A talk given at the 2007 Annual Conf. of the Chin. Math. Soc. (Beijing, Nov. 3)

SOME FAMOUS PROBLEMS AND RELATED RESULTS 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. Erdős-Turán Conjectures, Szemerédi's theorem and the Green-Tao theorem

Pigeon-hole Principle (Dirichlet's Principle). *If we put at least* $n+1$ *objects into* n *drawers where* $n \in \mathbb{Z}^+ = \{1, 2, \ldots\}$, *then some drawer contains at least two objects.*

Note that a distribution of all elements of a set A into n drawers corresponds to an ordered partition $A = A_1 \cup \cdots \cup A_n$ with $A_1, \ldots, A_n$ pairwise disjoint. We may also call such a partition an n-coloring of A with elements in A_i colored in the ith color.

A vast generalization of the pigeon-hole principle was obtained by F. P. Ramsey in 1930 in his paper "*On a problem of formal logic*" in which he aimed to prove a logical result which is actually impossible by an undecidable result of Gödel. Ramsey's theorem plays a central role in the famous Ramsey theory.

Ramsey's Theorem (Ramsey, 1930). *Let $q_1,\ldots,q_n\geqslant r\geqslant 1$ be integers. If S is a set with $|S|$ large enough and we arbitrarily distribute all r-subsets of S into n ordered drawers, then for some $1\leqslant i\leqslant n$ the set S has a q_i-subset whose all r-subsets lie in the ith drawer.*

Here is a classical theorem in Ramsey theory which is a consequence of Ramsey's theorem.

Schur's Theorem (Schur, 1916). *If we distribute $1,\ldots,\lfloor n!e\rfloor$ into n drawers, then some drawer contains certain x,y,z with $x+y=z$.*

In 1927 van der Waerden established the following result conjectured by Schur; this contribution made him famous as a young mathematician.

van der Waerden Theorem. *For any positive integers k and m, if n is sufficiently large and we distribute $1,\ldots,n$ into m drawers, then some drawer contains an AP (arithmetic progression) of length k.*

In 1933 R. Rado, one of Schur's students, proved a theorem which includes both Schur's theorem and van der Waerden's theorem as special cases.

For $a_1,\ldots,a_m\in\mathbb{Z}^+$ with $m\geqslant 2$, we define the two-color Rado number $R(a_1,\ldots,a_m)$ to be the least positive integer n such that whenever we distribute $1,\ldots,n$ into two drawers we can find $x_0,\ldots,x_m$ in the same drawer satisfying the equation $a_1x_1+\cdots+a_mx_m=x_0$. In 2005 S. Guo and Z. W. Sun [J. Combin. Theory Ser. A, in press] proved that the exact value of $R(a_1,\ldots,a_m)$ is av^2+v-a, where

$$a=\min\{a_1,\ldots,a_m\}\ \text{ and }\ v=a_1+\cdots+a_m.$$

This confirms a conjecture of B. Hopkins and D. Schaal.

In 1963 Hales and Jewett established a Ramsey-type result which stripes the van der Waerden theorem of its unessential elements and reveals the heart of Ramsey Theory. To avoid too technical definitions, here we don't state the Hales-Jewett theorem.

For a set $A \subseteq \mathbb{Z}^+$ we define its upper (asymptotic) density by

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

Note that if we distribute $1, \ldots, n$ into m drawers then some drawer contains at least δn elements where $\delta = 1/m$. Thus the following deep conjecture is stronger than the van der Waerden theorem.

A Conjecture of P. Erdős and Turán (1936). *If A is a subset of $\mathbb{Z}^+$ with positive upper density, then A contains an arbitrarily long AP.*

In 1956 K. Roth proved this result for $k = 3$ by the circle method in analytic number theory. In 1969 E. Szemerédi handled the case $k = 4$ by a combinatorial method. The case of general k was settled by Szemerédi in 1975 in a paper which was regarded as "*a masterpiece of combinatorial reasoning*" by R. L. Graham. Now the conjecture is known as the famous Szemerédi theorem. Here we state another version of it.

Szemerédi's Theorem. *Let $0 < \delta \leqslant 1$ and $k \in \{3, 4, \ldots\}$. Then there is $N(k, \delta) \in \mathbb{Z}^+$ such that if $n \geqslant N(k, \delta)$ and $A \subseteq [1, n]$ with $|A| \geqslant \delta n$ then A contains an AP of length k.*

The most important technique used by Szemerédi in his combinatorial

proof of Szemerédi's theorem is his powerful regularity lemma in graph-theoretic language.

