J. Combin. Theory Ser. A 116(2009), no. 8, 1374–1381.

A NEW EXTENSION OF THE ERDŐS-HEILBRONN CONJECTURE

Hao Pan and Zhi-Wei Sun

Department of Mathematics, Nanjing University
Nanjing 210093, People's Republic of China
haopan79@yahoo.com.cn, zwsun@nju.edu.cn

Abstract. Let $A_1,\ldots,A_n$ be finite subsets of a field F, and let

$$f(x_1,\ldots,x_n)=x_1^k+\cdots+x_n^k+g(x_1,\ldots,x_n)\in F[x_1,\ldots,x_n]$$

with $\deg g<k$. We obtain a lower bound for the cardinality of

$$\{f(x_1,\ldots,x_n):\, x_1\in A_1,\ldots,x_n\in A_n,\ \text{and}\ x_i\neq x_j\ \text{if}\ i\neq j\}.$$

The result extends the Erdős-Heilbronn conjecture in a new way.

1. Introduction

In 1964 P. Erdős and H. Heilbronn [EH] made the following challenging conjecture: If p is a prime, then for any subset A of the finite field $\mathbb{Z}/p\mathbb{Z}$ we have

$$|\{x_1+x_2:\, x_1,x_2\in A \text{ and } x_1\neq x_2\}|\geqslant\min\{p,\,2|A|-3\}.$$

It had remained open for thirty years until it was confirmed fully by Dias da Silva and Hamidoune [DH] who actually obtained the following generalization with the help of the representation theory of symmetric groups: For any finite subset A of a field F, we have the inequality

$$\begin{aligned}|\{x_1+\cdots+x_n:\, x_1,\ldots,x_n\in A,\ \text{and}\ x_i\neq x_j\ \text{if}\ i\neq j\}|\\ \geqslant\min\{p(F),\,n(|A|-n)+1\},\end{aligned}$$

Key words and phrases. Erdős-Heilbronn conjecture, Combinatorial Nullstellensatz, value sets of polynomials.

2000 *Mathematics Subject Classification.* Primary 11B75; Secondary 05A05, 11P99, 11T06, 12E10.

The second author is responsible for communications, and supported by the National Natural Science Foundation (grant 10871087) of China.

where $p(F) = p$ if the characteristic of F is a prime p, and $p(F) = +\infty$ if F is of characteristic zero. Recently P. Balister and J. P. Wheeler [BW] extended the Erdős-Heilbronn conjecture to any finite group; namely they showed that for any nonempty subsets A_1 and A_2 of a finite group G written additively we have

$$|\{x_1 + x_2 : x_1 \in A_1,\, x_2 \in A_2 \text{ and } x_1 \neq x_2\}| \geqslant \min\{p(G),\, |A_1| + |A_2| - 3\},$$

where $p(G)$ is the least positive order of a nonzero element of G, and $p(G)$ is regarded as $+\infty$ if G is torsion-free.

In 1996 N. Alon, M. B. Nathanson and I. Z. Ruzsa [ANR] used the so-called polynomial method (see also Alon [A], Nathanson [N, pp. 98–107], and T. Tao and V. H. Vu [TV, pp. 329–345]) to deduce the following result: If $A_1, \ldots, A_n$ are finite subsets of a field F with $0 < |A_1| < \cdots < |A_n|$, then

$$\begin{aligned}&|\{x_1 + \cdots + x_n : x_1 \in A_1, \ldots, x_n \in A_n, \text{ and } x_i \neq x_j \text{ if } i \neq j\}|\\ &\qquad\geqslant \min\left\{p(F),\, 1 + \sum_{i=1}^{n}(|A_i| - i)\right\}.\end{aligned}$$

Consequently, if $A_1, \ldots, A_n$ are finite subsets of a field F with $|A_i| \geqslant i$ for all $i = 1, \ldots, n$, then

$$\begin{aligned}&|\{x_1 + \cdots + x_n : x_1 \in A_1, \ldots, x_n \in A_n, \text{ and } x_i \neq x_j \text{ if } i \neq j\}|\\ &\qquad\geqslant \min\left\{p(F),\, 1 + \sum_{i=1}^{n}\min_{i \leqslant j \leqslant n}(|A_j| - j)\right\}.\end{aligned}$$

(Choose $A_i' \subseteq A_i$ with $|A_i'| = i + \min_{i \leqslant j \leqslant n}(|A_j| - j) \leqslant |A_i|$. Then $|A_1'| < \cdots < |A_n'|$.) For other results on restricted sumsets obtained by the polynomial method, the reader may consult [HS], [PS], [S03], [SY] and [S08a].

