A talk given at Genova Univ. (2004-06-23) and Univ. California at Irvine (2005-11-10).

ON SOME CONJECTURES OF ERDÖS-HEILBRONN, LEV AND SNEVILY

Zhi-Wei Sun

Department of Mathematics
Nanjing University
Nanjing 210093, P. R. China
zwsun@nju.edu.cn
http://pweb.nju.edu.cn/zwsun

Abstract. In 1964 P. Erdös and H. Heilbronn conjectured that if $\emptyset \neq A \subseteq \mathbb{Z}/p\mathbb{Z}$ (where p is a prime) then there are at least $\min\{p, 2|A|-3\}$ residue classes in $\mathbb{Z}/p\mathbb{Z}$ that can be written as the sum of two distinct elements of A. This was confirmed thirty years later and soon a powerful tool called "the polynomial method" arose. In this talk we will introduce the method and its various applications including Károlyi's recent extension of the Erdös-Heilbronn conjecture to any abelian group.

Motivated by the Erdős-Heilbronn conjecture and the Kemperman-Scherk theorem, V. F. Lev proposed in 2003 the following conjecture: If A and B are finite nonempty subsets of an abelian group G, then

$$|\{a+b:\ a\in A,\ b\in B \text{ and } a\neq b\}| \geqslant |A|+|B|-2-\min_{c\in A+B}\nu_{A,B}(c),$$

where $\nu_{A,B}(c)=|\{(a,b)\in A\times B:\ a+b=c\}|$. We will talk about the recent progress on Lev's conjecture made by H. Pan and the speaker.

A conjecture of Snevily posed in 1999 states that if A and B are k-subsets of an additive abelian group of odd order then there is a numbering $\{a_i\}_{i=1}^k$ of the elements of A and a numbering $\{b_i\}_{i=1}^k$ of the elements of B such that all the k corresponding sums a_i+b_i are distinct. This has been proved for cyclic groups of odd order by a dramatic application of the polynomial method. In this talk we will also introduce this result together with the speaker's extension.

1. The Erdős-Heilbronn conjecture and the birth of 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

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

So 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 $2A=A+A$.

The following theorem is well known and quite useful in additive number theory.

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

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

In 1964 Erdős and Heilbronn [Acta Arith.] made the following conjecture.

The Erdős-Heilbronn Conjecture. *Let p be a prime, and let A be a nonempty subset of the field $\mathbb{Z}_p$. 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 [Bull. London. Math. Soc. 1994] thirty years later, with the help of the representation theory of groups.

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

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

The da Silva–Hamidoune Theorem [Bull. London Math. Soc. 1994]**.** *Let F be a field and n be a positive integer. Then for any finite subset A of F we have*

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

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

If p is a prime, $A \subseteq \mathbb{Z}_p$ and $|A| > \sqrt{4p-7}$, then by the da Silva–Hamidoune theorem, any element of $\mathbb{Z}_p$ can be written as a sum of $\lfloor |A|/2 \rfloor$ distinct elements of A.

In 1995–1996 Alon, Nathanson and Ruzsa [Amer. Math. Monthly 1995, J. Number Theory 1996] developed a polynomial method rooted in [Alon and Tarsi, Combinatorica 1989] 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 so-called polynomial method.

Lemma 1.1. *Let F be a field and $A_1, \cdots, A_n$ its subsets which are finite and nonempty. Let $f(x_1, \cdots, x_n) \in F[x_1, \cdots, x_n]$ have degree less than*

$k_i = |A_i|$ in x_i for each $i = 1, \cdots, n$. If $f(a_1, \cdots, a_n) = 0$ for all $a_1 \in A_1, \cdots, a_n \in A_n$, then $f(x_1, \cdots, x_n)$ is identically zero.

Proof. It is well-known that a nonzero polynomial $P(x) \in F[x]$ of degree less than a positive integer k can't have k distinct roots in F, so the lemma is true in the case $n = 1$.

Now let $n > 1$ and assume that the lemma holds for small values of n. Write

$$f(x_1, \cdots, x_{n-1}, x_n) = \sum_{i=0}^{k_n - 1} g_i(x_1, \cdots, x_{n-1}) x_n^i,$$

where $g_i(x_1, \cdots, x_{n-1}) \in F[x_1, \cdots, x_{n-1}]$ has degree at most $k_j - 1$ in x_j for $j = 1, \cdots, n-1$.

