

周期为合数长屏蔽二元互补序列偶构造方法研究

彭秀平^{1,2,3}, 郑德亮¹, 冀惠璞¹, 张桂茹⁴, 刘元慧⁵

(1. 燕山大学信息科学与工程学院, 河北秦皇岛 066004; 2. 河北省信息传输与信号处理重点实验室, 河北秦皇岛 066004; 3. 通信网信息传输与分发技术重点实验室, 河北石家庄 050081; 4. 河北建材职业技术学院, 河北秦皇岛 066004; 5. 燕山大学理学院, 河北秦皇岛 066004)

摘 要: 互补序列应用于多载波码分多址系统因理论上可同时消除多径干扰和多址干扰而备受关注. 基于中国剩余定理, 本文提出一种周期为合数长的屏蔽二元互补序列偶的构造方法. 构造得到的屏蔽二元互补序列偶可扩展互补序列的存在范围. 为了进一步研究屏蔽二元互补序列偶, 本文提出一种新的区组设计——屏蔽差族偶, 并将屏蔽差族偶与屏蔽二元互补序列偶建立了等价关系, 为应用屏蔽差族偶这一新的区组设计研究屏蔽二元互补序列偶提供了理论依据.

关键词: 多载波码分多址; 屏蔽序列; 屏蔽二元互补序列偶; 屏蔽差族偶

中图分类号: TN911.2 **文献标识码:** A **文章编号:** 0372-2112(2021)08-1466-08

电子学报 URL: <http://www.ejournal.org.cn> **DOI:** 10.12263/DZXB.20190456

Study on the Construction Method of Punctured Binary Complementary Sequence Pairs with Composite Length

PENG Xiu-ping^{1,2,3}, ZHENG De-liang¹, JI Hui-pu¹, ZHANG Gui-ru⁴, LIU Yuan-hui⁵

(1. School of Information Science and Engineering, Yanshan University, Qinhuangdao, Hebei 066004, China;

2. Hebei Province Key Laboratory of Information Transmission and Signal Processing, Qinhuangdao, Hebei 066004, China;

3. Key Laboratory of Communication Network Information Transmission and Distribution Technology, Shijiazhuang, Hebei 050081, China;

4. Hebei Construction Material Vocational and Technical College, Qinhuangdao, Hebei 066004, China;

5. School of Sciences, Yanshan University, Qinhuangdao, Hebei 066004, China)

Abstract: Complementary sequences (CSs) have attracted more attention in application of multicarrier code-division multiple-access (MC-CDMA) communication system since they are able to remove multipath interference (MPI) and multi-access interference (MAI). Based on Chinese remainder theorem, a construction method of punctured binary complementary sequence pairs (PBCSPs) with composite length has been proposed. This result can greatly extend the range of complementary sequence. To further study PBCSPs, we present a new block design—punctured difference family pair (PDFP), and establish the equivalent relationship between PDFP and PBCSPs, which provides a theoretical basis for the study of PBCSPs by using the new block design of PDFP.

Key words: MC-CDMA; punctured sequence; punctured binary complementary sequence pairs; punctured difference family pair

1 引言

多载波码分多址(MC-CDMA)扩频技术因其具有抗频率选择性衰落、抗符号间干扰、高频谱利用率、同时容纳的用户数量庞大和能实现软切换等特点正成为当前无线通信中具有竞争力的首选方案^[1]. 在各类

适用MC-CDMA通信系统的序列研究中,最受关注的是互补序列及其应用. 互补序列不同于单一序列(单一序列的相关性受到Welch界的限制,不可能在整个周期内同时具有理想的自相关和互相关性能),互补序列则通过各子序列的异相自相关和互相关的对消,

收稿日期:2019-04-25;修回日期:2020-11-25;责任编辑:孙瑶

基金项目:河北省高等学校青年拔尖人才计划(No.BJ2018018);河北省教育厅高等学校科技计划重点项目(No.ZD2019039);装备预研重点实验室基金(No.6142104190109)

可同时达到理想的自相关和互相关性能^[2]. 互补序列最早由 Golay 提出并在雷达中获得了广泛的应用,而传统二元互补序列数目相对较少,在周期长度 100 以内,非周期二元互补序列仅存在长度为 2、4、8、10、16、20、26、32、40、52、64、80 的 12 种情况^[3],周期二元互补序列仅存在长度为 2、4、8、10、16、20、26、32、34、40、50、52、58、64、68、72、74、80、82 的 19 种情况^[4,5],且到目前为止,周期二元互补序列未知的最小存在长度为 90^[4]. 近年来,为了获得更多能应用于通信系统中的互补序列,关于周期互补序列的研究主要分为两个方向,一是通过牺牲序列的相关性能,即不完全要求互补序列在整个周期上的相关函数值和为 0,提出了如 ZCZ 互补序列^[6]、准互补序列^[7]、零相关区互补序列集^[8]等;二是按通信系统的发送端和接收端可以采用不同序列的指导思想,提出了周期互补序列偶^[9]、周期屏蔽互补序列偶^[10,11]、零相关区互补序列偶集^[12]等.

屏蔽序列偶 (x, y) 在序列 x 基础上通过将某些位元素设为 0 得到屏蔽序列 y ,屏蔽序列偶信号的提出,大大地扩展了最佳序列(偶)的存在空间,有关它的研究引起了国内外学者的广泛关注^[13,14]. 为了给 MC-CDMA 提供更多的互补序列,文献[10]将屏蔽序列偶的概念引入互补序列的研究中,提出了周期屏蔽二元互补序列偶,而这些研究仅停留在周期屏蔽二元互补序列偶概念的提出、性质的研究及如何利用循环相关信号性质来构造互补序列偶上,导致目前得到的周期屏蔽二元互补序列偶数量很少. 本文将对周期屏蔽二元互补序列偶的构造方法做进一步研究,提出利用中国剩余定理来构造周期屏蔽二元互补序列偶的新思想,相比于将已有序列进行逆序和取反变换进行构造的方法^[10],能够简单地产生出更多的屏蔽互补序列偶,进而扩大了周期互补序列偶的存在空间;此外,基于差集偶^[15]和屏蔽差集偶^[14,16]提出了屏蔽差族偶的概念,并将屏蔽差族偶同周期屏蔽二元互补序列偶建立了等价关系,可以为周期互补序列偶的研究提供更多的数学工具.

