零相关区阵列偶集的递归构造研究

柯品惠* 张胜元
(福建师范大学网络安全与密码技术重点实验室 福州 350007)

摘 要：该文给出了零相关区(ZCZ)阵列偶集的一种递归构造方法。利用正交矩阵，对具有相同主峰值的阵列偶集进行交织和直积构造。由该方法得到的阵列偶集不仅具有更大的体积，而且保持了良好的相关特性。此方法可以推广为 ZCZ 屏蔽阵列偶集的递归构造。

关键词：阵列偶集；零相关区；相关函数；递归构造
中图分类号：TN911.2　　**文献标识码**：A　　**文章编号**：1009-5896(2011)05-1257-04
DOI: 10.3724/SP.J.1146.2010.00848

Study on the Recursive Constructions of Zero Correlation Zone Array Pairs Set

Ke Pin-hui　　Zhang Sheng-yuan
(*Key Laboratory of Network Security and Cryptology*, *Fujian Normal University*, *Fuzhou* 350007, *China*)

Abstract: A recursive construction of Zero Correlation Zone (ZCZ) array pairs set is proposed. By using the orthogonal matrix, the interleaving and direct product techniques are applied to an array pairs set with the same energy. The obtained ZCZ array pair set not only has larger size but also preserves good correlation properties. The proposed technique can be generalized as a recursive construction of ZCZ punctured array pairs set.

Key words: Array pairs set; Zero Correlation Zone (ZCZ); Correlation function; Recursive construction

1 引言

在雷达、声纳和扩频通信等通信系统中常要求所处理的信号具有良好的相关性质[1]。因此，在过去的几十年中，国内外的学者就具有良好相关性质的序列(信号)的分析和构造给予了大量的研究并得到了丰富的研究成果[1-10]。但是，由于 Welch 界等理论界的限制，不存在理想的序列集，即自相关函数是冲击函数而互相关函数都为零。为了满足工程的需要，人们做了两个方面的推广。一方面，对序列的维数进行了推广，提出了各种阵列及阵列偶的概念[1,3-5]。另一方面，放宽对相关区域的要求，提出了零相关区(ZCZ)和低相关区(LCZ)序列集[6,7]。近年来，结合这两个方向的研究内容，人们提出 ZCZ 阵列偶[8]及 ZCZ 屏蔽阵列偶[9]的概念，并给出了一些构造，更好地满足实际工程的需要。但总体而言，构造方法非常有限，除了文献[8-10]给出的构造外，尚未见到其它的研究成果。

注意到已有的 ZCZ 阵列偶集的构造都是直接构造，本文提出了一种 ZCZ 阵列偶集的递归构造方法。该方法构造的阵列偶集包含的阵列偶不仅有更大的体积，而且保持了良好的相关性，并给予了严格证明。本文提出的方法拓展了 ZCZ 阵列偶集的存在范围。

2 基本定义及性质

令 $\boldsymbol{X}=(x_0,x_1,\cdots,x_{n-1})$，$\boldsymbol{Y}=(y_0,y_1,\cdots,y_{n-1})$ 是两个 n 长的二进序列，其中 $x_i,y_i\in\{-1,\ 1\}$，$0\le i<n$，则它们在 $\tau,\ 0\le\tau<n$ 的周期互相关函数定义为

$$C_{\boldsymbol{X},\boldsymbol{Y}}(\tau)=\sum_{i=0}^{n-1}x_i y_{(i+\tau)\bmod n} \tag{1}$$

2 维阵列是序列的推广。

定义 1[3] 设 $\boldsymbol{X}=[x_{ij}]$, $\boldsymbol{Y}=[y_{ij}]$，其中 $x_{ij},y_{ij}\in\{-1,\ 1\}$, $0\le i<N_1$, $0\le j<N_2$，称 $\{\boldsymbol{X},\boldsymbol{Y}\}$ 是一个 $N_1\times N_2$ 阶(2 维)阵列偶，并称 $N_1\times N_2$ 为该阵列偶的体积。

