A talk given at the Institute of Mathematics (Beijing, June 29, 2008)

STUDY COVERS OF GROUPS VIA CHARACTERS AND 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

Abstract. Tools from number theory and algebra are very helpful in the study of some combinatorial problems. What is the smallest positive integer k such that an abelian group G can be irredundantly covered by k cosets of subgroups one of which has index n? We will talk about the solution to this combinatorial problem provided by G. Lettl and the speaker via characters of abelian groups and algebraic number theory. The Herzog-Schönheim conjecture asserts that if a group G is partitioned into $k>1$ left cosets $a_1G_1,\ldots,a_kG_k$ then the indices $[G:G_1],\ldots,[G:G_k]$ cannot be distinct. We will also introduce the speaker's approach to the Herzog-Schönheim conjecture via analytic number theory and some combinatorial arguments. Some related conjectures will be also mentioned in the talk.

1. Basic results on covers of groups by left 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 (H_G denotes 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

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

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.

Proof (Tomkinson). We prove the inequality in (ii) by induction.

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 $\{a_iG_i\}_{i\in I}$ 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

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

and hence

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

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

Definition of m-covers. Let m be a positive integer, and let $A = \{a_iG_i\}_{i=1}^k$ be a finite system of left cosets in a group G. If each element of G is covered by A at least (resp., exactly) m times, then we call A an *m-cover* (resp., *exact m-cover*) of G. If A is an m-cover of G but none of its proper subsystems does, then A is said to be a *minimal m-cover* of G.

The Neumann-Tomkinson theorem can be extended to minimal m-covers of groups (cf. Corollary 1 of Z. W. Sun [Fund. Math. 134(1990)]); it also has applications in Galois theory, groups rings, Banach spaces, projective geometry and Riemann surfaces as pointed out by T. Soundararajan and K. Venkatachaliengar [Acta Math. Vietnam 19(1994)].

2. Extremal problems for exact m-covers

Let $A=\{a_iG_i\}_{i=1}^k$ be an exact m-cover of a group G with $\bigcap_{i=1}^k G_i=H$. By the Neumann-Tomkinson theorem, $[G:H]\leqslant k!$. How to provide a sharp lower bound of k in terms of G and H?

An Example of Š. Znám. Let $n>1$ be an integer with the factorization $\prod_{t=1}^r p_t^{\alpha_t}$, where $p_1,\ldots,p_r$ are distinct primes and $\alpha_1,\ldots,\alpha_r\in\mathbb{Z}^+=\{1,2,3,\ldots\}$. Then $0(\mathrm{mod}\ n)$ and the following $f(n)=\sum_{s=1}^r\alpha_s(p_s-1)$ residue classes

$$jp_1^{\alpha_1}\cdots p_{s-1}^{\alpha_{s-1}}p_s^{\alpha-1}(\mathrm{mod}\ p_1^{\alpha_1}\cdots p_{s-1}^{\alpha_{s-1}}p_s^{\alpha})$$
$$(\alpha=1,\ldots,\alpha_s;\ j=1,\ldots,p_s-1;\ s=1,\ldots,r)$$

form a disjoint cover of $\mathbb{Z}$ whose moduli have the least common multiple n. As a convention we define $f(1)=0$. The function f is called the Mycielski function.

An Example of Z. W. Sun. Let H be a subnormal subgroup of a group G with finite index. Let

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

be a composition series from H to G. For each $i=0,\ldots,n-1$, write

$$H_{i+1}\setminus H_i=\bigcup_{j=1}^{[H_{i+1}:H_i]-1}b_j^{(i)}H_i.$$

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

$$b_j^{(i)}H_i\ (0\leqslant i<n;\ 1\leqslant j<[H_{i+1}:H_i]),$$

together with H and $m-1$ copies of G, form an exact m-cover of G by $m+d(G,H)$ left cosets of subgroups whose intersection is H. (In the case $H=G$ we define $d(G,H)=0$.)

Relation between the Mycielski Function f and $d(G,H)$ (Z. W. Sun, Fund. Math. 1990; European J. Combin. 2001). Let H be any subnormal subgroup of G with finite index. Then

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

Also, $d(G,H)=f([G:H])$ 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 $i=1,\dots,k$.*

Related Results on Exact m-covers. *Let $A=\{a_iG_i\}_{i=1}^k$ be an exact m-cover of a group G with $\bigcap_{i=1}^k G_i = H$.*

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

(ii) (Z. W. Sun [European J. Combin., 2001]) *If $G_1,\dots,G_k$ are subnormal in G, then $k \geqslant m+d(G,H)$, with the lower bound best possible.*

The proof is by induction, on the basis of the following key lemma.