Recently Z. W. Sun [S08] obtained the following result on value sets of polynomials.

Theorem 1.1 (Z. W. Sun [S08]). *Let $A_1, \ldots, A_n$ be finite nonempty subsets of a field F, and let*

$$f(x_1, \ldots, x_n) = a_1 x_1^k + \cdots + a_n x_n^k + g(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n] \quad (1.1)$$

with

$$k \in \mathbb{Z}^+ = \{1, 2, 3, \ldots\},\ a_1, \ldots, a_n \in F^* = F \setminus \{0\} \text{ and } \deg g < k. \quad (1.2)$$

(i) *We have*

$$|\{f(x_1,\dots,x_n):\ x_1\in A_1,\dots,x_n\in A_n\}| \geqslant \min\left\{p(F),\ 1+\sum_{i=1}^{n}\left\lfloor\frac{|A_i|-1}{k}\right\rfloor\right\}. \tag{1.3}$$

(ii) *If* $k\geqslant n$ *and* $|A_i|\geqslant i$ *for* $i=1,\dots,n$, *then*

$$|\{f(x_1,\dots,x_n):\ x_1\in A_1,\dots,x_n\in A_n,\ \text{and } x_i\neq x_j \text{ if } i\neq j\}| \geqslant \min\left\{p(F),\ 1+\sum_{i=1}^{n}\left\lfloor\frac{|A_i|-i}{k}\right\rfloor\right\}. \tag{1.4}$$

Throughout this paper, for a predicate P we let

$$[\![P]\!]=\begin{cases}1 & \text{if } P \text{ holds},\\ 0 & \text{otherwise.}\end{cases}$$

For $a\in\mathbb{Z}$ and $k\in\mathbb{Z}^+$, we use $\{a\}_k$ to denote the least nonnegative residue of a modulo k.

Let $\mathbb{C}$ be the field of complex numbers. By [S08, Example 4.1], if $k\in\mathbb{Z}^+$, $q\in\{0,1,\dots\}$, and $A=\{z\in\mathbb{C}:\ z^k\in\{1,\dots,q\}\}\cup R$ with $R\subseteq\{z\in\mathbb{C}:\ z^k=q+1\}$ and $|R|=r<k$, then $|A|=kq+r$ and

$$|\{x_1^k+\dots+x_n^k:\ x_1,\dots,x_n\in A,\ \text{and } x_i\neq x_j \text{ if } i\neq j\}| = \frac{n(|A|-n)-\{n\}_k\{|A|-n\}_k}{k}+r[\![\{n\}_k>r]\!]+1.$$

Motivated by this example, Sun [S08] raised the following extension of the Erdős-Heilbronn conjecture.

Conjecture 1.1 (Z. W. Sun [S08])**.** *Let* $f(x_1,\dots,x_n)$ *be a polynomial over a field* F *given by* (1.1) *and* (1.2). *Provided* $n\geqslant k$, *for any finite subset* A *of* F *we have*

$$|\{f(x_1,\dots,x_n):\ x_1,\dots,x_n\in A,\ \text{and } x_i\neq x_j \text{ if } i\neq j\}| \geqslant \min\left\{p(F)-[\![n=2\ \&\ a_1=-a_2]\!],\ \frac{n(|A|-n)-\{n\}_k\{|A|-n\}_k}{k}+1\right\}. \tag{1.5}$$

Sun [S08] noted that this conjecture in the case $n=2$ follows from [PS, Corollary 3], and proved (1.5) with the lower bound replaced by $\min\{p(F),\ |A|-n+1\}$.

