Number Theory (S. Kanemitsu & J.-Y. Liu, eds.), World Sci., Singapore, 2007, pp. 190-213.

A Survey of Problems and Results on Restricted Sumsets

Zhi-Wei Sun

Department of Mathematics, Nanjing University
Nanjing 210093, People's Republic of China
zwsun@nju.edu.cn
http://math.nju.edu.cn/~zwsun

Abstract

Additive number theory is currently an active field related to combinatorics. In this paper we give a survey of problems and results concerning lower bounds for cardinalities of various restricted sumsets with elements in a field or an abelian group.

1. Erdős-Heilbronn conjecture and the polynomial method

Let $A = \{a_1, \ldots, a_k\}$ and $B = \{b_1, \ldots, b_l\}$ be two finite subsets of $\mathbb{Z}$ with $a_1 < \cdots < a_k$ and $b_1 < \cdots < b_l$. Observe that

$$a_1 + b_1 < a_2 + b_1 < \cdots < a_k + b_1 < a_k + b_2 < \cdots < a_k + b_l,$$

whence we see that the sumset

$$A + B = \{a + b \colon a \in A \text{ and } b \in B\}$$

contains at least $k + l - 1$ elements. In particular, $|2A| \geqslant 2|A| - 1$, where $|A|$ denotes the cardinality of A, and $2A$ stands for $A + A$.

The following fundamental theorem was first proved by A. Cauchy [9] in 1813 and then rediscovered by H. Davenport [11] in 1935.

Cauchy-Davenport Theorem. *Let A and B be non-empty subsets of the field $\mathbb{Z}/p\mathbb{Z}$ where p is a prime. Then*

$$|A + B| \geqslant \min\{p, |A| + |B| - 1\}. \tag{1.1}$$

For lots of important results on sumsets over $\mathbb{Z}$, the reader is referred to the recent book [38] by T. Tao and V. H. Vu. In this paper we mainly focus our attention on restricted sumsets with elements in a field or an abelian group.

In combinatorics, for a finite sequence $\{A_i\}_{i=1}^n$ of sets, a sequence $\{a_i\}_{i=1}^n$ is called a *system of distinct representatives* of $\{A_i\}_{i=1}^n$ if $a_1 \in A_1, \ldots, a_n \in A_n$ and $a_1, \ldots, a_n$ are distinct. A fundamental theorem of P. Hall [17] states that $\{A_i\}_{i=1}^n$ has a system of distinct

Supported by the National Science Fund (No. 10425103) for Distinguished Young Scholars in China.

representatives if and only if $|\bigcup_{i\in I} A_i| \geqslant |I|$ for all $I \subseteq \{1,\ldots,n\}$. The reader may consult [31] for a simple proof of Hall's theorem.

In 1964 P. Erdős and H. Heilbronn [13] made the following challenging conjecture.

Erdős-Heilbronn Conjecture. *Let p be a prime, and let A be a non-empty subset of the field $\mathbb{Z}/p\mathbb{Z}$. Then $|2^\wedge A| \geqslant \min\{p, 2|A|-3\}$, where*

$$2^\wedge A = \{a+b:\ a,b\in A \text{ and } a\neq b\}.$$

This conjecture remained open until it was confirmed by Dias da Silva and Y. Hamidoune [12] thirty years later, with the help of the representation theory of groups.

For a general field F, the additive order of the (multiplicative) identity of F is either infinite or a prime, which we denote by $p(F)$. The *characteristic* of the field F is defined as follows:

$$\mathrm{ch}(F) = \begin{cases} p & \text{if } p(F) \text{ is a prime } p,\\ 0 & \text{if } p(F)=\infty. \end{cases} \tag{1.2}$$

Now we state Dias da Silva and Y. Hamidoune's extension of the Erdős-Heilbronn conjecture.

Dias da Silva–Hamidoune Theorem [12]**.** *Let F be a field, and let $n \in \mathbb{Z}^+ = \{1,2,3,\ldots\}$. Then, for any finite subset A of F, we have*

$$|n^\wedge A| \geq \min\{p(F),\ n|A| - n^2 + 1\}, \tag{1.3}$$

where $n^\wedge A$ denotes the set of all sums of n distinct elements of A.

If p is a prime, $A \subseteq \mathbb{Z}/p\mathbb{Z}$ and $|A| > \sqrt{4p-7}$, then by the Dias da Silva–Hamidoune theorem, any element of $\mathbb{Z}/p\mathbb{Z}$ can be written as a sum of $\lfloor |A|/2 \rfloor$ distinct elements of A (see [12]), where $\lfloor\cdot\rfloor$ is the well-known floor function.

In 1995–1996 N. Alon, M. B. Nathanson and I. Z. Ruzsa ([4],[5]) developed a polynomial method rooted in [6] to prove the Erdős-Heilbronn conjecture and some similar results. The method turns out to be very powerful and has many applications in number theory and combinatorics.

Now we introduce the above-mentioned polynomial method. We begin with a lemma.

Lemma 1.1 (Alon, Nathanson and Ruzsa [4][5])**.** *Let F be a field and let $A_1,\ldots,A_n$ be non-empty finite subsets of F. Let $f(x_1,\ldots,x_n) \in F[x_1,\ldots,x_n]$ have degree less than $k_i = |A_i|$ in x_i for each $i = 1,\ldots,n$. If $f(a_1,\ldots,a_n) = 0$ for all $a_1 \in A_1,\ldots,a_n \in A_n$, then $f(x_1,\ldots,x_n)$ is identically zero.*

This lemma can be proved by using induction on n and noting that a non-zero polynomial $P(x) \in F[x]$ of degree less than a positive integer k cannot have k distinct zeroes in F.

The central part of the polynomial method is the following important principle formulated by Alon in 1999.

Combinatorial Nullstellensatz (Alon [1])**.** *Let $A_1,\ldots,A_n$ be finite subsets of a field F, and let $f(x_1,\ldots,x_n) \in F[x_1,\ldots,x_n]$.*

(i) *Set $g_i(x) = \prod_{a\in A_i}(x-a)$ for $i = 1,\ldots,n$. Then*

$$f(a_1,\ldots,a_n) = 0 \ \text{ for all } a_1\in A_1,\ldots,a_n\in A_n \tag{1.4}$$

if and only if there are $h_1(x_1,\ldots,x_n),\ldots,h_n(x_1,\ldots,x_n) \in F[x_1,\ldots,x_n]$ with $\deg h_i \leqslant \deg f - \deg g_i$ for $i = 1,\ldots,n$, such that

$$f(x_1,\ldots,x_n) = \sum_{i=1}^n g_i(x_i)h_i(x_1,\ldots,x_n). \tag{1.5}$$

(ii) *Suppose that* $\deg f = k_1 + \cdots + k_n$ *where* $0 \leqslant k_i < |A_i|$ *for* $i = 1, \ldots, n$. *If* (1.4) *holds then*

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

where $[x_1^{k_1} \cdots x_n^{k_n}] f(x_1, \ldots, x_n)$ *denotes the coefficient of* $x_1^{k_1} \cdots x_n^{k_n}$ *in* $f(x_1, \ldots, x_n)$.

Proof. (i) If there are $h_1(x_1, \ldots, x_n), \ldots, h_n(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$ such that (1.5) holds, then for any $a_1 \in A_1, \ldots, a_n \in A_n$ we have

$$f(a_1, \ldots, a_n) = \sum_{i=1}^{n} g_i(a_i) h_i(a_1, \ldots, a_n) = 0.$$

Now we consider the converse. Write

$$f(x_1, \ldots, x_n) = \sum_{j_1, \ldots, j_n \geqslant 0} f_{j_1, \ldots, j_n} x_1^{j_1} \ldots x_n^{j_n}$$

and

$$x^j = g_i(x) q_{ij}(x) + r_i^{(j)}(x),$$

where $q_{ij}(x), r_i^{(j)}(x) \in F[x]$ and $\deg r_i^{(j)}(x) < \deg g_i(x) = |A_i|$. Note that both $r_i^{(j)}(x)$ and $g_i(x) q_{ij}(x) = x^j - r_i^{(j)}(x)$ have degree not exceeding j. Clearly

$$\begin{aligned} f(x_1, \ldots, x_n) = & \sum_{\substack{j_1, \ldots, j_n \geqslant 0 \\ j_1 + \cdots + j_n \leqslant \deg f}} f_{j_1, \ldots, j_n} \prod_{i=1}^{n} \left(g_i(x_i) q_{ij_i}(x_i) + r_i^{(j_i)}(x_i) \right) \\ = & \bar{f}(x_1, \ldots, x_n) + \sum_{i=1}^{n} g_i(x_i) h_i(x_1, \ldots, x_n), \end{aligned}$$

where

$$\bar{f}(x_1, \ldots, x_n) = \sum_{j_1, \ldots, j_n \geqslant 0} f_{j_1, \ldots, j_n} \prod_{i=1}^{n} r_i^{(j_i)}(x_i)$$

and each $h_i(x_1, \ldots, x_n)$ is a suitable polynomial over F with $\deg g_i + \deg h_i \leqslant \deg f$. If $a_1 \in A_1, \ldots, a_n \in A_n$, then

$$\bar{f}(a_1, \ldots, a_n) = \sum_{j_1, \ldots, j_n \geqslant 0} f_{j_1, \ldots, j_n} \prod_{i=1}^{n} a_i^{j_i} = f(a_1, \ldots, a_n) = 0.$$

Since the degree of $\bar{f}(x_1, \ldots, x_n)$ in x_i is smaller than $|A_i|$, by Lemma 1.1 the polynomial $\bar{f}(x_1, \ldots, x_n)$ is identically zero. Therefore (1.5) holds.

