中国科学: 数学 2023 年 第 53 卷 第 2 期: 407～418
SCIENTIA SINICA Mathematica
论 文

可分集与几乎可分集的新构造

献给朱烈教授 80 华诞

周君灵, 常彦勋*

北京交通大学数学研究所, 北京 100044
E-mail: jlzhou@bjtu.edu.cn, yxchang@bjtu.edu.cn

收稿日期: 2022-02-24; 接受日期: 2022-04-18; 网络出版日期: 2022-05-27; * 通信作者
国家自然科学基金 (批准号: 11971053 和 12171028) 和北京市自然科学基金 (批准号: 1222013) 资助项目

摘要 可分集 (partitionable set, PS) 与几乎可分集 (almost partitionable set, APS) 是组合设计理论中两类重要的组合构型, 与许多其他组合结构具有密切联系, 如 $\mathbb{Z}$- 循环 Whist 竞赛图、循环差阵、不含邻点的循环平衡样本设计、不交差族及光正交码等. 由于可分集与几乎可分集的要求比较严苛, 其存在性问题迄今远未解决. 本文针对 $p\equiv 7 \pmod 8$ 为素数的情形, 建立 p^2 阶可分集与 p 阶几乎可分集的新构造方法, 给出两类组合构型存在性的若干新结果. 特别地, 对于 $p\equiv 7 \pmod 8$ 的素数 p, 本文确定 $p<30{,}000$ 的绝大部分 p^2 阶 PS 的存在性, 给出特定条件下 p 阶 APS 的存在性和渐近存在性, 并得到 $p<50{,}000$ 除去 16 个可能例外的 p 阶 APS 的存在性.

关键词 可分集 几乎可分集 Whist 竞赛图 分圆类

MSC (2020) 主题分类 05B05

1 引言

令 $(G,+)$ 是群, 其单位元记作 0. 设 $v\equiv 1 \pmod 4$. v 阶群 $(G,+)$ 上的可分集 (PS) 记作 PS(G), 是 G 中 $(v-1)/4$ 个有序对的集合 S, 满足以下两个条件:

(1) $\bigcup_{(x,y)\in S}\pm\{x,y\}=G\setminus\{0\}$;

(2) $\bigcup_{(x,y)\in S}\pm\{x-y,x+y\}=G\setminus\{0\}$.

设 $v\equiv 3 \pmod 4$, 给定 v 阶群 $(G,+)$ 上两个非零元 α 和 β. 参数为 (G,α,β) 的几乎可分集 (APS) 记作 APS(G,α,β), 是 G 中 $(v-3)/4$ 个有序对的集合 S, 满足以下两个条件:

(1) $\bigcup_{(x,y)\in S}\pm\{x,y\}=G\setminus\{0,\pm\alpha\}$;

(2) $\bigcup_{(x,y)\in S}\pm\{x-y,x+y\}=G\setminus\{0,\pm\beta\}$.

当群 G 为交换群时, 可分集或几乎可分集中的有序对通常用无序对表示. 当群 G 为剩余类加群 $\mathbb{Z}_v$ 时, PS(G) 也记作 PS(v), APS(G,α,β) 也记作 APS(v,α,β).

英文引用格式: Zhou J L, Chang Y X. New constructions for partitionable sets and almost partitionable sets (in Chinese). Sci Sin Math, 2023, 53: 407–418, doi: 10.1360/SSM-2022-0031

令 $v=4n$ (或 $v=4n+1$), 由 v 个参与者组成的 Whist 竞赛图 Wh(v) 是形如 (a b c d) 的赛程表, 其中对子 $\{a,c\}$ 和 $\{b,d\}$ 中的两成员互为队友, 其余对子 $\{a,b\}$、$\{c,d\}$、$\{a,d\}$ 和 $\{b,c\}$ 中的两成员均为对手, 赛程安排满足以下条件:

(1) 共安排 $4n-1$ (或 $4n+1$) 轮比赛, 每轮包括 n 场比赛;

(2) 每个参与者每轮 (或除去一轮以外) 正好参加一次比赛;

(3) 每个参与者与其余任意参与者做队友正好一次;

(4) 每个参与者与其余任意参与者做对手正好两次.

设 $v=4n+1$. 若假定 v 个参与者取值于剩余类加群 $\mathbb{Z}_{4n+1}$ 且第 $j+1$ 轮比赛由第 j 轮比赛每个成员 $+1$ (mod $4n+1$) 生成, 则该 Wh(v) 被称为 $\mathbb{Z}$- 循环的. 类似地, 若参与者取值于 $\mathbb{Z}_{4n-1}\cup\{\infty\}$ 且所有比赛由首轮比赛在 $\mathbb{Z}_{4n-1}$ 作用下循环生成 (需要注意 ∞ 为不动点), 则称 Wh($4n$) 是 $\mathbb{Z}$- 循环的. 通常假定 $\mathbb{Z}$- 循环 Wh($4n+1$) 在首轮比赛中参与者 0 不参赛. 进一步地, 若首轮比赛的所有队友组正好为 $\{\{x,-x\}:x\in\mathbb{Z}_v\setminus\{0\}\}$ (对应 $v=4n+1$) 或 $\{\{x,-x\}:x\in\mathbb{Z}_v\setminus\{0\}\}\cup\{\{\infty,0\}\}$ (对应 $v=4n$), 则称该竞赛图为 $\mathbb{Z}$- 循环初始模式 ($\mathbb{Z}$-cyclic patterned starter Whist tournament, ZCPS) Wh(v), 简记为 ZCPS-Wh(v).

Whist 竞赛图问题的研究历史已经有一百余年, 其已知成果非常丰富. 相对地, $\mathbb{Z}$- 循环 Whist 竞赛图的研究始于二十余年前, 其存在性问题远未解决. 2009 年, Zhang 和 Chang [11] 首次定义了可分集的概念, 证明了当 $v\equiv 9$ (mod 12) 但 $v\not\equiv 81$ (mod 108) 时不存在 PS(v); 同时他们猜测 $v\equiv 81$ (mod 108) 时, PS(v) 也不存在. 2011 年, Abel 等 [1] 对 ZCPS-Wh(v) 也给出同样的结论与猜想.

最近, Chang 等 [3] 指出 PS(v) 与 ZCPS-Wh(v) 以及 APS(v,α,α) 与 ZCPS-Wh($v+1$) 的等价性.

定理 1.1 (参见文献 [3, 命题 2.3]) 当 $v\equiv 1$ (mod 4) 时, ZCPS-Wh(v) 存在当且仅当 PS(v) 存在. 当 $v\equiv 3$ (mod 4) 时, ZCPS-Wh($v+1$) 存在当且仅当对于某 $\alpha\in\mathbb{Z}_v$ 存在 APS(v,α,α).

