最优 $(m, n, 4, 1)$ 光正交签名码的进一步结果

潘蓉, 常彦勋*

北京交通大学数学系, 北京 100044

E-mail: 10118358@bjtu.edu.cn, yxchang@bjtu.edu.cn

收稿日期: 2014-01-15; 接受日期: 2014-07-05; * 通信作者

国家自然科学基金 (批准号: 11271042) 资助项目

摘要 为支持高速多址网络中二维图像的传输, Kitayama 首次提出码分多址并行图像传输系统的概念. 作为码分多址并行图像传输系统的首选光地址码, 光正交签名码 (OOSPC) 是一族具有良好相关性的 Hamming 重量为 k 的 $m \times n$ $(0, 1)$ - 矩阵. 用 $\Theta(m, n, k, \lambda)$ 表示所有参数为 (m, n, k, λ) 的 OOSPC 中码字容量可能的最大值, 则称码字容量为 $\Theta(m, n, k, \lambda)$ 的 (m, n, k, λ) -OOSPC 是最优的. 本文将针对满足下列条件之一的正整数 m 和 n :

(1) $mn \equiv 8, 16 \pmod{24}$, $\gcd(m, n, 2) = 2$, 且 $mn \equiv 16 \pmod{32}$ 和 $\gcd(m, n, 4) = 2$ 不同时成立, 其中 m 和 n 的所有奇素因子均模 6 余 1;

(2) $mn \equiv 0 \pmod{24}$ 且 $\gcd(m, n, 6) = 2$, 证明 $\Theta(m, n, 4, 1) = \lfloor \frac{mn-1}{12} \rfloor$, 即构造码字容量为 $\lfloor \frac{mn-1}{12} \rfloor$ 的最优 $(m, n, 4, 1)$ -OOSPC.

关键词 光正交签名码 严格 G - 不变填充设计 差阵

MSC (2010) 主题分类 05B40

1 引言

光纤通信凭借着高速、宽带、灵活、高效和智能化等优点成为当今通信技术的主导, 光码分多址 (OCDMA) 通信技术正是国内外在光纤通信方面研究的一个热点. 然而在宽带业务需求不断增加的今天, 很多宽带业务, 如医学图像、数字视频广播和超计算机可视图图像的传输, 都要求 OCDMA 系统能够实现高吞吐量图像的传输. 因此, Kitayama 在 1994 年提出了一种采用空间扩频技术实现的码分多址并行图像传输系统, 用来支持二维图像的传输. 作为码分多址并行图像传输系统的首选光地址码, 光正交签名码受到信息论领域和组合设计领域等众多学者的关注. 关于光正交签名码的更多信息, 参见文献 [1–3].

设 m, n, k 和 λ 为正整数. 参数为 (m, n, k, λ) 的光正交签名码 (简记为 (m, n, k, λ) -OOSPC) $\mathcal{C}$ 是一族 Hamming 重量为 k 的 $m \times n$ $(0, 1)$ - 矩阵 (称为码字), 并满足:

(1) 自相关性: 对任意 $A = (a_{ij}) \in \mathcal{C}$ 和任意整数 s, t , $(s \pmod{m}, t \pmod{n}) \neq (0, 0)$, 有

$$\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} a_{i,j} a_{i \oplus s, j \oplus t} \leq \lambda;$$

英文引用格式: Pan R, Chang Y X. Further results on optimal $(m, n, 4, 1)$ optical orthogonal signature pattern codes (in Chinese). Sci Sin Math, 2014, 44: 1141–1152, doi: 10.1360/012014-49

(2) 互相关性: 对任意 $A = (a_{ij}) \in \mathcal{C}$, $B = (b_{ij}) \in \mathcal{C}$, $A \neq B$, 以及任意整数 s 和 t , 有

$$\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} a_{i,j} b_{i \oplus s, j \hat{\oplus} t} \leq \lambda,$$

其中 $\oplus$ 和 $\hat{\oplus}$ 分别为模 m 和 n 的加法运算.

设 Z_l 为模 l 剩余类加群. (m, n, k, λ) -OOSPC 中任意码字 $A = (a_{ij})$ 均可等价表示为 $Z_m \times Z_n$ 的一个 k 元子集 X , 其中 $a_{ij} = 1$ 当且仅当 $(i, j) \in X$. 下面用集合的语言给出光正交签名码的另一等价定义.

设 $X + (i, j) = \{(x \oplus i, y \hat{\oplus} j) : (x, y) \in X\}$. (m, n, k, λ) -OOSPC $\mathcal{C}$ 是一个由 $Z_m \times Z_n$ 的 k 元子集构成的集合, 且满足:

(1) 自相关性: 对任意 $X \in \mathcal{C}$ 和任意 $(s, t) \in Z_m \times Z_n \setminus \{(0, 0)\}$, 均有 $|X \cap (X + (s, t))| \leq \lambda$;

(2) 互相关性: 对任意 $X \in \mathcal{C}$, $Y \in \mathcal{C}$, $X \neq Y$ 和任意 $(s, t) \in Z_m \times Z_n$, 均有 $|X \cap (Y + (s, t))| \leq \lambda$.

一个光正交签名码所含码字的个数称为该光正交签名码的码字容量. 所有 (m, n, k, λ) -OOSPC 中码字容量的最大值记为 $\Theta(m, n, k, \lambda)$, 而码字容量为 $\Theta(m, n, k, \lambda)$ 的 (m, n, k, λ) -OOSPC 称为最优的 (或最大的). 由常重码 Johnson 界^[4]可知, $\Theta(m, n, k, \lambda)$ 上界为

$$\left\lfloor \frac{1}{k} \left\lfloor \frac{mn-1}{k-1} \left\lfloor \frac{mn-2}{k-2} \left[\cdots \left\lfloor \frac{mn-\lambda}{k-\lambda} \right\rfloor \cdots \right] \right\rfloor \right\rfloor \right\rfloor =: J(mn, k, \lambda),$$

其中 $\lfloor x \rfloor$ 表示不超过 x 的最大整数.

在实际应用中, 一个 (m, n, k, λ) -OOSPC 的码字容量将决定光码分多址并行图像传输系统能同时承载的最大用户量, 因此, 确定 $\Theta(m, n, k, \lambda)$ 的精确值并构造最优的 (m, n, k, λ) -OOSPC 有着重要的实际应用意义. 注意到, 当 $\gcd(m, n) = 1$ 时, (m, n, k, λ) -OOSPC 等价于 (mn, k, λ) 光正交码 (简记为 (mn, k, λ) -OOC), 其中有关光正交码的详细介绍见文献 [5, 6]. 此时, 最优 OOSPC 的构造可参见文献 [7-14] 中最优光正交码 (OOC) 的构造. 而当 $\gcd(m, n) \neq 1$ 时, 已知的最优 (m, n, k, λ) -OOSPC 仅有如下几类:

(1) $\lambda = 1$, $k = 3$, m 和 n 为奇数且不同时模 6 余 5^[15];

(2) $\lambda = 1$, $k = 3$, $m = 3$, n 为任意正整数^[15];

(3) $\lambda = 1$, $k = 4$, $\gcd(m, 18) = 3$, $n \equiv 0 \pmod{12}$ ^[16];

(4) $\lambda = 2$, $k = 4$, $m = 2^\varepsilon x$, $n = y$, 其中 $\varepsilon \in \{1, 2\}$, x 和 y 的所有因子分别为模 120 余 53 或 77 且小于 500000 的素数, 或属于 $S = \{5, 13, 17, 25, 29, 37, 41, 53, 61, 85, 89, 97, 101, 113, 137, 149, 157, 169, 173, 193, 197, 229, 233, 289, 293, 317\}$ ^[17].

本文将针对 $mn \equiv 0 \pmod{8}$ 的情形讨论码字容量为 $J(mn, 4, 1)$ 的最优 $(m, n, 4, 1)$ -OOSPC 的构造问题.

2 等价关系

光正交签名码与组合设计中一类特殊的填充设计有着密切的关系. 为更好地理解光正交签名码的组合结构, 首先给出填充设计的定义.

设 v 和 k 为正整数. 设 V 为一个 v 元集, $\mathcal{B}$ 为 V 的一些 k 元子集 (称为区组) 组成的集合. 若 V 中任意两个不同的元素都至多包含在一个 $\mathcal{B}$ 的区组中, 则称 $(V, \mathcal{B})$ 为一个 $(v, k, 1)$ 填充设计.