In this paper we establish a similar version of (1.4) for the case $n\geqslant k$ under the condition $a_1=\dots=a_n$. It implies Conjecture 1.1 in the case $a_1=\dots=a_n$.

Here is our first result.

Theorem 1.2. *Let $A_1,\ldots,A_n$ be finite subsets of a field F with $|A_i|\geqslant i$ for $i=1,\ldots,n$. Let*

$$f(x_1,\ldots,x_n)=x_1^k+\cdots+x_n^k+g(x_1,\ldots,x_n)\in F[x_1,\ldots,x_n] \tag{1.6}$$

with $\deg g<k\leqslant n$. *Then*

$$\begin{aligned}|\{f(x_1,\ldots,x_n):\ &x_1\in A_1,\ldots,x_n\in A_n,\ \text{and } x_i\neq x_j \text{ if } i\neq j\}|\\ &\geqslant \min\{p(F),\ q_1+\cdots+q_n+1\}\end{aligned} \tag{1.7}$$

where

$$q_i=\min_{\substack{i\leqslant j\leqslant n\\ j\equiv i\ (\mathrm{mod}\ k)}}\left\lfloor\frac{|A_j|-j}{k}\right\rfloor \quad \text{for } i=1,\ldots,n. \tag{1.8}$$

Remark 1.1. If $k\geqslant n$ then $q_i=\lfloor(|A_i|-i)/k\rfloor$ for $i=1,\ldots,n$. So Theorem 1.2 is a complement to Theorem 1.1(ii). In the case $k=1$, Theorem 1.2 yields the main result of [ANR].

Theorem 1.2, together with Theorem 1.1(ii), implies the following extension of the Erdős-Heilbronn conjecture.

Theorem 1.3. *Let $A_1,\ldots,A_n$ be finite subsets of a field F with $|A_1|=\cdots=|A_n|=m\geqslant n$, and let $f(x_1,\ldots,x_n)$ be given by* (1.6) *with* $\deg g<k$. *Then*

$$\begin{aligned}&|\{f(x_1,\ldots,x_n):\ x_1\in A_1,\ldots,x_n\in A_n,\ \text{ and } x_i\neq x_j \text{ if } i\neq j\}|\\ &\geqslant \min\left\{p(F),\ \frac{n(m-n)-\{n\}_k\{m-n\}_k}{k}+\{n\}_k[\![\{m\}_k<\{n\}_k]\!]+1\right\}.\end{aligned} \tag{1.9}$$

Remark 1.2. If n or $m-n$ is divisible by k, then the lower bound in (1.9) becomes $\min\{p(F),n(m-n)/k+1\}$. In the case $k=1$ and $A_1=\cdots=A_n$, Theorem 1.3 yields the Dias da Silva-Hamidoune extension (cf. [DH]) of the Erdős-Heilbronn conjecture.

In the next section we are going to present an auxiliary theorem. Theorems 1.2 and 1.3 will be proved in Section 3.

2. An Auxiliary Theorem

For a polynomial $P(x_1,\ldots,x_n)$ over a field, by $[x_1^{k_1}\cdots x_n^{k_n}]P(x_1,\ldots,x_n)$ we mean the coefficient of the monomial $x_1^{k_1}\cdots x_n^{k_n}$ in $P(x_1,\ldots,x_n)$.

In this section we prove the following auxiliary result.

Theorem 2.1. *Let* $q_1, \ldots, q_n \in \mathbb{N} = \{0, 1, 2, \ldots\}$ *and* $k \in \{1, \ldots, n\}$. *Then*

$$\begin{aligned}&\Big[\prod_{j=1}^{n} x_j^{kq_j+j-1}\Big](x_1^k + \cdots + x_n^k)^N \prod_{1\leqslant i<j\leqslant n}(x_j - x_i)\\ =&N! \prod_{s=1}^{k} \frac{\prod_{0\leqslant i<j\leqslant \lfloor (n-s)/k\rfloor}(q_{jk+s} + j - (q_{ik+s} + i))}{\prod_{j=0}^{\lfloor (n-s)/k\rfloor}(q_{jk+s} + j)!},\end{aligned} \tag{2.1}$$

where $N = q_1 + \cdots + q_n$.