如前所述, 当 $v\equiv 9$ (mod 12) 时, 文献 [1,11] 给出了 PS(v) 或 ZCPS-Wh(v) 不存在的猜想, Hu 和 Ge [5] 证明了该猜想的正确性; 当 $v\equiv 3$ (mod 4) 时, 文献 [6] 给出了 ZCPS-Wh(v) 即 APS(v,α,α) 的必要条件及一些存在性结果. 文献 [3] 首次提出了几乎可分集的概念. 下列命题给出 PS 及 APS 存在的必要条件.

命题 1.1 (1) (参见文献 [5, 定理 2.1]) 令 $v\equiv 1$ (mod 4). 若 PS(v) 存在, 则 $v\equiv 1,5$ (mod 12).

(2) (参见文献 [5, 定理 2.2] 和 [6, 定理2.1]) 设 APS(v,α,α) 存在. 则当 $v\equiv 7,11$ (mod 12) 时, v 含有平方因子; 而当 $v\equiv 3$ (mod 12) 时, $v=3^{2a+1}v_1$, 其中 $a\geqslant 0$, $v_1\equiv 1$ (mod 12).

(3) (参见文献 [3, 引理 3.1]) 设 APS(v,α,β) 存在. 则当 $v\equiv 3$ (mod 12) 时, $2\alpha^2-\beta^2\equiv v/3$ (mod v); 当 $v\equiv 7,11$ (mod 12) 时, $2\alpha^2-\beta^2\equiv 0$ (mod v).

可分集与几乎可分集的存在性问题是组合设计中亟待解决的理论问题, 下面列出 PS 的已知结果以及 APS 在 $\alpha\neq\beta$ 时的主要结论 ($\alpha=\beta$ 时的结果非常零散).

定理 1.2 对下列阶数 v, PS(v) 都存在.

(1) (参见文献 [10]) v 是有限个模 4 余 1 素数的乘积.

(2) (参见文献 [6, 定理 5.6]) $v\leqslant 300$, $v\equiv 1,5$ (mod 12).

(3) (参见文献 [7]) $v=p^2$, 其中 p 为素数, $3<p<3{,}500$, $p\equiv 3$ (mod 4).

(4) (参见文献 [3, 定理 6.4]) $v=pq$, 其中 $p,q\equiv 3$ (mod 4) 均为大于 3 的素数, $q<200$, $(p-1)\mid(q-1)$.

定理 1.3 (参见文献 [3, 定理 6.6]) 令 $v\equiv 3$ (mod 4), $v<300$, $\alpha\beta\neq 0$. APS(v,α,β) 存在当且仅当命题 1.1(3) 中的必要条件满足.

定理 1.4 (参见文献 [2, 定理 3.2]) 令 $u,v\equiv 1 \pmod 4$. 若 PS(u) 与 PS(v) 都存在, 则 PS(uv) 也存在.

定理 1.4 给出的乘积构造仅适用于 $u,v\equiv 1 \pmod 4$ 的情形. 当 $u,v\equiv 3 \pmod 4$ 时, 如何构造 PS(uv) 是长期以来一个棘手问题. 文献 [7] 给出了 $p\equiv 3 \pmod 4$ 时 PS(p^2) 的直接构造, 其中假设首轮比赛由 $(p+1)/2$ 或 $(p+1)/4$ 个比赛在 $\mathbb{Z}_{p^2}$ 可逆元中所有 $2p$ 或 p 次剩余作用下生成, 借助计算机搜索, 得到一系列可分集, 结果见定理 1.2(3). 文献 [3] 建立了当素数 $p\equiv 7 \pmod 8$ 且满足特定条件时 APS($p,\alpha,\sqrt{2}\alpha$) 的存在性 (参见文献 [3, 引理 4.1]), 且对某些小素数 p 构造出 PS(p^2) (参见文献 [3, 注 7.11]). 本文将推广文献 [3] 针对可分集与几乎可分集的构造方法, 扩展 PS 及 APS 的存在性范围.

除了 ZCPS-Wh(v), 可分集和几乎可分集还与其他组合结构具有密切联系, 如循环差阵、不含邻点的循环平衡样本设计和不交差族等. 可分集与几乎可分集还可用于构造大容量的光正交码, 从而在光码分多址系统具有重要应用.

2 构造可分集

对于正整数 n, 用 $\mathbb{Z}_n$ 表示模 n 的剩余类环, 记 $\mathbb{Z}_n^*=\mathbb{Z}_n\setminus\{0\}$; 用 $U(n)$ 表示 $\mathbb{Z}_n^*$ 中所有乘法可逆元做成的乘法群, 显然 $U(n)$ 由 $\mathbb{Z}_n$ 中所有与 n 互素的成员构成, 即 $|U(n)|=\varphi(n)$. 特别地, 当 n 为素数时, $U(n)=\mathbb{Z}_n^*$.

现约定本节通用的记号. 令 $p\equiv 7 \pmod 8$ 为素数, 易知 2 在 $\mathbb{Z}_p$ 与 $\mathbb{Z}_{p^2}$ 中均为平方元, 记其在 $\mathbb{Z}_{p^2}$ 中的一个平方根为 $\sqrt{2}$. 若不作特别说明, 本节运算均默认在 $\mathbb{Z}_{p^2}$ 中进行. 令 $\theta=1+\sqrt{2}$. 考虑 θ 与 $-\theta$ 生成的乘法群 $H=\langle\theta,-\theta\rangle$. 显然 H 是 $U(p^2)$ 的子群, 且 H 是一个循环群, $H=\langle\xi\rangle$, 其中若 θ 的乘法阶为偶数, 则 $\xi=\theta$; 否则 $\xi=-\theta$. 由于 $2\,|\,|H|, |H|\,|\,|U(p^2)|=p(p-1)$, 故 $|H|\equiv 2 \pmod 4$. 特别地, 注意本节常用以下两个假定:

(A1) 假定 ξ 在 $U(p^2)$ 中的阶 (即 $|H|$) 为 p 的倍数并记 $|H|=ps$ (显然, s 为偶数, $s\mid p-1$). 这等价于 $\xi^{p-1}=\theta^{p-1}\not\equiv 1 \pmod{p^2}$.

(A2) 假定 $2\in H$. 设 $2=\xi^b$. 由于 2 是平方元, 故 $1=2^{p(p-1)/2}=\xi^{bp(p-1)/2}$, 因此 $|H|\,|\,\frac{bp(p-1)}{2}$. 注意到 $|H|\equiv 2 \pmod 4$, $p\equiv 7 \pmod 8$, 则必有 b 为偶数. 在 H 中 2 对 ξ 的指数本节记为 $\mathrm{ind}(2)=2a$, $1\leqslant a\leqslant ps/2-1$.

文献 [3] 曾讨论 $H=U(p^2)$ 情形下 PS 的构造, 此时假定 (A1) 和 (A2) 自然满足. 文献 [3] 给出了对于任意素数 $p\equiv 7 \pmod 8$, $p<600$ 且 $p\notin\{71,311,367,463\}$, 都存在 PS($p^2$). 本节将推广相关构造方法, 产生更多的 PS.

引理 2.1 [8] 设 $x\in U(p^2)$ 且 x 在 $\mathbb{Z}_p$ 中的乘法阶为 t, 则 x 在 $\mathbb{Z}_{p^2}$ 中的乘法阶为 t 或 pt.

