A talk given at Department of Mathematics, Zhejiang University (2007-04-06).

ADDITIVE COMBINATORICS AND LATIN TRANSVERSALS

Zhi-Wei Sun

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

Abstract. Additive combinatorics is currently a highly active area of research which has attracted many first-rate mathematicians including Noga Alon, Ben Green and Terence Tao. We will talk about the main results in this field and the powerful polynomial method. In particular, we will focus on two famous conjectures of Snevily and related Latin transversals.

While in the past many of the basic combinatorial results were obtained mainly by ingenuity and detailed reasoning, the modern theory has grown out of this early stage, and often relies on deep, well developed tools.

—Noga Alon (ICM, Beijing, 2002)

Additive combinatorics is currently a highly active area of research. One remarkable feature of the field is the use of tools from many diverse fields of mathematics.

—Terence Tao & V. Vu (2006)

1. Introduction to additive combinatorics

During his study of Goldbach's conjecture, L. G. Shnirel'man introduced in 1933 the Shnirel'man density of a subset A of $\mathbb{N}=\{0,1,2,\ldots\}$:

$$\sigma(A):=\inf_{n\geqslant 1}\frac{|\{a\in A:\ 0\leqslant a<n\}|}{n}.$$

Using this concept he showed that there exists a constant $c>0$ such that each integer greater than one can be expressed as a sum of at most c primes; this is the first important progress on Goldbach's conjecture.

In 1942 Mann established the following fundamental result conjectured by Shnirel'man.

Mann's Theorem. *Let A and B be subsets of $\mathbb{N}$ containing 0. Then*

$$\sigma(A+B)\geqslant\min\{1,\,\sigma(A)+\sigma(B)\},$$

where $A+B$ denotes the sumset $\{a+b:\ a\in A,\ b\in B\}$.

Let A and B be nonempty subsets of an abelian group G. For $e\in G$ we let

$$A_e=A\cup(e+B)\supseteq A\text{ and }B_e=(A-e)\cap B\subseteq B,$$

and call the pair (A_e,B_e) the Dyson e-transformation of the pair (A,B). It is easy to see that $A_e+B_e\subseteq A+B$, and $|A_e|+|B_e|=|A|+|B|$ if A and B are finite. For some $e\in G$ one might have $|B_e|<|B|$. Thus Dyson's transformation plays an important role in induction proofs of some additive results such as Mann's theorem.

Let p be a prime. Then $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z} = \{\bar{a} = a + p\mathbb{Z} : a \in \mathbb{Z}\}$ is a field with p elements. If $A = \{\bar{1}, \ldots, \bar{k}\}$ and $B = \{\bar{1}, \ldots, \bar{l}\}$ with $|A| = k \leqslant p$ and $|B| = l \leqslant p$, then $A + B = \{\bar{2}, \ldots, \overline{k+l}\}$ and hence

$$|A + B| = \min\{p, k + l - 1\} = \min\{p, |A| + |B| - 1\}.$$

Cauchy-Davenport Theorem. *Let p be any prime. If A and B are nonempty subsets of $\mathbb{Z}_p$, then*

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

In 1953 Kneser extended the Cauchy-Davenport theorem to general abelian groups.

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*

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

Corollary. *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

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

Freiman's Theorem (Freiman, 1966)**.** *Let A be a finite nonempty subset of $\mathbb{Z}$ with $|A+A|\leqslant c|A|$. Then A is contained in an n-dimensional AP*

$$Q=Q(a;q_1,\ldots,q_n;l_1,\ldots,l_n)=\{a+x_1q_1+\cdots+x_nq_n:\ 0\leqslant x_i<l_i\}$$

with $|Q|\leqslant c'|A|$, where c' and n only depend on c.

This deep theorem plays a crucial role in the Fields medalist W. T. Gowers' quantitative proof [Geom. Func. Analysis Appl., 2001] of the famous Szemerédi theorem. Ben Green and I. Z. Ruzsa [J. London Math. Soc., in press] extended Freiman's theorem to any abelian group.