一个定义在 V 上的置换群若能保持 $\mathcal{B}$ 不变, 则称该置换群为填充设计 $(V, \mathcal{B})$ 的一个自同构群. 给定填充设计 $(V, \mathcal{B})$ 的一个自同构群 G , 若对任意 $x, y \in V$, 恰存在一个 $\sigma \in G$ 使得 $x^\sigma = y$, 则称该填充设计是 G -不变的. 对任意 $B \in \mathcal{B}$, 称集合 $\text{Orb}_G(B) = \{B^\sigma : \sigma \in G\}$ 为 B 的 G -轨道. 若一个填充设计 $(V, \mathcal{B})$ 是 G -不变的, 并且对任意 $B \in \mathcal{B}$ 有 $|\text{Orb}_G(B)| = |G|$, 则称其为严格 G -不变的.

给定一个严格 $Z_m \times Z_n$ -不变的 $(mn, k, 1)$ 填充设计 (简记为 $(m \times n, k, 1)$ -SP) $(V, \mathcal{B})$. 对任意 $B \in \mathcal{B}$, 易知 $\text{Orb}_G(B) = \{B + (i, j) : (i, j) \in Z_m \times Z_n\}$. 在 $\mathcal{B}$ 的每个区组轨道中各取一个代表区组 (基区组), 易知该填充设计的所有基区组的集合对应一个 $(m, n, k, 1)$ -OOSPC. 令 $\hat{A}(mn, k)$ 表示所有 $(m \times n, k, 1)$ -SP 中基区组个数的最大值, 则含 $\hat{A}(mn, k)$ 个基区组的 $(m \times n, k, 1)$ -SP 称为最优的 (或最大的). 因此有如下的等价关系.

引理 2.1 ^[17] 一个最优的 $(m, n, k, 1)$ -OOSPC 等价于一个最优的严格 $Z_m \times Z_n$ -不变 $(mn, k, 1)$ 填充设计 (即最优 $(m \times n, k, 1)$ -SP).

基于上述等价关系, 本文将通过构造最优 $(m \times n, k, 1)$ -SP 的方式来获得所需的最优 $(m, n, k, 1)$ -OOSPC. 下面给出 $s \times t$ -正则 $(m \times n, k, 1)$ -SP 的定义.

设 $\mathcal{B}$ 为一个 $(m \times n, k, 1)$ -SP 的所有基区组组成的集合. 不失一般性, 总可以假设 $\mathcal{B}$ 中的每一个基区组都包含元素 $(0, 0)$, 即任意 $B \in \mathcal{B}$ 都可写为 $B = \{(x_0, y_0) = (0, 0), (x_1, y_1), \dots, (x_{k-1}, y_{k-1})\}$ 的形式. 设 $\Delta B = \{(x_i, y_i) - (x_j, y_j) : 0 \leq i, j \leq k-1, i \neq j\}$, $\Delta \mathcal{B} = \bigcup_{B \in \mathcal{B}} \Delta B$, 易知 $\Delta \mathcal{B}$ 包含 $Z_m \times Z_n$ 中每一个非零元至多一次. 设 $\text{DL}(\mathcal{B}) = \{(i, j) \in Z_m \times Z_n : (0, 0) \neq (i, j) \notin \Delta \mathcal{B}\}$, 若 $\text{DL}(\mathcal{B}) \cup \{(0, 0)\} = S \times T$ 是 $Z_m \times Z_n$ 的一个加法子群, 其中 S 为 Z_m 的一个 s 阶加法子群, T 为 Z_n 的一个 t 阶加法子群, 则称该 $(m \times n, k, 1)$ -SP 是 $s \times t$ -正则的, 简记为 $(m \times n, s \times t, k, 1)$ -SP. 值得一提的是, 一个 $(m \times n, s \times t, k, 1)$ -SP 也是一个 $(Z_m \times Z_n, S \times T, k, 1)$ -差族 (简记为 $(Z_m \times Z_n, S \times T, k, 1)$ -DF), 其中此差族的详细定义可参见文献 [18]. 此外, 设正整数 $g = g_1 g_2$, $u = u_1 u_2$, $\gcd(g_1 u_1, g_2 u_2) = 1$, 则 $(g_1 u_1 \times g_2 u_2, g_1 \times g_2, k, 1)$ -SP 等价于文献 [6] 中定义的 g -正则 $(gu, k, 1)$ -OOC.

例 2.2 含下列基区组的 $(2 \times 48, 4, 1)$ -SP 是 2×6 -正则的,

$\{(0, 0), (0, 1), (0, 10), (1, 4)\}, \{(0, 0), (0, 2), (0, 14), (1, 21)\}, \{(0, 0), (0, 3), (0, 33), (1, 2)\},$
 $\{(0, 0), (0, 4), (0, 23), (1, 38)\}, \{(0, 0), (0, 5), (0, 27), (1, 18)\}, \{(0, 0), (0, 6), (0, 37), (1, 26)\},$
 $\{(0, 0), (0, 7), (0, 20), (1, 43)\}.$

由 $(m \times n, s \times t, k, 1)$ -SP 的定义知其含 $\frac{mn-st}{k(k-1)}$ 个基区组, 因此有如下结论.

引理 2.3 若 $1 \leq st \leq k(k-1)$, 则 $(m \times n, s \times t, k, 1)$ -SP 是最优的.

引理 2.4 若含 b_1 个基区组的 $(m \times n, s \times t, k, 1)$ -SP 和含 b_2 个基区组的 $(s \times t, k, 1)$ -SP 都存在, 则含 $b_1 + b_2$ 个基区组的 $(m \times n, k, 1)$ -SP 存在. 特别地, 若存在的 $(s \times t, k, 1)$ -SP 是 $g \times h$ -正则的, 则得到的 $(m \times n, k, 1)$ -SP 也是 $g \times h$ -正则的.

3 递归构造

设 $(G, \cdot)$ 是一个 v 阶群. G 上的一个 $k \times \lambda v$ 矩阵 $D = (d_{ij})$ 若满足对任意不同的两行 x 和 y , 多元集 $\{d_{xi} \cdot d_{yi}^{-1} : 1 \leq i \leq \lambda v\}$ 包含 G 中每个元素恰好 λ 次, 则称 D 为 (G, k, λ) 差阵 (简记为 (G, k, λ) -DM). 若 G 为交换群, G 上运算 “ $\cdot$ ” 可视为加法, 相应地, $d_{xi} \cdot d_{yi}^{-1}$ 可视为 $d_{xi} - d_{yi}$. 若 $G = Z_v$, 则称差阵 D 是循环的, 简记为 (v, k, λ) -CDM.

差阵作为组合设计理论中一个重要的辅助设计, 在很多组合构形 (如正交拉丁方和 Steiner 三元系等) 的构造中起着重要的作用, 也因此受到组合设计领域学者的广泛关注. 下面仅列出差阵的一些

已有结果, 而更多的结果可参见文献 [19].

引理 3.1^[19] 设 v 和 k 为正整数, $\gcd(v, (k-1)!) = 1$, 则存在 $(v, k, 1)$ -CDM.

引理 3.2^[18, 定理 2.13] 设 G 为有限群, k 为 $|G|$ 的最小素因子, 则存在 $(G, k, 1)$ -DM.

引理 3.3^[18, 推论 2.6] 设 G 为一个有限群, H 为 G 的一个正规子群. 若 $(G/H, k, \lambda)$ -DM 和 (H, k, μ) -DM 都存在, 则 $(G, k, \lambda\mu)$ -DM 存在.

引理 3.4 设 $d \geq 1$ 为正整数, 则存在 $(Z_2 \times Z_{2^d}, 4, 1)$ -DM.

