Proc. of the 4th ICCM, Vol. I, Higher Edu. Press, Beijing, 2007, pp. 475–495.

Groups in Combinatorial Number Theory

Zhi-Wei Sun*

Abstract

In combinatorial number theory, there are many topics related to group structure. Even for abelian or cyclic groups, there are some very challenging unsolved conjectures. In this talk we give a survey of problems, results and methods in several fields of combinatorial number theory. The topics include sumsets in additive combinatorics, Snevily's conjecture and Latin transversals, covers of the integers and groups.

2000 Mathematics Subject Classification: 05E99, 11B75, 20D60.
Keywords and Phrases: Combinatorial number theory, Additive combinatorics, Group, Sumset, Cover, Zero-sum.

1. Sumsets in 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 $\mathbb{N} = \{0, 1, 2, \dots\}$:

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

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 H. Mann [35] established the following fundamental result conjectured by Shnirel'man.

*Department of Mathematics, Nanjing University, Nanjing 210093, P. R. China. E-mail: zwsun@nju.edu.cn URL: http://math.nju.edu.cn/∼zwsun

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

Theorem 1.1 (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

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

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. Any cyclic group of order p is isomorphic to the additive group $\mathbb{Z}_p=\mathbb{Z}/p\mathbb{Z}=\{\bar a = a+p\mathbb{Z}:\ a\in\mathbb{Z}\}$. 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

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

Theorem 1.2 (Cauchy-Davenport Theorem (cf. [69])). *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 M. Kneser [31] extended the Cauchy-Davenport theorem to general abelian groups.

Theorem 1.3 (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 stabilizer $\{g\in G:\ g+A+B=A+B\}$. If $|A+B|\leqslant|A|+|B|-1$, then*

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

Corollary 1.1. *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

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

The following deep theorem was first established by G. Freiman [19] in 1966 via a complicated geometric method.

Theorem 1.4 (Freiman's Theorem)**.** *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*

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

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

B. Green and I. Z. Ruzsa [22] extended Freiman's theorem to any abelian group. Freiman's theorem plays a crucial role in the Fields medalist T. Gowers' quantitative proof (cf. [20]) of the famous Szemerédi theorem [68], which partially motivated B. Green and T. Tao [23] to obtain the following celebrated theorem first conjectured by P. Erdős and P. Turán [17] in 1936.

Theorem 1.5 (Green-Tao Theorem)**.** *For each integer $k \geqslant 3$, there are k distinct primes so that they form an arithmetic progression of length k.*

Conjecture 1.1 (Erdős-Szemerédi Conjecture [16])**.** *Let A be a finite nonempty set of integers or reals. Then for any $\varepsilon > 0$ there is a constant $c_\varepsilon > 0$ such that*

$$|A+A| + |AA| \geqslant c_\varepsilon |A|^{2-\varepsilon},$$

where $AA = \{a_1a_2 : \ a_1, a_2 \in A\}$.

Theorem 1.6. *Let p be a prime and let $\emptyset \neq A \subseteq \mathbb{Z}_p$.*

(i) (J. Bourgain, N. Katz & T. Tao [8], J. Bourgain & S. Konyagin [9]) *If $|A| < p^{1-\delta}$ with $\delta > 0$, then there are $c(\delta) > 0$ and $\varepsilon(\delta) > 0$ such that*

$$\max\{|A+A|, \ |AA|\} \geqslant c(\delta)|A|^{1+\varepsilon(\delta)}.$$

(ii) (N. Katz & C. Y. Shen [29]) *If $|A| < \sqrt{p}$, then*

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

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

Let $A_1, \dots, A_n$ be sets. If $a_1 \in A_1, \dots, a_n \in A_n$, 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 $I \subseteq \{1, \dots, n\}$.*

If $A_1, \dots, A_n$ 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

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

In 1964 Erdős and Heilbronn [15] made the following challenging conjecture.

Conjecture 1.2 (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*

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

This conjecture is so difficult that it had been open for thirty years until it was finally confirmed by J. A. Dias da Silva and Y. O. Hamidoune [13] in 1994, with the help of the representation theory of groups.

For a field F, clearly $p(F)$ coincides with the additive order of the (multiplicative) identity of F, which is either a prime or the infinity $+\infty$.

Theorem 1.7 (Dias da Silva–Hamidoune Theorem). *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.

Corollary 1.2. *If p is a prime, $A \subseteq \mathbb{Z}_p$ and $|A| > \sqrt{4p-7}$, then any element of $\mathbb{Z}_p$ can be written as a sum of $\lfloor |A|/2 \rfloor$ distinct elements of A.*

Proof. Let $n = \lfloor |A|/2 \rfloor$. It is easy to see that $n|A| - n^2 + 1 \geqslant p$. Thus, by the Dias da Silva–Hamidoune theorem, we have $|n^\wedge A| \geqslant p$ and hence $n^\wedge A = \mathbb{Z}_p$. □

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

Conjecture 1.3 (Jäger'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 [5] confirmed the conjecture in the case when $|F|$ is not a prime. Moreover their method later resulted in the following powerful principle (see Alon [1]).

Theorem 1.8 (Combinatorial Nullstellensatz). *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 $\sum_{i=1}^n k_i$, and the coefficient $[x_1^{k_1} \cdots x_n^{k_n}]f(x_1, \ldots, x_n)$ (of the monomial $x_1^{k_1} \cdots x_n^{k_n}$ 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 the 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

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

The method using the Combinatorial Nullstellensatz is also called the polynomial method. By means of this tool, Alon, Nathanson and Ruzsa [4] obtained the following result on restricted sumsets in 1996.

Theorem 1.9 (Alon, Nathanson, Ruzsa). *Let $A_1, \ldots, A_n$ be finite nonempty subsets of a field F with $|A_1| < \cdots < |A_n|$. Then*

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

Theorem 1.7 follows from Theorem 1.9 since for each set A with $|A| = k \geqslant n$ we can choose subsets $A_1, \ldots, A_n$ of A with cardinalities $k - n + 1, k - n + 2, \ldots, k$ respectively.

In 2002 Q. H. Hou and Z. W. Sun [27] generalized the Erdős-Heilbronn conjecture in another direction.

