Electron. J. Combin. 33 (2026), no. 1, to appear.

ON TWO NEW KINDS OF RESTRICTED SUMSETS

HAN WANG AND ZHI-WEI SUN

Abstract. Let $A_1,\ldots,A_n$ be finite subsets of an additive abelian group G with $|A_1|=\cdots=|A_n|\geqslant 2$. Concerning the two new kinds of restricted sumsets

$$L(A_1,\ldots,A_n)=\{a_1+\cdots+a_n:\ a_1\in A_1,\ldots,a_n\in A_n,\ \text{and } a_i\neq a_{i+1}\text{ for }1\leqslant i<n\}$$

and

$$C(A_1,\ldots,A_n)=\{a_1+\cdots+a_n:\ a_i\in A_i\ (1\leqslant i\leqslant n)\text{ and } a_1\neq a_2\neq\cdots\neq a_n\neq a_1\},$$

when G is the additive group of a field we obtain lower bounds for $|L(A_1,\ldots,A_n)|$ and $|C(A_1,\ldots,A_n)|$ via the polynomial method in a quite nontrivial way. Moreover, when G is torsion-free and $A_1=\cdots=A_n$, we determine completely when $|L(A_1,\ldots,A_n)|$ or $|C(A_1,\ldots,A_n)|$ attains its lower bound.

1. Introduction

Let G be an additive group. For finite subsets $A_1,\ldots,A_n$ of G, their sumset is defined by

$$A_1+\cdots+A_n=\{a_1+\cdots+a_n:\ a_1\in A_1,\ldots,a_n\in A_n\},$$

and their sumset with distinct summands is given by

$$A_1\dot{+}\cdots\dot{+}A_n=\{a_1+\cdots+a_n:\ a_1\in A_1,\ldots,a_n\in A_n,\ \text{and } a_1,\ldots,a_n\text{ are pairwise distinct}\}.$$

When $A_1=\cdots=A_n=A$, we use nA to mean $A_1+\cdots+A_n$, and $n^{\wedge}A$ to stand for $A_1\dot{+}\cdots\dot{+}A_n$.

The famous Erdős-Heilbronn conjecture [6] posed in 1964 asserts that for any prime p and $A\subseteq\mathbb{Z}/p\mathbb{Z}$, we have

$$|2^{\wedge}A|\geqslant\min\{p,\,2|A|-3\}.$$

This was first confirmed by Dias da Silva and Hamidoune [5] in 1994 via exterior algebra. An extension of this involving kth powers over a field was given by H. Pan and Z.-W. Sun [10] in 2009.

Let G be an additive group with $|G|>1$. We define $p(G)$ as the minimum of orders of nonzero elements of G if G contains a nonzero element of finite order, otherwise we consider $p(G)$ as $+\infty$. In 2004 G. Károlyi [8] extended the Erdős-Heilbronn conjecture to any abelian group G with $|G|>1$; moreover, in 2009 P. Balister and J. P. Wheeler [4] obtained the

Key words and phrases. Additive combinatorics, sumset, field, the polynomial method, torsion-free abelian group.

2020 *Mathematics Subject Classification.* Primary 05E16, 11B13; Secondary 11P70, 11T06, 20K15.

Supported by the Natural Science Foundation of China (grant no. 12371004).

following extension of the Erdős-Heilbronn conjecture to any finite group G with $|G|>1$: For any nonempty subset A of G we have

$$|2^{\wedge}A|\geqslant \min\{p(G),\, 2|A|-3\}.$$

In graph theory, given a graph with n vertices $v_1,\ldots,v_n$ and given a set A_i of colors for each vertex v_i, a *proper list coloring* is a choice function that maps every vertex v_i to a color a_i in the list A_i, such that no two adjacent vertices receive the same color. Thus, sumsets with distinct summands are related to list colorings of complete graphs.

For a subset A of an additive group G, obviously

$$2^{\wedge}A=\{a_1+a_2:\ a_1,a_2\in A \text{ and } a_1\neq a_2\}$$

and

$$3^{\wedge}A=\{a_1+a_2+a_3:\ a_1,a_2,a_3\in A \text{ and } a_1\neq a_2\neq a_3\neq a_1\}.$$

This reminds us linear and circular permutations. Thus, it is natural to consider restricted sumsets related to list colorings of paths and cycles instead of complete graphs. Motivated by this, the second author [13] introduced two new kinds of sumsets. Namely, for finite subsets $A_1,\ldots,A_n$ of an additive group G, Sun defined

$$L(A_1,\ldots,A_n)=\{a_1+\cdots+a_n:\ a_i\in A_i \text{ for } i=1,\ldots,n,\ \text{and } a_i\neq a_{i+1} \text{ for all } 0<i<n\}$$

and

$$C(A_1,\ldots,A_n)=\{a_1+\cdots+a_n:\ a_i\in A_i\ (1\leqslant i\leqslant n) \text{ and } \ a_1\neq a_2\neq\cdots\neq a_n\neq a_1\}.$$

Clearly

$$L(A_1,A_2)=C(A_1,A_2)=A_1\dot{+}A_2,\ \text{and } C(A_1,A_2,A_3)=A_1\dot{+}A_2\dot{+}A_3.$$

When $A_1=\cdots=A_n=A$, we simply write $n\tilde{}A$ to denote $L(A_1,\ldots,A_n)$, and $n^{\circ}A$ to denote $C(A_1,\ldots,A_n)$.

In 2022, the second author [13] made the following general conjecture.

Conjecture 1.1. *Let G be an additive group with $|G|>1$, and let $A_1,\ldots,A_n$ $(n>1)$ be finite subsets of G with $|A_i|>1$ for all $i=1,\ldots,n$. Then*

$$|L(A_1,\ldots,A_n)|\geqslant \min\{p(G),\,|A_1|+\cdots+|A_n|-2n+1+\{n\}_2\} \tag{1.1}$$

and

$$|C(A_1,\ldots,A_n)|\geqslant \min\{p(G),\,|A_1|+\cdots+|A_n|-2n+(-1)^n(1+\{n\}_2)\}, \tag{1.2}$$

where $\{n\}_2$ denotes the least nonnegative residue of n modulo 2.

This conjecture is motivated by Sun's following observation: For any integer $n>1$ and $A=\{0,\ldots,k-1\}$ with $k\in\mathbb{Z}^+=\{1,2,3,\ldots\}$, we have

$$|n\tilde{}A|=n|A|-2n+1+\{n\}_2$$

and

$$|n^{\circ}A|=n|A|-2n+(-1)^n(1+\{n\}_2).$$

By Sun [11, Corollary 1.5], if $A_i \subseteq \mathbb{Z}$ and $|A_i| \geqslant 3$ for all $i = 1, \ldots, n$, then $|C(A_1, \ldots, A_n)| \geqslant \sum_{i=1}^n |A_i| - 3n + 1$.

For a field F, we let $\mathrm{ch}(F)$ be the characteristic of F. Clearly,

$$p(F) = \begin{cases} p & \text{if } \mathrm{ch}(F) \text{ is a prime } p, \\ +\infty & \text{if } \mathrm{ch}(F) = 0. \end{cases}$$

Applying Theorem 1.3 of Sun and L. Zhao [15] with

$$P(x_1, \ldots, x_n) = (x_1 - x_2)(x_2 - x_3) \cdots (x_{n-1} - x_n)(x_n - x_1)$$

or

$$P(x_1, \ldots, x_n) = (x_1 - x_2)(x_2 - x_3) \cdots (x_{n-1} - x_n),$$

we see that if $A_1, \ldots, A_n$ are finite subsets of a field F with $|A_i| > 2$ for all $i = 1, \ldots, n$ then

$$|C(A_1, \ldots, A_n)| \geqslant \min\{p(F) - n,\ |A_1| + \cdots + |A_n| - 3n + 1\}$$

and

$$|L(A_1, \ldots, A_n)| \geqslant \min\{p(F) - n + 1,\ |A_1| + \cdots + |A_n| - 3n + 3\}.$$

Note that the lower bounds here are not optimal in view of Conjecture 1.1.