Let $G=(V,E)$ be an undirected graph (without multiple edges). For $A,B\subseteq V$ we call

$$d(A,B)=\frac{|E\cap(A\times B)|}{|A\times B|},$$

the *density of edges* between A and B. For $\varepsilon>0$ the pair (A,B) is said to be *ε-regular* if $|d(X,Y)-d(A,B)|<\varepsilon$ for all those $X\subseteq A$ and $Y\subseteq B$ with $|X|\geqslant\varepsilon|A|$ and $|Y|\geqslant\varepsilon|B|$.

Szemerédi's Regularity Lemma. *Let $0<\varepsilon<1$ and $m_0\in\mathbb{Z}^+$. Then there are positive integers $M=M(\varepsilon,m_0)$ and $N=N(\varepsilon,m_0)$ such that whenever $G=(V,E)$ is an undirected graph with $|V|\geqslant N$ there is a partition $V_0\cup V_1\cup\cdots\cup V_m$ of V with*

$$|V_0|\leqslant\varepsilon|V|,\quad |V_1|=\cdots=|V_m|,\quad m_0\leqslant m\leqslant M \tag{$\star$}$$

and at most εm^2 pairs (V_i,V_j) $(1\leqslant i<j\leqslant m)$ not ε-regular.

Using Szemerédi's Regularity Lemma, one can deduce the following Triangle Removal Lemma which implies Roth's theorem.

Triangle Removal Lemma (Ruzsa and Szemerédi, 1978)**.** *For each $0<\delta\leqslant 1$, there exists $0<c(\delta)<1$ with the following property: If $G=(V,E)$ is an undirected graph with $|V|$ sufficiently large, and G contains fewer than $c(\delta)|V|^3$ triangles and then it is possible to remove fewer than $\delta|V|^2$ edges from G to create a graph containing no triangles.*

In 1977 H. Furstenberg used ergodic theory to give a new proof of Szemerédi's theorem, his work connecting combinatorial number theory with ergodic theory led him to win the Wolf prize in 2007. In a long paper published in 2001, W. T. Gowers employed harmonic analysis and combinatorics (including Frieman's theorem on sumsets) to reprove the Szemeredi theorem with explicit bounds; this is the main reason why Gowers won the Fields Medal in 1998.

Here are some known bounds for $N(k,\delta)$ in Szemerédi's theorem:

$$c^{\log(1/\delta)^{k-1}} \leqslant N(k,\delta) \leqslant 2^{2^{\delta^{-2^{2^{k+9}}}}},$$

where the lower bound is due to Behrend (for $k=3$) and Rankin (1962), and the upper bound is due to Gowers (2001). In 1999 J. Bourgain showed that $N(3,\delta) \leqslant c^{\delta^{-2}\log(1/\delta)}$.

Roth's theorem (Szemeredi's theorem in the case $k=3$) can be restated as follows: If $n>0$ is odd, and $A \subseteq \mathbb{Z}/n\mathbb{Z}$ does not contain any AP of length 3, then $|A| = O(n/\log\log n)$. Szemerédi, and Heath-Brown improved this independently by obtaining $|A| = O(n/\log^{\varepsilon} n)$ where $\varepsilon > 0$. Here is an extension of Roth's theorem to abelian groups of odd order established via characters of abelian groups.

Meshulam's Theorem [J. Combin. Theory Ser. A 71(1995)]**.** *Let G be an abelian group of odd order and write $G \cong \mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/\mathbb{Z}_{n_r}$ with $1 < n_1 \mid n_2 \mid \cdots \mid n_r$. If $A \subseteq G$ does not contain any AP of three terms, then $|A| \leqslant 2|G|/r$.*

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 (Ben Green and Terence Tao, 2004)**.** *There are arbitrarily long APs of primes.*

This achievement is part of the representative work of the 2006 Fields medalist Terence Tao (born in 1975). It has also brought several awards (including the Clay Research Award (2005) and the Ramanujan prize (2007)) to Ben Green (born in 1977), who was a former PhD student of the Fields Madalist W.T. Gowers.

It is well-known that $\sum_{p\in\mathbb{P}}\frac{1}{p}$ diverges, where $\mathbb{P}$ is the set of all primes. Thus, the following difficult conjecture includes both Szemerédi's theorem and the Green-Tao theorem as special cases.

Erdős-Turán Conjecture. *Let $a_1 < a_2 < \cdots$ be a sequence of positive integers with $\sum_{n=1}^\infty 1/a_n$ divergent. Then, for any $k = 3, 4, \ldots$ the sequence has a subsequence which is an AP of length k.*

In my opinion this conjecture might be too strong to hold. I'd like to modify this conjecture as follows: If $a_1 < a_2 < \cdots$ is a sequence of positive integers with $\sum_{n=1}^\infty 1/a_n = \infty$ and $\sum_{i\in I} 1/a_i \notin \mathbb{Z}^+$ for any finite subset I of $\mathbb{Z}^+$, then the sequence contains arbitrarily long APs.

