

最优变重量光正交码的一些构造

袁 宁, 王小苗*

(宁波大学 理学院, 浙江 宁波 315211)

摘要: 光正交码是具有良好的自相关性和互相关性的序列, 在光纤码分多址(OCDMA)系统中有着重要的应用. 利用分圆类的方法, 给出了一些最优且 g -正则的循环填充设计的直接构造. 通过建立循环填充设计与变重量光正交码之间的关系, 得到了权重为 3 和 4 的最优变重量光正交码的构造方法. 证明了当 $Q \in \{(1/3, 2/3), (2/3, 1/3), (1/2, 1/2)\}$ 时, 最优 $(v, \{3, 4\}, 1, Q)$ -光正交码存在的无穷类.

关键词: 填充设计; 光正交码; 变重量; 分圆类; 最优

中图分类号: O157.2

文献标志码: A

文章编号: 1001-5132 (2013) 03-0066-06

1989 年 Salehi 等^[1-2]提到, 光正交码作为一种特征序列广泛应用于光纤信道上的码分多址系统. 大量已有的工作集中在码重相同的光正交码的研究上. 然而, 如文献[3]中提到, 由于光正交码的码字个数依赖于重量, 因而变重量光正交码相对于常重量光正交码能产生更多的码字. 为了满足多种服务的需求, Yang^[4]在 1996 年引入了变重量光正交码的概念. 近几年来, 变重量光正交码引起了更多人的关注, 相关结果参见文献[5-9].

基于文献[4]的记号, 令 W, L, Q 分别表示集合 $\{w_0, w_1, \dots, w_p\}$, $\{\lambda_a^0, \lambda_a^1, \dots, \lambda_a^p\}$ 以及 $\{q_0, q_1, \dots, q_p\}$. 不失一般性, 设 $w_0 < w_1 < \dots < w_p$. 一个 (n, W, L, λ_c, Q) -变重量光正交码 C , 简记为 (n, W, L, λ_c, Q) -OOC, 是一组长度为 n 的 $(0, 1)$ 序列, 满足以下 3 个性质.

(1) 码字重量分布. C 中任意一个 n 长序列的汉明重量均在集合 W 中; 且 C 中恰好有 $q_i |C|$ 个重量为 w_i 的码字, $1 \leq i \leq p$, 即 q_i 是重量为 w_i 的码字在 C 中所占的比重, 其中 $\sum_{i=1}^p q_i = 1$.

(2) 周期自相关性. 对于任意的 $X = \{x_0, x_1, \dots, x_{n-1}\} \in C$, 其汉明重量 $w_i \in W$, 有 $\sum_{t=0}^{n-1} x_t x_{t \oplus \tau} \leq \lambda_a^i$, 其中 τ 为任意整数, $0 < \tau < n$.

(3) 周期互相关性. 对于任意的 $X = \{x_0, x_1, \dots, x_{n-1}\} \in C$, $Y = \{y_0, y_1, \dots, y_{n-1}\} \in C$, $X \neq Y$, 以及对任意整数 τ , 有 $\sum_{t=0}^{n-1} x_t y_{t \oplus \tau} \leq \lambda_c$. $\oplus$ 表示模 n 的加法运算.

当 $\lambda_a^0 = \lambda_a^1 = \dots = \lambda_a^p = \lambda_c = \lambda$ 时, (n, W, L, λ_c, Q) -OOC 简记为 (n, W, λ, Q) -OOC.

1 预备知识

定义 1 令 K 是正整数集, 一个 2 -CP($K, 1; v$) (循环填充)是指 Z_v 上的 t 个子集(基区组)族 $\mathcal{F} = \{B_1, B_2, \dots, B_t\}$, $K = \{|B_i| : 1 \leq i \leq t\} = \{k_1, k_2, \dots, k_h\}$, 使 $\Delta \mathcal{F} = \{b_{ic} - b_{ic'} : 1 \leq i \leq t, 1 \leq c, c' \leq |B_i|, c \neq c'\}$ 覆盖 Z_v 的非零元最多一次, 且对于每个 $B_i = \{b_1, b_2, \dots, b_h\} \in \mathcal{F}$, $B + i$, $0 \leq i \leq v-1$, 是成对互不相同的, 其中 $B + i = \{b_1 + i, b_2 + i, \dots, b_h + i\} \subset Z_v$. 一个 2 -CP($K, 1, Q; v$)是指一个 2 -CP($K, 1; v$), 使得大小为 k_j 的基区组的个数所占的比重是 q_j , $1 \leq j \leq h$, 其中 $Q = \{q_1, q_2, \dots, q_h\}$.