Fix $a_1 \in A_1, \cdots, a_{n-1} \in A_{n-1}$. As

$$P(x_n) = f(a_1, \cdots, a_{n-1}, x_n) = \sum_{i=0}^{k_n - 1} g_i(a_1, \cdots, a_{n-1}) x_n^i$$

has degree less than $k_n = |A_n|$ in x_n and $P(a) = 0$ for all $a \in A_n$, $P(x_n)$ is identically zero and hence $g_i(a_1, \cdots, a_{n-1}) = 0$ for every $i = 0, \cdots, k_n - 1$.

By the induction hypothesis, all the $g_i(x_1, \cdots, x_{n-1})$ are identically zero and therefore so is $f(x_1, \cdots, x_n)$.

By the above we have proved the lemma by induction. □

Combinatorial Nullstellensatz [Alon, Comb. Probab. Comput. 1999]**.** *Let $A_1, \cdots, A_n$ be finite subsets of a field F, and let $f(x_1, \cdots, x_n) \in F[x_1, \cdots, x_n]$.*

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

$$f(a_1, \cdots, a_n) = 0 \ \text{ for all } a_1 \in A_1, \cdots, a_n \in A_n \tag{1.1}$$

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

$$f(x_1,\cdots,x_n)=\sum_{i=1}^{n} g_i(x_i)h_i(x_1,\cdots,x_n). \tag{1.2}$$

(ii) *Suppose that* $\deg f=k_1+\cdots+k_n$ *where* $0\leqslant k_i<|A_i|$ *for* $i=1,\ldots,n$. *If* (1.1) *holds, then*

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

Proof. (i) If there are $h_1(x_1,\cdots,x_n),\cdots,h_n(x_1,\cdots,x_n)\in F[x_1,\cdots,x_n]$ such that (1.2) holds, then for any $a_1\in A_1,\cdots,a_n\in A_n$ we have

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

Now we consider the converse. Write

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

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

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

where

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

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

$$\bar{f}(a_1,\cdots,a_n)=f(a_1,\cdots,a_n)=0.$$

As the degree of $\bar{f}(x_1,\cdots,x_n)$ with respect to x_i is less than $|A_i|$, by Lemma 1.1 the polynomial $\bar{f}(x_1,\cdots,x_n)$ is identically zero. Therefore (1.2) holds.

(ii) By part (i) we can write

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

where $h_i(x_1,\cdots,x_n)\in F[x_1,\cdots,x_n]$ and $\deg h_i\le\deg f-\deg g_i$. Thus

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

We are done. □.

The Alon-Nathanson-Ruzsa Lemma [Amer. Math. Monthly 1995; J. Number Theory 1996]. *Let $A_1,\cdots,A_n$ be finite subsets of a field F with $k_i=|A_i|>0$ for $i=1,\cdots,n$. Let $f(x_1,\cdots,x_n)\in F[x_1,\cdots,x_n]\setminus\{0\}$ and $\deg f\leqslant\sum_{i=1}^n(k_i-1)$. If*

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

then

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

Proof. Let $C = \{a_1 + \cdots + a_n : a_i \in A_i,\ f(a_1, \cdots, a_n) \neq 0\}$. Assume that $|C| \leq K = \sum_{i=1}^{n}(k_i - 1) - \deg f$. Then the polynomial

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

is of degree $\sum_{i=1}^{n}(k_i - 1)$ and its coefficient of $x_1^{k_1-1} \cdots x_n^{k_n-1}$ is nonzero. Applying the second part of Combinatorial Nullstellensatz we find that $P(a_1, \cdots, a_n) \neq 0$ 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 $f(a_1, \ldots, a_n) \neq 0$. $\square$

Remark. A variant of this result appeared in [Q. H. Hou and Z. W. Sun, Acta Arith. 102(2002)].

The Alon-Nathanson-Ruzsa Theoreom [J. Number Theory 1996]**.** *Let $A_1, \cdots, A_n$ be finite nonempty subsets of a field F with $|A_1| < \cdots < |A_n|$. Then, for the set*

$$A_1 \dot{+} \cdots \dot{+} A_n = \left\{ \sum_{i=1}^{n} a_i : a_i \in A_i,\ \textit{and } a_i \neq a_j \textit{ if } i \neq j \right\},$$

we have

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

This follows from the ANR lemma and the following fact. If $k_1, \cdots, k_n$ are positive integers, then

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

The 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,

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

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

2. More additive results obtained by the polynomial method

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

(i) [Q. H. Hou and Z. W. Sun, Acta Arith. 102(2002)] *We have*

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

(ii) [Z. W. Sun and Y. N. Yeh, J. Number Theory 114(2005)] *If $m > 0$ then*

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

Theorem 2.1. *Let k, m be nonnegative integers and n a positive integer. Let F be a field with $p(F)/n$ greater than m and $k+m-mn-1$. Let $A_1, \cdots, A_n$ be finite subsets of F with $|A_n| = k$. Set*

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

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

(i) [Q. H. Hou and Z. W. Sun, Acta Arith. 102(2002)] *If* $|A_1| = \cdots = |A_{n-1}| = k$, *and* $|S_{ij}| \leqslant 2m$ *for all* $1 \leqslant i < j \leqslant n$, *then we have* $|C| \geqslant (k + m - mn - 1)n + 1$.