2 屏蔽二元互补序列偶

定义 1^[9] 设 $a = (a(0), a(1), \dots, a(N-1))$ 和 $b = (b(0), b(1), \dots, b(N-1))$ 均为 N 长的二元序列,将序列 a 和 b 的互相关函数定义为序列偶 (a, b) 周期自相关函数,具体定义为

$$R_{(a,b)}(\tau) = \sum_{j=0}^{N-1} a(j)b(j+\tau) = \begin{cases} F(\neq 0), & \tau = 0 \\ \gamma, & \tau \neq 0 \end{cases} \quad (1)$$

其中 $0 \leq \tau \leq N-1, j+\tau = (j+\tau) \bmod N, a(j), b(j) \in$

$\{1, -1\}$. 当 $\tau = 0$ 时, F 称为自相关函数的峰值;当 $\tau \neq 0$ 时, γ 称为旁瓣值. 当 $a = b$ 时,退化为序列 a 的自相关函数 $R_a(\tau)$.

定义 2^[9] 设 $\{(a_i, b_i), 0 \leq i \leq Q-1\}$ 是 Q 对 N 长二元序列偶的集合,如果它们的自相关函数和满足:

$$\sum_{i=0}^{Q-1} R_{(a_i, b_i)}(\tau) = \begin{cases} C, & \tau = 0 \\ 0, & \tau \neq 0 \end{cases} \quad (2)$$

其中 C 为一个非零常数,则称 $\{(a_i, b_i), 0 \leq i \leq Q-1\}$ 为周期二元互补序列偶. 当 $Q = 2$ 时,称为二对二元互补序列偶或二元互补序列偶对;当 $Q \geq 3$ 时,称为多对二元互补序列偶. 当 $a_i = b_i (0 \leq i \leq Q-1)$ 时,周期二元互补序列偶退化为周期二元互补序列.

定义 3^[11] 设序列 x_i 的 m -屏蔽序列 y_i 为

$$y_i(j) = \begin{cases} 0, & j \in P_i \\ x_i(j), & j \notin P_i \end{cases} \quad (3)$$

其中 P_i 为序列 x_i 的屏蔽位置集合且 $|P_i| = m$. 如果 $x_i(j) \in \{1, -1\}$,那么 $y_i(j) \in \{-1, 0, 1\}$,则称 (x_i, y_i) 为屏蔽二元序列偶.

定义 4 若 $\{(x_i, y_i), 0 \leq i \leq Q-1\}$ 是 Q 对 N 长屏蔽二元序列偶,如果它们的周期自相关函数和满足:

$$\sum_{i=0}^{Q-1} R_{(x_i, y_i)}(\tau) = \begin{cases} E, & \tau = 0 \\ 0, & \tau \neq 0 \end{cases} \quad (4)$$

其中 E 为一个非零常数,则称 $\{(x_i, y_i), 0 \leq i \leq Q-1\}$ 为屏蔽二元互补序列偶.

3 屏蔽差族偶和屏蔽二元互补序列偶

定义 5^[17] 设集合 U_i 为整数环 $Z_N = \{0, 1, \dots, N-1\}$ 上的子集,二元序列 x_i 等价对应于集合 U_i ,即

$$x_i(j) = \begin{cases} 1, & j \in U_i \\ -1, & j \notin U_i \end{cases} \quad (5)$$

其中 $0 \leq j \leq N-1$,则称集合 U_i 为序列 x_i 的特征集,序列 x_i 为集合 U_i 的特征序列.

定义 6 设 N, λ 为正整数,集合 $U, P, K, K', E, U', W, W'$ 均为整数环 Z_N 上的子集, $Z_N^* = Z_N \setminus \{0\}$ 为 Z_N 中的非零元素集合. 设 $U = \{U_0, U_1, \dots, U_{Q-1}\}, P = \{P_0, P_1, \dots, P_{Q-1}\}$, 其中 $U_i = \{u_{i,0}, u_{i,1}, \dots, u_{i,k_i-1}\}, P_i = \{p_{i,0}, p_{i,1}, \dots, p_{i,k'_i-1}\}$ 分别表示有 k_i 和 k'_i 个元素的集合. 设 $K = \{k_0, k_1, \dots, k_{Q-1}\}, K' = \{k'_0, k'_1, \dots, k'_{Q-1}\}, E = \{e_0, e_1, \dots, e_{Q-1}\}$, 其中 $k_i = |U_i| \neq 0, k'_i = |P_i| \neq 0, e_i = |U_i \cap P_i|$ 分别是集合 U_i, P_i 和 $U_i \cap P_i$ 的元素个数. 再设 $U' = \{U'_0, U'_1, \dots, U'_{Q-1}\}, W = \{W_0, W_1, \dots, W_{Q-1}\}, W' = \{W'_0, W'_1, \dots, W'_{Q-1}\}$, 其中 $U'_i = U_i - U_i \cap P_i = \{u'_{i,0}, u'_{i,1}, \dots, u'_{i,(k_i-e_i)-1}\}, W_i = \overline{U}_i = \{w_{i,0}, w_{i,1}, \dots, w_{i,(N-k_i)-1}\}, W'_i = W_i - W_i \cap P_i = \{w'_{i,0}, w'_{i,1}, \dots, w'_{i,(N+e_i-k_i-k'_i)-1}\}, 0 \leq i \leq Q-1$. 若对于非零元 $r \in Z_N^*$ 在

差表式(6)中恰好出现 λ 次,则称 (U, P) 为 Z_N 上的 (N, K, K', E, λ) 屏蔽差族偶. 当 $Q = 1$ 时,屏蔽差族偶

$$\bigcup_{i=0}^{Q-1} \left\{ \{(u_{i,m} - u'_{i,n}) \pmod N : u_{i,m} \in U_i, u'_{i,n} \in U'_i, u_{i,m} \neq u'_{i,n}, 0 \leq m \leq k_i - 1, 0 \leq n \leq (k_i - e_i) - 1\} \right. \\ \left. \cup \{(w_{i,l} - w'_{i,v}) \pmod N : w_{i,l} \in W_i, w'_{i,v} \in W'_i, w_{i,l} \neq w'_{i,v}, 0 \leq l \leq (N - k_i) - 1, 0 \leq v \leq (N + e_i - k_i - k'_i) - 1\} \right\} \quad (6)$$

定理 1 设集合 U 和 P 是 Z_N 上的子集, $x_i(0 \leq i \leq Q - 1)$ 为二元序列,序列 y_i 为 x_i 的屏蔽序列,令 U_i 为 x_i 的特征集, P_i 为 x_i 的屏蔽位置集合,则 $\{(x_i, y_i), 0 \leq i \leq Q - 1\}$ 为屏蔽二元互补序列偶的充要条件是 (U, P) 为 Z_N 上参数满足 $QN - (\sum_{i=0}^{Q-1} k'_i + 2\lambda) = 0$ 的 (N, K, K', E, λ) 屏蔽差族偶.