To prove Theorem 2.1, we need a lemma.

Lemma 2.1. *Let* σ *be a permutation of a finite nonempty set* X. *Suppose that* A *is a subset of* X *with* $\sigma(A) = A$. *Then*

$$\varepsilon(\sigma) = \varepsilon(\sigma|_A)\varepsilon(\sigma|_{X\setminus A}), \tag{2.2}$$

where $\varepsilon(\sigma)$ *stands for the sign of* σ *and* $\sigma|_A$ *denotes the restriction of* σ *on* A.

Proof. Write $\sigma = \tau_1\tau_2\cdots\tau_k$, where $\tau_1, \tau_2, \ldots, \tau_k$ are disjoint cycles. As $\sigma(A) = A$, for each $i = 1, \ldots, k$, either all elements in the cycle τ_i lie in A, or none of the elements in the cycle τ_i belongs to A. Set

$$I = \{1 \leqslant i \leqslant k : \text{all the elements in the cycle } \tau_i \text{ lie in } A\}$$

and

$$\bar{I} = \{1 \leqslant i \leqslant k : \text{all the elements in the cycle } \tau_i \text{ lie in } X \setminus A\}$$

Then

$$I \cup \bar{I} = \{1, \ldots, k\},\ \sigma|_A = \prod_{i\in I} \tau_i|_A \text{ and } \sigma|_{X\setminus A} = \prod_{i\in \bar{I}} \tau_i|_{X\setminus A}.$$

Therefore

$$\varepsilon(\sigma) = \prod_{i=1}^{k} \varepsilon(\tau_i) = \prod_{i\in I} \varepsilon(\tau_i) \times \prod_{j\in \bar{I}} \varepsilon(\tau_j) = \varepsilon(\sigma|_A)\varepsilon(\sigma|_{X\setminus A}).$$

This completes the proof. □

For a finite nonempty set X, we let $S(X)$ denote the symmetric group of all permutations of X. If $|X| = n$, then the group $S(X)$ is isomorphic to the symmetry group $S_n = S(\{1, \ldots, n\})$. Recall that the determinant of a matrix $[a_{i,j}]_{1\leqslant i,j\leqslant n}$ over a field is defined as

$$\det[a_{i,j}]_{1\leqslant i,j\leqslant n} = \sum_{\sigma\in S_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)} = \sum_{\sigma\in S_n} \varepsilon(\sigma) \prod_{j=1}^{n} a_{\sigma(j),j}.$$

Proof of Theorem 2.1. By the multinomial theorem,

$$(x_1^k+\cdots+x_n^k)^N=\sum_{\substack{i_1,\ldots,i_n\in\mathbb{N}\\ i_1+\cdots+i_n=N}}\frac{N!}{i_1!\cdots i_n!}x_1^{ki_1}\cdots x_n^{ki_n}.$$

In view of linear algebra,

$$\sum_{\sigma\in S_n}\varepsilon(\sigma)\prod_{j=1}^n x_j^{\sigma(j)-1}=\det[x_j^{i-1}]_{1\leqslant i,j\leqslant n}=\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)\ \text{(Vandermonde)}.$$

Thus

$$\begin{aligned}&\left[\prod_{j=1}^n x_j^{kq_j+j-1}\right](x_1^k+\cdots+x_n^k)^N\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)\\ =&\left[\prod_{j=1}^n x_j^{kq_j+j-1}\right]N!\sum_{\substack{i_1,\ldots,i_n\in\mathbb{N}\\ i_1+\cdots+i_n=N}}\sum_{\substack{\sigma\in S_n\\ k\mid\sigma(j)-j\\ \text{for } j=1,\ldots,n}}\varepsilon(\sigma)\prod_{j=1}^n\frac{x_j^{ki_j+\sigma(j)-1}}{i_j!}\\ =&\left[\prod_{j=1}^n x_j^{kq_j+j-1}\right]N!\sum_{\substack{i_1,\ldots,i_n\in\mathbb{N}\\ i_1+\cdots+i_n=N}}\sum_{\substack{\sigma\in S_n\\ \sigma(X_s)=X_s\\ \text{for } s=1,\ldots,k}}\varepsilon(\sigma)\prod_{j=1}^n\frac{x_j^{ki_j+\sigma(j)-1}}{i_j!},\end{aligned}$$

