Journal of Combinatorial Theory, Series A 119 (2012) 364–381

Contents lists available at SciVerse ScienceDirect

Journal of Combinatorial Theory, Series A

www.elsevier.com/locate/jcta

Linear extension of the Erdős–Heilbronn conjecture

Zhi-Wei Sun [a,1], Li-Lu Zhao [b]

[a] Department of Mathematics, Nanjing University, Nanjing 210093, People's Republic of China

[b] Department of Mathematics, The University of Hong Kong, Pokfulam Road, Hong Kong

ARTICLE INFO

Article history:
Received 1 September 2009
Available online 12 October 2011

Keywords:
Combinatorial Nullstellensatz
Erdős–Heilbronn conjecture
Linear extension
Value sets of polynomials over a field

ABSTRACT

The famous Erdős–Heilbronn conjecture plays an important role in the development of additive combinatorial number theory. In 2007 Z.W. Sun made the following further conjecture (which is the linear extension of the Erdős–Heilbronn conjecture): For any finite subset A of a field F and nonzero elements $a_1, \ldots, a_n$ of F, we have

$$\bigl|\{a_1x_1 + \cdots + a_nx_n\colon x_1, \ldots, x_n \in A, \text{ and } x_i \neq x_j \text{ if } i \neq j\}\bigr| \geqslant \min\bigl\{p(F) - \delta,\ n\bigl(|A| - n\bigr) + 1\bigr\},$$

where the additive order $p(F)$ of the multiplicative identity of F is different from $n + 1$, and $\delta \in \{0, 1\}$ takes the value 1 if and only if $n = 2$ and $a_1 + a_2 = 0$. In this paper we prove this conjecture of Sun when $p(F) \geqslant n(3n - 5)/2$. We also obtain a sharp lower bound for the cardinality of the restricted sumset

$$\bigl\{x_1 + \cdots + x_n\colon x_1 \in A_1, \ldots, x_n \in A_n, \text{ and } P(x_1, \ldots, x_n) \neq 0\bigr\},$$

where $A_1, \ldots, A_n$ are finite subsets of a field F and $P(x_1, \ldots, x_n)$ is a general polynomial over F.

1. Introduction

A basic objective in the active field of additive combinatorial number theory is the sumset of finite subsets $A_1, \ldots, A_n$ of a field F given by

$$A_1 + \cdots + A_n = \{x_1 + \cdots + x_n\colon x_1 \in A_1, \ldots, x_n \in A_n\}.$$

E-mail addresses: zwsun@nju.edu.cn (Z.-W. Sun), zhaolilu@gmail.com (L.-L. Zhao).

[1] Supported by the National Natural Science Foundation (grants 10871087 and 11171140) of China.

0097-3165/$ – see front matter
doi:10.1016/j.jcta.2011.09.003

(See, e.g., [16] and [24].) The well-known Cauchy–Davenport theorem asserts that

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

where $p(F)$ is the additive order of the multiplicative identity of F (which is the characteristic of F if F is of a prime characteristic, and the positive infinity if F is of characteristic zero). When $n=2$ and $F=\mathbb{Z}/p\mathbb{Z}$ with p a prime, this gives the original form of the Cauchy–Davenport theorem.

In 1964 P. Erdős and H. Heilbronn [10] conjectured that if p is a prime and A is a subset of $\mathbb{Z}/p\mathbb{Z}$ then

$$\left|\{x+y:\ x,y\in A \text{ and } x\neq y\}\right| \geqslant \min\{p,\ 2|A|-3\}.$$

This challenging conjecture was finally solved by J.A. Dias da Silva and Y.O. Hamidoune [8] in 1994 who employed exterior algebras to show that for any subset A of a field F we have

$$\left|\{x_1+\cdots+x_n:\ x_i\in A,\ x_i\neq x_j \text{ if } i\neq j\}\right| \geqslant \min\{p(F),\ n|A|-n^2+1\}.$$

Recently P. Balister and J.P. Wheeler [5] extended the Erdős–Heilbronn conjecture to any finite group.

In 1995–1996 N. Alon, M.B. Nathanson and I.Z. Ruzsa [2,3] used the so-called polynomial method rooted in [4] to prove that if $A_1,\ldots,A_n$ are finite subsets of a field F with $0<|A_1|<\cdots<|A_n|$ then

$$\left|\{x_1+\cdots+x_n:\ x_i\in A_i,\ x_i\neq x_j \text{ if } i\neq j\}\right| \geqslant \min\left\{p(F),\ \sum_{i=1}^{n}\big(|A_i|-i\big)+1\right\}.$$

The polynomial method was further refined by Alon [1] in 1999, who presented the following useful principle.

Combinatorial Nullstellensatz. (See Alon [1].) *Let $A_1,\ldots,A_n$ be finite subsets of a field F with $|A_i|>k_i$ for all $i=1,\ldots,n$ where $k_1,\ldots,k_n\in\mathbb{N}=\{0,1,2,\ldots\}$. Suppose that $P(x_1,\ldots,x_n)$ is a polynomial over F with $[x_1^{k_1}\cdots x_n^{k_n}]P(x_1,\ldots,x_n)$ (the coefficient of the monomial $x_1^{k_1}\cdots x_n^{k_n}$ in the polynomial $P(x_1,\ldots,x_n)$) nonzero and $k_1+\cdots+k_n=\deg P$. Then there are $x_1\in A_1,\ldots,x_n\in A_n$ such that $P(x_1,\ldots,x_n)\neq 0$.*

The Combinatorial Nullstellensatz has been applied to investigate some sumsets with polynomial restrictions by various authors, see [7,13,15,17,20,23,14,22].

Throughout this paper, for a predicate P we let

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

For $a,b\in\mathbb{Z}$ we define $[a,b]=\{m\in\mathbb{Z}:\ a\leqslant m\leqslant b\}$. For a field F we let F^* be the multiplicative group of all nonzero elements of F. As usual the symmetric group on $\{1,\ldots,n\}$ is denoted by S_n. For $\sigma\in S_n$ we use $\operatorname{sgn}(\sigma)$ to stand for the sign of the permutation σ. We also set $(x)_0=1$ and $(x)_n=\prod_{j=0}^{n-1}(x-j)$ for $n=1,2,3,\ldots$.

Recently Z.W. Sun made the following conjecture (cf. [21]) which can be viewed as the linear extension of the Erdős–Heilbronn conjecture.

Conjecture 1.1 *(Sun). Let A be a finite subset of a field F and let $a_1,\ldots,a_n\in F^*=F\setminus\{0\}$. Provided $p(F)\neq n+1$ we have*

$$\begin{aligned}&\left|\{a_1x_1+\cdots+a_nx_n:\ x_1,\ldots,x_n\in A,\ \text{and } x_i\neq x_j \text{ if } i\neq j\}\right|\\ &\quad\geqslant \min\{p(F)-[\![n=2\ \&\ a_1=-a_2]\!],\quad n\big(|A|-n\big)+1\}.\end{aligned}\tag{1.1}$$

Example 1.1. Let p be an odd prime and let k be a positive integer relatively prime to $p-1$. As $k\not\equiv 0 \pmod{p-1}$, we have $\sum_{x\in F_p}x^k=0$ where $F_p=\mathbb{Z}/p\mathbb{Z}$. For any distinct $x,y\in F_p$ we cannot have $x^k=y^k$ since $ku+(p-1)v=1$ for some $u,v\in\mathbb{Z}$. Thus

$$\left|\{x_1^k+\cdots+x_{p-2}^k+2x_{p-1}^k:\ x_1,\ldots,x_{p-1}\in F_p \text{ are distinct}\}\right|=\left|F_p^*\right|=p-1.$$

In the case $k = 1$ and $p \in \{5, 7\}$, this was noted by Mr. Wen-Long Zhang (at Nanjing University) in Feb. 2011 via computation under the guidance of the first author.

All known proofs of the Erdős–Heilbronn conjecture (including the recent one given by S. Guo and Sun [12] based on Tao's harmonic analysis method) cannot be modified easily to confirm the above conjecture. New ideas are needed!

Concerning Conjecture 1.1 we are able to establish the following result.

Theorem 1.1. *Let A be a finite subset of a field F and let $a_1, \ldots, a_n \in F^*$. Then (1.1) holds if $p(F) \geqslant n(3n-5)/2$.*

We obtain Theorem 1.1 by combining our next two theorems.

Theorem 1.2. *Let n be a positive integer, and let F be a field with $p(F) \geqslant (n-1)^2$. Let $a_1, \ldots, a_n \in F^*$, and suppose that $A_i \subseteq F$ and $|A_i| \geqslant 2n-2$ for $i = 1, \ldots, n$. Then, for the set*

$$C = \{a_1x_1 + \cdots + a_nx_n \colon x_1 \in A_1, \ldots, x_n \in A_n, \text{ and } x_i \neq x_j \text{ if } i \neq j\} \tag{1.2}$$

we have

$$|C| \geqslant \min\{p(F) - [\![n = 2 \,\&\, a_1 + a_2 = 0]\!],\ |A_1| + \cdots + |A_n| - n^2 + 1\}. \tag{1.3}$$

Theorem 1.2 has the following consequence.

