组合数论最新进展

孙智伟 (Zhi-Wei Sun) (南京大学数学系)

E-mail: zwsun@nju.edu.cn

Home Page: http://pweb.nju.edu.cn/zwsun

摘要


(I) 零和问题：对加法 Abel 群 \(G\) 中元序列 \(\{a_i\}_{i=1}^n\) 是否有 \(I \subseteq \{1, \cdots, n\}\) 使得 \(|I|\) 符合指定要求且 \(\sum_{i \in I} a_i = 0\)？

(II) 子集和问题：给定加法 Abel 群 \(G\) 或整数环 \(\mathbb{Z}\) 的有穷子集 \(A_1, \cdots, A_n\)，如何估计受限制子集和

\[ S = \{a_1 + \cdots + a_n : a_i \in A_i, \text{ 且 } a_1, \cdots, a_n\text{ 满足给定限制条件}\} \]

的基数下界？

(III) 覆盖问题：整数环 \(\mathbb{Z}\) 的覆盖 \(A = \{a_i + n_i \mathbb{Z}\}_{i=1}^k\) (由 \(k\) 个剩余类构成) 中模 \(n_1, \cdots, n_k\) 应具有怎样的特性？更一般地，对于群 \(G\) 的左陪集覆盖 \(A = \{a_iG_i\}_{i=1}^k\)，指标 \(n_1 = [G : G_1], \cdots, n_k = [G : G_k]\) 满足什么规律？
1. 零和问题


定理 1.1. 任给正整数 $n$ 及长为 $2n - 1$ 的整数列 $\{a_i\}_{i=1}^{2n-1}$，必有 $I \subseteq \{1, \ldots, 2n - 1\}$ 使得 $|I| = n$ 且 $\sum_{i \in I} a_i \equiv 0 \pmod{n}$。

上述 EGZ 定理是零和理论的第一项开创性工作，其影响极其深远。容易将 EGZ 定理化归为 $n$ 是素数 $p$ 的情形，注意剩余类环 $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ 是 $p$ 元有限域。


EGZ 定理可从下述著名结果方便地导出。

定理 1.2 (Chevalley-Warning 定理). 设 $F$ 是 $p^n$ 元有限域，其中 $p$ 为素数，$\alpha$ 为正整数。又设 $f_1(x_1, \cdots, x_n), \cdots, f_m(x_1, \cdots, x_n) \in F[x_1, \cdots, x_n]$，

$$Z(f_1, \cdots, f_m) = \{(x_1, \cdots, x_n) \in F^n: f_1(x_1, \cdots, x_n) = \cdots = f_m(x_1, \cdots, x_n) = 0\}.$$

如果 $\sum_{i=1}^{m} \deg f_i < n$，则 $|Z(f_1, \cdots, f_m)|$ 是 $p$ 的倍数。

$n$ 为素数 $p$ 时 EGZ 定理的证明：设 $a_1, \cdots, a_{2p-1}$ 属于 $p$ 元域 $F = \mathbb{Z}/p\mathbb{Z}$。令

$$f_1(x_1, \cdots, x_{2p-1}) = \sum_{i=1}^{2p-1} x_i^{2p-1}, \quad f_2(x_1, \cdots, x_{2p-1}) = \sum_{i=1}^{2p-1} a_i x_i^{2p-1}.$$

显然 $\deg f_1 + \deg f_2 = 2p - 2 < 2p - 1$，而 $(0, \cdots, 0) \in Z(f_1, f_2)$。依 Chevalley-Warning 定理，有不全为 0 的 $x_1, \cdots, x_{2p-1} \in F$ 使得 $(x_1, \cdots, x_{2p-1}) \in$
下述结果在 $G = \mathbb{Z}/p\mathbb{Z}$ ($p$ 为素数) 时首先由年高维东 [J. Number Theory, 56(1996)] 通过提炼他的初等方法得到，一般形式由刘建新，孙智伟 [南京大学学报，37(2001)] 给出。

定理 1.3. 设 $G$ 为 $n$ 阶加法 Abel 群，$S = \{a_i\}_{i=1}^{2n-1}$ 是 $G$ 中元序列，
对 $a \in G$ 让 $r(S,a)$ 表示将 $a$ 写成 $S$ 中 $n$ 项之和的方法数。如果有
特征为素数 $p$ 的域 $F$ 以 $G$ 为其加法子群，则

$$r(S,a) \equiv \begin{cases} 1 \pmod{p} & \text{当 } a = 0 \text{时}, \\ 0 \pmod{p} & \text{此外}. \end{cases}$$

设 $G$ 为有限 (加法) Abel 群。如果一个 $G$ 中元序列的各项之
和为零，就说它是个零和列。我们以 $s(G)$ 表示满足下条件的最
小正整数 $k$：长为 $k$ 的 $G$ 中元序列必含长为 $|G|$ 的零和子列。 $n$
阶循环群 $C_n$ 同构于加法群 $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{\bar{a} = a + n\mathbb{Z} : a \in \mathbb{Z}\}$，而由
$n-1$ 个 $\bar{0}$ 与 $n-1$ 个 $\bar{1}$ 组成的长为 $2n-2$ 的序列不含零和子列，
故由 EGZ 定理知 $s(C_n) = s(\mathbb{Z}_n) = 2n-1$.