设假定 (A1) 成立, 即 $|H|=ps$. 由引理 2.1 及前面讨论知 $|H_p|=s\equiv 2 \pmod 4$, 其中 H_p 为 ξ 在 $\mathbb{Z}_p^*$ 乘法下生成的子群 (显然 $s>2$). 设 $R=\{b_0,b_1,\ldots,b_{t-1}\}$ 为 H_p 在 $\mathbb{Z}_p^*$ 中的陪集完全代表系, 易知 R 也形成 H 在 $U(p^2)$ 中的陪集完全代表系. 从而对于任意 $c\in U(p^2)$, 有

$$\begin{aligned}\mathbb{Z}_{p^2}^* &= U(p^2)\cup\{p,2p,\ldots,(p-1)p\}\\ &=\Big(\bigcup_{i=0}^{t-1}b_iH\Big)\cup\Big(\bigcup_{i=0}^{t-1}b_icpH_p\Big)\\ &=\bigcup_{i=0}^{t-1}b_i(H\cup cpH_p).\end{aligned}\tag{2.1}$$

构造 2.1 设 $p\equiv 7 \pmod 8$ 为素数且满足假定 (A1). 取定 $c\in U(p^2)$, 假设在区间 $[0,ps/2-1)$ 上存在 3 个整数 $x_1<x_2<x_3$ 满足 $x_1\equiv x_3\not\equiv x_2 \pmod 2$ 且

$$\pm\sqrt{2}\{\xi^{x_1},\xi^{x_2},\xi^{x_3},cp\}=\pm\{\xi^{x_i}-\xi^{x_j},\xi^{x_i}+\xi^{x_j},\xi^{x_k}-cp,\xi^{x_k}+cp\},$$

其中 $\{i,j,k\}=\{1,2,3\}$. 则存在 $\mathrm{PS}(p^2)$.

证明 由 (2.1) 知, $\mathbb{Z}_{p^2}^*=\bigcup_{i=0}^{t-1}b_iY$, 其中 $Y=H\cup cpH_p$, $\{b_0,b_1,\ldots,b_{t-1}\}$ 为 H_p 在 $\mathbb{Z}_p^*$ 中的陪集完全代表系.

若 x_1 和 x_3 为奇数而 x_2 为偶数, 则构作如下对子集 S:

$$\begin{aligned}
&\xi^{2l-1}\{1,\xi\},\quad 1\leqslant l\leqslant\frac{x_1-1}{2},\\
&\xi^{2l}\{1,\xi\},\quad \frac{x_1+1}{2}\leqslant l\leqslant\frac{x_2-2}{2},\\
&\xi^{2l-1}\{1,\xi\},\quad \frac{x_2+2}{2}\leqslant l\leqslant\frac{x_3-1}{2},\\
&\xi^{2l}\{1,\xi\},\quad \frac{x_3+1}{2}\leqslant l\leqslant\frac{ps-2}{4},\\
&cp\xi^{2l-1}\{1,\xi\},\quad 1\leqslant l\leqslant\frac{s-2}{4},\\
&\{\xi^{x_i},\xi^{x_j}\},\quad \{\xi^{x_k},cp\}.
\end{aligned}$$

易知 $Y=H\cup cpH_p=\bigcup_{\{x,y\}\in S}\pm\{x,y\}$. 注意到 $\xi\in\{\theta,-\theta\}$, $\theta-1=\sqrt{2}$, $(\theta+1)/(\theta-1)=\theta$, 易证

$$\bigcup_{\{x,y\}\in S}\pm\{x-y,x+y\}=\sqrt{2}(Y\setminus(\pm\{\xi^{x_1},\xi^{x_2},\xi^{x_3},cp\}))\cup(\pm\{\xi^{x_i}-\xi^{x_j},\xi^{x_i}+\xi^{x_j},\xi^{x_k}-cp,\xi^{x_k}+cp\}).$$

若定理条件满足, 则 $\bigcup_{\{x,y\}\in S}\pm\{x-y,x+y\}=\sqrt{2}Y$, 因此

$$\{b_i\{x,y\}:\{x,y\}\in S,0\leqslant i\leqslant t-1\}$$

构成 $\mathbb{Z}_{p^2}$ 上的可分集 $\mathrm{PS}(p^2)$.

若 x_1 和 x_3 为偶数而 x_2 为奇数, 则构作如下对子集 S:

$$\begin{aligned}
&\xi^{2l-2}\{1,\xi\},\quad 1\leqslant l\leqslant\frac{x_1}{2},\\
&\xi^{2l-1}\{1,\xi\},\quad \frac{x_1+2}{2}\leqslant l\leqslant\frac{x_2-1}{2},\\
&\xi^{2l-2}\{1,\xi\},\quad \frac{x_2+3}{2}\leqslant l\leqslant\frac{x_3}{2},\\
&\xi^{2l-1}\{1,\xi\},\quad \frac{x_3+2}{2}\leqslant l\leqslant\frac{ps-2}{4},\\
&cp\xi^{2l-1}\{1,\xi\},\quad 1\leqslant l\leqslant\frac{s-2}{4},\\
&\{\xi^{x_i},\xi^{x_j}\},\quad \{\xi^{x_k},cp\}.
\end{aligned}$$

类似上一情形, 可证 $\{b_i\{x,y\}:\{x,y\}\in S,0\leqslant i\leqslant t-1\}$ 构成 $\mathbb{Z}_{p^2}$ 上的可分集 $\mathrm{PS}(p^2)$. □

下面针对构造 2.1 的条件进一步刻画 3 个整数 x_1、x_2 和 x_3 的性质.

引理 2.2 设 $p\equiv 7 \pmod 8$ 为素数且满足假定 (A1) 和 (A2). 区间 $[0,ps/2-1)$ 上存在 3 个互不相同的整数 x、y 和 z 满足 $\mathbb{Z}_{p^2}$ 中的集合等式

$$\pm\sqrt{2}\{\xi^x,\xi^y,\xi^z,cp\}=\pm\{\xi^x-\xi^y,\xi^x+\xi^y,\xi^z-cp,\xi^z+cp\},\tag{2.2}$$

其中 $c\in U(p^2)$, 当且仅当

$$\begin{cases} y=x+ls, \quad \gcd(l,p)=1,\\ z\equiv x+a+\dfrac{ls}{2}\ \left(\bmod\ \dfrac{ps}{2}\right), \end{cases}\tag{2.3}$$

或者

$$\begin{cases} y=x+\dfrac{(2l+1)s}{2}, \quad \gcd(2l+1,p)=1,\\ z\equiv x+a+\dfrac{(2l+1+p)s}{4}\ \left(\bmod\ \dfrac{ps}{2}\right), \end{cases}\tag{2.4}$$

其中 l 为整数.