Corollary 1.1. *Let $p > 7$ be a prime and let $A \subseteq F_p = \mathbb{Z}/p\mathbb{Z}$ with $|A| \geqslant \sqrt{4p-7}$. Let $n = \lfloor |A|/2 \rfloor$ and $a_1, \ldots, a_n \in F_p^*$. Then every element of F_p can be written in the linear form $a_1x_1 + \cdots + a_nx_n$ with $x_1, \ldots, x_n \in A$ distinct.*

Remark 1.1. In the case $a_1 = \cdots = a_n = 1$, Corollary 1.1 is a refinement of a conjecture of Erdős proved by da Silva and Hamidoune [8] via exterior algebras.

By Theorem 1.1, Conjecture 1.1 is valid for $n = 2$. Now we explain why Conjecture 1.1 holds in the case $n = 3$. Let A be a finite subset of a field F and let $a_1, a_2, a_3 \in F^*$. Clearly (1.1) holds if $|A| \leqslant n$. Below we assume $|A| > n = 3$. By Theorem 1.1, (1.1) with $n = 3$ holds if $p(F) \geqslant 3(3 \times 3 - 5)/2 = 6$. When $p(F) = 5$, we have (1.1) by Theorem 1.2. If $p(F) = 2$ and c_1, c_2, c_3, c_4 are four distinct elements of A, then

$$\begin{aligned} &\bigl|\{a_1x_1 + a_2x_2 + a_3x_3 \colon x_1, x_2, x_3 \in A \text{ and } x_1, x_2, x_3 \text{ are distinct}\}\bigr| \\ &\quad \geqslant \bigl|\{a_1c_1 + a_2c_2 + a_3c_3, a_1c_1 + a_2c_2 + a_3c_4\}\bigr| \\ &\quad = 2 = \min\bigl\{p(F),\ 3\bigl(|A| - 3\bigr) + 1\bigr\}. \end{aligned}$$

In the case $p(F) = 3$, for some $1 \leqslant s < t \leqslant 3$ we have $a_s + a_t \neq 0$, hence for any $c \in A$ we have

$$\begin{aligned} &\bigl|\{a_1x_1 + a_2x_2 + a_3x_3 \colon x_1, x_2, x_3 \in A \text{ and } x_1, x_2, x_3 \text{ are distinct}\}\bigr| \\ &\quad \geqslant \bigl|\bigl\{a_sx_s + a_tx_t \colon x_s, x_t \in A \setminus \{c\} \text{ and } x_s \neq x_t\bigr\}\bigr| \\ &\quad \geqslant \min\bigl\{p(F),\ 2\bigl(\bigl|A \setminus \{c\}\bigr| - 2\bigr) + 1\bigr\} \quad \text{(by Theorem 1.1 with } n = 2) \\ &\quad = 3 = \min\bigl\{p(F),\ 3\bigl(|A| - 3\bigr) + 1\bigr\}. \end{aligned}$$

In this paper we also apply the Combinatorial Nullstellensatz *twice* to deduce the following result on sumsets with *general* polynomial restrictions.

Theorem 1.3. *Let $P(x_1,\dots,x_n)$ be a polynomial over a field F. Suppose that $k_1,\dots,k_n$ are nonnegative integers with $k_1+\dots+k_n=\deg P$ and $[x_1^{k_1}\cdots x_n^{k_n}]P(x_1,\dots,x_n)\neq 0$. Let $A_1,\dots,A_n$ be finite subsets of F with $|A_i|>k_i$ for $i=1,\dots,n$. Then, for the restricted sumset*

$$C=\{x_1+\dots+x_n:\ x_1\in A_1,\dots,x_n\in A_n,\ \text{and } P(x_1,\dots,x_n)\neq 0\},\tag{1.4}$$

we have

$$|C|\geqslant \min\{p(F)-\deg P,\ |A_1|+\dots+|A_n|-n-2\deg P+1\}.\tag{1.5}$$

Remark 1.2. Theorem 1.3 in the case $P(x_1,\dots,x_n)=1$ gives the Cauchy–Davenport theorem. When F is of characteristic zero (i.e., $p(F)=+\infty$), Theorem 1.3 extends a result of Sun [19, Theorem 1.1] on sums of subsets of $\mathbb{Z}$ with various linear restrictions.

The following example shows that the lower bound in Theorem 1.3 is essentially best possible.

Example 1.2. Let p be a prime and let F_p be the finite field $\mathbb{Z}/p\mathbb{Z}$.

(i) Let

$$P(x_1,\dots,x_n)=\prod_{s\in S}(x_1+\dots+x_n-s)$$

where S is a nonempty subset of F_p. Then

$$\begin{aligned}&\left|\{x_1+\dots+x_n:\ x_1,\dots,x_n\in F_p \text{ and } P(x_1,\dots,x_n)\neq 0\}\right|\\&\quad=|F_p\setminus S|=|F_p|-|S|=p-\deg P.\end{aligned}$$

(ii) Let $A=\{\bar r=r+p\mathbb{Z}:\ r\in[0,m-1]\}\subseteq F_p$ with $n\leqslant m\leqslant p$, where n is a positive integer. If $p\geqslant n(m-n)+1$, then

$$\begin{aligned}&\left|\{x_1+\dots+x_n:\ x_1,\dots,x_n\in A,\ \text{and } x_i\neq x_j \text{ if } i\neq j\}\right|\\&\quad=\left|\{\bar r:\ r\in[0+\dots+(n-1),\ (m-n)+\dots+(m-1)]\}\right|\\&\quad=n(m-n)+1=n|A|-n-2\deg\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)+1.\end{aligned}$$

Here are some consequences of Theorem 1.3.

Corollary 1.2. *Let A be a finite subset of a field F, and let $a_1,\dots,a_n\in F^*$.*

(i) *For any $f(x)\in F[x]$ with $\deg f=m\geqslant 0$, we have*

$$\begin{aligned}&\left|\{a_1x_1+\dots+a_nx_n:\ x_1,\dots,x_n\in A,\ \text{and } f(x_i)\neq f(x_j) \text{ if } i\neq j\}\right|\\&\quad\geqslant\min\left\{p(F)-m\binom{n}{2},\ n\big(|A|-1-m(n-1)\big)+1\right\}.\end{aligned}\tag{1.6}$$

(ii) *Let $S_{ij}\subseteq F$ with $|S_{ij}|\leqslant 2m-1$ for all $1\leqslant i<j\leqslant n$. Then*

$$\begin{aligned}&\left|\{a_1x_1+\dots+a_nx_n:\ x_1,\dots,x_n\in A,\ \text{and } x_i-x_j\notin S_{ij} \text{ if } i<j\}\right|\\&\quad\geqslant\min\left\{p(F)-(2m-1)\binom{n}{2},\ n\big(|A|-1-(2m-1)(n-1)\big)+1\right\}.\end{aligned}\tag{1.7}$$

Remark 1.3. In the case $m=1$, each of the two parts in Corollary 1.2 yields the inequality

$$\begin{aligned}&\left|\{a_1x_1+\dots+a_nx_n:\ x_1,\dots,x_n\in A,\ \text{and } x_i\neq x_j \text{ if } i\neq j\}\right|\\&\quad\geqslant\min\left\{p(F)-\binom{n}{2},\ n\big(|A|-n\big)+1\right\}.\end{aligned}\tag{1.8}$$

Let $m_1, \ldots, m_n \in \mathbb{N}$. When we expand $\prod_{1\leqslant i,j\leqslant n,\ i\neq j}(1 - x_i/x_j)^{m_j}$ as a Laurent polynomial (with negative exponents allowed), the constant term was conjectured to be the multinomial coefficient $(\sum_{i=1}^n m_i)!/\prod_{i=1}^n m_i!$ by F.J. Dyson [9] in 1962. A simple proof of Dyson's conjecture given by I.J. Good [11] employs the Lagrange interpolation formula. Using Dyson's conjecture we can deduce the following result from Theorem 1.3.

Corollary 1.3. *Let $A_1, \ldots, A_n$ $(n > 1)$ be finite nonempty subsets of a field F, and let S_{ij} $(1 \leqslant i \neq j \leqslant n)$ be subsets of F with $|S_{ij}| \leqslant (|A_i| - 1)/(n-1)$. Then, for any $a_1, \ldots, a_n \in F^*$, we have*

$$\begin{aligned}&\bigl|\{a_1x_1 + \cdots + a_nx_n\colon x_1 \in A_1, \ldots, x_n \in A_n,\ \text{and } x_i - x_j \notin S_{ij} \text{ if } i \neq j\}\bigr| \\ &\quad\geqslant \min\left\{p(F) - (n-1)\sum_{i=1}^n m_i,\ \sum_{i=1}^n\bigl(|A_i| - 1\bigr) - 2(n-1)\sum_{i=1}^n m_i + 1\right\},\end{aligned} \tag{1.9}$$

where $m_i = \max_{j\in[1,n]\setminus\{i\}} |S_{ij}|$ for $i = 1, \ldots, n$.

In the next section we will prove Theorem 1.2 with the help of several lemmas. Section 3 is devoted to the proof of Theorem 1.3. Theorem 1.1 and Corollaries 1.1–1.3 will be shown in Section 4. Finally, in Section 5 we deduce a further extension of Theorem 1.3.

