An on-line talk invited by Beijing Jiaotong Univ.

Covers of the Integers by Residue Classes and their Extensions to Groups

Zhi-Wei Sun

Nanjing University
Nanjing 210093, P. R. China
zwsun@nju.edu.cn
http://maths.nju.edu.cn/∼zwsun

April 15, 2021

Abstract

A system $A = \{a_s + n_s\mathbb{Z}\}_{s=1}^{k}$ of k residue classes is called a *cover of* $\mathbb{Z}$ if any integer belongs to one of the k residue classes. This concept was introduced by P. Erdős in the 1930s. Erdős ever conjectured that A is a cover of $\mathbb{Z}$ whenever it covers $1, \ldots, 2^k$.

In this talk we introduce some basic results on covers of $\mathbb{Z}$ as well as their elegant proofs. We will also talk about covers of groups by finitely many cosets, give a proof of the Neumann-Tomkinson theorem, and introduce progress on the Herzog-Schőheim conjecture and the speaker's disjoint cosets conjecture.

Part I. Covers of $\mathbb{Z}$ by residue classes

Covering systems of residue classes

For $a \in \mathbb{Z}$ and $n \in \mathbb{Z}^+ = \{1, 2, 3, \ldots\}$, let $a \pmod n = a + n\mathbb{Z}$ and

$$[\![x \equiv a \pmod n]\!] = \begin{cases} 1 & \text{if } x \equiv a \pmod n, \\ 0 & \text{otherwise.} \end{cases}$$

For a finite system $A = \{a_s \pmod{n_s}\}_{s=1}^k$ of residue classes, if $\bigcup_{s=1}^k a_s \pmod{n_s} = \mathbb{Z}$ then we call A a *covering system* or a *cover of* $\mathbb{Z}$; if A covers each integer exactly once then A is called an *exact cover* of $\mathbb{Z}$. For example, $\{r + n\mathbb{Z}\}_{r=0}^{n-1}$ is a exact cover of $\mathbb{Z}$.

The concept of covering system was introduced by Paul Erdős who gave the following example:

$$\{0 \pmod 2,\ 0 \pmod 3,\ 1 \pmod 4,\ 5 \pmod 6,\ 7 \pmod{12}\}.$$

Another Example.

$$A = \{1 \pmod 2,\ 2 \pmod{2^2},\ \ldots,\ 2^{k-1} \pmod{2^k},\ 0 \pmod{2^k}\}$$

is an exact cover of $\mathbb{Z}$. Note that $B = \{2^{s-1} \pmod{2^s}\}_{s=1}^k$ covers $1, \ldots, 2^k - 1$ but it does not cover 0.

An application of covers with distinct moduli

P. Erdős: Some residue class $a \pmod d$ with d even and a odd contains no numbers of the form $p + 2^n$ with p prime and $n \in \mathbb{N}$.

Proof. Let $A = \{a_1 \pmod{n_1}, \ldots, a_6 \pmod{n_6}\}$ be

$$\{0 \pmod 2, 0 \pmod 3, 1 \pmod 4, 3 \pmod 8, 7 \pmod{12}, 23 \pmod{24}\}.$$

This is a cover of $\mathbb{Z}$ with all the moduli distinct. Let $p_1 = 3,\ p_2 = 7,\ p_3 = 5,\ p_4 = 17,\ p_5 = 13,\ p_6 = 241$. Then $p_s \mid 2^{n_s} - 1$ but $p_s \nmid 2^n - 1$ for $0 < n < n_s$. As $2^5 \equiv 1 \pmod{31}$, we have $|\{p_s + 2^n \bmod 31 :\ 1 \leqslant s \leqslant 6,\ n \in \mathbb{N}\}| \leqslant 6 \times 5 < 31$. In fact, $p_s + 2^n \not\equiv 3 \pmod{31}$. Let $a \pmod d$ denote the residue class

$$1 \pmod 2 \cap 3 \pmod{31} \cap 2^{a_1} \pmod{p_1} \cap \ldots \cap 2^{a_6} \pmod{p_6}.$$