证明 充分性:若 $\{(x_i, y_i), 0 \leq i \leq Q - 1\}$ 为屏蔽二元互补序列偶,基于定义5和定义6可知

$$x_i(j) = \begin{cases} 1, & j \in U_i \\ -1, & j \notin U_i \end{cases} = \begin{cases} 1, & j \in U_i \\ -1, & j \in W_i \end{cases} \\ y_i(j) = \begin{cases} 0, & j \in P_i \\ x_i(j), & j \notin P_i \end{cases} = \begin{cases} 1, & j \in U'_i \\ -1, & j \in W'_i \\ 0, & j \in P_i \end{cases}$$

那么有

$$R_{(x_i, y_i)}(\tau) = \sum_{j=0}^{N-1} x_i(j) y_i(j + \tau) \\ = \sum_{\substack{j \in U_i \\ j + \tau \in U'_i}} 1 - \sum_{\substack{j \in U_i \\ j + \tau \in W'_i}} 1 - \sum_{\substack{j \in W_i \\ j + \tau \in U'_i}} 1 + \sum_{\substack{j \in W_i \\ j + \tau \in W'_i}} 1$$

当 $\tau = 0$ 时,

$$R_{(x_i, y_i)}(0) = \sum_{\substack{j \in U_i \\ j + \tau \in U'_i}} 1 - \sum_{\substack{j \in U_i \\ j + \tau \in W'_i}} 1 - \sum_{\substack{j \in W_i \\ j + \tau \in U'_i}} 1 + \sum_{\substack{j \in W_i \\ j + \tau \in W'_i}} 1 \\ = k_i - e_i + N - k_i - k'_i + e_i \\ = N - k'_i$$

当 $\tau \neq 0$ 时, λ_i 表示序列偶 (x_i, y_i) 时非零元 r 在差表式(6)中出现的次数,则有

$$R_{(x_i, y_i)}(\tau) = |(U_i + \tau) \cap U'_i| + |(W_i + \tau) \cap W'_i| \\ - |(U_i + \tau) \cap W'_i| - |(W_i + \tau) \cap U'_i| \\ = \lambda_i - |(Z_N - W_i + \tau) \cap W'_i| \\ - |(Z_N - U_i + \tau) \cap U'_i| \\ = \lambda_i - (|W'_i| + |U'_i| - \lambda_i) \\ = 2\lambda_i - (N - k_i - k'_i + e_i + k_i - e_i) \\ = 2\lambda_i - N + k'_i$$

可得到 $\sum_{i=0}^{Q-1} R_{(x_i, y_i)}(\tau) = 2\lambda - QN + \sum_{i=0}^{Q-1} k'_i$, 所以有 $QN -$

$(\sum_{i=0}^{Q-1} k'_i + 2\lambda) = 0$, 则对于每个非零元 $r \in Z_N^*$ 在差表式

(6)中都出现 $\lambda = (QN - \sum_{i=0}^{Q-1} k'_i)/2$ 次,所以 (U, P) 为 Z_N 上

(U, P) 退化屏蔽差集偶.

的 (N, K, K', E, λ) 屏蔽差族偶.

必要性:如果 (U, P) 为 Z_N 上参数满足 $QN - (\sum_{i=0}^{Q-1} k'_i + 2\lambda) = 0$ 的 (N, K, K', E, λ) 屏蔽差族偶,则对于

每个非零元 r 在差表式(6)中都有 $\lambda = (QN - \sum_{i=0}^{Q-1} k'_i)/2$ 个

解,即 $QN - \sum_{i=0}^{Q-1} k'_i \uparrow \sum_{j=0}^{Q-1} x_i(j) y_i(j + \tau)$ 中“+1”和“-1”元

素个数相等,所以有 $\sum_{i=0}^{Q-1} \sum_{j=0}^{N-1} x_i(j) y_i(j + \tau) = 0$,由定义4

知, $\{(x_i, y_i), 0 \leq i \leq Q - 1\}$ 为屏蔽二元互补序列偶.

综上可得,屏蔽二元互补序列偶对应着参数满足一定条件的屏蔽差族偶,反之,满足一定条件的 (N, K, K', E, λ) 屏蔽差族偶对应着屏蔽二元互补序列偶,所以两者存在等价关系.

4 合数长屏蔽二元互补序列偶构造方法

本节将给出合数长 $N = np$ 的屏蔽二元互补序列偶的构造方法,其中 n 为奇素数且 $\gcd(n, p) = 1$. 首先给出一般构造法,然后再根据 $n = 4m + 3$ 和 $n = 4m + 1$ 两种不同情况进行讨论.