证明 当 $d = 1$ 时, $(Z_2 \times Z_2, 4, 1)$ -DM 同构于有限域 $\text{GF}(4)$ 的乘法表. 当 $d \geq 2$ 时, 按如下方法可构造所需的 $(Z_2 \times Z_{2^d}, 4, 1)$ -DM. 为方便起见, 用 i_j 表示 $Z_2 \times Z_{2^d}$ 中的元素 (i, j) . 设 $I_1 = \{0, 1, \dots, 2^{d-2} - 1\}$, $I_2 = \{2^{d-2}, 2^{d-2} + 1, \dots, 2^{d-1} - 1\}$. 对任意 $r \in \{0, 1, 2, 3\}$, 构造 $4 \times 2^{d-1}$ 矩阵 $D_r = [c_0^{(r)} c_1^{(r)} \cdots c_{2^{d-1}-1}^{(r)}]$, 其中

$$\begin{aligned} c_i^{(0)} &= \begin{cases} (0_0, 0_{2i}, 0_{4i}, 0_{-2i})^\top, & \text{若 } i \in I_1, \\ (0_0, 0_{2i}, 1_{4i}, 1_{-2i})^\top, & \text{若 } i \in I_2, \end{cases} \\ c_i^{(1)} &= \begin{cases} (0_0, 1_{2i}, 0_{4i+1}, 1_{-2i-1})^\top, & \text{若 } i \in I_1, \\ (0_0, 1_{2i}, 1_{4i+1}, 0_{-2i-1})^\top, & \text{若 } i \in I_2, \end{cases} \\ c_i^{(2)} &= \begin{cases} (0_0, 0_{2i+1}, 0_{4i+2}, 0_{-2i-1})^\top, & \text{若 } i \in I_1, \\ (0_0, 0_{2i+1}, 1_{4i+2}, 1_{-2i-1})^\top, & \text{若 } i \in I_2, \end{cases} \\ c_i^{(3)} &= \begin{cases} (0_0, 1_{2i+1}, 0_{4i+3}, 1_{-2i-2})^\top, & \text{若 } i \in (I_1 \setminus \{2^{d-2} - 1\}) \cup \{2^{d-1} - 1\}, \\ (0_0, 1_{2i+1}, 1_{4i+3}, 0_{-2i-2})^\top, & \text{若 } i \in (I_2 \setminus \{2^{d-1} - 1\}) \cup \{2^{d-2} - 1\}. \end{cases} \end{aligned}$$

令

$$D = [D_0 \mid D_1 \mid D_2 \mid D_3] = \begin{bmatrix} R_1 \\ R_2 \\ R_3 \\ R_4 \end{bmatrix},$$

下面验证 D 是一个 $(Z_2 \times Z_{2^d}, 4, 1)$ -DM. 显然, R_2, R_3 和 R_4 均包含 $Z_2 \times Z_{2^d}$ 中每个元素恰好一次, 且 $R_2 - R_3 = R_4, R_2 - R_4 = R_3$. 因此, 只需验证 $R_3 - R_4$ 包含 $Z_2 \times Z_{2^d}$ 中每个元素也恰好一次. 首先在 D_0 中, 第 3 与第 4 行对应元素之差的集合为 $\{0_{6i} \mid i \in I_1 \cup I_2\}$. 对任意 $i, j \in I_1 \cup I_2$, 由中国剩余定理可知, $6i \equiv 6j \pmod{2^d}$ 当且仅当 $i = j$, 故有

$$\{0_{6i} \mid i \in I_1 \cup I_2\} = \{0_i \mid i \equiv 0 \pmod{2}\}.$$

类似地可以验证在 D_1, D_2 和 D_3 中, 第 3 与第 4 行对应元素之差的集合分别为 $\{1_i \mid i \equiv 0 \pmod{2}\}, \{0_i \mid i \equiv 1 \pmod{2}\}$ 和 $\{1_i \mid i \equiv 1 \pmod{2}\}$. 故结论得证. $\square$

为理解引理 3.4 中的构造, 给出下述例子.

例 3.5 令 D_0, D_1, D_2 和 D_3 分别为如下四个矩阵:

$$\begin{bmatrix} 0_0 & 0_0 & 0_0 & 0_0 \\ 0_0 & 0_2 & 0_4 & 0_6 \\ 0_0 & 0_4 & 1_0 & 1_4 \\ 0_0 & 0_6 & 1_4 & 1_2 \end{bmatrix}, \begin{bmatrix} 0_0 & 0_0 & 0_0 & 0_0 \\ 1_0 & 1_2 & 1_4 & 1_6 \\ 0_1 & 0_5 & 1_1 & 1_5 \\ 1_7 & 1_5 & 0_3 & 0_1 \end{bmatrix}, \begin{bmatrix} 0_0 & 0_0 & 0_0 & 0_0 \\ 0_1 & 0_3 & 0_5 & 0_7 \\ 0_2 & 0_6 & 1_2 & 1_6 \\ 0_7 & 0_5 & 1_3 & 1_1 \end{bmatrix}, \begin{bmatrix} 0_0 & 0_0 & 0_0 & 0_0 \\ 1_1 & 1_3 & 1_5 & 1_7 \\ 0_3 & 1_7 & 1_3 & 0_7 \\ 1_6 & 0_4 & 0_2 & 1_0 \end{bmatrix},$$

则 $D = [D_0 \mid D_1 \mid D_2 \mid D_3]$ 是一个 $(Z_2 \times Z_8, 4, 1)$ -DM.

结合引理 3.3 和 3.4 可得下述结论.

引理 3.6 设 $a, b \geq 1$ 为正整数, 则存在 $(Z_{2^a} \times Z_{2^b}, 4, 1)$ -DM.

证明 当 $a = 1$ 或 $b = 1$ 时, 由引理 3.4 即得结论. 当 $a, b \geq 2$ 时, 设 $G = Z_{2^a} \times Z_{2^b}$, $H = 2Z_{2^a} \times 2^{b-1}Z_{2^b}$, 则有 $G/H \cong Z_2 \times Z_{2^{b-1}}$, $H \cong Z_{2^{a-1}} \times Z_2$. 因此, 结合引理 3.3 和 3.4 即得结论. $\square$

构造 3.7^[18, 推论 5.8] 设 G 为一个有限群, H 为 G 的一个正规子群, N 为 G 的一个子群, $H \subset N \subset G$. 若 $(G/H, N/H, k, \lambda)$ -DF 和 (H, k, μ) -DM 都存在, 则 $(G, N, k, \lambda\mu)$ -DF 存在.

构造 3.8 设 m, n, u 和 v 为正整数. 若 $(m \times n, s \times t, k, 1)$ -SP 和 $(Z_u \times Z_v, k, 1)$ -DM 都存在, 则 $(mu \times nv, su \times tv, k, 1)$ -SP 存在.

证明 设 $G = Z_{mu} \times Z_{nv}$, $N = (\frac{m}{s}Z_{mu}) \times (\frac{n}{t}Z_{nv})$, $H = (mZ_{mu}) \times (nZ_{nv})$, 易知 $G/H \cong Z_m \times Z_n$, $N/H \cong (\frac{m}{s}Z_m) \times (\frac{n}{t}Z_n)$. 由题设可知, $(m \times n, s \times t, k, 1)$ -SP 和 $(Z_u \times Z_v, k, 1)$ -DM 都存在, 即存在 $(G/H, N/H, k, 1)$ -DF 和 $(H, k, 1)$ -DM. 故由构造 3.7 知存在 $(mu \times nv, su \times tv, k, 1)$ -SP (即 $(G, N, k, 1)$ -DF).

为简化下文的证明, 给出构造 3.8 的下述推论.

构造 3.9^[16] 设 m, n 和 v 为正整数. 若 $(m \times n, s \times t, k, 1)$ -SP 和 $(v, k, 1)$ -CDM 都存在, 则 $(m \times nv, s \times tv, k, 1)$ -SP (或 $(mv \times n, sv \times t, k, 1)$ -SP) 存在.

推论 3.10 设 a, b, m 和 n 为正整数. 若 $(m \times n, s \times t, 4, 1)$ -SP 存在, 则 $(2^a m \times 2^b n, 2^a s \times 2^b t, 4, 1)$ -SP 存在.

证明 结合构造 3.8 和引理 3.6 即得结论. $\square$

推论 3.11 设 m 和 n 为正整数. 若 $(m \times n, s \times t, 4, 1)$ -SP 存在, 则 $(2m \times 6n, 2s \times 6t, 4, 1)$ -SP 存在.

证明 由文献 [20, 定理 3.44] 知, $(Z_2 \times Z_6, 4, 1)$ -DM 存在, 因此, 利用构造 3.8 即得结论. $\square$

4 $mn \equiv 8, 16 \pmod{24}$ 情形下的最优 $(m \times n, 4, 1)$ -SP

本节将考虑 $mn \equiv 8, 16 \pmod{24}$ 情形下最优 $(m \times n, 4, 1)$ -SP 的构造. 首先列出 OOC 的一些已有结果, 并给出一些小参数的 $(m \times n, 4, 1)$ -SP. 为方便起见, 令 $\mathcal{P}_n$ 为每个素因子均模 n 余 1 的正整数组成的集合.

