

强差族及其在相对差族、可分组设计和光正交码中的应用

杨凯璐, 王小苗*

(宁波大学 数学与统计学院, 浙江 宁波 315211)

摘要: 强差族在构造其他组合设计时发挥了重要作用. 本文给出了循环群上新的强差族, 尤其是借助型为2的强差族获得相对差族的更好的渐近存在结果. 通过分析与强差族相关的分圆条件, 从渐近存在和离散例子两个角度构造了相对差族. 利用计算机搜索的直接构造方法, 找到阶数小于下界的相对差族. 作为应用, 讨论了 $k \in \{6, 7, 8, 9\}$ 时区组大小为 k , 且组型为 $(k(k-1))^u$ 的可分组设计, 得到了权重为6、7、8或9的最优光正交码的无穷类.

关键词: 强差族; 相对差族; 分圆类; 可分组设计; 光正交码

中图分类号: O157.2

文献标志码: A

文章编号: 1001-5132 (2021) 05-0033-06

组合设计是组合数学的一个重要分支, 主要研究各种离散结构的存在性和构造性、分类和计数问题等. 近几十年来, 组合设计在通信技术和信息安全领域发挥了重要作用. 作为相对差集的自然推广, 相对差族在1998年由Buratti^[1]提出. 相对差族是构造组合设计的强有力工具, 在研究光正交码、光正交签名码方面具有重要应用.

由于相对差族的研究缺乏系统的构造方法, 1999年Buratti^[2]首次提出了强差族概念. 此后近10年对强差族的研究进展十分缓慢, 直到2008年, Buratti等^[3]讨论了任意图上的强差族, 推广了任意图上恰顶点可迁的完全多部图的图分解. 并建立了二面体群上的强差族, 从而得到了一类可分组设计. Momihara^[4]构造了循环强差族的无穷类, 同时给出了特殊参数强差族的不存在性证明. 此外, 借助平方和思想, 完全解决了二阶循环群上区组大小任意的强差族. Costa等^[5]借助强差族得到了框架差族, 即对应于可分解的循环相对差族. Bao等^[6]指出, 可分解的循环相对差族是构造严格最优跳频序列的重要工具, 跳频多址系统在现代通信系统, 如超宽带、军事通信等方面有广泛应用. Buratti^[7]通过引入哈达玛强差族得到了可划分差族. Ding

等^[8]利用可划分差族构造了最优常重复码, 后者在电力线通信的多进制数字频率调制中应用广泛. 关于强差族的相关成果, 还可参见文献[9-12].

本研究得到了循环群上强差族的新的结果, 并构造了相对差族的渐近存在和离散例子, 且利用相对差族扩大了可分组设计的存在性, 最后给出了组合设计理论在最优光正交码上的应用.

1 预备知识

在全文中, 集合和多重集分别用大括号 $\{\}$ 和方括号 $[\]$ 表示, 每个并集指保留元素重数的多重集的并. $A \cup A \cup \cdots \cup A$ (h 次)用 hA 表示.

令 $(G, +)$ 是一个有限群, 其中恒等元记作0. 令 $K = [k_1, k_2, \dots, k_s]$ 为正整数的集合, $\Sigma = [F_1, F_2, \dots, F_s]$ 是 G 的多重集构成的集族, 其中 $F_i = [f_{i,1}, f_{i,2}, \dots, f_{i,k_i}]$, $1 \leq i \leq s$. 若满足条件:

$$\Delta \Sigma := \bigcup_{i=1}^s \Delta F_i := \bigcup_{i=1}^s [f_{i,a} - f_{i,b} : 1 \leq a, b \leq k_i, a \neq b] = \mu G,$$

即 G 中每个元素(包括0)在多重集 $\Delta \Sigma$ 中恰出现 μ 次, 则 Σ 称为一个 (G, K, μ) -强差族(SDF). Σ 中元素称为基区组. 显然, $\mu | G| = \sum_{i=1}^s k_i(k_i - 1)$. 值得

收稿日期: 2021-03-11.

宁波大学学报(理工版)网址: <http://journallg.nbu.edu.cn/>

基金项目: 国家自然科学基金(11771227); 浙江省自然科学基金(LY21A010005); 宁波市自然科学基金(202003N4141); 浙江省省属高校基本科研业务费专项资金(SJLY2020008).

第一作者: 杨凯璐(1997-), 女, 浙江宁波人, 在读硕士研究生, 主要研究方向: 组合设计与编码理论. E-mail: yangkailu1997@163.com

*通信作者: 王小苗(1984-), 女, 浙江温州人, 博士/副教授, 主要研究方向: 组合设计与编码理论. E-mail: wangxiaomiao@nbu.edu.cn

注意的是, 由于元素 $0 \in G$ 在任意多重集中作为差总是出现偶数次, 故 μ 一定是偶数. 若每个基区组的大小均为 k , 则简记为 (G, k, μ) -SDF.

命题 1 若存在一个 (G, k, μ) -SDF, 则 μ 为偶数且 $\mu | G| \equiv 0 \pmod{k(k-1)}$.

对于正整数 r 和基区组 B , 令 $\underline{r}B$ 表示 B 在基区组的集合中出现 r 次.