Let $A_1,\ldots,A_n$ be sets. If $a_1\in A_1,\ldots,a_n\in A_n$, and $a_i\neq a_j$ for all $1\leqslant i<j\leqslant n$, then $\{a_i\}_{i=1}^n$ is called an SDR (*systems of distinct representatives* of $\{A_i\}_{i=1}^n$. In 1935 P. Hall proved the following fundamental theorem in discrete mathematics: *$\{A_i\}_{i=1}^n$ has an SDR if and only if $|\bigcup_{i\in I}A_i|\geqslant|I|$ for all $I\subseteq\{1,\ldots,n\}$.*

If $A_1,\ldots,A_n$ are subsets of an additive abelian group, then we may consider the sum of the elements in an SDR of $\{A_i\}_{i=1}^n$. Different SDR's may lead the same sum. So it is interesting to find a sharp lower bound for the cardinality of the restricted sumset

$$A_1\dot{+}\cdots\dot{+}A_n=\{a_1+\cdots+a_n\colon\{a_i\}_{i=1}^n\text{ forms an SDR of }\{A_i\}_{i=1}^n\}.$$

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

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

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

This conjecture is so difficult that it had been open for thirty years until it was finally confirmed by Dias da Silva and Y. Hamidoune [Bull. London. Math. Soc. 1994], with the help of the representation theory of groups.

For a field F, $p(F)$ is the additive order of the (multiplicative) identity of F, and the *characteristic* of F is given by

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

Dias 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 Dias 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.

Motivated by his study of graph theory, F. Jaeger posed in 1982 the following conjecture.

Jaeger's Conjecture. *Let F be a finite field with at least 4 elements, and let A be an invertible $n \times n$ matrix with entries in F. There there exists a vector $\vec{x} \in F^n$ such that both $\vec{x}$ and $A\vec{x}$ have no zero component.*

In 1989 N. Alon and M. Tarsi [Combinarorica, 9(1989)] confirmed the conjecture in the case when $|F|$ is not a prime. Moreover their method later resulted in the following powerful principle.

Combinatorial Nullstellensatz [Alon, Comb. Probab. Comput. 1999]**.** *Let $A_1,\ldots,A_n$ be finite subsets of a field F with $|A_i|>k_i\in\mathbb{N}$ for $i=1,\ldots,n$. If $f(x_1,\ldots,x_n)\in F[x_1,\ldots,x_n]$ has degree $k_1+\cdots+k_n$, and $[x_1^{k_1}\cdots x_n^{k_n}]f(x_1,\ldots,x_n)$ (the coefficient of $x_1^{k_1}\cdots x_n^{k_n}$ in f) does not vanish, then there are $a_1\in A_1,\ldots,a_n\in A_n$ such that $f(a_1,\ldots,a_n)\neq 0$.*

Let F be a finite field with $|F|=p^\alpha$ where p is a prime and α is an integer greater than one. Let $A=(a_{ij})_{1\leqslant i,j\leqslant n}$ be an invertible matrix over F. In view of Combinatorial Nullstellensatz, Alon and Tarsi's result can be reduced to the following one: There exist nonnegative integers $k_1,\ldots,k_n$ smaller than $|F\setminus\{0\}|$ such that

$$[x_1^{k_1}\cdots x_n^{k_n}]\prod_{i=1}^n\sum_{j=1}^n a_{ij}x_j\neq 0.$$

Combinatorial Nullstellensatz implies the following useful lemma of N. Alon, M. B. Nathanson and I. Z. Ruzsa [J. Number Theory 56(1996)].

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

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

then we have

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

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

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

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

The ANR lemma can be used to obtain lower bounds for various restricted sumsets, e.g. the Erdős-Heilbronn conjecture can be proved easily with the help of this lemma while the first proof of the conjecture given by Dias da Silva and Hamidoune [Bull. London. Math. Soc.] in 1994 involved the representation theory of symmetric groups.

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

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

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 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,

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

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

The speaker has published several papers on sumsets with polynomial restrictions; see Z. W. Sun [Acta Arith. 2001], Q. H. Hou and Z. W. Sun [Acta Arith. 102(2002)], J. X. Liu and Z. W. Sun [J. Number Theory 2002], H. Pan and Z. W. Sun [J. Combin. Theory Ser. A 2002], Z. W. Sun [J. Combin. Theory Ser. A, 2003], Z. W. Sun and Y. N. Yeh [J. Number Theory 2005]), H. Pan and Z. W. Sun [Israel J. Math. 2006].

