Invited talk given at the 4th ICCM (Hangzhou, Dec. 21, 2007)

GROUPS IN COMBINATORIAL NUMBER THEORY

Zhi-Wei Sun

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

1. Sumsets in additive combinatorics

Shnirel'man's Theorem (Shnirel'man, 1933). *If* $0 \in A \subseteq \mathbb{N} = \{0, 1, 2, \ldots\}$ *and*

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

then there is $n \in \mathbb{Z}^+$ *such that*

$$nA = A + \cdots + A = \mathbb{N}.$$

It follows that there is a constant $k \in \mathbb{Z}^+$ *such that each integer greater than one can be written as a sum of at most* k *primes.*

Mann's Theorem (Mann [Ann. of Math., 1942]). *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* $\{a + b : \ a \in A, \ b \in B\}$.

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

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

i.e.,

$$\delta(A+B)\geqslant \min\left\{1,\delta(A)+\delta(B)-\delta(\{0\})\right\},$$

where $\delta(S)=|S|/|\mathbb{Z}_p|$ for any $S\subseteq\mathbb{Z}_p$.

Szemeredi's Theorem (Conjectured by Erdős and Turán in 1936)**.** *If $A\subseteq\mathbb{N}$ has positive upper (asymptotic) density, i.e.,*

$$\bar{d}(A)=\limsup_{n\to\infty}\frac{|\{a\in A:\ 1\leqslant a\leqslant n\}|}{n}>0,$$

then A contains an AP (arithmetic progression) of any given length.

In a long paper published in 2001, W. T. Gowers employed harmonic analysis and the following deep theorem of G. Freiman to obtain a quantitative proof of Szemeredi's theorem; this is the main reason why Gowers won the Fields Medal in 1998.

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 depend only on c.

Szemerédi's theorem plays an important role in the proof of the following celebrated result which was also conjectured by Erdős and Turán in 1936.

Green-Tao Theorem. *There are arbitrarily long APs of primes.*

In 2003 E. S. Croot [Ann. of Math.] used the sieve method to confirm the following long-standing conjecture.

Erdős-Graham Conjecture proved by E. Croot. *If* $\{2,3,\dots\}$ *is partitioned into finitely many subsets, then one of the subsets contains finitely many distinct integers* $x_1,\dots,x_m$ *satisfying* $\sum_{k=1}^m 1/x_k = 1$.

A Conjecture (Z. W. Sun, 2007)**.** *If* $A \subseteq \{2,3,\dots\}$ *has positive upper (asymptotic) density, then there are finitely many distinct elements* $a_1 < \cdots < a_m$ *of* A *with* $\sum_{k=1}^m 1/a_k = 1$.

The set $\{3,5,7,\dots\}$ has asymptotic density $1/2$, and it is known that

$$\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{9}+\frac{1}{11}+\frac{1}{33}+\frac{1}{35}+\frac{1}{45}+\frac{1}{55}+\frac{1}{77}+\frac{1}{105}=1.$$

Erdős-Szemerédi Conjecture. *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*

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

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

Bourgain-Katz-Tao Theorem. *Let* p *be a prime and let* $\emptyset \neq A \subseteq \mathbb{Z}_p$. *If* $|A| < p^{1-\delta}$ *with* $\delta > 0$, *then there are* $c(\delta) > 0$ *and* $\varepsilon(\delta) > 0$ *such that*

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

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 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. *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

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

In 2005, G. Károlyi proved that the corollary remains valid if G is just a finite group (which may not be abelian).

Erdős-Heilbronn Conjecture (1964)**.** *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.

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.

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

The following conjecture was originally motivated by graph theory.

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 $f(a_1, \ldots, a_n) \neq 0$.*

The method using the Combinatorial Nullstellensatz is also called the polynomial method.

Alon-Nathanson-Ruzsa Theorem [J. Number Theory 56(1996)]. *Let $A_1,\ldots,A_n$ be finite nonempty subsets of a field F with $|A_1|<\cdots<|A_n|$. Then, for the restricted sumset*

$$A_1\dot{+}\cdots\dot{+}A_n=\{a_1+\cdots+a_n:\ a_1\in A,\ldots,a_n\in A_n,\ \text{and}\ a_i\neq a_j\ \text{if}\ i\neq j\},$$

we have

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

The Dias da Silva–Hamidoune Theorem follows from the ANR Theorem 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 generalized the Erdős-Heilbronn conjecture in another direction.