where

$$X_s=\{1\leqslant j\leqslant n:\ j\equiv s\ (\mathrm{mod}\ k)\}.$$

Set $n_s=|X_s|$. Then

$$n_s=|\{q\in\mathbb{N}:\ s+kq\leqslant n\}|=\left\lfloor\frac{n-s}{k}\right\rfloor+1.$$

If $\sigma\in S_n$ and $\sigma(X_s)=X_s$ for all $s=1,\ldots,k$, then

$$\varepsilon(\sigma)=\varepsilon(\sigma|_{X_1})\varepsilon(\sigma|_{X_2\cup\cdots\cup X_k})=\cdots=\varepsilon(\sigma|_{X_1})\cdots\varepsilon(\sigma|_{X_k})$$

by Lemma 2.1.

Let $(x)_0 = 1$ and $(x)_i = \prod_{r=0}^{i-1}(x-r)$ for $i = 1, 2, 3, \ldots$. By the above,

$$\begin{aligned}
&\left[\prod_{j=1}^{n} x_j^{kq_j+j-1}\right]\frac{(x_1^k+\cdots+x_n^k)^N}{N!}\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)\\
=&\left[\prod_{j=1}^{n} x_j^{kq_j+j-1}\right]\sum_{\substack{i_1,\ldots,i_n\in\mathbb{N}\\ i_1+\cdots+i_n=N}}\prod_{s=1}^{k}\Bigg(\sum_{\sigma\in S(X_s)}\varepsilon(\sigma)\prod_{j\in X_s}\frac{x_j^{ki_j+\sigma(j)-1}}{i_j!}\Bigg)\\
=&\prod_{s=1}^{k}\Bigg(\sum_{\substack{\sigma\in S(X_s)\\ q_j+(j-\sigma(j))/k\geqslant 0\\ \text{for } j\in X_s}}\varepsilon(\sigma)\prod_{j\in X_s}\frac{1}{(q_j+(j-\sigma(j))/k)!}\Bigg)\\
=&\prod_{s=1}^{k}\Bigg(\sum_{\sigma\in S_{n_s}}\varepsilon(\sigma)\prod_{j=1}^{n_s}\frac{(q_{(j-1)k+s}+j-1)_{\sigma(j)-1}}{(q_{(j-1)k+s}+j-1)!}\Bigg)\\
=&\prod_{s=1}^{k}\frac{\det[(q_{(j-1)k+s}+j-1)_{i-1}]_{1\leqslant i,j\leqslant n_s}}{\prod_{j=1}^{n_s}(q_{(j-1)k+s}+j-1)!}=\prod_{s=1}^{k}\frac{\det[(q_{jk+s}+j)_i]_{0\leqslant i,j\leqslant n_s-1}}{\prod_{j=0}^{n_s-1}(q_{jk+s}+j)!}.
\end{aligned}$$

It is well known that

$$y^i = (y)_i + \sum_{0\leqslant r<i} S(i,r)(y)_r \quad \text{for } i = 0, 1, 2, \ldots,$$

where $S(i,r)$ $(0 \leqslant r < i)$ are Stirling numbers of the second kind. So

$$\begin{aligned}
&\det[(q_{jk+s}+j)_i]_{0\leqslant i,j<n_s} = \det[(q_{jk+s}+j)^i]_{0\leqslant i,j<n_s}\\
=&\prod_{0\leqslant i<j<n_s}(q_{jk+s}+j-(q_{ik+s}+i)) \quad \text{(Vandermonde)},
\end{aligned}$$

and hence (2.1) follows. $\square$

3. Proofs of Theorems 1.2 and 1.3

Let us recall the following powerful tool.