设 $\mathcal{F}$ 为一个 2 -CP($W, 1, Q; v$). 对于任一 $B \in \mathcal{F}$, 由 B 所产生的差记为 $\Delta B = \{a - b : a, b \in B, a \neq b\}$. 令 $\Delta \mathcal{F} = \bigcup_{B \in \mathcal{F}} \Delta B$. Z_v 中没有被 $\Delta \mathcal{F}$ 覆盖的非零整数构成的集合称为 $\mathcal{F}$ 的差剩余, 记为 $DL(\mathcal{F})$. 若

$DL(\mathcal{F}) \cup \{0\}$ 构成 Z_v 中的一个 g 阶加法子群, 则称该 2-CP($W, 1, Q; v$) $\mathcal{F}$ 为 g -正则的.

引理 1^[5] 最优 2-CP($W, 1, Q; v$) 的存在性等价于最优 ($v, W, 1, Q$)-OOC 的存在性.

引理 2^[5] 记 $Q=(a_1/b, \dots, a_r/b)$, 若 $1 \leq g \leq w$, 则 g -正则 2-CP($W, 1, Q; v$) 是最优的, 其中 $w = \sum_{i=1}^r a_i w_i (w_i - 1)$.

令 $q \equiv 1 \pmod{n}$ 为素数, 记 $\theta \in GF(q)$ 为本原元. $C_0^n = \{\theta^i : 0 \leq i \leq (q-1)/n\}$. C_j^n 为 C_0^n 的陪集, 即 $C_j^n = \theta^j C_0^n$, $0 \leq j \leq n-1$. C_0^n 的陪集的相异代表元系记为 SDRC.

对于 $B = \{(x_1, i_1), (x_2, i_2), \dots, (x_k, i_k)\} \in (Z_q \times Z_s)^k$. 令 $c \in Z_q$, 定义 $c \cdot B = \{(cx_1, i_1), (cx_2, i_2), \dots, (cx_k, i_k)\}$.

假设 B 是集合 $Z_q \times Z_s$ 的子集, 定义 $D_j = \{d : (d, j) \text{ 是由 } B \text{ 得到的差}\}$.

引理 3^[10] 令 q 为素数, $q \equiv 1 \pmod{e}$ 且 $q - [\sum_{r=0}^{s-2} \binom{s}{r} (s-r-1)(e-1)^{s-r}] \sqrt{q} - se^{s-1} > 0$. 则对于任意给定的 s -元组 $(i_1, i_2, \dots, i_s) \in \{0, 1, \dots, e-1\}^s$, 以及 $GF(q)$ 上成对互不相同的元素构成的 s -元组 $(c_1, c_2, \dots, c_s)$, 存在元素 $x \in GF(q)$, 使得 $x + c_r \in C_{i_r}^e$, 其中 $1 \leq r \leq s$.

引理 4 (1) 当 $q \equiv 13 \pmod{24}$ 为素数且 $q > 105841$ 时, 存在 $x \in Z_q^*$, 使得:

- (I) $x \in C_1^6, x-1 \in C_0^6, x+1 \in C_3^6$,
- (II) $x \in C_5^6, x-1 \in C_3^6, x+1 \in C_3^6$.

(2) 当 $q \equiv 7 \pmod{12}$ 为素数, 且 $q > 105841$ 时, 存在 $x \in Z_q^*$, 使得:

- (I) $x \in C_1^3, x-1 \in C_3^6, x+1 \in C_2^3$,
- (II) $x \in C_2^3, x-1 \in C_3^6, x+1 \in C_1^3$.

(3) 当 $q \equiv 7 \pmod{12}$ 为素数, 且 $q > 105841$ 时, 存在 $x \in Z_q^*$, 使得:

- (I) $x \in C_1^6, x-1 \in C_1^6, x+1 \in C_2^6$,
- (II) $x \in C_1^6, x-1 \in C_4^6, x+1 \in C_5^6$,
- (III) $x \in C_5^6, x-1 \in C_2^6, x+1 \in C_1^6$,
- (IV) $x \in C_5^6, x-1 \in C_5^6, x+1 \in C_4^6$.

(4) 当 $q \equiv 7 \pmod{12}$ 为素数, 且 $q > 837$ 时, 存在 $x \in Z_q^*$, 使得:

- (I) $x \in C_1^3, x-1 \in C_1^3, x+1 \in C_2^3$,
- (II) $x \in C_2^3, x-1 \in C_3^6, x+1 \in C_1^3$.