2. Proof of Theorem 1.2

Lemma 2.1. *Let $a_1, \ldots, a_n$ be nonzero elements in a field F with $p(F) \neq 2$. Then, for some $\sigma \in S_n$ we have*

$$a_{\sigma(2i-1)} + a_{\sigma(2i)} \neq 0 \quad \text{for all } 0 < i \leqslant \left\lfloor \frac{n}{2} \right\rfloor - \delta(a_1, \ldots, a_n),$$

where $\delta(a_1, \ldots, a_n) \in \{0, 1\}$ takes the value 1 if and only if there exists $a \in F^*$ such that $\{a_1, \ldots, a_n\} = \{a, -a\}$ and

$$\bigl|\{1 \leqslant i \leqslant n\colon a_i = a\}\bigr| \equiv \bigl|\{1 \leqslant i \leqslant n\colon a_i = -a\}\bigr| \equiv 1 \pmod 2. \tag{2.1}$$

Proof. We use induction on n.

The case $n \in \{1, 2\}$ is trivial.

Now let $n > 2$ and assume the desired result for smaller values of n.

In the case $\delta(a_1, \ldots, a_n) = 1$, there is an element $a \in F^*$ such that $\{a_1, \ldots, a_n\} = \{a, -a\}$ and (2.1) holds; thus the desired result follows immediately since $a + a \neq 0$ and $-a + (-a) \neq 0$.

Below we let $\delta(a_1, \ldots, a_n) = 0$. If $a_1 + a_2 = a_1 + a_3 = a_2 + a_3 = 0$, then $a_1 = a_2 = a_3 = 0$ which contradicts the condition $a_1, \ldots, a_n \in F^*$. So for some $1 \leqslant s < t \leqslant n$ we have $a_s + a_t \neq 0$. Without loss of generality we simply suppose that $a_{n-1} + a_n \neq 0$. By the induction hypothesis, for some $\sigma \in S_{n-2}$ we have

$$a_{\sigma(2i-1)} + a_{\sigma(2i)} \neq 0 \quad \text{for all } 0 < i \leqslant \left\lfloor \frac{n-2}{2} \right\rfloor - \delta(a_1, \ldots, a_{n-2}).$$

If $\delta(a_1, \ldots, a_{n-2}) = 0$, then it suffices to set $\sigma(2\lfloor n/2\rfloor - 1) = n - 1$ and $\sigma(2\lfloor n/2\rfloor) = n$.

Now let $\delta(a_1, \ldots, a_{n-2}) = 1$. Then for some $a \in F^*$ we have both $\{a_1, \ldots, a_{n-2}\} = \{a, -a\}$ and

$$\bigl|\{1 \leqslant i \leqslant n-2\colon a_i = a\}\bigr| \equiv \bigl|\{1 \leqslant i \leqslant n-2\colon a_i = -a\}\bigr| \equiv 1 \pmod 2.$$

Case 1. $\{a, -a\} \cap \{a_{n-1}, a_n\} = \emptyset$.

In this case, $a + a_{n-1} \neq 0$ and $-a + a_n \neq 0$. Thus there exists $\sigma \in S_n$ such that $a_{\sigma(2i-1)} = a_{\sigma(2i)} \in \{a, -a\}$ for all $0 < i < \lfloor (n-2)/2\rfloor$, and also

$$a_{\sigma(2\lfloor(n-2)/2\rfloor - 1)} = a, \qquad a_{\sigma(2\lfloor(n-2)/2\rfloor)} = a_{n-1}$$

and

$$a_{\sigma(2\lfloor n/2\rfloor - 1)} = -a, \qquad a_{\sigma(2\lfloor n/2\rfloor)} = a_n.$$

Case 2. $\{a, -a\} \cap \{a_{n-1}, a_n\} \neq \emptyset$.

Without loss of generality we assume that $a_{n-1} = a$. As $\delta(a_1, \ldots, a_n) = 0$ we cannot have $a_{n-1} = a_n \in \{a, -a\}$. Thus $a_n \neq a$. Now $a + a_{n-1} = 2a \neq 0$ and $-a + a_n \neq 0$. As in Case 1 there exists $\sigma \in S_n$ such that $a_{\sigma(2i-1)} = a_{\sigma(2i)} \in \{a, -a\}$ for all $0 < i \leqslant \lfloor n/2 \rfloor$.

So far we have proved the desired result by induction. $\square$

Lemma 2.2. *Let $k_1, \ldots, k_n \in \mathbb{N}$ and $a_1, \ldots, a_n \in F^*$, where F is a field with $p(F) \neq 2$. Set*

$$f(x_1, \ldots, x_n) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{j=1}^{n} (k_j - x_j)_{\sigma(j)-1} a_j^{\sigma(j)-1} \tag{2.2}$$

and let $\delta(a_1, \ldots, a_n)$ be as in Lemma 2.1. Provided the following (i) *or* (ii), *there are $m_1, \ldots, m_n \in \mathbb{N}$ not exceeding* $\max\{2n-3, 0\}$ *such that $m_1 + \cdots + m_n = \binom{n}{2}$ and $f(m_1, \ldots, m_n) \neq 0$.*

(i) $\delta(a_1, \ldots, a_n) = 0$.
(ii) $\delta(a_1, \ldots, a_n) = 1$, *and for some $1 \leqslant s < t \leqslant n$ we have $a_s + a_t = 0$ and $k_s + k_t \not\equiv 1$* $(\mathrm{mod}\ p(F))$. (*A congruence modulo ∞ refers to the corresponding equality.*)

Proof. We use induction on n.

When $n = 1$, obviously we can take $m_1 = \cdots = m_n = 0$ to meet the requirement.

In the case $n = 2$, we have $f(x_1, x_2) = a_2(k_2 - x_2) - a_1(k_1 - x_1)$. Clearly $f(1, 0) - f(0, 1) = a_1 + a_2$. If $f(1, 0) = f(0, 1)$, then $a_1 + a_2 = 0$, $\delta(a_1, a_2) = 1$ and $f(0, 1) = a_2(k_2 - 1) - a_1 k_1 = a_2(k_1 + k_2 - 1) \neq 0$ by condition (ii). Anyway, we have $f(m_1, m_2) \neq 0$ for some $m_1 \in \{0, 1\}$ and $m_2 = 1 - m_1$.

Below we let $n \geqslant 3$ and assume the desired result for smaller values of n. In case (ii), clearly $\delta(a_3, \ldots, a_n) = 0$, and we may simply assume that $s = 1$ and $t = 2$ without loss of generality. By Lemma 2.1, there is a rearrangement $a'_1, \ldots, a'_n$ of $a_1, \ldots, a_n$ such that $a'_{n-2i-1} + a'_{n-2i} \neq 0$ for all $0 \leqslant i < \lfloor n/2 \rfloor - \delta(a_1, \ldots, a_n)$, and $a'_1 = a_1$ and $a'_2 = a_2$ in case (ii). Suppose that $a'_i = a_{\tau(i)}$ for $i = 1, \ldots, n$, where $\tau \in S_n$, and $\tau(1) = 1$ and $\tau(2) = 2$ in case (ii). Set $k'_i = k_{\tau(i)}$ for $i = 1, \ldots, n$. Then

$$\begin{aligned} f(x_1, \ldots, x_n) &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} (k_{\tau(i)} - x_{\tau(i)})_{\sigma\tau(i)-1} \left(a'_i\right)^{\sigma\tau(i)-1} \\ &= \operatorname{sgn}(\tau) \sum_{\pi \in S_n} \operatorname{sgn}(\pi) \prod_{i=1}^{n} \left(k'_i - x_{\tau(i)}\right)_{\pi(i)-1} \left(a'_i\right)^{\pi(i)-1}. \end{aligned}$$

Hence $f(m_1, \ldots, m_n) \neq 0$ for some $m_1, \ldots, m_n \in [0, 2n-3]$ if and only if

$$\sum_{\pi \in S_n} \operatorname{sgn}(\pi) \prod_{i=1}^{n} \left(k'_i - m'_i\right)_{\pi(i)-1} \left(a'_i\right)^{\pi(i)-1} \neq 0$$

for some $m'_1, \ldots, m'_n \in [0, 2n-3]$. Without loss of generality, below we simply assume that $a'_i = a_i$ and $k'_i = k_i$ for all $i = 1, \ldots, n$.

By the induction hypothesis, there are $m_1, \ldots, m_{n-2} \in [0, 2n-3]$ such that $\sum_{j=1}^{n-2} m_j = \binom{n-2}{2}$ and

$$\Sigma := \sum_{\sigma \in S_{n-2}} \operatorname{sgn}(\sigma) \prod_{j=1}^{n-2} (k_j - m_j)_{\sigma(j)-1} a_j^{\sigma(j)-1} \neq 0.$$

Define

$$\begin{aligned} g(x) &= f\left(m_1, \ldots, m_{n-2}, x, \binom{n}{2} - x - m_1 - \cdots - m_{n-2}\right) \\ &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{j=1}^{n-2} (k_j - m_j)_{\sigma(j)-1} a_j^{\sigma(j)-1} \times (k_{n-1} - x)_{\sigma(n-1)-1} a_{n-1}^{\sigma(n-1)-1} \end{aligned}$$

$$\times\left(k_n-\binom{n}{2}+x+\sum_{j=1}^{n-2}m_j\right)_{\sigma(n)-1}a_n^{\sigma(n)-1}.$$