(This intersection is nonempty by the Chinese Remainder Theorem.) If $x \equiv a \pmod d$ and $x = p + 2^n$ with p prime and $n \in \mathbb{N}$. For some $1 \leqslant s \leqslant 6$, we have $n \equiv a_s \pmod{n_s}$ and hence $2^n \equiv 2^{a_s} \equiv x \pmod{p_s}$. Thus $p_s \mid p$ and $p_s = p$. But $x \not\equiv p_s + 2^n \pmod{31}$, so we get a contradiction.

Covering function

For $A = \{a_s (\mathrm{mod}\ n_s)\}_{s=1}^{k}$, its *covering function* $w_A : \mathbb{Z} \to \mathbb{Z}$ is defined by

$$w_A(x) = |\{1 \leqslant s \leqslant k : \ x \equiv a_s \pmod{n_s}\}|.$$

Clearly w_A is periodic modulo $N_A = [n_1, \ldots, n_k]$. Observe that

$$\begin{aligned}\frac{1}{N_A}\sum_{x=0}^{N_A-1} w_A(x) &= \frac{1}{N_A}\sum_{x=0}^{N_A-1}\sum_{s=1}^{k}[\![x \equiv a_s \pmod{n_s}]\!] \\ &= \sum_{s=1}^{k}\frac{1}{N_A}|\{0 \leqslant x < N_A : \ x \equiv a_s \pmod{n_s}\}| \\ &= \sum_{s=1}^{k}\frac{1}{N_A}\cdot\frac{N_A}{n_s} = \sum_{s=1}^{k}\frac{1}{n_s}.\end{aligned}$$

If A covers each integer at least m times, then we call A an *m-cover* (of $\mathbb{Z}$) and note that $\sum_{s=1}^{k}\frac{1}{n_s} \geqslant m$. If A covers each integer exactly m times, then we call A an *exact m-cover* (of $\mathbb{Z}$) and note that $\sum_{s=1}^{k}\frac{1}{n_s} = m$ in this case.

Davenport-Mirsky-Newman-Rado Result

In the 1960s Paul Erdős made the following conjecture: *If* $A = \{a_s \pmod{n_s}\}_{s=1}^{k}$ $(k > 1)$ *is a disjoint system with the moduli* $n_1, \ldots, n_k$ *distinct, then it cannot be a cover of* $\mathbb{Z}$.

H. Davenport, L. Mirsky, D. Newman and R. Radó (1960s): If $A = \{a_s \pmod{n_s}\}_{s=1}^{k}$ $(k > 1)$ 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 let $0 \leqslant a_s < n_s$ $(1 \leqslant s \leqslant k)$. 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

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

a contradiction!

Burshtein's conjecture

Let $A = \{a_s(n_s)\}_{s=1}^{k}$ be a disjoint cover of $\mathbb{Z}$ with each modulus occurring at most M times. Write $[n_1, \ldots, n_k] = \prod_{t=1}^{r} p_t^{\alpha_t}$, where $p_1 < \cdots < p_r$ are distinct primes and $\alpha_1, \ldots, \alpha_r$ are positive integers. N. Burshtein [Discrete Math. 14(1976)] conjectured that

$$p_r \leqslant M \prod_{p \leqslant p_r} \frac{p}{p-1}.$$

R. J. Simpson [Discrete Math. 59(1986)] proved further that

$$p_r \leqslant M \prod_{t=1}^{r-1} \frac{p_t}{p_t - 1}.$$

The last inequality implies that $M \geqslant p_1 > 1$; in fact, if $r \geqslant 2$ then

$$M > p_r \prod_{t=1}^{r-1} \frac{p_t - 1}{p_t} \geqslant p_{r-1} \prod_{t=1}^{r-2} \frac{p_t - 1}{p_t} \geqslant \cdots \geqslant p_2 \frac{p_1 - 1}{p_1} > p_1 - 1.$$

This gives a combinatorial approach to the Erdös conjecture.