A Lemma (Z. W. Sun [European J. Combin., 2001]). *Let $\mathcal{A}=\{a_iG_i\}_{i=1}^k$ be an exact m-cover of a group G by left cosets of subnormal subgroups $G_1,\dots,G_k$. For any maximal normal subgroup H of G, we have*

$$\{C \in G/H : C \supseteq a_iG_i \text{ for some } i=1,\dots,k\} = \emptyset \text{ or } G/H.$$

Note that Korec's result is stronger than Mycielski's conjecture, and also Sun's result has the following consequence.

A 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. □

3. An extremal problem for minimal m-covers of abelian groups

Korec's and Sun's results on exact m-covers can be extended to minimal m-covers of $\mathbb{Z}$, see R. J. Simpson [Acta Arith., 1985] for the case $m=1$ and Z. W. Sun [Internat. J. Math. 17(2006)] for general $m\geqslant 1$. However, they cannot be extended to minimal m-covers of abelian groups as illustrated by the following example.

An Example of G. Lettl and Z. W. Sun. Let G be the abelian group $C_p\times C_p$ where p is a prime and C_p is the cyclic group of order p. Then any element $a\neq e$ of G has order p. Let $G_1,\ldots,G_k$ be all the distinct subgroups of G with order p. If $1\leqslant i<j\leqslant k$, then $G_i\cap G_j=\{e\}$.

Thus $\{G_s\}_{s=1}^k$ forms a minimal cover of G with $\bigcap_{s=1}^k G_s = \{e\}$. Since $1+k(p-1) = |\bigcup_{s=1}^k G_s| = |G| = p^2$, we have

$$k = p+1 \geqslant 1 + f([G:G_s]) = 1 + f(p) = p.$$

However,

$$k = p+1 \leqslant 2p-1 = 1 + f([G:\{e\}]) = 1 + d\Big(G, \bigcap_{s=1}^k G_s\Big),$$

and the last inequality becomes strict when $p>2$.

An Extremal Problem on m-Covers of Abelian Groups. *Let m and n be positive integers. Is $m+f(n)$ the smallest positive integer k such that for any abelian group having a subgroup of index n there is a minimal m-cover of G by k cosets of subgroups one of which has index n?*

G. Lettl and Z. W. Sun has provided an affirmative answer to this problem.

A Theorem of Lettl and Sun [Acta Arith. 131(2008)]**.** *Let $A = \{a_sG_s\}_{s=1}^k$ be a minimal m-cover of an abelian group G by left cosets. Then*

$$k \geqslant m + f([G:G_t]) \qquad \text{for any } \ t = 1, \ldots, k.$$

This theorem implies the following conjecture of W. D. Gao and A. Geroldinger [European J. Combin. 2003] who proved it for elementary abelian p-groups.

Gao-Geroldinger Conjecture (W. D. Gao and A. Geroldinger)**.** *Let G be a finite abelian group with identity e. If $G \setminus \{e\}$ is a union of k cosets $a_1G_1, \ldots, a_kG_k$, then we have $k \geqslant f(|G|)$.*

In fact, if we set $a_0 = e$ and $G_0 = \{e\}$ then $\{a_sG_s\}_{s=0}^k$ forms a cover of G with a_0G_0 irredundant and hence $k+1 \geqslant 1+f([G:G_0]) = 1+f(|G|)$.

A Conjecture of Z. W. Sun. (i) (2008) *Whenever $A = \{a_iG_i\}_{i=1}^k$ forms an m-cover of a group G by left cosets with a_tG_t irredundant, we have the inequality $k \geqslant m + f([G:G_t])$ and hence $[G:G_t] \leqslant 2^{k-m}$.*

(ii) (2004) *If $A = \{a_iG_i\}_{i=1}^k$ forms a minimal m-cover of an abelian group G by left cosets or an exact m-cover of a solvable group G by left cosets, then we have $k \geqslant m + f(N)$, where N is the least common multiple of the indices $[G:G_1], \ldots, [G:G_k]$.*

When $\{a_iG_i\}_{i=1}^k$ forms an exact m-cover of a solvable group G, the inequality $k \geqslant m + f([G:G_t])$ was shown by Berger, Felzenbaum and Fraenkel [Colloq. Math. 1988] in the case $m = 1$ and proved by the speaker [European J. Combin. 2003] for general m.

Concerning covers of abelian groups by subgroups, Song Guo and the speaker have made the following conjecture.