引理 4.1^[10, 引理 4.4] 设整数 $n \geq 7$, 则存在 g -正则 $(2^n, 4, 1)$ -OOC, 其中 $g = 8$, 或 16, 或 32, 或 64.

引理 4.2^[10, 定理 5.1] 设 $u \in \mathcal{P}_6$, 则存在码字容量为 $\frac{u-1}{6}$ 的最优 $(2u, 4, 1)$ -OOC.

引理 4.3 设 $(m, n, s, t) \in \{(2, 32, 2, 2), (2, 64, 2, 4), (2, 128, 2, 2), (4, 4, 2, 2), (4, 8, 2, 4), (4, 16, 2, 2), (4, 32, 2, 4)\}$, 则存在 $(m \times n, s \times t, 4, 1)$ -SP.

证明 利用计算机搜索, 所需 $(m \times n, s \times t, 4, 1)$ -SP 含下列基区组:

$(m, n, s, t) = (2, 32, 2, 2) :$

$\{(0, 0), (0, 1), (0, 14), (1, 11)\}, \{(0, 0), (0, 2), (1, 8), (1, 15)\}, \{(0, 0), (0, 3), (1, 4), (1, 12)\},$
 $\{(0, 0), (0, 4), (0, 10), (0, 15)\}, \{(0, 0), (0, 9), (1, 2), (1, 14)\};$

$(m, n, s, t) = (2, 64, 2, 4) :$

$\{(0, 0), (0, 1), (1, 13), (1, 44)\}, \{(0, 0), (0, 2), (1, 9), (1, 47)\}, \{(0, 0), (0, 3), (0, 11), (1, 14)\},$
 $\{(0, 0), (0, 5), (0, 46), (1, 41)\}, \{(0, 0), (0, 6), (0, 15), (1, 39)\}, \{(0, 0), (0, 7), (1, 15), (1, 34)\},$
 $\{(0, 0), (0, 10), (0, 35), (0, 47)\}, \{(0, 0), (0, 13), (0, 34), (1, 35)\}, \{(0, 0), (0, 14), (0, 36), (1, 10)\},$
 $\{(0, 0), (1, 2), (1, 6), (1, 46)\};$

$(m, n, s, t) = (2, 128, 2, 2) :$

$\{(0, 0), (0, 1), (0, 30), (1, 27)\}, \{(0, 0), (0, 2), (0, 40), (1, 60)\}, \{(0, 0), (0, 3), (0, 37), (1, 15)\},$
 $\{(0, 0), (0, 4), (0, 26), (1, 10)\}, \{(0, 0), (0, 5), (0, 28), (1, 126)\}, \{(0, 0), (0, 6), (0, 51), (1, 56)\},$
 $\{(0, 0), (0, 7), (0, 31), (1, 35)\}, \{(0, 0), (0, 8), (0, 35), (1, 82)\}, \{(0, 0), (0, 9), (0, 96), (1, 8)\},$
 $\{(0, 0), (0, 10), (0, 95), (1, 119)\}, \{(0, 0), (0, 11), (0, 86), (1, 63)\}, \{(0, 0), (0, 12), (0, 61), (1, 103)\},$
 $\{(0, 0), (0, 13), (0, 84), (1, 66)\}, \{(0, 0), (0, 14), (0, 69), (1, 83)\}, \{(0, 0), (0, 15), (0, 63), (1, 107)\},$
 $\{(0, 0), (0, 16), (0, 76), (1, 89)\}, \{(0, 0), (0, 17), (0, 56), (1, 94)\}, \{(0, 0), (0, 18), (0, 54), (1, 97)\},$
 $\{(0, 0), (0, 19), (0, 81), (1, 48)\}, \{(0, 0), (0, 20), (0, 78), (1, 61)\}, \{(0, 0), (0, 21), (0, 46), (1, 117)\};$

$(m, n, s, t) = (4, 4, 2, 2) :$

$\{(0, 0), (0, 1), (1, 0), (3, 3)\};$

$(m, n, s, t) = (4, 8, 2, 4) :$

$\{(0, 0), (0, 1), (1, 0), (1, 3)\}, \{(0, 0), (1, 1), (2, 5), (3, 2)\};$

$(m, n, s, t) = (4, 16, 2, 2) :$

$\{(0, 0), (0, 1), (1, 5), (3, 9)\}, \{(0, 0), (0, 2), (0, 6), (0, 13)\}, \{(0, 0), (1, 0), (2, 10), (3, 3)\},$
 $\{(0, 0), (1, 2), (2, 5), (3, 4)\}, \{(0, 0), (1, 6), (2, 1), (3, 15)\};$

$(m, n, s, t) = (4, 32, 2, 4) :$

$\{(0, 0), (0, 1), (2, 4), (2, 13)\}, \{(0, 0), (0, 2), (1, 9), (1, 27)\}, \{(0, 0), (0, 3), (0, 7), (3, 17)\},$
 $\{(0, 0), (0, 5), (1, 26), (2, 26)\}, \{(0, 0), (0, 6), (1, 16), (2, 15)\}, \{(0, 0), (0, 10), (1, 1), (1, 12)\},$
 $\{(0, 0), (0, 12), (1, 4), (1, 17)\}, \{(0, 0), (0, 15), (1, 3), (2, 1)\}, \{(0, 0), (1, 6), (2, 2), (3, 13)\},$
 $\{(0, 0), (1, 8), (2, 5), (3, 18)\}.$

□

引理 4.4 设整数 $\beta \geq 2$, $\beta \neq 3$, 则存在 $(2 \times 2^\beta, 2 \times g, 4, 1)$ -SP, 其中 $g = 2$, 或 4, 或 16.

证明 当 $\beta \in \{2, 4\}$ 时, 结论显然成立. 当 $\beta = 5, 6, 7$ 时, 由引理 4.3 即得结论. 当 $\beta \geq 8$ 时, 由引理 4.1 知, $(1 \times 2^{\beta-1}, 1 \times g', 4, 1)$ -SP 存在, 其中 $g' = 8$, 或 16, 或 32, 或 64. 在推论 3.10 中令 $(a, b) = (1, 1)$ 有 $(2 \times 2^\beta, 2 \times 2g', 4, 1)$ -SP. 最后, 结合引理 2.4 和 $\beta = 4, 5, 6, 7$ 时的结论, 则有 $(2 \times 2^\beta, 2 \times g, 4, 1)$ -SP, 其中 $g = 2$, 或 4, 或 16. □

引理 4.5 设整数 $\beta \geq 2$, 则存在 $(4 \times 2^\beta, 2 \times g, 4, 1)$ -SP, 其中 $g = 2$ 或 4.

证明 当 $\beta \in \{2, 3, 4, 5\}$ 时, 由引理 4.3 即得结论. 当 $\beta \geq 6$ 时, 由引理 4.4 知, $(2 \times 2^{\beta-1}, 2 \times g', 4, 1)$ -SP 存在, 其中 $g' = 2$, 或 4, 或 16. 在推论 3.10 中令 $(a, b) = (1, 1)$ 有 $(4 \times 2^\beta, 4 \times 2g', 4, 1)$ -SP. 最后, 结合引理 2.4 和 $\beta = 2, 3, 5$ 时的结论, 则有 $(4 \times 2^\beta, 2 \times g, 4, 1)$ -SP, 其中 $g = 2$ 或 4. □

引理 4.6 设整数 $i \in \{3, 4, 5\}$, $\beta \geq i$, 则存在 $(2^i \times 2^\beta, 2 \times g, 4, 1)$ -SP, 其中 $g = 2$ 或 4.

证明 当 $i = 3$ 时, 由引理 4.5 知, $(4 \times 2^{\beta-1}, 2 \times g', 4, 1)$ -SP 存在, 其中 $g' = 2$ 或 4. 在推论 3.10 中令 $(a, b) = (1, 1)$ 有 $(8 \times 2^{\beta}, 4 \times 2g', 4, 1)$ -SP. 最后, 结合引理 2.4 和 4.3, 则有 $(8 \times 2^{\beta}, 2 \times g, 4, 1)$ -SP, 其中 $g = 2$ 或 4. 当 $i = 4, 5$ 时, 可类似地证明. $\square$

引理 4.7 设整数 $\beta \geq \alpha \geq 1$, $(\alpha, \beta) \neq (1, 1), (1, 3)$, 则存在 $(2^{\alpha} \times 2^{\beta}, 2 \times g, 4, 1)$ -SP, 其中 $g = 2$, 或 4, 或 16.