(ii) [Z. W. Sun and Y. N. Yeh, J. Number Theory 114(2005)] *If* $|A_i| = k - n + i$ *for* $i = 1, \ldots, n-1$, *and* $|S_{ij}| < 2m$ *for all* $1 \leqslant i < j \leqslant n$, *then* $|C| \geqslant (k + m - mn - 1)n + 1$.

Lemma 2.2 [J. X. Liu and Z. W. Sun, J. Number Theory 97(2002)]**.** *Let* k, m, n *be positive integers with* $k - 1 \geqslant m(n-1)$. *Then*

$$[x_1^{k-n} \cdots x_n^{k-1}] \prod_{1 \leq i < j \leq n} (x_j^m - x_i^m)(x_1 + \cdots + x_n)^{(k-1)n-(m+1)\binom{n}{2}}$$
$$= (-m)^{\binom{n}{2}} \frac{((k-1)n - (m+1)\binom{n}{2})!1!2! \cdots (n-1)!}{(k-1)!(k-1-m)! \cdots (k-1-(n-1)m)!}.$$

Theorem 2.2 [J. X. Liu and Z. W. Sun, J. Number Theory 97(2002)]**.** *Let* k, m, n *be positive integers with* $k > m(n-1)$, *and let* F *be a field with* $p(F) > K = (k-1)n - (m+1)\binom{n}{2}$. *Let* $A_1, \cdots, A_n$ *be subsets of* F *for which*

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

Let $P_1(x), \ldots, P_n(x) \in F[x]$ *be monic and of degree* m. *Then we have*

$$|\{a_1 + \cdots + a_n : a_i \in A_i, \text{ and } P_i(a_i) \neq P_j(a_j) \text{ if } i \neq j\}| \geqslant K + 1.$$

Lemma 2.3 [Z. W. Sun, J. Combin. Theory Ser. A 103(2003)]**.** *Let R be a commutative ring with identity, and let $A=(a_{ij})_{1\leqslant i,j\leqslant n}$ be a matrix with all the a_{ij} in R. Let $k,m_1,\cdots,m_n$ be nonnegative integers.*

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

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

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

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

where $\mathrm{per}(A)$ is the permanent $\sum_{\sigma\in S_n}a_{1\sigma(1)}\cdots a_{n\sigma(n)}$.

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

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

Theorem 2.3 [Z. W. Sun, J. Combin. Theory Ser. A 103(2003)]**.** *Let k,m,n be positive integers with $k>m(n-1)$, and let $A_1,\cdots,A_n$ be subsets of a field F with cardinality k. Let $K=(k-1)n-m\binom{n}{2}$ and $P_1(x),\cdots,P_n(x)\in F[x]$ have degree m.*

(i) *If $p(F)>K$ and all the $b_i=[x^m]P_i(x)$ $(i=1,\cdots,n)$ are pairwise distinct, then $|S|\geqslant K+1$ where*

$$S=\left\{\sum_{i=1}^n a_i\colon a_1\in A_1,\cdots,a_n\in A_n,\ \text{and } P_i(a_i)\neq P_j(a_j)\ \text{if } i\neq j\right\}.$$

(ii) *If* $p(F) > K - \binom{n}{2}$ *and the permanent of* $B = (b_j^{i-1})_{1\leqslant i,j\leqslant n}$ *does not vanish, then* $|T| \geqslant K - \binom{n}{2} + 1$ *where*

$$T = \left\{ \sum_{i=1}^{n} a_i \colon a_i \in A_i,\ a_i \neq a_j \text{ and } P_i(a_i) \neq P_j(a_j) \text{ if } i \neq j \right\}.$$

(iii) *We have* $\mathrm{per}(B) \neq 0$, *if* F *is the complex field* $\mathbb{C}$, $b_1, \cdots, b_n$ *are* q*th roots of unity, and* $n!$ *does not belong to the set*

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

What can we say about the cardinality of the restricted sumset

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

where $P(x, y)$ is a general polynomial over a field F? H. Pan and Z. W. Sun [J. Combin. Theory Ser. A 100(2002)] 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 known explicitly.