A Conjecture of S. Guo and Z. W. Sun (2004)**.** *If $\{G_i\}_{i=1}^k$ forms a minimal m-cover of an abelian group G with $[G : \bigcap_{i=1}^k G_i] = \prod_{t=1}^r p_t^{\alpha_t}$, where $p_1, \ldots, p_r$ are distinct primes and $\alpha_1, \ldots, \alpha_r$ are positive integers.*

Then we have

$$k > m + \sum_{t=1}^{r} (\alpha_t - 1)(p_t - 1).$$

4. Proof of the Lettl-Sun result

The Lettl-Sun result cannot be shown in the way that we prove Korec's or Sun's result in Section 2, because we don't have the corresponding lemma for minimal m-covers of abelian groups. Thus, new ideas are needed!

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. 131(2008)]). *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 $\bar{\mathbb{Z}}$ of algebraic integers.*

Let n be any positive integer and let $\Phi_n(x)$ be the nth cyclotomic polynomial given by

$$\Phi_n(x) = \prod_{\substack{m=1 \\ (m,n)=1}}^{n} (x - e^{2\pi i m/n}).$$

Observe that

$$x^n - 1 = \prod_{m=1}^{n} \left(x - e^{2\pi i m/n}\right) = \prod_{d \mid n} \prod_{\substack{c=1 \\ (c,d)=1}}^{d} \left(x - e^{2\pi i c/d}\right) = \prod_{d \mid n} \Phi_d(x).$$

Applying the Möbius inversion we obtain

$$\Phi_n(x)=\prod_{d\mid n}(x^d-1)^{\mu(n/d)}\in\mathbb{Z}[x].$$

If $n>1$, then $\sum_{d\mid n}\mu(n/d)=\sum_{d\mid n}\mu(d)=0$, thus

$$\Phi_n(x)=\prod_{d\mid n}\left(\frac{x^d-1}{x-1}\right)^{\mu(n/d)}=\prod_{d\mid n}(1+x+\cdots+x^{d-1})^{\mu(n/d)}$$

and hence

$$\Phi_n(1)=\prod_{d\mid n}d^{\mu(n/d)}.$$

Recall that the Mangoldt function is given by

$$\Lambda(n)=\begin{cases}\log p & \text{if } n=p^a \text{ for some prime } p \text{ and } a\in\mathbb{Z}^+,\\ 0 & \text{otherwise.}\end{cases}$$

If n has the primary factorization $\prod_{i=1}^r p_i^{\alpha_i}$ where $p_1,\ldots,p_r$ are distinct primes and $\alpha_1,\ldots,\alpha_r\in\mathbb{N}$, then

$$\sum_{d\mid n}\Lambda(d)=\sum_{i=1}^r\sum_{\beta_i=0}^{\alpha_i}\Lambda(p_i^{\beta_i})=\sum_{i=1}^r\alpha_i\log p_i=\log\prod_{i=1}^r p_i^{\alpha_i}=\log n.$$

Applying the Möbius inversion formula we get

$$\sum_{d\mid n}\mu\left(\frac{n}{d}\right)\log d=\Lambda(n).$$

Therefore

$$\log\Phi_n(1)=\sum_{d\mid n}\mu\left(\frac{n}{d}\right)\log d=\begin{cases}\log p & \text{if } n \text{ is a power of some prime } p,\\ 0 & \text{otherwise.}\end{cases}$$

So we have

$$\prod_{\substack{m=1\\(m,n)=1}}^{n}(1-e^{2\pi im/n})=\Phi_n(1)=\begin{cases}p & \text{if } n \text{ is a power of some prime } p,\\ 1 & \text{otherwise.}\end{cases}$$

In particular,

$$\prod_{m=1}^{p-1}(1-e^{2\pi im/p})=p\quad\text{for any prime } p.$$

Proof of the Lemma of Lettl and Sun. Note that

$$n=\prod_{p\mid n}p^{\mathrm{ord}_p(n)}=\prod_{p\mid n}\prod_{m=1}^{p-1}(1-e^{2\pi im/p})^{\mathrm{ord}_p(n)}.$$

So there exist $f(n)=\sum_{p\mid n}\mathrm{ord}_p(n)(p-1)$ roots of unity $\zeta_1,\ldots,\zeta_{f(n)}\neq 1$ such that n divides $(1-\zeta_1)\cdots(1-\zeta_{f(n)})$ in the ring $\bar{\mathbb{Z}}$ of all algebraic integers.