Theorem 1.10 (Hou & Sun). *Let $k, m \in \mathbb{N}$ and $n \in \mathbb{Z}^+ = \{1, 2, 3, \ldots\}$. Let F be a field with $p(F)$ greater than mn and $(k - 1 - m(n-1))n$. If $A_1, \ldots, A_n$ are subsets of F with cardinality k, and $S_{ij} \subseteq F$ and $|S_{ij}| \leqslant m$ for all $i, j = 1, \ldots, n$ with $i \neq j$, then for the difference-restricted sumset*

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

we have $|C| \geqslant (k - 1 - m(n-1))n + 1$.

A key step in the proof of Theorem 1.10 is to show that if $k,m,n\in\mathbb{N}$, $n\geqslant 2$ and $k>m(n-1)$ then

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

In 2004 G. Károlyi [28] was able to extend the Erdős-Heilbronn conjecture to general abelian groups.

Theorem 1.11 (G. Károlyi). *Let G be an additive abelian group. Then, for any finite nonempty subset A of G, we have*

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

The following conjecture of V. F. Lev [34] was motivated by the Erdős-Heilbronn conjecture and the Kemperman-Scherk theorem (cf. [30] and [44]).

Conjecture 1.4 (Lev's Conjecture). *Let G be an abelian group, and let A and B be finite non-empty subsets of G. Then we have*

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

where

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

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

In 2006 H. Pan and Z. W. Sun [39] applied the Combinatorial Nullstellensatz in a new way to make the following progress on Lev's conjecture.

Theorem 1.12 (Pan and Sun). *Let G be an abelian group, and let A,B,S be finite non-empty subsets of G with*

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

(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 the torsion subgroup* $\mathrm{Tor}(G)=\{g\in G:\ g \text{ has a finite order}\}$ *is cyclic, then*

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

Recently, Z. W. Sun [65] extended the Cauchy-Davenport theorem in a new direction, and H. Pan and Sun [41] generalized the Erdős-Heilbronn conjecture in the same spirit.

Theorem 1.13. *Let* $A_1,\ldots,A_n$ *be finite nonempty subsets of* F, *and let*

$$f(x_1,\ldots,x_n)=c_1x_1^k+\cdots+c_nx_n^k+g(x_1,\ldots,x_n)\in F[x_1,\ldots,x_n]$$

with $k\in\mathbb{Z}^+$, $c_1,\ldots,c_n\in F\setminus\{0\}$ *and* $\deg g<k$.

(i) (Sun [65]) *We have*

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

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

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

If $n\geqslant k$, *then for any finite subset* A *of* F *we have*

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

(ii) (Pan & Sun [41]) *In the case* $c_1=\cdots=c_n$, *we have*

$$\begin{aligned}&|\{f(a_1,\ldots,a_n):\ a_1,\ldots,a_n\in A,\ \text{and } a_i\neq a_j \text{ if } i\neq j\}|\\&\qquad\geqslant \min\{p(F),\ q_1+\cdots+q_n+1\},\end{aligned}$$

where

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

2. Snevily's Conjecture 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 $(a_ib_j)_{1\leqslant i,j\leqslant n}$ (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 [25] obtained the converse.

Theorem 2.1 (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 a permutation $\sigma\in S_n$ such that*

$$\{a_{\sigma(1)}+b_1,\ldots,a_{\sigma(n)}+b_n\}=G,$$

where S_n is the symmetric group of all permutations on $\{1,\ldots,n\}$.

Here is a consequence observed by Sun and Yeh [67] which answers an open question of Parker.

Corollary 2.1 (Sun and Yeh). *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 $b_i=a_{\sigma(i)}+a_{\tau(i)}$. □

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

$$0+1+\cdots+(n-1)\equiv b_1+\cdots+b_n\equiv 0 \pmod n$$

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. Obviously 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 [46] made the following interesting conjecture.

Conjecture 2.1 (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.*

Snevily's conjecture can be restated in terms of Latin transversals.

Conjecture 2.1′ (Snevily's Conjecture). *Let $G = \{a_1, \ldots, a_N\}$ be an additive abelian group with $|G| = N$ odd, and let M be the Latin square $(a_i + a_j)_{1 \leqslant i,j \leqslant N}$ formed by the Cayley addition table. Then any $n \times n$ submatrix of M contains a Latin transversal.*

To prove Snevily's conjecture for the additive group $\mathbb{Z}_p$ where p is an odd prime, Alon [2] first showed that if $0 < n < p$ then

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

and then employed the Combinatorial Nullstellensatz.

Let $m > 0$ be an odd integer. As $2^{\varphi(m)} \equiv 1 \pmod{m}$ by Euler's theorem, 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 [12] enabled them to reduce Snevily's conjecture for cyclic groups of odd order to the following statement in view of the 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*

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

This can be easily shown via Vandermonde determinants.

Theorem 2.2 (Dasgupta, Károlyi, Serra and Szegedy). *Snevily's conjecture holds for any cyclic group of odd order.*

By using some knowledge from algebraic number theory, Z. W. Sun [57] established the following extension of Theorem 2.2.

Theorem 2.3 (Sun). *Let G be an additive abelian group with* $\mathrm{Tor}(G)$ *cyclic. Let $A_1,\ldots,A_n$ be finite subsets of G with cardinality $k > m(n-1)$ (where $m \in \mathbb{Z}^+$), and let $b_1,\ldots,b_n$ be elements of G.*

(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*

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

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 distinct and of odd order, or they have finite order and $n!$ cannot be written in the form $\sum_{p\in P} px_p$ with $x_p \in \mathbb{N}$, where 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. [12]

Actually Theorem 2.3 follows from Sun's following result on sumsets with polynomial restrictions.

Theorem 2.4 (Sun). *Let $k,m,n \in \mathbb{Z}^+$ with $k > m(n-1)$, and let $A_i \subseteq F$ and $|A_i| = k$ for $i=1,\ldots,n$. Let $P_1(x),\ldots,P_n(x) \in F[x]$ have degree m with leading coefficients $b_1,\ldots,b_n$ respectively.*

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

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

(ii) *If $p(F) > (k-1)n-(m+1)\binom{n}{2}$ and $\sum_{\sigma\in S_n}\prod_{i=1}^n b_{\sigma(i)}^{i-1} \neq 0$, then*

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

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? Here is a recent result due to Z. W. Sun [66].