证明 当 $\alpha \in \{1, 2, 3, 4, 5\}$, $\beta \geq \alpha$, $(\alpha, \beta) \neq (1, 1), (1, 3)$ 时, 由引理 4.4–4.6 即得结论. 当 $\beta \geq \alpha \geq 6$ 时, 由引理 4.4 知, $(2^{\alpha-1} \times 2, g \times 2, 4, 1)$ -SP 存在, 其中 $g = 2$, 或 4, 或 16, 故在推论 3.10 中令 $(a, b) = (1, \beta-1)$ 有 $(2^{\alpha} \times 2^{\beta}, 2g \times 2^{\beta}, 4, 1)$ -SP. 最后, 结合引理 2.4、4.5 和 4.6, 则有 $(2^{\alpha} \times 2^{\beta}, 2 \times g, 4, 1)$ -SP. $\square$

引理 4.8 设整数 $\beta \geq \alpha \geq 1$, $(\alpha, \beta) \neq (1, 1), (1, 3)$, $u, v \in \mathcal{P}_6$, 则存在 $(2^{\alpha}u \times 2^{\beta}v, 2 \times g, 4, 1)$ -SP, 其中 $g = 2$, 或 4, 或 16.

证明 首先证明存在 $(u \times 2v, 1 \times 2, 4, 1)$ -SP. 由引理 4.2 知, $(1 \times 2v, 1 \times 2, 4, 1)$ -SP 和 $(u \times 2, 1 \times 2, 4, 1)$ -SP 均存在, 而由引理 3.1 知, $(u, 4, 1)$ -CDM 存在. 因此, 利用构造 3.9 和引理 2.4, 则有 $(u \times 2v, 1 \times 2, 4, 1)$ -SP. 接着, 在推论 3.10 中令 $(a, b) = (\alpha, \beta-1)$ 有 $(2^{\alpha}u \times 2^{\beta}v, 2^{\alpha} \times 2^{\beta}, 4, 1)$ -SP. 最后, 结合引理 2.4 和 4.7, 则有 $(2^{\alpha}u \times 2^{\beta}v, 2 \times g, 4, 1)$ -SP, 其中 $g = 2$, 或 4, 或 16. $\square$

定理 4.9 设 m 和 n 为偶数, $mn \equiv 8, 16 \pmod{24}$, 且 $mn \equiv 16 \pmod{32}$ 和 $\gcd(m, n, 4) = 2$ 不同时成立, 其中 m 和 n 的所有奇素因子均模 6 余 1, 则存在含 $J(mn, 4, 1)$ 个基区组的最优 $(m \times n, 4, 1)$ -SP.

证明 不失一般性, 设 $m = 2^{\alpha}u$, $n = 2^{\beta}v$, 其中 $\beta \geq \alpha \geq 1$, $(\alpha, \beta) \neq (1, 1), (1, 3)$, $u, v \in \mathcal{P}_6$. 由引理 4.8 知, $(m \times n, 2 \times g, 4, 1)$ -SP 存在, 其中 $g = 2$, 或 4, 或 16. 又因为对任意 $g \in \{2, 4\}$ 存在平凡的最优 $(2 \times g, 4, 1)$ -SP (不含基区组), 以及存在含两个基区组 $\{(0, 0), (0, 1), (0, 3), (1, 4)\}$ 和 $\{(0, 0), (0, 4), (0, 9), (1, 11)\}$ 的最优 $(2 \times 16, 4, 1)$ -SP. 故利用引理 2.4 即得结论: 存在含 $J(mn, 4, 1)$ 个基区组的最优 $(m \times n, 4, 1)$ -SP. $\square$

5 $mn \equiv 0 \pmod{24}$ 情形下的最优 $(m \times n, 4, 1)$ -SP

本节将针对 $mn \equiv 0 \pmod{24}$ 且 $\gcd(m, n, 6) = 2$ 的情形, 构造一族最优 $(m \times n, 4, 1)$ -SP.

引理 5.1 设整数 $n \geq 3$, 则存在 g -正则 $(3 \cdot 2^n, 4, 1)$ -OOC, 其中 $g = 12$, 或 24, 或 48.

证明 结合引理 2.4 和文献 [8, 引理 4.5 和 6.4] 即得结论. $\square$

引理 5.2 设整数 $n \geq 2$, 则存在 6-正则 $(6 \cdot 3^n, 4, 1)$ -OOC.

证明 由文献 [13, 定理 4.3] 的证明即得结论. $\square$

引理 5.3 设正整数 g, u 和 v 满足 $g = 24$ 且 $\gcd(u, 6) = \gcd(v, 6) = 1$, 或 $g = 6$, $\gcd(u, 150) = 1, 25$, 且 $\gcd(v, 150) = 1, 25$, 则存在 $(u \times gv, 1 \times g, 4, 1)$ -SP.

证明 对给定的参数 g, u 和 v , 由文献 [13, 引理 2.6 和 5.1] 知, $(u \times g, 1 \times g, 4, 1)$ -SP 和 $(1 \times gv, 1 \times g, 4, 1)$ -SP 均存在, 且由引理 3.1 知, $(u, 4, 1)$ -CDM 也存在. 故利用构造 3.9 和引理 2.4 即得结论. $\square$

引理 5.4 设整数 $(m, n, s, t) \in \{(2, 36, 2, 6), (2, 60, 2, 12), (2, 72, 2, 12), (2, 96, 2, 12), (2, 120, 2, 12), (4, 12, 2, 6), (4, 24, 2, 12), (4, 36, 2, 12), (4, 48, 2, 12)\}$, 则存在 $(m \times n, s \times t, 4, 1)$ -SP.

证明 利用计算机搜索, 所需 $(m \times n, s \times t, 4, 1)$ -SP 含下列基区组:

$(m, n, s, t) = (2, 36, 2, 6)$:

$\{(0, 0), (0, 1), (1, 8), (1, 17)\}, \{(0, 0), (0, 2), (0, 16), (1, 11)\}, \{(0, 0), (0, 4), (1, 1), (1, 14)\},$

$\{(0, 0), (0, 5), (0, 8), (0, 15)\}, \{(0, 0), (0, 17), (1, 2), (1, 13)\};$

$(m, n, s, t) = (2, 60, 2, 12)$:

$\{(0, 0), (0, 1), (0, 12), (1, 4)\}, \{(0, 0), (0, 2), (0, 28), (1, 29)\}, \{(0, 0), (0, 3), (0, 22), (1, 9)\},$
 $\{(0, 0), (0, 4), (0, 17), (1, 41)\}, \{(0, 0), (0, 6), (0, 29), (1, 17)\}, \{(0, 0), (0, 7), (0, 21), (1, 39)\},$
 $\{(0, 0), (0, 8), (0, 24), (1, 22)\}, \{(0, 0), (0, 9), (0, 27), (1, 53)\};$

$(m, n, s, t) = (2, 72, 2, 12) :$

$\{(0, 0), (0, 1), (0, 53), (1, 52)\}, \{(0, 0), (0, 2), (0, 15), (1, 49)\}, \{(0, 0), (0, 3), (0, 7), (1, 46)\},$
 $\{(0, 0), (0, 8), (0, 39), (1, 17)\}, \{(0, 0), (0, 9), (0, 14), (0, 37)\}, \{(0, 0), (0, 10), (1, 3), (1, 14)\},$
 $\{(0, 0), (0, 16), (0, 38), (1, 11)\}, \{(0, 0), (0, 17), (0, 43), (1, 15)\}, \{(0, 0), (0, 40), (1, 8), (1, 53)\},$
 $\{(0, 0), (0, 47), (1, 16), (1, 37)\};$

$(m, n, s, t) = (2, 96, 2, 12) :$

$\{(0, 0), (0, 1), (0, 13), (0, 74)\}, \{(0, 0), (0, 2), (1, 15), (1, 21)\}, \{(0, 0), (0, 3), (0, 47), (1, 42)\},$
 $\{(0, 0), (0, 4), (1, 18), (1, 59)\}, \{(0, 0), (0, 5), (0, 30), (1, 68)\}, \{(0, 0), (0, 7), (0, 21), (1, 67)\},$
 $\{(0, 0), (0, 9), (0, 29), (1, 6)\}, \{(0, 0), (0, 10), (0, 46), (1, 1)\}, \{(0, 0), (0, 11), (0, 39), (1, 22)\},$
 $\{(0, 0), (0, 15), (0, 34), (1, 86)\}, \{(0, 0), (0, 17), (0, 43), (1, 70)\}, \{(0, 0), (0, 18), (0, 51), (1, 20)\},$
 $\{(0, 0), (0, 27), (0, 58), (1, 62)\}, \{(0, 0), (0, 37), (1, 7), (1, 49)\};$