Now suppose that $\prod_{s=1}^{k}(1-\zeta_s)\equiv 0 \pmod n$, where ζ_s is a primitive n_sth root of unity with $n_s>1$. Recall that

$$\prod_{\substack{r=1\\(r,n_s)=1}}^{n_s}(1-\zeta_s^r)=\prod_{\substack{m=1\\(m,n_s)=1}}^{n_s}(1-e^{2\pi im/n_s})$$
$$=\begin{cases}p & \text{if } n_s \text{ is a power of some prime } p,\\ 1 & \text{otherwise.}\end{cases}$$

Let N be the least common multiple of $n_1,\ldots,n_k$. Then

$$n^{\varphi(N)}\ \Big|\ \prod_{s=1}^{k}\left((1-\zeta_s)^{\varphi(n_s)}\right)^{\varphi(N)/\varphi(n_s)}\ \Big|\ \prod_{\substack{s=1\\ n_s \text{ is a prime power}}}^{k}p(n_s)^{\varphi(N)/\varphi(n_s)},$$

where $p(n_s)$ denotes the smallest prime divisor of n_s. So, for any prime p we have

$$\mathrm{ord}_p(n)\varphi(N) \leqslant \sum_{\substack{s=1\\ n_s \text{ is a power of } p}}^{k} \frac{\varphi(N)}{\varphi(n_s)}$$

and hence

$$|\{1 \leqslant s \leqslant k :\ n_s \text{ is a power of } p\}| \geqslant \mathrm{ord}_p(n)(p-1).$$

It follows that

$$k \geqslant \sum_{p\mid n} |\{1 \leqslant s \leqslant k :\ n_s \text{ is a power of } p\}| \geqslant \sum_{p\mid n} \mathrm{ord}_p(n)(p-1) = f(n).$$

This concludes the proof of the lemma. $\square$

For a finite abelian group G, let $\widehat{G}$ denote the group of all complex-valued characters of G. One has $\widehat{G} \cong G$. For any subgroup H of G let $H^{\perp}$ denote the group of those characters $\chi \in \widehat{G}$ with $\ker(\chi) = \{x \in G :\ \chi(x) = 1\}$ containing H. Then there is a canonical isomorphism $H^{\perp} \cong \widehat{G/H}$ by putting $\chi(aH) = \chi(a)$ for any $a \in G$ and any $\chi \in H^{\perp}$. Furthermore, for each $a \in G \setminus H$ there exists some $\chi \in H^{\perp}$ with $\chi(a) \neq 1$.

Proof of the Lettl-Sun Result. As $H = \bigcap_{s=1}^{k} G_s$ is of finite index in G. Instead of the minimal m-cover $A = \{a_s G_s\}_{s=1}^{k}$ of G, we may consider the minimal m-cover $\bar{A} = \{\bar{a}_s \bar{G}_s\}_{s=1}^{k}$ of the finite abelian group $\bar{G} = G/H$, where $\bar{a}_s = a_s H$ and $\bar{G}_s = G_s/H$ (hence $[\bar{G} : \bar{G}_s] = [G : G_s]$). Therefore, without any loss of generality, we can assume that G is finite.

Fix $1 \leqslant t \leqslant k$. As $\{a_s G_s\}_{s\neq t}$ is not an m-cover of G, there is an $a \in a_t G_t$ such that it is covered by exactly m cosets in A and hence

$J=\{1\leqslant j\leqslant k:\ a\notin a_jG_j\}$ has cardinality $k-m$. For each $j\in J$ we may choose a $\chi_j\in G_j^{\perp}$ with $\zeta_j:=\chi_j(a^{-1}a_j)\neq 1$. For any $x\in G\setminus G_t$ we have $ax\notin aG_t=a_tG_t$. Since A is an m-cover of G, there exists some $j\in J$ such that $ax\in a_jG_j$, and therefore $\chi_j(x)=\chi_j(a^{-1}a_j)=\zeta_j$ by the choice of χ_j and the definition of ζ_j.

For $x\in G$ we define

$$\Psi(x)=\prod_{j\in J}\left(\chi_j(x)-\zeta_j\right).$$

If $\chi\in G_t^{\perp}$ and $\chi(x)\neq 1$, then $x\notin G_t$ and hence $\Psi(x)=0$ by the above. Thus $\Psi\chi=\Psi$ for all $\chi\in G_t^{\perp}$.