(5) 当 $q \equiv 7 \pmod{12}$ 为素数, 且 $q > 105841$ 时, 存在 $x, y \in Z_q^*$, 使得:

$$(I) \ x \in C_1^6, x-1 \in C_4^6, x+1 \in C_5^6, y \in C_4^6, y+1 \in C_3^6, \\ y-1 \in C_2^3,$$

$$(II) \ x \in C_4^6, x-1 \in C_1^6, x+1 \in C_2^6, y \in C_1^6, y+1 \in C_3^6, \\ y-1 \in C_2^3,$$

$$(III) \ x \in C_2^6, x-1 \in C_5^6, x+1 \in C_4^6, y \in C_5^6, y+1 \in C_3^6, \\ y-1 \in C_1^3,$$

$$(IV) \ x \in C_5^6, x-1 \in C_2^6, x+1 \in C_1^6, y \in C_2^6, y+1 \in C_3^6, \\ y-1 \in C_1^3.$$

(6) 当 $q \equiv 19 \pmod{36}$ 为素数, 且 $q > 114342193$ 时, 存在 $x, y \in Z_q^*$, 使得:

$$(I) \ y \in C_1^{18}, y+1 \in C_{12}^{18}, y-1 \in C_{12}^{18}, x \in C_8^{18}, x+1 \in \\ C_6^{18},$$

$$(II) \ y \in C_{10}^{18}, y+1 \in C_3^{18}, y-1 \in C_{12}^{18}, x \in C_8^{18}, x+1 \in \\ C_{15}^{18},$$

$$(III) \ y \in C_4^{18}, y+1 \in C_3^{18}, y-1 \in C_{12}^{18}, x \in C_{14}^{18}, x+ \\ 1 \in C_{15}^{18},$$

$$(IV) \ y \in C_{13}^{18}, y+1 \in C_{12}^{18}, y-1 \in C_{12}^{18}, x \in C_{14}^{18}, x+ \\ 1 \in C_6^{18},$$

$$(V) \ y \in C_8^{18}, y+1 \in C_{15}^{18}, y-1 \in C_6^{18}, x \in C_{10}^{18}, x+ \\ 1 \in C_3^{18},$$

$$(VI) \ y \in C_{17}^{18}, y+1 \in C_6^{18}, y-1 \in C_6^{18}, x \in C_{10}^{18}, x+ \\ 1 \in C_{12}^{18},$$

$$(VII) \ y \in C_2^{18}, y+1 \in C_{15}^{18}, y-1 \in C_6^{18}, x \in C_{16}^{18}, x+ \\ 1 \in C_3^{18},$$

$$(VIII) \ y \in C_{11}^{18}, y+1 \in C_6^{18}, y-1 \in C_6^{18}, x \in C_{16}^{18}, x+ \\ 1 \in C_{12}^{18},$$

$$(IX) \ y \in C_5^{18}, y+1 \in C_6^{18}, y-1 \in C_6^{18}, x \in C_4^{18}, x+ \\ 1 \in C_{12}^{18},$$

$$(X) \ y \in C_{14}^{18}, y+1 \in C_{15}^{18}, y-1 \in C_6^{18}, x \in C_4^{18}, x+1 \in \\ C_3^{18},$$

$$(XI) \ y \in C_7^{18}, y+1 \in C_{12}^{18}, y-1 \in C_{12}^{18}, x \in C_2^{18}, x+ \\ 1 \in C_6^{18},$$

$$(XII) \ y \in C_{16}^{18}, y+1 \in C_3^{18}, y-1 \in C_{12}^{18}, x \in C_2^{18}, x+ \\ 1 \in C_{15}^{18}.$$

证明 以下仅证明(2)和(6)两种情况, 其余情况可类似得到.

(2) 当 $q \equiv 7 \pmod{12}$ 为素数, 且 $q > 105841$ 时, 应用引理 3, 取 $e=6$, $s=3$, 则存在元素 $x \in Z_q^*$, 满足条件(I)或(II).

(6) 当 $q \equiv 19 \pmod{36}$ 为素数, 且 $q > 114342193$ 时, 应用引理 3, 取 $e=18$, $s=3$, 则存在元素

$y \in Z_q^*$, 满足其中任一条件. 当 $q \equiv 19(\text{mod } 36)$, 且 $q > 83592$ 时, 再次利用引理 3, 取 $e=18$, $s=2$, 则存在元素 $x \in Z_q^*$ 满足条件.

2 循环填充设计的构造

2.1 2-CP({3,4},1,{2/3,1/3};v)的构造

引理 5 若 $q \equiv 13(\text{mod } 24)$ 为素数, 则存在一个最优, 且 2-正则 2-CP({3,4},1,{2/3,1/3};2q).