设 $G$ 为有限 (加法) Abel 群，Davenport 常数 $D(G)$ 是具有下述性质的最小正整数 $l$：任给长为 $l$ 的 $G$ 中元序列 $\{a_i\}_{i=1}^l$，必有
$0 \neq I \subseteq \{1, \cdots, l\}$ 使得 $\sum_{i \in I} a_i = 0$. $l = |G|$ 时，由于诸 $s_k = \sum_{0 < i \leq k} a_i$ ($k = 0, 1, \cdots, l$) 中必有两个相等（依抽屉原理），$\{a_i\}_{i=1}^l$ 的若干相继项之和为零。可见 $D(G)$ 存在且 $D(G) \leq |G|$. $0 < l < n$ 个 $\bar{1} = 1 + n\mathbb{Z}$ 之和不等于 $\bar{0}$，故 $D(C_n) = D(\mathbb{Z}_n) = n$.

1996 年高维东 [J. Number Theory, 56(1996)] 证明了下述基本关系式：
定理 1.4. 设 $G$ 为有限阶 Abel 群，则 $s(G) - D(G) = |G| - 1$.

对于 $n$ 阶非循环的 Abel 群 $G$, R. B. Eggleton 与 Erdös [Acta Arith. 21(1972)] 证明了 $D(G) \leq \frac{n}{2} + 1$, 从而 $s(G) \leq \frac{3}{4} n$. N. Alon 指出仅当 $G$ 形如 $\mathbb{Z}_2 \oplus \mathbb{Z}_{2m}$ 时 $s(G) = \frac{3}{4} n$.

设 $G$ 为一般的有限加法群（未必可换）。对于 $G$ 中元序列 $S = \{a_i\}^k_{i=1}$，如果存在 $\{1, \cdots , k\}$ 上置换 $\sigma$ 使得 $\sum_{i=1}^k a_{\sigma(i)} = 0$，就说 $S$ 是个零和列。我们也可定义 $s(G)$ 与 $D(G)$. 1976 年 J. E. Olson [J. Number Theory, 8(1976)] 把 EGZ 定理推广到任意有限群 $G$ 上，即证明了 $s(G) \leq 2|G| - 1$.

EGZ 定理还可推广成

定理 1.5. 任给正整数 $n$ 及其正因子 $d$, 对整数列 $\{a_i\}^n_{i=1}$，必有 $I \subseteq \{1, \cdots , n + d - 1\}$ 使得 $|I| = n$ 且 $\sum_{i \in I} a_i \equiv 0 \pmod{d}$.

比定理 5 更一般的下述猜想至今尚未解决。

猜想 1.1. 设 $\{a_i\}_{i=1}^n$ 为整数列且 $\sum_{i=1}^n a_i \equiv 0 \pmod{m}$, 则长为 $m + n - 1$ 的整数列 $\{b_j\}_{j=1}^n$ 必有长为 $n$ 的子序列 $\{b_{j_k}\}_{k=1}^n$ 适合 $\sum_{i=1}^n a_i b_{j_k} \equiv 0 \pmod{m}$.

显然 $m \mid n$ 且 $a_1 = \cdots = a_n = 1$ 时上猜想退化为定理 5, Alon, A. Bialostocki 与 Y. Caro 证明了 $m$ 为素数时猜想正确。

1983 年 A. Kemnitz 提出下述猜想。

猜想 1.2. 任给 $a_1, \cdots , a_{4n-3} \in \mathbb{Z}_n \oplus \mathbb{Z}_n$, 必有 $I \subseteq \{1, \cdots , 4n - 3\}$ 使得 $|I| = n$ 且 $\sum_{i \in I} a_i = 0$.

上述 $4n - 3$ 不能换成 $4n - 4$, 因为由 $(0,0),(0,1),(1,0),(1,1)$ 各重复 $n - 1$ 次组成的序列没有长为 $n$ 的零和子列。
2000年L. Rónya [Combinatorica, 20(2000)]取得了重要突破，他创造了新方法证明了

**定理 1.6.** 猜想 1.2 中 $4n-3$ 换成 $\lfloor \frac{n}{4} \rfloor$ 时结论正确，$n$ 为素数时 $4n-3$ 还可换为 $4n-2$。

Rónya 得到上述定理的关键性引理如下：

**引理 1.1.** 设 $F$ 为域，$n$ 为正整数。以 $V$ 表示全体从 $\{0,1\}^m$ 到 $F$ 的函数所构成的 $F$ 上线形空间，则 $V$ 有组基底

$$f_I(x_1, \cdots, x_n) = \prod_{i \in I} x_i \quad (I \subseteq \{1, \cdots, n\}).$$