For $\sigma\in S_n$, if $\sigma(1)-1+(\sigma(2)-1)=2n-3$ then $\{\sigma(1),\sigma(2)\}=\{n-1,n\}$. Thus

$$\begin{aligned}\left[x^{2n-3}\right]g(x)&=\sum_{\substack{\sigma\in S_n\\ \{\sigma(n-1),\sigma(n)\}=\{n-1,n\}}}\operatorname{sgn}(\sigma)\prod_{j=1}^{n-2}(k_j-m_j)_{\sigma(j)-1}a_j^{\sigma(j)-1}\\&\quad\times(-a_{n-1})^{\sigma(n-1)-1}a_n^{\sigma(n)-1}\\&=\sum_{\sigma\in S_{n-2}}\operatorname{sgn}(\sigma)\prod_{j=1}^{n-2}(k_j-m_j)_{\sigma(j)-1}a_j^{\sigma(j)-1}\\&\quad\times\left((-a_{n-1})^{n-2}a_n^{n-1}-(-a_{n-1})^{n-1}a_n^{n-2}\right)\\&=(-1)^n(a_{n-1}a_n)^{n-2}(a_{n-1}+a_n)\Sigma\neq 0.\end{aligned}$$

Since $\deg g(x)=2n-3$, there is an integer $m_{n-1}\in[0,2n-3]$ such that $g(m_{n-1})\neq 0$. Set

$$m_n=\binom{n}{2}-\sum_{j=1}^{n-1}m_j=\binom{n}{2}-\binom{n-2}{2}-m_{n-1}=2n-3-m_{n-1}.$$

Then

$$f(m_1,\dots,m_n)=g(m_{n-1})\neq 0.$$

This concludes the induction step and we are done. □

Lemma 2.3. *Let F be a field with $p(F)\neq 2$, and let $a_1,\dots,a_n$ $(n\geqslant 4)$ be nonzero elements of F with $\delta(a_1,\dots,a_n)=1$. Suppose that $p(F)\geqslant\sum_{j=1}^n k_j-n^2+n+1$ where $k_1,\dots,k_n$ are integers not smaller than $2n-3$. Then there are $1\leqslant s<t\leqslant n$ such that $a_s+a_t=0$ and $k_s+k_t\not\equiv 1\pmod{p(F)}$, unless $n=4$ and there is a permutation $\sigma\in S_4$ such that $a_{\sigma(1)}=a_{\sigma(2)}=a_{\sigma(3)}$, $k_{\sigma(1)}=k_{\sigma(2)}=k_{\sigma(3)}=5$ and $k_{\sigma(4)}=p(F)-4$.*

Proof. For any $1\leqslant s<t\leqslant n$ we have

$$\begin{aligned}p(F)-(k_s+k_t-1)&\geqslant\sum_{\substack{1\leqslant j\leqslant n\\ j\neq s,t}}k_j-n^2+n+2\\&\geqslant(n-2)(2n-3)-n^2+n+2=(n-2)(n-4)\end{aligned}$$

and hence

$$\begin{aligned}&k_s+k_t\equiv 1\pmod{p(F)}\\&\iff\quad k_s+k_t-1=p(F),\quad k_i=2n-3\text{ for }i\in[1,n]\setminus\{s,t\},\text{ and }n=4.\end{aligned}$$

Since $\delta(a_1,\dots,a_n)=1$, for some $1\leqslant s<t\leqslant n$ we have $a_s+a_t=0$; also $k_s+k_t\not\equiv 1\pmod{p(F)}$ if $n>4$. This proves the desired result for $n>4$.

Now assume $n=4$. By $\delta(a_1,a_2,a_3,a_4)=1$, there is a permutation $\sigma\in S_4$ such that $a_{\sigma(1)}=a_{\sigma(2)}=a_{\sigma(3)}=-a_{\sigma(4)}$. Clearly $a_{\sigma(i)}+a_{\sigma(4)}=0$ for any $i=1,2,3$. Suppose that $k_{\sigma(i)}+k_{\sigma(4)}\equiv 1\pmod{p(F)}$ for all $i=1,2,3$. By the above, $k_{\sigma(i)}+k_{\sigma(4)}-1=p(F)$ for $i=1,2,3$, and $k_{\sigma(1)}=k_{\sigma(2)}=k_{\sigma(3)}=2n-3=5$. It follows that $k_{\sigma(4)}=p(F)-4$.

The proof of Lemma 2.3 is now complete. □

Lemma 2.4. *Let F be a field of prime characteristic with $p(F) = p \geqslant 7$ and let $a_1 = a_2 = a_3 = a \in F^*$ and $a_4 = -a$. Let $k_1 = k_2 = k_3 = 5$ and $k_4 = p - 4$. Then there are $m_1, m_2, m_3, m_4 \in [0, 3]$ such that $m_1 + m_2 + m_3 + m_4 = \binom{4}{2} = 6$ and*

$$\sum_{\sigma \in S_4} \operatorname{sgn}(\sigma) \prod_{j=1}^{4} (k_j - m_j)_{\sigma(j)-1} a_j^{\sigma(j)-1} \neq 0.$$

Proof. Set $m_1 = 0$, $m_2 = 2$, $m_3 = 3$ and $m_4 = 1$. Then

$$\begin{aligned}
&\sum_{\sigma \in S_4} \operatorname{sgn}(\sigma) \prod_{j=1}^{4} (k_j - m_j)_{\sigma(j)-1} a_j^{\sigma(j)-1} \\
&\quad = \sum_{\sigma \in S_4} \operatorname{sgn}(\sigma) \prod_{j=1}^{3} (5 - m_j)_{\sigma(j)-1} \times (-4 - m_4)_{\sigma(4)-1} (-1)^{\sigma(4)-1} a^{0+1+2+3} \\
&\quad = -480 a^6 \neq 0
\end{aligned}$$

since p does not divide 480. We are done. $\square$

Proof of Theorem 1.2. Set $A_i' = a_i A_i = \{a_i x_i \colon x_i \in A_i\}$ and $a_i' = a_i^{-1}$ for $i = 1, \ldots, n$. Then

$$C = \{y_1 + \cdots + y_n \colon y_1 \in A_1', \ldots, y_n \in A_n', \text{ and } a_i' y_i \neq a_j' y_j \text{ if } i \neq j\}.$$

In the case $n = 1$, clearly

$$|C| = |A_1'| = |A_1| \geqslant \min\{p(F),\ |A_1| - 1^2 + 1\}.$$

When $n = 2$, we have

$$\begin{aligned}
|C| &= \left|\{y_1 + y_2 \colon y_1 \in A_1',\ y_2 \in A_2' \text{ and } y_1 - (a_1')^{-1} a_2' y_2 \neq 0\}\right| \\
&\geqslant \min\{p(F) - [\![a_1' = a_2']\!],\ |A_1'| + |A_2'| - 3\} \quad (\text{by [17, Corollary 3]}) \\
&= \min\{p(F) - [\![a_1 = a_2]\!], |A_1| + |A_2| - 2^2 + 1\}.
\end{aligned}$$

Below we let $n > 2$. Clearly $p(F) \geqslant (n-1)^2 > 2$. Define

$$N = \sum_{j=1}^{n} |A_j| - n^2. \tag{2.3}$$

We want to show that $|C| \geqslant \min\{p(F),\ N + 1\}$.

Let's first assume that $p(F) > N$. Note that $p(F) \geqslant (4-1)^2 > 7$ if $n \geqslant 4$. In view of Lemmas 2.1–2.4, there are $m_1, \ldots, m_n \in [0, 2n-3]$ such that $m_1 + \cdots + m_n = \binom{n}{2}$ and

$$S = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{j=1}^{n} \left(|A_j'| - 1 - m_j\right)_{\sigma(j)-1} (a_j')^{\sigma(j)-1} \neq 0. \tag{2.4}$$

Clearly it suffices to deduce a contradiction under the assumption that $|C| \leqslant N$. Let $P(x_1, \ldots, x_n)$ be the polynomial

$$\prod_{1 \leqslant i < j \leqslant n} (a_j' x_j - a_i' x_i) \times \prod_{j=1}^{n} x_j^{m_j} \times \prod_{x \in C} (x_1 + \cdots + x_n - c) \times (x_1 + \cdots + x_n)^{N - |C|}.$$

Then $\deg P = \sum_{j=1}^{n}(|A'_j|-1)$, since

$$\begin{aligned}
&\big[x_1^{|A'_1|-1}\cdots x_n^{|A'_n|-1}\big]P(x_1,\ldots,x_n)\\
&\quad=\left[\prod_{j=1}^{n}x_j^{|A'_j|-1-m_j}\right]\sum_{\sigma\in S_n}\operatorname{sgn}(\sigma)\prod_{j=1}^{n}\big(a'_jx_j\big)^{\sigma(j)-1}\times(x_1+\cdots+x_n)^N\\
&\quad=\sum_{\substack{\sigma\in S_n\\ \sigma(j)\leqslant|A'_j|-m_j\ \text{for}\ j\in[1,n]}}\operatorname{sgn}(\sigma)\frac{N!}{\prod_{j=1}^{n}(|A'_j|-m_j-\sigma(j))!}\prod_{j=1}^{n}\big(a'_j\big)^{\sigma(j)-1}
\end{aligned}$$

and hence

$$\prod_{j=1}^{n}\big(|A'_j|-1-m_j\big)!\times\big[x_1^{|A'_1|-1}\cdots x_n^{|A'_n|-1}\big]P(x_1,\ldots,x_n)=N!S\neq 0.$$

Thus, by the Combinatorial Nullstellensatz there are $y_1\in A'_1,\ldots,y_n\in A'_n$ such that $P(y_1,\ldots,y_n)\neq 0$ which contradicts the definition of C.