If A_1, A_2, A_3 are finite nonempty subsets of a field F, then in the spirit of [3, Theorem 3.2], the cardinality of $C(A_1, A_2, A_3) = A_1 \dot{+} A_2 \dot{+} A_3$ is at least

$$\min\left\{p(F),\ 1 + \sum_{i=1}^3 (|A_i| - 3)\right\} = \min\{p(F),\ |A_1| + |A_2| + |A_3| - 2 \times 3 + (-1)^3(1 + \{3\}_2)\},$$

which is essentially the inequality (1.2) with $n = 3$ and $G = F$.

When G is the additive group of a field, our following theorem confirms the inequality (1.2) in the case $n = 3$ and $|A_1| = |A_2| = |A_3|$.

Theorem 1.1. (i) *Let F be any field, and let A_1, A_2, A_3 be finite subsets of F with $|A_1|, |A_3| \geqslant 2$ and $|A_2| - |A_1| \in \{0, 1\}$. Then we have*

$$|L(A_1, A_2, A_3)| \geqslant \min\{p(F), |A_1| + |A_2| + |A_3| - 4\}. \tag{1.3}$$

(ii) *Let G be a torsion-free additive abelian group, and let A_1, A_2, A_3 be finite subsets of G with cardinality $2 \leqslant |A_1| \leqslant |A_2| \leqslant |A_3|$. Then we have*

$$|L(A_1, A_2, A_3)| \geqslant |A_1| + |A_2| + |A_3| - 4. \tag{1.4}$$

Corollary 1.1. *Let p be any prime. For any $A \subseteq \mathbb{F}_p$ with $|A| \geqslant \lfloor p/3 \rfloor + 2$, each element of $\mathbb{F}_p$ can be written as $a_1 + a_2 + a_3$ with $a_1, a_2, a_3 \in A$ and $a_1 \neq a_2 \neq a_3$.*

Our next two theorems deal with Conjecture 1.1 when G is the additive group of a field, and $|A_1| = \cdots = |A_n|$.

Theorem 1.2. *Let n be any positive even integer, and let $A_1,\ldots,A_n$ be subsets of a field F with $|A_1|=\cdots=|A_n|\geqslant 2$. Suppose that $p(F)>\sum_{i=1}^n|A_i|-2n$. Then*

$$|L(A_1,\ldots,A_n)|\geqslant|C(A_1,\ldots,A_n)|\geqslant\sum_{i=1}^n|A_i|-2n+1. \tag{1.5}$$

Theorem 1.3. *Let n be any positive odd integer, and let $A_1,\ldots,A_n$ be subsets of a field F with $|A_1|=\cdots=|A_n|\geqslant 2$. Suppose that $p(F)>\sum_{i=1}^n|A_i|-2n+1$. Then*

$$|L(A_1,\ldots,A_n)|\geqslant\sum_{i=1}^n|A_i|-2n+2. \tag{1.6}$$

We will prove Theorem 1.1 and Corollary 1.1, and Theorem 1.2–1.3 in Sections 2 and 3 respectively, via the so-called polynomial method involving the famous Combinatorial Nullstellensatz of N. Alon [1]. A key and challenging step is to prove the following novel results:

$$[x_1^k\ldots x_n^k](x_1-x_2)\cdots(x_{n-1}-x_n)(x_n-x_1)(x_1+\cdots+x_n)^{(k-1)n}=\frac{((k-1)n)!}{k!^n}2k^{n/2}$$

if n is even, and

$$[x_1^k\cdots x_n^k](x_1-x_2)\cdots(x_{n-1}-x_n)(x_1+\cdots+x_n)^{(k-1)n+1}=\frac{((k-1)n+1)!}{(k!)^n}\times k^{(n-1)/2}$$

if n is odd, where k is a positive integer, and $[x_1^k\ldots x_n^k]P(x_1,\ldots,x_n)$ denotes the coefficient of $x_1^k\ldots x_n^k$ in a polynomial $P(x_1,\ldots,x_n)$.

In 1995, M. B. Nathanson [9] proved that for any finite subset A of $\mathbb{Z}$ with $|A|\geqslant 5$ and $n\in\{2,\ldots,|A|-2\}$ we have $|n^\wedge A|\geqslant n|A|-n^2+1$, and equality holds if and only if A is an AP (arithmetic progression).

For any torsion-free abelian group G, we confirm Conjecture 1.1 in the case $A_1=\cdots=A_n$. Namely, we have the following theorem.

Theorem 1.4. *Let A be any finite subset of a torsion-free additive abelian group G with $|A|\geqslant 2$. For any integer $n>1$, we have*

$$|n\tilde{}A|\geqslant n|A|-2n+1+\{n\}_2 \tag{1.7}$$

and

$$|n^\circ A|\geqslant n|A|-2n+(-1)^n(1+\{n\}_2). \tag{1.8}$$

When G is a torsion-free abelian group, we determine completely when equality in (1.7) or (1.8) holds.

Theorem 1.5. *Let $n>2$ be an integer, and let A be any finite subset of an additive torsion-free abelian group G with $|A|\geqslant 3$. Then*

$$|n\tilde{}A|=n|A|-2n+1+\{n\}_2 \tag{1.9}$$

if and only A is an AP (arithmetic progression). Also,

$$|n^\circ A|=n|A|-2n+(-1)^n(1+\{n\}_2) \tag{1.10}$$

if and only if A is an AP, or $k = 3$ and $n = 5$.

2. Proofs of Theorem 1.1 and Corollary 1.1

For a polynomial $P(x_1, \ldots, x_n)$ over a field, and nonnegative integers $k_1, \ldots, k_n$ as usual we write $[x^{k_1} \cdots x_n^{k_n}]P(x_1, \ldots, x_n)$ to mean the coefficient of $x^{k_1} \cdots x_n^{k_n}$ in $P(x_1, \ldots, x_n)$.

The following lemma is essentially Theorem 2.1 of [3] although its original form deals with $F = \mathbb{Z}/p\mathbb{Z}$ with p prime, the reader may also consult [12] for a proof via Alon's Combinatorial Nullstellensatz [1].

Lemma 2.1. *Let F be any field, and let $A_1, \ldots, A_n$ be finite nonempty subsets of F. Let $f(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n] \setminus \{0\}$ with $\deg f \leqslant \sum_{i=1}^n (|A_i| - 1)$. If*

$$[x_1^{|A_1|-1} \ldots x_n^{|A_n|-1}] f(x_1, \ldots, x_n)(x_1 + \cdots + x_n)^{\sum_{i=1}^n (|A_i|-1) - \deg f} \neq 0,$$

then we have

$$|\{a_1 + \cdots + a_n : a_i \in A_i, f(a_1, \ldots, a_n) \neq 0\}| \geqslant \sum_{i=1}^n (|A_i| - 1) - \deg f + 1.$$

The following lemma is essentially due to N. Alon, M.B. Nathanson and I.Z. Ruzsa [2, 3].

Lemma 2.2. *If A and B are finite subsets of a field F with $0 < |A| < |B|$, then*

$$|A \dot{+} B| \geqslant \min\{p(F),\ |A| + |B| - 2\}. \tag{2.1}$$

Lemma 2.3. *For any $k_1, k_2, k_3 \in \mathbb{Z}^+$, we have*

$$\begin{aligned} &[x_1^{k_1} x_2^{k_2} x_3^{k_3}](x_1 - x_2)(x_2 - x_3)(x_1 + x_2 + x_3)^{k_1+k_2+k_3-2} \\ =&\frac{(k_1 + k_2 + k_3 - 2)!}{k_1! k_2! k_3!}(k_2 + (k_2 - k_1)(k_3 - k_2)). \end{aligned} \tag{2.2}$$

Proof. Note that $(x_1 - x_2)(x_2 - x_3) = x_1x_2 - x_1x_3 + x_2x_3 - x_2^2$. With the aid of the multi-nomial theorem, we see that

$$\begin{aligned} &[x_1^{k_1} x_2^{k_2} x_3^{k_3}](x_1x_2 - x_1x_3 + x_2x_3 - x_2^2)(x_1 + x_2 + x_3)^{k_1+k_2+k_3-2} \\ =& \binom{k_1 + k_2 + k_3 - 2}{k_1 - 1, k_2 - 1, k_3} - \binom{k_1 + k_2 + k_3 - 2}{k_1 - 1, k_2, k_3 - 1} + \binom{k_1 + k_2 + k_3 - 2}{k_1, k_2 - 1, k_3 - 1} - \binom{k_1 + k_2 + k_3 - 2}{k_1, k_2 - 2, k_3} \\ =& \frac{(k_1 + k_2 + k_3 - 2)!}{k_1! k_2! k_3!}(k_1k_2 - k_1k_3 + k_2k_3 - k_2(k_2 - 1)) \\ =& \frac{(k_1 + k_2 + k_3 - 2)!}{k_1! k_2! k_3!}(k_2 + (k_2 - k_1)(k_3 - k_2)). \end{aligned}$$