### 2. 子集和问题

设 $G$ 为加法 Abel 群，$A_1, \ldots, A_n$ 为其有穷非空子集。我们称

$$A_1 + \cdots + A_n = \{a_1 + \cdots + a_n : a_i \in A_i, \ldots, a_n \in A_n\}$$

为子集 $A_1, \ldots, A_n$ 的和集，$A_1 = \cdots = A_n = A$ 时把这个和集简记为 $nA$。

假设 $G$ 为无挠加法 Abel 群，$A_1, \ldots, A_n$ 为其有穷非空子集，则由有限集 $A = \bigcup_{i=1}^n A_i$ 生成的子群同构于某个 $Z^n$。设 $G = Z^n, S = A_1 + \cdots + A_n, X = \max_{x \in S} \max_{1 \leq i \leq n} |x_i|$, 则 $Z^n$ 到 $Z$ 的群同态 $f(x_1, \cdots, x_n) = \sum_{i=1}^n x_i(2X+1)^{i-1}$ 把 $S$ 中不同元映到 $Z$ 中不同元。因此无挠加法 Abel 群中子集和问题可归约为整数环 $Z$ 的子集和问题。

由于 $Z$ 中元可排序，用构造性方法不难证明

**定理 2.1.** 设 $A$ 与 $B$ 是 $Z$ 的有穷非空子集，则

$$|A + B| \geq |A| + |B| - 1,$$
且等号成立当且仅当 $A$ 与 $B$ 是具有相同公差的算术级数。

关于域上子集和，我们有下述著名的 Cauchy-Davenport 定理。

**定理 2.2.** 设 $F$ 是特征为素数 $p$ 的域，$A$ 与 $B$ 是 $F$ 的有穷非空子集，则

$$|A + B| \geq \min\{|p, |A| + |B| - 1|.$$  

Cauchy-Davenport 定理中等号成立的充要条件是什么？1956 年 A. G. Vosper 解决了这一问题。

**定理 2.3.** 设 $p$ 为素数，$A, B$ 是 $F = \mathbb{Z}/p\mathbb{Z}$ 的非空子集，$A + B \neq F$，则

$$|A + B| = |A| + |B| - 1$$

当且仅当下面的 (i)-(iii) 之一成立：

(i) $\min\{|A|, |B|\} = 1$;

(ii) 存在 $c \in F$ 使得 $c - A = F \setminus B$;

(iii) $A, B$ 是有相同公差的算术级数。

M. Kneser [Math. Zeit. 58(1953)] 对 Cauchy-Davenport 定理作出了下述重要推广：

**定理 2.4.** 设 $G$ 为 Abel 群，$A$ 与 $B$ 为它的有穷非空子集，$H$ 表示子群 $\{g \in G : g + A + B = A + B\}$，则

$$|A + B| \geq |A + H| + |B + H| - |H|.$$  

在上定理中取 $G$ 为素数阶循环群 $\mathbb{Z}/p\mathbb{Z}$ 即得 Cauchy-Davenport 定理（因为 $|A + B| < |G|$ 时 $H \neq G$ 从而 $|H| = 1$)。
设 $G$ 为加法 Abel 群，$A_1, \ldots, A_n$ 为其有穷非空子集。我们称

$$A_1 \land \cdots \land A_n = \{a_1 + \cdots + a_n : a_i \in A_i, 诸 a_i 两两不同\}$$

为子集 $A_1, \ldots, A_n$ 的异元和集。$A_1 = \cdots = A_n = A$ 时把这异元和集简记为 $n^A$.


**定理 2.5.** 设 $A$ 为 $\mathbb{Z}$ 的有穷非空子集，则

$$|n^A| \geq n(|A| - n) + 1,$$

且等号成立当且仅当 $n \in \{1, |A| - 1\}$，或 $A$ 为算术级数，或者 $n = 2$ 且 $A$ 可表成 $\{a_1, a_2, a_3, a_4\}$，其中 $a_1 < a_2 < a_3 < a_4$ 且 $a_4 - a_3 = a_2 - a_1$。


**定理 2.6.** 设 $F$ 是特征为素数 $p$ 的域，$A$ 是 $F$ 的有穷非空子集，则

$$|n^A| \geq \min\{p, n|A| - n^2 + 1\},$$

定理 2.6 蕴涵着下述重要结果:

**定理 2.7.** 设 $p$ 为素数，$A \subseteq \mathbb{Z}_p$ 且 $|A| > \lfloor \sqrt{4p-7} \rfloor$ 则 $\mathbb{Z}_p$ 中每个元都可表成 $A$ 中 $\lfloor |A| / 2 \rfloor$ 不同元之和.