A Result of Q. H. Hou and Z. W. Sun (Acta Arith., 2002). *Let $k,m\in\mathbb{N}$ and $n\in\mathbb{Z}^+$. 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 the Hou-Sun result is to show that if $k,m,n\in$

$\mathbb{N}$, $n \geqslant 2$ and $k > m(n-1)$ then

$$[x_1^{k-1} \cdots x_n^{k-1}](x_1 + \cdots + x_n)^{((k-1-m(n-1))n} \prod_{1 \leqslant i < j \leqslant n} (x_j - x_i)^{2m}$$

$$= (-1)^{(m-1)n(n-1)/2} \frac{(((k-1-m(n-1))n)!}{n!(m!)^n} \prod_{j=1}^{n} \frac{(jm)!}{(k-1-(j-1)m)!}.$$

This is very sophisticated!

Recently P. Balister and J. P. Wheeler extended the Erdős -Heilbronn conjecture to any finite group via several ingenious steps.

A Result of Balister and Wheeler (Acta Arith., to appear)**.** *Let G be any finite group written additively. Then, for any nonempty subsets A and B, we have*

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

One of the needed lemmas is the following famous result.

Feit-Thompson Theorem (1963)**.** *Every group of odd order is solvable.*

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

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

where

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

In particular, $|A \dot{+} B| \geqslant |A| + |B| - 1$ 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 applied the Combinatorial Nullstellensatz in a new way to make the following progress on Lev's conjecture.

A Result of H. Pan and Z. W. Sun (Israel J. Math., 2006)**.** *Let G be an abelian group, and let A, B, S be finite non-empty subsets of G with*

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

(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 [Finite Fields Appl.] extended the Cauchy-Davenport theorem in a new direction, and Pan and Sun generalized the Erdős-Heilbronn conjecture in the same spirit.

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

$$f(x_1, \ldots, x_n) = c_1 x_1^k + \cdots + c_n x_n^k + g(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$$

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

(i) (Sun [Finite Fields Appl.]) *We have*

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

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

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

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

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

(ii) (Pan & Sun, 2007) *In the case $c_1 = \cdots = c_n$, we have*

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

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. On Snevily's conjecture and related results

Snevily's Conjecture (1999)**.** *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.*

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 $A = B = \{0, g\}$.

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

Another Version of 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.*

A Result of Dasgupta, Károlyi, Serra and Szegedy. *Snevily's conjecture holds for any cyclic group of odd order.*

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 [Israel J. Math. 2001] 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*

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

This can be easily shown via Vandermonde determinants.

By using the Combinatorial Nullstellensatz and some knowledge from algebraic number theory, Z. W. Sun [J. Combin. Theory Ser. A 2003] made a further extension of the Dasgupta-Károlyi-Serra-Szegedy result via restricted sumsets in fields.

A Result of Z. W. Sun (`arXiv:math.CO/0610981`)**.** *Let G be any abelian group with $\mathrm{Tor}(G)$ cyclic, and let A, B and C be subsets of G with cardinality n. There there is a numbering $\{a_i\}_{i=1}^n$ of the elements of*

A, a numbering $\{b_i\}_{i=1}^n$ of the elements of B, and a numbering $\{c_i\}_{i=1}^n$ of the elements of C such that $a_1+b_1+c_1,\ldots,a_n+b_n+c_n$ are distinct.

We cannot replace the group G in the result even by the Klein quaternion group

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

Corollary (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.*

In 1967 H. J. Ryser conjectured that every Latin square of odd order has a Latin transversal. Here is a similar conjecture motivated by the above corollary.

A Conjecture of Z. W. Sun. *Every $n\times n\times n$ Latin cube contains a Latin transversal.*

3. Covers of $\mathbb{Z}$ and two local-global theorems

For $a\in\mathbb{Z}$ and $n\in\mathbb{Z}^+$ we let

$$a(n)=a+n\mathbb{Z}=\{a+nq:\ q\in\mathbb{Z}\}=\{x\in\mathbb{Z}:\ x\equiv a\ (\mathrm{mod}\ n)\}.$$

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

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

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.