证明 从集合等式 (2.2) 两边模 p 比较可得 $\pm\{\xi^x+\xi^y\}=\pm\{\sqrt{2}cp\}$, 或 $\pm\{\xi^x-\xi^y\}=\pm\{\sqrt{2}cp\}$. 因此 (2.2) 等价于

$$\begin{cases} \pm\{\xi^x-\xi^y\}=\pm\{\sqrt{2}cp\},\\ \pm\sqrt{2}\{\xi^x,\xi^y,\xi^z\}=\pm\{\xi^x+\xi^y,\xi^z-cp,\xi^z+cp\}, \end{cases}\tag{2.5}$$

或者

$$\begin{cases} \pm\{\xi^x+\xi^y\}=\pm\{\sqrt{2}cp\},\\ \pm\sqrt{2}\{\xi^x,\xi^y,\xi^z\}=\pm\{\xi^x-\xi^y,\xi^z-cp,\xi^z+cp\}. \end{cases}\tag{2.6}$$

由 (2.5) 可得 ((2.5) 中第二个式子模 p)

(i) $\pm\{\xi^x-\xi^y\}=\pm\{\sqrt{2}pc\}$;

(ii) $\pm\{\sqrt{2}\xi^z\}=\pm\{\xi^x+\xi^y\}$;

(iii) $\pm\sqrt{2}\{\xi^x,\xi^y\}=\pm\{\xi^z-cp,\xi^z+cp\}$.

易知若 (i) 和 (ii) 同时成立可推导出 (iii), 并且有 (vi) $2\xi^{x+y}=\xi^{2z}$. 反之, 由 (i) 和 (vi) 可得

$$(\xi^x+\xi^y)^2=(\xi^x-\xi^y)^2+4\xi^{x+y}\equiv 2\xi^{2z} \pmod{p^2},$$

即得 (ii). 从而 (2.5) 等价于

$$\begin{cases} \pm\{\xi^x-\xi^y\}=\pm\{\sqrt{2}pc\},\\ 2\xi^{x+y}=\xi^{2z}. \end{cases}$$

上述方程中第一式推导出 $\xi^y\equiv\xi^x \pmod p$, 从而存在整数 l 使得 $y=x+ls$, 而 $\xi^y\not\equiv\xi^x \pmod{p^2}$, 因此 $\gcd(l,p)=1$. 由于 $\mathrm{ind}(2)=2a$, 故由方程第二式可得 $z\equiv x+a+\frac{ls}{2} \pmod{\frac{ps}{2}}$, 因此得到 (2.3). 反之, 若 (2.3) 成立, 则显然 $\xi^{2z}=2\xi^{x+y}$, $\xi^x-\xi^y=\xi^x(1-\xi^{ls})\equiv 0 \pmod p$, 故可设 $\pm\{\xi^x-\xi^y\}=\pm\{\sqrt{2}pc\}$. 由于 $\xi^x-\xi^y$ 模 p^2 不余 0, 故 $c\in U(p^2)$. 从而证明 (2.3) 等价于 (2.5).

类似上面情形, 可证 (2.6) 等价于

$$\begin{cases}\pm\{\xi^x+\xi^y\}=\pm\{\sqrt{2}pc\},\\ 2\xi^{x+y}=-\xi^{2z}.\end{cases}$$

注意 $\xi^{\frac{ps}{2}}=-1$, 进而可证其等价于 (2.4). □

推论 2.1 设 $p\equiv 7 \pmod 8$ 为素数且满足假定 (A1) 和 (A2).

(1) 当 a 为偶数且 $a>\frac{(p+3)s}{4}$ 或 $a<\frac{(p-1)s}{4}$ 时, 存在 PS(p^2);

(2) 当 a 为奇数且 $a>\frac{(p+1)s}{4}$ 或 $a<\frac{(p-3)s}{4}$ 时, 存在 PS(p^2).

证明 (1) 设 a 为偶数. 当 $a>\frac{(p+3)s}{4}$ 时, 在 (2.4) 中取 $x=0$, $l=1$, $y=\frac{3s}{2}$, $z=a-\frac{(p-3)s}{4}$. 显然 x 和 z 为偶数, y 为奇数, 且 $x<y<z<\frac{ps}{2}-1$. 取 $(x_1,x_2,x_3)=(x,y,z)$, 应用构造 2.1 与引理 2.2 即得 PS(p^2) 存在. 当 $a<\frac{(p-1)s}{4}$ 时, 在 (2.3) 中取 $x=0$, $l=\frac{p-1}{2}$, $y=\frac{(p-1)s}{2}$, $z=a+\frac{(p-1)s}{4}$. 显然 x 和 y 为偶数, z 为奇数, 且 $x<z<y<\frac{ps}{2}-1$. 取 $(x_1,x_2,x_3)=(x,z,y)$, 应用构造 2.1 与引理 2.2 即得 PS(p^2) 存在.

(2) 设 a 为奇数. 当 $a>\frac{(p+1)s}{4}$ 时, 在 (2.4) 中取 $x=0$, $l=0$, $y=\frac{s}{2}$, $z=a-\frac{(p-1)s}{4}$. 显然 x 和 z 为偶数, y 为奇数, 且 $x<y<z<\frac{ps}{2}-1$. 取 $(x_1,x_2,x_3)=(x,y,z)$, 应用构造 2.1 与引理 2.2 即得 PS(p^2) 存在. 当 $a<\frac{(p-3)s}{4}$ 时, 在 (2.3) 中取 $x=0$, $l=\frac{p-3}{2}$, $y=\frac{(p-3)s}{2}$, $z=a+\frac{(p-3)s}{4}$. 显然 x 和 y 为偶数, z 为奇数, 且 $x<z<y<\frac{ps}{2}-1$. 取 $(x_1,x_2,x_3)=(x,z,y)$, 应用构造 2.1 与引理 2.2 即得 PS(p^2) 存在. □

定理 2.1 设 $p\equiv 7 \pmod 8$ 为 30,000 以内的素数, 除去 $p\in E$ 的 141 个可能的例外值, 都存在 PS(p^2), 其中 E 中元素如下:

3,511	3,559	3,911	3,967	4,111	4,159	4,327	4,447	4,463	4,663	4,831	4,903	4,943
4,951	4,999	5,039	5,231	5,351	5,503	5,527	5,591	5,743	5,839	6,007	6,367	6,679
6,703	6,791	6,823	6,871	7,159	7,583	7,591	7,687	7,759	8,191	8,231	8,311	8,527
8,599	8,647	8,887	9,103	9,127	9,151	9,311	9,343	9,871	9,967	10,039	10,151	10,271
10,391	10,567	10,687	10,847	11,071	11,503	11,527	12,391	12,511	12,799	12,823	13,711	13,759
13,831	13,903	13,999	14,551	14,831	14,983	15,319	15,511	15,607	15,671	15,823	15,991	16,183
16,231	16,447	16,567	16,831	16,871	16,927	17,047	17,431	17,599	18,311	18,911	19,447	19,543
19,727	20,023	20,071	20,431	21,031	21,191	21,751	22,063	22,159	22,303	22,727	22,751	22,807
22,871	23,143	23,167	23,431	23,447	23,719	23,767	23,831	23,887	24,103	24,223	24,439	24,847
24,919	25,183	25,303	25,423	25,447	25,999	26,711	26,839	27,271	27,487	27,791	27,919	27,943
28,463	28,591	28,687	28,711	28,751	29,023	29,191	29,231	29,527	29,863	29,983.		