证明 当 $q \equiv 13(\text{mod } 24)$ 为素数, 且 $q > 105841$ 时, $\gcd(2,q)=1$, 故 $Z_q \times Z_2 \cong Z_{2q}$. 令

$$A_1 = \{(0,0), (1,0), (x,1), (x^2,1)\},$$

$$A_2 = \{(0,0), (x^4,1), (x^5,1)\},$$

$$A_3 = \{(0,0), (-x^2,0), (x^3,0)\},$$

则

$$D_0 = \pm\{1, x^2 - x, x^5 - x^4, x^2, x^3, x^3 + x^2\},$$

$$D_1 = \pm\{x, x^2, x-1, x^2-1, x^4, x^5\}.$$

由于 $q \equiv 13(\text{mod } 24)$, 故 $-1 \in C_6^{12}$, 则由引理 4(1)知, 存在元素 $x \in Z_q^*$, 使得 D_0, D_1 均为 C_0^{12} 的一个 SDRC. 令 $\mathcal{F} = \{h \cdot A_i : i=1,2,3, h \in C_0^{12}\}$, 则 $\Delta\mathcal{F}$ 恰好覆盖 $(Z_q \times Z_2) \setminus (\{0\} \times Z_2)$ 中的每个元素一次, 而不含 $\{0\} \times Z_2$ 中的任何元素. 故 $\mathcal{F}$ 构成了一个 2-正则 2-CP({3,4},1,{2/3,1/3};2q), 因为 $g=2 < 24$, 由引理 2 知, 此循环填充是最优的.

当 $q \equiv 13(\text{mod } 24)$ 为素数, $q \leq 105841$, 且 $q \notin \{13, 37, 61, 157\}$ 时, 利用计算机搜索可以找到 Z_q^* 中满足引理 4(1)的 x . 在表 1 中仅列出当 $q \leq 853$ 时满足相应条件的三元组 (q, θ, x) .

表 1 (q, θ, x) , 其中 $q \leq 853$

q	θ	x	q	θ	x
109	6	18	181	2	50
349	2	250	373	2	141
541	2	230	613	2	316
733	6	130	757	2	497
q	θ	x	q	θ	x
229	6	142	277	5	53
397	5	184	421	2	378
661	2	200	709	2	97
829	2	699	853	2	342

当 $q \in \{13, 37, 61, 157\}$ 时, 以上的集合 A_1, A_2, A_3 分别用 $A_1 = \{(0,0), (1,0), (2,1), (a,1)\}$, $A_2 = \{(0,0), (b,1), (c,1)\}$, $A_3 = \{(0,0), (d,0), (e,0)\}$ 来替换, 其中:

$$q=13: (a,b,c,d,e) = (5,3,7,2,7),$$

$$q=37: (a,b,c,d,e) = (5,6,12,2,18),$$

$$q=61: (a,b,c,d,e) = (12,5,10,2,25),$$

$$q=157: (a,b,c,d,e) = (10,5,15,5,18).$$

引理 6 若 $q \equiv 7(\text{mod } 12)$ 是素数, 则存在一个最优, 且 4-正则 2-CP({3,4},1,{2/3,1/3};4q).

证明 当 $q \equiv 7(\text{mod } 12)$ 为素数, 且 $q > 105841$ 时, 由 $\gcd(4,q)=1$ 知 $Z_q \times Z_4 \cong Z_{4q}$. 令

$$A_1 = \{(0,0), (1,1), (x,2), (x^2,3)\},$$

$$A_2 = \{(0,0), (x,1), (-x^2,3)\},$$

$$A_3 = \{(0,0), (1,0), (x+1,0)\},$$

则

$$D_0 = \pm\{1, x, x+1\},$$

$$D_1 = \{1, x-1, x^2-x, -x^2, x, x^2\},$$

$$D_2 = \pm\{x, x^2-1, x^2+x\}.$$

由于 $q \equiv 7(\text{mod } 12)$, 故 $-1 \in C_3^6$. 则由引理 4(2)知, 存在元素 $x \in Z_q^*$, 使得 D_j 是 C_0^6 的一个 SDRC, $0 \leq j \leq 2$. 令 $\mathcal{F} = \{h \cdot A_i : i=1,2,3, h \in C_0^6\}$, 则 $\Delta\mathcal{F}$ 恰好覆盖 $(Z_q \times Z_4) \setminus (\{0\} \times Z_4)$ 中的每个元素一次, 而不含 $\{0\} \times Z_4$ 中的任何元素. 故 $\mathcal{F}$ 构成了一个 4-正则 2-CP({3,4},1,{2/3,1/3};4q). 因为 $g=4 < 24$, 由引理 2 知, 此循环填充是最优的.

当 $q \equiv 7(\text{mod } 12)$ 为素数, $q \leq 105841$, 且 $q \notin \{7, 31\}$ 时, 利用计算机搜索可以找到 Z_q^* 中满足引理 4(2)的 x . 在表 2 中仅列出当 $q \leq 331$ 时满足相应条件的三元组 (q, θ, x) .