构造法 设 $\{s_i(k) | 0 \leq i \leq Q - 1, 0 \leq k \leq p - 1\}$ 为 Q 条 p 长的周期二元互补序列,定义矩阵 $A_i = (a_{h,k})_i$ 和 $B_i = (b_{h,k})_i$ 如下:

$$A_i = \begin{pmatrix} a_{0,0} & a_{0,1} & \cdots & a_{0,p-1} \\ a_{1,0} & a_{1,1} & \cdots & a_{1,p-1} \\ \vdots & \vdots & \cdots & \vdots \\ a_{n-1,0} & a_{n-1,1} & \cdots & a_{n-1,p-1} \end{pmatrix}_i \\ B_i = \begin{pmatrix} b_{0,0} & b_{0,1} & \cdots & b_{0,p-1} \\ b_{1,0} & b_{1,1} & \cdots & b_{1,p-1} \\ \vdots & \vdots & \cdots & \vdots \\ b_{n-1,0} & b_{n-1,1} & \cdots & b_{n-1,p-1} \end{pmatrix}_i$$

其中 $0 \leq h \leq n - 1, 0 \leq k \leq p - 1, (a_{h,k})_i$ 和 $(b_{h,k})_i$ 将根据不同情况由序列 $s_i(k)$ 决定. 令 $x_i = (x_i(0), x_i(1), \dots, x_i(np - 1))$ 和 $y_i = (y_i(0), y_i(1), \dots, y_i(np - 1))$ 均为 $N = np$ 长的二元序列且其元素定义为

$$x_i(j) = (a_{h,k})_i \\ y_i(j) = (b_{h,k})_i$$

其中,

$$\begin{cases} j \equiv h \pmod{n} \\ j \equiv k \pmod{p} \end{cases}$$

接下来将给出两种基于构造法得到 $N = np$ 长屏蔽二元互补序列偶的方法,在下文中, $(0)_p$ 表示一个周期为 p 的全 0 序列, 0_p 表示同时出现 p 个 0 元素, $\bar{s}(t) = -s(t)$ 表示对序列 s 的每个元素取反. 在下文的定理证明中需要用到分圆类的部分内容,下面对其作简要说明.

定义 7^[18] 设 $n = ef + 1$ 为奇素数幂, $\text{GF}(n)$ 为 n 阶有限域. 设 θ 为 $\text{GF}(n)$ 的本原元, $\varepsilon = \theta^e$, 令

$$D_i^{(e,n)} = \{\theta^i, \theta^i \varepsilon, \theta^i \varepsilon^2, \dots, \theta^i \varepsilon^{f-1}\}, \quad 0 \leq i \leq e - 1$$

则称 $D_i^{(e,n)}$ 为 e 阶分圆类.

定义 8^[18] 设 $n = ef + 1$ 为奇素数幂, 对 $0 \leq l, m \leq e - 1$, 令

$$(l, m)_e = |\{(x, y) | x \in D_l^{(e,n)}, y \in D_m^{(e,n)}, x + 1 = y\}|$$

称 $(l, m)_e$ 为基于 $\text{GF}(n)$ 的 e 阶分圆数.

引理 1^[18] 当 $e = 2$ 时有

当 $n \equiv 1 \pmod{4}$ 时, 有

$$(0, 0)_2 = (n - 5)/4$$

$$(0, 1)_2 = (1, 0)_2 = (1, 1)_2 = (n - 1)/4$$

当 $n \equiv 3 \pmod{4}$ 时, 有

$$(0, 1)_2 = (n + 1)/4$$

$$(0, 0)_2 = (1, 0)_2 = (1, 1)_2 = (n - 3)/4$$

定理 2 令 $n = 4m + 3$ 为奇素数, 设 $\{s_i(k) | 0 \leq i \leq Q - 1, 0 \leq k \leq p - 1\}$ 为 Q 条 p 长的二元互补序列. 按照构造法定义矩阵 $\mathbf{A}_i, \mathbf{B}_i$, 其中 $(a_{h,k})_i$ 和 $(b_{h,k})_i$ 定义为

$$(a_{h,k})_i = \begin{cases} s_i(k), & h = 0 \\ s_i(k), & h \in D_0^{(2,n)} \\ \bar{s}_i(k), & h \in D_1^{(2,n)} \end{cases}$$

$$(b_{h,k})_i = \begin{cases} s_i(k), & h = 0 \\ s_i(k), & h \in D_0^{(2,n)} \\ (0)_p, & h \in D_1^{(2,n)} \end{cases}$$

则由构造法得到的 $\{(x_i, y_i), 0 \leq i \leq Q - 1\}$ 为 $N = np$ 长的屏蔽二元互补序列偶且其相关函数值满足:

$$\sum_{i=0}^{Q-1} R_{(x_i, y_i)}(\tau) = \begin{cases} \frac{n+1}{2} Qp, & \tau = 0 \\ 0, & \text{其他} \end{cases} \quad (7)$$

证明 当 $h = 0$ 和 $h \in D_0^{(2,n)}$ 时, $(a_{h,k})_i$ 和 $(b_{h,k})_i$ 的取值相同, 仅当 $h \in D_1^{(2,n)}$ 时, $(a_{h,k})_i$ 取值为 $\bar{s}_i(k)$, $(b_{h,k})_i$ 取值为 $(0)_p$. 由定义 3 可知, $((a_{h,k})_i, (b_{h,k})_i)$ 为屏蔽二元序列偶. 由于 $\text{gcd}(n, p) = 1$, 根据中国剩余定理^[19] 有 $Z_{np} \cong Z_n \times Z_p$, 对任意的 $\tau = (\tau_1, \tau_2)$, 序列偶 (x_i, y_i) 的相关函数可以写为

$$R_{(x_i, y_i)}(\tau) = \sum_{j=0}^{np-1} x_i(j) y_i(j + \tau) = \sum_{h=0}^{n-1} \sum_{k=0}^{p-1} (a_{h,k})_i (b_{h+\tau_1, k+\tau_2})_i$$

则 $\{(x_i, y_i), 0 \leq i \leq Q - 1\}$ 的相关函数值可通过以下四种情况讨论.