定理 2.8. 设 $F$ 是特征为素数 $p$ 的域，$A_1, \cdots, A_n$ 是 $F$ 的有穷子集且 $0 < |A_1| < \cdots < |A_n|$. 则

$$|A_1 \cap \cdots \cap A_n| \geq \min \left\{ p, \sum_{i=1}^{n} |A_i| - \frac{n(n+1)}{2} + 1 \right\}.$$  

1998年曹惠琴、孙智伟 [Acta Arith. 87(1998)] 利用归纳法构造性地证明了

定理 2.9. 设 $A_1, \cdots, A_n$ 是 $\mathbb{Z}$ 的有穷子集且 $0 < |A_1| < \cdots < |A_n|$. 则

$$|A_1 \cap \cdots \cap A_n| \geq 1 + \sum_{i=1}^{n} (|A_i| - i).$$

如果等号成立，则 $m = n$ 或 $|A_m| < |A_{m+1}| - 1$ 时有 $\bigcup_{i=1}^{m} A_i = A_m$, 且 $A_n = \bigcup_{i=1}^{m} A_i$ 为算术级数除非 $n = 1$ 或 $|A_1| \leq 3$.

2001年孙智伟 [Acta Arith. 99(2001), 41-60] 证明了下述一般性结果:

定理 2.10. 设 $A_1, \cdots, A_n$ 是 $\mathbb{Z}$ 的有穷子集，$|A_i| \geq i$ ($i = 1, \cdots, n$) 且 $|A_1| \leq \cdots \leq |A_n|$. 则

$$(*) \quad |A_1 \cap \cdots \cap A_n| \geq 1 + \sum_{i=1}^{n} \min_{i \leq j \leq n} (|A_j| - j).$$

如果等号成立，则对

$$M = \{1 \leq i \leq n : i < j \leq n \text{ 时 } |A_i| - i < |A_j| - j \}$$

中元 $m$ 有 $\bigcup_{i=1}^{m} A_i = A_m$, 而且 $|A_i| > i$ ($i = 1, \cdots, n$) 时 $A_n = \bigcup_{i=1}^{m} A_i$ 为算术级数除非出现下述三种情况:
(i) \( n = 1 \) 或 \( |A_n| = n + 1 \);

(ii) \( n = 2 \) 且 \( |A_1| \in \{3, 4\} \) 且 \( A_2 \) 可表为 \( \{a_1, \cdots, a_4\} \); 这儿 \( a_1 < a_2 < a_3 < a_4 \) 且 \( a_4 - a_3 = a_2 - a_1 \);

(iii) \( n > 1 \) 且 \( |A_{n-1}| = n \) 且 \( A_n \setminus A_{n-1} \) 是有相同公差的算术级数。

此定理加上孙智伟的下述猜测将完整地解决 (a) 何时取等号的问题。

**猜测 2.1.** 设 \( A_1, \cdots, A_n \) 是 \( \mathbb{Z} \) 的有限子集，
\( k_i = |A_i| \geq i \) (\( i = 1, \cdots, n \)), \( |A_1| \leq \cdots \leq |A_n| \), \( m \in M \) 时 \( \bigcup_{i=1}^{m} A_i = A_m \)。假定 \( A_n = [0, k_n - 1] \), 尽管 \( A_{n-1} \) 与 \( A_n \setminus A_{n-1} \) 是有相同公差的算术级数，

随着 \( n \rightarrow \infty \) 且 \( (\ast) \) 中等号成立，则对一切 \( m \in M \) 都有 \( A_m = [0, k_m - 1] \), 除非 \( M = \{1, n\} \), \( k_n - k_1 = n \) 且 \( A_1 = [0, k_1] \setminus \{k_1 - 1\} \).

最近庞伟、孙智伟已证实了这一猜测。


**定理 2.11.** 设 \( A_1, \cdots, A_n \) 是 \( \mathbb{Z} \) 的有限子集，集合 \( V \) 中元都是这样的五元组 \( (s, t, \mu, \nu, w) \), 其中 \( 1 \leq s, t \leq n \), \( s \neq t \), \( \mu, \nu, w \in \mathbb{Z} \) 且 \( \mu \nu \neq 0 \). 让

\[
C = \{a_1 + \cdots + a_n : a_i \in A_i, \ (i, j, \mu, \nu, w) \in V \text{ 且 } \mu a_i + \nu a_j \neq w\}.
\]

如果每个 \( V_i = \{(s, t, \mu, \nu, w) \in V : i \in \{s, t\}\} \) 基数都小于 \( |A_i| \), 则

\[
|C| \geq \sum_{i=1}^{n} |A_i| - 2|V| - n + 1 = 1 + \sum_{i=1}^{n} (|A_i| - |V_i| - 1) > 0.
\]

侯庆虎、孙智伟 [Acta Arith., 102(2002)] 证明了

**定理 2.12.** 设 \( k, m \geq 0 \) 及 \( n > 0 \) 为整数。又设 \( F \) 是特征为素数 \( p \) 的域，这儿 \( p/n > \max\{m, k + m - mn - 1\} \). 假如 \( A_1, \cdots, A_n \) 都是 \( F \) 的
$k$ 元子集，$1 \leq i, j \leq n$ 且 $i \neq j$ 时，$S_{ij} \subseteq F$ 且 $|S_{ij}| \leq m$。则

$$C = \{a_1 + \cdots + a_n : a_1 \in A_1, \cdots, a_n \in A_n, \text{ 且 } i \neq j \text{ 时 } a_i - a_j \not\in S_{ij}\}$$

