Reported originally on the 8th Confer. on Combin. and the 11th Confer. on Graph Theory (Dalian, 2001)

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

组合数论研究整数环 $\mathbb{Z}$ 或者抽象群 G 的子集或序列的组合性质。我们将介绍以下三个课题方面的进展，它们都有强烈的应用背景（参见 Alford, Granville 和 Pomerance 关于伪素数的著名工作 [Ann. Math. 140(1994)]、1998 年 Fields 奖获得者 W. T. Gowers 在 van der Waerden 定理上的突破性工作以及 P. Erdös 在 2^n+p 型数方面的原创性工作）。

(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 $A=\{a_s+n_s\mathbb{Z}\}_{s=1}^k$ (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 $\mathcal{A}=\{a_iG_i\}_{i=1}^k$, 指标 $n_1=[G:G_1],\cdots,n_k=[G:G_k]$ 满足什么规律？

1. 零和问题

1961 年 P. Erdös, A. Ginzburg 和 A. Ziv [Bull. Res. Council Israel, 10F(1961)] 证明了下述引人注目的新结果：

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 $I \subseteq \{1,\cdots,2n-1\}$ 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。

1980 年以前 EGZ 定理尚不被我国人所知。柯召与孙琦曾猜测有这样的结果， 1983 年单尊 [数学进展， 12(1983)] 用解析方法证明了它， 1985 年高维东 [东北师大学报， 4(1985)] 给出了一个纯初等的证明。

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^α 元有限域, 其中 p 为素数，α 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 $\deg f_1 + \deg f_2 = 2p-2 < 2p-1$, 而且 $(0,\cdots,0)\in Z(f_1,f_2)$. 依 Chevalley-Warning 定理， 有不全为 0 的 $x_1,\cdots,x_{2p-1}\in F$ 使得 $(x_1,\cdots,x_{2p-1}) \in$

$Z(f_1,f_2)$. 让 $I=\{1\leqslant i\leqslant 2p-1\colon x_i\neq 0\}$, 则 $0<|I|<2p$. 因 $\sum_{i=1}^{2p-1}x_i^{p-1}=|I|1=0$，必定 $|I|=p$. 注意 $\sum_{i\in I}a_i=\sum_{i=1}^{2p-1}a_ix_i^{p-1}=0$. □

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 $\mathbb{Z}_n=\mathbb{Z}/n\mathbb{Z}=\{\bar{a}=a+n\mathbb{Z}\colon a\in\mathbb{Z}\}$，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 $\emptyset\neq I\subseteq\{1,\cdots,l\}$ 使得 $\sum_{i\in I}a_i=0$。$l=|G|$ 时，由于诸 $s_k=\sum_{0<i\leqslant k}a_i$ ($k=0,1,\cdots,l$) 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 $D(G)\leqslant|G|$. $0<l<n$ 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, 58(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 $D(G)\leqslant \frac{n}{2}+1$, 从而 $s(G)\leqslant \frac{3}{2}n$. N. Alon 指出仅当 G 形如 $\mathbb{Z}_2\oplus\mathbb{Z}_{2m}$ 时 $s(G)=\frac{3}{2}n$.

设 G 为一般的有限加法群（未必可换）。对于 G 中元序列 $S=\{a_i\}_{i=1}^k$, 如果存在 $\{1,\cdots,k\}$ 上置换 σ 使得 $\sum_{i=1}^n a_{\sigma(i)}=0$，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 $s(G)\leqslant 2|G|-1$.

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 $\{a_i\}_{i=1}^{n+d-1}$, 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 $\{b_j\}_{j=1}^{m+n-1}$ 必有长为 n 的子序列 $\{b_{j_i}\}_{i=1}^n$ 适合 $\sum_{i=1}^n a_ib_{j_i}\equiv 0\pmod m$.

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 $[\frac{41}{10}n]$ 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

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

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

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

为子集 $A_1,\cdots,A_n$ 的和集， $A_1=\cdots=A_n=A$ 时把这和集简记为 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 $\mathbb{Z}^n$. 设 $G=\mathbb{Z}^n$, $S=A_1+\cdots+A_n$, $X=\max_{\vec{x}\in S}\max_{1\leqslant i\leqslant n}|x_i|$, 则 $\mathbb{Z}^n$ 到 $\mathbb{Z}$ 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 $\mathbb{Z}$ 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 $\mathbb{Z}$ 的子集和问题。

由于 $\mathbb{Z}$ 中元可排序，用构造性方法不难证明

定理 2.1. 设 A 与 B 是 $\mathbb{Z}$ 的有穷非空子集，则

$$|A+B|\geqslant|A|+|B|-1,$$

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

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

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) 有 $c\in F$ 使 $c-A=F\setminus B$;

(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

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

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， $A_1,\dots,A_n$ 为其有穷非空子集．我们称

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

为子集 $A_1,\cdots,A_n$ 的异元和集， $A_1=\cdots=A_n=A$ 时把这异元和集简记为 $n\hat{}A$.