(ii) By part (i) we can write

$$f(x_1, \ldots, x_n) = \sum_{i=1}^{n} g_i(x_i) h_i(x_1, \ldots, x_n)$$

with $h_i(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$ and $\deg h_i \leqslant \deg f - \deg g_i$. Since $k_1 + \cdots + k_n = \deg f$ and $k_i < |A_i|$ for $i = 1, \ldots, n$, we have

$$[x_1^{k_1} \cdots x_n^{k_n}] f(x_1, \ldots, x_n) = \sum_{i=1}^{n} [x_1^{k_1} \cdots x_n^{k_n}] x_i^{|A_i|} h_i(x_1, \ldots, x_n) = 0.$$

This concludes the proof.

Here is a useful lemma implied by the Combinatorial Nullstellensatz.

ANR Lemma [5]. *Let $A_1, \ldots, A_n$ be finite subsets of a field F with $k_i = |A_i| > 0$ for $i = 1, \ldots, n$. Let $f(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n] \setminus \{0\}$ and $\deg f \leqslant \sum_{i=1}^n (k_i - 1)$. If*

$$[x_1^{k_1-1} \cdots x_n^{k_n-1}] f(x_1, \ldots, x_n)(x_1 + \cdots + x_n)^{\sum_{i=1}^n (k_i-1) - \deg f} \neq 0, \tag{1.6}$$

then

$$|\{a_1 + \cdots + a_n \colon a_i \in A_i,\ f(a_1, \ldots, a_n) \neq 0\}| \geqslant \sum_{i=1}^n (k_i - 1) - \deg f + 1. \tag{1.7}$$

Proof. Assume that $C = \{a_1 + \cdots + a_n \colon a_i \in A_i,\ f(a_1, \ldots, a_n) \neq 0\}$ has cardinality not exceeding $K = \sum_{i=1}^n (k_i - 1) - \deg f$. Then the polynomial

$$P(x_1, \ldots, x_n) := f(x_1, \ldots, x_n)(x_1 + \cdots + x_n)^{K-|C|} \prod_{c \in C} (x_1 + \cdots + x_n - c)$$

is of degree $\sum_{i=1}^n (k_i - 1)$ with the coefficient of $x_1^{k_1-1} \cdots x_n^{k_n-1}$ non-zero. Applying the second part of the Combinatorial Nullstellensatz, we find that $P(a_1, \ldots, a_n) \neq 0$ for some $a_1 \in A_1, \ldots, a_n \in A_n$. This is impossible since $a_1 + \cdots + a_n \in C$ if $f(a_1, \ldots, a_n) \neq 0$.

We remark that a variant of this lemma appeared in Q. H. Hou and Z. W. Sun [18].

Alon-Nathanson-Ruzsa Theorem [5]. *Let $A_1, \ldots, A_n$ be finite non-empty subsets of a field F with $|A_1| < \cdots < |A_n|$. Then, for the set*

$$A_1 \dot{+} \cdots \dot{+} A_n = \Big\{ \sum_{i=1}^n a_i \colon a_i \in A_i,\ \text{and } a_i \neq a_j \text{ if } i \neq j \Big\}, \tag{1.8}$$

we have

$$|A_1 \dot{+} \cdots \dot{+} A_n| \geqslant \min \Big\{ p(F), \sum_{i=1}^n |A_i| - \frac{n(n+1)}{2} + 1 \Big\}. \tag{1.9}$$

This follows from the ANR lemma and the following fact. If $k_1, \ldots, k_n \in \mathbb{Z}^+$, then

$$\begin{aligned} &[x_1^{k_1-1} \cdots x_n^{k_n-1}] \prod_{1 \leqslant i < j \leqslant n} (x_j - x_i) \times (x_1 + \cdots + x_n)^{\sum_{i=1}^n k_i - n(n+1)/2} \\ &\quad = \frac{(k_1 + \cdots + k_n - n(n+1)/2)!}{(k_1 - 1)! \cdots (k_n - 1)!} \prod_{1 \leqslant i < j \leqslant n} (k_j - k_i). \end{aligned} \tag{1.10}$$

The Dias da Silva–Hamidoune theorem can be deduced from the ANR theorem in the following way: Suppose that $|A| = k \geqslant n$. Let $A_1, \ldots, A_n$ be subsets of A with cardinalities $k - n + 1, k - n + 2, \ldots, k$ respectively. By the ANR theorem,

$$|A_1 \dot{+} \cdots \dot{+} A_n| \geqslant \min \Big\{ p(F), \sum_{i=1}^n (|A_i| - i) + 1 \Big\} = \min\{p(F), (k-n)n + 1\}.$$

As $n^\wedge A \supseteq A_1 \dot{+} \cdots \dot{+} A_n$, the desired inequality (1.3) follows.

In addition, the reader may also consult [24], [3] and [38] for the polynomial method, and [34] for its connections with covers of $\mathbb{Z}$ by residue classes and zero-sum problems on abelian p-groups.

2. Various sumsets with polynomial restrictions

By a sophisticated induction argument (cf. [7] and [30]), it can be shown that if $A_1,\ldots,A_n$ are finite subsets of $\mathbb{Z}$ with $|A_1|\leqslant\cdots\leqslant|A_n|$ and $|A_i|\geqslant i$ for all $i=1,\ldots,n$, then

$$|A_1\dot{+}\cdots\dot{+}A_n|\geqslant 1+\sum_{i=1}^n\min_{i\leqslant j\leqslant n}(|A_j|-j).$$

Now we state a result on sumsets with linear restrictions over $\mathbb{Z}$.

Theorem 2.1 (Z. W. Sun [30]). *Let $A_1,\ldots,A_n$ be finite subsets of $\mathbb{Z}$, and let V be a set of quin-tuples (s,t,μ,ν,w) with $1\leqslant s,t\leqslant n$, $s\neq t$, $\mu,\nu\in\mathbb{Z}\setminus\{0\}$ and $w\in\mathbb{Z}$. If each $V_i=\{(s,t,\mu,\nu,w)\in V: i\in\{s,t\}\}$ has cardinality less than $|A_i|$, then*

$$\begin{aligned}&|\{a_1+\ldots+a_n: a_i\in A_i,\ \text{and } \mu a_i+\nu a_j\neq w \text{ if } (i,j,\mu,\nu,w)\in V\}|\\ &\geqslant\sum_{i=1}^n|A_i|-2|V|-n+1=1+\sum_{i=1}^n(|A_i|-|V_i|-1)>0.\end{aligned}\tag{2.1}$$

Clearly Theorem 2.1 has the following consequence.

Corollary 2.1 (Z. W. Sun [30]). *Let $A_1,\ldots,A_n$ be finite subsets of $\mathbb{Z}$ with $|A_i|\geqslant 2n-1$ for all $i=1,\ldots,n$. Then*

$$\left|\left\{\sum_{i=1}^n a_i:\ a_i\in A_i,\ a_i\neq\pm a_j\ \text{if } i\neq j\right\}\right|\geqslant\sum_{i=1}^n|A_i|-2n^2+n+1.\tag{2.2}$$

All the remaining theorems in this section have been obtained via the polynomial method. Preceding a theorem we usually state a lemma which makes the method applicable.

Lemma 2.1. *Let k,m,n be integers with $m\geqslant 0$, $n>1$ and $k>m(n-1)$.*

(i) (Q. H. Hou and Z. W. Sun [18]) *We have*

$$\begin{aligned}&[x_1^{k-1}\cdots x_n^{k-1}]\prod_{1\leq i<j\leq n}(x_i-x_j)^{2m}(x_1+\cdots+x_n)^{(k-1-m(n-1))n}\\ &=(-1)^{mn(n-1)/2}\frac{((k-1-m(n-1))n)!}{(m!)^n}\prod_{j=1}^n\frac{(jm)!}{(k-1-(j-1)m)!}.\end{aligned}\tag{2.3}$$

(ii) (Z. W. Sun and Y. N. Yeh [37]) *If $m>0$ then*

$$\begin{aligned}&[x_1^{k-n}\cdots x_n^{k-1}]\prod_{1\leqslant i<j\leqslant n}(x_i-x_j)^{2m-1}(x_1+\cdots+x_n)^{(k-1-m(n-1))n}\\ &=(-1)^{(m-1)n(n-1)/2}\frac{((k-1-m(n-1))n)!}{(m!)^n n!}\prod_{j=1}^n\frac{(jm)!}{(k-1-(j-1)m)!}.\end{aligned}\tag{2.4}$$

Theorem 2.2. *Let $k,m\in\mathbb{N}=\{0,1,2,\ldots\}$ and $n\in\mathbb{Z}^+$. Let F be a field with $p(F)>\max\{mn,(k-1-m(n-1))n\}$, and let $A_1,\ldots,A_n$ be finite subsets of F with $\max_{1\leqslant i\leqslant n}|A_i|=k$. Set*

$$C=\{a_1+\cdots+a_n\colon a_1\in A_1,\ldots,a_n\in A_n,\ a_i-a_j\notin S_{ij}\ \text{if } i<j\},$$

where S_{ij} $(1\leqslant i<j\leqslant n)$ are subsets of F.