引理 1^[12] 当 $(v, k, \mu) \in \{(56, 8, 4), (56, 8, 6), (72, 9, 4)\}$ 时, 存在一个 $(\mathbb{Z}_v, k, \mu)$ -SDF 为:

$(\mathbb{Z}_{56}, 8, 4)$ -SDF:

$$\begin{aligned} & [0, 0, 2, 9, 19, 32, 36, 50], \\ & [0, 0, 3, 9, 14, 34, 44, 52], \\ & [0, 1, 5, 11, 12, 28, 40, 41], \\ & [0, 2, 7, 21, 32, 40, 53, 55]. \end{aligned}$$

$(\mathbb{Z}_{56}, 8, 6)$ -SDF:

$$\begin{aligned} & \underline{2}[0, 1, 5, 11, 12, 30, 44, 52], \\ & \underline{2}[0, 2, 5, 21, 34, 37, 44, 52], \\ & [0, 0, 2, 13, 27, 30, 36, 36], \\ & [0, 0, 1, 8, 15, 26, 36, 54]. \end{aligned}$$

$(\mathbb{Z}_{72}, 9, 4)$ -SDF:

$$\begin{aligned} & [0, 0, 2, 12, 28, 36, 45, 59, 67], \\ & \underline{2}[0, 1, 2, 6, 24, 32, 53, 59, 62], \\ & [0, 0, 3, 18, 28, 35, 52, 61, 68]. \end{aligned}$$

一个 (G, N, k, λ) 相对差族 (DF), 或含有 n 阶子群 N 的 g 阶群 $(G, +)$ 上的 (g, n, k, λ) -DF 是指 G 的 k -元子集构成的族 $\mathfrak{B} = [B_1, B_2, \dots, B_r]$ (基区组), 使得:

$$\Delta \mathfrak{B} := \bigcup_{i=1}^r \Delta B_i := \bigcup_{i=1}^r [x - y : x, y \in B_i, x \neq y] = \underline{\lambda}(G \setminus N),$$

即, $G \setminus N$ 中的每个元素在多重集 $\Delta \mathfrak{B}$ 中恰出现 λ 次, 且 N 中的元素在 $\Delta \mathfrak{B}$ 中不出现. 若 G 是循环群, 称 (g, n, k, λ) -DF 是循环的.

2 强差族和相对差族

令 q 为素数幂, $\mathbb{F}_q$ 为 q 阶有限群, $\mathbb{F}_q^*$ 为 $\mathbb{F}_q$ 的乘法群. 若 $q \equiv 1 \pmod{e}$, $C_0^{e,q}$ 表示模 q 时本原 e 次幂构成的乘法子群. 给定 $\mathbb{F}_q$ 的本原元 ω , 令 $C_i^{e,q} = \omega^i \cdot C_0^{e,q}$, 其中 $i = 0, 1, \dots, e-1$, 称 $\mathbb{F}_q^*$ 中 $C_0^{e,q}$ 的陪集 $C_0^{e,q}, C_1^{e,q}, \dots, C_{e-1}^{e,q}$ 为指数是 e 的分圆类. 令 A 是 $\mathbb{F}_q^*$ 的多重子集, 对于 $0 \leq i \leq e-1$, 若每个分

圆陪集 $C_i^{e,q}$ 恰包含 A 中的 λ 个元素, 则称 A 为这些陪集的 λ -横截. 若 A 是 1-横截, A 通常被称为 $\mathbb{F}_q^*$ 中 $C_0^{e,q}$ 的陪集的代表元系.

全文中, 给定正整数 d 和 m , 令

$$Q(d, m) = \frac{1}{4} \left(U + \sqrt{U^2 + 4d^{m-1}m} \right)^2,$$

其中: $U = \sum_{h=1}^m \binom{m}{h} (d-1)^h (h-1)$.

定理 1^[4] 若存在一个 (G, k, μ) -SDF, 其中 $\mu = \lambda d$, 则当 λ 为偶数, 素数幂 $q \equiv 1 \pmod{d}$ 且 $q > Q(d, k-1)$ 时; 或者当 λ 为奇数, 素数幂 $q \equiv d+1 \pmod{2d}$ 且 $q > Q(d, k-1)$ 时, 存在一个 $(G \times \mathbb{F}_q, G \times \{0\}, k, \lambda)$ -DF.

引理 2 存在一个 $(\mathbb{Z}_{30}, 6, 4)$ -SDF.

证明 所求的 SDF 为 $\Sigma = [A_1, A_2, A_3, A_4]$, 其中:

$$\begin{aligned} A_1 &= [0, 0, 1, 7, 15, 20], \quad A_2 = [0, 0, 2, 13, 18, 26], \\ A_3 &= A_4 = [0, 1, 3, 6, 10, 22]. \end{aligned}$$

令 G 为一个群, C 是 $G \times \mathbb{F}_q$ 的子集. 令 $s \in \mathbb{F}_q^*$, 定义符号 $C \cdot \{(1, s)\} := \{(x, ys) : (x, y) \in C\}$.

定理 2 当素数 $q \equiv 5 \pmod{8}$ 且 $q > 13$ 时, 存在一个 $(\mathbb{Z}_{30} \times \mathbb{F}_q, \mathbb{Z}_{30} \times \{0\}, 6, 1)$ -DF.