Theorem 2.4 [H. Pan and Z. W. Sun, J. Combin. Theory Ser. A 100(2002)]**.** *Let* F *be a field of characteristic* p, *and let* A *and* B *be two finite nonempty subsets of* F. *Furthermore, let* $P(x, y)$ *be a polynomial over* F *of degree* $d = \deg P(x, y)$ *such that for some* $i \in [0, |A| - 1]$ *and* $j \in [0, |B| - 1]$ *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 E of F, let $m_{P^*}(\alpha)$ denote the multiplicity of α as a zero of $P^*(x)$. Then

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

where

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

and

$$\mathcal{P}(p)=\begin{cases}\{1,p,p^2,\cdots\} & \text{if } p\neq 0,\\ \{1\} & \text{if } p=0.\end{cases}$$

For the sake of clarity here we state a consequence of Theorem 2.4.

Corollary [H. Pan and Z. W. Sun, J. Combin. Theory Ser. A 2002]**.** *Let F be a field of characteristic $p\neq 2$, and let A,B and S be finite nonempty subsets of F. Then*

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

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

3. Working on abelian groups: Snevily's conjecture and an extension of the Erdős-Heilbronn conjecture

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

In 1999 Snevily [Amer. Math. Monthly] made the following 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 $a_1 + b_1, \cdots, a_n + b_n$ are pairwise distinct.*

Theorem 3.1. (i)[N. Alon, Israel J. Math. 117(2000)] *Let p be an odd prime and A be a subset of $\mathbb{Z}_p$ with cardinality $n < p$. For any given $b_1, \ldots, b_n \in \mathbb{Z}_p$ 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, Acta Arith. 102(2002)] *Let $k \geqslant n \geqslant 1$ be integers, and F be a field with $p(F)$ greater than n and $(k-n)n$. Let $A_1, \cdots, A_n$ be subsets of F with cardinality k, and $b_1, \cdots, b_n$ be elements of F. Then the sumset*

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

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 2.1 (due to Hou and Sun) in the case $m = 1$.

Theorem 3.2 [Dasgupta, Károlyi, Serra and Szegedy, Israel J. Math. 2001]**.** *Snevily's conjecture holds for any cyclic group with odd order.*

Proof (Dasgupta, Károlyi, Serra and Szegedy). Let $m > 0$ be an odd integer. As $2^{\varphi(m)} \equiv 1 \pmod m$, the **multiplicative** group of the finite field with order $2^{\varphi(m)}$ has a cyclic subgroup of order m. Thus Snevily's conjecture for the cyclic group of order m can be reduced to the following statement in view of the Combinatorial Nullstellensatz.

If F is a field of characteristic 2 and $b_1, \cdots, b_n$ are distinct elements of $F^* = F \setminus \{0\}$, then

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

In fact,

$$\prod_{1 \leqslant i < j \leqslant n} (x_j - x_i)(b_j x_j - b_i x_i) = (-1)^{\binom{n}{2}} |x_j^{n-i}|_{1 \leqslant i,j \leqslant n} |b_j^{i-1} x_j^{i-1}|_{1 \leqslant i,j \leqslant n}$$

$$= (-1)^{\binom{n}{2}} \sum_{\sigma \in S_n} \mathrm{sign}(\sigma) \prod_{i=1}^n x_{\sigma(i)}^{n-i} \sum_{\tau \in S_n} \mathrm{sign}(\tau) \prod_{i=1}^n b_{\tau(i)}^{i-1} x_{\tau(i)}^{i-1}.$$

Therefore

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

This concludes the proof. □

Z. W. Sun [J. Combin. Theory Ser. A 103(2003)] 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 and hence it can be viewed as a subgroup of the multiplicative group $\mathbb{C}^*$ of nonzero complex numbers. This observation together with Theorem 2.3 enabled Sun to establish the following theorem which extends both Theorem 3.1 and Theorem 3.2.

Theorem 3.3 [Z. W. Sun, J. Combin. Theory Ser. A 103(2003)]**.** *Let G be an additive abelian group whose finite subgroups are all cyclic. Let $A_1, \cdots, A_n$ be finite subsets of G with cardinality $k > m(n-1)$ (where m is a positive integer), and let $b_1, \cdots, b_n$ be elements of G.*

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

(ii) *The sets*

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

and

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

have more than $(k-1)n - (m+1)\binom{n}{2} \geqslant (m-1)\binom{n}{2}$ elements, provided that $b_1, \cdots, b_n$ 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 nonnegative integers and P is the set of primes dividing one of the orders of $b_1, \cdots, b_n$.