Combinatorial Nullstellensatz (Alon [A]). *Let $A_1, \cdots, A_n$ be finite subsets of a field F, and let $P(x_1, \cdots, x_n) \in F[x_1, \cdots, x_n]$. Suppose that* $\deg P = k_1 + \cdots + k_n$ *where* $0 \leqslant k_i < |A_i|$ *for* $i = 1, \ldots, n$. *If*

$$[x_1^{k_1}\cdots x_n^{k_n}]P(x_1,\ldots,x_n) \neq 0,$$

then $P(x_1, \ldots, x_n) \neq 0$ for some $x_1 \in A_1, \ldots, x_n \in A_n$.

Proof of Theorem 1.2. Let m be the least nonnegative integer not exceeding n such that $\sum_{m<i\leqslant n} q_i < p(F)$. For each $m < i \leqslant n$ let A_i' be a subset of

A_i with cardinality $kq_i + i \leqslant |A_i|$. In the case $m > 0$, $p = p(F)$ is a prime and we let A'_m be a subset of A_m with

$$|A'_m| = k\left(p - 1 - \sum_{m<i\leqslant n} q_i\right) + m < kq_m + m \leqslant |A_m|.$$

If $0 < i < m$ then we let $A'_i \subseteq A_i$ with $|A_i| = i$. Clearly $q'_i = (|A'_i| - i)/k \leqslant q_i$. Whether $m = 0$ or not, we have $\sum_{i=1}^n (|A'_i| - i) = k\sum_{i=1}^n q'_i = k(N-1)$, where

$$N = \min\{p(F),\, q_1 + \cdots + q_n + 1\}.$$

Let $s \in \{1, \ldots, k\}$. For any $0 < i < n_s = \lfloor (n-s)/k \rfloor + 1$ we have

$$q_{(i-1)k+s} = \min_{\substack{(i-1)k+s\leqslant j\leqslant n \\ j\equiv s \pmod{k}}} \left\lfloor \frac{|A_j| - j}{k} \right\rfloor \leqslant \min_{\substack{ik+s\leqslant j\leqslant n \\ j\equiv s \pmod{k}}} \left\lfloor \frac{|A_j| - j}{k} \right\rfloor = q_{ik+s}$$

and hence $q'_{(i-1)k+s} \leqslant q'_{ik+s}$. (If $(i-1)k + s = m$ then $q'_{(i-1)k+s} \leqslant q_{(i-1)k+s} \leqslant q_{ik+s} = q'_{ik+s}$.) So

$$0 \leqslant q'_s < q'_{k+s} + 1 < q'_{2k+s} + 2 < \cdots < q'_{(n_s-1)k+s} + n_s - 1.$$

Define

$$P(x_1, \ldots, x_n) = (x_1^k + \cdots + x_n^k)^{N-1} \prod_{1\leqslant i<j\leqslant n} (x_j - x_i) \in F[x_1, \ldots, x_n].$$

In light of Theorem 2.1,

$$\left[\prod_{j=1}^n x_j^{kq'_j + j - 1}\right] P(x_1, \ldots, x_n) = he,$$

where e is the identity of the field F, and

$$h = (N-1)! \Big/ \prod_{s=1}^k \prod_{j=0}^{n_s - 1} \prod_{\substack{0\leqslant r<q'_{jk+s}+j \\ r\notin\{q'_{ik+s}+i:\, 0\leqslant i<j\}}} (q'_{jk+s} + j - r)$$

is an integer dividing $(N-1)!$. Since $p(F) > N - 1$, we have $he \neq 0$.