In 2004 G. Károlyi was able to extend the Erdős-Heilbronn conjecture to abelian groups.

Theorem [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*

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

Finally we mention a recent result which is an improvement of previous work of J. Bourgain, N. Katz and T. Tao [Geom. Func. Analysis Appl. 14(2004)] and M. Z. Garaev [`arXiv:math.NT/0702780`].

Theorem (N. Katz and C. Y. Shen, `arXiv:math.NT/0703614`)**.** *Let p be a prime and let $A \subseteq \mathbb{Z}_p$ with $|A| < \sqrt{p}$. Then*

$$\max\{|A+A|, |AA|\} \geqslant c|A|^{14/13}/(\ln|A|)^{\alpha},$$

where c and α are positive constants (independent of p and A).

2. On two conjectures of Snevily and Latin transversals

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

Let $G = \{a_1, \ldots, a_n\}$ be a group of order n. The matrix $(a_i b_j)_{1 \leqslant i,j \leqslant n}$ (i.e., the Cayley multiplication table of G) is obviously a Latin square over G since the cancellation law holds.

Let $b_1, \ldots, b_n$ be (not necessarily distinct) elements of an abelian group G of order n. If both $\{a_i\}_{i=1}^n$ and $\{a_i + b_i\}_{i=1}^n$ are numberings of the elements of G, then $\sum_{i=1}^n (a_i + b_i) = \sum_{i=1}^n a_i$ and hence $b_1 + \cdots + b_n = 0$. In 1952 M. Hall [Proc. Amer. Math. Soc.] obtained the converse.

M. Hall's theorem. *Let $G = \{a_1, \ldots, a_n\}$ be an additive abelian group, and let $b_1, \ldots, b_n$ be elements of G with $b_1 + \cdots + b_n = 0$. Then there exists $\sigma \in S_n$ such that $a_{\sigma(1)} + b_1, \ldots, a_{\sigma(n)} + b_n$ are distinct, where S_n is the symmetric group of all permutations on $\{1, \ldots, n\}$.*

Hall's proof of the above theorem is highly technical. Here is a consequence (observed by Sun and Yeh) which answers an open question of Parker (cf. Guy [Amer. Math. Monthly 100(1993)]).

Corollary 2.1[Z. W. Sun and Y. N. Yeh, J. Number Theory 2005]**.** *Let $G=\{0,a_1,\ldots,a_{n-1}\}$ be an additive abelian group of order $n>1$, and let $b_1,\ldots,b_{n-1}$ be elements of G with $b_1+\cdots+b_{n-1}=0$. Then there are permutations $\sigma,\tau\in S_{n-1}$ such that $b_i=a_{\sigma(i)}+a_{\tau(i)}$ for all $i=1,\ldots,n$.*

Proof. Set $a_n=b_n=0$. As $G=\{-a_1,\ldots,-a_n\}$, by M. Hall's theorem there is a permutation $\lambda\in S_n$ such that $b_1-a_{\lambda(1)},\ldots,b_n-a_{\lambda(n)}$ are distinct. Choose a permutation $\sigma\in S_{n-1}$ such that

$$a_{\sigma(i)}=a_{\lambda(i)}-a_{\lambda(n)}\neq 0\quad \text{for every } i=1,\ldots,n-1.$$

Since $\{b_i-a_{\sigma(i)}:\ i=1,\ldots,n-1\}=G\setminus\{0\}$, there is a permutation $\tau\in S_{n-1}$ such that for any $i=1,\ldots,n-1$ we have $b_i-a_{\sigma(i)}=a_{\tau(i)}$ and hence $b_i=a_{\sigma(i)}+a_{\tau(i)}$. $\square$

In 1999 H. Snevily [Amer. Math. Monthly] made the following conjecture.