的基数至少为 $(k + m - mn - 1)n + 1$。

刘建新、孙智伟 [J. Number Theory, 2002] 最近又研究了多项式限制下的和集，获得了下述结果：

**定理 2.13.** 设 $F$ 是特征为素数 $p$ 的域，多项式 $P(x) \in F[x]$ 次数为 $m > 0$. 由设 $A_1, \cdots, A_n$ 是 $F$ 的有穷子集，$|A_k| = k > m(n - 1)$ 且 $i < n$ 时 $|A_{i+1}| - |A_i| \in \{0, 1\}$. 如果 $p > (k - 1)n - (m + 1)\binom{n}{2}$, 则对受限制和集

$$C = \{a_1 + \cdots + a_n : a_1 \in A_1, \cdots, a_n \in A_n, \text{ 且 } i \neq j \text{ 时 } P(a_i) \neq P(a_j)\}$$

有 $|C| \geq 1 + (k - 1)n - (m + 1)\binom{n}{2}$.

定理 2.12, 2.13 证明的关键在于确定某种多元多项式中特定项的系数。

**定理 2.14.** 设 $k, m, n$ 为正整数且 $k > m(n - 1)$. 则

(i) 多项式

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

中 $x_1^{k-1} \cdots x_n^{k-1}$ 项系数为

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

(ii) 多项式

$$\prod_{1 \leq i < j \leq n} (x_i^m - x_j^m)(x_1 + \cdots + x_n)^{(k - 1)n - (m + 1)\frac{n(n - 1)}{2}}$$
中 \( x_1^n \cdots x_{n-1}^{n-1} \) 项系数为

\[
1! \cdots (n-1)!(-1)^{\frac{m(n-1)}{2}} \frac{((k-1)n - (m+1)n(n-1))!}{(k-1)!(k-1-m)\cdots (k-1-(n-1)m)!}.
\]


定理 2.15. 以 \( p_F \) 表示域 \( F \) 的特征，但 \( F \) 的特征为 0 时让 \( p_F = +\infty \)。设 \( A \) 与 \( B \) 为域 \( F \) 的有限非空子集，\( P(x,y) \in F[x,y] \) 且 \( P(x,y) - y^{\deg P} P^*(x/y) \) 次数小于 \( \deg P \)，这儿 \( P^*(x) \in F[x] \)。假定有 \( i < |A| \) 及 \( j < |B| \) 适合 \( [x^i y^{\deg P-i}]P(x,y) \neq 0 \neq [x^{\deg P-j}]P(x,y) \)。则

\[
[a + b: \ a \in A, \ b \in B \ & \ P(a, b) \neq 0] \\
\geq \min\{p_F - \ord_x + 1 P^*(x), \ |A| + |B| - 1 - \deg P - N(P^*)\},
\]

这儿

\[
N(P^*) = \max_{q \in \mathbb{P}(p_F)} \{\{a \in F: \ a \neq 0, -1 \ \text{且} \ \ord_{x-a} P^*(x) \geq q\}\},
\]

其中 \( F \) 表示域 \( F \) 的代数闭包，\( \mathbb{P}(p_F) \) 在 \( p_F < \infty \) 时为 \( \{1, p, p^2, \cdots\} \)，在 \( p_F = \infty \) 时为 \( \{1\} \)。

下述猜想近来格外引人注目，一般循环群的情形已被 S. Das-gupta, G. Károlyi, O. Serra, B. Szegedy [Israel J. Math. 126(2001)] 所解决。

猜测 2.2 [H. S. Snevily, Amer. Math. Monthly, 106(1999)]。对奇数阶加法

\(\text{Abel} \) 群的两个 \( k \) 元子集 \( A \) 与 \( B \)，存在 \( A \) 与 \( B \) 中元素的列举使对

应元之和两两不同。
3. 覆盖问题

让 $\mathbb{N} = \{0, 1, 2, \cdots \}$, $\mathbb{Z}^+ = \mathbb{N} \setminus \{0\}$. 对 $a \in \mathbb{Z}$ 与 $n \in \mathbb{Z}^+$ 我们称

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

是一个模为 $n$ 的剩余类或公差为 $n$ 的算术序列. 对于有限个剩余类构成的系

$$A = \{ a_s(n_s) \}_{s=1}^k,$$

如果每个整数都属于 $A$ 中某个剩余类，则称 $A$ 为 $\mathbb{Z}$ 的覆盖. $A$ 的覆盖函数

$$w_A(x) = |\{ 1 \leq s \leq k : x \in a_s(n_s) \}|$$

显然具有周期 $N = [n_1, \cdots, n_k]$. 覆盖函数 $w_A(x)$ 在一个周期内的算术平均为

$$\frac{1}{N} \sum_{x=0}^{N-1} w_A(x) = \frac{1}{N} \sum_{x=0}^{N-1} \sum_{s=1}^k \frac{1}{n_s} = \sum_{s=1}^k \frac{1}{N} \sum_{x=0}^{N-1} \frac{1}{n_s} = \sum_{s=1}^k \frac{1}{n_s}.$$

因此 $A$ 为 $m$- 覆盖 (即恒有 $w_A(x) \geq m$) 时 $\sum_{s=1}^k \frac{1}{n_s} \geq m; A$ 为恰好 $m$- 覆盖 (即恒有 $w_A(x) = m$) 时 $\sum_{s=1}^k \frac{1}{n_s} = m$.