表 2 (q, θ, x) , 其中 $q \leq 331$

q	θ	x	q	θ	x
19	2	13	43	3	9
103	5	40	127	3	81
163	2	32	199	3	192
271	6	193	283	3	80
q	θ	x	q	θ	x
67	2	28	79	3	59
139	2	24	151	6	88
211	2	201	223	3	96
307	5	212	331	3	227

当 $q=31$ 时, 以上的集合 A_1, A_2, A_3 分别用 $A_1 = \{(0,0), (1,1), (6,2), (9,3)\}$, $A_2 = \{(0,0), (7,1), (2,3)\}$, $A_3 = \{(0,0), (1,0), (6,0)\}$ 来替换.

当 $q=7$ 时, 存在 Z_{28} 上的最优 4-正则 2-CP({3,

4}, 1, \{2/3, 1/3\}; 28), 其基区组为 \{0, 1, 3, 12\}, \{0, 4, 10\}, \{0, 5, 13\}.

引理 7 若 $q \equiv 7 \pmod{12}$ 为素数, 则存在一个最优且 8-正则 $2\text{-CP}(\{3, 4\}, 1, \{2/3, 1/3\}; 8q)$.

证明 当 $q \equiv 7 \pmod{12}$ 为素数, 且 $q > 105841$ 时, 由 $\gcd(8, q) = 1$ 知 $Z_q \times Z_8 \cong Z_{8q}$. 令

$$\begin{aligned} A_1 &= \{(0, 0), (1, 1), (x, 2), (x^2, 3)\}, \\ A_2 &= \{(0, 0), (-1, 1), (-x, 2), (-x^2, 3)\}, \\ A_3 &= \{(0, 0), (1, 3), (-x, 3)\}, \\ A_4 &= \{(0, 0), (x, 3), (x^3, 3)\}, \\ A_5 &= \{(0, 0), (x^2, 2), (x^4, 4)\}, \\ A_6 &= \{(0, 0), (x^2, 4), (x^3, 4)\}, \end{aligned}$$

则

$$\begin{aligned} D_0 &= \pm\{x+1, x^3-x, x^3-x^2\}, \\ D_1 &= \pm\{1, x-1, x^2-x\}, \\ D_2 &= \pm\{x, \pm(x^2-1), x^2, x^4-x^2\}, \\ D_3 &= \pm\{x^2, \pm x, 1, x^3\}, \quad D_4 = \pm\{x^2, x^3, x^4\}. \end{aligned}$$

由于 $q \equiv 7 \pmod{12}$, 故 $-1 \in C_3^6$. 则由引理 4(3) 知, 存在元素 $x \in Z_q^*$, 使得 D_j 是 C_0^6 的一个 SDR, $0 \leq j \leq 4$. 令 $\mathcal{F} = \{h \cdot A_i : i = 1, \dots, 6, h \in C_0^6\}$, 则 $\Delta\mathcal{F}$ 恰好覆盖 $(Z_q \times Z_8) \setminus (\{0\} \times Z_8)$ 中的每个元素一次, 而不含 $\{0\} \times Z_8$ 中的任何元素, 故 $\mathcal{F}$ 构成了一个 8-正则 $2\text{-CP}(\{3, 4\}, 1, \{2/3, 1/3\}; 8q)$. 因为 $g = 8 < 24$, 由引理 2 知, 此循环填充是最优的.

当 $q \equiv 7 \pmod{12}$ 为素数, $q \leq 105841$, 且 $q \notin \{7, 67\}$ 时, 利用计算机搜索可以找到 Z_q^* 中满足引理 4(3) 的 x . 在表 3 中仅列出当 $q \leq 331$ 时满足相应条件的三元组 (q, θ, x) .

表 3 (q, θ, x) , 其中 $q \leq 331$

q	θ	x	q	θ	x
19	2	3	31	3	11
103	5	5	127	3	45
163	2	130	199	3	166
271	6	234	283	3	170
q	θ	x	q	θ	x
43	3	30	79	3	48
139	2	21	151	6	146
211	2	3	223	3	70
307	5	214	331	3	3

当 $q = 67$ 时, 以上的集合 $A_1, \dots, A_6$ 分别用 $A_1 = \{(0, 0), (1, 1), (3, 2), (2, 3)\}$, $A_2 = \{(0, 0), (4, 1), (2, 2),$

$(14, 3)\}$, $A_3 = \{(0, 0), (3, 3), (4, 3)\}$, $A_4 = \{(0, 0), (6, 3), (12, 3)\}$, $A_5 = \{(0, 0), (4, 2), (11, 4)\}$, $A_6 = \{(0, 0), (1, 4), (13, 4)\}$ 来替换.

当 $q = 7$ 时, 存在 Z_{56} 上最优 8-正则 $2\text{-CP}(\{3, 4\}, 1, \{2/3, 1/3\}; 56)$, 其基区组为: $\{0, 1, 3, 9\}$, $\{0, 4, 15, 38\}$, $\{0, 5, 25\}$, $\{0, 10, 26\}$, $\{0, 12, 29\}$, $\{0, 13, 32\}$.