类似于序列的周期互相关函数，阵列偶的周期相关函数定义如下：

定义 2[3] 设 $\boldsymbol{P}=\{\boldsymbol{X},\boldsymbol{Y}\},\boldsymbol{P}'=\{\boldsymbol{X}',\boldsymbol{Y}'\}$ 是两个体积为 $N_1\times N_2$ 阵列偶，对任意的 $\tau=(s,t)$, $0\le s<N_1$, $0\le t<N_2$，称

2010-08-12 收到，2011-01-17 改回
福建省高校服务海西建设重点项目(基于数学的信息化技术研究)，福建省自然科学基金(2010J01319)和福建师范大学青年骨干教师培养基金(2008100211)资助课题
*通信作者：柯品惠 keph@fjnu.edu.cn

$$C_{\boldsymbol{P},\boldsymbol{P}'}(\tau)=\sum_{i=0}^{N_1-1}\sum_{j=0}^{N_2-1}x_{i,j}y'_{(i+s)\bmod N_1,(j+t)\bmod N_2} \quad (2)$$

为$\boldsymbol{P}$和$\boldsymbol{P}'$在τ的周期互相关函数。

假设$\boldsymbol{X}_i,\boldsymbol{Y}_i,\boldsymbol{X}_i',\boldsymbol{Y}_i',0\le i\le N_1-1$，分别是阵列偶 $\boldsymbol{P}=\{\boldsymbol{X},\boldsymbol{Y}\},\boldsymbol{P}'=\{\boldsymbol{X}',\boldsymbol{Y}'\}$ 的行序列，这里$\boldsymbol{X}_i,\boldsymbol{Y}_i,\boldsymbol{X}_i',\boldsymbol{Y}_i'$都是$N_2$长的二进序列，则式(2)可表示为

$$C_{\boldsymbol{P},\boldsymbol{P}'}(\tau)=\sum_{i=0}^{N_1-1}C_{\boldsymbol{X}_i\boldsymbol{Y}'_{(i+s)\bmod N_1}}(t) \quad (3)$$

注意，式(2)和式(3)中的下标都是模运算，为书写的简便，在背景清楚的情况下其模运算的符号省略。若$\boldsymbol{P}=\boldsymbol{P}'$，此时称为阵列偶$\boldsymbol{P}$在$\tau$的周期自相关函数，并简记为$C_{\boldsymbol{P}}(\tau)$。

若阵列偶$\boldsymbol{P}=\{\boldsymbol{X},\boldsymbol{Y}\}$的周期自相关函数满足：

$$C_{\boldsymbol{P}}(\tau)=\begin{cases}E\ne 0, & s\equiv 0\bmod N_1, t\equiv 0\bmod N_2\\ 0, & \text{其它}\end{cases} \quad (4)$$

则称该阵列偶是最佳的[3]，其中E称为该阵列偶主峰值。

定义3[8] 设$\boldsymbol{P}^0,\boldsymbol{P}^1,\cdots,\boldsymbol{P}^{M-1}$是$M$个$N_1\times N_2$阶阵列偶，其零相关区定义为

$L=\max\{(T_1,T_2):C_{\boldsymbol{P}^i,\boldsymbol{P}^j}(s,t)=0$, 对所有$|s|<T_1,|t|<T_2,0\le i\ne j<M$，且$C_{\boldsymbol{P}^i}(s,t)=0$，对所有$|s|<T_1,|t|<T_2$, 且$(s,t)\ne(0,0),0\le i<M\}$。

若$L\ne(0,0)$，则称$\boldsymbol{P}^0,\boldsymbol{P}^1,\cdots,\boldsymbol{P}^{M-1}$为$(N_1\times N_2, M,L)$零相关区阵列偶集。