Set

$$C = \{f(x_1, \ldots, x_n) :\, x_1 \in A'_1, \ldots, x_n \in A'_n, \text{ and } x_i \neq x_j \text{ if } i \neq j\}.$$

Suppose that $|C| \leqslant N-1$ and let $Q(x_1,\dots,x_n)$ denote the polynomial

$$f(x_1,\dots,x_n)^{N-1-|C|}\prod_{c\in C}(f(x_1,\dots,x_n)-c)\times\prod_{1\leqslant i<j\leqslant n}(x_j-x_i).$$

Then

$$\deg Q = k(N-1)+\binom{n}{2}=\sum_{i=1}^{n}(|A_i'|-1)=\sum_{i=1}^{n}(kq_i'+i-1)$$

and

$$\left[x_1^{|A_1'|-1}\cdots x_n^{|A_n'|-1}\right]Q(x_1,\dots,x_n)=\left[\prod_{j=1}^{n}x_j^{kq_j'+j-1}\right]P(x_1,\dots,x_n)\neq 0.$$

In light of the Combinatorial Nullstellensatz, there are $x_1\in A_1',\dots,x_n\in A_n'$ such that $Q(x_1,\dots,x_n)\neq 0$. This contradicts the fact $f(x_1,\dots,x_n)\in C$.

By the above, we have

$$|\{f(x_1,\dots,x_n):\, x_1\in A_1,\dots,x_n\in A_n,\text{ and } x_i\neq x_j \text{ if } i\neq j\}|\geqslant |C|\geqslant N.$$

This concludes the proof. □

Proof of Theorem 1.3. Write $n=kq_0+n_0$ with $q_0\in\mathbb{N}$ and $1\leqslant n_0\leqslant k$. Then

$$\begin{aligned}
&\sum_{i=1}^{n}\min_{\substack{i\leqslant j\leqslant n\\ j\equiv i\,(\mathrm{mod}\ k)}}\left\lfloor\frac{|A_j|-j}{k}\right\rfloor\\
=&\sum_{r=1}^{k}\sum_{0\leqslant q\leqslant\lfloor(n-r)/k\rfloor}\min_{\substack{kq+r\leqslant j\leqslant n\\ j\equiv r\,(\mathrm{mod}\ k)}}\left\lfloor\frac{m-j}{k}\right\rfloor\\
=&\sum_{r=1}^{k}\sum_{0\leqslant q\leqslant\lfloor(n-r)/k\rfloor}\left\lfloor\frac{m-r-k\lfloor(n-r)/k\rfloor}{k}\right\rfloor\\
=&\sum_{r=1}^{k}\left(\left\lfloor\frac{n-r}{k}\right\rfloor+1\right)\left(\left\lfloor\frac{m-r}{k}\right\rfloor-\left\lfloor\frac{n-r}{k}\right\rfloor\right)\\
=&\sum_{r=1}^{n_0}(q_0+1)\left(\left\lfloor\frac{m-r}{k}\right\rfloor-q_0\right)+\sum_{n_0<r\leqslant k}q_0\left(\left\lfloor\frac{m-r}{k}\right\rfloor-q_0+1\right)\\
=&q_0\sum_{r=1}^{k}\left\lfloor\frac{m-r}{k}\right\rfloor+\sum_{r=1}^{n_0}\left\lfloor\frac{m-r}{k}\right\rfloor-q_0((q_0+1)n_0+(q_0-1)(k-n_0)).
\end{aligned}$$

Observe that

$$\sum_{r=1}^{k}\left\lfloor\frac{m-r}{k}\right\rfloor=\sum_{r=1}^{k}\left(\frac{m-r}{k}-\frac{\{m-r\}_k}{k}\right)=m-\sum_{r=1}^{k}\frac{r}{k}-\sum_{s=0}^{k-1}\frac{s}{k}=m-k.$$

So we have

$$\begin{aligned}&\sum_{i=1}^{n}\min_{\substack{i\leqslant j\leqslant n\\ j\equiv i\,(\mathrm{mod}\ k)}}\left\lfloor\frac{|A_j|-j}{k}\right\rfloor\\ =&\sum_{r=1}^{n_0}\left\lfloor\frac{m-r}{k}\right\rfloor+q_0(m-k)-q_0(2n_0+k(q_0-1))\\ =&\sum_{r=1}^{n_0}\left(\left\lfloor\frac{m-r}{k}\right\rfloor-q_0\right)+q_0(m-n).\end{aligned}$$