证明 由引理 2 知, 存在一个 $(\mathbb{Z}_{30}, 6, 4)$ -SDF. 利用定理 1 得到素数 $q \equiv 5 \pmod{8}$ 且 $q > Q(4, 5) = 7938048$ 时的 DF. 当 $q \equiv 5 \pmod{8}$ 且 $q \leq Q(4, 5)$ 时, 利用计算机搜索, 得到 $(\mathbb{Z}_{30} \times \mathbb{F}_q, \mathbb{Z}_{30} \times \{0\}, 6, 1)$ -DF 中 $1 \leq i \leq 15$ 时 a_i 的所有值:

$$\begin{aligned} & \{(0, 0), (0, a_1), (1, a_2), (7, a_3), (15, a_4), \\ & \quad (20, a_5)\} \cdot \{(1, x)\}, \\ & \{(0, 0), (0, a_6), (2, a_7), (13, a_8), (18, a_9), \\ & \quad (26, a_{10})\} \cdot \{(1, x)\}, \\ & \{(0, 0), (1, a_{11}), (3, a_{12}), (6, a_{13}), (10, a_{14}), \\ & \quad (22, a_{15})\} \cdot \{(1, y)\}, \end{aligned}$$

其中: x 取遍 $C_0^{4,q}$; y 取遍 $C_0^{2,q}$.

感兴趣的读者可从作者处得到这些数据. 因 2020 年 Chang 等^[10]在定理 3 中已给出了素数 $q \equiv 1 \pmod{6}$ 时 $(\mathbb{Z}_{30} \times \mathbb{F}_q, \mathbb{Z}_{30} \times \{0\}, 6, 1)$ -DF, 因此这里只罗列 $q \not\equiv 1 \pmod{6}$ 时的情况. 如当 $13 < q < 200$ 时取

$$\begin{aligned} q = 29 : & (a_1, \dots, a_{15}) = \\ & (1, 7, 11, 2, 19, 2, 14, 3, 1, 7, 2, 1, 3, 6, 14); \\ q = 53 : & (a_1, \dots, a_{15}) = \\ & (1, 10, 11, 2, 17, 2, 20, 5, 22, 21, 2, 1, 20, 19, 35); \end{aligned}$$

$$q = 101 : (a_1, \dots, a_{15}) = (1, 5, 6, 2, 8, 2, 1, 16, 41, 55, 2, 4, 12, 6, 28);$$

$$q = 149 : (a_1, \dots, a_{15}) = (1, 3, 5, 2, 7, 2, 1, 5, 69, 14, 1, 3, 4, 11, 54);$$

$$q = 173 : (a_1, \dots, a_{15}) = (1, 3, 10, 2, 12, 2, 1, 10, 25, 43, 1, 3, 4, 6, 23);$$

$$q = 197 : (a_1, \dots, a_{15}) = (1, 12, 13, 2, 14, 2, 1, 4, 50, 82, 1, 3, 2, 9, 10).$$

如下给出一个 $(\mathbb{Z}_{30} \times \mathbb{F}_{29}, \mathbb{Z}_{30} \times \{0\}, 6, 1)$ -DF 的例子来解释定理 2 的构造方法.

例 1 存在一个 $(\mathbb{Z}_{30} \times \mathbb{F}_{29}, \mathbb{Z}_{30} \times \{0\}, 6, 1)$ -DF.

证明 构造基区组的集合 $\mathcal{C} = \{C_1, C_2, C_3, C_4\}$, 其中基区组的第一部分来自引理 2 中的 $(\mathbb{Z}_{30}, 6, 4)$ -SDF.

$$\begin{aligned} C_1 &= \{(0, 0), (0, 1), (1, 7), (7, 11), (15, 2), (20, 19)\}, \\ C_2 &= \{(0, 0), (0, 2), (2, 14), (13, 3), (18, 1), (26, 7)\}, \\ C_3 &= \{(0, 0), (1, 2), (3, 1), (6, 3), (10, 6), (22, 14)\}, \\ C_4 &= \{(0, 0), (1, -2), (3, -1), (6, -3), (10, -6), \\ &\quad (22, -14)\}. \end{aligned}$$

易验证

$$\Delta \mathcal{C} = \bigcup_{g \in \mathbb{Z}_{30}} (\{g\} \times D_g),$$

其中: $D_0 = \pm\{1, 2\}$, $D_1 = \{6, 7, \pm 2\}$, $D_2 = \{12, 14, \pm 1\}$, $D_3 = \pm\{1, 2\}$, $D_4 = \{22, 24, \pm 3\}$, $D_5 = \{17, 27, \pm 1\}$, $D_6 = \{4, 7, \pm 3\}$, $D_7 = \{10, 11, \pm 5\}$, $D_8 = \{6, 20, \pm 14\}$, $D_9 = \pm\{4, 12\}$, $D_{10} = \{10, 11, \pm 6\}$, $D_{11} = \{17, 18, \pm 13\}$, $D_{12} = \pm\{1, 8\}$, $D_{13} = \{1, 3, 4, 8\}$, $D_{14} = \{13, 24, \pm 1\}$, $D_{15} = \pm\{1, 2\}$, 且对于 $16 \leq i \leq 29$, 有 $D_i = -D_{30-i}$. 注意到 $-1 \in C_2^{4,29}$. 对于任意的 $g \in \mathbb{Z}_{30}$, 每个 D_g 是 $\mathbb{F}_{29}^*$ 中 $C_0^{4,29}$ 的陪集的一个 1-横截, 故集族 $\{C \cdot \{(1, s)\} : s \in C_0^{4,29}, C \in \mathcal{C}\}$ 构成一个 $(\mathbb{Z}_{30} \times \mathbb{F}_{29}, \mathbb{Z}_{30} \times \{0\}, 6, 1)$ -DF.