A conjecture of Stein

A Conjecture of S.K. Stein [Math. Ann. 134(1958)]: If $A = \{a_s (\mathrm{mod}\ n_s)\}_{s=1}^{k}$ $(1 < n_1 < \ldots < n_k)$ is a disjoint system, then one of $1, \ldots, 2^k$ is not covered by A.

Note that if $A = \{a_s (\mathrm{mod}\ n_s)\}_{s=1}^{k}$ $(1 < n_1 < \ldots < n_k)$ is a disjoint system then it is not a cover of $\mathbb{Z}$ by the Davenport-Mirsky-Newman-Rado result.

P. Erdős [Mat. Lapok 13(1962)] proved a weaker version of Stein's Conjecture with 2^k replaced by $k2^k$.

Erdős' Conjecture

In 1965, P. Erdős offered $25 prize for a proof of his following conjecture which is a refinement of Stein's conjecture.

Erdős' Conjecture (1962). $A = \{a_s (\mathrm{mod}\ n_s)\}_{s=1}^{k}$ is a covering system if it covers all those integers from 1 to 2^k.

Remark. The 2^k in Erdős' conjecture is best possible because $\{2^{s-1} (\mathrm{mod}\ 2^s)\}_{s=1}^{k}$ covers $1, \ldots, 2^k - 1$ but does not cover any multiple of 2^k.

In 1969–1970 R. B. Crittenden and C. L. Vanden Eynden [Bull. Amer. Math. Soc. 1969; Proc. Amer. Math. Soc. 1970] supplied a long and awkward proof of the Erdős conjecture which involves some deep results concerning the distribution of primes. They actually proved that if the conjecture failed then there would be a counterexample with $k < 20$, and then claimed that the case $k < 20$ "*may be checked by more special arguments*".

A local-global theorem

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

For real numbers α and $\beta > 0$, we define

$$\alpha + \beta\mathbb{Z} := \{\alpha + \beta x : \ x \in \mathbb{Z}\}.$$

The First Local-Global Theorem (Z.-W. Sun [Acta Arith. 72(1995)]). Let $\alpha_1, \ldots, \alpha_k$ be real numbers and $\beta_1, \ldots, \beta_k$ be positive real numbers. Then $A = \{\alpha_s + \beta_s\mathbb{Z}\}_{s=1}^k$ covers all the integers at least m times if it covers $|S|$ consecutive integers at least m times, where

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

Remark. For $1 \leqslant m \leqslant k$, clearly an integer x is covered by $A = \{\alpha_s + \beta_s\mathbb{Z}\}_{s=1}^k$ at least m times if and only if it is covered by $\{\alpha_s + \beta_s\mathbb{Z}\}_{\substack{s=1 \\ s\notin J}}^k$ for all $J \subseteq \{1, \ldots, k\}$ with $|J| = m - 1$. So the theorem is reduced to the case $m = 1$.

Proof of the Local-Global Theorem with $m = 1$

For any integer x, clearly

$$
\begin{aligned}
& x \text{ is covered by } A \\
\iff & e^{2\pi i(\alpha_s - x)/\beta_s} = 1 \text{ for some } s = 1, \ldots, k \\
\iff & \prod_{s=1}^{k} \left(1 - e^{2\pi i(\alpha_s - x)/\beta_s}\right) = 0 \\
\iff & \sum_{I \subseteq \{1,\ldots,k\}} (-1)^{|I|} e^{2\pi i \sum_{s\in I} \alpha_s/\beta_s} \cdot e^{-2\pi i x \sum_{s\in I} 1/\beta_s} = 0 \\
\iff & \sum_{\theta \in S} e^{-2\pi i x \theta} z_\theta = 0,
\end{aligned}
$$

where

$$
z_\theta = \sum_{\substack{I \subseteq \{1,\ldots,k\} \\ \{\sum_{s\in I} 1/\beta_s\} = \theta}} (-1)^{|I|} e^{2\pi i \sum_{s\in I} \alpha_s/\beta_s}.
$$