2.2 $2\text{-CP}(\{3, 4\}, 1, \{1/3, 2/3\}; \nu)$ 的构造

引理 8 若 $q \equiv 7 \pmod{12}$ 为素数, 则存在一个最优, 且 5-正则 $2\text{-CP}(\{3, 4\}, 1, \{1/3, 2/3\}; 5q)$.

证明 当 $q \equiv 7 \pmod{12}$ 为素数, 且 $q > 837$ 时, 由 $\gcd(5, q) = 1$ 知 $Z_q \times Z_5 \cong Z_{5q}$. 令

$$\begin{aligned} A_1 &= \{(0, 0), (1, 1), (x, 2), (x^2, 4)\}, \\ A_2 &= \{(0, 0), (-1, 1), (-x, 2), (-x^2, 4)\}, \\ A_3 &= \{(0, 0), (-1, 0), (x, 0)\}, \end{aligned}$$

则

$$\begin{aligned} D_0 &= \pm\{1, x, x+1\}, \\ D_1 &= \pm\{1, x-1, x^2\}, \\ D_2 &= \pm\{x, x^2-x, x^2-1\}. \end{aligned}$$

由于 $q \equiv 7 \pmod{12}$, 故 $-1 \in C_3^6$. 则由引理 4(4) 知, 存在元素 $x \in Z_q^*$, 使得 D_j 是 C_0^6 的一个 SDR, $0 \leq j \leq 2$. 令 $\mathcal{F} = \{h \cdot A_i : i = 1, 2, 3, h \in C_0^6\}$, 则 $\Delta\mathcal{F}$ 恰好覆盖 $(Z_q \times Z_5) \setminus (\{0\} \times Z_5)$ 中的每个元素一次, 而不含 $\{0\} \times Z_5$ 中的任何元素, 故 $\mathcal{F}$ 构成了一个 5-正则的 $2\text{-CP}(\{3, 4\}, 1, \{1/3, 2/3\}; 5q)$. 因为 $g = 5 < 30$, 由引理 2 知, 此循环填充是最优的.

当 $q \equiv 7 \pmod{12}$ 为素数, 且 $q \leq 837$ 时, 利用计算机搜索可以找到 Z_q^* 中满足引理 4(4) 的 x . 在表 4 中仅列出当 $q \leq 283$ 时满足相应条件的三元组 (q, θ, x) .

表 4 (q, θ, x) , 其中 $q \leq 283$

q	θ	x	q	θ	x
7	3	4	19	2	3
67	2	19	79	3	3
139	2	16	151	6	36
211	2	45	233	3	185
q	θ	x	q	θ	x
31	3	25	43	3	30
103	5	5	127	3	22
163	2	42	199	3	3
271	6	114	283	3	185

引理 9 若 $q \equiv 7 \pmod{12}$ 为素数, 则存在一个

最优, 且 10-正则 2-CP($\{3,4\}, 1, \{1/3, 2/3\}; 10q$).

证明 当 $q \equiv 7 \pmod{12}$ 为素数, 且 $q > 105841$ 时, 由 $\gcd(10, q) = 1$ 知 $Z_q \times Z_{10} \cong Z_{10q}$. 令

$$\begin{aligned} A_1 &= \{(0, 0), (1, 1), (x, 2), (x^2, 3)\}, \\ A_2 &= \{(0, 0), (-1, 1), (-x^2, 3), (-x, 5)\}, \\ A_3 &= \{(0, 0), (x^2, 2), (x, 3), (x^3, 5)\}, \\ A_4 &= \{(0, 0), (1, 0), (y, 0), (y+1, 4)\}, \\ A_5 &= \{(0, 0), (x^3, 3), (x^3 + x^2, 7)\}, \\ A_6 &= \{(0, 0), (x^2 - x, 4), (x^2, 5)\}, \end{aligned}$$

则

$$\begin{aligned} D_0 &= \pm\{1, y, y-1\}, \\ D_1 &= \{\pm 1, \pm(x^2 - x), x, x-1\}, \\ D_2 &= \{x, \pm(x^2 - 1), x^2, x^2 - x, x^3 - x\}, \\ D_3 &= \{\pm x^2, x, x^3 - x^2, x^3, -(x^3 + x^2)\}, \\ D_4 &= \{1 - x, x^2 - x, x^2, 1, y, y+1\}, \\ D_5 &= \pm\{x, x^2, x^3\}. \end{aligned}$$

由于 $q \equiv 7 \pmod{12}$, 故 $-1 \in C_3^6$. 则由引理 4(5) 知, 存在元素 $x \in Z_q^*$, 使得 D_j 是 C_0^6 的一个 SDRC, $0 \leq j \leq 5$. 令 $\mathcal{F} = \{h \cdot A_i : i = 1, \dots, 6, h \in C_0^6\}$, 则 $\Delta\mathcal{F}$ 恰好覆盖 $(Z_q \times Z_{10}) \setminus (\{0\} \times Z_{10})$ 中的每个元素一次, 而不含 $\{0\} \times Z_{10}$ 中的任何元素, 故 $\mathcal{F}$ 构成了一个 10-正则 2-CP($\{3,4\}, 1, \{1/3, 2/3\}; 10q$). 因为 $g = 10 < 30$, 由引理 2 知, 此循环填充是最优的.