(1) 当 $\tau_1 \equiv 0 \pmod{n}$ 且 $\tau_2 \equiv 0 \pmod{p}$ 时, 有

$$R_{(x_i, y_i)}(\tau) = R_{s_i, s_i}(0) + \frac{n-1}{2} R_{s_i, s_i}(0) + \frac{n-1}{2} R_{\bar{s}_i, (0)_p}(0) = \frac{n+1}{2} R_{s_i, s_i}(0) = \frac{n+1}{2} p$$

$$\sum_{i=0}^{Q-1} R_{(x_i, y_i)}(\tau) = \sum_{i=0}^{Q-1} \frac{n+1}{2} p = \frac{n+1}{2} Qp$$

(2) 当 $\tau_1 \equiv 0 \pmod{n}$ 且 $\tau_2 \not\equiv 0 \pmod{p}$ 时, 由 $s_i(k)$ 可得 $\sum_{i=0}^{Q-1} R_{s_i, s_i}(\tau \neq 0) = 0$, 则

$$R_{(x_i, y_i)}(\tau) = R_{s_i, s_i}(\tau_2) + \frac{n-1}{2} R_{s_i, s_i}(\tau_2) + \frac{n-1}{2} R_{\bar{s}_i, (0)_p}(\tau_2) = \frac{n+1}{2} R_{s_i, s_i}(\tau_2)$$

$$\sum_{i=0}^{Q-1} R_{(x_i, y_i)}(\tau) = \sum_{i=0}^{Q-1} \frac{n+1}{2} R_{s_i, s_i}(\tau_2) = 0$$

(3) 当 $\tau_1 \in D_0^{(2,n)}$ 时,

$$R_{(x_i, y_i)}(\tau) = \sum_{k=0}^{p-1} (a_{0,k})_i (b_{\tau_1, k+\tau_2})_i + \sum_{k=0}^{p-1} (a_{-\tau_1, k})_i (b_{0, k+\tau_2})_i + \left(\sum_{\substack{h \in D_0^{(2,n)} \\ h + \tau_1 \in D_0^{(2,n)}}} + \sum_{\substack{h \in D_0^{(2,n)} \\ h + \tau_1 \in D_1^{(2,n)}}} + \sum_{\substack{h \in D_1^{(2,n)} \\ h + \tau_1 \in D_0^{(2,n)}}} + \sum_{\substack{h \in D_1^{(2,n)} \\ h + \tau_1 \in D_1^{(2,n)}}} \right) \times \sum_{k=0}^{p-1} (a_{h,k})_i (b_{h+\tau_1, k+\tau_2})_i$$

当 $n \equiv 3 \pmod{4}$ 时, $-1 \in D_1^{(2,n)}$, 则 $-\tau_1 \in D_1^{(2,n)}$,

$$R_{(x_i, y_i)}(\tau) = R_{s_i, s_i}(\tau_2) + R_{\bar{s}_i, s_i}(\tau_2) + (0, 0)_2 R_{s_i, s_i}(\tau_2) + (0, 1)_2 R_{s_i, (0)_p}(\tau_2) + (1, 0)_2 R_{\bar{s}_i, s_i}(\tau_2) + (1, 1)_2 R_{\bar{s}_i, (0)_p}(\tau_2)$$

当 $\tau_2 = 0$ 时, $R_{(x_i, y_i)}(\tau) = (0, 0)_2 p - (1, 0)_2 p$, 由引理

1 得 $R_{(x_i, y_i)}(\tau) = 0$, 则 $\sum_{i=0}^{Q-1} R_{(x_i, y_i)}(\tau) = 0$.

当 $\tau_2 \neq 0$ 时,

$$R_{(x_i, y_i)}(\tau) = (0, 0)_2 R_{s_i, s_i}(\tau_2) - (1, 0)_2 \cdot R_{s_i, s_i}(\tau_2) = 0$$

则 $\sum_{i=0}^{Q-1} R_{(x_i, y_i)}(\tau) = 0$.

(4) 当 $\tau_1 \in D_1^{(2,n)}$ 时,

$$R_{(x_i, y_i)}(\tau) = R_{s_i, 0}(\tau_2) + R_{s_i, s_i}(\tau_2) + (1, 1)_2 R_{s_i, s_i}(\tau_2) + (1, 0)_2 R_{s_i, 0}(\tau_2) + (0, 1)_2 R_{\bar{s}_i, s_i}(\tau_2) + (0, 0)_2 R_{\bar{s}_i, 0}(\tau_2)$$

当 $\tau_2 = 0$ 时,

$$R_{(x_i, y_i)}(\tau) = p + (1, 1)_2 p - (0, 1)_2 p$$

由引理 1 得 $R_{(x_i, y_i)}(\tau) = 0$, 则 $\sum_{i=0}^{Q-1} R_{(x_i, y_i)}(\tau) = 0$.

当 $\tau_2 \neq 0$ 时,

$$R_{(x_i, y_i)}(\tau) = R_{s_i, s_i}(\tau_2) + (1, 1)_2 R_{s_i, s_i}(\tau_2) - (0, 1)_2 R_{s_i, s_i}(\tau_2) = 0$$

则有 $\sum_{i=0}^{Q-1} R_{(x_i, y_i)}(\tau) = 0$.

综合上述四种情况, 可得式(7), 则由构造法和定理 2 得到的 $\{(x_i, y_i), 0 \leq i \leq Q-1\}$ 为屏蔽二元互补序列偶.

例 1 设 $\begin{pmatrix} s_0(k) \\ s_1(k) \end{pmatrix} = \begin{pmatrix} 1, 1, 1, -1, 1, 1, -1, 1 \\ 1, 1, 1, -1, -1, -1, 1, -1 \end{pmatrix}, n =$

3, 得到两对 $N = 24$ 长二元序列偶为

$$\begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \begin{pmatrix} 1, 1, -1, -1, 1, -1, -1, 1, -1, 1, 1, 1, 1, \\ 1, 1, 1, 1, -1, 1, -1, -1, 1, -1, -1, \\ 1, 1, 0, -1, 1, 0, -1, 1, 0, 1, 1, 0, 1, \\ 1, 0, 1, 1, 0, 1, -1, 0, 1, -1, 0 \end{pmatrix}$$

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = \begin{pmatrix} 1, 1, -1, -1, -1, 1, 1, -1, -1, 1, 1, 1, -1, \\ -1, -1, -1, 1, -1, 1, -1, 1, -1, 1, 1, \\ 1, 1, 0, -1, -1, 0, 1, -1, 0, 1, 1, 0, -1, \\ -1, 0, -1, 1, 0, 1, -1, 0, -1, 1, 0 \end{pmatrix}$$

由定义 3 知序列 y_i 是 x_i 的屏蔽序列, 序列偶 (x_i, y_i) 相关函数值为

$$R_{(x_0, y_0)}(\tau) = \{16, 0_2, 8, 0_{17}, 8, 0_2\}$$

$$R_{(x_1, y_1)}(\tau) = \{16, 0_2, -8, 0_{17}, -8, 0_2\}$$

$\sum_{i=0}^1 R_{(x_i, y_i)}(\tau) = \{32, 0_{23}\}$, 所以 $\{(x_0, y_0), (x_1, y_1)\}$ 为屏蔽二元互补序列偶对.