证明 若 $p\equiv 7 \pmod 8$ 且 $p<3{,}500$, 则 PS(p^2) 的存在性可由定理 1.2 得到. 借助计算机可验证: 除去 E 中成员, 所有 3,500–30,000 之间模 8 余 7 的素数 p (共 555 个) 同时满足假定 (A1) 和 (A2) 及推论 2.1 中条件, 相关数据参见文献 [12, 表 I] (包括 3,500–5,000 之间数据, 完整列表可联系作者). 应用推论 2.1 可知存在 PS(p^2). □

注 2.1 除去上述定理证明中列举事实, 借助计算机, 还可验证 30,000 以内模 8 余 7 的总共 817 个素数中:

(1) 只有唯一一例 $p=31$ 不满足假定 (A1);

(2) 只有唯一一例 $p=71$ 满足假定 (A1) 和 (A2), 但不满足推论 2.1 中条件, 具体地, $\sqrt{2}=414$, $\xi=4{,}626$, $s=70$, $a=1{,}268$;

(3) 3,500 以内模 8 余 7 的素数中有 23 个不满足 (A2), 它们是 31、79、103、199、239、487、599、607、751、1,031、1,151、1,279、1,447、1,471、1,879、2,111、2,311、2,647、2,671、2,719、2,887、3,079 和 3,191.

由此可见, 应用推论 2.1 的最大障碍来源于假定 (A2). 30,000 以内模 8 余 7 的素数中约 20% 不满足假定 (A2). 比较而言, 在假定 (A2) 成立的情形下, 推论 2.1 对于 ind(2) 的限制条件较容易满足.

3 构造几乎可分集

本节依然令 $p\equiv 7 \pmod 8$ 为素数, 记 2 在 $\mathbb{Z}_p$ 中的一个平方根为 $\sqrt{2}$. 本节运算均默认在 $\mathbb{Z}_p$ 中进行, 并通用记号 $\theta=1+\sqrt{2}$, $H=\langle\xi\rangle$, 其中, 若 θ 的乘法阶为偶数, 则 $\xi=\theta$; 否则 $\xi=-\theta$.

取定 $\mathbb{Z}_p$ 的一个本原根 ω 及正整数 t ($t\mid p-1$). 记 $\mathbb{Z}_p^*$ 的子群 $C_0^t=\{\omega^{it}:0\leqslant i\leqslant (p-t-1)/t\}$, 用 C_i^t 表示 C_0^t 在 $\mathbb{Z}_p^*$ 中以 ω^i 为代表元的陪集, 即 $C_i^t=\omega^i C_0^t$, $0\leqslant i\leqslant t-1$, 这些称为 t 次分圆陪集或 t 次分圆类. 显然, $\mathbb{Z}_p^*$ 的子群 $H=\langle\xi\rangle$ 是一个分圆陪集 C_0^t, 其中 $t=(p-1)/|H|$. 本节考虑的都是 H 对应的分圆类. 文献 [3] 在只有一个分圆类即 $H=\mathbb{Z}_p^*$ 时给出 APS 的构造. 本节考虑分圆类个数 $t>1$ 时 APS 的构造方法. 由于 $p\equiv 7 \pmod 8$, 故 $|H|\equiv 2 \pmod 4$, t 为奇数.

引理 3.1 (参见文献 [3, 引理 4.1]) 令 $p\equiv 7 \pmod 8$ 为素数且 $H=\mathbb{Z}_p^*$. 则对于任意 $\alpha\in\mathbb{Z}_p^*$ 都存在 APS$(p,\alpha,\sqrt{2}\alpha)$.

下述构造主要处理分圆类个数 $t\equiv 1 \pmod 4$ 的情形.

构造 3.1 设 $p\equiv 7 \pmod 8$ 为素数. 取 H 在 $\mathbb{Z}_p^*$ 陪集的完全代表系 $R=\{b_0,b_1,\ldots,b_{t-1}\}$. 假设存在 $\alpha,\beta\in R$, 使得 R 可划分成满足以下两个条件的对子集 S:

(1) $\bigcup_{\{x,y\}\in S}\pm\{x,y\}=\pm(R\setminus\{\alpha\})$;

(2) $\bigcup_{\{x,y\}\in S}\pm\{x-y,x+y\}=\pm\sqrt{2}(R\setminus\{\beta\})$,

则存在 APS$(p,\alpha,\sqrt{2}\beta)$.

证明 设 $S_0=\{\{\xi^{2i-1},\xi^{2i}\}:1\leqslant i\leqslant\frac{|H|-2}{4}\}$, 则易证

$$\bigcup_{\{x,y\}\in S_0}\pm\{x,y\}=\bigcup_{i=1}^{(|H|-2)/4}\pm\{\xi^{2i-1},\xi^{2i}\}=H\setminus\{\pm 1\}.$$

由于 $\xi\in\{\theta,-\theta\}$, 故 $\pm\{1+\xi,1-\xi\}=\pm(\theta-1)\{1,\theta\}=\pm\sqrt{2}\{1,\theta\}=\pm\sqrt{2}\{1,\xi\}$, 从而有

$$\begin{aligned}\bigcup_{\{x,y\}\in S_0}\pm\{x-y,x+y\}&=\bigcup_{i=1}^{(|H|-2)/4}\pm\{\xi^{2i-1}(1-\xi),\xi^{2i-1}(\xi+1)\}\\&=\bigcup_{i=1}^{(|H|-2)/4}\pm\sqrt{2}\{\xi^{2i-1},\xi^{2i}\}\\&=\sqrt{2}(H\setminus\{\pm 1\}).\end{aligned}$$

令 $T=(\bigcup_{i=0}^{t-1}b_iS_0)\cup S$. 应用条件 (1) 和 (2), 易证

$$\bigcup_{\{x,y\}\in T}\pm\{x,y\}=\mathbb{Z}_p\setminus\{0,\pm\alpha\},\qquad\bigcup_{\{x,y\}\in T}\pm\{x-y,x+y\}=\mathbb{Z}_p\setminus\{0,\pm\sqrt{2}\beta\}.$$

因此 T 为 APS$(p,\alpha,\sqrt{2}\beta)$. □

应用 Weil 定理[9], 文献 [4] 给出了指定若干分圆类时其代表元选取的可能性.

引理 3.2 (参见文献 [4, 定理 3.2]) 令 p 为素数, $p\equiv 1 \pmod t$, 且

$$p-\left(\sum_{i=0}^{s-2}\binom{s}{i}(s-i-1)(t-1)^{s-i}\right)\sqrt{p}-st^{s-1}>0.$$

则对于任意给定的 s 元组 $(j_1,j_2,\ldots,j_s)\in\{0,1,\ldots,t-1\}^s$ 以及 $\mathbb{Z}_p$ 中互不相同元素做成的 s 元组 $(c_1,c_2,\ldots,c_s)$, 存在 $x\in\mathbb{Z}_p$ 使得 $x+c_i\in C_{j_i}^t$ 对于任意 $i\in\{1,2,\ldots,s\}$ 都成立.