Theorem 2.5 (Sun)**.** *Let G be any additive abelian group with cyclic torsion subgroup, and let $A_1, \ldots, A_m$ be subsets of G with cardinality $n \in \mathbb{Z}^+$. 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.*

Theorem 2.5 is sharp. We even cannot replace the group G in Theorem 2.5 by the Klein quaternion group

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1)\}.$$

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 2.2 (Sun)**.** *Let N be any positive integer. For the $N \times N \times N$ Latin cube over $\mathbb{Z}_N$ 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 2.5 with $G = \mathbb{Z}_N$ and $m = 3$. □

In 1967 H. J. Ryser [43] conjectured that every Latin square of odd order has a Latin transversal. Here is a similar conjecture of Z. W. Sun [66] motivated by Corollary 2.2.

Conjecture 2.2 (Sun)**.** *Every $n \times n \times n$ Latin cube contains a Latin transversal.*

Note that Conjecture 2.2 does not imply Corollary 2.2 since an $n \times n \times n$ sub-cube of a Latin cube might have more than n distinct entries.

Theorem 2.5 can be further extended via restricted sumsets in a field (cf. Sun [66]).

3. Covers of the Integers and Groups

Any infinite cyclic group is isomorphic to the additive group $\mathbb{Z}$ of all integers. Subgroups of $\mathbb{Z}$ different from $\{0\}$ are those $n\mathbb{Z} = \{nq : q \in \mathbb{Z}\}$ with $n \in \mathbb{Z}^+$. A coset of the subgroup $n\mathbb{Z}$ of $\mathbb{Z}$ has the form

$$a + n\mathbb{Z} = \{a + nq : q \in \mathbb{Z}\} = \{x \in \mathbb{Z} : x \equiv a \pmod n\}$$

which is called a *residue class* with *modulus* n or an arithmetic sequence with common difference n. For convenience we also write $a(n)$ or $a(\bmod n)$ for $a + n\mathbb{Z}$, thus $0(1)$ coincides with $\mathbb{Z}$, and $1(2)$ is the set of odd integers.

We can decompose the group $\mathbb{Z}$ into n cosets of $n\mathbb{Z}$, namely

$$\{r(n)\}_{r=0}^{n-1} = \{0(n),\ 1(n),\ \dots,\ n-1(n)\}$$

is a partition of $\mathbb{Z}$ (i.e., a disjoint cover of $\mathbb{Z}$). For the index of the subgroup $n\mathbb{Z}$ of $\mathbb{Z}$, we clearly have $[\mathbb{Z} : n\mathbb{Z}] = |\mathbb{Z}/n\mathbb{Z}| = n$.

A finite system $A = \{a_s(n_s)\}_{s=1}^k$ of residue classes is called a *cover* of $\mathbb{Z}$ or a *covering system* if $\bigcup_{s=1}^k a_s(n_s) = \mathbb{Z}$. Covers of $\mathbb{Z}$ were first introduced by P. Erdős in the early 1930s. He noted that $\{0(2),\ 0(3),\ 1(4),\ 5(6),\ 7(12)\}$ is a cover of $\mathbb{Z}$ with the moduli $2, 3, 4, 6, 12$ distinct. A famous unsolved problem of Erdős asks whether for any $c > 0$ we can find a cover $\{a_s(n_s)\}_{s=1}^k$ of $\mathbb{Z}$ with $c < n_1 < \ldots < n_k$ (cf. R. K. Guy [24, sections F13 & F14]). A recent breakthrough on Erdős' problem was made by M. Filaseta, K. Ford, S, Konyagin, C. Pomerance and G. Yu [18], who used the sieve method to get the following result: *For any $L > 0$ there is a constant $c(L) > 0$ such that $\sum_{s=1}^k 1/n_s > L$ for any cover $\{a_s(n_s)\}_{s=1}^k$ of $\mathbb{Z}$ with $c(L) < n_1 < \cdots < n_k$.*

Since $0(2^n)$ is a disjoint union of the residue classes $2^n(2^{n+1})$ and $0(2^{n+1})$, the systems

$$\begin{aligned} A_1 =& \{1(2), 0(2)\},\\ A_2 =& \{1(2), 2(4), 0(4)\},\\ &\dots\dots\dots\dots\dots\dots\dots\\ A_k =& \{1(2), 2(2^2), \dots, 2^{k-1}(2^k), 0(2^k)\} \end{aligned}$$

are disjoint covers of $\mathbb{Z}$. Note that $\{1(2), 2(2^2), \dots, 2^{k-1}(2^k)\}$ covers $1, \dots, 2^k - 1$ but does not cover any multiple of 2^k. In 1965 P. Erdős made the following conjecture.

Conjecture 3.1 (P. Erdős). *$A = \{a_s(n_s)\}_{s=1}^k$ forms a cover of $\mathbb{Z}$ if it covers those integers from 1 to 2^k.*

In 1969–1970 R. B. Crittenden and C. L. Vanden Eynden [10, 11] supplied a long (and somewhat awkward) proof of the Erdős conjecture for $k \geqslant 20$, which involves some deep results concerning the distribution of primes.

By using roots of unity and Vandermonde determinants, Z. W. Sun [49, 50] obtained the following local-global result which is stronger than Conjecture 1.1.

Theorem 3.1 (Sun [49, 50]). *Let $A = \{a_s(n_s)\}_{s=1}^k$ be a finite system of residue classes, and let $m_1, \ldots, m_k$ be integers relatively prime to $n_1, \ldots, n_k$ respectively. Then system A forms an m-cover of $\mathbb{Z}$ (i.e., A covers every integer at least m times) if it covers $|S|$ consecutive integers at least m times, where*

$$S = \left\{\left\{\sum_{s\in I}\frac{m_s}{n_s}\right\} : I \subseteq \{1, \ldots, k\}\right\}.$$

(As usual the fractional part of a real number x is denoted by $\{x\}$.)

Now we give an interesting consequence of Theorem 3.1.

Corollary 3.1 (Sun [56]). *Let $m_1, \ldots, m_{n-1}$ be integers relatively prime to $n > 1$. Then the set $\{\sum_{s\in I} m_s : I \subseteq \{1, \ldots, k\}\}$ contains a complete system of residues modulo n.*

Proof. Observe that the system $C = \{r(n)\}_{r=1}^{n-1}$ covers $n-1$ consecutive integers $1, \ldots, n-1$. If $W = |\{\{\sum_{s\in I} m_s/n\} : I \subseteq \{1, \ldots, n-1\}\}|$ is less than n, then C covers $1, \ldots, W$ and hence it covers all the integers. Since C does not cover 0, we must have $W = n$ and hence the desired result follows. □

Here is another local-global result obtained by Sun [61] via recurrence sequences.