Observe that

$$\Psi(x)=\sum_{I\subseteq J}\left(\prod_{j\in I}\chi_j(x)\right)\prod_{j\in J\setminus I}(-\zeta_j)=\sum_{\psi\in\widehat{G}}c(\psi)\psi(x),$$

where

$$c(\psi)=\sum_{\substack{I\subseteq J\\ \prod_{j\in I}\chi_j=\psi}}\ \prod_{j\in J\setminus I}(-\zeta_j)\in\overline{\mathbb{Z}}.$$

Let $\mathbb{C}$ be the complex field. As the set $\widehat{G}$ is a basis of the $\mathbb{C}$-vector space

$$\mathbb{C}^G=\{g:\ g \text{ is a function from } G \text{ to } \mathbb{C}\},$$

for any $\chi\in G_t^{\perp}$ we have $c(\psi\chi)=c(\psi)$ for all $\psi\in\widehat{G}$ because $\Psi\chi^{-1}=\Psi$.

Clearly

$$\prod_{j\in J}(1-\zeta_j)=\Psi(e)=\sum_{\psi\in\widehat{G}}c(\psi)\psi(e)=\sum_{\psi\in\widehat{G}}c(\psi).$$

Let $\psi_1 G_t^\perp \cup \cdots \cup \psi_l G_t^\perp$ be a coset decomposition of $\widehat{G}$ where $l = [\widehat{G} : G_t^\perp]$. Then

$$\sum_{\psi \in \widehat{G}} c(\psi) = \sum_{r=1}^{l} \sum_{\chi \in G_t^\perp} c(\psi_r \chi) = \sum_{r=1}^{l} |G_t^\perp| c(\psi_r) = [G : G_t] \sum_{r=1}^{l} c(\psi_r).$$

Therefore $[G : G_t]$ divides $\prod_{j \in J}(1 - \zeta_j)$ in the ring $\overline{\mathbb{Z}}$ of all algebraic integers, and the lemma of Lettl and Sun gives

$$k - m = |J| \geqslant f([G : G_t]).$$

4. On the Herzog-Schönheim conjecture

Soon after his invention of covers of $\mathbb{Z}$, Erdős made the following conjecture: *If $A = \{a_s(\mathrm{mod}\ n_s)\}_{s=1}^k$ $(k > 1)$ 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 $A = \{a_s(\mathrm{mod}\ n_s)\}_{s=1}^k$ 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! □

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 $[n_1, \dots, n_k] = \prod_{t=1}^r p_t^{\alpha_t}$, where $p_1 < \cdots < p_r$ are distinct primes and $\alpha_1, \dots, \alpha_r$ 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.

The following conjecture extends the conjecture of P. Erdős to disjoint covers of groups.

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 $G_1, \dots, G_k$. Then the indices $n_1 = [G : G_1], \dots, n_k = [G : G_k]$ 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 $\mathcal{A}=\{a_iG_i\}_{i=1}^k$ 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 indices*

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

each occurs at most $M\in\mathbb{Z}^+$ times. Let p_* and p^* be the smallest and the largest prime divisors of $N=[n_1,\dots,n_k]$ respectively. Suppose that all the G_i with $n_i\geqslant p^*$ are subnormal in G, or G/H is a solvable group having a normal Sylow p'-subgroup where H is the core $(\bigcap_{i=1}^k G_i)_G$ and p' is the greatest prime divisor of $|G/H|$. Then we have the following (i)–(iv) *with the O-constants absolute.*

(i) *$M\geqslant p_*$, moreover among the k indices $n_1,\dots,n_k$ there exists a multiple of p^* occurring at least $1+\lfloor p^*\prod_{p\mid N}(p-1)/p\rfloor\geqslant p_*$ times.*

(ii) *All prime divisors of $n_1,\dots,n_k$ are smaller than $e^\gamma M\log M+O(M\log\log M)$.*

(iii) *The number of distinct prime divisors of $n_1,\dots,n_k$ does not exceed $e^\gamma M+O(M/\log M)$.*

(iv) *For the least index, $\log n_1\leqslant\frac{e^\gamma}{\log 2}M\log^2 M+O(M\log M\log\log M)$.*

The above theorem 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*

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

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

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

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 $|\bigcup_{i=1}0(\text{mod } n_i)\cap\{0,1,\ldots,N-1\}|$ 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*

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

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

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*

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

By making use of the above two theorems we can deduce the following lemma which plays an important role in the proof of Sun's result.

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*

$$q < e^{\gamma} M \log M + O(M \log\log M) \quad \textit{and} \quad \pi(q) \leqslant e^{\gamma} M + O(M/\log M).$$

where $\pi(q)$ is the number of primes not exceeding q and the O-constants are absolute.

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 $k = 2$. Recently, W.-J. Zhu [Int. J. Mod. Math. 3(2008), no. 2] 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 $k \leqslant 20$.