This proves (2.2). □

Lemma 2.4. *Let F be any field, and let A_1, A_2, A_3 be finite subsets of F with $|A_1|, |A_3| \geqslant 2$ and $|A_2| - |A_1| \in \{0, 1\}$. Suppose that $p(F) \geqslant \sum_{i=1}^3 |A_i| - 4$. Then we have*

$$|L(A_1, A_2, A_3)| \geqslant \sum_{i=1}^3 |A_i| - 4. \tag{2.3}$$

Proof. Set $k_i = |A_i| - 1$ for $i = 1, 2, 3$. In light of Lemma 2.1, it suffices to prove that $he \neq 0$, where e is the identity of F, and h is the coefficient of $x_1^{k_1} x_2^{k_2} x_3^{k_3}$ in the polynomial

$$(x_1 - x_2)(x_2 - x_3)(x_1 + x_2 + x_3)^{k_1+k_2+k_3-2} \in \mathbb{Z}[x].$$

Let $\delta = |A_2| - |A_1|$. Then $k_2 - k_1 = \delta \in \{0, 1\}$. In light of (2.2), we have

$$h = \frac{(k_1 + k_2 + k_3 - 2)! k_{2+\delta}}{k_1! k_2! k_3!}.$$

Since $p(F) \geqslant \sum_{i=1}^3 (|A_i| - 1) - 1 = k_1 + k_2 + k_3 - 1 > k_{2+\delta}$, we clearly have $he \neq 0$ as desired. This concludes the proof. □

Proof of Theorem 1.1. (i) When $p(F) \geqslant \sum_{i=1}^3 |A_i| - 4$, the conclusion follows from Lemma 2.4.

Below we assume that $p(F) = p < \sum_{i=1}^3 |A_i| - 4$.

Case 1. $p = 2$.

In this case, $|A_1| + |A_2| > p + 4 - |A_3| = 6 - |A_3|$.

Suppose $|A_3| = 2$. Then $|A_1| + |A_2| > 4$ and hence $|A_2| \geqslant 3$. Let a_1 and a_1' be two distinct elements of A_1, and choose $a_2 \in A_2$ different from a_1 and a_1'. Also, take $a_3 \in A_3$ with $a_3 \neq a_2$. Then $a_1 + a_2 + a_3$ and $a_1' + a_2 + a_3$ are distinct elements of $L(A_1, A_2, A_3)$ and hence

$$|L(A_1, A_2, A_3)| \geqslant 2 = p = \min\{p, |A_1| + A_2| + |A_3| - 4\}.$$

Now assume $|A_3| \geqslant 3$. Take $a_1 \in A_1$ and choose $a_2 \in A_2$ with $a_2 \neq a_1$. As $|A_3| \geqslant 3$, there are two distinct elements a_3 and a_3' of A_3 different from a_2. Thus $a_1 + a_2 + a_3$ and $a_1 + a_2 + a_3'$ are distinct elements of $L(A_1, A_2, A_3)$, and hence $|L(A_1, A_2, A_3)| \geqslant 2 = \min\{p, |A_1| + |A_2| + |A_3| - 4\}$.

Case 2. $p \neq 2$ and $|A_3| = 2$.

In this case, $|A_1| + |A_2| > p + 4 - |A_3| = p + 2$. Let b be an element of A_3. We claim that

$$|A_1 \dot{+} (A_2 \setminus \{b\})| \geqslant p. \tag{2.4}$$

Subcase 2.1. $b \in A_2$.

By Lemma 2.2, if $|A_1| = |A_2|$ then

$$|A_1 \dot{+} (A_2 \setminus \{b\})| \geqslant \min\{p, |A_1| + |A_2 \setminus \{b\}| - 2\} = \min\{p, |A_1| + |A_2| - 3\} = p.$$

When $|A_2| = |A_1| + 1$, we take $a \in A_1$ and then by Lemma 2.2 we get

$$\begin{aligned} |A_1 \dot{+} A_2 \setminus \{b\}| &\geqslant |(A_1 \setminus \{a\}) \dot{+} (A_2 \setminus \{b\})| \\ &\geqslant \min\{p, |A_1 \setminus \{a\}| + |A_2 \setminus \{b\}| - 2\} = \min\{p, |A_1| + |A_2| - 4\}. \end{aligned}$$

As $|A_1|+|A_2|-4 \geqslant p-1$ and $|A_2| \not\equiv |A_1| \pmod 2$, we must have $|A_1|+|A_2| \geqslant p+4$ and hence $|A_1 \dot{+} A_2 \setminus \{b\}| \geqslant p$.

Subcase 2.2. $b \notin A_2$.

When $|A_1| = |A_2|$, we take $c \in A_2$, and hence by Lemma 2.2 we have

$$|A_1 \dot{+} (A_2 \setminus \{b\})| \geqslant |A_1 \dot{+} (A_2 \setminus \{c\})| \geqslant \min\{p, |A_1|+|A_2 \setminus \{c\}|-2\} = \min\{p, |A_1|+|A_2|-3\} = p.$$

If $|A_2| = |A_1|+1$, then by Lemma 2.2 we have

$$|A_1 \dot{+} (A_2 \setminus \{b\})| = |A_1 \dot{+} A_2| \geqslant \min\{p, |A_1|+|A_2|-2\} = p.$$

By our discussion of subcases 2.1 and 2.2, we see that (2.4) holds. For any $x \in A_1 \dot{+} (A_2 \setminus \{b\})$, we may write $x = a_1 + a_2$ with $a_1 \in A_1$, $a_2 \in A_2$ and $a_1 \neq a_2 \neq b$ and thus $x+b \in L(A_1, A_2, A_3)$. Combining this with (2.4), we obtain

$$|L(A_1, A_2, A_3)| \geqslant |A_1 \dot{+} (A_2 \setminus \{b\})| \geqslant p = \min\{p,\ |A_1|+|A_2|+|A_3|-4\}.$$

Case 3. $p \geqslant 3$ and $|A_3| \geqslant 3$.

If $|A_2| \leqslant (p+1)/2$, then $3 \leqslant p+4-(|A_1|+|A_2|) < |A_3|$ and so we may take $A_3' \subseteq A_3$ with $|A_3'| = p+4-(|A_1|+|A_2|)$, hence by Lemma 2.4 we have

$$|L(A_1, A_2, A_3)| \geqslant |L(A_1, A_2, A_3')| \geqslant |A_1|+|A_2|+|A_3'|-4 = p = \min\{p,\ |A_1|+|A_2|+|A_3|-4\}.$$

Below we assume that $|A_2| > (p+1)/2$. We may take $A_1' \subseteq A_1$ and $A_2' \subseteq A_2$ with $|A_1'| = |A_2'| = (p+1)/2$, and also take $A_3' \subseteq A_3$ with $|A_3'| = 3$. Note that $|A_1'|+|A_2'|+|A_3'|-4 = p$. Applying Lemma 2.4 we obtain

$$|L(A_1, A_2, A_3)| \geqslant |L(A_1', A_2', A_3')| \geqslant p = \min\{p, |A_1|+|A_2|+|A_3|-4\}.$$

(ii) Now we turn to prove part (ii) of Theorem 1.1. Since the field $\mathbb{R}$ of real numbers is an infinite dimensional vector space over the field $\mathbb{Q}$ of rational numbers, any r linearly independent real numbers generate a subgroup isomorphic to $\mathbb{Z}^r$. Thus, without loss of generality, we may suppose that G is the additive group of the field $\mathbb{R}$.