(i) (Q. H. Hou and Z. W. Sun [18]) *If $|A_1|=\cdots=|A_n|=k$, and $|S_{ij}|\leqslant 2m$ for all $1\leqslant i<j\leqslant n$, then we have $|C|\geqslant(k-1-m(n-1))n+1$.*

(ii) (Z. W. Sun and Y. N. Yeh [37]) *If* $|A_i| = k-n+i$ *for* $i = 1, \ldots, n$, *and* $|S_{ij}| < 2m$ *for all* $1 \leqslant i < j \leqslant n$, *then* $|C| \geqslant (k-1-m(n-1))n+1$.

The following conjecture posed by Z. W. Sun in [18] is open even for the rational field.

Conjecture 2.1 (Z. W. Sun, 2002)**.** *Let* $A_1, \ldots, A_n$ *be finite non-empty subsets of a field* F. *For* $1 \leqslant i < j \leqslant n$, *let* S_{ij} *and* S_{ji} *be finite subsets of* F *with* $|S_{ij}| \equiv |S_{ji}| \pmod 2$. *Then*

$$\begin{aligned} &|\{a_1+\cdots+a_n\colon a_1 \in A_1, \ldots, a_n \in A_n,\ a_i - a_j \notin S_{ij} \text{ if } i \neq j\}| \\ &\quad \geqslant \min\Big\{p(F), \sum_{i=1}^n |A_i| - \sum_{1\leqslant i<j\leqslant n} (|S_{ij}|+|S_{ji}|) - n + 1\Big\}. \end{aligned} \tag{2.5}$$

Lemma 2.2 (J. X. Liu and Z. W. Sun [23])**.** *Let* $k, m, n \in \mathbb{Z}^+$ *with* $k-1 \geqslant m(n-1)$. *Then*

$$\begin{aligned} &[x_1^{k-n}\cdots x_n^{k-1}] \prod_{1\leqslant i<j\leqslant n} (x_j^m - x_i^m)(x_1+\cdots+x_n)^{(k-1)n-(m+1)\binom{n}{2}} \\ &= (-m)^{\binom{n}{2}} \frac{((k-1)n-(m+1)\binom{n}{2})!1!2!\cdots(n-1)!}{(k-1)!(k-1-m)!\cdots(k-1-(n-1)m)!}. \end{aligned} \tag{2.6}$$

Theorem 2.3 (J. X. Liu and Z. W. Sun [23])**.** *Let* $k, m, n \in \mathbb{Z}^+$ *with* $k > m(n-1)$, *and let* $A_1, \ldots, A_n$ *be subsets of a field* F *such that*

$$|A_n| = k \text{ and } |A_{i+1}| - |A_i| \in \{0,1\} \text{ for } i = 1, \ldots, n-1.$$

Let $P_1(x), \ldots, P_n(x) \in F[x]$ *be monic and of degree* m. *If* $p(F) > (k-1)n - (m+1)\binom{n}{2}$, *then*

$$|\{a_1+\cdots+a_n\colon a_i \in A_i, \text{and } P_i(a_i) \neq P_j(a_j) \text{ if } i \neq j\}| \geqslant (k-1)n-(m+1)\binom{n}{2}+1. \tag{2.7}$$

Here we pose the following conjecture.

Conjecture 2.2. *Under the conditions of Theorem 2.3, we have*

$$|\{a_1+\cdots+a_n\colon a_i \in A_i, \text{and } P_i(a_i) \neq P_j(a_j) \text{ if } i \neq j\}| \geqslant p(F)$$

if $p(F) \leqslant (k-1)n-(m+1)\binom{n}{2}$.

Lemma 2.3 (Z. W. Sun [33])**.** *Let* R *be a commutative ring with identity. Let* $A = (a_{ij})_{1\leqslant i,j\leqslant n}$ *be a matrix over* R, *and let* $\det(A) = |a_{ij}|_{1\leqslant i,j\leqslant n}$ *be the determinant of* A. *Let* $k, m_1, \ldots, m_n \in \mathbb{N}$.

(i) *If* $m_1 \leqslant \cdots \leqslant m_n \leqslant k$, *then we have*

$$[x_1^k\cdots x_n^k]|a_{ij}x_j^{m_i}|_{1\leqslant i,j\leqslant n}(x_1+\cdots+x_n)^{kn-\sum_{i=1}^n m_i} = \frac{(kn-\sum_{i=1}^n m_i)!}{\prod_{i=1}^n (k-m_i)!}\det(A). \tag{2.8}$$

(ii) *If* $m_1 < \cdots < m_n \leqslant k$ *then*

$$\begin{aligned} &[x_1^k\cdots x_n^k]|a_{ij}x_j^{m_i}|_{1\leqslant i,j\leqslant n} \prod_{1\leqslant i<j\leqslant n}(x_j-x_i)\cdot\Big(\sum_{s=1}^n x_s\Big)^{kn-\binom{n}{2}-\sum_{i=1}^n m_i} \\ &\quad = (-1)^{\binom{n}{2}} \frac{(kn-\binom{n}{2}-\sum_{i=1}^n m_i)!}{\prod_{i=1}^n \prod_{\substack{m_i<j\leqslant k \\ j\neq m_{i+1},\ldots,m_n}} (j-m_i)} \mathrm{per}(A), \end{aligned} \tag{2.9}$$

where $\mathrm{per}(A)$ *is the permanent* $\|a_{ij}\|_{1\leqslant i,j\leqslant n}=\sum_{\sigma\in S_n}a_{1,\sigma(1)}\cdots a_{n,\sigma(n)}$ *and* S_n *is the symmetric group of all the permutations on* $\{1,\ldots,n\}$.

(iii) *Suppose that* $K=kn-\sum_{i=1}^n(l_i+m_i)\geqslant 0$ *where* $l_1,\ldots,l_n\in\mathbb{N}$. *Then*

$$\begin{aligned}&[x_1^k\cdots x_n^k]|a_{ij}x_j^{l_i}|_{1\leqslant i,j\leqslant n}|x_j^{m_i}|_{1\leqslant i,j\leqslant n}(x_1+\cdots+x_n)^K\\=&[x_1^k\cdots x_n^k]|a_{ij}x_j^{m_i}|_{1\leqslant i,j\leqslant n}|x_j^{l_i}|_{1\leqslant i,j\leqslant n}(x_1+\cdots+x_n)^K.\end{aligned}\tag{2.10}$$

Theorem 2.4 (Z. W. Sun [33]). *Let* $k,m,n\in\mathbb{Z}^+$ *with* $k>m(n-1)$, *and let* $A_1,\ldots,A_n$ *be subsets of a field* F *with cardinality* k. *Let* $P_1(x),\ldots,P_n(x)\in F[x]$ *have degree* m *with leading coefficients* $b_1,\ldots,b_n$ *respectively.*

(i) *Suppose that* $b_1,\ldots,b_n$ *are distinct. If* $p(F)>(k-1)n-m\binom{n}{2}$, *then*

$$\left|\left\{\sum_{i=1}^n a_i\colon a_1\in A_1,\ldots,a_n\in A_n,\ \text{and } P_i(a_i)\neq P_j(a_j)\ \text{if } i\neq j\right\}\right|\geqslant(k-1)n-m\binom{n}{2}+1.\tag{2.11}$$

(ii) *Assume that the permanent* $\|b_j^{i-1}\|_{1\leqslant i,j\leqslant n}$ *does not vanish. If* $p(F)$ *is greater than* $(k-1)n-(m+1)\binom{n}{2}$, *then*

$$\left|\left\{\sum_{i=1}^n a_i\colon a_i\in A_i,\ a_i\neq a_j\text{ and }P_i(a_i)\neq P_j(a_j)\ \text{if } i\neq j\right\}\right|\geqslant(k-1)n-(m+1)\binom{n}{2}+1.\tag{2.12}$$

(iii) *We have* $\|b_j^{i-1}\|_{1\leqslant i,j\leqslant n}\neq 0$, *if* F *is the complex field* $\mathbb{C}$, $b_1,\ldots,b_n$ *are* q*th roots of unity, and* $n!$ *does not belong to the set*

$$D(q)=\left\{\sum_{p\mid q}px_p\colon x_p\in\{0,1,2,\ldots\}\text{ for any prime divisor } p \text{ of } q\right\}.$$

Now we raise the following conjecture.