Theorem 3.2 (Sun [56]). *Let G be any abelian group written additively, and let $\psi_1, \ldots, \psi_k$ be maps from $\mathbb{Z}$ to G with periods $n_1, \ldots, n_k \in \mathbb{Z}^+$ respectively. Set $\psi = \psi_1 + \cdots + \psi_k$ and*

$$T(n_1, \ldots, n_k) = \bigcup_{s=1}^k \left\{\frac{r}{n_s} : r = 0, \ldots, n_s - 1\right\}.$$

(i) *There are periodic maps $f_0, \ldots, f_{|T(n_1,\ldots,n_k)|-1} : \mathbb{Z} \to \mathbb{Z}$ depending only on $T(n_1, \ldots, n_k)$ such that $\psi(x) = \sum_{0\leqslant r<|T(n_1,\ldots,n_k)|} f_r(x)\psi(r)$*

for all $x \in \mathbb{Z}$. In particular, values of ψ are completely determined by the set $T(n_1, \ldots, n_k)$ and the initial values $\psi(0), \ldots, \psi(|T(n_1, \ldots, n_k)|-1)$.

(ii) *ψ is constant if $\psi(x)$ equals a constant for $|T(n_1, \ldots, n_k)| \leqslant n_1 + \cdots + n_k - k + 1$ consecutive integers x.*

Corollary 3.2 (Sun [59]). *Suppose that $A = \{a_s(n_s)\}_{s=1}^k$ covers consecutive $|T(n_1, \ldots, n_k)|$ integers exactly m times. Then it forms an exact m-cover of $\mathbb{Z}$ (i.e., A covers each integer exactly m times).*

Proof. For $1 \leqslant s \leqslant k$ and $x \in \mathbb{Z}$ let $\psi_s(x)$ be 1 or 0 according to whether $x \equiv a_s \pmod{n_s}$ or not. By Theorem 3.2(ii), if

$$w_A(x) = |\{1 \leqslant s \leqslant k : \ x \in a_s(n_s)\}| = \sum_{s=1}^{k} \psi_s(x)$$

coincides with m for consecutive $|T(n_1, \ldots, n_k)|$ integers, then $w_A(x) = m$ for all $x \in \mathbb{Z}$. □

Soon after his invention of covers of $\mathbb{Z}$, Erdős made the following conjecture: *If $A = \{a_s(n_s)\}_{s=1}^k$ $(k > 1)$ is a system of residue classes with the moduli $n_1, \ldots, n_k$ distinct, then it cannot be a disjoint cover of $\mathbb{Z}$.*

Theorem 3.3. *Let $A = \{a_s(n_s)\}_{s=1}^k$.*

(i) (H. Davenport, L. Mirsky, D. Newman and R. Radó) *If A is a disjoint cover of $\mathbb{Z}$ with $1 < n_1 \leqslant n_2 \leqslant \cdots \leqslant n_{k-1} \leqslant n_k$, then we must have $n_{k-1} = n_k$.*

(ii) (Sun [48]) *Let n_0 be a positive period of the function $w_A(x) = |\{1 \leqslant s \leqslant k : x \in a_s(n_s)\}|$. For any positive integer d with $d \nmid n_0$ and $I(d) = \{1 \leqslant s \leqslant k : d \mid n_s\} \neq \emptyset$, we have*

$$|I(d)| \geqslant |\{a_s \bmod d : \ s \in I(d)\}| \geqslant \min_{\substack{0 \leqslant s \leqslant k \\ d \nmid n_s}} \frac{d}{\gcd(d, n_s)} \geqslant p(d),$$

where $p(d)$ is the least prime divisor of d.

Proof of Theorem 3.3(i). Without loss of generality we assume $0 \leqslant a_s < n_s$ $(1 \leqslant s \leqslant k)$. For $|z| < 1$ we have

$$\sum_{s=1}^{k} \frac{z^{a_s}}{1 - z^{n_s}} = \sum_{s=1}^{k} \sum_{q=0}^{\infty} z^{a_s + q n_s} = \sum_{n=0}^{\infty} z^n = \frac{1}{1-z}.$$

If $n_{k-1} < n_k$, then

$$\infty = \lim_{\substack{z \to e^{2\pi i/n_k} \\ |z|<1}} \frac{z^{a_k}}{1 - z^{n_k}} = \lim_{\substack{z \to e^{2\pi i/n_k} \\ |z|<1}} \left(\frac{1}{1-z} - \sum_{s=1}^{k-1} \frac{z^{a_s}}{1 - z^{n_s}} \right) < \infty,$$

which leads a contradiction! □

Theorem 3.3(ii) in the case $n_0 = 1$ and $d = n_k$ yields the Davenport-Mirsky-Newman-Radó result; a further extension was given by Z. W. Sun [60].

We mention that covers of $\mathbb{Z}$ by residue classes have many surprising applications. In 1964 R. L. Graham [21] used covers of $\mathbb{Z}$ to construct two positive integers $a, b \in \mathbb{Z}^+$ with $\gcd(a, b) = 1$ such that the Fibonacci-like sequence $\{w_n\}_{n\geqslant 0}$ defined by

$$w_0 = a,\ w_1 = b \text{ and } w_{n+1} = w_n + w_{n-1}\ (n = 1, 2, 3, \dots),$$

contains no primes. On the basis of Cohen and Selfridge's work, Z. W. Sun [53] employed covers of $\mathbb{Z}$ to show that if

$$x \equiv 47867742232066880047611079 \pmod{M}$$

then x is not of the form $\pm p^a \pm q^b$, where p, q are primes and a, b are nonnegative integers, and M is a 29-digit number given by

$$\begin{aligned}\prod_{p\leqslant 19} p \times 31 \times 37 \times 41 \times 61 \times 73 \times 97 \times 109 \times 151 \times 241 \times 257 \times 331\\ = 66483084961588510124010691590.\end{aligned}$$

Now we mention a recent result of Z. W. Sun [56, 64] which connects covers of $\mathbb{Z}$ with zero-sum problems.