Let $k_i = |A_i| - 1$ for $i = 1, 2, 3$. Then $1 \leqslant k_1 \leqslant k_2 \leqslant k_3$ and hence

$$[x_1^{k_1} x_2^{k_2} x_3^{k_3}](x_1 - x_2)(x_2 - x_3)(x_1 + x_2 + x_3)^{k_1+k_2+k_3-2} > 0$$

by (2.2). Thus, applying Lemma 2.1 we see that

$$|L(A_1, A_2, A_3)| \geqslant \sum_{i=1}^{3} k_i - 1 = |A_1| + |A_2| + |A_3| - 4.$$

In view of the above, we have completed the proof of Theorem 1.1. □

Proof of Corollary 1.1. Applying Theorem 1.1(i) with $F = \mathbb{F}_p$ and $A_1 = A_2 = A_3 = A$, we get

$$|3\tilde{}A| \geqslant \min\{p, 3|A|-4\}.$$

As $|A| \geqslant \lfloor p/3 \rfloor + 2$, we have $3|A|-4 \geqslant 3\lfloor p/3 \rfloor + 2 \geqslant p$. Thus $|3\tilde{}A| \geqslant p$ and hence $3\tilde{}A = \mathbb{F}_p$. This concludes the proof. □

3. Proofs of Theorems 1.2 and 1.3

The following lemma is essentially due to Q.-H. Hou and Z.-W. Sun [7], and a generalization was given by Sun and Y.-N. Yeh [14, Lemma 2.1].

Lemma 3.1. *Let*

$$P(x_1,\ldots,x_n)=\sum_{\substack{j_1,\ldots,j_n\geqslant 0\\ j_1+\cdots+j_n=m}} c_{j_1,\ldots,j_n}x_1^{j_1}\cdots x_n^{j_n}\in\mathbb{C}[x_1,\ldots,x_n]$$

and

$$\mathcal{L}(P)(x)=\sum_{\substack{j_1,\ldots,j_n\geqslant 0\\ j_1+\cdots+j_n=m}} c_{j_1,\ldots,j_n}(x)_{j_1}\cdots(x)_{j_n}.$$

Suppose that $0\leqslant \deg P\leqslant kn$ *with* $k\in\mathbb{N}$. *Then*

$$[x_1^k\cdots x_n^k]P(x_1,\ldots,x_n)(x_1+\cdots+x_n)^{kn-\deg P}=\frac{(kn-\deg P)!}{(k!)^n}\mathcal{L}(P)(k).$$

Lemma 3.2. *Let*

$$P_n(x_1,\ldots,x_n)=(x_1-x_2)(x_2-x_3)\cdots(x_{n-1}-x_n)(x_n-x_1)$$

with n *even. Then we have*

$$\mathcal{L}(P_n)(x)=2x^{n/2}. \tag{3.1}$$

Proof. Write

$$P_n(x_1,\ldots,x_n)=\sum_{\substack{I,J\subseteq\{1,\ldots,n\}\\ I\cap J=\emptyset\ \&\ |I|=|J|}} c(I,J)\prod_{i\in I}x_i^2\times\prod_{j\in J}x_j^0\times\prod_{\substack{k=1\\ k\notin I\cup J}}^{n}x_k$$

with $c(I,J)\in\mathbb{Z}$. Then

$$\mathcal{L}(P_n)(x)=\sum_{\substack{I,J\subseteq\{1,\ldots,n\}\\ I\cap J=\emptyset\ \&\ |I|=|J|}}\prod_{i\in I}(x)_2\times\prod_{\substack{k=1\\ k\notin I\cup J}}^{n}(x)_1=\sum_{m=0}^{n/2}c_m(x)_2^m(x)_1^{n-2m}=\sum_{m=0}^{n/2}c_m x^{n-m}(x-1)^m, \tag{3.2}$$

where

$$c_m=\sum_{\substack{I,J\subseteq\{1,\ldots,n\}\\ I\cap J=\emptyset\ \&\ |I|=|J|=m}} c(I,J).$$

Let $I,J\subseteq\{1,\ldots,n\}$ with $I\cap J=\emptyset$ and $|I|=|J|=m$. Suppose that $j,k\in J$, $j<k$ and $s\notin J$ for all $j<s<k$. Then there are only $k-j-1$ choices of the corresponding terms chosen from

$$(x_j-x_{j+1})(x_{j+1}-x_{j+2})\ldots(x_{k-2}-x_{k-1})(x_{k-1}-x_k),$$

which are

$$\prod_{j<r\leqslant s}(-x_r)\times\prod_{s\leqslant t<k}x_t=(-1)^{s-j}x_s^2\prod_{\substack{j<r<k\\ r\neq s}}x_r\quad(j<s<k).$$

Note that

$$\sum_{j<s<k}\mathcal{L}\bigg((-1)^{s-j}x_s^2\prod_{\substack{j<r<k\\ r\neq s}}x_r\bigg)=\sum_{j<s<k}(-1)^{s-j}x(x-1)\prod_{\substack{j<r<k\\ r\neq s}}x=(\{k-j\}_2-1)(x-1)x^{k-j-1}$$

which vanishes if $j\not\equiv k\pmod 2$.

Let $J\subseteq\{1,\ldots,n\}$ with $|J|=m$. Write $J=\{j_1,j_2,\ldots,j_m\}$ with $j_1<\cdots<j_m$. Consider the the polynomial P_J given by

$$\begin{aligned}&\prod_{i=1}^{m-1}\bigg(\sum_{j_i<s<j_{i+1}}\prod_{j_i<r\leqslant s}(-x_r)\times\prod_{s\leqslant t<j_{i+1}}x_t\bigg)\\&\times\bigg(\sum_{j_m<s\leqslant n}\prod_{j_m<r\leqslant s}(-x_r)\times\prod_{\substack{s\leqslant t\leqslant n\\ \text{or }\ 1\leqslant t<j_1}}x_t+\sum_{1\leqslant s<j_1}\prod_{\substack{j_m<r\leqslant n\\ \text{or }\ 1\leqslant r\leqslant s}}(-x_r)\times\prod_{s\leqslant t<j_1}x_t\bigg).\end{aligned}$$

In the spirit of the last paragraph, $j_1\equiv j_2\equiv\cdots\equiv j_m\pmod 2$, and we have

$$\mathcal{L}(P_J)(x)=\prod_{i=1}^{m-1}\big(-(x-1)x^{j_{i+1}-j_i-1}\big)\times\big(-(x-1)x^{(n+j_1)-j_m-1}\big)=(-1)^m(x-1)^mx^{n-m}.$$

Thus

$$\sum_{\substack{I\subseteq\{1,\ldots,n\}\setminus J\\ |I|=m}}c(I,J)=(-1)^m.$$

By the last paragraph, we have

$$\begin{aligned}c_m&=\sum_{\substack{J\subseteq\{2s:\ s=1,\ldots,n/2\}\\ |J|=m}}\sum_{\substack{I\subseteq\{1,\ldots,n\}\setminus J\\ |I|=m}}c(I,J)+\sum_{\substack{J\subseteq\{2s-1:\ s=1,\ldots,n/2\}\\ |J|=m}}\sum_{\substack{I\subseteq\{1,\ldots,n\}\setminus J\\ |I|=m}}c(I,J)\\&=\binom{n/2}{m}(-1)^m+\binom{n/2}{m}(-1)^m=(-1)^m2\binom{n/2}{m}.\end{aligned}$$

Combining this with (3.2) we get

$$\mathcal{L}(P_n)(x)=\sum_{m=0}^{n/2}(-1)^m2\binom{n/2}{m}x^{n-m}(x-1)^m=2x^{n/2}$$

by the binomial theorem. This concludes our proof. □

Proof of Theorem 1.2. It is apparent that

$$L(A_1,\ldots,A_n)\supseteq C(A_1,\ldots,A_n).$$

So, we only to show the second inequality of (1.5).

