基于交织方法的 ZCZ 阵列偶集的构造研究

柯品惠 王志华 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：该文提出了使用移位序列集构造 ZCZ 阵列偶集的方法，与已有结果相比，该方法构造得到的阵列偶集包含更多的阵列偶数目。为了计算该阵列偶集的零相关区的大小，提出了移位序列集的差矩阵，并给出了更多的移位序列的构造。此方法可以推广用于构造 ZCZ 屏蔽阵列偶集。

关键词：最佳阵列偶；零相关区；交织方法；相关函数
中图分类号：TN911.2 **文献标识码**： A **文章编号**：1009-5896(2010)12-3037-04
DOI: 10.3724/SP.J.1146.2010.00052

Constructions of ZCZ Array Pairs Set by Interleaving Techniques

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

Abstract: By using shift sequence set, a new construction of ZCZ (Zero Correlation Zone) array pairs set is proposed. Compared with known results, the obtained ZCZ array pair sets include more array pairs. For computing the size of zero correlation zone, the difference matrix of shift sequence set is introduced. Furthermore, more constructions of shift sequences are presented. The proposed technique can be used to construct the ZCZ punctured arrays set.

Key words: Perfect signal array; Zero Correlation Zone (ZCZ); Interleaving technique; Correlation function

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集满足如下两个条件或其中之一[1]：(1)信号集里的每一个信号都容易与自身的移位信号区分开来；(2)信号集里的每一个信号都容易与该信号集的其它信号及其延时信号区分开。在应用中，为简化工程系统，常要求信号是周期的。关于周期信号，上述两个条件可以分别用其采样信号的周期自相关函数和周期互相关函数来刻画。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，提出了阵列及阵列偶的概念，包括最佳二进阵列[1]，最佳二进阵列偶[3,6]，几乎最佳二进阵列偶[4]，最佳屏蔽阵列偶[5]等。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)序列集的概念，并给出了许多构造方法，如文献[7–10]。近年来，有学者结合这两个方向的研究内容，提出 ZCZ 阵列偶[11]及 ZCZ 屏蔽阵列偶[12]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，构造方法还是比较有限。

本文对 ZCZ 阵列偶给予了进一步的研究，通过分析文献[11,12]基于交织方法和正交矩阵的 ZCZ 阵列偶集及屏蔽阵列偶集的构造，提出了使用不用的移位序列来构造 ZCZ 阵列偶集的新的方法，新提出的构造方法得到的 ZCZ 阵列偶集较之文献[11]包含了更多的阵列偶数目。而且通过分析其相关函数，提出移位序列集的差矩阵，并给出了通过差矩阵计算 ZCZ 阵列偶集的零相关区大小的有效方法，该方法不仅能对已有的构造给予简明的合理性证明，还有利于寻找满足要求的移位序列进而得到具有一定零相关区域的 ZCZ 阵列偶集的构造。注意到，把本文的阵列偶换成屏蔽阵列偶就可以得到相应的 ZCZ 屏蔽阵列偶集的构造，进而推广文献[12]的结果。

2 基本定义及性质

令 $X=(x_0,x_1,\cdots,x_{n-1})$, $Y=(y_0,y_1,\cdots,y_{n-1})$ 是两

2010-01-19 收到，2010-06-01 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)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

个 n 长的二进序列，即 $x_i, y_i \in \{-1, 1\}$, $0 \le i < n$, 则它们在 τ, $0 \le \tau < n$, 的周期相关函数定义为

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

二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(二维)阵列偶，其中，$N_1 \times N_2$ 称为该阵列偶的体积。

类似于序列的周期相关函数，阵列偶的周期相关函数定义如下：

定义 2[3] 设 $\boldsymbol{P} = \{\boldsymbol{X}, \boldsymbol{Y}\}$ 为一个 $N_1 \times N_2$ 阶阵列偶，对任意的 $\tau = (s,t)$, $0 \le s < N_1$, $0 \le t < N_2$，称

$$C_P(\tau) = \sum_{i=0}^{N_1-1} \sum_{j=0}^{N_2-1} x_{ij} y_{(i+s) \bmod N_1, (j+t) \bmod N_2} \tag{2}$$

为该阵列偶在 τ 的周期自相关函数。

记 X_i，Y_i，$0 \le i \le N_1 - 1$，分别为 $N_1 \times N_2$ 阶阵列偶 $\boldsymbol{P} = \{\boldsymbol{X}, \boldsymbol{Y}\}$ 的行子序列，则易见

$$C_P(\tau) = \sum_{i=0}^{N_1-1} C_{X_i Y_{(i+s) \bmod N_1}}(t) \tag{3}$$

注意，和式中的下标都是模运算，为简单起见，在背景清楚的情况下其模运算的符号省略。

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

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

则称该阵列偶是最佳的[3]。

设 $\boldsymbol{P}^{(1)} = \{\boldsymbol{X}^{(1)}, \boldsymbol{Y}^{(1)}\}$, $\boldsymbol{P}^{(2)} = \{\boldsymbol{X}^{(2)}, \boldsymbol{Y}^{(2)}\}$ 是两个 $N_1 \times N_2$ 阶阵列偶，则 $\boldsymbol{P}^{(1)}$ 和 $\boldsymbol{P}^{(2)}$ 在 $\tau = (s,t)$ 的周期互相关定义为

$$C_{P^{(1)}, P^{(2)}}(\tau) = \sum_{i=0}^{N_1-1} \sum_{j=0}^{N_2-1} x_{ij}^{(1)} y_{(i+s) \bmod N_1, (j+t) \bmod N_2}^{(2)} \tag{5}$$