E. Croot [Annals of Math. 157(2003)] solved the following difficult conjecture of P. Erdős and R. L. Graham by the sieve method.

Erdős-Graham Conjecture proved by E. Croot. *If we distribute*

all integers greater than one into n drawers, then some drawer contains integers $x_1, \ldots, x_m$ with $\sum_{k=1}^m 1/x_k = 1$.

I have made a conjecture stronger than this result.

A Conjecture of Z. W. Sun (Jan. 28, 2007)**.** *If A is a subset of $\{2, 3, \ldots\}$ with positive upper (asymptotic) density, then there are finitely many distinct elements $a_1 < \cdots < a_m$ of A with $\sum_{k=1}^m 1/a_k = 1$.*

Note that the set $\{3, 5, 7, \ldots\}$ has asymptotic density $1/2$, and

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

I have ever discussed the above conjecture with T. Tao via e-mails. At first he thought that it might be false, but later he agreed my argument over his intuitive reasons.

Unlike van der Waerden's theorem, Schur's theorem does not have a density version. For, the set $\{1, 3, 5, \ldots\}$ has asymptotic density $1/2$ but you cannot find three positive odd integers x, y, z such that $x + y = z$.

Recently A. Khalfalah and E. Szemeredi [Combin. Probab. Comput. 15(2006)] confirmed the following conjecture.

Erdős-Roth-Sárközy-Sós Conjecture proved by Khalfalah and Szemeredi). *Suppose that $\psi(x) \in \mathbb{Z}[x]$ have positive leading coefficient with $\psi(0)\psi(1)$ even (e.g., $\psi(x) = x^2$). If we distribute all positive integers into n drawers, then there are distinct x and y in the same drawer such that $x + y = \psi(z)$ for some $z \in \mathbb{Z}$.*

H.-Z. Li and H. Pan recently strengthened this result by using Green's basic idea in his proof of Roth's theorem in primes.

A Result of Li and Pan (2007, arXiv:0710.5344). *Let $a \geqslant b \geqslant 1$ be integers with $(a,b)=1$. Let $\psi(x) \in \mathbb{Z}[x]$ have positive leading coefficient. Suppose that $\psi(b-1)$ is even if a is odd, and $\psi(b)\psi(b-1)$ is even if a is even. If we distribute all positive integers into n drawers, then there are distinct x and y in the same drawer and an integer z such that $x+y=\psi(z)$ and $az+b$ is a prime.*

In the case $a=b=1$, this result says that if we distribute all positive integers into n drawers, then for any $\psi(x) \in \mathbb{Z}[x]$ with positive leading coefficient and even constant term, there exist distinct x and y in the same drawer such that $x+y=\psi(p-1)$ for some prime p.

2. On Snevily's conjecture and related results

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 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 $\{1,\ldots,n\}$.

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 $2 \nmid n$.

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 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.

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.*

In 2000 Noga Alon [Israel J. Math.] employed the following powerful tool to confirm Snevily's conjecture for the additive group $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ where p is an odd prime.

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 $m>0$ 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.

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

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.

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 (2006).

A Result of Z. W. 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.*

The case $m = 3$ is most interesting. We even cannot replace the group G in the result by the Klein quaternion group

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

A 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. A conjecture of Erdős and two local-global theorems

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

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

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.

By using roots of unity and Vandermonde determinants, in 1995-1996 Z. W. Sun obtained the following local-global result which is stronger than Conjecture 1.1.

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, 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 this theorem.

A Corollary(Z. W. Sun, 2003). *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 Z. W. Sun [J. Algebra 2005] via recurrence sequences.

The Second Local-Global Theorem (Z. W. Sun, [J. Algebra, 2005]). *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.*

A 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 $x\in\mathbb{Z}$. □

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

Soon after his invention of covers of $\mathbb{Z}$, Erdős made the following con-

jecture: *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

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

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! $\square$

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.

A Basic Theorem on Covers of Groups. *Let* $\mathcal{A} = \{a_i G_i\}_{i=1}^{k}$ *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.

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

We want to show that

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

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

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

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

$$a\bigg(\bigcap_{i\in I}G_i\bigg)=\bigcup_{\substack{j\notin I\\ a_jG_j\cap a(\bigcap_{i\in I}G_i)\neq\emptyset}}\bigg(a_jG_j\cap a\bigg(\bigcap_{i\in I}G_i\bigg)\bigg)$$

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. □

For a subgroup H of a group G with $[G:H]=k<\infty$, 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.

The following conjecture extends a 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. Below is the latest progress due to Z. W. Sun.

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 we have $|\bigcup_{i=1}^k a_iG_i|\geqslant|\bigcup_{i=1}^k G_i|$ for all $i=1,\ldots,k$.*

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 I 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 $k\leqslant 20$.