Let $k=|A_1|-1=\cdots=|A_n|-1$. If $k=1$, then the second equality of (1.5) holds trivially. Below we assume that $k\geqslant 2$. By Lemmas 3.1 and 3.2, we have the identity

$$[x_1^k\ldots x_n^k](x_1-x_2)\cdots(x_{n-1}-x_n)(x_n-x_1)(x_1+\cdots+x_n)^{(k-1)n}=\frac{((k-1)n)!}{k!^n}2k^{n/2}.\quad(3.3)$$

Let h denote the right-hand side of (3.3) which is an integer. Let e be the identity of F. As $p(F) > (k-1)n \geqslant \max\{k, 2\}$, we see that the coefficient of $x_1^k \ldots x_n^k$ in the polynomial

$$(x_1 - x_2)\cdots(x_{n-1} - x_n)(x_n - x_1)(x_1 + \cdots + x_n)^{(k-1)n} \in F[x_1, \ldots, x_n]$$

coincides with he which is nonzero. Therefore, by Lemma 2.1 we have

$$|C(A_1, \ldots, A_n)| \geqslant (k-1)n + 1 = \sum_{i=1}^{n} |A_i| - 2n + 1.$$

This concludes our proof. □

Lemma 3.3. *For any odd integer $n > 1$ and the polynomial*

$$Q_n(x_1, \ldots, x_n) = (x_1 - x_2)(x_2 - x_3)\cdots(x_{n-1} - x_n),$$

we have

$$\mathcal{L}(Q_n)(x) = x^{(n-1)/2}. \tag{3.4}$$

Proof. We use induction on n.

Clearly

$$Q_3(x_1, x_2, x_3) = (x_1 - x_2)(x_2 - x_3) = x_1x_2 - x_1x_3 + x_2x_3 - x_2^2$$

and hence

$$\mathcal{L}(Q_3)(x) = xx - xx + xx - (x)_2 = x^2 - x(x-1) = x^{(3-1)/2}.$$

Thus (3.4) holds when $n = 3$.

Now let n be an odd integer greater than 3, and assume that $\mathcal{L}(Q_{n-2})(x) = x^{(n-3)/2}$. Write

$$Q_n(x_1, \ldots, x_n) = \sum_{i_1, \ldots, i_n \in \mathbb{N}} c_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n} \text{ with } c_{i_1,\ldots,i_n} \in \mathbb{Z},$$

and define

$$P_{n+1}(x_1, \ldots, x_n, x_{n+1}) = Q_n(x_1, \ldots, x_n)(x_n - x_{n+1})(x_{n+1} - x_1).$$

Then

$$\begin{aligned} P_{n+1}(x_1, \ldots, x_{n+1}) &= \sum_{i_1, \ldots, i_n \in \mathbb{N}} c_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n} (x_n x_{n+1} - x_1 x_n + x_1 x_{n+1} - x_{n+1}^2) \\ &= \sum_{i_1, \ldots, i_n \in \mathbb{N}} c_{i_1,\ldots,i_n} \left(x_1^{i_1} \cdots x_{n-1}^{i_{n-1}} x_n^{i_n+1} x_{n+1} - x_1^{i_1+1} x_2^{i_2} \cdots x_{n-1}^{i_{n-1}} x_n^{i_n+1} \right) \\ &\quad + \sum_{i_1, \ldots, i_n \in \mathbb{N}} c_{i_1,\ldots,i_n} \left(x_1^{i_1+1} x_2^{i_2} \cdots x_n^{i_n} x_{n+1} - x_1^{i_1} \cdots x_n^{i_n} x_{n+1}^2 \right) \end{aligned}$$

and hence

$$\mathcal{L}(P_{n+1})(x) = \sum_{i_1, \ldots, i_n \in \mathbb{N}} c_{i_1,\ldots,i_n} R(i_1, \ldots, i_n, x),$$

where

$$R(i_1, \ldots, i_n, x) = (x)_{i_1} \cdots (x)_{i_{n-1}} (x)_{i_n+1} x - (x)_{i_1+1} (x)_{i_2} \cdots (x)_{i_{n-1}} (x)_{i_n+1}$$

$$\begin{aligned}&+(x)_{i_1+1}(x)_{i_2}\cdots(x)_{i_n}x-(x)_{i_1}\cdots(x)_{i_n}(x)_2\\&=(x)_{i_1}\cdots(x)_{i_n}\left(x(x-i_n)-(x-i_1)(x-i_n)+x(x-i_1)-x(x-1)\right)\\&=(x)_{i_1}\cdots(x)_{i_n}(x-i_1i_n).\end{aligned}$$

Thus

$$\mathcal{L}(P_{n+1})(x)=x\mathcal{L}(Q_n)(x)-\mathcal{L}(Q_n^*)(x), \tag{3.5}$$

where

$$Q_n^*(x_1,\ldots,x_n)=\sum_{i_1,\ldots,i_n\in\mathbb{N}}c_{i_1,\ldots,i_n}x_1x_n\frac{\partial^2}{\partial x_1\partial x_n}(x_1^{i_1}\cdots x_n^{i_n})=x_1x_n\frac{\partial^2}{\partial x_1\partial x_n}Q_n(x_1,\ldots,x_n).$$

Observe that

$$\begin{aligned}x_1x_n\frac{\partial^2}{\partial x_1\partial x_n}Q_n(x_1,\ldots,x_n)&=x_1x_n\frac{\partial^2}{\partial x_1\partial x_n}(x_1-x_2)\cdots(x_{n-1}-x_n)\\&=x_1x_n\left((x_2-x_3)\cdots(x_{n-2}-x_{n-1})(-1)\right)\end{aligned}$$

and thus

$$\mathcal{L}(Q_n^*)(x)=-x^2\mathcal{L}(Q_{n-2})(x).$$

Combining this with (3.5), we obtain the relation

$$\mathcal{L}(P_{n+1})(x)=x\mathcal{L}(Q_n)(x)+x^2\mathcal{L}(Q_{n-2})(x). \tag{3.6}$$

Note that $\mathcal{L}(Q_{n-2})(x)=x^{(n-3)/2}$ by the induction hypothesis, and $\mathcal{L}(P_{n+1})(x)=2x^{(n+1)/2}$ by Lemma 3.2. Therefore,

$$x\mathcal{L}(Q_n)(x)=2x^{(n+1)/2}-x^2x^{(n-3)/2}=x^{(n+1)/2}$$

and hence $\mathcal{L}(Q_n)(x)=x^{(n-1)/2}$ as desired.

In view of the above, we have completed the induction proof of Lemma 3.3.

Proof of Theorem 1.3. Let $k=|A_1|-1=\cdots=|A_n|-1$. By Lemmas 3.1 and 3.3, we have

$$[x_1^k\cdots x_n^k](x_1-x_2)\cdots(x_{n-1}-x_n)(x_1+\cdots+x_n)^{(k-1)n+1}=\frac{((k-1)n+1)!}{(k!)^n}\times k^{(n-1)/2}. \tag{3.7}$$

Let h be the integer given by the right-hand side of (3.7), and let e be the identity of the field F. Clearly, the coefficient of $x_1^k\cdots x_n^k$ in the polynomial

$$(x_1-x_2)\cdots(x_{n-1}-x_n)(x_1+\cdots+x_n)^{(k-1)n+1}\in F[x_1,\ldots,x_n]$$

is he, which is nonzero since $p(F)>(k-1)n+1\geqslant k$. Applying Lemma 2.1, we get

$$|L(A_1,\ldots,A_n)|\geqslant(k-1)n+2=\sum_{i=1}^n|A_i|-2n+2.$$

This concludes our proof. □

4. Proofs of Theorems 1.4 and 1.5

For any finite subset A of a torsion-free additive abelian group G, the subgroup of G generated by A is a finitely generated torsion-free abelian group. Thus, by the first paragraph in the proof of Theorem 1.1 (ii), without loss of generality we may simply assume that G in Theorems 1.4 and 1.5 is just the additive group of the field $\mathbb{R}$ of real numbers.

Proof of Theorem 1.4 with $G=\mathbb{R}$. When n is even, we obtain the desired result by applying Theorem 1.2 with $F=\mathbb{R}$ and $A_1=\cdots=A_n=A$. Similarly, when n is odd we have (1.7) by applying Theorem 1.3.

Below we assume that n is odd, and want to prove (1.8). For convenience, we write $A=\{a_1,a_2,\ldots,a_k\}$ with $a_1<a_2<\ldots<a_k$.

Clearly (1.8) holds trivially when $k=2$. Below we assume that $k\geqslant 3$.