设$\{\boldsymbol{X}_0,\boldsymbol{X}_1,\cdots,\boldsymbol{X}_{m-1}\}$是$m$个$n$长的二进序列，其中$\boldsymbol{X}_i=x_{i,0}x_{i,1}\cdots x_{i,n-1}$，$0\le i<m$，$\boldsymbol{b}=(b_0,b_1,\cdots,b_{m-1})$是一个$m$长的二进序列，定义

$$\boldsymbol{I}(\boldsymbol{X}_0,\boldsymbol{X}_1,\cdots,\boldsymbol{X}_{m-1})\circ\boldsymbol{b}=\begin{bmatrix}b_0\cdot x_{0,0} & b_1\cdot x_{1,0} & \cdots & b_{m-1}\cdot x_{m-1,0}\\ b_0\cdot x_{0,1} & b_1\cdot x_{1,1} & \cdots & b_{m-1}\cdot x_{m-1,1}\\ \vdots & \vdots & & \vdots\\ b_0\cdot x_{0,n-1} & b_1\cdot x_{1,n-1} & \cdots & b_{m-1}\cdot x_{m-1,n-1}\end{bmatrix} \quad (5)$$

然后，按行依次取$\boldsymbol{I}(\boldsymbol{X}_0,\boldsymbol{X}_1,\cdots,\boldsymbol{X}_{m-1})\circ\boldsymbol{b}$的元素，得到一个$mn$长的二进序列。为方便起见，我们也把该序列$\{z_t\}_{t=0}^{mn-1}$记为$\boldsymbol{I}(\boldsymbol{X}_0,\boldsymbol{X}_1,\cdots,\boldsymbol{X}_{m-1})\circ\boldsymbol{b}$。给定周期比较小的序列，公式(5)结合了交织和直接的方法，构造了一个周期更大的序列。

设$z'=\{z_t'\}_{t=0}^{mn-1}=\boldsymbol{I}(\boldsymbol{Y}_0,\boldsymbol{Y}_1,\cdots,\boldsymbol{Y}_{m-1})\circ\boldsymbol{a}$，由文献[2]知，对$\tau$, $0\le\tau<mn$，记$\tau=t_1m+t_2$, $0\le t_1<n$, $0\le t_2<m$, 序列$\boldsymbol{z}$和$\boldsymbol{z}'$在τ的相关值为

$$C_{\boldsymbol{z},\boldsymbol{z}'}(\tau)=\sum_{i=0}^{m-t_2-1}b_ia_{i+t_2}C_{\boldsymbol{X}_i,\boldsymbol{Y}_{i+t_2}}(t_1)+\sum_{i=m-t_2}^{m-1}b_ia_{i+t_2}C_{\boldsymbol{X}_i,\boldsymbol{Y}_{i+t_2}}(t_1+1) \quad (6)$$

3 ZCZ阵列偶集的递归构造

给定具有相同主峰值的ZCZ阵列偶集，本节给出ZCZ阵列偶集的一种递归构造方法。构造得到的阵列偶不仅具有更大的体积，而且保持了良好的相关特性。

设$\mathbb{P}^0=\{\boldsymbol{P}^{0,0},\boldsymbol{P}^{0,1},\cdots,\boldsymbol{P}^{0,N-1}\}$为($N_1\times NN_2$，$N$，($N_1$，$L$))的ZCZ阵列偶集，而且每个阵列偶的主峰值都是$NE$，例如文献[8,10]给出了满足该条件的阵列偶集。

递归构造步骤如下： 对$k=1,2,\cdots$，

(1)设$N=S_kT_k$，这里S_k,T_k都是正整数，并约定$S_0=1$，$T_0=N$。同$\boldsymbol{H}^k=\{\boldsymbol{H}^{k,0},\boldsymbol{H}^{k,1},\cdots,\boldsymbol{H}^{k,T_k-1}\}$是$T_k$个$S_k$阶的正交矩阵的集合，这里正交矩阵$\boldsymbol{H}^{k,i}$，$0\le i<T_k$，允许相同。