Theorem 3.4 (Kneser's Theorem)**.** *Let G be an additive abelian group. Let A and B be finite nonempty subsets of G, and let $H = H(A+B)$ be*

the stablizer $\{g \in G : g + A + B = A + B\}$. *If* $|A + B| \leqslant |A| + |B| - 1$, *then*

$$|A + B| = |A + H| + |B + H| - |H|.$$

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

Corollary 3.1. *Let* G *be an additive abelian group. Let* $p(G)$ *be the least order of a nonzero element of* G, *or* $p(G) = +\infty$ *if* G *is torsion-free. Then, for any finite nonempty subsets* A *and* B *of* G, *we have*

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

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. □

Quite recently G. Károlyi was able to extend the Erdős-Heilbronn conjecture to abelian groups.

Theorem 3.5 [G. Károlyi, Israel J. Math. 139(2004)]**.** *Let* G *be an additive abelian group. Then, for any finite nonempty subset* A *of* G, *we have*

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

As 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 3.5 in two steps. First, he showed that Theorem 3.5 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 he can actually prove a more general result.

Theorem 3.6 [G. Károlyi, Israel J. Math. 139(2004)]**.** *Let $\emptyset \neq A, B \subseteq \mathbb{Z}_q$, where $q = p^\alpha$ is a power of a prime p. Then*

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

For nonempty subsets A and B of $\mathbb{Z}_p$ (where p is 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, $\mathbb{Z}_q$ 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 nonzero complex numbers.

Lemma 3.1 [Z. W. Sun, Trans. Amer. Math. Soc. 348(1996); Combinatorica 23(2004)]**.** *Let $\lambda_1,\cdots,\lambda_k$ be nth roots of unity, and $c_1,\cdots,c_k$ nonnegative integers such that $c_1\lambda_1+\cdots+c_k\lambda_k=0$. Then $c_1+\cdots+c_k$ belongs to the set*

$$D(n)=\bigg\{\sum_{p\mid n}px_p:\ x_p\in\{0,1,2,\ldots\}\ \text{for each prime divisor } p \text{ of } n\bigg\}.$$

Proof of Theorem 3.6. Since $\mathbb{Z}_q$ 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 $|A'|+|B'|-3=p$. So, without loss of generality, we may assume that $k+l-3\leqslant p$ where $k=|A|$ and $l=|B|$.

Suppose that $|C|\ngeq\min\{p,k+l-3\}=k+l-3$ 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 $c\in C$, this leads a contradiction since $a\neq b$ and $ab\in C$. Thus, it suffices to show that $c_0\neq 0$.

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. As $\binom{k+l-4}{l-2}\notin D(q)=\{pn:\ n=0,1,2,\ldots\}$, we have $c_0\neq 0$ by Lemma 3.1. $\square$

4. On a conjecture of Lev

Let A and B be finite nonempty subsets of an (additively written) abelian group G. In contrast with the Cauchy-Davenport theorem, Kemperman [Acta Math. 103(1960)] and Scherk [Amer. Math. Monthly 62(1955)] proved that

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

where

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

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, in 2003 Lev [J. Théor. Nombres Bordeaux 17(2005)] proposed the following interesting conjecture.

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

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

Recently, by a sophisticated application of the Combinatorial Nullstellensatz, H. Pan and Z. W. Sun made considerable progress on Lev's conjecture.

Theorem 4.1 [H. Pan and Z. W. Sun, Israel J. Math., 154(2006)]**.** *Let A and B be finite nonempty subsets of a field F. Let $P(x,y)\in F[x,y]$ and*

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

If C is nonempty, then

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

Theorem 4.2 [H. Pan and Z. W. Sun, Israel J. Math. 154(2006)]**.** *Let A and B be finite nonempty subsets of an abelian group G whose torsion subgroup*

$$\mathrm{Tor}(G)=\{g\in G\colon g\ \textit{has a finite order}\}$$

is cyclic. For $i=1,\ldots,l$ let m_i and n_i be nonnegative integers and let $d_i\in G$. Suppose that

$$C=\{a+b\colon a\in A,\ b\in B,\ \textit{and } m_ia-n_ib\neq d_i\ \textit{for all } i=1,\ldots,l\}$$

is nonempty. Then

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

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

Theorem 4.3 [H. Pan and Z. W. Sun, Israel J. Math. 154(2006)]**.** *Let G be an abelian group, and let A,B,S be finite nonempty subsets of G with*

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

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

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

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

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

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 in the case $P(x, y) = \prod_{s\in S}(x - y - s)$.

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 the second part. □