Theorem 3.4 (Sun)**.** *Let G be an abelian group of prime power order.*

(i) *If $A = \{a_s(n_s)\}_{s=1}^k$ covers each integer either $2|G| - 1$ times or $2|G|$ times, then for any $c_1, \dots, c_k \in G$ there is an $I \subseteq \{1, \dots, k\}$ such that $\sum_{s\in I} c_s = 0$ and $\sum_{s\in I} 1/n_s = |G|$.*

(ii) *If $A = \{a_s(n_s)\}_{s=1}^k$ covers each integer exactly $3|G|$ times, then for any $c_1, \dots, c_k \in G \oplus G$ with $c_1 + \cdots + c_k = 0$ there exists an $I \subseteq \{1, \dots, k\}$ such that $\sum_{s\in I} c_s = 0$ and $\sum_{s\in I} 1/n_s = |G|$.*

Sun conjectured that the group G in Theorem 3.4 can be replaced by any finite abelian group, but this seems very challenging. It is interesting to view $1/n_s$ in Theorem 3.4 as a weight of $s \in \{1, \dots, k\}$. For more connections between covers of $\mathbb{Z}$ and unit fractions, the reader may consult [40, 51, 52, 55, 63].

Theorem 3.4 in the case $n_1 = \cdots = n_k = 1$ yields the following classical results in the theory of zero-sums.

Corollary 3.3. (i) (Erdős-Ginzburg-Ziv Theorem [14]) *Let $q \in \mathbb{Z}^+$ and $c_1, \dots, c_{2q-1} \in \mathbb{Z}_q$. Then $\sum_{s\in I} c_s = 0$ for some $I \subseteq \{1, \dots, k\}$ with $|I| = q$.*

(ii) (Alon-Dubiner Lemma [3]) *Let q be a prime power, and let $c_1, \dots, c_{3q} \in \mathbb{Z}_q \oplus \mathbb{Z}_q$ with $c_1 + \cdots + c_{3q} = 0$. Then $\sum_{s\in I} c_s = 0$ for some $I \subseteq \{1, \dots, k\}$ with $|I| = q$.*

The Erdős-Ginzburg-Ziv theorem [14] was discovered in 1961; since then it has stimulated lots of further researches on zero-sum sequences. The Alon-Dubiner lemma obtained in 1993, plays an indispensable role in C. Reiher's proof of the Kemnitz conjecture which states that if $c_1, \dots, c_{4n-3} \in \mathbb{Z}_n \oplus \mathbb{Z}_n$ then $\sum_{s\in I} c_s = 0$ for some $I \subseteq \{1, \dots, 4n-3\}$ with $|I| = n$ (cf. [42]).

Let $G_1, \cdots, G_k$ be subgroups of a group G, and let $a_1, \cdots, a_k \in G$. If the system $\mathcal{A} = \{a_i G_i\}_{i=1}^k$ of left cosets covers all the elements of G at least m times but none of its proper subsystems does, then all the indices $[G : G_i]$ are known to be finite.

Theorem 3.5. *Let $\mathcal{A} = \{a_i G_i\}_{i=1}^k$ be a finite system of left cosets in a group G where $G_1, \dots, G_k$ are subgroups of G. Suppose that $\mathcal{A}$ forms a minimal cover G (i.e. $\mathcal{A}$ covers all the elements of G but none of its proper systems does).*

(i) (B. H. Neumann [36, 37]) *There is a constant c_k depending only on k such that $[G : G_i] \leqslant c_k$ for all $i = 1, \dots, k$.*

(ii) (M. J. Tomkinson [70]) We have $[G : \bigcap_{i=1}^k G_i] \leqslant k!$ where the upper bound $k!$ is best possible.

Proof (Tomkinson). We prove (ii) by induction. (Part (ii) is stronger than part (i).)

We want to show that

$$\left[\bigcap_{i\in I} G_i : \bigcap_{i=1}^k G_i\right] \leqslant (k - |I|)! \qquad (*_I)$$

for all $I \subseteq \{1, \dots, k\}$, where $\bigcap_{i\in\emptyset} G_i$ is regarded as G.

Clearly $(*_I)$ holds for $I = \{1, \dots, k\}$.

Now let $I \subset \{1, \dots, k\}$ and assume $(*_J)$ for all $J \subseteq \{1, \dots, k\}$ with $|J| > |I|$. Since $\{a_i G_i\}_{i\in I}$ is not a cover of G, there is an $a \in G$ not covered by $\{a_i G_i\}_{i\in I}$. Clearly $a(\bigcap_{i\in I} G_i)$ is disjoint from the union $\bigcup_{i\in I} a_i G_i$ and hence contained in $\bigcup_{j\notin I} a_j G_j$. Thus

$$a\Big(\bigcap_{i\in I} G_i\Big) = \bigcup_{\substack{j\notin I \\ a_j G_j \cap a(\bigcap_{i\in I} G_i) \neq \emptyset}} \left(a_j G_j \cap a\Big(\bigcap_{i\in I} G_i\Big)\right)$$

and hence

$$\left[\bigcap_{i\in I} G_i : H\right] \leqslant \sum_{j\notin I}\left[G_j \cap \bigcap_{i\in I} G_i : H\right] \leqslant \sum_{j\notin I}(k-(|I|+1))! = (k-|I|)!$$

where $H = \bigcap_{i=1}^{k} G_i$. This concludes the induction proof. □

Definition 3.1. (i) The *Mycielski function* $f : \mathbb{Z}^+ \to \mathbb{N}$ is defined by

$$f(p_1^{a_1}\cdots p_r^{a_r}) = \sum_{i=1}^{r} a_i(p_i - 1),$$

where $a_1, \ldots, a_r$ are nonnegative integers and $p_1, \ldots, p_r$ are distinct primes.

(ii) Let H be a subnormal subgroup of a group G with finite index, and

$$H_0 = H \subset H_1 \subset \cdots \subset H_n = G$$

be a composition series from H to G (i.e. H_i is maximal normal in H_{i+1} for each $0 \leqslant i < n$). If the length n is zero (i.e. $H = G$), then we set $d(G, H) = 0$, otherwise we put

$$d(G, H) = \sum_{i=0}^{n-1}([H_{i+1} : H_i] - 1).$$

(By the Jordan–Hölder theorem, $d(G, H)$ does not depend on the choice of the composition series from H to G.)