Now we handle the case $p(F)\leqslant N$. Since $n(2n-2)-n^2\leqslant p(F)-1<\sum_{j=1}^{n}|A_j|-n^2$, we can choose $B_j\subseteq A_j$ with $|B_j|\geqslant 2n-2$ so that $M=\sum_{j=1}^{n}|B_j|-n^2=p(F)-1$. As $p(F)>M$, by the above we have

$$\begin{aligned}
|C|&\geqslant\big|\{a_1x_1+\cdots+a_nx_n\colon x_1\in B_1,\ldots,x_n\in B_n,\ \text{and}\ x_i\neq x_j\ \text{if}\ i\neq j\}\big|\\
&\geqslant M+1=\min\big\{p(F),N\big\}.
\end{aligned}$$

The proof of Theorem 1.2 is now complete. □

3. Proof of Theorem 1.3

The inequality (1.5) holds trivially if $p(F)\leqslant\deg P$ or $\sum_{i=1}^{n}|A_i|<n+2\deg P$. Below we assume that $p(F)>\deg P$ and $\sum_{i=1}^{n}|A_i|\geqslant n+2\deg P$.

Write

$$P(x_1,\ldots,x_n)=\sum_{\substack{j_1,\ldots,j_n\geqslant 0\\ j_1+\cdots+j_n\leqslant\deg P}}c_{j_1,\ldots,j_n}x_1^{j_1}\cdots x_n^{j_n}\quad\text{with}\ c_{j_1,\ldots,j_n}\in F,\tag{3.1}$$

and define

$$P^*(x_1,\ldots,x_n)=\sum_{\substack{j_1,\ldots,j_n\geqslant 0\\ j_1+\cdots+j_n=\deg P}}c_{j_1,\ldots,j_n}(x_1)_{j_1}\cdots(x_n)_{j_n}\in F[x_1,\ldots,x_n].\tag{3.2}$$

It is easy to see that

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

To distinguish from the integer 1, we use e to denote the multiplicative identity of the field F. For each $i=1,\ldots,n$, clearly the set

$$B_i=\big\{me\colon m\in\big[|A_i|-k_i-1,|A_i|-1\big]\big\}$$

has cardinality k_i+1 since $k_i\leqslant\deg P<p(F)$. Thus, by the Combinatorial Nullstellensatz, there are

$$m_1\in\big[|A_1|-k_1-1,|A_1|-1\big],\ \ldots,\ m_n\in\big[|A_n|-k_n-1,|A_n|-1\big]\tag{3.3}$$

such that

$$P^*(m_1e,\dots,m_ne)\neq 0. \tag{3.4}$$

Define

$$M=m_1+\cdots+m_n-\deg P. \tag{3.5}$$

Clearly

$$M\geqslant\sum_{i=1}^n\bigl(|A_i|-k_i-1\bigr)-\deg P=\sum_{i=1}^n|A_i|-n-2\deg P\geqslant 0.$$

Observe that

$$\begin{aligned}&\bigl[x_1^{m_1}\cdots x_n^{m_n}\bigr]P(x_1,\dots,x_n)(x_1+\cdots+x_n)^M\\&=\sum_{\substack{j_1\in[0,m_1],\dots,j_n\in[0,m_n]\\ j_1+\cdots+j_n=\deg P}}\frac{M!}{(m_1-j_1)!\cdots(m_n-j_n)!}c_{j_1,\dots,j_n}\end{aligned}$$

and thus

$$\begin{aligned}&m_1!\cdots m_n!\bigl[x_1^{m_1}\cdots x_n^{m_n}\bigr]P(x_1,\dots,x_n)(x_1+\cdots+x_n)^M\\&=M!\sum_{\substack{j_1,\dots,j_n\geqslant 0\\ j_1+\cdots+j_n=\deg P}}(m_1e)_{j_1}\cdots(m_ne)_{j_n}c_{j_1,\dots,j_n}\\&=M!P^*(m_1e,\dots,m_ne).\end{aligned}$$

In the case $|C|\leqslant M<p(F)$, with the help of (3.4) we have

$$\begin{aligned}&\bigl[x_1^{m_1}\cdots x_n^{m_n}\bigr]P(x_1,\dots,x_n)(x_1+\cdots+x_n)^{M-|C|}\prod_{c\in C}(x_1+\cdots+x_n-c)\\&=\bigl[x_1^{m_1}\cdots x_n^{m_n}\bigr]P(x_1,\dots,x_n)(x_1+\cdots+x_n)^M\neq 0,\end{aligned}$$

hence by the Combinatorial Nullstellensatz there are $x_1\in A_1,\dots,x_n\in A_n$ such that

$$P(x_1,\dots,x_n)(x_1+\cdots+x_n)^{M-|C|}\prod_{c\in C}(x_1+\cdots+x_n-c)\neq 0$$

which is impossible by the definition of C. Therefore, either

$$p(F)\leqslant M\leqslant\sum_{i=1}^n\bigl(|A_i|-1\bigr)-\deg P \tag{3.6}$$

or

$$|C|\geqslant M+1\geqslant\sum_{i=1}^n|A_i|-n-2\deg P+1. \tag{3.7}$$

If $p(F)>\sum_{i=1}^n(|A_i|-1)-\deg P$, then (3.6) fails and hence

$$\begin{aligned}|C|&\geqslant\sum_{i=1}^n|A_i|-n-2\deg P+1\\&=\min\Biggl\{p(F)-\deg P,\ \sum_{i=1}^n|A_i|-n-2\deg P+1\Biggr\}.\end{aligned}$$

In the case $p(F) \leqslant \sum_{i=1}^n (|A_i|-1) - \deg P$, as $\sum_{i=1}^n k_i = \deg P$ there are $A_1' \subseteq A_1, \ldots, A_n' \subseteq A_n$ such that

$$\left|A_1'\right| > k_1, \ldots, \left|A_n'\right| > k_n, \quad \text{and} \quad \sum_{i=1}^n \left(\left|A_i'\right| - 1\right) - \deg P = p(F) - 1 < p(F),$$

therefore

$$\begin{aligned} |C| &\geqslant \left|\left\{x_1 + \cdots + x_n\colon x_1 \in A_1', \ldots, x_n \in A_n', \text{ and } P(x_1, \ldots, x_n) \neq 0\right\}\right| \\ &\geqslant \min\left\{p(F) - \deg P,\ \sum_{i=1}^n \left|A_i'\right| - n - 2\deg P + 1\right\} \\ &= p(F) - \deg P = \min\left\{p(F) - \deg P,\ \sum_{i=1}^n |A_i| - n - 2\deg P + 1\right\}. \end{aligned}$$

This concludes the proof. □

4. Proofs of Corollaries 1.1–1.3 and Theorem 1.1

Proof of Corollary 1.1. As A has a subset of cardinality $\lceil \sqrt{4p-7}\,\rceil$, it suffices to consider the case $|A| = \lceil \sqrt{4p-7}\,\rceil$. Since $n-1 \leqslant |A|/2 - 1 < \sqrt{p}$ and $(n - A|/2)^2 \leqslant |A|^2/4 - p + 1$, applying Theorem 1.2 we get

$$\{a_1x_1 + \cdots + a_nx_n\colon x_1, \ldots, x_n \in A \text{ and } x_i \neq x_j \text{ if } i \neq j\} = F_p.$$

This concludes the proof. □

Proof of Corollary 1.2. Both (1.6) and (1.7) are trivial in the case $|A| \leqslant m(n-1)$. Below we assume that $|A| > m(n-1)$, and put $A_i = \{a_ix\colon x \in A\}$ for $i = 1, \ldots, n$.

(i) Set $b_j = [x^m]f(x)a_j^{-m}$ for $j \in [1, n]$, and define

$$P(x_1, \ldots, x_n) = \prod_{1 \leqslant i < j \leqslant n} \left(f\left(a_j^{-1}x_j\right) - f\left(a_i^{-1}x_i\right)\right).$$

Note that

$$\begin{aligned} \prod_{1 \leqslant i < j \leqslant n} \left(b_jx_j^m - b_ix_i^m\right) &= \det\left(\left(b_jx_j^m\right)^{i-1}\right)_{1 \leqslant i, j \leqslant n} \\ &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^n b_{\sigma(i)}^{i-1} x_{\sigma(i)}^{(i-1)m}. \end{aligned}$$

Therefore

$$\left[\prod_{i=1}^n x_i^{(i-1)m}\right] P(x_1, \ldots, x_n) \neq 0 \quad \text{and} \quad \sum_{i=1}^n (i-1)m = \deg P.$$

In view of Theorem 1.3,

$$\begin{aligned} &\left|\left\{a_1x_1 + \cdots + a_nx_n\colon x_1, \ldots, x_n \in A, \text{ and } f(x_i) \neq f(x_j) \text{ if } i \neq j\right\}\right| \\ &\quad = \left|\left\{y_1 + \cdots + y_n\colon y_1 \in A_1, \ldots, y_n \in A_n, \text{ and } P(y_1, \ldots, y_n) \neq 0\right\}\right| \\ &\quad \geqslant \min\left\{p(F) - \deg P,\ |A_1| + \cdots + |A_n| - n - 2\deg P + 1\right\} \\ &\quad = \min\left\{p(F) - m\binom{n}{2},\ n\left(|A| - 1\right) - mn(n-1) + 1\right\}. \end{aligned}$$

So we have (1.6).