Proof of the Local-Global Theorem with $m = 1$

Suppose that A covers $|S|$ consecutive integers

$$a, a+1, \ldots, a+|S|-1$$

where $a \in \mathbb{Z}$. By the above,

$$\sum_{\theta \in S} (e^{-2\pi i\theta})^r (e^{-2\pi ia\theta} z_\theta) = 0$$

for $r = 0, 1, \ldots, |S|-1$. As the determinant

$$\left| (e^{-2\pi i\theta})^r \right|_{0 \leqslant r < |S|,\, \theta \in S}$$

is of Vandermonde's type and hence nonzero, by Cramer's rule we have $z_\theta = 0$ for all $\theta \in S$. Therefore

$$\sum_{\theta \in S} e^{-2\pi ix\theta} z_\theta = 0$$

for all $x \in \mathbb{Z}$, i.e., any $x \in \mathbb{Z}$ is covered by A.

A corollary

Corollary. Let $A = \{a_s (\mathrm{mod}\ n_s)\}_{s=1}^k$ and $M = \max_{n\in\mathbb{Z}^+} |\{1 \leqslant s \leqslant k : \ n_s = n\}|$. If A covers $2^{k-M}(M+1)$ consecutive integers at least m times then A is an m-cover.

Proof. Choose $n \in \mathbb{Z}^+$ with $J = \{1 \leqslant s \leqslant k : \ n_s = n\}$ of cardinality M. Then

$$\begin{aligned}
&\left|\left\{\left\{\sum_{s\in I}\frac{1}{n_s}\right\} : \ I \subseteq \{1,\dots,k\}\right\}\right| \\
\leqslant &\left|\left\{\sum_{s\in I\cap J}\frac{1}{n_s} + \sum_{s\in I\setminus J}\frac{1}{n_s} : \ I \subseteq \{1,\dots,k\}\right\}\right| \\
\leqslant &\left|\left\{\sum_{s\in I}\frac{1}{n_s} : \ I \subseteq J\right\}\right| \times \left|\left\{\sum_{s\in I}\frac{1}{n_s} : \ I \subseteq \{1,\dots,k\}\setminus J\right\}\right| \\
\leqslant &\left|\left\{\frac{|I|}{n} : \ I \subseteq J\right\}\right| \times |\{I : \ I \subseteq \{1,\dots,k\}\setminus J\}| \\
= &(|J|+1)2^{k-|J|} = (M+1)2^{k-M}.
\end{aligned}$$

Crittenden-Vanden Eynden Conjecture

Example: Let $1 \leqslant \ell \leqslant k$. Then the residue classes

$$2^{i-1} (\mathrm{mod}\ 2^i) \ \ (i = 1, \ldots, k - \ell + 1)$$

are disjoint and their union is $\mathbb{Z} \setminus 0 (\mathrm{mod}\ 2^{k-\ell+1})$. Thus the k residue classes

$$1 (\mathrm{mod}\ \ell), \ldots, \ell - 1 (\mathrm{mod}\ \ell), \ell (\mathrm{mod}\ 2\ell), \ldots, 2^{k-\ell} \ell (\mathrm{mod}\ 2^{k-\ell+1} \ell)$$

are disjoint and their union is $\mathbb{Z} \setminus 0 (\mathrm{mod}\ 2^{k-\ell+1} \ell)$. So, the system A of these k residue classes covers $1, \ldots, 2^{k-\ell+1} \ell - 1$ but it is not a cover of $\mathbb{Z}$. Note that each modulus in A occurs at most $\ell - 1$ times and also every modulus of A is at least ℓ.