Conjecture 2.3. *When* F *is a field with* $p(F)\leqslant(k-1)n-m\binom{n}{2}$, *the right-hand side of the inequality* (2.11) *in Theorem* 2.4(i) *should be replaced by* $p(F)$. *Similarly, when* F *is a field with* $p(F)\leqslant(k-1)n-(m+1)\binom{n}{2}$, *the right-hand side of the inequality* (2.12) *in Theorem* 2.4(ii) *should be replaced by* $p(F)$.

The following lemma has the same flavor as Lemma 2.3, but it was only recently noted and applied by the author.

Lemma 2.4 (Z. W. Sun [35]). *Let* R *be a commutative ring with identity. Let* $A=(a_{ij})_{1\leqslant i,j\leqslant n}$ *be a matrix over* R, *and let* $\mathrm{per}(A)=\|a_{ij}\|_{1\leqslant i,j\leqslant n}$ *be the permanent of* A. *Let* $k,m_1,\ldots,m_n\in\mathbb{N}$.

(i) *If* $m_1\leqslant\cdots\leqslant m_n\leqslant k$, *then we have*

$$[x_1^k\cdots x_n^k]\|a_{ij}x_j^{m_i}\|_{1\leqslant i,j\leqslant n}(x_1+\cdots+x_n)^{kn-\sum_{i=1}^n m_i}\frac{(kn-\sum_{i=1}^n m_i)!}{\prod_{i=1}^n(k-m_i)!}\mathrm{per}(A).\tag{2.13}$$

(ii) *If* $m_1<\cdots<m_n\leqslant k$ *then*

$$\begin{aligned}&[x_1^k\cdots x_n^k]\|a_{ij}x_j^{m_i}\|_{1\leqslant i,j\leqslant n}\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)\cdot\Big(\sum_{s=1}^n x_s\Big)^{kn-\binom{n}{2}-\sum_{i=1}^n m_i}\\&=(-1)^{\binom{n}{2}}\frac{(kn-\binom{n}{2}-\sum_{i=1}^n m_i)!}{\prod_{i=1}^n\prod_{\substack{m_i<j\leqslant k\\ j\neq m_{i+1},\ldots,m_n}}(j-m_i)}\det(A).\end{aligned}\tag{2.14}$$

(iii) *Suppose that* $K = kn - \sum_{i=1}^n (l_i + m_i) \geqslant 0$ *where* $l_1, \ldots, l_n$ *are also non-negative integers. Then*

$$\begin{aligned}&[x_1^k \cdots x_n^k] \|a_{ij} x_j^{l_i}\|_{1\leqslant i,j\leqslant n} |x_j^{m_i}|_{1\leqslant i,j\leqslant n} (x_1 + \cdots + x_n)^K \\ =&[x_1^k \cdots x_n^k] \|a_{ij} x_j^{m_i}\|_{1\leqslant i,j\leqslant n} |x_j^{l_i}|_{1\leqslant i,j\leqslant n} (x_1 + \cdots + x_n)^K\end{aligned} \tag{2.15}$$

and also

$$\begin{aligned}&[x_1^k \cdots x_n^k] \|a_{ij} x_j^{l_i}\|_{1\leqslant i,j\leqslant n} \|x_j^{m_i}\|_{1\leqslant i,j\leqslant n} (x_1 + \cdots + x_n)^K \\ =&[x_1^k \cdots x_n^k] \|a_{ij} x_j^{m_i}\|_{1\leqslant i,j\leqslant n} \|x_j^{l_i}\|_{1\leqslant i,j\leqslant n} (x_1 + \cdots + x_n)^K\end{aligned} \tag{2.16}$$

Theorem 2.5 (Z. W. Sun [35]). *Let* $A_1, \ldots, A_n$ *be finite subsets of a field* F *with* $|A_1| = \cdots = |A_n| = k > m(n-1)$ *where* $m \in \mathbb{Z}^+$, *and let* $P_1(x), \ldots, P_n(x) \in F[x]$ *have degree at most* m *with* $[x^m]P_1(x), \ldots, [x^m]P_n(x)$ *distinct. If* $p(F) > (k-1)n - (m+1)\binom{n}{2}$, *then the restricted sumset*

$$\left\{ \sum_{i=1}^n a_i : a_i \in A_i,\ a_i \neq a_j \text{ for } i \neq j,\ \text{and } \|P_j(a_j)^{i-1}\|_{1\leqslant i,j\leqslant n} \neq 0 \right\} \tag{2.17}$$

has cardinality at least $(k-1)n - (m+1)\binom{n}{2} + 1 > (m-1)\binom{n}{2}$.

Conjecture 2.4. *Under the conditions of Theorem 2.5, if* $p(F) \leqslant (k-1)n - (m+1)\binom{n}{2}$ *then the restricted sumset in* (2.17) *has cardinality at least* $p(F)$.

Corollary 2.2 (Z. W. Sun [35]). *Let* $A_1, \ldots, A_n$ *and* $B = \{b_1, \ldots, b_n\}$ *be subsets of a field with cardinality* n. *Then there are distinct* $a_1 \in A_1, \ldots, a_n \in A_n$ *such that the permanent* $\|(a_j b_j)^{i-1}\|_{1\leqslant i,j\leqslant n}$ *is non-zero.*

Theorem 2.6 (Z. W. Sun [35]). *Let* h, k, l, m, n *be positive integers satisfying*

$$k - 1 \geqslant m(n-1) \quad \text{and} \quad l - 1 \geqslant h(n-1).$$

Let F *be a field with* $p(F) > \max\{K, L\}$, *where*

$$K = (k-1)n - (m+1)\binom{n}{2} \text{ and } L = (l-1)n - (h+1)\binom{n}{2}.$$

Assume that $c_1, \ldots, c_n \in F$ *are distinct and* $A_1, \ldots, A_n, B_1, \ldots, B_n$ *are subsets of* F *with*

$$|A_1| = \cdots = |A_n| = k \text{ and } |B_1| = \cdots = |B_n| = l.$$

Let $P_1(x), \ldots, P_n(x), Q_1(x), \ldots, Q_n(x) \in F[x]$ *be monic polynomials with* $\deg P_i(x) = m$ *and* $\deg Q_i(x) = h$ *for* $i = 1, \ldots, n$. *Then, for any* $S, T \subseteq F$ *with* $|S| \leqslant K$ *and* $|T| \leqslant L$, *there exist* $a_1 \in A_1, \ldots, a_n \in A_n, b_1 \in B_1, \ldots, b_n \in B_n$ *such that* $a_1 + \cdots + a_n \notin S$, $b_1 + \cdots + b_n \notin T$, *and also*

$$a_i b_i c_i \neq a_j b_j c_j,\ P_i(a_i) \neq P_j(a_j),\ Q_i(b_i) \neq Q_j(b_j) \quad \text{if } 1 \leqslant i < j \leqslant n. \tag{2.18}$$

Lemma 2.5 (Z. W. Sun [35]). *Let* $k, m, n \in \mathbb{Z}^+$ *with* $k - 1 \geqslant m(n-1)$. *Then*

$$\begin{aligned}&[x_1^{k-1} \cdots x_n^{k-1}] \prod_{1\leqslant i<j\leqslant n} (x_j - x_i)^{2m-1} (x_j y_j - x_i y_i) \cdot (x_1 + \cdots + x_n)^N \\ &= (-1)^{m\binom{n}{2}} \frac{(mn)! N!}{(m!)^n n!} \prod_{r=0}^{n-1} \frac{(rm)!}{(k-1-rm)!} \cdot \|y_j^{i-1}\|_{1\leqslant i,j\leqslant n},\end{aligned} \tag{2.19}$$

where $N=(k-1-m(n-1))n$.

Theorem 2.7 (Z. W. Sun [35]). *Let* k,m,n *be positive integers with* $k-1\geqslant m(n-1)$, *and let* F *be a field with* $p(F)>\max\{mn,(k-1-m(n-1))n\}$. *Assume that* $c_1,\ldots,c_n\in F$ *are distinct, and* $A_1,\ldots,A_n,B_1,\ldots,B_n$ *are subsets of* F *with* $|A_1|=\cdots=|A_n|=k$ *and* $|B_1|=\cdots=|B_n|=n$. *Let* $S_{ij}\subseteq F$ *with* $|S_{ij}|<2m$ *for all* $1\leqslant i<j\leqslant n$. *Then there are distinct* $b_1\in B_1,\ldots,b_n\in B_n$ *such that the restricted sumset*

$$S=\{a_1+\cdots+a_n:\ a_i\in A_i,\ a_i-a_j\notin S_{ij}\ \text{and}\ a_ib_ic_i\neq a_jb_jc_j\ \text{if}\ i<j\}\tag{2.20}$$

has at least $(k-1-m(n-1))n+1$ *elements.*

3. Snevily's conjecture and additive theorems

Suppose that $\{a_1,\ldots,a_n\}$, $\{b_1,\ldots,b_n\}$ and $\{a_1+b_1,\ldots,a_n+b_n\}$ are complete systems of residues modulo n. Let $\sigma=0+1+\cdots+(n-1)=n(n-1)/2$. Since $\sum_{i=1}^n(a_i+b_i)=\sum_{i=1}^n a_i+\sum_{i=1}^n b_i$, we have $\sigma\equiv\sigma+\sigma\pmod n$ and hence $2\nmid n$.