For a subnormal subgroup H of a group G with $[G : H] < \infty$, it is known that (cf. Sun [47, 54])

$$[G : H] - 1 \geqslant d(G, H) \geqslant f([G : H]) \geqslant \log_2[G : H],$$

and $d(G, H) = f([G : H])$ if and only if G/H_G is solvable, where $H_G = \bigcap_{g\in G} gHg^{-1}$ is the largest normal subgroup of G contained in H.

Conjecture 3.2. (i) (J. Mycielski, 1966) *If $\{a_iG_i\}_{i=1}^{k}$ is a disjoint cover of an abelian group G, then $k \geqslant 1 + f([G : G_i])$ for all $i = 1, \ldots, k$.*

(ii) (Š. Znám, 1968) *If $A = \{a_s(n_s)\}_{s=1}^{k}$ is a disjoint cover of $\mathbb{Z}$ then*

$$k \geqslant 1 + f(N_A) \quad \textit{and hence } N_A \leqslant 2^{k-1},$$

where $N_A = \mathrm{lcm}[n_1, \ldots, n_k] = [\mathbb{Z} : \bigcap_{s=1}^{k} n_s\mathbb{Z}]$.

In 1974 I. Korec [32] confirmed Znám's conjecture and Mycielski's conjecture by proving the following deep result: *Let $\{a_iG_i\}_{i=1}^{k}$*

be a partition of a group into left cosets of normal subgroups. Then $k \geqslant 1 + f([G : \bigcap_{i=1}^{k} G_i])$. On the other hand, in 1988 M. A. Berger, A. Felzenbaum and A. S. Fraenkel [7] obtained the following result by geometric method: *If* $\{a_iG_i\}_{i=1}^{k}$ *is a disjoint cover of a finite solvable group* G *by left cosets, then* $k \geqslant 1 + f([G : G_i])$ *for every* $i = 1, \cdots, k$.

Here are some further results in this direction. (Recall that a subgroup H of a group G is called a Hall subgroup if $|H|$ is relatively prime to $[G : H]$.)

Theorem 3.6. *Let* $\{a_iG_i\}_{i=1}^{k}$ *be a finite system of left cosets in a group* G *that forms a minimal* m*-cover of* G *(i.e., it cover each elements of* G *at least* m *times but none of its proper systems does).*

(i) (Sun [47]) *We have* $[G : \bigcap_{i=1}^{k} G_i] \leqslant k!$.

(ii) (Sun [54]) *Suppose that* $\{a_iG_i\}_{i=1}^{k}$ *cover each elements of* G *exactly* m *times. If* $G_1, \ldots, G_k$ *are subnormal in* G*, then*

$$k \geqslant m + d\left(G, \bigcap_{i=1}^{k} G_i\right)$$

(*and hence* $[G : \bigcap_{i=1}^{k} G_i] \leqslant 2^{k-m}$), *where the lower bound can be attained; moreover, for any subgroup* K *of* G *not contained in all the* G_i *we have*

$$|\{1 \leqslant i \leqslant k : K \not\subseteq G_i\}| \geqslant 1 + d\left(K, K \cap \bigcap_{i=1}^{k} G_i\right).$$

For those $i = 1, \ldots, k$ *with* $G/(G_i)_G$ *solvable we have the inequality* $k \geqslant m + f([G : G_i])$.

(iii) (Sun [62]) *If* G *is cyclic or* $G_1, \ldots, G_k$ *are normal Hall subgroups of* G*, then*

$$k \geqslant m + d\left(G, \bigcap_{i=1}^{k} G_i\right).$$

(iv) (G. Lettl & Sun [33]) *If* G *is abelian, then we have* $k \geqslant m + f([G : G_i])$ *for all* $i = 1, \ldots, k$.

Proofs of Theorem 3.6(i)-(iii) involve a sophisticated use of induction argument. Part (iii) in the case $G = \mathbb{Z}$ and $m = 1$, was first conjectured by Š. Znám in 1975 and proved by R. J. Simpson [45] in 1985. Part (iv) was obtained via characters of abelian groups and algebraic number theory; below is a key lemma used for the proof.

Lemma 3.1 (Lettl & Sun, 2004)**.** *Let $n > 1$ be an integer. Then $f(n)$ is the smallest positive integer k such that there are roots of unity $\zeta_1, \ldots, \zeta_k$ different from 1 for which $\prod_{s=1}^{k}(1-\zeta_s) \equiv 0 \pmod{n}$ in the ring of algebraic integers.*

Corollary 3.4 (Sun [47])**.** *Let H be a subnormal subgroup of a group G with $[G:H] < \infty$. Then*

$$[G:H] \geqslant 1 + d(G, H_G) \geqslant 1 + f([G:H_G])$$

and hence

$$|G/H_G| \leqslant 2^{[G:H]-1}.$$

Proof. Let $\{Ha_i\}_{i=1}^{k}$ be a right coset decomposition of G where $k = [G:H]$. Then $\{a_iG_i\}_{i=1}^{k}$ is a disjoint cover of G where all the $G_i = a_i^{-1}Ha_i$ are subnormal in G. Observe that

$$\bigcap_{i=1}^{k} G_i = \bigcap_{i=1}^{k} \bigcap_{h \in H} a_i^{-1}h^{-1}Hha_i = \bigcap_{g \in G} g^{-1}Hg = H_G.$$

So the desired result follows from Theorem 3.6. □

The following conjecture extends a conjecture of P. Erdős on covers of $\mathbb{Z}$.

Conjecture 3.3 (M. Herzog & J. Schönheim [26])**.** *Let $\{a_iG_i\}_{i=1}^{k}$ $(k > 1)$ be a partition of a group G into left cosets of subgroups $G_1, \ldots, G_k$. Then the indices $n_1 = [G:G_1], \ldots, n_k = [G:G_k]$ cannot be distinct.*

By using the structure of finite nilpotent groups and lattice parallelotopes, Berger, Felzenbaum and Fraenkel [6] confirmed Conjecture 3.3 for finite nilpotent groups. Below is the latest progress due to Sun [58].