Observe that

$$\begin{aligned}&a_1+a_2+a_1+a_2+\cdots+a_1+a_2+a_3\\&<a_1+a_2+a_1+a_2+\cdots+a_1+a_2+a_4<\cdots\\&<a_1+a_2+a_1+a_2+\cdots+a_1+a_2+a_k\end{aligned}$$

for $k\geqslant 4$, and

$$\begin{aligned}&a_1+a_i+a_1+a_i+\cdots+a_1+a_i+a_k\\&<a_1+a_{i+1}+a_1+a_i+\cdots+a_1+a_i+a_k<\cdots\\&<a_1+a_{i+1}+a_1+a_{i+1}+\cdots+a_1+a_{i+1}+a_k\end{aligned}$$

for $2\leqslant i\leqslant k-2$. Also,

$$\begin{aligned}&a_1+a_{k-1}+a_1+a_{k-1}+\cdots+a_1+a_{k-1}+a_1+a_{k-1}+a_k\\&<a_1+a_k+a_1+a_{k-1}+\cdots+a_1+a_{k-1}+a_1+a_{k-1}+a_k<\cdots\\&<a_1+a_k+a_1+a_k+\cdots+a_1+a_k+a_1+a_{k-1}+a_k,\end{aligned}$$

and

$$\begin{aligned}&a_i+a_k+a_i+a_k+\cdots+a_i+a_k+a_i+a_{k-1}+a_k\\&<a_{i+1}+a_k+a_i+a_k+\cdots+a_i+a_k+a_i+a_{k-1}+a_k<\cdots\\&<a_{i+1}+a_k+a_{i+1}+a_k+\cdots+a_{i+1}+a_k+a_{i+1}+a_{k-1}+a_k\end{aligned}$$

for $1\leqslant i\leqslant k-3$. Note also that

$$\begin{aligned}&a_{k-2}+a_k+a_{k-2}+a_k+\cdots+a_{k-2}+a_k+a_{k-2}+a_{k-1}+a_k\\&<a_{k-1}+a_k+a_{k-2}+a_k+\cdots+a_{k-2}+a_k+a_{k-2}+a_{k-1}+a_k<\cdots\\&<a_{k-1}+a_k+a_{k-1}+a_k+\cdots+a_{k-1}+a_k+a_{k-2}+a_{k-1}+a_k.\end{aligned}$$

So we have found

$$\begin{aligned}&1+(k-3)+2\times\left(\frac{n-3}{2}(k-2)+(k-3)\right)\\&=(k-2)n-2=n|A|-2n+(-1)^n(1+\{n\}_2)\end{aligned}$$

different elements of $n^\circ A$. Therefore (1.8) is valid.

In view of the above, we have completed our proof of Theorem 1.4. □

Proof of Theorem 1.5 with $G=\mathbb{R}$. Write $A=\{a_1,a_2,\ldots,a_k\}$ with $a_1<a_2<\cdots<a_k$.

(i) If A is an AP with $|A|=k$, then for $A_0=\{0,\ldots,k-1\}$ we clearly have

$$|n\tilde{}A|=|n\tilde{}A_0| \text{ and } |n^\circ A|=|n^\circ A_0|.$$

If $n=2m$ with $m\in\mathbb{Z}^+$, then

$$n\tilde{}A_0=n^\circ A_0=\{m,m+1,\ldots,m(2k-3)\}$$

with $m=0+1+0+1+\cdots+0+1$ and

$$m(2k-3)=(k-1)+(k-2)+\cdots+(k-1)+(k-2),$$

and hence

$$|n\tilde{}A|=|\{m,m+1,\ldots,m(2k-3)\}|=m(2k-3)-(m-1)=2m(k-2)+1=n|A|-2n+1.$$

If $n=2m+1$ with $m\in\mathbb{Z}^+$, then

$$n\tilde{}A_0=\{m,m+1,\ldots,m(2k-3)+k-1\}$$

with $m=0+1+0+1+\cdots+0+1+0$ and

$$m(2k-3)=(k-1)+(k-2)+\cdots+(k-1)+(k-2)+(k-1),$$

hence

$$|n\tilde{}A|=|\{m,m+1,\ldots,m(2k-3)+k-1\}|=(2m+1)k-4m=kn-2(n-1)=|A|n-2n+1+\{n\}_2.$$

For $n=2m+1$ with $m\in\mathbb{Z}^+$, we have

$$n^\circ A_0=\{m+2,m+3,\ldots,m(2k-3)+k-3\}$$

with $m=0+1+0+1+\cdots+0+1+2$ and

$$m(2k-3)+k-3=(k-1)+(k-2)+\cdots+(k-1)+(k-2)+(k-1)+(k-3),$$

hence

$$|n^\circ A|=|\{m+2,m+3,\ldots,m(2k-3)+k-3\}|=(2m+1)k-4m-4=|A|n-2n+(-1)^n(1+\{n\}_2).$$

Thus both (1.9) and (1.10) hold if A is an AP.

Now we consider the case $n=5$ and $A=\{a_1,a_2,a_3\}$ with $a_1<a_2<a_3$. Clearly, any element of $5^\circ A$ can be written as $\sum_{k=1}^3 n_k a_k$ with $n_1,n_2,n_3\in\mathbb{N}$ and $n_1+n_2+n_3=5$. Note that $n_k\in\{1,2\}$ for all $k=1,2,3$ (otherwise we get a contradiction in view of the definition of $5^\circ A$). Thus two of n_1,n_2,n_3 are 2 and the remaining one is 1. Hence

$$\begin{aligned}5^\circ A&=\{a_1+a_2+a_1+a_2+a_3,\ a_1+a_3+a_1+a_2+a_3,\ a_2+a_3+a_1+a_2+a_3\}\\&=\{2a_1+2a_2+a_3,\ 2a_1+2a_3+a_2,\ 2a_2+2a_3+a_1\}\end{aligned}$$

contains exactly 3 elements, and so (1.10) holds for $k=3$ and $n=5$.

(ii) Now we write $A=\{a_1,\ldots,a_k\}$ with $a_1<\cdots<a_k$. If (1.10) holds for $n=3$, then $|3^\wedge A|=|3^\circ A|=3k-8$ and hence A is an AP by Nathanson [9]. Below we divide our remaining discussions into four cases.

Case 1. $k\geqslant 4$ and $2\mid n$.

In this case, both the right-hand sides of (1.9) and (1.10) are $kn-2n+1$. As $n\tilde{A}\supseteq n^\circ A$, if $|n\tilde{A}|=kn-2n+1$, then $|n^\circ A|=kn-2n+1$ by (1.8).

Now we suppose that $|n^\circ A|=kn-2n+1$. Note that

$$\begin{aligned}&a_1+a_i+a_1+a_i+\cdots+a_1+a_i\\<\ &a_1+a_{i+1}+a_1+a_i+\cdots+a_1+a_i<\ldots\\<\ &a_1+a_{i+1}+a_1+a_{i+1}+\cdots+a_1+a_{i+1}\end{aligned}$$

for all $i\in\{2,3,\ldots,k-1\}$ and

$$\begin{aligned}&a_i+a_k+a_i+a_k+\cdots+a_i+a_k\\<\ &a_{i+1}+a_k+a_i+a_k+\cdots+a_i+a_k<\ldots\\<\ &a_{i+1}+a_k+a_{i+1}+a_k+\cdots+a_{i+1}+a_k\end{aligned}$$

for all $i\in\{1,2,\ldots,k-2\}$. Therefore we get

$$1+\frac{n}{2}(k-2)\times 2=(k-2)n+1$$

different elements of $n^\circ A$. They are all the elements of A since $|n^\circ A|=(k-2)n+1$.