引理 3 存在一个 $(\mathbb{Z}_{42}, 7, 4)$ -SDF.

证明 所求的 SDF 为 $\Sigma = [A_1, A_2, A_3, A_4]$, 其中 $A_1 = [0, 0, 2, 14, 21, 31, 36]$, $A_2 = [0, 0, 3, 11, 16, 26, 33]$, $A_3 = A_4 = [0, 1, 2, 5, 25, 29, 35]$.

定理 3 当素数 $q \equiv 5 \pmod{8}$ 且 $q > 13$ 时, 存在一个 $(\mathbb{Z}_{42} \times \mathbb{F}_q, \mathbb{Z}_{42} \times \{0\}, 7, 1)$ -DF.

证明 由引理 3 知, 存在一个 $(\mathbb{Z}_{42}, 7, 4)$ -SDF. 应用定理 1 得到素数 $q \equiv 5 \pmod{8}$ 且 $q > Q(4, 6) = 205561856$ 时的 DF. 当 $q \equiv 5 \pmod{8}$ 且 $q \leq Q(4, 6)$ 时, 利用计算机搜索得到如下 $(\mathbb{Z}_{42} \times \mathbb{F}_q, \mathbb{Z}_{42} \times \{0\},$

7, 1)-DF 中 $1 \leq i \leq 18$ 时 a_i 的所有值:

$$\begin{aligned} &\{(0, 0), (0, a_1), (2, a_2), (14, a_3), (21, a_4), (31, a_5), \\ &\quad (36, a_6)\} \cdot \{(1, x)\}, \\ &\{(0, 0), (0, a_7), (3, a_8), (11, a_9), (16, a_{10}), (26, a_{11}), \\ &\quad (33, a_{12})\} \cdot \{(1, x)\}, \\ &\{(0, 0), (1, a_{13}), (2, a_{14}), (5, a_{15}), (25, a_{16}), (29, a_{17}), \\ &\quad (35, a_{18})\} \cdot \{(1, y)\}, \end{aligned}$$

其中: x 取遍 $C_0^{4,q}$; y 取遍 $C_0^{2,q}$.

感兴趣的读者可以从作者处得到这些数据.

例如, 当 $13 < q < 200$ 时, 取

$$\begin{aligned} q = 29 : (a_1, \dots, a_{18}) &= (1, 7, 11, 2, 15, 18, 2, 17, 9, \\ &\quad 27, 18, 22, 1, 3, 4, 18, 5, 21); \\ q = 37 : (a_1, \dots, a_{18}) &= (1, 11, 12, 2, 3, 20, 2, 15, 4, \\ &\quad 33, 26, 22, 1, 6, 3, 14, 7, 32); \\ q = 53 : (a_1, \dots, a_{18}) &= (1, 10, 11, 2, 4, 17, 2, 34, 19, \\ &\quad 28, 26, 35, 1, 3, 2, 14, 22, 20); \\ q = 61 : (a_1, \dots, a_{18}) &= (1, 7, 8, 2, 3, 14, 2, 14, \\ &\quad 4, 11, 56, 30, 1, 3, 5, 10, 40, 16); \\ q = 101 : (a_1, \dots, a_{18}) &= (1, 5, 6, 2, 4, 8, 2, 10, 13, \\ &\quad 92, 18, 41, 1, 3, 2, 16, 51, 46); \\ q = 109 : (a_1, \dots, a_{18}) &= (1, 4, 5, 2, 3, 11, 2, 1, 49, \\ &\quad 30, 34, 82, 1, 11, 3, 4, 53, 58); \\ q = 149 : (a_1, \dots, a_{18}) &= (1, 3, 5, 2, 4, 7, 2, 1, 70, \\ &\quad 128, 69, 59, 1, 4, 6, 2, 14, 28); \\ q = 157 : (a_1, \dots, a_{18}) &= (1, 6, 10, 2, 3, 11, 2, 3, 5, \\ &\quad 96, 49, 146, 1, 3, 9, 11, 24, 31); \\ q = 173 : (a_1, \dots, a_{18}) &= (1, 3, 10, 2, 4, 12, 2, 1, 79, \\ &\quad 118, 32, 147, 1, 4, 6, 2, 69, 40); \\ q = 181 : (a_1, \dots, a_{18}) &= (1, 4, 5, 2, 3, 7, 2, 1, 83, \\ &\quad 117, 150, 14, 1, 7, 17, 3, 31, 91); \\ q = 197 : (a_1, \dots, a_{18}) &= (1, 12, 13, 2, 4, 14, 2, 1, 4, \\ &\quad 154, 106, 173, 1, 4, 2, 48, 37, 133). \end{aligned}$$

引理 4^[12] 当 $u \in \{61, 67\}$ 时, 存在一个 $(\mathbb{Z}_{56} \times \mathbb{F}_u, \mathbb{Z}_{56} \times \{0\}, 8, 1)$ -DF.