(ii) Let $P(x_1,\dots,x_n)$ be the polynomial

$$\prod_{1\leqslant i<j\leqslant n}\left(\left(a_j^{-1}x_j-a_i^{-1}x_i\right)^{2m-1-|S_{ij}|}\prod_{s\in S_{ij}}\left(a_j^{-1}x_j-a_i^{-1}x_i+s\right)\right).$$

By [23, (2.8)],

$$\begin{aligned}&\left[\prod_{i=1}^n x_i^{(m-1)(n-1)+i-1}\right]P(a_1x_1,\dots,a_nx_n)\\&=\left[\prod_{i=1}^n x_i^{(m-1)(n-1)+i-1}\right]\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)^{2m-1}=(-1)^{(m-1)\binom n2}Ne,\end{aligned}$$

where $N=(mn)!/(m!^n n!)\in\mathbb{Z}^+=\{1,2,3,\dots\}$. Clearly $N=1$ if $m=1$ or $n=1$. If $\min\{m,n\}\geqslant 2$ and $mn\geqslant p(F)$, then

$$\begin{aligned}p(F)-(2m-1)\binom n2&\leqslant mn-1-\left(m-\frac12\right)n(n-1)\\&=n\left(m-\left(m-\frac12\right)(n-1)\right)-1\leqslant 0.\end{aligned}$$

So (1.7) holds trivially if $mn\geqslant p(F)$.

Below we handle the case $mn<p(F)$, thus $Ne\neq 0$. Note that

$$\left[\prod_{i=1}^n x_i^{(m-1)(n-1)+i-1}\right]P(x_1,\dots,x_n)\neq 0.$$

Clearly $\sum_{i=1}^n((m-1)(n-1)+i-1)=(2m-1)\binom n2=\deg P$. Observe that $|A_i|=|A|>m(n-1)\geqslant (m-1)(n-1)+i-1$ for all $i\in[1,n]$. Applying Theorem 1.3 we get

$$\begin{aligned}&\left|\{a_1x_1+\dots+a_nx_n\colon x_1,\dots,x_n\in A,\text{ and } x_i-x_j\notin S_{ij}\text{ if } i<j\}\right|\\&\geqslant\left|\left\{y_1+\dots+y_n\colon y_1\in A_1,\dots,y_n\in A_n,\text{ and } P(y_1,\dots,y_n)\neq 0\right\}\right|\\&\geqslant\min\left\{p(F)-\deg P,\ |A_1|+\dots+|A_n|-n-2\deg P+1\right\}\\&=\min\left\{p(F)-(2m-1)\binom n2,\ n\left(|A|-1\right)-(2m-1)n(n-1)+1\right\}.\end{aligned}$$

This proves (1.7).

So far we have completed the proof of Corollary 1.2. □

The Dyson conjecture mentioned in Section 1 can be restated as follows: For any $m_1,\dots,m_n\in\mathbb{N}$ we have

$$\begin{aligned}&\left[x_1^{m_1(n-1)}\cdots x_n^{m_n(n-1)}\right]\prod_{1\leqslant i<j\leqslant n}(x_i-x_j)^{m_i+m_j}\\&=(-1)^{\sum_{j=1}^n(j-1)m_j}\frac{(m_1+\dots+m_n)!}{m_1!\cdots m_n!}.\end{aligned}\tag{4.1}$$

A combinatorial proof of this was given by D. Zeilberger [26] in 1982. Below we use (4.1) to prove Corollary 1.3.

Proof of Corollary 1.3. We only need to consider the nontrivial case $\sum_{i=1}^n m_i<p(F)$. Similar to the proof of Corollary 1.2, it suffices to note that the coefficient of the monomial $\prod_{i=1}^n x_i^{m_i(n-1)}$ in the polynomial $\prod_{1\leqslant i<j\leqslant n}(x_i-x_j)^{m_i+m_j}$ over F does not vanish by (4.1) and $\sum_{k=1}^n m_k<p(F)$. □

Proof of Theorem 1.1. If $p(F) - \binom{n}{2} \geqslant n|A| - n^2 + 1$, then (1.1) follows from (1.8).

Now assume that $p(F) - \binom{n}{2} \leqslant n|A| - n^2$. Then

$$n|A| \geqslant p(F) - \binom{n}{2} + n^2 \geqslant \frac{3n^2 - 5n}{2} - \frac{n^2 - n}{2} + n^2 = 2n^2 - 2n$$

and hence $|A| \geqslant 2n - 2$. Note also that if $n > 1$ then $p(F) \geqslant n(3n-5)/2 \geqslant (n-1)^2$. Thus, by applying Theorem 1.2 we obtain the desired result. □

5. A further extension of Theorem 1.3

Recently Z.W. Sun [21] employed the Combinatorial Nullstellensatz to establish the following result on value sets of polynomials.

Theorem 5.1. *(See Sun [21].) Let $A_1, \ldots, A_n$ be finite nonempty subsets of a field F, and let*

$$f(x_1, \ldots, x_n) = a_1 x_1^k + \cdots + a_n x_n^k + g(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n] \tag{5.1}$$

with

$$k \in \mathbb{Z}^+,\ a_1, \ldots, a_n \in F^* \text{ and } \deg g < k. \tag{5.2}$$

(i) *We have*

$$\bigl|\bigl\{f(x_1, \ldots, x_n):\ x_1 \in A_1, \ldots, x_n \in A_n\bigr\}\bigr| \geqslant \min\Biggl\{p(F), \sum_{i=1}^{n} \biggl\lfloor \frac{|A_i| - 1}{k} \biggr\rfloor + 1\Biggr\}.$$

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

$$\bigl|\bigl\{f(x_1, \ldots, x_n):\ x_1 \in A_1, \ldots, x_n \in A_n,\ \text{and } x_i \neq x_j \text{ if } i \neq j\bigr\}\bigr| \geqslant \min\Biggl\{p(F),\ \sum_{i=1}^{n} \biggl\lfloor \frac{|A_i| - i}{k} \biggr\rfloor + 1\Biggr\}.$$

Remark 5.1. Let $a_1, \ldots, a_n$ be nonzero elements of a finite field F and let k be a positive integer. Concerning lower bounds for $|\{a_1 x_1^k + \cdots + a_k x_n^k:\ x_1, \ldots, x_n \in F\}|$, the reader may consult [6] and [25] for earlier results.

Motivated by a concrete example, Sun [21] actually raised the following extension of Conjecture 1.1.

Conjecture 5.1. *(See Sun [21].) Let $f(x_1, \ldots, x_n)$ be a polynomial over a field F given by* (5.1) *and* (5.2). *Provided that $p(F) \neq n+1$ and $n > k$, for any finite subset A of F we have*

$$\bigl|\bigl\{f(x_1, \ldots, x_n):\ x_1, \ldots, x_n \in A,\ \text{and } x_i \neq x_j \text{ if } i \neq j\bigr\}\bigr| \geqslant \min\Biggl\{p(F) - [\![n = 2\ \&\ a_1 = -a_2]\!],\ \frac{n(|A| - n) - \{n\}_k\{|A| - n\}_k}{k} + 1\Biggr\},$$

where we use $\{m\}_k$ to denote the least nonnegative residue of an integer m modulo k.

Sun [21] proved the last inequality with the lower bound replaced by $\min\{p(F),\ |A| - n + 1\}$.

Theorem 1.3 on restricted sumsets can be extended to the following general result on restricted value sets.

Theorem 5.2. *Let F be a field, and let $f(x_1,\dots,x_n)\in F[x_1,\dots,x_n]$ be given by (5.1) and (5.2). Let $P(x_1,\dots,x_n)$ be a polynomial over F with $[x_1^{k_1}\cdots x_n^{k_n}]P(x_1,\dots,x_n)\neq 0$, where $k_1,\dots,k_n$ are nonnegative integers with $k_1+\dots+k_n=\deg P$. Let $A_1,\dots,A_n$ be finite subsets of F with $|A_i|>k_i$ for $i=1,\dots,n$. Then, for the restricted value set*

$$V=\bigl\{f(x_1,\dots,x_n)\colon\ x_1\in A_1,\dots,x_n\in A_n,\ \text{and } P(x_1,\dots,x_n)\neq 0\bigr\},\tag{5.3}$$

we have

$$|V|\geqslant\min\left\{p(F)-\sum_{i=1}^n\left\lfloor\frac{k_i}{k}\right\rfloor,\ \sum_{i=1}^n\left(\left\lfloor\frac{|A_i|-k_i-1}{k}\right\rfloor-\left\lfloor\frac{k_i}{k}\right\rfloor\right)+1\right\}.\tag{5.4}$$

Proof. It suffices to consider the nontrivial case

$$p(F)>\sum_{i=1}^n\left\lfloor\frac{k_i}{k}\right\rfloor\quad\text{and}\quad\sum_{i=1}^n\left(\left\lfloor\frac{|A_i|-k_i-1}{k}\right\rfloor-\left\lfloor\frac{k_i}{k}\right\rfloor\right)\geqslant 0.$$

For $i=1,\dots,n$ let r_i be the least nonnegative residue of k_i modulo k. Write $P(x_1,\dots,x_n)$ in the form (3.1) and consider the polynomial

$$\bar P(x_1,\dots,x_n)=\sum_{\substack{j_i\in r_i+k\mathbb{N}\ \text{for}\ i=1,\dots,n\\ j_1+\dots+j_n=\deg P}}c_{j_1,\dots,j_n}\prod_{i=1}^n a_i^{(r_i-j_i)/k}(x_i)_{(j_i-r_i)/k}.$$