In 1999 H. S. Snevily [28] made the following interesting conjecture.

Snevily's Conjecture. *Let* G *be an additive abelian group with* $|G|$ *odd. Let* A *and* B *be subsets of* G *with cardinality* $n>0$. *Then there is a numbering* $\{a_i\}_{i=1}^n$ *of the elements of* A *and a numbering* $\{b_i\}_{i=1}^n$ *of the elements of* B *such that* $a_1+b_1,\ldots,a_n+b_n$ *are distinct.*

Theorem 3.1. (i) (N. Alon [2]) *Let* p *be an odd prime and* A *be a non-empty subset of* $\mathbb{Z}/p\mathbb{Z}$ *with cardinality* $n<p$. *For any given* $b_1,\ldots,b_n\in\mathbb{Z}/p\mathbb{Z}$, *we can find a numbering* $\{a_i\}_{i=1}^n$ *of the elements of* A *such that the sums* $a_1+b_1,\cdots,a_n+b_n$ *are distinct.*

(ii) (Q. H. Hou and Z. W. Sun [18]) *Let* $k\geqslant n\geqslant 1$ *be integers, and let* F *be a field with* $p(F)>\max\{n,(k-n)n\}$. *Let* $A_1,\ldots,A_n$ *be subsets of* F *with cardinality* k, *and let* $b_1,\ldots,b_n$ *be elements of* F. *Then the restricted sumset*

$$\{a_1+\cdots+a_n\colon a_i\in A_i,\ a_i\neq a_j\ \text{and}\ a_i+b_i\neq a_j+b_j\ \text{if}\ i\neq j\}$$

has more than $(k-n)n$ *elements.*

Note that part (ii) in the case $k=n$ and $A_1=\cdots=A_n$ yields part (i). In order to get part (i) by the polynomial method, Alon noted that

$$[x_1^{n-1}\cdots x_n^{n-1}]\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)(x_j+b_j-(x_i+b_i))=(-1)^{n(n-1)/2}n!.$$

Part (ii) is a consequence of Theorem 2.2 (due to Hou and Sun) with $m=1$.

Theorem 3.2 (Dasgupta, Károlyi, Serra and Szegedy [10]). *Snevily's conjecture holds for any cyclic group of odd order.*

Proof (Dasgupta, Károlyi, Serra and Szegedy). Let $m>0$ be any odd integer. As $2^{\varphi(m)}\equiv 1\pmod m$ by Euler's theorem, the `multiplicative` group of the finite field with order $2^{\varphi(m)}$ has a cyclic subgroup of order m. Thus, in view of the Combinatorial Nullstellensatz, Snevily's conjecture for the cyclic group of order m follows from the following statement: *If* F *is a field of characteristic* 2 *and* $b_1,\ldots,b_n$ *are distinct elements of* $F^*=F\setminus\{0\}$, *then*

$$c:=[x_1^{n-1}\cdots x_n^{n-1}]\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)(b_jx_j-b_ix_i)\neq 0.$$

In fact,

$$\begin{aligned}&\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)(b_jx_j-b_ix_i)\\ =&(-1)^{\binom{n}{2}}|x_j^{n-i}|_{1\leqslant i,j\leqslant n}|b_j^{i-1}x_j^{i-1}|_{1\leqslant i,j\leqslant n}\ \text{(Vandermonde)}\\ =&(-1)^{\binom{n}{2}}\sum_{\sigma\in S_n}\mathrm{sign}(\sigma)\prod_{i=1}^n x_{\sigma(i)}^{n-i}\cdot\sum_{\tau\in S_n}\mathrm{sign}(\tau)\prod_{i=1}^n b_{\tau(i)}^{i-1}x_{\tau(i)}^{i-1},\end{aligned}$$

where $\mathrm{sign}(\sigma)$ (the sign of σ) is 1 or -1 according as $\sigma\in S_n$ is even or odd. Therefore

$$\begin{aligned}(-1)^{\binom{n}{2}}c&=\sum_{\tau\in S_n}\prod_{i=1}^n b_{\tau(i)}^{i-1}\\ &=\sum_{\tau\in S_n}\mathrm{sign}(\tau)\prod_{i=1}^n b_{\tau(i)}^{i-1}\ \ \text{(because ch}(F)=2)\\ &=|b_j^{i-1}|_{1\leqslant i,j\leqslant n}=\prod_{1\leqslant i<j\leqslant n}(b_j-b_i)\neq 0.\end{aligned}$$

It is well known that all finite subgroups of the multiplicative group of a field are cyclic. On the other hand, Z. W. Sun [33] observed that any finitely generated abelian group whose finite subgroups are all cyclic, can be embedded in the unit group of a suitable cyclotomic field, which allows us to view it as a subgroup of the multiplicative group $\mathbb{C}^*$ of non-zero complex numbers. So we have the following lemma.

Lemma 3.1. *Let G be a finitely generated abelian group. Then the torsion group*

$$\mathrm{Tor}(G)=\{a\in G:\ a\text{ has a finite order}\}\tag{3.1}$$

is cyclic if and only if there is a field F such that the multiplicative group $F^*=F\setminus\{0\}$ contains a subgroup isomorphic to G.

This lemma, together with Theorem 2.4, enabled the author to establish the following theorem which extends both Theorem 3.1 and Theorem 3.2.

Theorem 3.3 (Z. W. Sun [33])**.** *Let G be an additive abelian group whose finite subgroups are all cyclic. Let m,n be positive integers and let $b_1,\ldots,b_n$ be elements of G. Assume that $A_1,\ldots,A_n$ are finite subsets of G with cardinality $k>m(n-1)$.*

(i) *If $b_1,\ldots,b_n$ are distinct, then there are at least $(k-1)n-m\binom{n}{2}+1$ multi-sets $\{a_1,\ldots,a_n\}$ such that $a_i\in A_i$ for $i=1,\ldots,n$ and all the ma_i+b_i are distinct.*

(ii) *The sets*

$$\{\{a_1,\ldots,a_n\}\colon a_i\in A_i,\ a_i\neq a_j\ \text{and}\ ma_i+b_i\neq ma_j+b_j\ \text{if}\ i\neq j\}\tag{3.2}$$

and

$$\{\{a_1,\ldots,a_n\}\colon a_i\in A_i,\ ma_i\neq ma_j\ \text{and}\ a_i+b_i\neq a_j+b_j\ \text{if}\ i\neq j\}\tag{3.3}$$

have more than $(k-1)n-(m+1)\binom{n}{2}\geqslant(m-1)\binom{n}{2}$ elements, provided that $b_1,\ldots,b_n$ are distinct and of odd order, or they have finite order and $n!$ cannot be written in the form $\sum_{p\in P}px_p$ where all the x_p are non-negative integers and P is the set of primes dividing one of the orders of $b_1,\ldots,b_n$.

In Snevily's conjecture the abelian group is required to have odd order. For a general abelian group G with cyclic torsion subgroup, what additive properties can we impose on several subsets of G with cardinality n?

Lemma 3.1 and Theorem 2.6 together yield the following result.

Theorem 3.4 (Z. W. Sun [35]). *Let G be an additive abelian group with cyclic torsion subgroup. Let $h,k,l,m,n\in\mathbb{Z}^+$ with $k>m(n-1)$ and $l>h(n-1)$. Assume that $c_1,\ldots,c_n\in G$ are distinct, and $A_1,\ldots,A_n,B_1,\ldots,B_n$ are subsets of G with $|A_1|=\cdots=|A_n|=k$ and $|B_1|=\cdots=|B_n|=l$. Then, for any sets S and T with $|S|\leqslant(k-1)n-(m+1)\binom{n}{2}$ and $|T|\leqslant(l-1)n-(h+1)\binom{n}{2}$, there are $a_1\in A_1,\ldots,a_n\in A_n,b_1\in B_1,\ldots,b_n\in B_n$ such that $\{a_1,\ldots,a_n\}\notin S$, $\{b_1,\ldots,b_n\}\notin T$, and also*

$$a_i+b_i+c_i\neq a_j+b_j+c_j,\ ma_i\neq ma_j,\ hb_i\neq hb_j\quad \text{if } 1\leqslant i<j\leqslant n. \tag{3.4}$$

Corollary 3.1 (Z. W. Sun [35]). *Let G be an additive abelian group with cyclic torsion subgroup, and let $A_1,\ldots,A_n,B_1,\ldots,B_n$ and $C=\{c_1,\ldots,c_n\}$ be finite subsets of G with the same cardinality $n>0$. Then there are distinct $a_1\in A_1,\ldots,a_n\in A_n$ and distinct $b_1\in B_1,\ldots,b_n\in B_n$ such that all the sums $a_1+b_1+c_1,\ldots,a_n+b_n+c_n$ are distinct.*

Proof. Just apply Theorem 3.4 with $k=l=n$ and $m=h=1$.

In contrast with Snevily's conjecture, Corollary 3.1 in the case $A_1=\cdots=A_n=A$ and $B_1=\cdots=B_n=B$ is of particular interest. Here we state a general additive theorem.