$(m, n, s, t) = (2, 120, 2, 12) :$

$\{(0, 0), (0, 1), (0, 23), (1, 5)\}, \{(0, 0), (0, 2), (0, 29), (1, 8)\}, \{(0, 0), (0, 3), (0, 34), (1, 19)\},$
 $\{(0, 0), (0, 4), (0, 96), (1, 17)\}, \{(0, 0), (0, 5), (0, 26), (1, 58)\}, \{(0, 0), (0, 6), (0, 85), (1, 84)\},$
 $\{(0, 0), (0, 7), (0, 74), (1, 72)\}, \{(0, 0), (0, 8), (0, 65), (1, 117)\}, \{(0, 0), (0, 9), (0, 42), (1, 106)\},$
 $\{(0, 0), (0, 11), (0, 48), (1, 77)\}, \{(0, 0), (0, 12), (0, 51), (1, 73)\}, \{(0, 0), (0, 13), (0, 56), (1, 82)\},$
 $\{(0, 0), (0, 14), (0, 52), (1, 85)\}, \{(0, 0), (0, 15), (0, 62), (1, 96)\}, \{(0, 0), (0, 16), (0, 61), (1, 92)\},$
 $\{(0, 0), (0, 17), (0, 49), (1, 74)\}, \{(0, 0), (0, 18), (0, 54), (1, 45)\}, \{(0, 0), (0, 19), (0, 44), (1, 7)\};$

$(m, n, s, t) = (4, 12, 2, 6) :$

$\{(0, 0), (0, 1), (1, 0), (1, 7)\}, \{(0, 0), (0, 3), (1, 1), (3, 10)\}, \{(0, 0), (1, 3), (2, 7), (3, 4)\};$

$(m, n, s, t) = (4, 24, 2, 12) :$

$\{(0, 0), (0, 1), (1, 0), (1, 3)\}, \{(0, 0), (0, 5), (1, 1), (1, 14)\}, \{(0, 0), (0, 7), (1, 5), (3, 12)\},$
 $\{(0, 0), (0, 9), (1, 6), (3, 17)\}, \{(0, 0), (1, 4), (2, 15), (3, 9)\}, \{(0, 0), (1, 8), (2, 1), (3, 11)\};$

$(m, n, s, t) = (4, 36, 2, 12) :$

$\{(0, 0), (0, 1), (1, 0), (3, 14)\}, \{(0, 0), (0, 2), (2, 10), (3, 28)\}, \{(0, 0), (0, 4), (1, 15), (3, 8)\},$
 $\{(0, 0), (0, 5), (1, 17), (3, 22)\}, \{(0, 0), (0, 7), (0, 20), (1, 4)\}, \{(0, 0), (0, 8), (1, 1), (2, 25)\},$
 $\{(0, 0), (0, 10), (1, 13), (3, 15)\}, \{(0, 0), (0, 11), (1, 2), (1, 16)\}, \{(0, 0), (0, 17), (1, 6), (2, 4)\},$
 $\{(0, 0), (1, 7), (2, 1), (3, 27)\};$

$(m, n, s, t) = (4, 48, 2, 12) :$

$\{(0, 0), (0, 1), (1, 6), (2, 3)\}, \{(0, 0), (0, 2), (0, 9), (3, 1)\}, \{(0, 0), (0, 3), (0, 13), (3, 13)\},$
 $\{(0, 0), (0, 5), (1, 25), (2, 14)\}, \{(0, 0), (0, 6), (0, 23), (3, 31)\}, \{(0, 0), (0, 11), (1, 29), (1, 44)\},$
 $\{(0, 0), (0, 14), (1, 2), (2, 15)\}, \{(0, 0), (0, 18), (1, 34), (3, 24)\}, \{(0, 0), (0, 19), (1, 26), (2, 37)\},$
 $\{(0, 0), (0, 21), (1, 4), (3, 39)\}, \{(0, 0), (0, 22), (1, 15), (2, 43)\}, \{(0, 0), (1, 3), (2, 25), (3, 9)\},$
 $\{(0, 0), (1, 10), (2, 29), (3, 27)\}, \{(0, 0), (1, 12), (2, 7), (3, 34)\}.$ $\square$

引理 5.5 设整数 $(m, n, s, t) \in \{(4, 72, 4, 12), (4, 96, 4, 12), (8, 72, 2, 12)\}$, 则存在 $(m \times n, s \times t, 4, 1)$ -SP.

证明 当 $(m, n, s, t) \in \{(4, 72, 4, 12), (4, 96, 4, 12)\}$ 时, 由引理 5.4 和例 2.2 知, $(\frac{m}{2} \times \frac{n}{2}, 2 \times 6, 4, 1)$ -SP 存在. 故在推论 3.10 中令 $(a, b) = (1, 1)$ 有 $(m \times n, 4 \times 12, 4, 1)$ -SP.

当 $(m, n, s, t) = (8, 72, 2, 12)$ 时, 由引理 5.4 知, $(4 \times 36, 2 \times 12, 4, 1)$ -SP 存在, 故在推论 3.10 中令 $(a, b) = (1, 1)$ 有 $(8 \times 72, 4 \times 24, 4, 1)$ -SP. 再由引理 5.4 知, $(4 \times 24, 2 \times 12, 4, 1)$ -SP 存在, 故利用引理 2.4 有 $(8 \times 72, 2 \times 12, 4, 1)$ -SP. $\square$

引理 5.6 设整数 $(m, n) \in \{(2, 6), (2, 12), (2, 24), (2, 30), (2, 48), (2, 60), (2, 120), (10, 6), (10, 12), (10, 24), (10, 30), (10, 60), (10, 120)\}$, 则存在含 $J(mn, 4, 1)$ 个基区组的最优 $(m \times n, 4, 1)$ -SP.

证明 当 $(m, n) = (2, 6)$ 时, 存在平凡的最优 $(2 \times 6, 4, 1)$ -SP. 当 $(m, n) = (2, 48)$ 时, 结合例 2.2 和引理 2.3 即得结论. 当 $(m, n) \in \{(2, 12), (2, 24), (2, 30), (10, 30)\}$ 时, 利用计算机搜索, 所需的最优 $(m \times n, 4, 1)$ -SP 含下列基区组:

$(m, n) = (2, 12)$:

$\{(0, 0), (0, 1), (0, 3), (1, 4)\}$;

$(m, n) = (2, 24)$:

$\{(0, 0), (0, 1), (0, 3), (0, 7)\}, \{(0, 0), (0, 5), (0, 13), (1, 2)\}, \{(0, 0), (0, 9), (1, 1), (1, 15)\}$;

$(m, n) = (2, 30)$:

$\{(0, 0), (0, 1), (0, 3), (0, 7)\}, \{(0, 0), (0, 5), (0, 13), (1, 1)\}, \{(0, 0), (0, 9), (0, 19), (1, 11)\},$
 $\{(0, 0), (0, 12), (1, 3), (1, 17)\}$;

$(m, n) = (10, 30)$:

$\{(0, 0), (0, 1), (1, 5), (2, 4)\}, \{(0, 0), (0, 2), (0, 5), (6, 19)\}, \{(0, 0), (0, 4), (1, 1), (4, 25)\},$
 $\{(0, 0), (0, 6), (1, 18), (3, 3)\}, \{(0, 0), (0, 8), (0, 18), (1, 8)\}, \{(0, 0), (0, 9), (4, 8), (5, 4)\},$
 $\{(0, 0), (0, 11), (3, 26), (4, 17)\}, \{(0, 0), (0, 13), (3, 22), (4, 14)\}, \{(0, 0), (0, 14), (4, 3), (4, 26)\},$
 $\{(0, 0), (1, 2), (6, 25), (7, 12)\}, \{(0, 0), (1, 3), (2, 18), (3, 29)\}, \{(0, 0), (1, 6), (2, 1), (3, 11)\},$
 $\{(0, 0), (1, 7), (2, 0), (3, 13)\}, \{(0, 0), (1, 9), (2, 7), (3, 1)\}, \{(0, 0), (1, 14), (3, 4), (5, 2)\},$
 $\{(0, 0), (1, 16), (3, 0), (5, 8)\}, \{(0, 0), (1, 19), (4, 10), (7, 22)\}, \{(0, 0), (2, 9), (4, 0), (6, 2)\},$
 $\{(0, 0), (2, 10), (4, 9), (7, 23)\}, \{(0, 0), (2, 11), (4, 4), (7, 14)\}, \{(0, 0), (2, 12), (5, 1), (7, 28)\},$
 $\{(0, 0), (2, 13), (4, 7), (7, 24)\}, \{(0, 0), (2, 17), (5, 10), (7, 5)\}, \{(0, 0), (2, 19), (5, 9), (7, 25)\}.$

当 $(m, n) \in \{(2, 60), (2, 120)\}$ 时, 由引理 5.4 知, $(m \times n, 2 \times 12, 4, 1)$ -SP 存在, 故结合引理 2.4 和已构造出的最优 $(2 \times 12, 4, 1)$ -SP 即得结论.