根据定义 5 和定义 6 有

$$P_0 = P_1 = \{2, 5, 8, 11, 14, 17, 20, 23\}$$

$$U_0 = \{0, 1, 4, 7, 9, 10, 11, 12, 13, 14, 15, 16, 18, 21\}$$

$$U'_0 = \{0, 1, 4, 7, 9, 10, 12, 13, 15, 16, 18, 21\}$$

$$U_1 = \{0, 1, 5, 6, 9, 10, 11, 16, 18, 20, 22, 23\}$$

$$U'_1 = \{0, 1, 6, 9, 10, 16, 18, 22\}$$

$$W_0 = \{2, 3, 5, 6, 8, 17, 19, 20, 22, 23\}$$

$$W'_0 = \{3, 6, 19, 22\}$$

$$W_1 = \{2, 3, 4, 7, 8, 12, 13, 14, 15, 17, 19, 21\}$$

$$W'_1 = \{3, 4, 7, 12, 13, 15, 19, 21\}$$

每个非零元 $r \in Z_{24}^*$ 在差表式(6)中出现的次数如表 1 所示, 每个非零元 $r \in Z_{24}^*$ 均出现了 16 次, 即 $\lambda = 16$, 所以得到 (U, P) 为 $(24, \{14, 12\}, \{8, 8\}, \{2, 4\}, 16)$ 的屏蔽差族偶.

表 1 $r \in Z_{24}^*$ 在差表中出现的次数

$r \in Z_{24}^*$	$\{u_{0,m} - u'_{0,n} : u_{0,m} \in U_0, u'_{0,n} \in U'_0, u_{0,m} \neq u'_{0,n}, 0 \leq m \leq 13, 0 \leq n \leq 11\}$	$\{w_{0,l} - w'_{0,v} : w_{0,l} \in W_0, w'_{0,v} \in W'_0, w_{0,l} \neq w'_{0,v}, 0 \leq l \leq 9, 0 \leq v \leq 3\}$	$\{u_{1,m} - u'_{1,n} : u_{1,m} \in U_1, u'_{1,n} \in U'_1, u_{1,m} \neq u'_{1,n}, 0 \leq m \leq 11, 0 \leq n \leq 7\}$	$\{w_{1,l} - w'_{1,v} : w_{1,l} \in W_1, w'_{1,v} \in W'_1, w_{1,l} \neq w'_{1,v}, 0 \leq l \leq 11, 0 \leq v \leq 7\}$
$\{1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23\}$	6	2	4	4
$\{3, 21\}$	10	2	2	2
$\{6, 9, 12, 15, 18\}$	8	0	4	4

定理 3 令 $n = 4m + 1$ 为奇素数, $\{s_i(k) | 0 \leq i \leq Q-1, 0 \leq k \leq p-1\}$ 为 Q 条 p 长的周期二元互补序列. 按照构造法定义矩阵 A_i 和 B_i , 其中 $(a_{h,k})_i$ 和 $(b_{h,k})_i$ 定义为

$$(a_{h,k})_i = \begin{cases} s_i(k), & h = 0 \\ s_i(k), & h \in D_0^{(2,n)} \\ \bar{s}_i(k), & h \in D_1^{(2,n)} \end{cases}$$

$$(b_{h,k})_i = \begin{cases} (0)_p, & h = 0 \\ s_i(k), & h \in D_0^{(2,n)} \\ (0)_p, & h \in D_1^{(2,n)} \end{cases}$$

则由构造法得到的 $\{(x_i, y_i), 0 \leq i \leq Q-1\}$ 为 $N = np$ 长的屏蔽二元互补序列偶且其相关函数值满足:

$$\sum_{i=0}^{Q-1} R_{(x_i, y_i)}(\tau) = \begin{cases} \frac{n-1}{2} Qp, & \tau = 0 \\ 0, & \text{其他} \end{cases} \quad (8)$$

证明 同定理 2 的证明类似, 可知 $((a_{h,k})_i, (b_{h,k})_i)$ 为屏蔽二元序列偶. 对任意的 $\tau = (\tau_1, \tau_2), \{(x_i, y_i), 0 \leq i \leq Q-1\}$ 的相关函数值可通过以下四种情况进行讨论.

(1) 当 $\tau_1 = 0 \pmod n$ 且 $\tau_2 = 0 \pmod p$ 时,

$$\sum_{i=0}^{Q-1} R_{(x_i, y_i)}(\tau) = \sum_{i=0}^{Q-1} \left[R_{s_i, (0)_p}(0) + \frac{n-1}{2} R_{s_i, s_i}(0) + \frac{n-1}{2} R_{\bar{s}_i, (0)_p}(0) \right] = \frac{n-1}{2} Qp$$

(2) 当 $\tau_1 = 0 \pmod n$ 且 $\tau_2 \neq 0 \pmod p$ 时,

$$\sum_{i=0}^{Q-1} R_{(x_i, y_i)}(\tau) = \sum_{i=0}^{Q-1} \left[R_{s_i, (0)_p}(\tau_2) + \frac{n-1}{2} R_{s_i, s_i}(\tau_2) + \frac{n-1}{2} R_{\bar{s}_i, (0)_p}(\tau_2) \right] = 0$$

(3) 当 $\tau_1 \in D_0^{(2, n)}$ 时, 由于 $n \equiv 1 \pmod{4}$ 时, 有 $-1 \in D_0^{(2, n)}$, 则 $-\tau_1 \in D_0^{(2, n)}$, 可得

$$R_{(x_i, y_i)}(\tau) = R_{s_i, s_i}(\tau_2) + R_{s_i, (0)_p}(\tau_2) + (0, 0)_2 R_{s_i, s_i}(\tau_2) + (0, 1)_2 R_{s_i, (0)_p}(\tau_2) + (1, 0)_2 R_{\bar{s}_i, s_i}(\tau_2) + (1, 1)_2 R_{\bar{s}_i, (0)_p}(\tau_2)$$

当 $\tau_2 = 0$ 和 $\tau_2 \neq 0$ 时, 均有 $\sum_{i=0}^{Q-1} R_{(x_i, y_i)}(\tau) = 0$.