Theorem 3.5 (Z. W. Sun [35]). *Let G be any additive abelian group with cyclic torsion subgroup, and let $A_1,\ldots,A_m$ be subsets of G with the same cardinality $n\in\mathbb{Z}^+$. If m is odd or all the elements of A_m are of odd order, then the elements of A_i $(1\leqslant i\leqslant m)$ can be listed in a suitable order $a_{i1},\ldots,a_{in}$, so that all the sums $\sum_{i=1}^m a_{ij}$ $(1\leqslant j\leqslant n)$ are distinct.*

Sun [35] also noted that Theorem 3.5 with m odd cannot be extended to general abelian groups since there are counter-examples for the Klein quaternion group $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$.

A line of a square, an $n\times n$ matrix, is a row or column of the matrix. We define a line of an $n\times n\times n$ cube in a similar way. A *Latin cube* over a set S of cardinality n is an $n\times n\times n$ cube whose entries come from the set S and no line of which contains a repeated element. A *transversal* of an $n\times n\times n$ cube is a collection of n cells no two of which lie in the same line. A *Latin transversal* of a cube is a transversal whose cells contain no repeated element.

Corollary 3.2 (Z. W. Sun [35]). *Let N be any positive integer. For the $N\times N\times N$ Latin cube over $\mathbb{Z}/N\mathbb{Z}$ formed by the Cayley addition table, each $n\times n\times n$ sub-cube with $n\leqslant N$ contains a Latin transversal.*

Proof. Just apply Theorem 3.5 with $m=3$ (or Corollary 3.1) to the cyclic group $\mathbb{Z}/NZ$.

In contrast, Theorem 3.2 has the following equivalent version observed by Snevily [28]: *Let N be a positive odd integer. For the $N\times N$ Latin square over $\mathbb{Z}/N\mathbb{Z}$ formed by the Cayley addition table, each of its sub-squares contains a Latin transversal.*

Conjecture 3.1 (Z. W. Sun [35]). *Every $n\times n\times n$ Latin cube contains a Latin transversal.*

4. On a conjecture of Lev and related results

Let A and B be finite non-empty subsets of an additive abelian group G. In contrast with the Cauchy-Davenport theorem, J.H.B. Kemperman [21] and P. Scherk [27] proved that

$$|A+B|\geqslant|A|+|B|-\min_{c\in A+B}\nu_{A,B}(c), \tag{4.1}$$

where

$$\nu_{A,B}(c)=|\{(a,b)\in A\times B\colon a+b=c\}|; \tag{4.2}$$

in particular, we have $|A+B| \geqslant |A|+|B|-1$ if some $c \in A+B$ can be uniquely written as $a+b$ with $a \in A$ and $b \in B$.

Motivated by the Kemperman-Scherk theorem and the Erdős-Heilbronn conjecture, V. F. Lev [22] proposed the following interesting conjecture.

Lev's Conjecture. *Let G be an abelian group, and let A and B be finite non-empty subsets of G. Then we have*

$$|A \dot{+} B| \geqslant |A|+|B|-2-\min_{c\in A+B} \nu_{A,B}(c). \tag{4.3}$$

By a sophisticated application of the first part of the Combinatorial Nullstellensatz, H. Pan and Z. W. Sun [26] made the following progress on Lev's conjecture.

Theorem 4.1 (H. Pan and Z. W. Sun [26])**.** *Let A and B be finite non-empty subsets of a field F. Let $P(x,y) \in F[x,y]$ and*

$$C = \{a+b\colon a \in A,\ b \in B,\ \text{and } P(a,b) \neq 0\}. \tag{4.4}$$

If C is non-empty, then

$$|C| \geqslant |A|+|B|-\deg P-\min_{c\in C} \nu_{A,B}(c). \tag{4.5}$$

Theorem 4.2 (H. Pan and Z. W. Sun [26])**.** *Let A and B be finite non-empty subsets of an abelian group G with cyclic torsion subgroup. For $i = 1,\ldots,l$ let m_i and n_i be non-negative integers and let $d_i \in G$. Suppose that*

$$C = \{a+b\colon a \in A,\ b \in B,\ \text{and } m_i a - n_i b \neq d_i \text{ for all } i = 1,\ldots,l\} \tag{4.6}$$

is non-empty. Then

$$|C| \geqslant |A|+|B|-\sum_{i=1}^{l}(m_i+n_i)-\min_{c\in C} \nu_{A,B}(c). \tag{4.7}$$

The following result on difference-restricted sumsets follows from Theorems 4.1 and 4.2.

Theorem 4.3 (H. Pan and Z. W. Sun [26])**.** *Let G be an abelian group, and let A, B, S be finite non-empty subsets of G with*

$$C = \{a+b\colon a \in A,\ b \in B,\ \text{and } a-b \notin S\} \neq \emptyset. \tag{4.8}$$

(i) *If G is torsion-free or elementary abelian, then*

$$|C| \geqslant |A|+|B|-|S|-\min_{c\in C} \nu_{A,B}(c). \tag{4.9}$$

(ii) *If $\mathrm{Tor}(G)$ is cyclic, then*

$$|C| \geqslant |A|+|B|-2|S|-\min_{c\in C} \nu_{A,B}(c). \tag{4.10}$$

Proof. Without loss of generality we can assume that G is generated by the finite set $A \cup B$.

If $G \cong \mathbb{Z}^n$, then we can simply view G as the ring of algebraic integers in an algebraic number field K with $[K:\mathbb{Q}] = n$. If $G \cong (\mathbb{Z}/p\mathbb{Z})^n$ where p is a prime, then G is isomorphic to the additive group of the finite field with p^n elements. Thus part (i) follows from Theorem 4.1 with $P(x,y) = \prod_{s\in S}(x-y-s)$.

Let $d_1, \ldots, d_l$ be all the distinct elements of S. Applying Theorem 4.2 with $m_i = n_i = 1$ for all $i = 1, \ldots, l$, we immediately get part (ii), completing the proof.

Given two finite subsets A and B of a field F and a general $P(x, y) \in F[x, y]$, what can we say about the cardinality of the restricted sumset $\{a+b\colon a \in A,\ b \in B,\ \text{and } P(a, b) \neq 0\}$? In 2002 H. Pan and Z. W. Sun [25] made progress in this direction by relaxing (to some extent) the limitations of the polynomial method, their approach allows one to draw conclusions even if no coefficients in question are explicitly known.

Lemma 4.1 (H. Pan and Z. W. Sun [25]). *Let $P(x)$ be a polynomial over a field F. Let $\bar{F}$ be the algebraic closure of the field F and $m_P(\alpha)$ be the multiplicity of $\alpha \in \bar{F}$ as a root of $P(x) = 0$ over $\bar{F}$. Suppose that there exist non-negative integers $k < l$ such that $[x^i]P(x) = 0$ for all i with $k < i < l$. Then either $x^l \mid P(x)$, or $\deg P(x) \leqslant k$, or $N_q(P) \geqslant l - k$ for some $q \in \mathcal{P}(p) = \{1, p, p^2, \ldots\}$, where $p = \mathrm{ch}(F)$,*

$$N_q(P) = q|\{\alpha \in \bar{F} \setminus \{0\}\colon m_P(\alpha) \geqslant q\}| - \sum_{\alpha \in \bar{F}\setminus\{0\}} \{m_P(\alpha)\}_q \tag{4.11}$$

and $\{m\}_q$ denotes the least non-negative residue of $m \in \mathbb{Z}$ modulo q.

We remark that $N_1(P)$ is the number of distinct roots in $\bar{F}\setminus\{0\}$ of the equation $P(x) = 0$ over $\bar{F}$.

Theorem 4.4 (H. Pan and Z. W. Sun [25]). *Let A and B be two finite non-empty subsets of a field F. Furthermore, let $P(x, y)$ be a polynomial over F of degree $d = \deg P(x, y)$ such that for some $i < |A|$ and $j < |B|$ we have $[x^i y^{d-i}]P(x, y) \neq 0$ and $[x^{d-j}y^j]P(x, y) \neq 0$. Define $P_0(x, y)$ to be the homogeneous polynomial of degree d such that $P(x, y) = P_0(x, y) + R(x, y)$ for some $R(x, y) \in F[x, y]$ with $\deg R(x, y) < d$, and put $P^*(x) = P_0(x, 1)$. For any α in the algebraic closure $\bar{F}$ of F, let $m_{P^*}(\alpha)$ denote the multiplicity of α as a zero of $P^*(x)$. Then*

$$\begin{aligned} &|\{a + b\colon a \in A,\ b \in B,\ \text{and } P(a, b) \neq 0\}| \\ &\geqslant \min\{p - m_{P^*}(-1),\ |A| + |B| - 1 - d - N(P^*)\}, \end{aligned} \tag{4.12}$$

where $p = \mathrm{ch}(F)$ and

$$N(P^*) = \max_{q \in \mathcal{P}(p)} q|\{\alpha \in \bar{F} \setminus \{0, -1\} : m_{P^*}(\alpha) \geqslant q\}|. \tag{4.13}$$

For the sake of clarity, here we state a consequence of Theorem 4.4.