1995 年 M. B. Nathanson [Trans. Amer. Math. Soc. 347(1995)] 证明了下述结果：

定理 2.5. 设 A 为 $\mathbb{Z}$ 的有穷非空子集，则

$$|n\hat{}A|\geqslant n(|A|-n)+1,$$

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 $a_4-a_3=a_2-a_1$.

1964 年 P. Erdös 与 H. Heilbronn [Acta Arith. 9(1964)] 提出如下猜测： p 为素数时对有限域 $\mathbb{Z}_p$ 的任一个非空子集 A 均有 $|2\hat{}A|\geqslant\min\{p,2|A|-3\}$. 三十年后这一猜测才被 J. A. Dias da Silva 与 Y. O. Hamidoune [Bull. London Math. Soc. 26(1994)] 彻底证实．他们用群表示论获得了下述推广：

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

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

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 $|A|>[\sqrt{4p-7}]$. 则 $\mathbb{Z}_p$ 中每个元都可表成 A 中 $[|A|/2]$ 不同元之和.

1995 年左右 N. Alon, M. B. Nathanson 及 I. Ruzsa [Amer. Math. Monthly, 102(1995); J. Number Theory, 56(1996)] 创造性地引入域上多元多项式方法来处理此类问题. 他们证明了

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

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

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

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

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 $A_n=\bigcup_{i=1}^{n}A_i$ 为算术级数除非 $n=1$ 或 $|A_1|\leqslant 3$.

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, $|A_i|\geqslant i$ $(i=1,\cdots,n)$ 且 $|A_1|\leqslant\cdots\leqslant|A_n|$. 则

$$(*)\qquad |A_1\wedge\cdots\wedge A_n|\geqslant 1+\sum_{i=1}^{n}\min_{i\leqslant j\leqslant n}(|A_j|-j).$$

如果等号成立, 则对

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

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

(i) $n=1$ 或 $|A_n|=n+1$;

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

(iii) $n>1$, $|A_{n-1}|=n$, 且 A_{n-1} 与 $A_n\setminus A_{n-1}$ 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 (*) 何时取等号的问题。

猜测 2.1. 设 $A_1,\cdots,A_n$ 是 $\mathbb{Z}$ 的有穷子集, $k_i=|A_i|\geqslant i$ $(i=1,\cdots,n)$, $|A_1|\leqslant\cdots\leqslant|A_n|$, $m\in M$ 时 $\bigcup_{i=1}^m A_i=A_m$. 假定 $A_n=[0,k_n-1]$, $\min A_{\min M}+\max A_{\min M}<k_n$, 且 (*) 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 $A_1=[0,k_1]\setminus\{k_1-1\}$.

最近潘颢、孙智伟已证实了这一猜测。

2001 年孙智伟 [Acta Arith. 99(2001), 41-60] 还研究了线性限制子集和问题, 得到如下一般性结果。

定理 2.11. 设 $A_1,\cdots,A_n$ 是 $\mathbb{Z}$ 的有穷子集, 集合 V 中元都是这样的五元组 (s,t,μ,ν,w), 其中 $1\leqslant s,t\leqslant n$, $s\neq t$, $\mu,\nu,w\in\mathbb{Z}$ 且 $\mu\nu\neq0$. 让

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

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

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

侯庆虎、孙智伟 [Acta Arith., 102(2002)] 证明了

定理 2.12. 设 $k,m\geqslant0$ 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， $1 \leqslant i, j \leqslant n$ 且 $i \neq j$ 时， $S_{ij} \subseteq F$ 且 $|S_{ij}| \leqslant m$. 则

$$C = \{a_1 + \cdots + a_n : \ a_1 \in A_1, \cdots, a_n \in A_n, \ i \neq j \text{ 时} a_i - a_j \notin S_{ij}\}$$

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， $|A_n| = k > m(n-1)$ 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 $|C| \geqslant 1 + (k-1)n - (m+1)\binom{n}{2}$.