Crittenden-Vanden Eynden Conjecture [Amer. Math. Monthly 79(1972)]. Let $A = \{a_s (\mathrm{mod}\ n_s)\}_{s=1}^{k}$ with each modulus at least ℓ, where $1 \leqslant \ell \leqslant k$. A is a cover of $\mathbb{Z}$ if it covers $1, \ldots, 2^{k-\ell+1} \ell$.

Remark. When $\ell = 1, 2$ this reduces to Erdős' conjecture. The above conjecture in the case $\ell = 3$ was proved by R.J. Simpson [J. Austral Math. Soc. 63(1972)].

An application of the First Local-Global Theorem

Theorem. Let $m_1, \ldots, m_{n-1}$ $(n > 1)$ be integers. If there is a permutation $\sigma \in S_{n-1}$ such that $n \nmid sm_{\sigma(s)}$ for all $s = 1, \ldots, n-1$, then the set

$$\left\{ \sum_{i \in I} m_i : \ I \subseteq \{1, \ldots, n-1\} \right\}$$

contains a complete system of residues modulo n.

Proof. $A = \{s + (n/m_{\sigma(s)})\mathbb{Z}\}_{s=1}^{n-1}$ covers $1, \ldots, n-1$ but it does not cover 0. By the Local-Global Theorem, the fractional parts

$$\left\{ \sum_{s \in I} \frac{1}{n/m_{\sigma(s)}} \right\} \quad (I \subseteq \{1, \ldots, n-1\})$$

must have more than $n-1$ distinct values. Thus, the set

$$\left\{ \sum_{i \in I} m_i : \ I \subseteq \{1, \ldots, n-1\} \right\} = \left\{ \sum_{s \in I} m_{\sigma(s)} : \ I \subseteq \{1, \ldots, n-1\} \right\}$$

contains a complete system of residues modulo n.

Ge and Sun's result for finite abelian groups

For a finite multiplicative group G, its exponent $\exp(G)$ is defined to be the least positive integer such that $x^n = e$ for all $x \in G$, where e is the identity of G. For a finite abelian group G, $\exp(G)$ is known to be $\max\{o(x) : \ x \in G\}$, where $o(x)$ denotes the order of x. If G is an additive group, then for $k \in \mathbb{Z}^+$ and $a \in G$ we write ka for the sum $a_1 + \ldots + a_k$ with $a_1 = \cdots = a_k = a$.

Theorem (F. Ge and Z.-W. Sun [Electron. J. Combin. 24(2017)]). Let G be a finite additive abelian group with exponent $n > 1$. For any $a_1, \ldots, a_{n-1} \in G$, there is a permutation $\sigma \in S_{n-1}$ such that all the elements $sa_{\sigma(s)}$ $(s = 1, \ldots, n-1)$ are nonzero if and only if

$$\left|\left\{1 \leqslant s < n : \ \frac{n}{d}a_s \neq 0\right\}\right| \geqslant d - 1 \ \text{ for all } d \in D(n).$$

where $D(n)$ denotes the set of all positive divisors of n.

Remark. This theorem for the cyclic group $\mathbb{Z}/n\mathbb{Z}$ was conjectured by Sun in 2004.

Zhang's result and its extensions

Ming-Zhi Zhang (1989): If $A=\{a_s(\mathrm{mod}\ n_s)\}_{s=1}^k$ is a cover of $\mathbb{Z}$ then $\sum_{s\in I}\frac{1}{n_s}\in\mathbb{Z}^+$ for some $\emptyset\neq I\subseteq\{1,\ldots,k\}$.

Z.-W. Sun [Israel J. Math. 77(1992)]: If $A=\{a_s(\mathrm{mod}\ n_s)\}_{s=1}^k$ is an exact m-cover of $\mathbb{Z}$, then for any $n=0,\ldots,m$ we have

$$\left|\left\{I\subseteq\{1,\ldots,k\}:\ \sum_{s\in I}\frac{1}{n_s}=n\right\}\right|\geqslant\binom{m}{n}.$$

Z.-W. Sun [Trans. Amer. Math. Soc. 348(1996)]: If $A=\{a_s(\mathrm{mod}\ n_s)\}_{s=1}^k$ is an m-cover of $\mathbb{Z}$, then for any $m_1,\ldots,m_k\in\mathbb{Z}^+$ there are at least m positive integers in the form $\sum_{s\in I}m_s/n_s$ with $I\subseteq\{1,\ldots,k\}$.