命题 2^[10] 令 $(G, +)$ 为一个群(不一定是交换群). 若一个 (G, k, μ) -SDF, 记为 Σ , 是 3 个集合 Σ_1 , Σ_2 和 Σ_3 的并集(每一个集合均可以是空集), 满足:

(1) 对于任意 $A \in \Sigma_1$, A 形如 $[x_1, \delta + x_1, x_2, \delta + x_2, \dots, x_{k/2}, \delta + x_{k/2}]$, 若 k 为偶数; $[0, x_1, \delta + x_1, x_2, \delta + x_2, \dots, x_{\lfloor k/2 \rfloor}, \delta + x_{\lfloor k/2 \rfloor}]$, 若 k 为奇数; 其中: δ 是 G

的一个对合或零, 且 $\Delta[x_1, x_2, \dots, x_{\lfloor k/2 \rfloor}]$ 既不包含对合也不包含零.

(2) 对于任意 $A \in \Sigma_2$, $\Delta(A)$ 中的每个元素是一个对合或零.

(3) 对于任意 $A \in \Sigma_3$, Σ_3 中 A 的重数是偶数且 $\Delta(A)$ 既不包含对合也不包含零.

则 Σ 称为型为 2 的 SDF.

引理 5 由命题 2 知, 型为 2 的 $(\mathbb{Z}_{56}, 8, 8)$ -SDF 中 Σ_1 和 Σ_3 如下所示:

$$\begin{aligned}\Sigma_1: & [0, 0, 5, 5, 19, 19, 41, 41], \\ & [0, 28, 3, 31, 7, 35, 20, 48], \\ \Sigma_3: & 2[0, 1, 2, 9, 15, 25, 26, 27], \\ & [0, 2, 4, 13, 23, 46, 50, 53], \\ & [0, 3, 9, 21, 27, 39, 43, 48].\end{aligned}$$

定理 4^[10] 如果存在满足命题 2 条件的一个 (G, k, μ) -SDF, 则存在一个 $(G \times \mathbb{F}_q, G \times \{0\}, k, 1)$ -DF, 其中素数幂 $q \equiv 1 \pmod{\mu}$ 且 $q > Q(\mu/2, k-1)$.

定理 5 当素数幂 $q \equiv 1 \pmod{4}$ 且 $q > Q(4, 7)$, 或 $q \equiv 7 \pmod{12}$ 且 $q > Q(6, 7)$ 时, 存在一个 $(\mathbb{Z}_{56} \times \mathbb{F}_q, \mathbb{Z}_{56} \times \{0\}, 8, 1)$ -DF.

证明 当 $q \equiv 1 \pmod{8}$ 且 $q > Q(4, 7)$ 时, 由引理 5 知, 存在一个型为 2 的 $(\mathbb{Z}_{56}, 8, 8)$ -SDF. 应用定理 4 得到所需的 DF. 当 $q \equiv 5 \pmod{8}$ 且 $q > Q(4, 7)$ 时, 由引理 1 知, 存在一个 $(\mathbb{Z}_{56}, 8, 4)$ -SDF. 应用定理 1 得到所需的 DF. 当 $q \equiv 7 \pmod{12}$ 且 $q > Q(6, 7)$ 时, 由引理 1 知, 存在一个 $(\mathbb{Z}_{56}, 8, 6)$ -SDF. 应用定理 1 得到所需的 DF.

定理 6 当素数 $q \equiv 5 \pmod{8}$ 时, 存在一个 $(\mathbb{Z}_{72} \times \mathbb{F}_q, \mathbb{Z}_{72} \times \{0\}, 9, 1)$ -DF, 其中 $q > Q(4, 8)$ 或 $37 \leq q \leq 9973$.

证明 当素数 $q \equiv 5 \pmod{8}$ 且 $q > Q(4, 8)$ 时, 由引理 1 知, 存在一个 $(\mathbb{Z}_{72}, 9, 4)$ -SDF. 应用定理 1 得到一个 $(\mathbb{Z}_{72} \times \mathbb{F}_q, \mathbb{Z}_{72} \times \{0\}, 9, 1)$ -DF. 当 $q \equiv 5 \pmod{8}$ 且 $37 \leq q \leq 9973$ 时, 利用计算机搜索可以得到如下 $(\mathbb{Z}_{72} \times \mathbb{F}_q, \mathbb{Z}_{72} \times \{0\}, 9, 1)$ -DF 中 $1 \leq i \leq 24$ 时 a_i 的所有值:

$$\begin{aligned}& \{(0, 0), (0, a_1), (2, a_2), (12, a_3), (28, a_4), (36, a_5), \\ & (45, a_6), (59, a_7), (67, a_8)\} \cdot \{(1, x)\}; \\ & \{(0, 0), (0, a_9), (3, a_{10}), (18, a_{11}), (28, a_{12}), (35, a_{13}), \\ & (52, a_{14}), (61, a_{15}), (68, a_{16})\} \cdot \{(1, x)\}; \\ & \{(0, 0), (1, a_{17}), (2, a_{18}), (6, a_{19}), (24, a_{20}), (32, a_{21}),\end{aligned}$$

$$(53, a_{22}), (59, a_{23}), (62, a_{24})\} \cdot \{(1, y)\},$$

其中: x 取遍 $C_0^{4,q}$; y 取遍 $C_0^{2,q}$.