(2) 利用$\mathbb{P}^{k-1}=\{\boldsymbol{P}^{k-1,0},\boldsymbol{P}^{k-1,1},\cdots,\boldsymbol{P}^{k-1,N-1}\}$及$\boldsymbol{H}^k=\{\boldsymbol{H}^{k,0},\boldsymbol{H}^{k,1},\cdots,\boldsymbol{H}^{k,T_k-1}\}$构造$\mathbb{P}^k=\{\boldsymbol{P}^{k,0},\boldsymbol{P}^{k,1},\cdots,\boldsymbol{P}^{k,N-1}\}$。具体步骤如下：

(a)把$\mathbb{P}^{k-1}$分为T_k个组$\{\mathbb{P}_0^{k-1},\mathbb{P}_1^{k-1},\cdots,\mathbb{P}_{T_k-1}^{k-1}\}$，每个组恰好包含$S_k$个阵列偶

$$\mathbb{P}_t^{k-1}=\{\boldsymbol{P}^{k-1,S_kt},\boldsymbol{P}^{k-1,S_kt+1},\cdots,\boldsymbol{P}^{k-1,S_k(t+1)-1}\},\ 0\le t<T_k \quad (7)$$

其中

$$P^{k-1,S_kt+i}=\{\boldsymbol{X}^{k-1,S_kt+i},\boldsymbol{Y}^{k-1,S_kt+i}\},\ \ 0\le i<S_k \quad (8)$$

是体积为$N_1\times NN_2\prod_{i=0}^{k-1}S_i$的阵列偶，

$$\boldsymbol{X}^{k-1,S_kt+i}=\begin{bmatrix}\boldsymbol{X}_0^{k-1,S_kt+i}\\ \boldsymbol{X}_1^{k-1,S_kt+i}\\ \vdots\\ \boldsymbol{X}_{N_1-1}^{k-1,S_kt+i}\end{bmatrix},\ \boldsymbol{Y}^{k-1,S_kt+i}=\begin{bmatrix}\boldsymbol{Y}_0^{k-1,S_kt+i}\\ \boldsymbol{Y}_1^{k-1,S_kt+i}\\ \vdots\\ \boldsymbol{Y}_{N_1-1}^{k-1,S_kt+i}\end{bmatrix} \quad (9)$$

(b)对$0\le t<T_k$，由$\mathbb{P}_t^{k-1}$和$\boldsymbol{H}^{k,t}$构造S_k个体积为$N_1\times NN_2\prod_{i=0}^{k}S_i$的阵列偶

$$\mathbb{P}_t^k=\{\boldsymbol{P}^{k,S_kt},\boldsymbol{P}^{k,S_kt+1},\cdots,\boldsymbol{P}^{k,S_k(t+1)-1}\} \quad (10)$$

其中

$$\boldsymbol{P}^{k,S_kt+i}=\{\boldsymbol{X}^{k,S_kt+i},\boldsymbol{Y}^{k,S_kt+i}\},\ \ 0\le i<S_k \quad (11)$$

$$\boldsymbol{X}^{k,S_kt+i}=\begin{bmatrix}\boldsymbol{I}(\boldsymbol{X}_0^{k-1,S_kt},\boldsymbol{X}_0^{k-1,S_kt+1},\cdots,\boldsymbol{X}_0^{k-1,S_k(t+1)-1})\\ \circ(h_{i,0}^{k,t},h_{i,1}^{k,t},\cdots,h_{i,S_k-1}^{k,t})\\ \vdots\\ \boldsymbol{I}(\boldsymbol{X}_{N_1-1}^{k-1,S_kt},\boldsymbol{X}_{N_1-1}^{k-1,S_kt+1},\cdots,\boldsymbol{X}_{N_1-1}^{k-1,S_k(t+1)-1})\\ \circ(h_{i,0}^{k,t},h_{i,1}^{k,t},\cdots,h_{i,S_k-1}^{k,t})\end{bmatrix} \quad (12)$$