Theorem 3.7 (Sun)**.** *Let G be a group, and $\mathcal{A} = \{a_iG_i\}_{i=1}^{k}$ $(k > 1)$ be a system of left cosets of subnormal subgroups. Suppose that $\mathcal{A}$ covers each $x \in G$ the same number of times, and*

$$n_1 = [G:G_1] \leqslant \cdots \leqslant n_k = [G:G_k].$$

Then the indices $n_1, \ldots, n_k$ cannot be distinct. Moreover, if each index occurs in $n_1, \ldots, n_k$ at most M times, then

$$\log n_1 \leqslant \frac{e^{\gamma}}{\log 2} M \log^2 M + O(M \log M \log\log M)$$

where $\gamma = 0.577\ldots$ is the Euler constant and the O-constant is absolute.

The above theorem also answers a question analogous to a famous problem of Erdős negatively. Theorem 3.7 was established by a combined use of tools from combinatorics, group theory and number theory.

One of the key lemmas is the following one which is the main reason why covers involving subnormal subgroups are better behaved than general covers.

Lemma 3.2. *Let G be a group, and let $P(n)$ denote the set of prime divisors of a positive integer n.*

(i) (Sun [54]) *If $G_1,\ldots,G_k$ are subnormal subgroups of G with finite index, then*

$$\Big[G:\bigcap_{i=1}^k G_i\Big]\ \Big|\ \prod_{i=1}^k [G:G_i] \text{ and hence } P\bigg(\Big[G:\bigcap_{i=1}^k G_i\Big]\bigg)=\bigcup_{i=1}^k P([G:G_i]).$$

(ii) (Sun [58]) *Let H be a subnormal subgroup of G with finite index. Then*

$$P(|G/H_G|)=P([G:H]).$$

We mention that part (ii) is a consequence of the first part, and the word "subnormal" cannot be removed from either part.

Here is another useful lemma of combinatorial nature.

Lemma 3.3 (Sun [58]). *Let G be a group and H its subgroup with finite index N. Let $a_1,\ldots,a_k\in G$, and let $G_1,\ldots,G_k$ be subnormal subgroups of G containing H. Then $\bigcup_{i=1}^k a_iG_i$ contains at least $|\bigcup_{i=1} 0(n_i)\cap\{0,1,\ldots,N-1\}|$ left cosets of H, where $n_i=[G:G_i]$.*

This lemma implies the following result (cf. Sun [62, Corollary 1.2]): *If $G_1,\ldots,G_k$ are normal Hall subgroups of a finite group G, then we have $|\bigcup_{i=1}^k a_iG_i|\geqslant|\bigcup_{i=1}^k G_i|$.*

The third lemma needed to prove Theorem 3.7 is well-known in analytic number theory.

Lemma 3.4. (i) (The Prime Number Theorem) *For $x\geqslant 2$ we have*

$$\pi(x)=\frac{x}{\log x}+O\left(\frac{x}{\log^2 x}\right),$$

where $\pi(x)=\sum_{p\leqslant x}1$ is the number of primes not exceeding x.

(ii) (Mertens' Theorem) *For $x\geqslant 2$ we have*

$$\prod_{p\leqslant x}\left(1-\frac{1}{p}\right)=\frac{e^{-\gamma}}{\log x}+O\left(\frac{1}{\log^2 x}\right).$$

Let us conclude this section with a challenging conjecture appeared in Sun [62, Conjecture 1.2].

Conjecture 3.4 (Sun, 2004). *Let G be a group, and $a_1G_1, \ldots, a_kG_k$ $(k > 1)$ be pairwise disjoint left cosets of G with all the indices $[G : G_i]$ finite. Then, for some $1 \leqslant i < j \leqslant k$ we have* $\gcd([G : G_i], [G : G_j]) \geqslant k$.

Sun [62] noted that this conjecture holds for p-groups as well as the special case $k = 2$. In 2007, Wan-Jie Zhu [71], a student at Nanjing University, proved Conjecture 3.4 for $k = 3, 4$ via several sophisticated lemmas. K. O'Bryant [38] confirmed the conjecture for $G = \mathbb{Z}$ in the case $k \leqslant 20$.

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 & M. Dubiner, Zero-sum sets of precribed size, in: *Combinatorics, Panul Erdős is Eighty*, János Bolyai Math. Soc., Budapest, 1993, 33–50.
4. N. Alon, M. B. Nathanson & I. Z. Ruzsa, The polynomial method and restricted sums of congruence classes, *J. Number Theory* 56 (1996), 404–417.
5. N. Alon & M. Tarsi, A nowhere-zero point in linear mappings, *Combinatorica* 9 (1989), 393–395.
6. M. A. Berger, A. Felzenbaum, A. S. Fraenkel, The Herzog-Schönheim conjecture for finite nilpotent groups, *Canad. Math. Bull.* 29 (1986), 329–333.
7. M. A. Berger, A. Felzenbaum, A. S. Fraenkel, Mycielski-Sierpiński conjecture and Korec-Znám result, *Colloq. Math.* 56 (1988), 241–249.
8. J. Bourgain, N. Katz & T. Tao, A sum product estimate in finite fields and applications, *GAFA* 14 (2004), 27–57.
9. J. Bourgain & S. Konyagin, Estimates for the number of sums and products and for exponential sums over subgroups in fields of prime order, *C.R. Acad. Sci. Paris* 337 (2003), 75–80.
10. R. B. Crittenden & C. L. Vanden Eynden, A proof of a conjecture of Erdős, *Bull. Amer. Math. Soc.* 75 (1969), 1326–1329.
11. R. B. Crittenden & C. L. Vanden Eynden, Any n arithmetic progressions covering the first 2^n integers cover all integers, *Proc. Amer. Math. Soc.* 24 (1970), 475–481.
12. S. Dasgupta, G. Károlyi, O. Serra & B. Szegedy, Transversals of additive Latin squares, *Israel J. Math.* 126 (2001), 17–28.

13. J. A. Dias da Silva & Y. O. Hamidoune, Cyclic spaces for Grassmann derivatives and additive theory, *Bull. London Math. Soc.* 26 (1994), 140–146.

14. P. Erdős, A. Ginzburg & A. Ziv, Theorem in the additive number theory, *Bull. Res. Council Israel* 10F (1961), 41–43.

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

16. P. Erdős & E. Szemerédi, On sums and products of integers, in: *Studies in Pure Mathematics: To the memory of Paul Turán* (eds., P. Erdős, L. Alpar and G. Halasz), Akademiai Kiado-Birkhauser, Budapest, 1983, pp. 213–218.