感兴趣的读者可以从作者处得到这些数据. 例如, 当 $37 \leq q \leq 100$ 时 a_i 的值可以在 Wang 等^[12] 引理 2.4 中找到, 其中 $1 \leq i \leq 24$. 当 $100 < q < 200$ 时, 取

$$\begin{aligned}q = 101: & (a_1, \dots, a_{24}) = \\ & (1, 5, 6, 2, 4, 12, 42, 71, 2, 84, 19, 14, 41, 87, \\ & 48, 93, 1, 3, 4, 22, 18, 16, 43, 32), \\ q = 109: & (a_1, \dots, a_{24}) = \\ & (1, 4, 5, 2, 3, 11, 91, 46, 2, 101, 66, 95, 28, 38, \\ & 70, 73, 1, 11, 3, 9, 41, 19, 63, 62), \\ q = 149: & (a_1, \dots, a_{24}) = \\ & (1, 3, 5, 2, 4, 7, 14, 103, 2, 116, 59, 110, 15, 10, \\ & 88, 50, 1, 4, 3, 2, 6, 46, 24, 42), \\ q = 157: & (a_1, \dots, a_{24}) = \\ & (1, 6, 10, 2, 3, 11, 21, 79, 2, 42, 104, 53, 133, 137, \\ & 12, 3, 1, 3, 5, 57, 25, 11, 156, 62), \\ q = 173: & (a_1, \dots, a_{24}) = \\ & (1, 3, 10, 2, 4, 12, 14, 22, 2, 25, 43, 146, 147, \\ & 131, 57, 28, 1, 4, 3, 62, 5, 30, 39, 67), \\ q = 181: & (a_1, \dots, a_{24}) = \\ & (1, 4, 5, 2, 3, 7, 19, 31, 2, 23, 137, 57, 63, 38, \\ & 170, 76, 1, 7, 2, 20, 13, 42, 33, 92), \\ q = 197: & (a_1, \dots, a_{24}) = \\ & (1, 12, 13, 2, 4, 14, 16, 126, 2, 124, 71, 97, 62, \\ & 68, 25, 126, 1, 4, 5, 48, 8, 20, 117, 58).\end{aligned}$$

3 组型为 $(k(k-1))^u$ 的 k -可分组设计

相对差族可以用来构造可分组设计. 令 K 为正整数的集合. 一个可分组设计(GDD) K -GDD 是指一个三元组 $(X, \mathcal{G}, \mathcal{A})$, 满足性质: (1) $\mathcal{G}$ 是有限集 X 的一个划分(称为组); (2) $\mathcal{A}$ 是 X 中大小取自 K 的子集构成的集合(称为区组), 使得 X 的每个 2-子集恰包含在一个区组中或恰包含在一个组中, 但不能同时包含在区组和组中. 若 $\mathcal{G}$ 含有 u_i 个大小为 g_i 的组, 其中 $1 \leq i \leq r$, 则称 $g_1^{u_1} g_2^{u_2} \dots g_r^{u_r}$ 为 GDD 的组型. 当 $K = \{k\}$ 时, 简记为 k -GDD.

引理 6

(1) 当 $u \in \{6, 16, 21, 25, 26, 36, 41, 42, 48, 49, 51, 66, 71, 76, 78, 81, 84, 85, 86, 90, 91, 96\} \cup \{q : q \equiv 1 \pmod{6}\}$ 是

素数}时, 存在一个组型为 30^u 的6-GDD^[10].

(2) 当 $u \in \{7, 8, 9, 15, 17, 28, 33, 36, 41, 49, 50, 56, 57, 63, 64, 65, 70, 71, 72, 73, 77, 78, 80, 81, 85, 88, 91, 92, 96, 97, 99\}$ 时, 存在一个组型为 42^u 的7-GDD^[13].

(3) 当 $u \in \{8, 9, 10, 15, 16, 17, 29, 30, 33, 36, 37, 41, 43, 44, 49, 50, 51, 53, 54, 55, 57, 58, 63, 64, 65, 71, 72, 73, 74\} \cup [79, 99]$ 时, 存在一个组型为 56^u 的8-GDD^[13].

(4) 当 $u \in \{9, 10, 17, 19, 49, 54, 55, 57, 58, 64, 65, 66, 73, 74, 80, 81, 89, 90, 91\}$ 时, 存在一个组型为 72^u 的9-GDD^[13].

引理7 当素数 $q \equiv 5(\text{mod } 8)$ 且 $q > 13$ 时, 存在一个组型为 30^q 的6-GDD.