Corollary 4.1 (H. Pan and Z. W. Sun [25]). *Let F be a field with $p = \mathrm{ch}(F) \neq 2$, and let A, B and S be finite non-empty subsets of F. Then*

$$|\{a + b\colon a \in A,\ b \in B,\ \text{and } a - b \notin S\}| \geq \min\{p,\ |A| + |B| - |S| - q - 1\}, \tag{4.14}$$

where q is the largest element of $\mathcal{P}(p)$ not exceeding $|S|$.

5. Working with general abelian groups

Theorem 5.1 (Kneser's Theorem). *Let G be an additive abelian group. Let A and B be finite non-empty subsets of G, and let $H = H(A+B)$ be the stabilizer $\{g \in G : g+A+B = A+B\}$. If $|A + B| \leqslant |A| + |B| - 1$, then*

$$|A + B| = |A + H| + |B + H| - |H|. \tag{5.1}$$

This is an extension of the Cauchy-Davenport theorem. For, if G is $\mathbb{Z}/p\mathbb{Z}$ with p a prime, and also $|A+B| < |A|+|B|-1$, then $H \neq \{0\}$ by Kneser's theorem, whence $H = G$ and $|A+B| \geqslant |G|+|G|-|G| = p$.

Corollary 5.1. *Let G be an additive abelian group. Let $p(G) = +\infty$ if G is torsion-free, otherwise we let $p(G)$ be the least order of a non-zero element of G. Then, for any finite non-empty subsets A and B of G, we have*

$$|A+B| \geqslant \min\{p(G),\, |A|+|B|-1\}. \tag{5.2}$$

Proof. Suppose that $|A+B| < |A|+|B|-1$. Then $H = H(A+B) \neq \{0\}$ by Kneser's theorem. Therefore $|H| \geqslant p(G)$ and hence

$$|A+B| = |A+H|+|B+H|-|H| \geqslant |A+H| \geqslant |H| \geqslant p(G).$$

We are done.

G. Károlyi ([19], [20]) extended the Erdős-Heilbronn conjecture to general abelian groups.

Theorem 5.2. *Let G be an additive abelian group and let A be a finite non-empty subset of G.*

(i) (G. Károlyi [19]) *We have*

$$|2^{\wedge}A| \geqslant \min\{p(G),\, 2|A|-3\}. \tag{5.3}$$

(ii) (G. Károlyi [20]) *When $|A| \geqslant 5$ and $p(G) > 2|A|-3$, the equality $|2^{\wedge}A| = 2|A|-3$ holds if and only if A is an arithmetic progression.*

Using the fact that any finitely generated abelian group can be written as the direct sum of some cyclic groups of infinite or prime power order, Károlyi proved Theorem 5.2 in two steps. First, he showed that Theorem 5.2 is true for any cyclic group G of infinite or prime power order; then, he proved that those abelian groups possessing the required property are closed under direct sum. In the first step for Theorem 5.2(i), he actually obtained the following more general result.

Theorem 5.3 (G. Károlyi [19])**.** *Let $\emptyset \neq A, B \subseteq \mathbb{Z}/q\mathbb{Z}$, where $q = p^{\alpha}$ is a power of a prime p. Then*

$$|A \dot{+} B| \geqslant \min\{p,\, |A|+|B|-3\}. \tag{5.4}$$

For non-empty subsets A and B of $\mathbb{Z}/p\mathbb{Z}$ with p a prime, if $|A| \neq |B|$ then we have

$$|A \dot{+} B| \geqslant \min\left\{p,\, |A|+|B|-\frac{2(2+1)}{2}+1\right\} = \min\{p,\, |A|+|B|-2\}$$

by the ANR theorem; if $|A| = |B|$ then

$$|A \dot{+} B| \geqslant |(A\setminus\{a_0\}) \dot{+} B)| \geqslant \min\{p,\, (|A|-1)+|B|-2\},$$

where a_0 is any fixed element of A.

When $q = p^{\alpha}$ is not a prime, $\mathbb{Z}/q\mathbb{Z}$ is not a subgroup of the additive group of a field but Károlyi considered it as the group of qth roots of unity (up to isomorphism) which can be viewed as a subgroup of the multiplicative group $\mathbb{C}^*$ of non-zero complex numbers.

Lemma 5.1 (Z. W. Sun [29][32])**.** *Let $\lambda_1, \ldots, \lambda_k$ be qth roots of unity, and let $c_1, \ldots, c_k$ be non-negative integers with $c_1\lambda_1 + \cdots + c_k\lambda_k = 0$. Then $c_1 + \cdots + c_k \in D(q)$, where $D(q)$ is as in Theorem* 2.4(iii)*.*

Proof of Theorem 5.3. Since $\mathbb{Z}/q\mathbb{Z}$ is isomorphic to the multiplicative group C_q of qth roots of unity, we may view A and B as subsets of C_q. If $|A|+|B|-3>p$, then we can choose $\emptyset\neq A'\subseteq A$ and $\emptyset\neq B'\subseteq B$ so that $|A'|+|B'|-3=p$. Thus, without loss of generality, we may assume that $k+l-3\leqslant p$ where $k=|A|$ and $l=|B|$.

Suppose that $|C|\ngeqslant \min\{p,\,k+l-3\}=k+l-3$, where

$$C=\{ab:\ a\in A,\ b\in B \text{ and } a\neq b\}.$$

If

$$c_0:=[x^{k-1}y^{l-1}](xy-1)\prod_{c\in C}(x-cy)\times(x-y)^{k+l-4-|C|}\neq 0,$$

then by the polynomial method, there exist $a\in A$ and $b^{-1}\in B^{-1}$ such that $ab^{-1}\neq 1$ and $a\neq cb^{-1}$ for all $c\in C$, which leads to a contradiction since $a\neq b$ and $ab\in C$. Thus, it suffices to show $c_0\neq 0$.

Observe that

$$c_0=[x^{k-2}y^{l-2}]\prod_{s=1}^{k+l-4}(x-\rho_s y)=(-1)^{l-2}\sum_{1\leqslant i_1<\cdots<i_{l-2}\leqslant k+l-4}\rho_{i_1}\cdots\rho_{i_{l-2}},$$

where $\rho_1,\ldots,\rho_{k+l-4}$ are suitable qth roots of unity. Since $\binom{k+l-4}{l-2}\notin D(q)=\{pn:\ n\in\mathbb{N}\}$, we have $c_0\neq 0$ by Lemma 5.1.

Now we mention a celebrated theorem of M. Hall which was conjectured by G. Cramer for cyclic groups.

Theorem 5.4 (M. Hall [16])**.** *Let $G=\{b_1,\ldots,b_n\}$ be an additive abelian group of order n, and let $a_1,\ldots,a_n$ be (not necessarily distinct) elements of G. Then $a_1+\cdots+a_n=0$ if and only if $\{a_i+b_{\sigma(i)}:\ i=1,\ldots,n\}=G$ for some $\sigma\in S_n$.*

Z. W. Sun and Y. N. Yeh [37] observed that Hall's theorem implies the following conjecture of Parker (cf. [14]): For integers $a_1,\ldots,a_n$ with $a_1+\cdots+a_n\equiv 0\pmod{n+1}$, there are $\sigma,\tau\in S_n$ such that $a_i\equiv\sigma(i)+\tau(i)\pmod{n+1}$ for all $i=1,\ldots,n$.

In contrast with Snevily's conjecture, we have the following consequence of Theorem 5.4.

Corollary 5.2. *Let G be a finite abelian group, and let $a_1,\ldots,a_n\in G$ with $n<|G|$. Then there are distinct $b_1,\ldots,b_n\in G$ such that the sums $a_1+b_1,\ldots,a_n+b_n$ are distinct.*

Proof. Write $G=\{c_1,\ldots,c_m\}$ with $m=|G|$. Set $a_{n+1}=-(a_1+\cdots+a_n)$ and $a_k=0$ for $n+1<k\leqslant m$. As $a_1+\cdots+a_m=0$, by Theorem 5.4, for some $\sigma\in S_m$ we have $\{a_i+c_{\sigma(i)}:\ i=1,\ldots,m\}=G$. Let $b_i=c_{\sigma(i)}$ for $i=1,\ldots,n$. Then $b_1,\ldots,b_n$ are distinct, and so are the sums $a_1+b_1,\ldots,a_n+b_n$. We are done.

Let us conclude this paper with a new open problem.

Problem 5.1. *Let G be a finite abelian group, and let n be a positive integer smaller than $|G|$. Determine the smallest positive integer $m\leqslant|G|$ such that whenever $a_1,\ldots,a_n\in G$ are distinct and $B\subseteq G$ with $|B|\geqslant m$ there are distinct $b_1,\ldots,b_n\in B$ such that all the sums $a_1+b_1,\ldots,a_n+b_n$ are distinct.*

6. On value sets of polynomials

Given a field F, we consider polynomials of the form

What can we say about the solvability of the equation $f(x_1,\ldots,x_n)=0$ over F^n?