$$\boldsymbol{Y}^{k,S_kt+i}=\begin{bmatrix}\boldsymbol{I}(\boldsymbol{Y}_0^{k-1,S_kt},\boldsymbol{Y}_0^{k-1,S_kt+1},\cdots,\boldsymbol{Y}_0^{k-1,S_k(t+1)-1})\\ \circ(h_{i,0}^{k,t},h_{i,1}^{k,t},\cdots,h_{i,S_k-1}^{k,t})\\ \vdots\\ \boldsymbol{I}(\boldsymbol{Y}_{N_1-1}^{k-1,S_kt},\boldsymbol{Y}_{N_1-1}^{k-1,S_kt+1},\cdots,\boldsymbol{Y}_{N_1-1}^{k-1,S_k(t+1)-1})\\ \circ(h_{i,0}^{k,t},h_{i,1}^{k,t},\cdots,h_{i,S_k-1}^{k,t})\end{bmatrix}$$

这里，$(h_{i,0}^{k,\,t},h_{i,1}^{k,\,t},\cdots,h_{i,S_k-1}^{k,\,t})$ 表示 $\boldsymbol{H}^{k,\,t}$ 的第 i 行。

由此，由 $\mathbb{P}_0^k,\mathbb{P}_1^k,\cdots,\mathbb{P}_{T_k-1}^k$ 得到一个包含 N 个体积为 $N_1\times NN_2\prod_{i=0}^{k}S_i$ 的阵列偶的集合

$$\mathbb{P}^k=\{\boldsymbol{P}^{k,0},\cdots,\boldsymbol{P}^{k,S_k-1},\cdots,\boldsymbol{P}^{k,S_k(T_k-1)},\cdots,\boldsymbol{P}^{k,N-1}\}$$

定理 1　如上构造得到的 $\mathbb{P}^k$ 是参数为 $\left(N_1\times NN_2\prod_{i=0}^{k}S_i,\ N,\ \left(N_1,\ \prod_{i=0}^{k}S_iL\right)\right)$ ZCZ 阵列偶集。

证明　用归纳法证明。当 $k=0$ 时，由文献[8]知 $\mathbb{P}^0=\{\boldsymbol{P}^{0,0},\boldsymbol{P}^{0,1},\cdots,\boldsymbol{P}^{0,N-1}\}$ 是($N_1\times NN_2$, N, (N_1, L))的 ZCZ 阵列偶集，结论显然成立。假设当 $k-1$ 时，结论成立。下面证明在 k 时，结论亦成立。首先，由递归构造的过程易知 $\mathbb{P}^k$ 恰好包含 N 个体积为 $N_1\times NN_2\prod_{i=0}^{k}S_i$ 的阵列偶。其次，证明 $\mathbb{P}^k$ 的零相关区域为 $\left(N_1,\ \prod_{i=0}^{k}S_iL\right)$。

(1) 自相关函数　任取 $\mathbb{P}^k$ 中的一个阵列偶 $\boldsymbol{P}^{k,h}=\{\boldsymbol{X}^{k,h},\boldsymbol{Y}^{k,h}\}$, $0\le h<N$ ，不妨设 $h=t\cdot S_k+r$, $0\le t<T_k$, $0\le r<S_k$ ，则 $\tau=(\tau_1,\tau_2)$, $\tau_2=S_kt_1+t_2$, $0\le t_1\le\prod_{i=0}^{k-1}S_iL$, $0\le t_2<S_k$ ，由式(6)有

$$\begin{aligned}C_{\boldsymbol{P}^{k,h}}(\tau)=&\sum_{j=0}^{S_k-t_2-1}h_{r,j}^{k,t}h_{r,j+t_2}^{k,t}C_{\boldsymbol{P}^{k-1,S_kt+j},\boldsymbol{P}^{k-1,S_kt+t_2+j}}(\tau_1,t_1)\\&+\sum_{j=S_k-t_2}^{S_k-1}h_{r,j}^{k,t}h_{r,j+t_2}^{k,t}C_{\boldsymbol{P}^{k-1,S_kt+j},\boldsymbol{P}^{k-1,S_kt+t_2+j}}(\tau_1,t_1+1)\end{aligned}$$