当 $(m, n) = (10, 6), (10, 12), (10, 24)$ 时, 含 $J(mn, 4, 1)$ 个基区组的最优 $(m \times n, 4, 1)$ -SP 分别与 $(m, n) = (2, 30), (2, 60), (2, 120)$ 情形下的最优 $(m \times n, 4, 1)$ -SP 等价, 故结论成立.

当 $(m, n) \in \{(10, 60), (10, 120)\}$ 时, 由引理 5.4 知, $(2 \times n, 2 \times 12, 4, 1)$ -SP 存在, 而由引理 3.1 知, $(5, 4, 1)$ -CDM 存在, 故利用构造 3.9 有 $(m \times n, 10 \times 12, 4, 1)$ -SP. 又因含 9 个基区组的最优 $(10 \times 12, 4, 1)$ -SP 存在 (等价于已知的最优 $(2 \times 60, 4, 1)$ -SP), 故利用引理 2.4 即得结论. $\square$

引理 5.7 设整数 $\beta \geq 2$, 则存在 $(2 \times 3 \cdot 2^\beta, 2 \times g, 4, 1)$ -SP, 其中 $g = 12$, 或 24, 或 48.

证明 当 $\beta \in \{2, 3, 4\}$ 时结论显然成立. 当 $\beta = 5$ 时, 由引理 5.4 即得结论. 当 $\beta \geq 6$ 时, 由引理 5.1 知, $(1 \times 3 \cdot 2^{\beta-1}, 1 \times g', 4, 1)$ -SP 存在, 其中 $g' = 12$, 或 24, 或 48, 故在推论 3.10 中令 $(a, b) = (1, 1)$ 有 $(2 \times 3 \cdot 2^\beta, 2 \times 2g', 4, 1)$ -SP. 最后, 结合引理 2.4 和 $\beta = 3, 4, 5$ 时的结论, 则有 $(2 \times 3 \cdot 2^\beta, 2 \times g, 4, 1)$ -SP, 其中 $g = 12$, 或 24, 或 48. $\square$

引理 5.8 设整数 $\beta \geq \alpha \geq 2$, 则存在 $(2^\alpha \times 3 \cdot 2^\beta, s \times t, 4, 1)$ -SP, 其中 $(s, t) = (2, 12)$ 或 $(4, 12)$.

证明 当 $(\alpha, \beta) = (2, 2)$ 时结论显然成立. 当 $\alpha = 2, \beta \in \{3, 4, 5\}$ 时, 由引理 5.4 和 5.5 即得结论. 当 $\alpha = 2$ 且 $\beta \geq 6$, 或 $\beta \geq \alpha \geq 3$ 时, 由引理 4.7 知, $(2^{\alpha-1} \times 2^{\beta-1}, 2 \times g', 4, 1)$ -SP 存在, 其中 $g' = 2$, 或 4,

或 16, 故利用推论 3.11 有 $(2^\alpha \times 3 \cdot 2^\beta, 4 \times 6g', 4, 1)$ -SP. 最后, 结合引理 2.4 和 $\alpha = 2, \beta = 2, 3, 5$ 时的结论, 则有 $(2^\alpha \times 3 \cdot 2^\beta, s \times t, 4, 1)$ -SP, 其中 $(s, t) = (2, 12)$ 或 $(4, 12)$. $\square$

引理 5.9 设整数 $\beta \geq \alpha \geq 1, (\alpha, \beta) \neq (1, 1)$, 则存在 $(2^\alpha \times 9 \cdot 2^\beta, s \times t, 4, 1)$ -SP, 其中 $(s, t) \in \{(2, 12), (2, 24), (2, 36), (2, 48), (4, 12)\}$.

证明 当 $(\alpha, \beta) = (1, 2)$ 时结论显然成立. 当 $(\alpha, \beta) \in \{(1, 3), (2, 2), (2, 3), (3, 3)\}$ 时, 由引理 5.4 和 5.5 即得结论. 当 $\alpha \geq 1, \beta \geq 4$ 时, 由文献 [9, 引理 2.3] 知, $(1 \times 72, 1 \times 12, 4, 1)$ -SP 存在, 故在推论 3.10 中令 $(a, b) = (\alpha, \beta - 3)$ 有 $(2^\alpha \times 9 \cdot 2^\beta, 2^\alpha \times 3 \cdot 2^{\beta-1}, 4, 1)$ -SP. 最后, 结合引理 2.4、5.7 和 5.8, 即得结论: 存在 $(2^\alpha \times 9 \cdot 2^\beta, s \times t, 4, 1)$ -SP, 其中 $(s, t) \in \{(2, 12), (2, 24), (2, 36), (2, 48), (4, 12)\}$. $\square$

引理 5.10 设整数 $\beta \geq \alpha \geq 1, (\alpha, \beta) \neq (1, 1), \gamma \geq 3$, 则存在 $(2^\alpha \times 2^\beta 3^\gamma, s \times t, 4, 1)$ -SP, 其中 $(s, t) \in \{(2, 12), (2, 24), (2, 48), (4, 12)\}$.

证明 对题设参数 α, β 和 γ , 由引理 5.2 知, $(1 \times 2 \cdot 3^\gamma, 1 \times 6, 4, 1)$ -SP 存在, 故在推论 3.10 中令 $(a, b) = (\alpha, \beta - 1)$ 有 $(2^\alpha \times 2^\beta 3^\gamma, 2^\alpha \times 3 \cdot 2^\beta, 4, 1)$ -SP. 最后, 结合引理 2.4、5.7 和 5.8, 即得结论: 存在 $(2^\alpha \times 2^\beta 3^\gamma, s \times t, 4, 1)$ -SP, 其中 $(s, t) \in \{(2, 12), (2, 24), (2, 48), (4, 12)\}$. $\square$

引理 5.11 设整数 $(s, t) \in \{(2, 12), (2, 24), (2, 36), (2, 48), (4, 12)\}$, $\gcd(u, 6) = \gcd(v, 6) = 1$, 则存在含 $J(stuv, 4, 1)$ 个基区组的最优 $(su \times tv, 4, 1)$ -SP.

证明 当 $(s, t) = (2, 48)$ 时, 由引理 5.3 知, $(u \times 24v, 1 \times 24, 4, 1)$ -SP 存在, 故在推论 3.10 中令 $(a, b) = (1, 1)$ 有 $(2u \times 48v, 2 \times 48, 4, 1)$ -SP. 又由引理 5.6 知, 含 $J(96, 4, 1) = 7$ 个基区组的最优 $(2 \times 48, 4, 1)$ -SP 存在, 因此利用引理 2.4 即得结论.