下述引理证明从略.

引理 3.3 令 $p\equiv 7 \pmod 8$ 为素数. 对于 $x,y,z,u\in\mathbb{Z}_p^*$, 等式 $(x+y,x-y)=(\sqrt{2}z,\sqrt{2}u)$ 等价于 $(z+u,z-u)=(\sqrt{2}x,\sqrt{2}y)$.

定理 3.1 令 $p\equiv 7 \pmod 8$ 为素数, $H=C_0^t$, 其中 $t\equiv 1 \pmod 4$. 则当 $p-(2(t-1)^3+3(t-1)^2)\sqrt{p}-3t^2>0$ 时, 对于任意 $\alpha\in\mathbb{Z}_p^*$, 存在 APS$(p,\alpha,\sqrt{2}\alpha)$.

证明 当 $t=1$ 时, 参见引理 3.1. 令 $t=4m+1$ $(m\geqslant 1)$, 则 t 次分圆类为 $C_0^t=H,C_1^t,\ldots,C_{t-1}^t$. 设 $\sqrt{2}\in C_k^t$. 对于任意 $0\leqslant i\leqslant m-1$, 取定 $b_{4i}\in C_{4i}^t$, 在引理 3.2 中取

$$s=3,\quad (j_1,j_2,j_3)=(4i+1,4i+2+k,4i+3+k)$$

(注意每个 j_i 模 t 取至区间 $[0,t-1]$ 上), 取 $(c_1,c_2,c_3)=(0,b_{4i},-b_{4i})$, 可得存在 $b_{4i+1}\in C_{4i+1}^t$ 使得 $b_{4i+1}+b_{4i}\in C_{4i+2+k}^t$, $b_{4i+1}-b_{4i}\in C_{4i+3+k}^t$. 设 $b_{4i+1}+b_{4i}=\sqrt{2}b_{4i+2}$, $b_{4i+1}-b_{4i}=\sqrt{2}b_{4i+3}$, 其中 $b_{4i+2}\in C_{4i+2}^t$, $b_{4i+3}\in C_{4i+3}^t$. 由引理 3.3 得 $b_{4i+2}+b_{4i+3}=\sqrt{2}b_{4i+1}$, $b_{4i+2}-b_{4i+3}=\sqrt{2}b_{4i}$. 令 $S=\big\{\{b_{2i},b_{2i+1}\}:0\leqslant i\leqslant 2m-1\big\}$, 则

$$\bigcup_{\{x,y\}\in S}\pm\{x,y\}=\pm(R\setminus\{b_{4m}\}),\qquad \bigcup_{\{x,y\}\in S}\pm\{x-y,x+y\}=\pm\sqrt{2}(R\setminus\{b_{4m}\}),$$

其中 $R=\{b_0,b_1,\ldots,b_{4m}\}$ 为分圆陪集完全代表系. 应用构造 3.1 可得 APS$(p,b_{4m},\sqrt{2}b_{4m})$, 替换 S 为 $\frac{\alpha}{b_{4m}}S$ 即得结论. □

在定理 3.1 中取 $t=5$, 简单计算可得以下推论.

推论 3.1 令 $p\equiv 7 \pmod 8$ 为素数且 $H=C_0^5$. 则当 $p\geqslant 31{,}127$ 时, 对于任意 $\alpha\in\mathbb{Z}_p^*$, 存在 APS$(p,\alpha,\sqrt{2}\alpha)$.

引理 3.4 令 $p\equiv 7 \pmod 8$ 为小于 50,000 的素数且 $H=C_0^t$, 其中 $t\equiv 1 \pmod 4$. 则对于任意 $\alpha\in\mathbb{Z}_p^*$, 存在 APS$(p,\alpha,\sqrt{2}\alpha)$.

证明 当 $t=1$ 时, 参见引理 3.1. 当 $t=5$ 且 $p\geqslant 31{,}127$ 时, 参见推论 3.1. 以下假定 $t\geqslant 5$, 若 $t=5$, 则令 $p<31{,}127$ (共 76 个). 当 $p\notin A:=\{239,4951,9103,9311,36847\}$ 时, 借助计算机搜索, 可以在 4 个分圆陪集 C_1^t、C_2^t、C_3^t 和 C_4^t 中各找到一个代表做成集合 $\{b_1,b_2,b_3,b_4\}$, 使得 $b_1+b_2=\sqrt{2}b_3$, $b_1-b_2=\sqrt{2}b_4$, 详见文献 [12, 表 II]. 注意到引理 3.3, 显然, $\{\omega^{4i}\{b_1,b_2\},\omega^{4i}\{b_3,b_4\}:0\leqslant i\leqslant m-1\}$ (ω 是 $\mathbb{Z}_p$ 的本原根) 做成满足构造 3.1 条件的对子集 S, 其中 $\alpha=1$, $\beta=1$. 故存在 APS$(p,1,\sqrt{2})$, 进而对于任意 $\alpha\in\mathbb{Z}_p^*$ 都存在 APS$(p,\alpha,\sqrt{2}\alpha)$. 类似方法处理 $p\in A$, 方法类似但不再规整. 为了给出满足构造 3.1 两条件的陪集划分, 我们给所有元素加下标表示其所在的分圆陪集, 即 y_a 表示元素 y 属于陪集 C_a^t, 也即 $y\in\omega^aC_0^t$, 具体信息见表 1. 特别地, 给定满足条件 $\pm\{y+z,y-z\}=\pm\sqrt{2}\{u,v\}$

表 1 引理 3.4 中 $p\in A$ 数据

p	$\sqrt{2}$	ξ	ω	t	(y_a,z_c,u_d,v_e)
239	99	139	7	17	$(7_1,220_2,123_3,92_8)$, $(11_4,225_{16},210_7,162_5)$, $(130_9,235_{13},23_{12},180_{10})$, $(61_6,237_{15},172_{11},131_{14})$
4,951	693	694	6	25	$(6_1,660_4,3023_3,1135_6)\cdot\{\omega^{4i}:0\leqslant i\leqslant 4\}$, $(36_2,1253_{21},3524_0,1620_{24})$
9,103	3,814	5,288	6	37	$(6_1,1017_2,2819_8,1859_3)\cdot\{\omega^{4i}:0\leqslant i\leqslant 6\}$, $(1_0,4020_4,3321_{33},493_{29})$, $(8479_{30},9008_{34},3420_{36},1630_{35})$
9,311	1,344	1,345	7	49	$(7_1,2401_4,7373_{10},2035_{19})\cdot\{\omega^{4i}:0\leqslant i\leqslant 9\}$, $(343_3,6557_7,9233_{11},4831_{15})$, $(6669_{41},6176_{44},543_{48},5411_{45})$
36,847	16,867	19,979	3	69	$(3_1,13970_4,23013_{10},27588_{19})\cdot\{\omega^{4i}:0\leqslant i\leqslant 14\}$, $(27_3,28117_7,20897_{61},29195_{64})$, $(1_0,12635_{11},4182_{65},12685_{15})$