(a)当 $\tau_1=0$ 且 $\tau_2=0$ 时，

$$\begin{aligned}C_{\boldsymbol{P}^{k,h}}(\tau)&=\sum_{j=0}^{S_k-1}C_{\boldsymbol{P}^{k-1,S_kt+j}}(0,0)\\&=S_k\cdot\prod_{i=0}^{k-1}S_iNE=\prod_{i=0}^{k}S_iNE\end{aligned}$$

(b)当 $\tau_1=0$ 且 $\tau_2\ne0$ 时，则 t_1 与 t_2 不同时为 0。若 $t_2=0$ ，则 $0<t_1<\prod_{i=0}^{k-1}S_iL$ 。由 $\mathbb{P}^{k-1}$ 是零相关区为 $\left(N_1,\prod_{i=0}^{k-1}S_iL\right)$ 的 ZCZ 阵列偶集知，$\mathbb{P}^{k-1}$ 中任意一个阵列偶在 $(0,t_1)$ 的自相关值为 0，即 $C_{\boldsymbol{P}^{k-1,S_kt+j}}(0,t_1)=0$， $0\le t<T_k$, $0\le j<S_k$ 。进而

$$C_{\boldsymbol{P}^{k,h}}(\tau)=\sum_{j=0}^{S_k-1}C_{\boldsymbol{P}^{k-1,S_kt+j}}(0,t_1)=0$$

若 $t_2\ne0$ ，则 $t_1<\prod_{i=0}^{k-1}S_iL$ (否则若 $t_1=\prod_{i=0}^{k-1}S_iL$, $t_2\ne0$ ，得 $\tau_2=S_kt_1+t_2>\prod_{i=0}^{k}S_iL$, 矛盾)。由 $\mathbb{P}^{k-1}$ 是零相关区为 $\left(N_1,\prod_{i=0}^{k-1}S_iL\right)$ 的 ZCZ 阵列偶集知，$\mathbb{P}^{k-1}$ 中任意两个不同的阵列偶在 $(0,t_1)$ 和 $(0,t_1+1)$ 的互相关值为 0，即对 $0\le t<T_k,0\le j<S_k$,

$$\begin{aligned}&C_{\boldsymbol{P}^{k-1,S_kt+j},\boldsymbol{P}^{k-1,S_kt+t_2+j}}(0,t_1)\\&=C_{\boldsymbol{P}^{k-1,S_kt+j},\boldsymbol{P}^{k-1,S_kt+t_2+j}}(0,t_1+1)=0\end{aligned}$$

进而

$$\begin{aligned}C_{\boldsymbol{P}^{k,h}}(\tau)=&\sum_{j=0}^{S_k-t_2-1}h_{r,j}^{k,t}h_{r,j+t_2}^{k,t}C_{\boldsymbol{P}^{k-1,S_kt+j},\boldsymbol{P}^{k-1,S_kt+t_2+j}}(0,t_1)\\&+\sum_{j=S_k-t_2}^{S_k-1}h_{r,j}^{k,t}h_{r,j+t_2}^{k,t}\\&\cdot C_{\boldsymbol{P}^{k-1,S_kt+j},\boldsymbol{P}^{k-1,S_kt+t_2+j}}(0,t_1+1)=0\end{aligned}$$

(c)当 $\tau_1\ne0$ 且 $\tau_2=0$ 时，由 $\mathbb{P}^{k-1}$ 的零相关区域是 $\left(N_1,\prod_{i=0}^{k-1}S_iL\right)$，亦知 $\mathbb{P}^{k-1}$ 中任意一个阵列偶在 $(\tau_1,0)$ 的自相关值为 0。进而，

$$C_{\boldsymbol{P}^{k,h}}(\tau)=\sum_{j=0}^{S_k-1}C_{\boldsymbol{P}^{k-1,S_kt+j}}(\tau_1,0)=0$$