**定理 3.1.** (i) [张明志，四川大学学报，1989] 如果 $A = \{ a_s(n_s) \}_{s=1}^k$ 为 $\mathbb{Z}$ 的覆盖，则

$$\text{(3.1)} \exists I \subseteq \{1, \cdots, k\} \text{使得} \sum_{s \in I} \frac{1}{n_s} \in \mathbb{Z}^+.$$

(ii) [孙智伟，Trans. Amer. Math. Soc., 348(1996)] 如果 $A = \{ a_s(n_s) \}_{s=1}^k$ 为 $\mathbb{Z}$ 的 $m$- 覆盖，即对任正整数 $m_1, \cdots, m_k$ 都有至少 $m$ 个正整数形如 $\sum_{s \in I} \frac{m_s}{n_s}$，其中 $I \subseteq \{1, \cdots, k\}$. 
(iii) [孙智伟， Proc. Amer. Math. Soc., 127(1999)] 设 \( A = \{a_s(n_s)\}_{s=1}^k \) 为 
\( m \)- 覆盖， \( J \subseteq \{1, \cdots, k\} \). 则对任何整数 \( m_1, \cdots, m_k \) 都有

\[
(3.2) \quad \left| \left\{ I \subseteq \{1, \cdots, k\} : I \neq J \text{且} \sum_{s \in I} \frac{m_s}{n_s} - \sum_{s \in J} \frac{m_s}{n_s} \in \mathbb{Z} \right\} \right| \geq m.
\]

上述 (ii) 与 (iii) 从不同角度推广了 (i).

对 \( \alpha \in \mathbb{R} \) 及 \( \beta > 0 \) 让 \( \alpha + \beta \mathbb{Z} = \{ \alpha + \beta x : x \in \mathbb{Z} \} \). 代替剩余类系我们可考虑更一般的

\[
(3.3) \quad A = \{ \alpha_s + \beta_s \mathbb{Z}\}_{s=1}^k.
\]

通过创造一种综合使用线性代数、分析、Stirling 数的新方法，
孙智伟首次对一般的覆盖进行了特征刻画。

**定理 3.2** [孙智伟， Acta Arith., 72(1995)]. 关于 (3.3)，下述几条等价:

(a) (3.3) 是 \( \mathbb{Z} \) 的 \( m \)- 覆盖。

(b) (3.3) 覆盖连续 \( |S(A)| \) 个整数至少 \( m \) 次，这儿

\[
(3.4) \quad S(A) = \left\{ \left. \left\{ \sum_{s \in I} \frac{1}{\beta_s} \right\} : I \subseteq \{1, \cdots, k\} \right\}.
\]

(c) 对任何 \( \theta \in [0,1) \) 及 \( n = 0, 1, \cdots, m - 1 \)，都有

\[
(3.5) \quad \sum_{\{I \subseteq \{1, \cdots, k\} : \sum_{s \in I} 1/\beta_s = \theta, \sum_{s \in I} a_s/\beta_s \}} (-1)^{\left| I \right|} \left( \sum_{s \in I} 1/\beta_s \right)^n e^{2\pi i \sum_{s \in I} a_s/\beta_s} = 0.
\]

注意 \( |S(A)| \leq 2^k \) 依赖于那些 \( \beta_s \)！因此，(b) \( \Rightarrow \) (a) 给出比下述 Erdös 猜想更详细的信息。

(3.6) \quad A = \{a_s(n_s)\}_{s=1}^k \) 覆盖 \( 1 \) 至 \( 2^k \) 时便覆盖全体整数.
定理 3.3. 设 $A = \{a_s(n_s)\}$ 为 $Z$ 的 $m$- 覆盖.