当 $q \equiv 7 \pmod{12}$ 为素数, $q \leq 105841$, 且 $q \notin \{7, 19, 31, 43, 67, 79, 127, 163\}$ 时, 利用计算机搜索可以找到 Z_q^* 中满足引理 4(5) 的 x, y . 在表 5 中仅列出当 $q \leq 379$ 时满足相应条件的四元组 (q, θ, x, y) .

表 5 (q, θ, x, y) , 其中 $q \leq 379$

q	θ	x	y	q	θ
103	5	5	36	139	2
199	3	166	10	211	2
271	6	234	18	283	3
331	3	128	219	367	6
x	y	q	θ	x	y
21	137	151	6	146	40
119	197	223	3	62	127
170	196	307	5	241	287
42	302	397	2	46	348

当 $q \in \{7, 19, 31, 43, 67, 79, 127, 163\}$ 时, 以上的集合 $A_1, \dots, A_6$ 分别用

$$A_1 = \{(0, 0), (1, 1), (a, 2), (b, 3)\},$$

$$A_2 = \{(0, 0), (c, 1), (d, 3), (e, 5)\},$$

$$A_3 = \{(0, 0), (f, 2), (g, 3), (h, 5)\},$$

$$A_4 = \{(0, 0), (1, 0), (h, 0), (i, 4)\},$$

$$A_5 = \{(0, 0), (j, 3), (k, 7)\},$$

$$A_6 = \{(0, 0), (l, 4), (m, 5)\},$$

来替换, 其中 $(a, b, c, d, e, f, g, h, i, j, k, l, m)$ 的值分别为:

$$q = 7: (3, 2, 5, 3, 2, 2, 6, 3, 3, 2, 4, 2, 3, 6),$$

$$q = 19: (3, 8, 4, 1, 10, 8, 2, 17, 4, 2, 5, 4, 10, 18),$$

$$q = 31: (6, 5, 3, 1, 10, 7, 21, 1, 6, 5, 3, 16, 3, 14),$$

$$q = 43: (3, 8, 6, 1, 9, 1, 10, 19, 7, 2, 3, 18, 7, 35),$$

$$q = 67: (3, 2, 4, 6, 2, 4, 11, 9, 7, 3, 1, 34, 1, 7),$$

$$q = 79: (3, 2, 3, 5, 10, 6, 1, 13, 4, 2, 3, 8, 12, 5),$$

$$q = 127: (6, 9, 9, 1, 12, 13, 6, 64, 12, 5, 13, 22, 29, 11),$$

$$q = 163: (3, 2, 3, 1, 13, 4, 8, 7, 3, 2, 4, 7, 4, 20).$$

2.3 2-CP($\{3,4\}, 1, \{1/2, 1/2\}; v$)的构造

引理 10 若 $q \equiv 19 \pmod{36}$ 为素数, 且 $q > 114342193$, 则存在一个 4-正则 2-CP($\{3,4\}, 1, \{1/2, 1/2\}; 4q$).

证明 当 $q \equiv 19 \pmod{36}$ 为素数, 且 $q > 114342193$ 时, 由 $\gcd(4, q) = 1$ 知 $Z_q \times Z_4 \cong Z_{4q}$. 令