17. P. Erdős and P. Turán, On some sequences of integers, *J. London Math. Soc.* 11 (1936), 261–264.

18. M. Filaseta, K. Ford, S. Konyagin, C. Pomerance and G. Yu, Sieving by large integers and covering systems of congruences, *J. Amer. Math. Soc.* 20 (2007), 495–517.

19. G. A. Freiman, *Foundations of a Structural Theory of Set Addition*, Kazan Gos. Ped. Inst., Kazan, 1966.

20. T. Gowers, A new proof of Szemerédi's theorem, *GAFA* 11 (2001), 465–588.

21. R. L. Graham, A Fibonacci-like sequence of composite numbers, Math. Mag. 37 (1964), 322–324.

22. B. Green and I. Z. Ruzsa, Freiman's theorem in an arbitrary abelian group, *J. London Math. Soc.* 75 (2007), 163–175.

23. B. Green and T. Tao, The primes contain arbitrarily long arithmetic progressions, *Ann. of Math.*, to appear.

24. R. K. Guy, *Unsolved Problems in Number Theory*, 3rd ed. Springer, New York, 2004.

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

26. M. Herzog & J. Schönheim, Research problem No. 9, *Canad. Math. Bull.* 17 (1974), 150.

27. Q. H. Hou & Z. W. Sun, Restricted sums in a field, *Acta Arith.* 102 (2002), 239–249.

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

29. N. H. Katz & C. Y. Shen, A slight improvement to Garaev's sum product estimate, *preprint*, 2007, `arXiv:math/0703614`.

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

31. M. Kneser, Abschätzungen der asymptotischen Dichte von Summenmengen, *Math. Z.* 58 (1953), 459–484.

32. I. Korec, On a generalization of Mycielski's and Znám's conjectures about coset decomposition of Abelian groups, *Fund. Math.* **85** (1974), 41–47.

33. G. Lettl & Z. W. Sun, On overs of abelian groups by cosets, *Acta Arith.*, in press. `http://arxiv.org/abs/math.GR/04111144`.

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

35. H. B. Mann, A proof of the fundamental theorem on the density of sums of sets of positive integers, *Ann. of Math.* 43 (1942), 523–527.

36. B. H. Neumann, Groups covered by permutable subsets, *J. London Math. Soc.* 29 (1954), 236–248.

37. B. H. Neumann, Groups covered by finitely many cosets, *Publ. Math. Debrecen* 3 (1954), 227–242.

38. K. O'Bryant, On Z.-W. Sun's disjoint congruence classes conjecture, in: *Combinatorial Number Theory* (eds., B.M. Landman, M.B. Nathanson, J. Nesetril, R.J. Nowakowski and C. Pomerance), Walter de Gruyter, 2007, pp. 403-412.

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

40. H. Pan & Z. W. Sun, A sharp result on m-covers, *Proc. Amer. Math. Soc.* 135 (2007), 3515–3520.

41. H. Pan & Z. W. Sun, A new extension of the Erdős-Heilbronn conjecture, *preprint*, 2007.

42. C. Reiher, On Kemnitz' conjecture concerning lattice-points in the plane, *Ramanujan J.* 13 (2007), 333–337.

43. H. J. Ryser, Neuere Probleme der Kombinatorik, in: *"Vorträge über Kombinatorik",* Oberwolfach, 1967; Math. Forschungsinstitut, Oberwolfach, 1968, pp. 69–91.

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

45. R. J. Simpson, Regular coverings of the integers by arithmetic progressions, *Acta Arith.* 45 (1985), 145–152.

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

47. Z. W. Sun, Finite coverings of groups, *Fund. Math.* 134 (1990), 37–53.

48. Z. W. Sun, An improvement to the Znám-Newman result, *Chinese Quart. J. Math.* 6(3)(1991), 90–96.

49. Z. W. Sun, Covering the integers by arithmetic sequences, *Acta Arith.* 72 (1995), 109–129.

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

51. Z. W. Sun, Exact m-covers and the linear form $\sum_{s=1}^{k} x_s/n_s$, *Acta Arith.* 81 (1997), 175–198.

52. Z. W. Sun, On covering multiplicity, *Proc. Amer. Math. Soc.* 127 (1999), 1293–1300.

53. Z. W. Sun, On integers not of the form $\pm p^a \pm q^b$, *Proc. Amer. Math. Soc.* 128 (2000), 997–1002.

54. Z. W. Sun, Exact m-covers of groups by cosets, *European J. Combin.* 22 (2001), 415–429.

55. 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.

56. 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.

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

58. Z. W. Sun, On the Herzog-Schönheim conjecture for uniform covers of groups, *J. Algebra* 273 (2004), 153–175.

59. Z. W. Sun, Arithmetic properties of periodic maps, *Math. Res. Lett.* 2004, 187–196.

60. Z. W. Sun, On the range of a covering function, *J. Number Theory* 111 (2005), 190–196.

61. Z. W. Sun, A local-global theorem on periodic maps, *J. Algebra* 293 (2005), 506–512.

62. Z. W. Sun, Finite covers of groups by cosets or subgroups, *Internat. J. Math.* 17 (2006), 1047–1064.

63. Z. W. Sun, A connection between covers of the integers and unit fractions, *Adv. in Appl. Math.* 38 (2007), 267–274.

64. Z. W. Sun, Zero-sum problems in abelian p-groups and covers of the integers by residue classes, *Israel J. Math.*, to appear.

65. Z. W. Sun, On value sets of polynomials over a field, *Finite Fields Appl.*, in press.

66. Z. W. Sun, An additive theorem and restricted sumsets, submitted. `http://arxiv.org/abs/math.CO/0610981`.

67. Z. W. Sun & Y. N. Yeh, On various restricted sumsets, *J. Number Theory* 114 (2005), 209–220.

68. E. Szemerédi, On sets of integers containing no k elements in arithmetic progression, *Acta Arith.* 27 (1975), 199–245.

69. T. Tao and V. H. Vu, *Additive Combinatorics*, Cambridge Univ. Press, Cambridge, 2006.
70. M. J. Tomkinson, Groups covered by finitely many cosets or subgroups, *Comm. in Algebra* 15 (1987), 845–859.
71. W. J. Zhu, On Sun's conjecture concerning disjoint cosets, *Int. J. Mod. Math.* 3 (2008), to appear.

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. H. Vu (2006)