For any $i\in\{3,\ldots,k-1\}$, in $n^\circ A$ we have

$$\begin{aligned}&a_1+a_i+a_1+a_i+\cdots+a_1+a_i+a_1+a_{i-1}\\<\ &a_1+a_i+a_1+a_i+\cdots+a_1+a_i+a_1+a_i\\<\ &a_1+a_{i+1}+a_1+a_i+\cdots+a_1+a_i+a_1+a_i\end{aligned}$$

and

$$\begin{aligned}&a_1+a_i+a_1+a_i+\cdots+a_1+a_i+a_1+a_{i-1}\\<\ &a_1+a_{i+1}+a_1+a_i+\cdots+a_1+a_i+a_1+a_{i-1}\\<\ &a_1+a_{i+1}+a_1+a_i+\cdots+a_1+a_i+a_1+a_i,\end{aligned}$$

thus

$$a_1+a_i+a_1+a_i+\cdots+a_1+a_i+a_1+a_i=a_1+a_{i+1}+a_1+a_i+\cdots+a_1+a_i+a_1+a_{i-1}$$

and hence $a_{i+1}-a_i=a_i-a_{i-1}$. Similarly, for any $i\in\{2,\ldots,k-2\}$, in $n^\circ A$ we have

$$\begin{aligned}&a_i+a_k+a_i+a_k+\cdots+a_i+a_k+a_{i-1}+a_k\\<\ &a_i+a_k+a_i+a_k+\cdots+a_i+a_k+a_i+a_k\\<\ &a_{i+1}+a_k+a_i+a_k+\cdots+a_i+a_k+a_i+a_k\end{aligned}$$

and

$$\begin{aligned}&a_i+a_k+a_i+a_k+\cdots+a_i+a_k+a_{i-1}+a_k\\<\ &a_{i+1}+a_k+a_i+a_k+\cdots+a_i+a_k+a_{i-1}+a_k\\<\ &a_{i+1}+a_k+a_i+a_k+\cdots+a_i+a_k+a_i+a_k,\end{aligned}$$

and hence $a_{i+1}-a_i=a_i-a_{i-1}$. Therefore $a_2-a_1=a_3-a_2=\ldots=a_k-a_{k-1}$, i.e., A is an AP.

Case 2. $k\geqslant 4$ and $2\nmid n$.

Clearly,

$$\begin{aligned} &a_1+a_i+a_1+a_i+\cdots+a_1+a_i+a_1\\ <\ &a_1+a_{i+1}+a_1+a_i+\cdots+a_1+a_i+a_1<\ldots\\ <\ &a_1+a_{i+1}+a_1+a_{i+1}+\cdots+a_1+a_{i+1}+a_1 \end{aligned}$$

for any $i\in\{2,3,\ldots,k-1\}$, and

$$\begin{aligned} &a_i+a_k+a_i+a_k+\cdots+a_i+a_k+a_i\\ <\ &a_{i+1}+a_k+a_i+a_k+\cdots+a_i+a_k+a_i<\ldots\\ <\ &a_{i+1}+a_k+a_{i+1}+a_k+\cdots+a_{i+1}+a_k+a_{i+1} \end{aligned}$$

for all $i\in\{1,2,\ldots,k-2\}$. Also,

$$\begin{aligned} &a_{k-1}+a_k+a_{k-1}+a_k+\cdots+a_{k-1}+a_k+a_{k-1}\\ <\ &a_k+a_{k-1}+a_k+a_{k-1}+\cdots+a_k+a_{k-1}+a_k. \end{aligned}$$

So we have found

$$1+\frac{n+1}{2}(k-2)+\frac{n-1}{2}(k-2)+1=2+(k-2)n=n|A|-2n+1+\{n\}_2$$

different elements of $n\tilde{}A$. They are all the elements of $n\tilde{}A$ if (1.9) holds.

Now suppose that (1.9) is valid. For any $i\in\{2,\ldots,k-2\}$, in $n\tilde{}A$ we have

$$\begin{aligned} &a_i+a_k+a_i+a_k+\cdots+a_i+a_k+a_{i-1}\\ <\ &a_i+a_k+a_i+a_k+\cdots+a_i+a_k+a_i\\ <\ &a_{i+1}+a_k+a_i+a_k+\cdots+a_i+a_k+a_i \end{aligned}$$

and

$$\begin{aligned} &a_i+a_k+a_i+a_k+\cdots+a_i+a_k+a_{i-1}\\ <\ &a_{i+1}+a_k+a_i+a_k+\cdots+a_i+a_k+a_{i-1}\\ <\ &a_{i+1}+a_k+a_i+a_k+\cdots+a_i+a_k+a_i, \end{aligned}$$

hence

$$a_i+a_k+a_i+a_k+\cdots+a_i+a_k+a_i=a_{i+1}+a_k+a_i+a_k+\cdots+a_i+a_k+a_{i-1}$$

and thus $a_{i+1}-a_i=a_i-a_{i-1}$. Moreover, in $n\tilde{}A$ we have

$$\begin{aligned} &a_{k-1}+a_k+a_{k-1}+a_k+\cdots+a_{k-1}+a_k+a_{k-2}\\ <\ &a_{k-1}+a_k+a_{k-1}+a_k+\cdots+a_{k-1}+a_k+a_{k-1}\\ <\ &a_k+a_{k-1}+a_k+a_{k-1}+\cdots+a_k+a_{k-1}+a_k \end{aligned}$$

and

$$\begin{aligned} &a_{k-1}+a_k+a_{k-1}+a_k+\cdots+a_{k-1}+a_k+a_{k-2}\\ <\ &a_k+a_{k-1}+a_k+a_{k-1}+\cdots+a_k+a_{k-2}+a_k\\ <\ &a_k+a_{k-1}+a_k+a_{k-1}+\cdots+a_k+a_{k-1}+a_k, \end{aligned}$$

thus

$$a_{k-1}+a_k+a_{k-1}+a_k+\cdots+a_{k-1}+a_k+a_{k-1}$$

$$= a_k + a_{k-1} + a_k + a_{k-1} + \cdots + a_k + a_{k-2} + a_k$$

and hence $a_{k-1} - a_{k-2} = a_k - a_{k-1}$.

Assume $n \geqslant 5$. For any $i \in \{3, \ldots, k-1\}$, in $n^\circ A$, by the proof of Theorem 1.4 and the equality (1.10), there is a unique element of $n^\circ A$ between

$a_1+a_i+a_1+a_i+\cdots+a_1+a_i+a_1+a_{i-1}+a_k$ and $a_1+a_{i+1}+a_1+a_i+\cdots+a_1+a_i+a_1+a_i+a_k$.

In $n^\circ A$, we clearly have

$$\begin{aligned} &a_1 + a_i + a_1 + a_i + \cdots + a_1 + a_i + a_1 + a_{i-1} + a_k \\ &< a_1 + a_i + a_1 + a_i + \cdots + a_1 + a_i + a_1 + a_i + a_k \\ &< a_1 + a_{i+1} + a_1 + a_i + \cdots + a_1 + a_i + a_1 + a_i + a_k \end{aligned}$$

and

$$\begin{aligned} &a_1 + a_i + a_1 + a_i + \cdots + a_1 + a_i + a_1 + a_{i-1} + a_k \\ &< a_1 + a_{i+1} + a_1 + a_i + \cdots + a_1 + a_i + a_1 + a_{i-1} + a_k \\ &< a_1 + a_{i+1} + a_1 + a_i + \cdots + a_1 + a_i + a_1 + a_i + a_k. \end{aligned}$$

Thus

$$a_1+a_i+a_1+a_i+\cdots+a_1+a_i+a_1+a_i+a_k = a_1+a_{i+1}+a_1+a_i+\cdots+a_1+a_i+a_1+a_{i-1}+a_k$$

and hence $a_{i+1} - a_i = a_i - a_{i-1}$.

Similarly, for $i \in \{2, \ldots, k-2\}$, by the proof of Theorem 1.4 and the equality (1.10), there is a unique element of $n^\circ A$ between

$a_i+a_k+a_i+a_k+\cdots+a_i+a_k+a_{i-1}+a_{k-1}+a_k$ and $a_{i+1}+a_k+a_i+a_k+\cdots+a_i+a_k+a_i+a_{k-1}+a_k$.

In $n^\circ A$ we have

$$\begin{aligned} &a_i + a_k + a_i + a_k + \cdots + a_i + a_k + a_{i-1} + a_{k-1} + a_k \\ &< a_i + a_k + a_i + a_k + \cdots + a_i + a_k + a_i + a_{k-1} + a_k \\ &< a_{i+1} + a_k + a_i + a_k + \cdots + a_i + a_k + a_i + a_{k-1} + a_k \end{aligned}$$

and

$$\begin{aligned} &a_i + a_k + a_i + a_k + \cdots + a_i + a_k + a_{i-1} + a_{k-1} + a_k \\ &< a_{i+1} + a_k + a_i + a_k + \cdots + a_i + a_k + a_{i-1} + a_{k-1} + a_k \\ &< a_{i+1} + a_k + a_i + a_k + \cdots + a_i + a_k + a_i + a_{k-1} + a_k, \end{aligned}$$

hence

$$\begin{aligned} &a_i + a_k + a_i + a_k + \cdots + a_i + a_k + a_i + a_{k-1} + a_k \\ &= a_{i+1} + a_k + a_i + a_k + \cdots + a_i + a_k + a_{i-1} + a_{k-1} + a_k \end{aligned}$$

and thus $a_{i+1} - a_i = a_i - a_{i-1}$. Therefore $a_2 - a_1 = a_3 - a_2 = \ldots = a_k - a_{k-1}$, i.e., A is an AP.