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

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

中 $x_1^{k-1} \cdots x_n^{k-1}$ 项系数为

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

(ii) 多项式

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

中 $x_1^{k-n}\cdots x_n^{k-1}$ 项系数为

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

最近潘颢、孙智伟 [J. Combin. Theory Ser. A, 2002] 对 $n=2$ 的情形解决了一般多项式限制下的子集和问题，所得结果如下：

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 的有穷非空子集，$P(x,y)\in F[x,y]$ 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 $[x^iy^{\deg P-i}]P(x,y)\neq 0\neq[x^{\deg P-j}y^j]P(x,y)$. 则

$$\begin{aligned}&|\{a+b\colon\ a\in A,\ b\in B\ \&\ P(a,b)\neq 0\}|\\ \geq&\min\{p_F-\mathrm{ord}_{x+1}P^*(x),\ |A|+|B|-1-\deg P-N(P^*)\},\end{aligned}$$

这儿

$$N(P^*)=\max_{q\in\mathcal{P}(p_F)}q|\{\alpha\in\bar{F}\colon\ \alpha\neq 0,-1\text{ 且 }\mathrm{ord}_{x-\alpha}P^*(x)\geq q\}|,$$

其中 $\bar{F}$ 表示域 F 的代数闭包，$\mathcal{P}(p_F)$ 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. Dasgupta, 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 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素之和两两不同。

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

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

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

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

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

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

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

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

(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, 则对任何正整数 $m_1,\cdots,m_k$ 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

$$\left|\left\{I\subseteq\{1,\cdots,k\}:\ I\neq J\ \&\ \sum_{s\in I}\frac{m_s}{n_s}-\sum_{s\in J}\frac{m_s}{n_s}\in\mathbb{Z}\right\}\right|\geqslant m. \tag{3.2}$$

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

$$\mathcal{A}=\{\alpha_s+\beta_s\mathbb{Z}\}_{s=1}^k. \tag{3.3}$$

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划。

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 $|S(\mathcal{A})|$ 个整数至少 m 次，这儿

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

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

$$\sum_{\substack{I\subseteq\{1,\cdots,k\}\\ \{\sum_{s\in I}1/\beta_s\}=\theta}}(-1)^{|I|}\binom{[\sum_{s\in I}1/\beta_s]}{n}e^{2\pi i\sum_{s\in I}\alpha_s/\beta_s}=0. \tag{3.5}$$

注意 $|S(\mathcal{A})|\leqslant 2^k$ 依赖于那些 β_s! 因此，(b)⇒(a) 给出比下述 Erdös 猜想更详细的信息：

$A=\{a_s(n_s)\}_{s=1}^k$ 覆盖1至2^k时便覆盖全体整数. (3.6)

(此猜想由 R.B. Crittenden 与 C.L. Vanden Eynden [Proc. Amer. Math. Soc. **24**(1970)] 首先用很繁杂的方法证得.)

(a) 与 (b) 的等价性表明 x 在长为 $|S(\mathcal{A})|$ 的区间 $[a, a+|S(\mathcal{A})|)$ 上变化时覆盖函数 $w_{\mathcal{A}}(x)$ $(x\in\mathbb{Z})$ 可取到其最小值 $m(A)=\min_{x\in\mathbb{Z}} w_A(x)$。

(a) 与 (c) 的等价性是很有用的, 从它可导出 m-覆盖中模的许多性质.

定理 3.3. 设 $A=\{a_s(n_s)\}$ 为 $\mathbb{Z}$ 的 m-覆盖.

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

$$n_1\leqslant\cdots\leqslant n_{k-l}<n_{k-l+1}=\cdots=n_k\ (0\leqslant l<k), \tag{3.7}$$

则

$$l\geqslant\frac{n_k}{n_{k-l}}>1,\ \text{或者}\ \sum_{s=1}^{k-l}\frac{1}{n_s}\geqslant m\ \text{从而}\ \sum_{s=1}^{k}\frac{1}{n_s}\geqslant m+\frac{1}{n_k}>m. \tag{3.8}$$

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

$$\frac{a}{n_t}\equiv\sum_{s\in I}\frac{1}{n_s}-\sum_{s\in J}\frac{1}{n_t}\pmod 1. \tag{3.9}$$

(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

$$S_t(A)=\left\{\left\{\sum_{s\in I}\frac{1}{n_s}\right\}:I\subseteq\{1,\cdots,k\}\setminus\{t\},\ \left[\sum_{s\in I}\frac{1}{n_s}\right]\geqslant m-1\right\} \tag{3.10}$$

包含

$$\left\{\frac{\alpha_t+r}{n_t}:\ r=0,1,\cdots,n_t-1\right\}. \tag{3.11}$$

上述 (i) 改进了著名的 Davenport-Mirsky-Newman-Rado 定理：如果 $l=1$ 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 $t=1,\cdots,k$ 集合

$$\left\{\left\{\sum_{s\in I}\frac{1}{n_s}\right\}: I\subseteq\{1,\cdots,k\}\setminus\{t\}\right\} \tag{3.12}$$

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 $\emptyset\neq I_1\subset\cdots\subset I_m\subseteq\{1,\cdots,k\}$ 使得

$$\text{对 } t=1,\cdots,m \text{ 有 } \sum_{s\in I_t}\frac{1}{n_s}\in\mathbb{Z}. \tag{3.13}$$