The Second Local-Global Theorem

The Second Local-Global Theorem (Z.-W. Sun [J. Algebra, 293(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

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

(i) There are periodic maps $f_0, \ldots, f_{|S(n_1,\ldots,n_k)|-1} : \mathbb{Z} \to \mathbb{Z}$ only depending on $S(n_1, \ldots, n_k)$ such that $\psi(x) = \sum_{0 \leqslant r < |S(n_1,\ldots,n_k)|} f_r(x)\psi(r)$ for all $x \in \mathbb{Z}$. In particular, values of ψ are completely determined by the set $S(n_1, \ldots, n_k)$ and the initial values $\psi(0), \ldots, \psi(|S(n_1, \ldots, n_k)| - 1)$.

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

Remarks on $|S(n_1,\ldots,n_k)|$

Let $D=\{d\in\mathbb{Z}^+:\ d\mid n_s \text{ for some } s=1,\ldots,k\}$. Then

$$|S(n_1,\ldots,n_k)|=\left|\bigcup_{d\in D}\left\{\frac{c}{d}:\ 0\leqslant c<d\ \&\ (c,d)=1\right\}\right|=\sum_{d\in D}\varphi(d),$$

where φ is the well-known Euler function.

As $|\bigcap_{s\in I}\{r/n_s:\ r=0,\ldots,n_s-1\}|=\gcd(n_s:\ s\in I)$ for all $\emptyset\neq I\subseteq\{1,\ldots,k\}$, by the inclusion-exclusion principle, we have

$$|S(n_1,\ldots,n_k)|=\sum_{\emptyset\neq I\subseteq\{1,\ldots,k\}}(-1)^{|I|-1}\gcd(n_s:\ s\in I).$$

Two corollaries

As $|S(m,n)| = m+n-\gcd(m,n)$, we have the following consequence.

Corollary 1. Let g and h be maps from $\mathbb{Z}$ to an additive abelian group G with positive periods m and n respectively. Then $\{g(x)-h(x) : x \in \mathbb{Z}\}$ is contained in the subgroup of G generated by those $g(r)-h(r)$ with $0 \leqslant r < m+n-\gcd(m,n)$; in particular, g and h are identical if $g(r)=h(r)$ for all $r = 0,\ldots,m+n-\gcd(m,n)-1$.

Fine-Wilf Theorem (N.J. Fine and H.S. Wilf [Proc. Amer. Math. Soc. 16(1965)]). Let g and h be maps from $\mathbb{Z}$ to the real field $\mathbb{R}$ with positive periods m and n respectively. If $g(r)=h(r)$ for all $r = 0,\ldots,m+n-\gcd(m,n)-1$, then we have $g=h$.

Corollary 2. $A = \{a_s (\mathrm{mod}\ n_s\}_{s=1}^k$ is an exact m-cover of $\mathbb{Z}$ if it covers $|\bigcup_{s=1}^k \{r/n_s : \ r = 0,\ldots,n_s-1\}|$ $(\leqslant \sum_{s=1}^k n_s - k + 1)$ consecutive integers exactly m times.

Part II. Covers of Groups by Cosets

Covers of groups by cosets

The addition group $\mathbb{Z}$ is an infinite cyclic group. Its subgroups have the form $n\mathbb{Z}$ $(n = 0, 1, 2, \ldots)$.

For $n \in \mathbb{Z}^+$, $n\mathbb{Z}$ is a normal subgroup of G and the quotient group $\mathbb{Z}/n\mathbb{Z}$ is of order n. A residue class $a + n\mathbb{Z}$ is a coset of $n\mathbb{Z}$ in $\mathbb{Z}$. Note also that n is the index of the subgroup $n\mathbb{Z}$ in $\mathbb{Z}$.