(i) [孙智伟， Trans. Amer. Math. Soc. 348(1996)] 假如

$$n_1 \leq \cdots \leq n_{k-l} < n_{k-l+1} = \cdots = n_k \ (0 \leq l < k),$$

则

$$l \geq \frac{n_k}{n_{k-l}} - 1, \text{ 或者 } \sum_{s=1}^{k-l} \frac{1}{n_s} \geq m \text{ 从而 } \sum_{s=1}^{k} \frac{1}{n_s} \geq m + \frac{1}{n_k} > m. \tag{3.7}$$

(ii) [孙智伟， Trans. Amer. Math. Soc. 348(1996)] 如果 $\{a_s(n_s)\}_{s \in \mathcal{A}}$ 不再为 $m$- 覆盖，则对任何 $a \in Z$ 存在 $I, J \subseteq \{1, \cdots, k\}$ 使得

$$\frac{a}{n_l} \equiv \sum_{s \in I} \frac{1}{n_s} - \sum_{s \in J} \frac{1}{n_l} \quad (\text{mod } 1). \tag{3.8}$$

(iii) [孙智伟， Proc. Amer. Math. Soc. 127(1999)] 假如 $A$ 为极小 $m$- 覆盖 (即 $A$ 的真子系不再是 $m$- 覆盖), 则对每个 $t = 1, \cdots, k$ 都存在 $\alpha_t \in [0,1)$ 使得

$$S_t(A) = \left\{ \left( \sum_{s \in I} \frac{1}{n_s} \right) : I \subseteq \{1, \cdots, k\} \setminus \{t\}, \ \left[ \sum_{s \in I} \frac{1}{n_s} \right] \geq m - 1 \right\} \tag{3.9}$$

包含

$$\left\{ \frac{\alpha_t + r}{n_t} : r = 0, 1, \cdots, n_t - 1 \right\}. \tag{3.10}$$
上述 (i) 改进了著名的 Davenport-Mirsky-Newman-Rado 定理：如果 \( t = 1 \) 则 \( \sum_{s=1}^{k} 1/n_s > 1 \) (即 \( A \) 不是不相交覆盖)，(ii) 表明 \( m \)-覆盖与差集有关，(iii) 表明 \( A \) 是极小 \( m \)-覆盖时对 \( t = 1, \ldots, k \) 集合

\[
(3.12) \quad \left\{ \left\{ \sum_{s \in I} \frac{1}{n_s} \right\} : I \subseteq \{1, \ldots, k\} \setminus \{t\} \right\}
\]

包含长为 \( n_t \) 公差为 \( 1/n_t \) 的算术级数。

猜想 3.1 (孙智伟)．设 \( A = \{a_s(n_s)\}_{s=1}^{k} \) 是极小 \( m \)-覆盖，

(i) 存在链 \( \emptyset \neq I_1 \subset \cdots \subset I_m \subseteq \{1, \ldots, k\} \) 使得

\[
(3.13) \quad \text{对 } t = 1, \ldots, m \text{ 有 } \sum_{s \in I_t} \frac{1}{n_s} \in \mathbb{Z}.
\]

(ii) 让

\[
(3.14) \quad S(A) = \left\{ \left\{ \sum_{s \in I} \frac{1}{n_s} \right\} : I \subseteq \{1, \ldots, k\} \right\},
\]

则

\[
(3.15) \quad |S(A)| \leq n_1 + \cdots + n_k, \text{ 且 } \frac{1}{d} \in S(A) \text{ 时 } S(A) \supseteq \left\{ \frac{r}{d} : 0 \leq r < d \right\}.
\]

张明志 [四川大学学报，1991] 用图论方法证明存在恰好 \( m \)-覆盖使其真子系不为恰好 \( n \)-覆盖 \((0 < n < m)\)。 孙智伟 [Acta Arith.，81(1997)] 用好几种方式刻划了恰好 \( m \)-覆盖。由这些刻划他导出了恰好 \( m \)-覆盖中模的一些深刻性质。

定理 3.4 [孙智伟， Acta Arith.，1995, 1997]．设 \( A = \{a_s(n_s)\}_{s=1}^{k} \) 为恰好 \( m \)-覆盖。

(i) 对任何 \( \emptyset \neq J \subset \{1, \ldots, k\} \),

\[
(3.16) \quad \text{有 } I \subseteq \{1, \ldots, k\} \text{ 使得 } I \neq J \text{ 且 } \sum_{s \in I} \frac{1}{n_s} = \sum_{s \in J} \frac{1}{n_s}.
\]
(ii) 对 $a=0,1,2,\cdots$ 及 $t=1,\cdots,k$ 有

$$
\left| \left\{ I \subseteq \{1,\cdots,k\} : t \not\in I \& \sum_{s \in I^{c}} \frac{1}{n_{s}} = \frac{a}{n_{t}} \right\} \right| \geq \binom{m-1}{\lceil a/n_{t} \rceil},
$$

这儿下界是最好的.