(4) 当 $\tau_1 \in D_1^{(2, n)}$ 时,

$$R_{(x_i, y_i)}(\tau) = R_{s_i, (0)_p}(\tau_2) + R_{\bar{s}_i, (0)_p}(\tau_2) + (1, 1)_2 R_{s_i, s_i}(\tau_2) + (1, 0)_2 R_{s_i, (0)_p}(\tau_2) + (0, 1)_2 R_{\bar{s}_i, s_i}(\tau_2) + (0, 0)_2 R_{\bar{s}_i, (0)_p}(\tau_2)$$

当 $\tau_2 = 0$ 和 $\tau_2 \neq 0$ 时, 均有 $\sum_{i=0}^{Q-1} R_{(x_i, y_i)}(\tau) = 0$.

综合上述四种情况, 可得式(8), 则通过构造法和定理3得到的 $\{(x_i, y_i), 0 \leq i \leq Q-1\}$ 为屏蔽二元互补序列偶.

例 2 设
$$\begin{pmatrix} s_0(k) \\ s_1(k) \\ s_2(k) \\ s_3(k) \end{pmatrix} = \begin{pmatrix} -1, 1, 1, 1, 1, 1, 1 \\ -1, -1, -1, 1, 1, 1, 1 \\ -1, -1, 1, 1, -1, 1, 1 \\ -1, 1, -1, 1, -1, 1, 1 \end{pmatrix}, n = 5,$$

得到四对 $N = 35$ 长二元序列偶

$$\begin{pmatrix} x_0 \\ y_0 \end{pmatrix} = \begin{pmatrix} -1, 1, -1, -1, 1, 1, 1, 1, -1, 1, 1, 1, -1, -1, -1, 1, 1 \\ -1, -1, 1, 1, -1, -1, -1, 1, 1, 1, -1, 1, 1, 1, -1, -1, 1 \\ 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, -1, 0, 1 \\ 0, 0, 1, 0, -1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1 \end{pmatrix}$$

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = \begin{pmatrix} -1, -1, 1, -1, 1, 1, 1, 1, 1, -1, 1, 1, -1, -1, -1, -1, -1 \\ -1, -1, 1, 1, -1, 1, 1, 1, 1, -1, 1, -1, -1, 1, -1, -1, 1 \\ 0, -1, 0, 0, 1, 0, 1, 0, 0, -1, 0, 1, 0, 0, -1, 0, -1 \\ 0, 0, 1, 0, -1, 0, 0, 1, 0, 1, 0, 0, -1, 0, 1, 0, 0, 1 \end{pmatrix}$$

$$\begin{pmatrix} x_2 \\ y_2 \end{pmatrix} = \begin{pmatrix} -1, -1, -1, -1, -1, 1, 1, 1, 1, 1, 1, -1, -1, -1, -1, -1, 1 \\ -1, 1, 1, 1, -1, 1, -1, 1, -1, 1, -1, 1, -1, 1, 1, -1, 1 \\ 0, -1, 0, 0, -1, 0, 1, 0, 0, 1, 0, -1, 0, 0, -1, 0, 1 \\ 0, 0, 1, 0, -1, 0, 0, 1, 0, 1, 0, 0, -1, 0, 1, 0, 0, 1 \end{pmatrix}$$

$$\begin{pmatrix} x_3 \\ y_3 \end{pmatrix} = \begin{pmatrix} -1, 1, 1, -1, -1, 1, 1, 1, -1, -1, 1, -1, -1, -1, -1, 1, -1 \\ -1, 1, 1, 1, -1, -1, 1, 1, -1, 1, -1, 1, 1, -1, 1, 1, -1, 1 \\ 0, 1, 0, 0, -1, 0, 1, 0, 0, -1, 0, -1, 0, 0, -1, 0, -1 \\ 0, 0, 1, 0, -1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1 \end{pmatrix}$$

由定义3可知序列 y_i 是 x_i 的屏蔽序列, 序列偶 (x_i, y_i) 相关函数为

$$\begin{aligned} R_{(x_0, y_0)}(\tau) &= \{14, 0_4, 6, 0_4, 6, 0_4, 6, 0_4, 6, 0_4, 6, 0_4, 6, 0_4\} \\ R_{(x_1, y_1)}(\tau) &= \{14, 0_4, -2, 0_4, -10, 0_4, 6, 0_4, 6, 0_4, -10, 0_4, -2, 0_4\} \\ R_{(x_2, y_2)}(\tau) &= \{14, 0_4, -10, 0_4, 6, 0_4, -2, 0_4, -2, 0_4, 6, 0_4, -10, 0_4\} \\ R_{(x_3, y_3)}(\tau) &= \{14, 0_4, 6, 0_4, -2, 0_4, -10, 0_4, -10, 0_4, -2, 0_4, 6, 0_4\} \end{aligned}$$

$\sum_{i=0}^3 R_{(x_i, y_i)}(\tau) = \{56, 0_{34}\}$, 所以 $\{(x_i, y_i), 0 \leq i \leq 3\}$ 为四对屏蔽二元互补序列偶. 由定义6, 定理1, 定理3可得参数为 $(35, \{20, 18, 17, 18\}, \{21, 21, 21, 21\}, \{8, 10, 9, 10\}, 28)$ 的屏蔽差族偶.

5 结论

本文基于中国剩余定理, 利用已有的周期二元互补序列, 对周期为 $N = np$ 屏蔽二元互补序列偶的构造方法

进行了研究, 其中 n 为奇素数且 $\gcd(n, p) = 1$. 表2列出了100以内目前已有的周期二元互补序列对 ($Q = 2$) 存在情况以及基于这些二元互补序列对采用本文方法可得到的周期屏蔽二元互补序列偶对在100以内的对比情况. 在周期长度100以内, 通过表2可知, 已有的周期二元互补序列对有19种, 而通过本文的构造法结合已有的周期二元互补序列对, 基于定理2可以得到22种不同长度的周期屏蔽二元互补序列偶对, 由定理3可以得到12种长度的屏蔽二元互补序列偶对, 基于本文

构造方法可以新得到22种长度的屏蔽二元互补序列偶对,扩大了二元互补序列的存在范围,可为MC-CDMA系统提供更多的可用互补序列.此外,提出了屏蔽差族偶的概念,并将屏蔽差族偶同屏蔽二元互补序列偶建立了等价关系,为应用屏蔽差族偶这种新的区组设计方法研究屏蔽二元互补序列偶提供了新的理论依据.