(d)当 $\tau_1\ne0$ 且 $\tau_2\ne0$ 时，类似于情形(b)分析。当 $t_2=0$ 时，

$$C_{\boldsymbol{P}^{k,h}}(\tau)=\sum_{j=0}^{S_k-1}C_{\boldsymbol{P}^{k-1,S_kt+j}}(\tau_1,t_1)=0$$

当 $t_2\ne0$ 时，

$$\begin{aligned}C_{\boldsymbol{P}^{k,h}}(\tau)=&\sum_{j=0}^{S_k-t_2-1}h_{r,j}^{k,t}h_{r,j+t_2}^{k,t}C_{\boldsymbol{P}^{k-1,S_kt+j},\boldsymbol{P}^{k-1,S_kt+t_2+j}}(\tau_1,t_1)\\&+\sum_{j=S_k-t_2}^{S_k-1}h_{r,j}^{k,t}h_{r,j+t_2}^{k,t}\\&\cdot C_{\boldsymbol{P}^{k-1,S_kt+j},\boldsymbol{P}^{k-1,S_kt+t_2+j}}(\tau_1,t_1+1)\end{aligned}$$

由 $\mathbb{P}^{k-1}$ 的零相关区域是 $\left(N_1,\prod_{i=0}^{k-1}S_iL\right)$，容易验证上述的相关值亦为零。

(2)互相关函数　设 $\boldsymbol{P}^{k,h_1},\boldsymbol{P}^{k,h_2}$ 是 $\mathbb{P}^k$ 中两个不同的阵列偶，即 $h_1\ne h_2$。计算它们在 $\tau=(\tau_1,\tau_2)$ 的互相关值。分两种情形讨论：

(a) $\lfloor h_1/S_k\rfloor=\lfloor h_2/S_k\rfloor$

不妨设 $P^{k,h_i}=\{X^{k,h_i},Y^{k,h_i}\}$, $h_i=tS_k+r_i,i=1,2$, $0\le t<T_k$, $0\le r_1\ne r_2<S_k$ 。

(i)当 $\tau_1=0$ 且 $\tau_2=0$ 时，

$$\begin{aligned}C_{\boldsymbol{P}^{k,h_1},\boldsymbol{P}^{k,h_2}}(\tau)&=\sum_{j=0}^{S_k-1}h_{r_1,j}^{k,t}h_{r_2,j}^{k,t}C_{\boldsymbol{P}^{k-1,S_kt+j},\boldsymbol{P}^{k-1,S_kt+j}}(0,0)\\&=\prod_{i=0}^{k-1}S_iNE\cdot\left(\sum_{j=0}^{S_k-1}h_{r_1,j}^{k,t}h_{r_2,j}^{k,t}\right)\end{aligned}$$

由 $\boldsymbol{H}^{k,\,t}$ 是正交矩阵知， $\boldsymbol{H}^{k,\,t}$ 中不同行的内积

为 0，即 $\sum_{j=0}^{S_k-1} h_{\tau_1,j}^{k,t} h_{\tau_2,j}^{k,t} = 0$ ，可知上式为 0。

(ii)其它情形，类似(1)中相应的情形可证，由于方法类似，不再赘述。

(b) $\lfloor h_1/S_k \rfloor \neq \lfloor h_2/S_k \rfloor$

在 $\tau_1 = 0$ 且 $\tau_2 = 0$ 时，此时 $\lfloor h_1/S_k \rfloor \neq \lfloor h_2/S_k \rfloor$ ，由 $\mathbb{P}^{k-1}$ 是 ZCZ 阵列偶集知， $\mathbb{P}^{k-1}$ 中两个不同的阵列偶在 $(0,0)$ 的互相关值为 0。其它情形类似(1)中相应的情形类似可证。 证毕