To simplify the last sum, we now subtract a term which will be added later. Clearly

$$\begin{aligned}&\sum_{r=1}^{n_0}\left(\left\lfloor\frac{m-r}{k}\right\rfloor-q_0\right)-n_0\left\lfloor\frac{m-n}{k}\right\rfloor\\ =&\sum_{r=1}^{n_0}\left(\left\lfloor\frac{m-n+n_0-r}{k}\right\rfloor-\left\lfloor\frac{m-n}{k}\right\rfloor\right)\\ =&\sum_{s=0}^{n_0-1}\left\lfloor\frac{\{m-n\}_k+s}{k}\right\rfloor.\end{aligned}$$

If $\{m\}_k\geqslant n_0$, then

$$\sum_{s=0}^{n_0-1}\left\lfloor\frac{\{m-n\}_k+s}{k}\right\rfloor=\sum_{s=0}^{n_0-1}\left\lfloor\frac{\{m\}_k-\{n\}_k+s}{k}\right\rfloor=0.$$

If $\{m\}_k<n_0$, then

$$\begin{aligned}&\sum_{s=0}^{n_0-1}\left\lfloor\frac{\{m-n\}_k+s}{k}\right\rfloor=\sum_{s=0}^{n_0-1}\left\lfloor\frac{\{m\}_k-n_0+k+s}{k}\right\rfloor\\ =&|\{s\in\{0,\ldots,n_0-1\}:\ s\geqslant n_0-\{m\}_k\}|=\{m\}_k.\end{aligned}$$

Therefore

$$\begin{aligned}&\sum_{i=1}^{n}\min_{\substack{i\leqslant j\leqslant n\\ j\equiv i\,(\mathrm{mod}\ k)}}\left\lfloor\frac{|A_j|-j}{k}\right\rfloor\\ =&q_0(m-n)+n_0\left\lfloor\frac{m-n}{k}\right\rfloor+\{m\}_k[\![\{m\}_k<n_0]\!]\\ =&(m-n)\left\lfloor\frac{n}{k}\right\rfloor+\{n\}_k\left\lfloor\frac{m-n}{k}\right\rfloor+\{m\}_k[\![\{m\}_k<\{n\}_k]\!]\\ =&\frac{n(m-n)}{k}-\frac{\{n\}_k\{m-n\}_k}{k}+\{m\}_k[\![\{m\}_k<\{n\}_k]\!].\end{aligned}$$

In view of the above, by applying Theorem 1.2 for $k \leqslant n$ and Theorem 1.1(ii) for $k \geqslant n$, we immediately get the desired (1.9). $\square$

References

[A] N. Alon, *Combinatorial Nullstellensatz*, Combin. Probab. Comput. **8** (1999), 7–29.

[ANR] 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.

[BW] P. Balister and J. P. Wheeler, *The Erdős-Heilbronn conjecture for finite groups*, Acta Arith., to appear.

[DH] 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.

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

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

[N] M. B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Graduate Texts in Math., Vol. 165, Springer, New York, 1996.

[PS] H. Pan and Z. W. Sun, *A lower bound for* $|\{a+b\colon a \in A,\ b \in B,\ P(a,b) \neq 0\}|$, J. Combin. Theory Ser. A **100** (2002), 387–393.

[S03] Z. W. Sun, *On Snevily's conjecture and restricted sumsets*, J. Combin. Theory Ser. A **103** (2003), 291–304.

[S08] Z. W. Sun, *On value sets of polynomials over a field*, *Finite Fields Appl.* **14** (2008), 470–481.

[S08a] Z. W. Sun, *An additive theorem and restricted sumsets*, *Math. Res. Lett.* **15** (2008), 1263–1276.

[SY] Z. W. Sun and Y. N. Yeh, *On various restricted sumsets*, J. Number Theory **114** (2005), 209–220.

[TV] T. Tao and V. H. Vu, *Additive Combinatorics*, Cambridge Univ. Press, Cambridge, 2006.