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

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

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

A Conjecture of 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 [Bull. AMS, Proc. AMS] 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.

The First Local-Global Theorem (Z. W. Sun [Trans. Amer. Math. Soc. 1996])**.** *Let $A=\{a_s(n_s)\}_{s=1}^k$ be a finite system of residue classes. 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

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

The Second Local-Global Theorem (Z. W. Sun [J. Algebra, 2005])**.** *Let $\psi_1,\ldots,\psi_k$ be maps from $\mathbb{Z}$ to an abelian group G with periods $n_1,\ldots,n_k\in\mathbb{Z}^+$ respectively. Set*

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

Then $\psi=\psi_1+\cdots+\psi_k$ 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 (Z. W. Sun, 2004)**.** *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 the Second Local-Global Theorem, 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 $x\in\mathbb{Z}$. □

We mention that covers of $\mathbb{Z}$ by residue classes have many surprising applications. In 1964 R. L. Graham 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

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

contains no primes. On the basis of Cohen and Selfridge's work, the author [Proc. AMS, 2000] employed covers of $\mathbb{Z}$ to show that if

$$x\equiv 47867742232066880047611079 \pmod{6648308496158851012401069 1590}$$

then x is not of the form $\pm p^a\pm q^b$, where p,q are primes and $a,b\in\mathbb{N}$.

Now we mention a recent result of the author which connects covers of $\mathbb{Z}$ with zero-sum problems in a surprising way.

A Result of Z. W. Sun ([Israel J. Math.]). *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 $c_1,\ldots,c_k\in G$ there is an $I\subseteq\{1,\ldots,k\}$ 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 $c_1,\ldots,c_k\in G\oplus G$ with $c_1+\cdots+c_k=0$ there exists an $I\subseteq\{1,\ldots,k\}$ such that $\sum_{s\in I}c_s=0$ and $\sum_{s\in I}1/n_s=|G|$.*

It is interesting to view $1/n_s$ in the above result as a weight of $s\in\{1,\ldots,k\}$. The above result in the case $n_1=\cdots=n_k=1$ yields the following classical results in the theory of zero-sums.

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

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

The Erdős-Ginzburg-Ziv theorem 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 $c_1, \ldots, c_{4n-3} \in \mathbb{Z}_n \oplus \mathbb{Z}_n$ then $\sum_{s\in I} c_s = 0$ for some $I \subseteq \{1, \ldots, 4n-3\}$ with $|I| = n$.

4. On covers of groups and the Herzog-Schönheim conjecture

Let H be a subgroup of a group G with $[G : H] = k < \infty$. Then we can partition G into k left cosets $g_1H, \ldots, g_kH$, and $\{g_iH\}_{i=1}^k$ forms a disjoint cover of G by left cosets. Let $\{Ha_i\}_{i=1}^k$ be a right coset decomposition of G. Then $\{a_iG_i\}_{i=1}^k$ is a disjoint cover of G where $G_i = a_i^{-1}Ha_i$. Observe that

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

is the normal core H_G of H in G (H_G denotes the largest normal subgroup of G contained in H).

A Basic Theorem on Covers of Groups. *Let $\mathcal{A} = \{a_iG_i\}_{i=1}^k$ be a finite system of left cosets in a group G where $G_1, \ldots, G_k$ 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, 1954) *There is a constant c_k depending only on k such that $[G : G_i] \leqslant c_k$ for all $i = 1, \ldots, k$.*

(ii) (M. J. Tomkinson, 1987) We have $[G : \bigcap_{i=1}^k G_i] \leqslant k!$ where the upper bound $k!$ is best possible.

Two Functions. (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 [Fund. Math., 1990; European J. Combin. 2001])

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

and $d(G,H)=f([G:H])$ if and only if G/H_G is solvable.

Mycielski's Conjecture. (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* $i=1,\ldots,k$.