Case 3. $k = 3$ and $2 \mid n$.

If (1.9) holds then so (1.10). Now suppose that (1.10) holds. In $n^{\circ}A$, we have

$$\begin{aligned} &a_1+a_2+a_1+a_2+\cdots+a_1+a_2\\ <\ &a_1+a_3+a_1+a_2+\cdots+a_1+a_2<\cdots\\ <\ &a_1+a_3+a_1+a_3+\cdots+a_1+a_3\\ <\ &a_2+a_3+a_2+a_3+\cdots+a_2+a_3<\cdots\\ <\ &a_2+a_3+a_2+a_3+\cdots+a_2+a_3, \end{aligned}$$

they give all the $n+1$ elements of $n^{\circ}A$. As

$$\begin{aligned} &a_1+a_3+a_1+a_3+\cdots+a_1+a_3+a_1+a_2\\ <\ &a_1+a_3+a_1+a_3+\cdots+a_1+a_3+a_1+a_3\\ <\ &a_2+a_3+a_1+a_3+\cdots+a_1+a_3+a_1+a_3 \end{aligned}$$

and

$$\begin{aligned} &a_1+a_3+a_1+a_3+\cdots+a_1+a_3+a_1+a_2\\ <\ &a_2+a_3+a_1+a_3+\cdots+a_1+a_3+a_1+a_2\\ <\ &a_2+a_3+a_1+a_3+\cdots+a_1+a_3+a_1+a_3, \end{aligned}$$

we must have

$$a_1+a_3+a_1+a_3+\cdots+a_1+a_3+a_1+a_3=a_2+a_3+a_1+a_3+\cdots+a_1+a_3+a_1+a_2,$$

and hence $a_3-a_2=a_2-a_1$.

Case 4. $k=3$ and $2\nmid n$.

In $n\tilde{A}$, we have

$$\begin{aligned} &a_1+a_2+a_1+a_2+\cdots+a_1+a_2+a_1\\ <\ &a_1+a_3+a_1+a_2+\cdots+a_1+a_2+a_1<\cdots\\ <\ &a_1+a_3+a_1+a_3+\cdots+a_1+a_3+a_1\\ <\ &a_2+a_3+a_1+a_3+\cdots+a_1+a_3+a_1<\cdots\\ <\ &a_2+a_3+a_2+a_3+\cdots+a_2+a_3+a_2\\ <\ &a_3+a_2+a_3+a_2+\cdots+a_3+a_2+a_3. \end{aligned}$$

Suppose that (1.9) holds. Then the above gives a list of all the $n+2$ elements of $n\tilde{A}$.

When $n=3$, in $n\tilde{A}$ we have

$$a_2+a_3+a_1<a_2+a_3+a_2<a_3+a_2+a_3$$

and

$$a_2+a_3+a_1<a_3+a_1+a_3<a_3+a_2+a_3,$$

hence $a_2+a_3+a_2=a_3+a_1+a_3$ and thus $a_2-a_1=a_3-a_2$. When $n\geqslant 5$, as

$$\begin{aligned} &a_1+a_3+a_1+a_3+\cdots+a_1+a_3+a_1+a_2+a_1\\ <&a_1+a_3+a_1+a_3+\cdots+a_1+a_3+a_1+a_3+a_1\\ <&a_2+a_3+a_1+a_3+\cdots+a_1+a_3+a_1+a_3+a_1 \end{aligned}$$

and

$$\begin{aligned}&a_1+a_3+a_1+a_3+\cdots+a_1+a_3+a_1+a_2+a_1\\<&\,a_2+a_3+a_1+a_3+\cdots+a_1+a_3+a_1+a_2+a_1\\<&\,a_2+a_3+a_1+a_3+\cdots+a_1+a_3+a_1+a_3+a_1,\end{aligned}$$

we must have

$$a_1+a_3+a_1+a_3+\cdots+a_1+a_3+a_1+a_3+a_1=a_2+a_3+a_1+a_3+\cdots+a_1+a_3+a_1+a_2+a_1$$

and hence $a_2-a_1=a_3-a_2$.

Assume $n\geqslant 7$ and suppose that (1.10) holds. By the proof of Theorem 1.4 and the equality (1.10), there is a unique element of $n^\circ A$ between

$$a_1+a_3+a_1+a_3+\cdots+a_1+a_3+a_1+a_2+a_1+a_2+a_3$$

and

$$a_2+a_3+a_1+a_3+\cdots+a_1+a_3+a_1+a_3+a_1+a_2+a_3.$$

In $n^\circ A$, we clearly have

$$\begin{aligned}&a_1+a_3+a_1+a_3+\cdots+a_1+a_3+a_1+a_2+a_1+a_2+a_3\\<&\,a_1+a_3+a_1+a_3+\cdots+a_1+a_3+a_1+a_3+a_1+a_2+a_3\\<&\,a_2+a_3+a_1+a_3+\cdots+a_1+a_3+a_1+a_3+a_1+a_2+a_3\end{aligned}$$

and

$$\begin{aligned}&a_1+a_3+a_1+a_3+\cdots+a_1+a_3+a_1+a_2+a_1+a_2+a_3\\<&\,a_2+a_3+a_1+a_3+\cdots+a_1+a_3+a_1+a_2+a_1+a_2+a_3\\<&\,a_2+a_3+a_1+a_3+\cdots+a_1+a_3+a_1+a_3+a_1+a_2+a_3.\end{aligned}$$

Thus

$$\begin{aligned}&a_1+a_3+a_1+a_3+\cdots+a_1+a_3+a_1+a_3+a_1+a_2+a_3\\=&\,a_2+a_3+a_1+a_3+\cdots+a_1+a_3+a_1+a_2+a_1+a_2+a_3,\end{aligned}$$

and hence $a_2-a_1=a_3-a_2$ as desired.

In view of the above, we have finished our proof of Theorem 1.5. □

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 Erdos-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 and H. Heilbronn, On the addition of residue classes modulo p, Acta Arith. **9**(1964), 149–159.

[7] Q.-H. Hou and Z.-W. Sun, *Restricted sums in a field*, Acta Arith. **102** (2002), 239–249.

[8] G. Károlyi, *The Erdős-Heilbronn problem in abelian groups*, Israel J. Math. **139** (2004), 349–359.

[9] M. B. Nathanson, *Inverse theorems for subset sums*, Trans. Amer. Math. Soc. **347** (1995), 1409–1418.
[10] H. Pan and Z.-W. Sun, *A new extension of the Erdos-Heilbronn conjecture*, J. Combin. Theory Ser. A **116** (2009), 1374–1381.
[11] Z.-W. Sun, *Restricted sums of subsets of* $\mathbb{Z}$, Acta Arith. **99** (2001), 41–60.
[12] Z.-W. Sun, *A survey of problems and results on restricted sumsets*, in: Number Theory (S. Kanemitsu and J.-Y. Liu, eds.), World Sci., Singapore, 2007, pp. 190-213.
[13] Z.-W. Sun, Sequence A357130 in OEIS (On-Line Encyclopedia of Integer Sequences), 2022. Website: `http://oeis.org/A357130`.
[14] Z.-W. Sun and Y.-N. Yeh, *On various restricted sumsets*, J. Number Theory **114** (2005), 209–220.
[15] Z.-W. Sun and L.-L. Zhao, *Linear extension of the Erdos-Heilbronn conjecture*, J. Combin. Theory Ser. A **119** (2012), 364–381.

(Han Wang) Department of Mathematics, Nanjing University, Nanjing 210093, People's Republic of China
E-mail address: `hWang@smail.nju.edu.cn`

(Zhi-Wei Sun, corresponding author) School of Mathematics, Nanjing University, Nanjing 210093, People's Republic of China
E-mail address: `zwsun@nju.edu.cn`