(ii) 让

$$S(A)=\left\{\left\{\sum_{s\in I}\frac{1}{n_s}\right\}: I\subseteq\{1,\cdots,k\}\right\}, \tag{3.14}$$

则

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

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 $\emptyset\neq J\subset\{1,\cdots,k\}$,

$$\text{有}I\subseteq\{1,\cdots,k\}\text{ 使得 } I\neq J\text{且}\sum_{s\in I}\frac{1}{n_s}=\sum_{s\in J}\frac{1}{n_s}. \tag{3.16}$$

(ii) 对 $a=0,1,2,\cdots$ 及 $t=1,\cdots,k$ 有

$$\left|\left\{I\subseteq\{1,\cdots,k\}: t\notin I\ \&\ \sum_{s\in I}\frac{1}{n_s}=\frac{a}{n_t}\right\}\right|\geqslant\binom{m-1}{[a/n_t]},\tag{3.17}$$

这儿下界是最好的.

(iii) 如果 $\emptyset\neq I\subseteq\{1,\cdots,k\}$ 且 $s,t\in I$ 时 $(n_s,n_t)\mid a_s-a_t$，则

$$\left\{\left\{\sum_{s\in J}\frac{1}{n_s}\right\}: J\subseteq\bar{I}\right\}\supseteq\left\{\frac{r}{[n_s]_{s\in I}}:\ 0\leqslant r<[n_s]_{s\in I}\right\},\tag{3.18}$$

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

$$\left|\left\{J\subseteq\bar{I}:\left\{\sum_{s\in J}\frac{1}{n_s}\right\}=\frac{r}{[n_s]_{s\in I}}\right\}\right|\geqslant\frac{\prod_{s\in I}n_s}{[n_s]_{s\in I}}.\tag{3.19}$$

(iv) 下述方程

$$\sum_{s=1}^{k}\frac{x_s}{n_s}=c\ \ (\text{其中 } x_s\in\mathbb{Z}\ \text{且}0\leqslant x_s<n_s).\tag{3.20}$$

的解数，在 $c\neq0,1,2,\cdots$ 时可表为 $n_1,\cdots,n_k$ 的一些（可重复）素因子之和 $c\neq0,1,2,\cdots$，在 c 为非负整数 n 时至少是 $\binom{k-m}{n}$.

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 $A=\{a_s(n_s)\}_{s=1}^k$ 的覆盖函数的周期. 则

(a) $\{\sum_{s\in J}\frac{1}{n_s}: J\subseteq\{1,\cdots,k-1\}\}\supseteq\{\frac{r}{n_k}: r=0,1,\cdots,\frac{n_k}{(n_0,n_k)}-1\}$.

(b) 假如 $n_1\leqslant\cdots\leqslant n_{k-l}<n_{k-l+1}=\cdots=n_k$ $(0<l<k)$，那么对每个正整数 $r<n_k/n_{k-l}$，或者 $r\equiv0\pmod{n_k/(n_0,n_k)}$，或者组合数 $\binom{l}{r}$ 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. Erdös 提出下述著名的未解决问题：是否对任意的 $c>0$ 有各模 $n_1,\cdots,n_k$ 互不相同且都大于 c 的覆盖 $A=\{a_s(n_s)\}_{s=1}^k$?

1954 年 B. H. Neumann [J. London Math. Soc. 29(1954); Publ. Math. Debrecen 3(1954)] 研究了一般群 G 的左陪集覆盖

$$\mathcal{A}=\{a_iG_i\}_{i=1}^k \quad (G_1,\cdots,G_k\text{为}G\text{的子群}),$$

他证明了 $\mathcal{A}$ 为 G 的极小覆盖时诸 G_i 指标有穷而且 $[G:\bigcap_{i=1}^k G_i]\leqslant c_k$, 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 $\mathcal{A}$ 为 G 的恰好 m- 覆盖，诸 G_i 次正规且 $\bigcap_{i=1}^k G_i=H$ 的最小 k 值。

Herzög-Schönheim猜想 [Canad. Math. Bull., 1974]. 设 G 为群， $\mathcal{A}=\{a_iG_i\}_{i=1}^k$ $(k>1)$ 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。

我们发现次正规子群有良好的数论性质。

引理 3.1 [孙智伟， European J. Combin. 22(2001)]. 设 $G_1,\cdots,G_k$ 都是群 G 的次正规子群，则

$$\left[G:\bigcap_{i=1}^k G_i\right]\ \Big|\ \prod_{i=1}^k[G:G_i].$$

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 $\{a_iG_i\}_{i=1}^k$ $(k>1)$ 为群 G 的均匀覆盖 (即它覆盖 G 中每个元素相同多次)， $G_1,\cdots,G_k$ 在 G 中次正规且

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

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

其中 γ 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 Erdös 问题答案否定。