Related Results on Exact m-covers. *Let G be a group, and let $a_1G_1, \ldots, a_kG_k$ be left cosets of subgroups $G_1, \ldots, G_k$ of G. Suppose that $\{a_iG_i\}_{i=1}^k$ covers each element of G exactly m times.*

(i) (I. Korec [Fund. Math., 1974]) *If $m = 1$ and $G_1, \ldots, G_k$ are normal in G, then $k \geqslant 1 + f([G : \bigcap_{i=1}^k G_i])$.*

(ii) (Z. W. Sun [European J. Combin., 2001]) *If $G_1, \ldots, G_k$ are subnormal in G, then $k \geqslant m + d(G, \bigcap_{i=1}^k G_i)$.*

Corollary (Sun [Fund. Math., 1990])**.** *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 and $\bigcap_{i=1}^k G_i = H_G$. So the desired result follows. □

Mycielski-type Results on Minimal m-covers. *Let G be a group, and let $a_1G_1, \ldots, a_kG_k$ be left cosets of subgroups $G_1, \ldots, G_k$ of G. Suppose that $\{a_iG_i\}_{i=1}^k$ covers each element of G at least m times but none of its proper systems does.*

(i) (R. J. Simpson [Acta Arith., 1985]) *If $m = 1$ and $G = \mathbb{Z}$, then $k \geqslant 1 + f([G : \bigcap_{i=1}^k G_i])$.*

(ii) (Z. W. Sun [Internat. J. Math., 2006]) *If G is cyclic or $G_1,\ldots,G_k$ are normal Hall subgroups of G, then $k\geqslant m+d(G,\bigcap_{i=1}^k G_i)$.*

(iii) (G. Lettl & Z. W. Sun [Acta Arith., to appear]) *If G is abelian, then we have $k\geqslant m+f([G:G_i])$ for all $i=1,\ldots,k$.*

We mention that the proof of the Lettl-Sun result was obtained via characters of abelian groups and algebraic number theory; below is a key lemma used for the proof.

A Lemma of Lettl and Sun ([Acta Arith., to appear])**.** *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.*

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 $\mathbb{Z}$.*

A Result of H. Davenport, L. Mirsky, D. Newman and R. Rado. *If $A=\{a_s(n_s)\}_{s=1}^k$ 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 $n_{k-1}=n_k$.*

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

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

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! □

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

Herzog-Schönheim Conjecture (1974). *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.*

It is known that any finite nilpotent group is the direct product of its Sylow subgroups. Using this fact and lattice parallelotopes, Berger, Felzenbaum and Fraenkel [Canad. Bull. Math. 1986] confirmed the above conjecture for finite nilpotent groups.

A Result of Z. W. Sun [J. Algebra 273(2004)]**.** *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; it 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.

A Lemma on Indices of Subnormal Subgroups (Z. W. Sun)**.** *Let G be a group, and let $P(n)$ denote the set of prime divisors of a positive integer n.*

(i) [European J. Combin. 2001] *If $G_1,\ldots,G_k$ are subnormal subgroups of G with finite index, then*

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

(ii) [J. Algebra, 2004] *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.

A Lemma on Unions of Cosets (Z. W. Sun [J. Algebra, 2004])**.** *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 of Z. W. Sun [Internat. J. Math. 2006]: *If $G_1,\ldots,G_k$ are normal Hall subgroups of a finite group G, then*

$$\left|\bigcup_{i=1}^k a_iG_i\right|\geqslant\left|\bigcup_{i=1}^k G_i\right|.$$

We also need the following deep theorems in analytic number theory.

The Prime Number Theorem with Error Terms. *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.

Mertens' Theorem. *For $x\geqslant 2$ we have*

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

Finally we mention a challenging conjecture arising from my study of Huhn-Megyesi problems and covers of groups.

A Conjecture on Disjoint Cosets (Z. W. Sun, [Internat. J. Math., 2006])**.** *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* $\gcd([G:G_i],[G:G_j])\geqslant k$.

Z. W. Sun [Internat. J. Math. 2006] noted that this conjecture holds for p-groups as well as the special case $k = 2$. In 2007, W.-J. Zhu, a student at Nanjing University, proved the conjecture for $k = 3, 4$ via several sophisticated lemmas. K. O'Bryant [Integers 2007] confirmed the conjecture for $G = \mathbb{Z}$ in the case $k \leqslant 20$.