Instead of covers of $\mathbb{Z}$ by finitely many residue classes $a_s + n_s\mathbb{Z}$ $(s = 1, \ldots, k)$, we may also study covers of a group G by finitely many left cosets $a_1 G_1, \ldots, a_k G_k$. Instead of the moduli n_s in the residue class $a_s + n_s\mathbb{Z}$, we may investigate the indices $n_s = [G : G_s]$.

Let H be a subgroup of a group G. Note that a right coset Ha of H is also a left coset $a(a^{-1}Ha)$ of $a^{-1}Ha$.

Disjoint covers of a group by left or right cosets

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 which is the largest normal subgroup of G contained in H.

In group theory, it is known that G/H_G can be embedded into the symmetric group $S_{[G:H]} = S_k$ and thus

$$\left[G : \bigcap_{i=1}^{k} G_i\right] = |G/H_G| \leqslant k!.$$

A basic theorem on covers of groups

An Example of M. J. Tomkinson. Let $k > 1$ be a positive integer, and let G be the symmetric group S_k and H be the stabilizer of 1. Then $G_i = (1i)^{-1}H(1i)$ is the stabilizer of i for each $i = 1, \ldots, k$. Clearly,

$$\{G_1, (12)G_2, \ldots, (1k)G_k\} = \{H, H(12), \ldots, H(1k)\}$$

forms a disjoint cover of G with $\bigcap_{i=1}^{k} G_i = H_G = \{e\}$. Note that $[G : \bigcap_{i=1}^{k} G_i] = |G| = k!$.

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 of 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.

Tomkinson's proof of the second part

We show by induction 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

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

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

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

Herzog-Schöheim Conjecture

Herzog-Schönheim Conjecture [Canad. Math. Bull. 17(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 (finite) indices $n_1 = [G : G_1], \ldots, n_k = [G : G_k]$ cannot be distinct.

This is an extension of the confirmed Erdős conjecture to covers of groups.

Berger, Felzenbaum and Fraenkel [Canad. Bull. Math. 1986]: The Herzog-Schöheim Conjecture holds for finite nilpotent groups.

L. Margolis and O. Schnabel [Beitr. Algebra Geom. 2019]: The Herzog-Schöheim Conjecture holds for all groups G with $|G| < 1440$.

Subnormal subgroups

A subgroup H of a group G is said to be *subnormal* in G if there are a finite chain of subgroups

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

such that H_i is normal in H_{i+1} for all $i = 0, \ldots, n-1$.

It is known that all the subgroups of a nilpotent group G are subnormal in G.

My result on the Herzog-Schöheim Conjecture

Z.-W. Sun [J. Algebra 273(2004)]. Let $\mathcal{A} = \{a_i G_i\}_{i=1}^k$ be a finite system of left cosets in a group G with not all the G_i equal to G. Suppose that $\mathcal{A}$ covers all the elements of G the same number of times, and that among the (finite) indices

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

each occurs at most $M \in \mathbb{Z}^+$ times. If all the G_i are subnormal in G, then $M > 1$ and

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

A lemma on subnormal subgroups

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

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

(ii) [J. Algebra, 2004] Let H be a subnormal subgroup of G with finite index. Then

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

A lemma on unions of cosets

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 the union $\bigcup_{i=1}^k a_i G_i$ contains at least $|\bigcup_{i=1}^k 0(\mathrm{mod}\ n_i) \cap \{0, 1, \ldots, N-1\}|$ 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*

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

(A subgroup H of a finite group G is called a *Hall subgroup* of G if $|H|$ is relatively prime to $[G : H]$.)

Tools from analytic number theory

We also need the following 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

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

Using the above two theorems we can deduce the following lemma.