表2 已有周期二元互补序列对长度与本文可得二元互补序列偶对长度对比(100以内)

PCS ^[4]	2, 4, 8, 10, 16, 20, 26, 32, 34, 40, 50, 52, 58, 64, 68, 72, 74, 80, 82
定理2	6, 12, 14, 22, 24, 28, 30, 38, 44, 46, 48, 56, 60, 62, 70, 76, 78, 86, 88, 92, 94, 96
定理3	10, 20, 26, 34, 40, 52, 58, 68, 74, 80, 82, 98

参考文献

- [1] Kim Y S, Jang J B, Chung J. Beyond 3G vision, requirements, and enabling technologies[J]. IEEE Communication Magazine, 2003, 41(3): 120 – 124.
- [2] Feng K, Shyue P J S, Xiang Q. On the aperiodic and periodic complementary binary sequences[J]. IEEE Transactions on Information Theory, 1999, 45(1): 296 – 303.
- [3] Borwein P B, Ferguson R A. A complete description of Golay pairs for lengths up to 100[J]. Mathematics of Computation, 2003, 73(7): 967 – 985.
- [4] Doković D Ž, Kotsireas I. Some new periodic golay pairs [J]. Numerical Algorithms, 2015, 69(3): 523 – 530.
- [5] Liu Z L, Paramalli U, Guan Y L. Optimal odd-length binary Z-complementary pairs[J]. IEEE Transactions on Information Theory, 2014, 60(9): 5768 – 5781.
- [6] Fan P Z, Yuan W, Tu Y. Z-complementary binary sequences [J]. IEEE Signal Processing Letters, 2007, 14(8): 509 – 512.
- [7] Liu Z, Paramalli U, Guan Y L, et al. Constructions of optimal and near-optimal quasi-complementary sequence sets from singer difference sets[J]. IEEE Wireless Communication Letters, 2013, 2(5): 487 – 490.
- [8] 李玉博, 许成谦, 刘凯. 一类四元零相关区非周期互补序列集构造法[J]. 电子学报, 2015, 43(9): 1800 – 1804.
Li Y B, Xu C Q, Liu K. A construction of quaternary aperiodic complementary sequence sets with zero correlation zone[J]. Acta Electronica Sinica, 2015, 43(9): 1800 – 1804. (in Chinese)
- [9] Xu C Q, Zhao X Q. Periodic complementary binary sequence pairs[J]. Journal of Electronics (China), 2002, 19(2): 152 – 159.
- [10] 赵成林, 蒋挺, 宋起柱, 等. 屏蔽二元互补序列偶构造方法的研究[J]. 通信学报, 2009, 30(12): 119 – 123, 131.
Zhao C L, Jiang T, Song Q Z, et al. Study of methods for constructing punctured binary complementary sequence pairs[J]. Journal on Communications, 2009, 30(12): 119 – 123, 131. (in Chinese)
- [11] Jiang T, Zhao X Q, Hou L T. On periodic punctured binary complementary sequence pairs[A]. IEEE Eighth International Conference on Communication System[C]. Singapore, Singapore: IEEE, 2002. 25 – 28.
- [12] 李琦, 李鼎, 高军萍, 等. 零相关区屏蔽四元周期互补序列偶集设计研究[J]. 电子与信息学报, 2016, 38(2): 318 – 324.
Li Q, Li D, Gao J P, et al. Design of zero correlation zone punctured quaternary periodic complementary sequence pairs sets[J]. Journal of Electronics & Information Technology, 2016, 38(2): 318 – 324. (in Chinese)
- [13] Jin H L, Qi S L, Zhang M, et al. Punctured difference set pair and perfect punctured binary sequence pair[J]. Journal of Networks, 2013, 8(9): 1982 – 1989.
- [14] Arasu K T, Arya D, Bakshi A. Constructions of punctured difference set pairs and their corresponding punctured binary array pairs[J]. IEEE Transactions on Information Theory, 2015, 61(4): 2191 – 2199.
- [15] 贾彦国, 沈秀敏, 张立超. 几类高能量效率的差集偶的研究[J]. 电子学报, 2018, 46(2): 304 – 307.
Jia Y G, Shen X M, Zhang L C. Research on several kinds of higher energy difference set pairs with efficiency[J]. Acta Electronica Sinica, 2018, 46(2): 304 – 307. (in Chinese)
- [16] 靳慧龙, 许成谦. 屏蔽差集偶与伪随机屏蔽二进制序列偶的研究[J]. 计算机工程与应用, 2012, 48(25): 24 – 27.
Jin H L, Xu C Q. Punctured difference set pairs and approach for study of pseudorandom punctured binary sequence pairs[J]. Computer Engineering and Applications, 2012, 48(25): 24 – 27. (in Chinese)
- [17] 许成谦. 差集偶与最佳二进制阵列偶的组合研究方法[J]. 电子学报, 2001, 29(1): 87 – 89.
Xu C Q. Differences set pairs and approach for the study of perfect binary array pairs[J]. Acta Electronica Sinica, 2001, 29(1): 87 – 89. (in Chinese)
- [18] 刘凯, 马国斌, 陈盼盼. 基于分圆类的完备高斯整数序列构造[J]. 电子学报, 2019, 47(4): 806 – 811.
Liu K, Ma G B, Chen P P. Construction of perfect Gaussian integer sequences based on cyclotomic classes[J]. Acta Electronica Sinica, 2019, 47(4): 806 – 811. (in Chinese)

[19] 阮传概, 孙伟. 近世代数及其应用[M]. 北京: 北京邮电大学出版社, 2001. 163 – 296.

作者简介



彭秀平 女, 1984年9月出生, 安徽安庆人. 博士, 现为燕山大学副教授, 硕士生导师, 主要研究方向为序列设计、编码理论.
E-mail: pengxp@ysu.edu.cn



郑德亮 男, 1994年12月出生, 四川巴中人. 2018年9月进入燕山大学信息科学与工程学院攻读硕士学位, 研究方向为序列设计、编码理论.