigma(X_1) \overset{\sigma}{+} X_1| = 1$ implies $\sigma(x_1) + x_2 = \sigma(x_2) + x_1$, and it follows from $|(\sigma(X_2) + X_3) \cup (\sigma(X_3) + X_2)| = 1$ that $\sigma(y_1) + y_2 = \sigma(y_2) + y_1$. By Lemma 5.1(i), $|(\sigma(X_1) + X_2) \cup (\sigma(X_2) + X_1)| = 2$ implies $\sigma(x_i) + y_1 = \sigma(y_1) + x_i$ for $i = 1, 2$. Similarly, we have $\sigma(x_i) + y_2 = \sigma(y_2) + x_i$ for $i = 1, 2$. So Theorem 4.1 holds for $n = 3$.

Suppose that $n = 2$. Clearly $\sigma(\bar{a}_1) + \bar{a}_2 = \sigma(\bar{a}_2) + \bar{a}_1$. Let $X_i = a_i + S_i$. The case $|S_2| = 1$ easily follows from the discussions for $n = 3$. Assume that $|S_2| = 2$. Then

$$|\sigma(X_1) \overset{\sigma}{+} X_1| = |\sigma(X_2) \overset{\sigma}{+} X_2| = 1, \quad |(\sigma(X_1) + X_2) \cup (\sigma(X_2) + X_1)| = 3.$$

Applying Lemma 5.1(ii), we get the desired result. Thus the proof of Theorem 4.1 is complete. ■

Acknowledgements. We are grateful to the anonymous referee for his/her very helpful suggestions. We also thank Professor Gyula Károlyi for pointing out a mistake in our earlier version.

The authors are supported by National Natural Science Foundation of China (Grant No. 11671197). The first author is also supported by the Scientific Research Foundation of Jinling Institute of Technology (2014-jit-n-07) and the Tianyuan Foundation of China (11626123). The second author is the corresponding author.

References

- [1] N. Alon, *Combinatorial Nullstellensatz*, *Combin. Probab. Comput.* 8 (1999), 7–29.
- [2] N. Alon, M. B. Nathanson and I. Z. Ruzsa, *Adding distinct congruence classes modulo a prime*, *Amer. Math. Monthly* 102 (1995), 250–255.
- [3] N. Alon, M. B. Nathanson and I. Z. Ruzsa, *The polynomial method and restricted sums of congruence classes*, *J. Number Theory* 56 (1996), 404–417.
- [4] P. Balister and J. P. Wheeler, *The Erdős–Heilbronn problem for finite groups*, *Acta Arith.* 140 (2009), 105–118.
- [5] 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.
- [6] P. Erdős, *On the addition of residue classes mod p* , in: *Proceedings of the 1963 Number Theory Conference at the University of Colorado*, Univ. of Colorado Press, 1963, 16–17.
- [7] P. Erdős, *Some problems in number theory*, in: *Computers in Number Theory*, A. O. L. Atkin and B. J. Birch (eds.), Academic Press, 1971, 405–414.
- [8] P. Erdős and H. Heilbronn, *On the addition of residue classes mod p* , *Acta Arith.* 9 (1964), 149–159.
- [9] W. Feit and J. G. Thompson, *Solvability of groups of odd order*, *Pacific J. Math.* 13 (1963), 775–1029.
- [10] S. M. Jayasuriya, G. Károlyi, S. D. Reich and J. P. Wheeler, *Concerning the inverse Erdős–Heilbronn problem in finite groups*, in preparation.
- [11] S. M. Jayasuriya, S. D. Reich and J. P. Wheeler, *On the inverse Erdős–Heilbronn problem for restricted set addition in finite groups*, arXiv:1210.6509 (2012).
- [12] G. Károlyi, *On restricted set addition in abelian groups*, *Ann. Univ. Sci. Budapest. Eötvös Sect. Math.* 46 (2003), 47–54.
- [13] G. Károlyi, *The Erdős–Heilbronn problem in abelian groups*, *Israel J. Math.* 139 (2004), 349–359.
- [14] G. Károlyi, *The Cauchy–Davenport theorem in group extensions*, *Enseign. Math.* 51 (2005), 239–254.
- [15] G. Károlyi, *An inverse theorem for the restricted set addition in abelian groups*, *J. Algebra* 290 (2005), 557–593.
- [16] G. Károlyi, *Restricted set addition: the exceptional case of the Erdős–Heilbronn conjecture*, *J. Combin. Theory Ser. A* 116 (2009), 741–746.
- [17] M. B. Nathanson, *Additive Number Theory. Inverse Problems and the Geometry of Sumsets*, *Grad. Texts in Math.* 165, Springer, New York, 1996.
- [18] J. E. Olson, *On the sum of two sets in a group*, *J. Number Theory* 18 (1984), 110–120.

- [19] J. H. van Lint and R. M. Wilson, *A Course in Combinatorics*, 2nd ed., Cambridge Univ. Press, Cambridge, 2001.
- [20] A. G. Vosper, *The critical pairs of subsets of a group of prime order*, J. London Math. Soc. 31 (1956), 200–205, Addendum 280–282.

Shanshan Du
The Fundamental Division
Jingling Institute of Technology
Nanjing 211169
People's Republic of China
E-mail: ssdu@jit.edu.com

Hao Pan (corresponding author)
Department of Mathematics
Nanjing University
Nanjing 210093
People's Republic of China
E-mail: haopan79@zoho.com