An Analytic Lemma (Z. W. Sun [J. Algebra, 2004]). For $M \geqslant 2$, if $q > 1$ is an integer with $q < M\prod_{p \leqslant q} p/(p-1)$ then

$$q < e^{\gamma} M \log M + O(M \log\log M) \text{ and } \pi(q) \leqslant e^{\gamma} M + O(M/\log M),$$

where the O-constants are absolute.

Huhn-Megyesi's problems on disjoint residue classes

A finite sequence $\{n_s\}_{s=1}^k$ of positive integers is called *harmonic* if $n_1, \ldots, n_k$ are the moduli of pairwise disjoint residue classes.

In 1982 A. P. Huhn and L. Megyesi [Discrete Math. 41(1982)] posed two open problems on harmonic sequences. Both were solved by Sun [Chinese Ann. Math. 13A(1992)] negatively.

A Problem of Huhn-Megyesi: Let $n_1, \ldots, n_k$ be positive integers with $\sum_{s=1}^k 1/n_s \leqslant 1$. Is the following a necessary and sufficient condition for $\{n_s\}_{s=1}^k$ to be harmonic?

$$\max_{\substack{i,j\in I\\ i\neq j}}(n_i, n_j) \geqslant |I| \quad \text{for all } I \subseteq \{1, \ldots, k\} \text{ with } |I| \geqslant 2. \qquad (*)$$

Sun [Chinese Ann. Math. 13A(1992)] showed that for $k \geqslant 5$ there are positive integers $n_1, \ldots, n_k$ satisfying $\sum_{s=1}^k 1/n_s \leqslant 1$ and $(*)$ but $\{n_s\}_{s=1}^k$ is *not* harmonic.

Sun [Discrete Math. 104(1992)] and Y.-G. Chen [Discrete Math. 162(1996)] gave some sufficient conditions for $\{n_s\}_{s=1}^k$ to be harmonic.

A challenging conjecture on disjoint cosets

Finally we mention a challenging conjecture arising from the speaker's 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 $k = 2$. If G_1 and G_2 are subgroups of G with $[G : G_1]$ and $[G : G_2]$ finite and relatively prime, then $G_1G_2 = G$ and $a_1G_1 \cap a_2G_2 \neq \emptyset$ for all $a_1, a_2 \in G$.

W.-J. Zhu [Int. J. Mod. Math. 3(2008)] proved the conjecture for $k = 3, 4$ via several sophisticated lemmas. In 2009, Z. Gong confirmed the conjecture in the case $k = 5$. K. O'Bryant [Integers 2007] confirmed the conjecture for $G = \mathbb{Z}$ in the case $k \leqslant 20$.

Reduce the Disjoint Cosets Conjecture to finite groups

Suppose that $a_1G_1, \ldots, a_kG_k$ $(k > 1)$ be pairwise disjoint left cosets of a group G with all the indices $[G : G_i]$ finite. By Poincare's theorem, the intersection $F = \bigcap_{i=1}^{k} G_i$ has a finite index in G and hence $H = F_G$ also has a finite index in G.

Let $\bar{G} = G/H$, $\overline{a_i} = a_iH$ and $\overline{G_i} = G_i/H$ for all $i = 1, \ldots, k$. Then

$$\overline{a_i}\,\overline{G_i} \quad (i = 1, \ldots, k)$$

are pairwise disjoint left cosets in the finite group $\bar{G} = G/H$. Note that

$$[\bar{G} : \overline{G_i}] = [G : G_i] \quad \text{for all } i = 1, \ldots, k.$$

By the above, the Disjoint Cosets Conjecture can be reduced to finite groups.

References

Main References

1. L. Margolis and O. Schnabel, *The Herzog-Schönheim conjecture for small groups and harmonic subgroups*, Beitr. Algebra Geom. **60** (2019), 399–418.

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

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

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

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

6. W.-J. Zhu, *On Sun's conjecture concerning disjoint cosets*, Int. J. Mod. Math. **3** (2008), 197–206. See also arXiv:0807.2207.

Thank you!