Conjecture 2.1 (Snevily, 1999)**.** *Let $m>n>0$ be integer. Then, for any $b_1,\ldots,b_n\in\mathbb{Z}$, there exists a permutation $\sigma\in S_n$ such that $1+b_{\sigma(1)},\ldots,n+b_{\sigma(n)}$ are pairwise distinct modulo m.*

In 2002 Kézdy and Snevily [Combin. Probab. Comput.] proved that the conjecture holds when $n\leqslant(m+1)/2$. This follows from the following result in the case $\alpha_1=\cdots=\alpha_n=1$ and $A_1=\cdots=A_n=\{1,\ldots,n\}$.

Theorem 2.2 (Sun and Yeh, J. Number Theory 2005]). *Let $\alpha_1,\ldots,\alpha_n$ be positive reals, and let $b_1,\ldots,b_n$ be integers. Let $A_1,\ldots,A_n$ be finite subsets of $\mathbb{Z}$ with cardinality $k\geqslant n$. For $1\leqslant i<j\leqslant n$ let m_{ij} be an integer greater than $2\max\{|x_i-x_j|:\ x_i\in A_i,\ x_j\in A_j\}|$. Then the restricted sumset*

$$\left\{\sum_{i=1}^n a_i:\ a_i\in A_i,\ a_i\alpha_i\neq a_j\alpha_j \text{ and } a_i+b_i\not\equiv a_j+b_j\ (\mathrm{mod}\ m_{ij}) \text{ if } i<j\right\}$$

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

For $1\leqslant i<j\leqslant n$, let r_{ij} denote the unique integer in the interval $(-m_{ij}/2,m_{ij}/2]$ which is congruent to b_i-b_j modulo m_{ij}. For $x_i\in A_i$ and $x_j\in A_j$, as $|x_i-x_j|<m_{ij}/2$ we have

$$x_i+b_i\equiv x_j+b_j\ (\mathrm{mod}\ m_{ij})\iff x_j-x_i=r_{ij}.$$

In view of the ANR Lemma, it suffices to show that the coefficient

$$\begin{aligned}&[x_1^{k-1}\cdots x_n^{k-1}](x_1+\cdots+x_n)^{(k-n)n}\prod_{1\leqslant i<j\leqslant n}(\alpha_jx_j-\alpha_ix_i)(x_j-x_i-r_{ij})\\&=[x_1^{k-1}\cdots x_n^{k-1}](x_1+\cdots+x_n)^{(k-n)n}\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)(\alpha_jx_j-\alpha_ix_i)\end{aligned}$$

is nonzero. In fact, the coefficient equals

$$(-1)^{n(n-1)/2}\frac{((k-n)n)!}{\prod_{n\leqslant j<k}(j)_n}\mathrm{per}(\alpha_j^{i-1})_{1\leqslant i,j\leqslant n},$$

where $(j)_n=j(j-1)\cdots(j-n+1)$ and

$$\mathrm{per}(\alpha_j^{i-1})_{1\leqslant i,j\leqslant n}=\sum_{\sigma\in S_n}\prod_{i=1}^n\alpha_{\sigma(i)}^{i-1}>0.$$

Let n be a positive integer. If $\{a_1,\ldots,a_n\}$, $\{b_1,\ldots,b_n\}$ and $\{a_1+b_1,\ldots,a_n+b_n\}$ are all complete systems of residues modulo n, then

$$0+1+\cdots+(n-1)\equiv b_1+\cdots+b_n\equiv 0\ (\mathrm{mod}\ n)$$

and hence $2\nmid n$.

Let n be a positive odd integer, and let $G=\{a_1,\ldots,a_n\}$ be an abelian group of order n. Clearly the Cayley addition table $M=(a_i+a_j)_{1\leqslant i,j\leqslant n}$ contains a Latin transversal $a_1+a_1,\ldots,a_n+a_n$ since

$$a_i+a_i=a_j+a_j\Rightarrow 2(a_i-a_j)=0\Rightarrow a_i=a_j\Rightarrow i=j.$$

In 1999 H. S. Snevily [Amer. Math. Monthly] 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 are 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 pairwise distinct.*