4 结束语

给定具有相同主峰值的阵列偶的ZCZ阵列偶集，本文提出ZCZ阵列偶集一种递归构造方法。注意到，在递归构造中若 N 的分解不同及 $\boldsymbol{H}^k$ 中正交矩阵选取不同，则递归构造得到的ZCZ阵列偶集也互不相同。由此，该方法可以得到大量的ZCZ阵列偶集。值得一提的是，本文的方法可以平移到ZCZ屏蔽阵列偶集的情形，此时只需把初始条件中的ZCZ阵列偶集换成ZCZ屏蔽阵列偶集即可。

参 考 文 献

[1] 杨义先. 最佳信号理论与设计[M]. 北京：人民邮电出版社, 1996: 35–39.
Yang Yi-xian. The Theory and Design of Perfect Signals [M]. Beijing: People's Posts and Telecommunication Publisher, 1996: 35–39.

[2] Golomb G and Gong G. Signal Designs with Good Correlations: for Wireless Communications, Cryptography and Radar Applications [M]. Cambridge, UK, Cambridge University Press, 2005: 219–318.

[3] 赵晓群, 何文才, 王仲文等. 最佳二进阵列偶理论研究[J]. 电子学报, 1999, 27(1): 34–37.
Zhao Xiao-qun, He Wen-cai, and Wang Zhong-wen, *et al.*. The theory of perfect binary array pairs [J]. *Acta Electronica Sinica*, 1999, 27(1): 34–37.

[4] 许成谦. 差集偶与最佳二进阵列偶的组合研究方法[J]. 电子学报, 2001, 29(1): 87–89.
Xu Cheng-qian. Differences set pairs and approach for the study of perfect binary array pairs [J]. *Acta Electronica Sinica*, 2001, 29(1): 87–89.

[5] 蒋挺, 赵晓群, 侯蓝田. 最佳屏蔽二进阵列偶理论研究[J]. 电子学报, 2005, 32(2): 282–286.
Jiang Ting, Zhao Xiao-qun, and Hou Lan-tian. The study of punctured binary array pairs[J]. *Acta Electronica Sinica*, 2005, 32(2): 282–286.

[6] Tang X H and Fan P Z. Lower bounds on the maximum correlation of sequence set with low and zero correlation zone[J]. *Electronics Letters*. 2000, 36(6): 551–552.

[7] Tang X H, Fan P Z, and Lindner J. Multiple binary ZCZ sequence sets with good cross-correlation property based on complementary sequence sets [J]. *IEEE Transaction on Information Theory*, 2010, 56(8): 4038–4045.

[8] 高军萍, 李琦, 戴居丰等. ZCZ阵列偶及其构造方法研究[J]. 通信学报, 2008, 29(9): 62–67.
Gao Jun-ping, Li Qi, and Dai Ju-feng, *et al.*. Research of ZCZ array pair and its construction methods [J]. *Journal of Communications*, 2008, 29(9): 62–67.

[9] 李兆斌, 蒋挺, 周正. ZCZ屏蔽阵列偶集的研究[J]. 电子学报, 2009, 37(3): 489–493.
Li Zhao-bin, Jiang Ting, and Zhou Zheng. Study on ZCZ punctured array pairs set[J]. *Acta Electronica Sinica*, 2009, 37(3): 489–493.

[10] 柯品惠, 王志华, 张胜元. 基于交织方法的ZCZ阵列偶的构造研究[J]. 电子与信息学报, 2010, 32(12): 3037–3040.
Ke Pin-hui, Wang Zhi-hua, and Zhang Sheng-yuan. Constructions of ZCZ array pairs set by interleaving techniques[J]. *Journal of Electronic & Information Technology*, 2010, 32(12): 3037–3040.

柯品惠： 男，1978 年生，副教授，研究方向为最佳信号设计、现代密码学中的布尔函数.

张胜元： 男，1966 年生，教授，研究方向为编码密码学、组合数学及信息安全.