证明 由定理2知, 当素数 $q \equiv 5(\text{mod } 8)$ 且 $q > 13$ 时, 存在一个 $(\mathbb{Z}_{30} \times \mathbb{F}_q, \mathbb{Z}_{30} \times \{0\}, 6, 1)$ -DF. 由 $\mathbb{Z}_{30} \times \mathbb{F}_q$ 上该DF的基区组可生成组型为 30^q 的6-GDD.

结合引理6中(1)和引理7, 得到以下定理.

定理7 当 $u \in \{6, 16, 21, 25, 26, 36, 41, 42, 48, 49, 51, 66, 71, 76, 78, 81, 84, 85, 86, 90, 91, 96\} \cup \{q: q > 5, q \equiv 1, 5, 7, 13, 19(\text{mod } 24) \text{ 是素数}\}$ 时, 存在一个组型为 30^u 的6-GDD.

引理8 当素数 $q \equiv 5(\text{mod } 8)$ 且 $q > 13$ 时, 存在一个组型为 42^q 的7-GDD.

证明 由定理3知, 当素数 $q \equiv 5(\text{mod } 8)$ 且 $q > 13$ 时, 存在一个 $(\mathbb{Z}_{42} \times \mathbb{F}_q, \mathbb{Z}_{42} \times \{0\}, 7, 1)$ -DF. 由 $\mathbb{Z}_{42} \times \mathbb{F}_q$ 上该DF的基区组可生成组型为 42^q 的7-GDD.

结合引理6中(2)和引理8, 得到以下定理.

定理8 当 $u \in \{7, 8, 9, 15, 17, 28, 33, 36, 41, 49, 50, 56, 57, 63, 64, 65, 70, 71, 72, 73, 77, 78, 80, 81, 85, 88, 91, 92, 96, 97, 99\} \cup \{q: q > 13, q \equiv 5(\text{mod } 8) \text{ 是素数}\}$ 时, 存在一个组型为 42^u 的7-GDD.

引理9 当素数 $q \equiv 1(\text{mod } 4)$ 且 $q > Q(4, 7)$, 或 $q \equiv 7(\text{mod } 12)$ 且 $q > Q(6, 7)$ 时, 存在一个组型为 56^q 的8-GDD.

证明 由定理5知, 当素数 $q \equiv 1(\text{mod } 4)$ 且 $q > Q(4, 7)$, 或 $q \equiv 7(\text{mod } 12)$ 且 $q > Q(6, 7)$ 时, 存在一个 $(\mathbb{Z}_{56} \times \mathbb{F}_q, \mathbb{Z}_{56} \times \{0\}, 8, 1)$ -DF. 由 $\mathbb{Z}_{56} \times \mathbb{F}_q$ 上该DF的基区组可生成组型为 56^q 的8-GDD.

定理9 当 $u \in \{8, 9, 10, 15, 16, 17, 29, 30, 33, 36, 37, 41, 43, 44, 49, 50, 51, 53, 54, 55, 57, 58, 61, 63, 64, 65, 67, 71, 72,$

$73, 74\} \cup [79, 99] \cup \{q: q > 4848812032, q \equiv 1(\text{mod } 4) \text{ 是素数}\} \cup \{q: q > 1830677303808, q \equiv 7(\text{mod } 12) \text{ 是素数}\}$ 时, 存在一个组型为 56^u 的8-GDD.

证明 由引理4知, 当 $u \in \{61, 67\}$ 时, 存在一个 $(\mathbb{Z}_{56} \times \mathbb{F}_u, \mathbb{Z}_{56} \times \{0\}, 8, 1)$ -DF, 故由 $\mathbb{Z}_{56} \times \mathbb{F}_u$ 上该DF的基区组可生成组型为 56^u 的8-GDD. 当 $u \notin \{61, 67\}$ 时, 由引理6中(3)和引理9可以得到组型为 56^u 的8-GDD, 其中 $Q(4, 7) = 4848812032$, $Q(6, 7) = 1830677303808$.

引理10 令素数 $q \equiv 5(\text{mod } 8)$. 当 $q > Q(4, 8)$ 或 $37 \leq q \leq 9973$ 时, 存在一个组型为 72^q 的9-GDD.

证明 由定理6知, 在 $\mathbb{Z}_{72} \times \mathbb{F}_q$ 上由 $(\mathbb{Z}_{72} \times \mathbb{F}_q, \mathbb{Z}_{72} \times \{0\}, 9, 1)$ -DF的基区组可以生成一个组型为 72^q 的9-GDD.

由于 $Q(4, 8) = 107375099904$, 故结合引理6中(4)和引理10得到以下定理.

定理10 当 $u \in \{9, 10, 17, 19, 49, 54, 55, 57, 58, 64, 65, 66, 73, 74, 80, 81, 89, 90, 91\} \cup \{q: q \in [37, 9973] \cup [107375099904, +\infty), q \equiv 5(\text{mod } 8) \text{ 是素数}\}$ 时, 存在一个组型为 72^u 的9-GDD.