的四元组 (y_a,z_c,u_d,v_e), 这对应构造 3.1 需要的划分集 S 中两个无序对 $\{y,z\}$ 和 $\{u,v\}$. 同时, 用 $(y_a,z_c,u_d,v_e)\cdot\{\omega^{4i}:i\in I\}$ 表示 $|I|$ 个四元组 $((y\cdot\omega^{4i})_{a+4i},(z\cdot\omega^{4i})_{c+4i},(u\cdot\omega^{4i})_{d+4i},(v\cdot\omega^{4i})_{e+4i})$, $i\in I$. □

定理 3.2 令 $p\equiv 7\pmod 8$ 为素数且 $H=C_0^5$. 则对于任意 $\alpha\in\mathbb{Z}_p^*$, 存在 APS$(p,\alpha,\sqrt{2}\alpha)$.

证明 结合引理 3.4 及推论 3.1 得证. □

为处理分圆类个数 $t\equiv 3\pmod 4$ 的情形, 我们给出一个新构造.

构造 3.2 令 $p\equiv 7\pmod 8$ 为素数且 $H=C_0^t$, $t\geqslant 3$. 取分圆陪集代表 $b_i\in C_i^t$, $0\leqslant i\leqslant t-1$ 且 $b_0=1$. 设存在奇数 x_1 和偶数 x_2 $(1\leqslant x_1<x_2\leqslant(|H|-2)/4)$, 使得 $\pm\{\xi^{x_1}+1,\xi^{x_1}-1\}=\pm\sqrt{2}\{\xi^{x_2},b_l\}$, 其中 $l\in\{1,2,\ldots,t-1\}$. 假设集合 $\bar{R}=\{b_i:1\leqslant i\leqslant t-1,i\neq l\}$ 可划分成满足以下两个条件的对子集 S (其中 $\alpha,\beta\in\bar{R}$):

(1) $\bigcup_{\{x,y\}\in S}\pm\{x,y\}=\pm(\bar{R}\setminus\{\alpha\})$;

(2) $\bigcup_{\{x,y\}\in S}\pm\{x-y,x+y\}=\pm\sqrt{2}(\bar{R}\setminus\{\beta\})$,

则存在 APS$(p,\alpha,\sqrt{2}\beta)$.

证明 构作如下对子集 S_0:

$$\begin{aligned}&\xi^{2i-1}\{1,\xi\},\quad 1\leqslant i\leqslant\frac{x_1-1}{2},\\&\xi^{2i}\{1,\xi\},\quad \frac{x_1+1}{2}\leqslant i\leqslant\frac{x_2-2}{2},\\&\xi^{2i-1}\{1,\xi\},\quad \frac{x_2+2}{2}\leqslant i\leqslant\frac{|H|-2}{4},\\&\{1,\xi^{x_1}\},\quad\{\xi^{x_2},b_l\}.\end{aligned}$$

由假设 $\pm\{\xi^{x_1}+1,\xi^{x_1}-1\}=\pm\sqrt{2}\{\xi^{x_2},b_l\}$ 可得

$$\pm\{\xi^{x_2}+b_l,\xi^{x_2}-b_l\}=\pm\sqrt{2}\{\xi^{x_1},1\},$$

从而

$$\bigcup_{\{x,y\}\in S_0}\pm\{x,y\}=H\cup\{\pm b_l\},\qquad\bigcup_{\{x,y\}\in S_0}\pm\{x-y,x+y\}=\sqrt{2}(H\cup\{\pm b_l\}).$$

对于任意 $j\in\{1,2,\ldots,t-1\}$, 令

$$S_j=\left\{b_j\{\xi^{2i-1},\xi^{2i}\}:1\leqslant i\leqslant\frac{|H|-2}{4}\right\}.$$

则

$$\bigcup_{\{x,y\}\in S_j}\pm\{x,y\}=b_jH\setminus\{\pm b_j\},\qquad\bigcup_{\{x,y\}\in S_j}\pm\{x-y,x+y\}=\sqrt{2}(b_jH\setminus\{\pm b_j\}).$$

最后令 $T=(\bigcup_{j=0}^{t-1}S_j)\cup S$. 应用两个已知条件, 易得 T 为 APS$(p,\alpha,\sqrt{2}\beta)$. □

引理 3.5 令 $p\equiv 7\pmod 8$ 为小于 50,000 的素数且 $H=C_0^t$, 其中 $t\equiv 3\pmod 4$. 若 $p\notin F:=\{599,1471,4447,4663,5039,6007,15319,15607,15991,16871,18911,26839,32887,37223,44087,47791\}$, 则对于任意 $\alpha\in\mathbb{Z}_p^*$, 存在 APS$(p,\alpha,\sqrt{2}\alpha)$.

证明 当 $p<300$ 时, 结论由定理 1.3 得到. 对于 50,000 以内其余模 8 余 7 的素数, 借助计算机搜索, 可验证构造 3.2 所需条件是否满足, 结果如下:

(1) $H=C_0^3$ 的素数共 184 个, 其中 $p>300$ 有 181 个元素, 均可以找到满足构造 3.2 条件的 x_1、x_2 和 b_l, 其中 $l=1,2$, 相关数据参见文献 [12, 表 III].

(2) $H=C_0^t$ ($t\equiv 3\pmod 4$, $t\geqslant 7$) 的素数共 55 个. 令

$$F'=\{2671,4463,5503,6791,8647,28463,28591,35527,39551\}.$$

当 $p\notin F\cup F'$ 时 (这样的 p 共 30 个), 均可以找到满足构造 3.2 条件的 x_1、x_2 和 b_l, 其中 $l=1,2$. 进一步地, 还可以在 4 个分圆陪集 C_3^t、C_4^t、C_5^t 和 C_6^t 中各找到一个代表做成集合 $\{y,z,u,v\}$ 且满足条件 $\pm\{y+z,y-z\}=\pm\sqrt{2}\{u,v\}$. 令

$$S=\left\{\omega^{4i}\{y,z\},\omega^{4i}\{u,v\}:0\leqslant i\leqslant\frac{t-7}{4}\right\}$$

(ω 是 $\mathbb{Z}_p$ 的本原根), 则 S 做成满足构造 3.2 条件的对子集 S, 其中,

$$\bar{R}=\left(\bigcup_{i=0}^{\frac{t-7}{4}}\omega^{4i}\{y,z,u,v\}\right)\cup\{\omega^j\},$$

$\{j,l\}=\{1,2\}$, $\alpha=\beta=\omega^j$. 相关数据参见文献 [12, 表 VI].

(3) 当 $p\in F'$ 时, 依然使用构造 3.2, 具体方法与上一情形类似, 但是此时 $l\neq 1,2$. 为了给出满足构造 3.2 两条件的陪集划分, 类似表 1, 本文给所有元素加下标表示其所在的分圆陪集, 即 y_a 表示 $y\in\omega^aC_0^t$, 具体信息见表 2.