当 $(s, t) \in \{(2, 12), (2, 24), (2, 36), (4, 12)\}$ 时, 令 $u = 5^i u', v = 5^j v'$, 其中 $i, j \in \{0, 1\}$, $\gcd(u', 150) = 1, 25$, $\gcd(v', 150) = 1, 25$. 由引理 5.3 知, $(u' \times 6v', 1 \times 6, 4, 1)$ -SP 存在, 故利用推论 3.10 或 3.11 有 $(su' \times tv', s \times t, 4, 1)$ -SP. 而由引理 5.4 知, $(2 \times 36, 2 \times 6, 4, 1)$ -SP 和 $(4 \times 12, 2 \times 6, 4, 1)$ -SP 均存在, 故利用引理 2.4 有 $(su' \times tv', 2 \times g, 4, 1)$ -SP, 其中 $g = 6$, 或 12, 或 24. 又因引理 3.1 知, $(5, 4, 1)$ -CDM 存在, 故多次利用构造 3.9 有 $(su \times tv, 2 \cdot 5^i \times 5^j g, 4, 1)$ -SP. 最后, 对任意 $i, j \in \{0, 1\}$, 由引理 5.6 知, 含 $J(2 \cdot 5^{i+j} g, 4, 1)$ 个基区组的最优 $(2 \cdot 5^i \times 5^j g, 4, 1)$ -SP 存在, 再次利用引理 2.4 即得结论. $\square$

值得注意的是, 当 $\gcd(m, v) = \gcd(n, v) = 1$ 时, $(m \times nv, 4, 1)$ -SP 与 $(mv \times n, 4, 1)$ -SP 是等价的. 下面给出本节的主要结论.

定理 5.12 设 $mn \equiv 0 \pmod{24}$ 且 $\gcd(m, n, 6) = 2$, 则存在含 $J(mn, 4, 1)$ 个基区组的最优 $(m \times n, 4, 1)$ -SP.

证明 对题设参数 m 和 n , 不妨令 $m = 2^\alpha u, n = 2^\beta 3^\gamma v$, 其中 $\beta \geq \alpha \geq 1, (\alpha, \beta) \neq (1, 1), \gamma \geq 1, \gcd(u, 6) = \gcd(v, 6) = 1$.

由引理 5.7–5.10 知, $(2^\alpha \times 2^\beta 3^\gamma, s \times t, 4, 1)$ -SP 存在, 其中 $(s, t) \in \{(2, 12), (2, 24), (2, 36), (2, 48), (4, 12)\}$, 而由引理 3.2 知, $(Z_u \times Z_v, 4, 1)$ -DM 存在. 故利用构造 3.8 有 $(m \times n, su \times tv, 4, 1)$ -SP. 最后, 由引理 5.11 知, 含 $J(stuv, 4, 1)$ 个基区组的最优 $(su \times tv, 4, 1)$ -SP 存在, 因此, 利用引理 2.4 即得结论. $\square$

6 结论

结合定理 4.9 和 5.12 即得如下结论.

定理 6.1 设正整数 m 和 n 满足下列条件之一:

(1) $mn \equiv 8, 16 \pmod{24}$, $\gcd(m, n, 2) = 2$, 且 $mn \equiv 16 \pmod{32}$ 和 $\gcd(m, n, 4) = 2$ 不同时成立, 其中 m 和 n 的所有奇素因子均模 6 余 1;

(2) $mn \equiv 0 \pmod{24}$ 且 $\gcd(m, n, 6) = 2$,

则有 $\Theta(m, n, 4, 1) = \lfloor \frac{mn-1}{12} \rfloor$, 即码字容量为 $\lfloor \frac{mn-1}{12} \rfloor$ 的最优 $(m, n, 4, 1)$ -OOSPC 存在.

证明 由引理 2.1 知, 码字容量为 $\lfloor \frac{mn-1}{12} \rfloor$ 的最优 $(m, n, 4, 1)$ -OOSPC 等价于一个含 $J(mn, 4, 1) = \lfloor \frac{mn-1}{12} \rfloor$ 个基区组的最优 $(m \times n, 4, 1)$ -SP, 因此, 结合定理 4.9 和 5.12 即得结论. $\square$

致谢 感谢审稿人对本文提出的宝贵意见和建议.

参考文献

- 1 Kitayama K. Novel spatial spread spectrum based fiber optic CDMA networks for image transmission. *IEEE J Sel Area Comm*, 1994, 12: 762–772
- 2 Kwong W C, Yang G C. Image transmission in multicore-fiber code-division multiple-access networks. *IEEE Commun Lett*, 1998, 2: 285–287
- 3 Yang G C, Kwong W C. Two-dimensional spatial signature patterns. *IEEE Trans Commun*, 1996, 44: 184–191
- 4 Johnson S M. A new upper bound for error-correcting codes. *IEEE Trans Inform Theory*, 1962, 8: 203–207
- 5 Chung F R K, Salehi J A, Wei V K. Optical orthogonal codes: Design, analysis, and applications. *IRE Trans Inform Theory*, 1989, 35: 595–604
- 6 Yin J. Some combinatorial constructions for optical orthogonal codes. *Discrete Math*, 1998, 185: 201–219
- 7 Abel R J R, Buratti M. Some progress on $(v, 4, 1)$ difference families and optical orthogonal codes. *J Combin Theory Ser A*, 2004, 106: 59–75
- 8 Chang Y, Fuji-Hara R, Miao Y. Combinatorial constructions of optimal optical orthogonal codes with weight 4. *IEEE Trans Inform Theory*, 2003, 49: 1283–1292
- 9 Chang Y, Miao Y. Constructions for optimal optical orthogonal codes. *Discrete Math*, 2003, 261: 127–139
- 10 Chang Y, Yin J. Further results on optimal optical orthogonal codes with weight 4. *Discrete Math*, 2004, 279: 135–151
- 11 Feng T, Chang Y, Ji L. Constructions for rotational Steiner quadruple systems. *J Combin Des*, 2009 17: 353–368
- 12 Fuji-Hara R, Miao Y, Yin J. Optimal $(9v, 4, 1)$ optical orthogonal codes. *SIAM J Discrete Math*, 2001, 14: 256–266
- 13 Ge G, Yin J. Constructions for optimal $(v, 4, 1)$ optical orthogonal codes. *IEEE Trans Inform Theory*, 2001, 47: 2998–3004
- 14 Wang X, Chang Y. Further results on $(v, 4, 1)$ -perfect difference families. *Discrete Math*, 2010, 310: 1995–2006
- 15 Sawa M, Kageyama S. Optimal optical orthogonal signature pattern codes of weight 3. *Biom Lett*, 2009, 46: 89–102
- 16 Pan R, Chang Y. Combinatorial constructions for maximum optical orthogonal signature pattern codes. *Discrete Math*, 2013, 313: 2918–2931
- 17 Sawa M. Optical orthogonal signature pattern codes with maximum collision parameter 2 and weight 4. *IEEE Trans Inform Theory*, 2010, 56: 3613–3620
- 18 Buratti M. Recursive constructions for difference matrices and relative difference families. *J Combin Des*, 1998, 6: 165–182
- 19 Colbourn C J. Difference matrices. In: Colbourn C J, Dinitz J H, eds. *CRC Handbook of Combinatorial Designs*. New York: CRC Press, 2007, 411–419
- 20 Abel R J R, Colbourn C J, Dinitz J H. Mutually orthogonal latin squares (MOLS). In: Colbourn C J, Dinitz J H, eds. *CRC Handbook of Combinatorial Designs*. New York: CRC Press, 2007, 160–193

Further results on optimal $(m, n, 4, 1)$ optical orthogonal signature pattern codes

PAN Rong & CHANG YanXun

Abstract To support high-speed multiple access network applications, especially image applications, Kitayama first presented the concept of optical orthogonal signature pattern code (OOSPC). An (m, n, k, λ) -OOSPC is a

family of $(0, 1)$ -matrices of Hamming weight k satisfying two correlation properties. Let $\Theta(m, n, k, \lambda)$ denote the largest possible number of codewords among all (m, n, k, λ) -OOSPCs. An (m, n, k, λ) -OOSPC with $\Theta(m, n, k, \lambda)$ codewords is said to be optimal. In this paper, we confirm $\Theta(m, n, 4, 1) = \lfloor \frac{mn-1}{12} \rfloor$, in other words, we construct an $(m, n, 4, 1)$ -OOSPC with $\lfloor \frac{mn-1}{12} \rfloor$ codewords for any positive integers m and n satisfying one of the following:

- (1) $mn \equiv 8, 16 \pmod{24}$, each of whose odd prime factor is congruent to 1 modulo 6, with the exception of $\gcd(m, n, 2) = 1$, or $mn \equiv 16 \pmod{32}$ and $\gcd(m, n, 4) = 2$;
- (2) $mn \equiv 0 \pmod{24}$ and $\gcd(m, n, 6) = 2$.

Keywords optical orthogonal signature pattern code, strictly G -invariant packing, difference matrix

MSC(2010) 05B40

doi: 10.1360/012014-49