(iii) 如果 $0 \neq I \subseteq \{1,\cdots,k\}$ 且 $s,t \in I$ 时 $(n_{s},n_{t}) | a_{s}-a_{t}$，则

$$
\left\{ \left\{ \sum_{s \in I^{c}} \frac{1}{n_{s}} \right\} : J \subseteq I \right\} \supseteq \left\{ \left\{ \frac{r}{n_{j}} \right\} : 0 \leq r < [n_{j}]_{s \in I} \right\},
$$

其中 $I = \{1,\cdots,k\} \setminus J$ 且 $[n_{j}]_{s \in I}$ 表示诸 $n_{s} (s \in I)$ 的最小公倍数. 对 $r = 0,1,\cdots,[n_{j}]_{s \in I} - 1$，还有

$$
\left| \left\{ J \subseteq I : \left\{ \sum_{s \in I^{c}} \frac{1}{n_{s}} \right\} = \frac{r}{n_{j}} \right\} \right| \geq \frac{n_{j}}{\prod_{s \in I} n_{s}}.
$$

(iv) 下述方程

$$
\sum_{s=1}^{k} \frac{x_{s}}{n_{s}} = c \quad (\text{其中 } x_{s} \in \mathbb{Z} \text{ 且 } 0 \leq x_{s} < n_{s}).
$$

的解数，在 $c \neq 0,1,2,\cdots$ 时可表为 $n_{1},\cdots,n_{k}$ 的一些（可重复）素因子之和 $c \neq 0,1,2,\cdots$, 在 $c$ 为非负整数 $n$ 时至少是 $(k-n)_{k}$.

下述一般性结果也是很有意思的.

定理 3.5 [孙智伟, Combinatorica, 已录用]. 设正整数 $n_{0}$ 是 $A = \{a_{s}(n_{0})\}_{s=1}^{k}$ 的覆盖函数的周期. 则

(a) $\left\{ \sum_{s \in J} \frac{1}{n_{s}} : J \subseteq \{1,\cdots,k-1\} \right\} \supseteq \{ \frac{x_{s}}{n_{s}} : r = 0,1,\cdots,\frac{a_{s}}{[n_{0} : n_{a}]} - 1 \}$.

(b) 假如 $n_{1} \leq \cdots \leq n_{k-1} < n_{k-1+1} = \cdots = n_{k}$ ($0 < l < k$), 那么对每个正整数 $r < n_{k}/n_{k-1}$，或者 $r \equiv 0 \pmod{n_{k}/(n_{0},n_{k})}$，或者组合数 $(\cdot)$ 可表成 $n_{k}$ 的一些（可重复）素因子之和.

(c) $M(A) = \max_{x \in \mathbb{Z}} w_{A}(x)$ 可表成 $\sum_{s=1}^{k} m_{s}/n_{s}$ 的形式, 这儿 $m_{1},\cdots,m_{k}$ 为正整数.
1960 年左右 P. Erdős 提出下述著名的未解决问题：是否对任意的 \( c > 0 \) 有各模 \( n_1, \ldots, n_k \) 互不相同且都大于 \( c \) 的覆盖 \( A = \{a_s(n_s)\}_{s=1}^k \)?


\[
A = \{a_i G_i\}_{i=1}^k \quad (G_1, \ldots, G_k \text{ 为} G \text{ 的子群}),
\]

他证明了 \( A \) 为 \( G \) 的极小覆盖时诸 \( G_i \) 指标有穷而且 \( [G: \bigcap_{i=1}^k G_i] \leq c_k \), 这儿 \( c_k \) 仅依赖于 \( k \). 1987 年 M. J. Tomkinson [Comm. Algebra, 15(1987)] 进一步证明了可取 \( c_k = k! \), 上界 \( k! \) 是最佳的。孙智伟 [Fund. Math. 134(1990); European J. Math. 22(2001)] 定出了使 \( A \) 为 \( G \) 的恰好 \( m \)- 覆盖，诸 \( G_i \) 次正则且 \( \bigcap_{i=1}^k G_i = H \) 的最小 \( k \) 值。

**Herzog-Schönheim 猜想** [Canad. Math. Bull., 1974]. 设 \( G \) 为群，\( A = \{a_i G_i\}_{i=1}^k \quad (k > 1) \) 为其不相交覆盖（即分划）。则诸指标 \( n_i = [G : G_i] \) 不可能两两不同。

我们发现次正则子群有良好的数论性质。

引理 3.1 [孙智伟, European J. Combin. 22(2001)]. 设 \( G_1, \ldots, G_k \) 都是群 \( G \) 的次正则子群，则

\[
\left[ \frac{G}{\bigcap_{i=1}^k G_i} \right] \leq \prod_{i=1}^k [G : G_i].
\]

利用此引理以及数论、群论、组合中许多工具，最近我们证明了

**定理 3.6** [孙智伟]. 设 \( \{a_i G_i\}_{i=1}^k \quad (k > 1) \) 为群 \( G \) 的均匀覆盖（即它覆盖 \( G \) 中每个元素相同次数），\( G_1, \ldots, G_k \) 在 \( G \) 中次正则且
$n_1 = [G:G_1] \leq \cdots \leq n_k = [G:G_k]$. 则指标 $n_1,\cdots,n_k$ 中必有相同的。

如果每个 $n_i$ 至多重复 $M > 1$ 次，则

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

其中 $\gamma$ 为 Euler 常数，与 $O$ 有关的常数是绝对的。

上结果表明对于次正规子群的均匀覆盖广义 Herzog-Schönheim 猜想成立，而且类似的 Erdős 问题答案否定。