Let p be a prime, and let $c_1,\ldots,c_n$ be non-zero elements of the field $F_p=\mathbb{Z}/p\mathbb{Z}$. In 1959 Chowla, Mann and Straus (cf. Theorem 2.8 of [24]) used Vosper's theorem (cf. pp. 52-57 of [24]) to deduce that if $p>3$, $1<k<(p-1)/2$ and $k\mid p-1$, then

$$|\{c_1x_1^k+\cdots+c_nx_n^k:\ x_1,\ldots,x_n\in F_p\}|\geqslant \min\left\{p,\,(2n-1)\frac{p-1}{k}+1\right\}.$$

In 1956 Carlitz [8] proved that whenever $n\geqslant k\geqslant 1$, $k\mid p-1$ and $g(x_1,\ldots,x_n)\in F_p[x_1,\ldots,x_n]$ with $\deg g<k$, the equation

$$c_1x_1^k+\cdots+c_nx_n^k+g(x_1,\ldots,x_n)=0$$

has a solution with $x_1,\ldots,x_n\in F_p$. In 2006 Felszeghy [15] extended this result by showing that

$$\{c_1x_1^k+\cdots+c_nx_n^k+g(x_1,\ldots,x_n):\ x_1,\ldots,x_n\in F_p\}=F_p$$

if $k\in\{1,\ldots,p-1\}$ and $n\geqslant (p-1)/\lfloor (p-1)/k\rfloor$.

With the help of the Combinatorial Nullstellensatz, recently Z. W. Sun established the following result on value sets of polynomials.

Theorem 6.1 (Z. W. Sun [36]). *Let F be a field, and let*

$$f(x_1,\ldots,x_n)=c_1x_1^k+\cdots+c_nx_n^k+g(x_1,\ldots,x_n)\in F(x_1,\ldots,x_n),\tag{6.1}$$

where

$$c_1,\ldots,c_n\in F^*=F\setminus\{0\}\quad\text{and}\quad \deg g<k\in\mathbb{Z}^+.\tag{6.2}$$

Then, for any non-empty finite subsets $A_1,\ldots,A_n$ of F, we have

$$\begin{aligned}&|\{f(a_1,\ldots,a_n):\ a_1\in A_1,\ldots,a_n\in A_n\}|\\&\geqslant \min\left\{p(F),\,\sum_{i=1}^n\left\lfloor\frac{|A_i|-1}{k}\right\rfloor+1\right\}.\end{aligned}\tag{6.3}$$

Note that Theorem 6.1 in the case $f(x_1,\ldots,x_n)=x_1+\cdots+x_n$ yields the Cauchy-Davenport theorem. Felszeghy's result is also a special case of Theorem 6.1.

Here is another result of [36] obtained by the Combinatorial Nullstellensatz.

Theorem 6.2 (Z. W. Sun [36]). *Let $f(x_1,\ldots,x_n)$ be a polynomial over a field F given by* (6.1) *and* (6.2) *with $n\leqslant k=\deg f$. And 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*

$$V=\{f(a_1,\ldots,a_n):\ a_1\in A_1,\ldots,a_n\in A_n,\ \text{and } a_i\neq a_j\ \text{if } i\neq j\},\tag{6.4}$$

we have

$$|V|\geqslant \min\left\{p(F),\,\sum_{i=1}^n\left\lfloor\frac{|A_i|-i}{k}\right\rfloor+1\right\}.\tag{6.5}$$

Theorem 6.2 has the following consequence for the case $n\geqslant k$.

Corollary 6.1 (Z. W. Sun [36]). *Let A be a finite subset of a field F, and let $f(x_1,\ldots,x_n)$ be a polynomial given by* (6.1) *and* (6.2). *If $n\geqslant k$, then we have*

$$\begin{aligned}&|\{f(a_1,\ldots,a_n):\ a_1,\ldots,a_n\in A,\ \text{and } a_i\neq a_j\ \text{if } i\neq j\}|\\&\geqslant \min\{p(F),\,|A|-n+1\}.\end{aligned}\tag{6.6}$$

Let us conclude this paper with a conjecture raised in [36].

Conjecture 6.1 (Z. W. Sun [36]). *Let $f(x_1,\ldots,x_n)$ be a polynomial over a field F given by* (6.1) *and* (6.2)*, and let A be any finite subset of F. Provided $n>k$, we have*

$$\begin{aligned}&|\{f(a_1,\ldots,a_n): a_1,\ldots,a_n\in A,\ \text{and } a_i\ne a_j \text{ if } i\ne j\}|\\ &\geqslant \min\left\{p(F)-\delta,\ \frac{n(|A|-n)}{k}-k\left\{\frac{n}{k}\right\}\left\{\frac{|A|-n}{k}\right\}+1\right\},\end{aligned}\tag{6.7}$$

where $\{\alpha\}$ denotes the fractional part $\alpha-\lfloor\alpha\rfloor$ of a real number α, and

$$\delta=\begin{cases}1 & \text{if } n=2 \text{ and } c_1=-c_2,\\ 0 & \text{otherwise.}\end{cases}$$

By Corollary 3 of [25], this conjecture holds when $n=2$. Note also that the Dias da Silva–Hamidoune theorem is a special case of Conjecture 6.1 with $k=1$.

References

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

[2] N. Alon, *Additive Latin transversals*, Israel J. Math. **117**(2000), 125–130.

[3] N. Alon, *Discrete mathematics: methods and challenges*, in: Proceedings of the International Congress of Mathematicians, Vol. I (Beijing, 2002), Higher Ed. Press, Beijing, 2002, pp. 119–135.

[4] N. Alon, M. B. Nathanson and I. Z. Ruzsa , *Adding distinct congruence classes modulo a prime*, Amer. Math. Monthly **102**(1995), 250–255.

[5] 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.

[6] N. Alon and M. Tarsi, *A nowhere-zero point in linear mappings*, Combinatorica **9**(1989), 393–395.

[7] H. Q. Cao and Z. W. Sun, *On sums of distinct representatives*, Acta Arith. **87**(1998), 159–169.

[8] L. Carlitz, *Solvablity of certain equations in a finite field*, Quart. J. Math. **7**(1956), 3–4.

[9] A. Cauchy, *Recherches sur les nombres*, Jour. Ecole Polytechn. **9**(1813), 99–116.

[10] S. Dasgupta, G. Károlyi, O. Serra and B. Szegedy, *Transversals of additive Latin squares*, Israel J. Math. **126**(2001), 17–28.

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

[12] 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.

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

[14] R. K. Guy, *Parker's permutation problem involves the Catalan numbers*, Amer. Math. Monthly **100**(1993), 287–289.

[15] B. Felzeghy, *On the solvability of some special equations over finite fields*, Publ. Math. Debrecen **68**(2006), 15–23.

[16] M. Hall, *A combinatorial problem on abelian groups*, Proc. Amer. Math. Soc. **3**(1952), 584–587.

[17] P. Hall, *On representatives of subsets*, J. London Math. Soc. **10**(1935), 26–30.

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

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

[20] G. Károlyi, *An inverse theorem for the restricted set addition in abelian groups*, J. Algebra **290**(2005), 557–593.

[21] J. H. B. Kemperman, *On small sumsets in an abelian group*, Acta Math. **103**(1960), 63–88.

[22] V. F. Lev, *Restricted set addition in Abelian groups: results and conjectures*, J. Théor. Nombres Bordeaux **17**(2005), 181–193.

[23] J. X. Liu and Z. W. Sun, *Sums of subsets with polynomial restrictions*, J. Number Theory **97**(2002), 301–304.

[24] M. B. Nathanson, Additive Number Theory: Inverse Problems and the Geometry of Sumsets (Graduated texts in mathematics; 165), Springer, New York, 1996.

[25] 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.

[26] H. Pan and Z. W. Sun, *Restricted sumsets and a conjecture of Lev*, Israel J. Math. **154**(2006), 21–28.

[27] P. Scherk, *Distinct elements in a set of sums*, Amer. Math. Monthly **62**(1955), 46–47.

[28] H. S. Snevily, *The Cayley addition table of* $\mathbb{Z}_n$, Amer. Math. Monthly **106**(1999), 584–585.

[29] Z. W. Sun, *Covering the integers by arithmetic sequences II*, Trans. Amer. Math. Soc. **348**(1996), 4279–4320.

[30] Z. W. Sun, *Restricted sums of subsets of* $\mathbb{Z}$, Acta Arith. **99**(2001), 41–60.

[31] Z. W. Sun, *Hall's theorem revisited*, Proc. Amer. Math. Soc. **129**(2001), 3129–3131.

[32] Z. W. Sun, *On the function* $w(x)=|\{1\leqslant s\leqslant k:\ x\equiv a_s\pmod{n_s}\}|$, Combinatorica **23**(2003), 681–691.

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

[34] Z. W. Sun, *Unification of zero-sum problems, subset sums and covers of* $\mathbb{Z}$, Electron. Res. Announc. Amer. Math. Soc. **9**(2003), 51–60.

[35] Z. W. Sun, *An additive theorem and restricted sumsets*, preprint, 2006. On-line version: `http://arxiv.org/abs/math.CO/0610981`.

[36] Z. W. Sun, *On value sets of polynomials over a field*, preprint, 2007. On-line version: `http://arxiv.org/abs/math.NT/0703180`.

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

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