To prove Snevily's conjecture for the additive group $\mathbb{Z}/p\mathbb{Z}$ where p is an odd prime, Alon [Israel J. Math. 117(2000)] first showed that if $0<n<p$ then

$$\begin{aligned}&[x_1^{n-1}\cdots x_n^{n-1}]\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)(x_j+b_j-(x_i+b_i))\\&=[x_1^{n-1}\cdots x_n^{n-1}]\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)^2\neq 0\ \ (\text{in the field }\mathbb{Z}/p\mathbb{Z}),\end{aligned}$$

and then employed the Combinatorial Nullstellensatz. It should be mentioned that Hou and Sun [Acta Arith. 102(2002)] obtained the following further result: If k, m, n are positive integers with $k-1 \geqslant m(n-1)$, then

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

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

$$\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)(b_jx_j-b_ix_i)=(-1)^{\binom{n}{2}}|x_j^{n-i}|_{1\leqslant i,j\leqslant n}\times|b_j^{i-1}x_j^{i-1}|_{1\leqslant i,j\leqslant n}$$
$$=(-1)^{\binom{n}{2}}\sum_{\sigma\in S_n}\varepsilon(\sigma)\prod_{i=1}^{n}x_{\sigma(i)}^{n-i}\sum_{\tau\in S_n}\varepsilon(\tau)\prod_{i=1}^{n}b_{\tau(i)}^{i-1}x_{\tau(i)}^{i-1},$$

where $\varepsilon(\sigma)$ denotes the sign of $\sigma\in S_n$ which is 1 or -1 according as σ is

even or odd. Therefore

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

This is exactly the way Dasgupta, Károlyi, Serra and Szegedy [Israel J. Math. 126(2001)] proved Snevily's conjecture for cyclic groups with odd order.

By using some knowledge from Algebraic Number Theory, Z. W. Sun [J. Combin. Theory Ser. A 103(2003)] was able to establish the following theorem.

Theorem 2.3 [Z. W. Sun, 2003]**.** *Let G be an additive abelian group whose finite subgroups are all cyclic. Let $A_1,\ldots,A_n$ $(n>1)$ be finite subsets of G with cardinality $k\geqslant n$, and let $b_1,\ldots,b_n$ be elements of G. Let m be any positive integer not exceeding $(k-1)/(n-1)$.*

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

(ii) *The sets*

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

and

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

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 pairwise 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* $b_1,\ldots,b_n$.

When G is a cyclic group with $|G|$ odd or a prime power, our Theorem 2.3 (ii) in the case $k=n$ and $m=1$, yields the main results of Dasgupta et al.

Actually Theorem 2.3 follows from Sun's stronger results on sumsets with polynomial restrictions.

3. Some recent results of the speaker

In Snevily's conjecture the abelian group is required to have odd order. (An abelian group of positive even order has an element g of order 2 and hence we don't have the described result for $A=B=\{0,g\}$.) For a general abelian group G with cyclic torsion subgroup, if we make no hypothesis on the order of G, what additive properties can we impose on several subsets of G with cardinality n? In this direction we establish the following new theorem of additive nature.

Theorem 3.1 [Z. W. Sun, `arXiv:math.CO/0610981`]**.** *Let* G *be any additive abelian group with cyclic torsion subgroup, and let* $A_1,\ldots,A_m$ *be arbitrary subsets of* G *with cardinality* $n\in\mathbb{Z}^+=\{1,2,3,\ldots\}$*, where* m *is odd. 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. In other words, for a certain subset* A_{m+1} *of* G *with* $|A_{m+1}|=n$*, there is a matrix* $(a_{ij})_{1\leqslant i\leqslant m+1,\,1\leqslant j\leqslant n}$ *such that* $\{a_{i1},\ldots,a_{in}\}=A_i$ *for all* $i=1,\ldots,m+1$ *and the column sum* $\sum_{i=1}^{m+1}a_{ij}$ *vanishes for every* $j=1,\ldots,n$*.*

Theorem 3.1 in the case $m=3$ is essential; the result for $m=5,7,\ldots$ can be obtained by repeated use of the case $m=3$.