Clearly

$$\begin{aligned}&\left[\prod_{i=1}^n x_i^{\lfloor k_i/k\rfloor}\right]\bar P(x_1,\dots,x_n)\\&\quad=\sum_{\substack{j_i\in k_i+k\mathbb{N}\ \text{for}\ i=1,\dots,n\\ \sum_{i=1}^n j_i=\sum_{i=1}^n k_i}}c_{j_1,\dots,j_n}\prod_{i=1}^n a_i^{(r_i-j_i)/k}\cdot\left[\prod_{i=1}^n x_i^{\lfloor k_i/k\rfloor}\right]\prod_{i=1}^n(x_i)_{(j_i-r_i)/k}\\&\quad=c_{k_1,\dots,k_n}\prod_{i=1}^n a_i^{(r_i-k_i)/k}\neq 0.\end{aligned}$$

For $i=1,\dots,n$ let $B_i=\{me\colon\ m\in I_i\}$ where

$$I_i=\left[\left\lfloor\frac{|A_i|-r_i-1}{k}\right\rfloor-\left\lfloor\frac{k_i}{k}\right\rfloor,\ \left\lfloor\frac{|A_i|-r_i-1}{k}\right\rfloor\right].$$

Clearly $|B_i|=\lfloor k_i/k\rfloor+1$ since $\lfloor k_i/k\rfloor<p(F)$. Note also that

$$\left\lfloor\frac{|A_i|-r_i-1}{k}\right\rfloor\geqslant\left\lfloor\frac{k_i-r_i}{k}\right\rfloor=\frac{k_i-r_i}{k}=\left\lfloor\frac{k_i}{k}\right\rfloor.$$

In light of the Combinatorial Nullstellensatz, there are $q_1\in I_1,\dots,q_n\in I_n$ such that

$$\bar P(q_1e,\dots,q_ne)\neq 0.\tag{5.5}$$

Set $m_i=kq_i+r_i$ for $i=1,\dots,n$. Then

$$\begin{aligned}M=\frac{\sum_{i=1}^n m_i-\deg P}{k}&=\sum_{i=1}^n\frac{m_i-k_i}{k}=\sum_{i=1}^n\left(q_i-\left\lfloor\frac{k_i}{k}\right\rfloor\right)\\&\geqslant\sum_{i=1}^n\left(\left\lfloor\frac{|A_i|-k_i-1}{k}\right\rfloor-\left\lfloor\frac{k_i}{k}\right\rfloor\right)\geqslant 0\end{aligned}$$

and

$$\begin{aligned}&\big[x_1^{m_1}\cdots x_n^{m_n}\big]P(x_1,\ldots,x_n)f(x_1,\ldots,x_n)^M\\&=\big[x_1^{m_1}\cdots x_n^{m_n}\big]P(x_1,\ldots,x_n)\big(a_1x_1^k+\cdots+a_nx_n^k\big)^M\\&=\sum_{\substack{j_i\in m_i-k\mathbb{N}\text{ for }i=1,\ldots,n\\ j_1+\cdots+j_n=\deg P}}c_{j_1,\ldots,j_n}\frac{M!}{\prod_{i=1}^n((m_i-j_i)/k)!}\prod_{i=1}^n a_i^{(m_i-j_i)/k}.\end{aligned}$$

So we have

$$\begin{aligned}&q_1!\cdots q_n!\big[x_1^{m_1}\cdots x_n^{m_n}\big]P(x_1,\ldots,x_n)f(x_1,\ldots,x_n)^M\\&=M!\sum_{\substack{j_i\in m_i-k\mathbb{N}\text{ for }i=1,\ldots,n\\ j_1+\cdots+j_n=\deg P}}c_{j_1,\ldots,j_n}\prod_{i=1}^n a_i^{(m_i-j_i)/k}(q_ie)_{\lfloor j_i/k\rfloor}\\&=M!a_1^{q_1}\cdots a_n^{q_n}\bar P(q_1e,\ldots,q_ne).\end{aligned}$$

If $|V|\leqslant M<p(F)$, then by (5.5) and the above we have

$$\begin{aligned}&\big[x_1^{m_1}\cdots x_n^{m_n}\big]P(x_1,\ldots,x_n)f(x_1,\ldots,x_n)^{M-|V|}\prod_{v\in V}\big(f(x_1,\ldots,x_n)-v\big)\\&=\big[x_1^{m_1}\cdots x_n^{m_n}\big]P(x_1,\ldots,x_n)f(x_1,\ldots,x_n)^M\neq 0,\end{aligned}$$

hence by the Combinatorial Nullstellensatz there are $x_1\in A_1,\ldots,x_n\in A_n$ such that

$$P(x_1,\ldots,x_n)f(x_1,\ldots,x_n)^{M-|V|}\prod_{v\in V}\big(f(x_1,\ldots,x_n)-v\big)\neq 0$$

which contradicts (5.3). Therefore, either

$$p(F)\leqslant M=\sum_{i=1}^n\left(q_i-\left\lfloor\frac{k_i}{k}\right\rfloor\right)\leqslant\sum_{i=1}^n\left(\left\lfloor\frac{|A_i|-r_i-1}{k}\right\rfloor-\left\lfloor\frac{k_i}{k}\right\rfloor\right)=\sum_{i=1}^n\left\lfloor\frac{|A_i|-k_i-1}{k}\right\rfloor$$

or

$$|V|\geqslant M+1\geqslant\sum_{i=1}^n\left(\left\lfloor\frac{|A_i|-k_i-1}{k}\right\rfloor-\left\lfloor\frac{k_i}{k}\right\rfloor\right)+1.$$

If $p(F)>\sum_{i=1}^n\lfloor(|A_i|-k_i-1)/k\rfloor$, then we have

$$\begin{aligned}|V|&\geqslant\sum_{i=1}^n\left(\left\lfloor\frac{|A_i|-k_i-1}{k}\right\rfloor-\left\lfloor\frac{k_i}{k}\right\rfloor\right)+1\\&=\min\left\{p(F)-\sum_{i=1}^n\left\lfloor\frac{k_i}{k}\right\rfloor,\ \sum_{i=1}^n\left(\left\lfloor\frac{|A_i|-k_i-1}{k}\right\rfloor-\left\lfloor\frac{k_i}{k}\right\rfloor\right)+1\right\}.\end{aligned}$$

In the case $p(F)\leqslant\sum_{i=1}^n\lfloor(|A_i|-k_i-1)/k\rfloor$, as $\sum_{i=1}^n k_i=\deg P$ there are $A_1'\subseteq A_1,\ldots,A_n'\subseteq A_n$ such that

$$\left|A_1'\right|>k_1,\ldots,\left|A_n'\right|>k_n,\quad\text{and}\quad\sum_{i=1}^n\left\lfloor\frac{|A_i'|-k_i-1}{k}\right\rfloor=p(F)-1<p(F),$$

therefore

$$\begin{aligned}|V| &\geqslant \left|\left\{x_1+\cdots+x_n\colon x_1\in A_1',\ldots,x_n\in A_n',\ \text{and}\ P(x_1,\ldots,x_n)\neq 0\right\}\right|\\ &\geqslant \min\left\{p(F)-\sum_{i=1}^n\left\lfloor\frac{k_i}{k}\right\rfloor,\ \sum_{i=1}^n\left(\left\lfloor\frac{|A_i'|-k_i-1}{k}\right\rfloor-\left\lfloor\frac{k_i}{k}\right\rfloor\right)+1\right\}\\ &= p(F)-\sum_{i=1}^n\left\lfloor\frac{k_i}{k}\right\rfloor\\ &= \min\left\{p(F)-\sum_{i=1}^n\left\lfloor\frac{k_i}{k}\right\rfloor,\ \sum_{i=1}^n\left(\left\lfloor\frac{|A_i|-k_i-1}{k}\right\rfloor-\left\lfloor\frac{k_i}{k}\right\rfloor\right)+1\right\}.\end{aligned}$$

We are done. □

Here is a consequence of Theorem 5.2.