4 最优光正交码

利用定理2、3、5和6来构造最优光正交码. 一个码重为 k 的 $(v, k, 1)$ -光正交码(OOC)是指 $\mathbb{Z}_v$ 的一些 k -元子集(称为码字)构成的集合, 要求子集中的任意2个元素做差, 使得该集合产生的所有的差均不重复, 称 $\mathbb{Z}_v$ 中不出现在这些差中的元素构成的集合为差剩余. 若差剩余的大小为小于或等于 $k(k-1)$, 则称该光正交码为最优的.

一个循环 $(gv, g, k, 1)$ -DF可被看作是一个 $(gv, k, 1)$ -OOC, 其中差剩余恰为 $\{0, v, 2v, \dots, (g-1)v\}$.

定理11 (1) 当素数 $q \equiv 5(\text{mod } 8)$ 且 $q > 13$ 时, 存在一个最优 $(k(k-1)q, k, 1)$ -OOC, 其中 $k \in \{6, 7\}$. (2) 当素数 $q \equiv 1(\text{mod } 4)$ 且 $q > Q(4, 7)$, 或 $q \equiv 7(\text{mod } 12)$ 且 $q > Q(6, 7)$ 时, 存在一个最优 $(56q, 8, 1)$ -OOC. (3) 令素数 $q \equiv 5(\text{mod } 8)$, 当 $q > Q(4, 8)$ 或 $37 \leq q \leq 9973$ 时, 存在一个最优 $(72q, 9, 1)$ -OOC.

证明 若 $k(k-1)$ 和 q 互素, 则 $\mathbb{Z}_{k(k-1)} \times \mathbb{Z}_q$ 同构于 $\mathbb{Z}_{k(k-1)q}$. 由定理2、3、5和6知, 存在一个循环 $(k(k-1)q, k(k-1), k, 1)$ -DF, 其中 $k \in \{6, 7, 8, 9\}$. 故存在一个 $(k(k-1)q, k, 1)$ -OOC, 其中差剩余为

$\{0, q, 2q, \dots, (k(k-1)-1)q\}$. 由于差剩余的大小恰好等于 $k(k-1)$, 因此得到的光正交码是最优的.

参考文献:

- [1] Buratti M. Recursive constructions for difference matrices and relative difference families[J]. Journal of Combinatorial Designs, 1998, 6(3):165-182.
- [2] Buratti M. Old and new designs via difference multisets and strong difference families[J]. Journal of Combinatorial Designs, 1999, 7(6):406-425.
- [3] Buratti M, Gionfriddo L. Strong difference families over arbitrary graphs[J]. Journal of Combinatorial Designs, 2008, 16(6):443-461.
- [4] Momihara K. Strong difference families, difference covers, and their applications for relative difference families[J]. Designs, Codes and Cryptography, 2009, 51(3):253-273.
- [5] Costa S, Feng T, Wang X M. Frame difference families and resolvable balanced incomplete block designs[J]. Designs, Codes and Cryptography, 2018, 86(12):2725-2745.
- [6] Bao J J, Ji L J. Frequency hopping sequences with optimal partial hamming correlation[J]. IEEE Transactions on Information Theory, 2016, 62(6):3768-3783.
- [7] Buratti M. Hadamard partitioned difference families and their descendants[J]. Cryptography and Communications, 2019, 11(4):557-562.
- [8] Ding C S, Yin J X. Combinatorial constructions of optimal constant-composition codes[J]. IEEE Transactions on Information Theory, 2005, 51(10):3671-3674.
- [9] Buratti M, Pasotti A. Combinatorial designs and the theorem of Weil on multiplicative character sums[J]. Finite Fields and Their Applications, 2009, 15(3):332-344.
- [10] Chang Y X, Costa S, Feng T, et al. Strong difference families of special types[J]. Discrete Mathematics, 2020, 343(4):111776.
- [11] Costa S, Feng T, Wang X M. New 2-designs from strong difference families[J]. Finite Fields and Their Applications, 2018, 50:391-405.
- [12] Wang X M, Feng T, Wang S X. Existence of strong difference families and constructions for eight new 2-designs[J]. Journal of Combinatorial Designs, 2021, 29(4):225-242.
- [13] Abel R J R, Greig M. CRC Handbook of Combinatorial Designs[M]. Boca Raton: Chapman & Hall/CRC Press, 2007:72-79.

Strong difference families and their applications in relative difference families, group divisible designs and optical orthogonal codes

YANG Kailu, WANG Xiaomiao*

(School of Mathematics and Statistics, Ningbo University, Ningbo 315211, China)

Abstract: The concept of strong difference family plays an important role in constructions of other combinatorial designs. In this paper, some new strong difference families in cyclic groups are presented. In particular, strong difference families of type 2 are focused to help investigate the asymptotic existence results for relative difference families. Through applying the cyclotomic conditions attached to strong difference families, relative difference families are produced from both asymptotic existences and discrete examples. Based on the computer search, direct construction is employed to obtain a relative difference family whose order is smaller than the lower bound. As given in applications, the group divisible designs of type $(k(k-1))^u$ with block size k are discussed for $k \in \{6, 7, 8, 9\}$, and several classes of optimal optical orthogonal codes with weights 6, 7, 8 or 9 are derived.

Key words: strong difference family; relative difference family; cyclotomic class; group divisible design; optical orthogonal code

(责任编辑 史小丽)