Example 3.1. In Theorem 3.1 the condition $2\nmid m$ is indispensable. Let G be an additive cyclic group of even order n. Then G has a unique element g of order 2 and hence $a\neq -a$ for all $a\in G\setminus\{0,g\}$. Thus $\sum_{a\in G}a=0+g=g$. For each $i=1,\ldots,m$ let $a_{i1},\ldots,a_{in}$ be a list of the n elements of G. If those $\sum_{i=1}^m a_{ij}$ with $1\leqslant j\leqslant n$ are distinct, then

$$\sum_{a\in G}a=\sum_{j=1}^n\sum_{i=1}^m a_{ij}=\sum_{i=1}^m\sum_{j=1}^n a_{ij}=m\sum_{a\in G}a,$$

hence $(m-1)g=(m-1)\sum_{a\in G}a=0$ and therefore m is odd.

Example 3.2. The group G in Theorem 3.1 cannot be replaced by an arbitrary abelian group. To illustrate this, we look at the Klein quaternion group

$$\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}=\{(0,0),(0,1),(1,0),(1,1)\}$$

and its subsets

$$A_1=\{(0,0),(0,1)\},\ A_2=\{(0,0),(1,0)\},\ A_3=\cdots=A_m=\{(0,0),(1,1)\},$$

where $m \geqslant 3$ is odd. For $i = 1, \ldots, m$ let a_i, a_i' be a list of the two elements of A_i, then

$$\sum_{i=1}^{m}(a_i + a_i') = (0,1) + (1,0) + (m-2)(1,1) = (0,0)$$

and hence $\sum_{i=1}^{m} a_i = -\sum_{i=1}^{m} a_i' = \sum_{i=1}^{m} a_i'$.

Recall that a line of 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 3.1. *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 $n \times n \times n$ subcube with $n \leqslant N$ contains a Latin transversal.*

Proof. Just apply Theorem 3.1 with $G = \mathbb{Z}/N\mathbb{Z}$ and $m = 3$. □

In 1967 H. J. Ryser conjectured that every Latin square of odd order has a Latin transversal. Another conjecture of Brualdi states that every Latin square of order n has a partial Latin transversal of size $n - 1$. These and Corollary 3.1 suggest that our following conjecture might be reasonable.

Conjecture 3.1 (Z. W. Sun, 2006)**.** *Every $n \times n \times n$ Latin cube contains a Latin transversal.*

Note that Conjecture 3.1 does not imply Theorem 3.1 since an $n\times n\times n$ subcube of a Latin cube might have more than n distinct entries.

Corollary 3.2. *Let G be any additive abelian group with cyclic torsion subgroup, and let $A_1,\ldots,A_m$ be subsets of G with cardinality $n\in\mathbb{Z}^+$, where m is even. Suppose that all the elements of A_m have 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.*

Proof. As $m-1$ is odd, by Theorem 3.1 the elements of A_i $(1\leqslant i\leqslant m-1)$ can be listed in a suitable order $a_{i1},\ldots,a_{in}$, such that all the sums $s_j=\sum_{i=1}^{m-1}a_{ij}$ $(1\leqslant j\leqslant n)$ are distinct. Since all the elements of A_m have odd order, by Theorem 1.1(ii) of Z. W. Sun [J. Combin. Theory Ser. A] there is a numbering $\{a_{mj}\}_{j=1}^n$ of the elements of A_m such that all the sums $s_j+a_{mj}=\sum_{i=1}^m a_{ij}$ $(1\leqslant j\leqslant n)$ are distinct. We are done. □

As an essential result, Theorem 3.1 might have various potential applications in additive number theory and combinatorial designs.

Since any abelian group with cyclic torsion subgroup can be embedded in the multiplicative group $\mathbb{C}^*=\mathbb{C}\setminus\{0\}$ (see Z. W. Sun [J. Combin. Theory Ser. A 2003] for the reason), Theorem 3.1 actually follows from the following result.