综合上述 3 种情形, 应用构造 3.2 即得最终结论. □

综合引理 3.4 和 3.5 即得几乎可分集的另一个主要定理.

定理 3.3 令 $p\equiv 7\pmod 8$ 为小于 50,000 的素数且 $p\notin F$, 则对于任意 $\alpha\in\mathbb{Z}_p^*$, 存在 APS$(p,\alpha,\sqrt{2}\alpha)$, 其中 F 定义见引理 3.5, 包含 16 个可能的例外值.

表 2 引理 3.5 中 $p \in F'$ 数据

p	$\sqrt{2}$	ξ	ω	t	(x_1, x_2, b_l)	(y_a, z_c, u_d, v_e)
2,671	468	469	7	15	$(11, 22, 930_{14})$	$(7_1, 1746_3, 1539_4, 1737_6)$, $(49_2, 2459_5, 1923_{13}, 2312_8)$, $(875_7, 1899_9, 63_{10}, 774_{12})$
4,463	1,571	1,572	5	23	$(3, 16, 255_{11})$	$(3125_5, 3110_2, 3913_3, 625_4) \cdot \{1, \omega^4, \omega^{12}\}$, $(5_1, 4178_{10}, 3210_{18}, 182_{22})$, $(1136_{12}, 258_{13}, 1552_{20}, 2367_{19})$
5,503	475	5,027	3	7	$(5, 172, 4026_6)$	$(9_2, 3719_3, 4920_4, 4858_1)$
6,791	982	983	7	7	$(49, 86, 3265_6)$	$(49_2, 5769_3, 4418_4, 2954_1)$
8,647	93	8,553	3	11	$(53, 194, 676_8)$	$(27_3, 625_4, 4377_5, 6781_6)$, $(3_1, 807_2, 3077_9, 5849_7)$
28,463	4,042	24,420	5	19	$(179, 252, 22921_6)$	$(5_1, 25376_2, 4675_3, 15535_4) \cdot \{\omega^{4i} : i = 0, 2, 3\}$, $(3125_5, 25092_7, 15168_{17}, 6973_8)$
28,591	10,823	17,767	3	15	$(41, 220, 6245_7)$	$(3_1, 12168_2, 3998_3, 28471_4) \cdot \{1, \omega^8\}$, $(243_5, 8034_6, 3184_{13}, 25024_8)$
35,527	3,120	32,406	3	31	$(133, 286, 26181_{24})$	$(3_1, 21437_2, 15493_3, 29394_4) \cdot \{\omega^{4i} : i = 0, 1, 2, 3, 4, 6\}$, $(32012_{21}, 26545_{23}, 9003_{30}, 2040_{29})$
39,551	7,950	31,600	7	35	$(17, 168, 22150_{34})$	$(16807_5, 17862_2, 13591_4, 38332_3) \cdot \{\omega^{4i} : 0 \leqslant i \leqslant 7\}$

4 结论

可分集 (PS) 与几乎可分集 (APS) 是组合设计理论中两类重要的组合构型, 与许多其他组合结构具有密切联系. 由于可分集与几乎可分集的要求比较严苛, 其存在性问题迄今远未解决. 本文针对 $p \equiv 7 \pmod 8$ 为素数的情形, 建立 p^2 阶可分集与 p 阶几乎可分集的新构造, 参见构造 2.1、3.1 和 3.2. 应用这些构造方法, 对于 $p \equiv 7 \pmod 8$ 的素数 p, 本文得到 $p < 30{,}000$ 的 PS(p^2) 的存在性, 余下 141 个可能例外值 (定理 2.1), 还给出特定条件下 APS($p, \alpha, \sqrt{2}\alpha$) 的存在性和渐近存在性 (定理 3.1 和 3.2), 并确定 $p < 50{,}000$ 的 APS($p, \alpha, \sqrt{2}\alpha$) 的存在性, 仅余 16 个可能例外值 (定理 3.3).

参考文献

1 Abel R J R, Anderson I, Finizio N J. Necessary conditions for the existence of two classes of ZCPS-Wh(v). Discrete Appl Math, 2011, 159: 848–851

2 Anderson I, Finizio N J, Leonard P A. New product theorems for Z-cyclic whist tournaments. J Combin Theory Ser A, 1999, 88: 162–166

3 Chang Y, Costa S, Feng T, et al. Partitionable sets, almost partitionable sets and their applications. J Combin Des, 2020, 28: 783–813

4 Chang Y, Ji L. Optimal $(4up, 5, 1)$ optical orthogonal codes. J Combin Des, 2004, 12: 346–361

5 Hu S, Ge G. Necessary conditions and frame constructions for Z-cyclic patterned starter whist tournaments. Discrete Appl Math, 2012, 160: 2188–2198

6 Hu S, Ge G. Some new results on Z-cyclic patterned starter whist tournaments and related frames. J Combin Des, 2013, 21: 181–203

7 Jones J W, Leonard P A. Z-cyclic whist tournaments for q^2 players. J Combin Math Combin Comput, 2008, 66: 215–223

8 Ko C, Sun Q. Lecture Notes on Number Theory (in Chinese), 2nd ed. Beijing: Higher Education Press, 2001 [柯召, 孙琦. 数论讲义第二版 (上). 北京: 高等教育出版社, 2001]

9 Lidl R, Niederreiter H. Finite Fields. Cambridge: Cambridge University Press, 1997

10 Watson G L. Bridge problem. Math Gaz, 1954, 38: 129–130

11 Zhang J, Chang Y. Partitionable sets and cyclic BSECs with block size four. J Statist Plann Inference, 2009, 139: 1974–1979
12 Zhou J, Chang Y. New constructions for partitionable sets and almost partitionable sets. ChinaXiv:202204.00126, 2022

New constructions for partitionable sets and almost partitionable sets

Junling Zhou & Yanxun Chang

Abstract Partitionable sets (PS) and almost partitionable sets (APS) are two important types of combinatorial configurations in the design theory. They have intimate connections with other combinatorial structures such as $\mathbb{Z}$-cyclic patterned starter Whist tournaments, cyclic difference matrices, cyclic balanced sampling plans excluding contiguous units, disjoint difference families, and optical orthogonal codes. The existing problems of PS and APS remain far from being settled as they demand stringent requirements. In this paper, we focus on the case where $p \equiv 7 \pmod 8$ is a prime and establish new constructions for partitionable sets of order p^2 and almost partitionable sets of order p. In particular, for $p \equiv 7 \pmod 8$, we show the existence of PS of order p^2 for a large portion of primes $p < 30{,}000$, the existence and asymptotic existence of APS under certain conditions, and also the existence of APS of order p for all primes $p < 50{,}000$ with 16 possible exceptions.

Keywords **partitionable set, almost partitionable set, Whist tournament, cyclotomic class**

MSC(2020) **05B05**

doi: 10.1360/SSM-2022-0031