Corollary 5.1. *Let F be a field and let $f(x_1,\ldots,x_n)\in F[x_1,\ldots,x_n]$ be given by (5.1) and (5.2). Let $A_1,\ldots,A_n$ be finite subsets of F with $|A_i|\geqslant i$ for $i=1,\ldots,n$. Then, for the restricted value set*

$$V=\left\{f(x_1,\ldots,x_n)\colon x_1\in A_1,\ldots,x_n\in A_n,\ \text{and}\ x_1,\ldots,x_n\ \text{are distinct}\right\},\tag{5.6}$$

we have

$$|V|+\Delta(n,k)\geqslant \min\left\{p(F),\sum_{i=1}^n\left\lfloor\frac{|A_i|-i}{k}\right\rfloor+1\right\},\tag{5.7}$$

where

$$\Delta(n,k)=\left\lfloor\frac{n}{k}\right\rfloor\left(n-k\frac{\lfloor n/k\rfloor+1}{2}\right).\tag{5.8}$$

Proof. We apply Theorem 5.2 with

$$P(x_1,\ldots,x_n)=\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)=\det\left(x_j^{i-1}\right)_{1\leqslant i,j\leqslant n}.$$

Note that $[\prod_{i=1}^n x_i^{i-1}]P(x_1,\ldots,x_n)=1\neq 0$. By Theorem 5.2,

$$|V|+\sum_{i=1}^n\left\lfloor\frac{i-1}{k}\right\rfloor\geqslant \min\left\{p(F),\ \sum_{i=1}^n\left\lfloor\frac{|A_i|-i}{k}\right\rfloor+1\right\}.$$

So it suffices to observe that

$$\begin{aligned}\sum_{i=1}^n\left\lfloor\frac{i-1}{k}\right\rfloor &= \sum_{q=0}^{\lfloor n/k\rfloor-1}\sum_{r=1}^{k}\left\lfloor\frac{qk+r-1}{k}\right\rfloor+\sum_{k\lfloor n/k\rfloor<i\leqslant n}\left\lfloor\frac{i-1}{k}\right\rfloor\\ &= \sum_{q=0}^{\lfloor n/k\rfloor-1}kq+\left(n-k\left\lfloor\frac{n}{k}\right\rfloor\right)\left\lfloor\frac{n}{k}\right\rfloor\\ &= k\left\lfloor\frac{n}{k}\right\rfloor\frac{\lfloor n/k\rfloor-1}{2}+\left(n-k\left\lfloor\frac{n}{k}\right\rfloor\right)\left\lfloor\frac{n}{k}\right\rfloor=\Delta(n,k).\end{aligned}$$

This concludes the proof. □

Lemma 5.1. *Let k and n be positive integers. Then, for any $m \in \mathbb{Z}$ we have*

$$\sum_{i=1}^{n}\left\lfloor \frac{m-i}{k}\right\rfloor = m\left\lfloor \frac{n}{k}\right\rfloor + \{n\}_k\left\lfloor \frac{m-n}{k}\right\rfloor - \frac{k}{2}\left\lfloor \frac{n}{k}\right\rfloor\left(\left\lfloor \frac{n}{k}\right\rfloor + 1\right) + \{m\}_k[\![\{m\}_k < \{n\}_k]\!]. \tag{5.9}$$

Proof. Let $f(m)$ and $g(m)$ denote the left-hand side and the right-hand side of (5.9) respectively. We first prove that $f(n) = g(n)$. In fact, by the proof of Corollary 5.1,

$$f(n) = \sum_{j=0}^{n-1}\left\lfloor \frac{j}{n}\right\rfloor = \Delta(n,k) = g(n).$$

Next we show that $f(m+1) - f(m) = g(m+1) - g(m)$ for any $m \in \mathbb{Z}$. Observe that

$$\begin{aligned} f(m+1) - f(m) &= \sum_{i=1}^{n}\left(\left\lfloor \frac{m+1-i}{k}\right\rfloor - \left\lfloor \frac{m-i}{k}\right\rfloor\right) \\ &= \left|\left\{1 \leqslant i \leqslant n\colon\ i \equiv m+1 \ (\mathrm{mod}\ k)\right\}\right| \\ &= \left|\left\{q \in \mathbb{N}\colon\ \{m\}_k + kq < n\right\}\right| = \left\lfloor \frac{n}{k}\right\rfloor + [\![\{m\}_k < \{n\}_k]\!]. \end{aligned}$$

Also,

$$\begin{aligned} & g(m+1) - g(m) - \left\lfloor \frac{n}{k}\right\rfloor \\ &= \{n\}_k[\![m+1 \equiv n \ (\mathrm{mod}\ k)]\!] + \{m+1\}_k[\![\{m+1\}_k < \{n\}_k]\!] - \{m\}_k[\![\{m\}_k < \{n\}_k]\!] \\ &= \{m+1\}_k[\![\{m+1\}_k \leqslant \{n\}_k]\!] - \{m\}_k[\![\{m\}_k < \{n\}_k]\!] \\ &= [\![\{m\}_k < \{n\}_k]\!]. \end{aligned}$$

So far we have proved (5.9) for all $m \in \mathbb{Z}$. □

The following result partially resolves Conjecture 5.1.

Corollary 5.2. *Let F be a field and let $f(x_1,\ldots,x_n) \in F[x_1,\ldots,x_n]$ be given by* (5.1) *and* (5.2). *Let $A_1,\ldots,A_n$ be finite subsets of F with $|A_1| = \cdots = |A_n| = m \geqslant n$. Then, for the restricted value set V in* (5.6) *we have*

$$|V| \geqslant \min\left\{p(F) - \Delta(n,k),\ \frac{n(m-n) - \{n\}_k\{m-n\}_k}{k} + r_{k,m,n} + 1\right\}, \tag{5.10}$$

where

$$r_{k,m,n} = \{m\}_k[\![\{m\}_k < \{n\}_k]\!]. \tag{5.11}$$

Remark 5.2. In the special case $a_1 = \cdots = a_n$, H. Pan and Sun [18] proved (5.10) with $\Delta(n,k)$ omitted.

Proof of Corollary 5.2. By Lemma 5.1,

$$\begin{aligned} \sum_{i=1}^{n}\left\lfloor \frac{m-i}{k}\right\rfloor - \Delta(n,k) &= (m-n)\left\lfloor \frac{n}{k}\right\rfloor + \{n\}_k\left\lfloor \frac{m-n}{k}\right\rfloor + r_{k,m,n} \\ &= \frac{n(m-n)}{k} - \{n\}_k\frac{m-n}{k} + \{n\}_k\left\lfloor \frac{m-n}{k}\right\rfloor + r_{k,m,n} \\ &= \frac{n(m-n) - \{n\}_k\{m-n\}_k}{k} + r_{k,m,n}. \end{aligned}$$

So, the desired result follows from Corollary 5.1. □

Acknowledgments

The authors are grateful to the two referees for their helpful comments.

References

[1] N. Alon, Combinatorial Nullstellensatz, Combin. Probab. Comput. 8 (1999) 7–29.
[2] N. Alon, M.B. Nathanson, I.Z. Ruzsa, Adding distinct congruence classes modulo a prime, Amer. Math. Monthly 102 (1995) 250–255.
[3] N. Alon, M.B. Nathanson, I.Z. Ruzsa, The polynomial method and restricted sums of congruence classes, J. Number Theory 56 (1996) 404–417.
[4] N. Alon, M. Tarsi, A nowhere-zero point in linear mappings, Combinatorica 9 (1989) 393–395.
[5] P. Balister, J.P. Wheeler, The Erdős–Heilbronn conjecture for finite groups, Acta Arith. 139 (2009) 185–197.
[6] S. Chowla, H.B. Mann, E.G. Straus, Some applications of the Cauchy–Davenport theorem, Nor. Vidensk. Selsk. Forh. Trondheim 32 (1959) 74–80.
[7] S. Dasgupta, G. Károlyi, O. Serra, B. Szegedy, Transversals of additive Latin squares, Israel J. Math. 126 (2001) 17–28.
[8] J.A. Dias da Silva, Y.O. Hamidoune, Cyclic spaces for Grassmann derivatives and additive theory, Bull. Lond. Math. Soc. 26 (1994) 140–146.
[9] F.J. Dyson, Statistical theory of the energy levels of complex systems I, J. Math. Phys. 3 (1962) 140–156.
[10] P. Erdős, H. Heilbronn, On the addition of residue classes modulo p, Acta Arith. 9 (1964) 149–159.
[11] I.J. Good, Short proof of a conjecture of Dyson, J. Math. Phys. 11 (1970) 1884.
[12] S. Guo, Z.W. Sun, A variant of Tao's method with application to restricted sumsets, J. Number Theory 129 (2009) 434–438.
[13] Q.H. Hou, Z.W. Sun, Restricted sums in a field, Acta Arith. 102 (2002) 239–249.
[14] G. Károlyi, An inverse theorem for the restricted set addition in abelian groups, J. Algebra 290 (2005) 557–593.
[15] J.X. Liu, Z.W. Sun, Sums of subsets with polynomial restrictions, J. Number Theory 97 (2002) 301–304.
[16] M.B. Nathanson, Additive Number Theory: Inverse Problems and the Geometry of Sumsets, Grad. Texts in Math., vol. 165, Springer, New York, 1996.
[17] H. Pan, 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.
[18] H. Pan, Z.W. Sun, A new extension of the Erdős–Heilbronn conjecture, J. Combin. Theory Ser. A 116 (2009) 1374–1381.
[19] Z.W. Sun, Restricted sums of subsets of $\mathbb{Z}$, Acta Arith. 99 (2001) 41–60.
[20] Z.W. Sun, On Snevily's conjecture and restricted sumsets, J. Combin. Theory Ser. A 103 (2003) 291–304.
[21] Z.W. Sun, On value sets of polynomials over a field, Finite Fields Appl. 14 (2008) 470–481.
[22] Z.W. Sun, An additive theorem and restricted sumsets, Math. Res. Lett. 15 (2008) 1263–1276.
[23] Z.W. Sun, Y.N. Yeh, On various restricted sumsets, J. Number Theory 114 (2005) 209–220.
[24] T. Tao, V.H. Vu, Additive Combinatorics, Cambridge Univ. Press, Cambridge, 2006.
[25] A. Tietäväinen, On diagonal forms over finite fields, Ann. Univ. Turku. Ser. A I 118 (1968) 1–10.
[26] D. Zeilberger, A combinatorial proof of Dyson's conjecture, Discrete Math. 41 (1982) 317–321.