Theorem 3.2 [Z. W. Sun, `arXiv:math.CO/0610981`]**.** *Let $A_1,\ldots,A_n$ and $B_1,\ldots,B_n$ be subsets of a field F with cardinality n, and let $c_1,\ldots,c_n$ be distinct elements of F. Then there is an SDR $\{a_i\}_{i=1}^n$ of $\{A_i\}_{i=1}^n$ and an SDR $\{b_i\}_{i=1}^n$ of $\{B_i\}_{i=1}^n$ such that the products $a_1b_1c_1,\ldots,a_nb_nc_n$ are*

distinct.

Proof. In view of the Combinatorial Nullstellensatz, it suffices to show that

$$c := [x_1^{n-1}\cdots x_n^{n-1}y_1^{n-1}\cdots y_n^{n-1}]\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)(y_j-y_i)(c_jx_jy_j-c_ix_iy_i)$$

does not vanish. In fact,

$$\begin{aligned}&\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)(y_j-y_i)(c_jx_jy_j-c_ix_iy_i)\\ =&|x_i^{j-1}|_{1\leqslant i,j\leqslant n}|y_i^{j-1}|_{1\leqslant i,j\leqslant n}|(c_ix_iy_i)^{j-1}|_{1\leqslant i,j\leqslant n}\\ =&\sum_{\sigma\in S_n}\varepsilon(\sigma)\prod_{i=1}^n x_i^{\sigma(i)-1}\times\sum_{\tau\in S_n}\varepsilon(\tau)\prod_{i=1}^n y_i^{\tau(i)-1}\times\sum_{\lambda\in S_n}\varepsilon(\lambda)\prod_{i=1}^n(c_ix_iy_i)^{\lambda(i)-1}\\ =&\sum_{\lambda\in S_n}\varepsilon(\lambda)\prod_{i=1}^n c_i^{\lambda(i)-1}\sum_{\sigma,\tau\in S_n}\varepsilon(\sigma\tau)\prod_{i=1}^n\left(x_i^{\lambda(i)+\sigma(i)-2}y_i^{\lambda(i)+\tau(i)-2}\right).\end{aligned}$$

and hence

$$c=\sum_{\lambda\in S_n}\left(\varepsilon(\lambda)\prod_{i=1}^n c_i^{\lambda(i)-1}\right)\varepsilon(\bar\lambda\bar\lambda)=|c_i^{j-1}|_{1\leqslant i,j\leqslant n}=\prod_{1\leqslant i<j\leqslant n}(c_j-c_i)\neq 0,$$

where $\bar\lambda(i)=n+1-\lambda(i)$ for $i=1,\ldots,n$. □

We can further extend Theorem 3.1 via restricted sumsets in a field.

Theorem 3.3 [Z. W. Sun, `arXiv:math.CO/0610981`]. *Let h,k,l,m,n be positive integers satisfying*

$$k-1\geqslant m(n-1)\quad\text{and}\quad l-1\geqslant h(n-1). \tag{3.1}$$

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

$$K=(k-1)n-(m+1)\binom{n}{2}\ \text{and}\ L=(l-1)n-(h+1)\binom{n}{2}. \tag{3.2}$$

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*

$$a_ib_ic_i\neq a_jb_jc_j,\ P_i(a_i)\neq P_j(a_j),\ Q_i(b_i)\neq Q_j(b_j)\ \text{ if } 1\leqslant i<j\leqslant n.$$

If h,k,l,m,n are positive integers satisfying (3.1), then the integers K and L given by (3.2) are nonnegative since

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

From Theorem 3.3 we can deduce the following extension of Theorem 3.1.

Theorem 3.4 [Z. W. Sun, `arXiv:math.CO/0610981`]. *Let* G *be an additive abelian group with cyclic torsion subgroup. Let* h,k,l,m,n *be positive integers satisfying* (3.1). *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*

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

Here is another extension of Theorem 3.1 via restricted sumsets in a field.

Theorem 3.5 [Z. W. Sun, `arXiv:math.CO/0610981`]. *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 is an SDR $\{b_i\}_{i=1}^n$ of $\{B_i\}_{i=1}^n$ such that the restricted sumset*

$$S = \{a_1 + \cdots + a_n : a_i \in A_i,\ a_i - a_j \notin S_{ij} \text{ and } a_i b_i c_i \neq a_j b_j c_j \text{ if } i < j\}$$

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