$$A_1 = \{(0, 0), (-1, 0), (y^2 - 1, 1), (y - 1, 3)\},$$

$$A_2 = \{(0, 0), (y^2, 0), (y, 1), (y^3, 2)\},$$

$$A_3 = \{(0, 0), (y^3, 0), (y^4, 0), (y^5, 1)\},$$

$$A_4 = \{(0, 0), (1, 1), (y, 2), (y^2, 3)\},$$

$$A_5 = \{(0, 0), (-x, 0), (x^2, 0)\},$$

$$A_6 = \{(0, 0), (x, 1), (x+1, 3)\},$$

$$A_7 = \{(0, 0), (x^7, 2), (x^8 + x^7, 2)\},$$

$$A_8 = \{(0, 0), (-x, 1), (x^2, 2)\},$$

则

$$D_0 = \pm\{1, y^2, y^3, y^4, y^4 - y^3, x, x^2, x^2 + x, x^8\},$$

$$D_1 = \{y^2 - 1, y^2, 1 - y, -y, y, y - y^2, y^3 - y, y^5,$$

$$y^5 - y^3, y^5 - y^4, 1, y - 1, y^2 - y,$$

$$-y^2, x, -x - 1, -x, x^2 + x\},$$

$$D_2 = \pm\{y^2 - y, y^3, y^3 - y^2, y, y^2 - 1, 1,$$

$$x^7, x^8 + x^7, x^2\}.$$

由于 $q \equiv 19 \pmod{36}$, 故 $-1 \in C_9^{18}$. 则由引理 4(6) 知, 存在元素 $x, y \in Z_q^*$, 使得 D_j 是 C_0^{18} 的一个 SDRC, $0 \leq j \leq 2$. 令 $\mathcal{F} = \{h \cdot A_i : 1 \leq i \leq 8, h \in C_0^{18}\}$. 则 $\Delta\mathcal{F}$ 恰好覆盖了 $(Z_q \times Z_4) \setminus (\{0\} \times Z_4)$ 中的每个元素一次, 而不含 $\{0\} \times Z_4$ 中的任何元素. 故 $\mathcal{F}$ 构成

了一个 4-正则 $2\text{-CP}(\{3,4\},1,\{1/2,1/2\};4q)$. 因为 $g=4<18$, 由引理 2 知, 此循环填充是最优的.

3 结论

由引理 5~10, 结合引理 1, 可得定理 1.

定理 1 对于素数 q , 存在最优 $(v,\{3,4\},1,Q)$ OOC, 其中 $q\equiv 13(\bmod 24)$, $v=2q$, $Q=\{2/3,1/3\}$; 或 $q\equiv 7(\bmod 12)$, $v=4q,8q$, $Q=\{2/3,1/3\}$; 或 $q\equiv 7(\bmod 12)$, $v=5q,10q$, $Q=\{1/3,2/3\}$; 或 $q\equiv 19(\bmod 36)$, $q>14342193$, $v=4q$, $Q=\{1/2,1/2\}$.

参考文献:

- [1] Salehi J A, Brackett C A. Code division multiple access technique in optical fiber network-Part II systems performance analysis[J]. IEEE Trans Commum, 1989, 37(8):834-842.
- [2] Salehi J A. Code division multiple access techniques in optical fiber networks-part I fundamental principles[J]. IEEE Trans Commun, 1989, 37(8):824-833.
- [3] Jiang J, Wu D, Fan P. General constructions of optimal variable-weight optical orthogonal codes[J]. IEEE Trans Inform Theory, 2011, 57(7):4488-4496.
- [4] Yang G C. Variable-weight optical orthogonal codes for CDMA networks with multiple performance requirements [J]. IEEE Trans Commun, 1996, 44(1):47-55.
- [5] Wu D, Zhao H, Fan P, et al. Optimal variable-weight optical orthogonal codes via difference packing[J]. IEEE Trans Inform Theory, 2010, 56(8):4053-4060.
- [6] Zhao H, Wu D, Fan P. Constructions of optimal variable-weight optical orthogonal codes[J]. J Combin Des, 2010, 18(4):274-291.
- [7] Buratti M, Wei Y, Wu D, et al. Relative difference families with variable block size and their related OOCs[J]. IEEE Trans Inform Theory, 2011, 57(11):7489-7497.
- [8] Zhao H, Wu D, Mo Z. Further results on optimal $(v,\{3,k\},1,\{1/2,1/2\})$ -OOCs for $k=4,5$ [J]. Discrete Math, 2011, 311(1):16-23.
- [9] Zhao H. On balanced optimal $(18u,\{3,4\},1)$ optical orthogonal codes[J]. J Combin Des, 2012, 20(6):290-303.
- [10] Chang Y, Ji L. Optimal $(4up,5,1)$ optical orthogonal codes[J]. J Combin Des, 2004, 12(5):346-361.

Some Constructions on Optimal Variable-weight Optical Orthogonal Codes

YUAN Ning, WANG Xiao-miao*

(Faculty of Science, Ningbo University, Ningbo 315211, China)

Abstract: An optical orthogonal code belongs to a family of sequences with good auto- and cross-correlation properties, which is applied in an optical code-division multiple access (OCDMA) system. Some direct constructions of optimal and g -regular cyclic packing design are presented using the method of cyclotomic class. With the relationship between cyclic packing and variable-weight optical orthogonal code, the constructions of optimal variable-weight optical orthogonal codes with weight three and four are obtained. When $Q\in\{(1/3,2/3),(2/3,1/3),(1/2,1/2)\}$, several infinite classes of optimal $(v,\{3,4\},1,Q)$ -optical orthogonal codes are established.

Key words: packing design; optical orthogonal code; variable-weight; cyclotomic class; optimal

(责任编辑 史小丽)