定义 3[11] 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

$L = \max\{(T_1, T_2) : C_{P^{(i)}, P^{(j)}}(s,t) = 0$, 对所有 $|s| < T_1, |t| < T_2, 0 \le i \ne j < M$,且 $C_{P^{(i)}}(s,t) = 0$，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 $P^{(0)}, P^{(1)}, \cdots, P^{(M-1)}$ 为 $(N_1 \times N_2, M, L)$ 阵列偶集。

交织方法是序列构造的一种重要方法，有关该方法的相关内容，请参考文献如[2,9]。对一个基序列为 B，移位序列为 E 的交织序列，简记为 $S = I(B,E)$。给定的两个 $N_1 N_2$ 长的交织序列 $S_1 = I(A,E), S_2 = I(B,F)$，其中 $A = \{a_i\}_{i=0}^{N_1-1}$, $B = \{b_i\}_{i=0}^{N_1-1}$, $E = \{e_i\}_{i=0}^{N_2-1}$, $F = \{f_i\}_{i=0}^{N_2-1}$ 文献[2]给出它们在 τ 的相关函数，记 $\tau = N_1 \tau_1 + \tau_2$, $0 \le \tau_1 < N_2$, $0 \le \tau_2 < N_1$，则

$$C_{S_1,S_2}(\tau) = \sum_{i=0}^{N_2-\tau_2-1} C_{A,B}(f_{i+\tau_2} - e_i + \tau_1) + \sum_{i=N_2-\tau_2}^{N_2-1} C_{A,B}(f_{i+\tau_2} - e_i + \tau_1 + 1) \tag{6}$$

定义 4[2] 称 N 阶矩阵 $\boldsymbol{H} = [h_{ij}]$ 为 Hadamard 矩阵，其中 $h_{ij} \in \{-1,1\}$，如果 $\boldsymbol{H}$ 的行向量满足正交关系，即

$$\boldsymbol{H} \times \boldsymbol{H}^{\mathrm{T}} = N I_N \tag{7}$$

3 ZCZ 阵列偶集的交织构造

给定 $N_1 \times N_2$ 阶最佳阵列偶或最佳屏蔽阵列偶 $\boldsymbol{P} = \{\boldsymbol{X}, \boldsymbol{Y}\}$ 以及 N 阶 Hadamard 矩阵 $\boldsymbol{H}$，文献[11, 12]分别用交织方法给出了体积为 $N_1 \times NN_2$ 阶 ZCZ 阵列偶集和 ZCZ 屏蔽阵列偶集的构造。本节将基于已有方法，通过适当选取不同的移位序列，构造包含更多阵列偶数目的阵列偶集。不妨设 $E^{(0)}, E^{(1)}, \cdots, E^{(M-1)}$ 是 M 个不同的移位序列，其中

$$E^{(i)} = \left\{e_0^{(i)}, e_1^{(i)}, \cdots, e_{N-1}^{(i)}\right\}, \ e_j^{(i)} \in \{0,1,\cdots,N_2-1\}, \ 0 \le i < M, \ 0 \le j < N$$

构造步骤如下：

(1)对每个移位序列 $E^{(i)} = \{e_0^{(i)}, e_1^{(i)}, \cdots, e_{N-1}^{(i)}\}$，构造体积为 $N_1 \times NN_2$ 的阵列偶 $\boldsymbol{P}^{(i)} = \{\widetilde{\boldsymbol{X}}^{(i)}, \widetilde{\boldsymbol{Y}}^{(i)}\}$，$0 \le i < M$，

$$\widetilde{\boldsymbol{X}}^{(i)} = \begin{bmatrix} I(X_0, E^{(i)}) \\ I(X_1, E^{(i)}) \\ \vdots \\ I(X_{N_1-1}, E^{(i)}) \end{bmatrix}, \ \widetilde{\boldsymbol{Y}}^{(i)} = \begin{bmatrix} I(Y_0, E^{(i)}) \\ I(Y_1, E^{(i)}) \\ \vdots \\ I(Y_{N_1-1}, E^{(i)}) \end{bmatrix} \tag{8}$$

(2)对每个 $p^{(i)}$ 及 h_j，$0 \le i < M$，$0 \le j < N$，构造阵列偶 $\boldsymbol{P}^{(i,j)} = \{\widetilde{\boldsymbol{X}}^{(ij)}, \widetilde{\boldsymbol{Y}}^{(ij)}\}$

$$\widetilde{\boldsymbol{X}}^{(ij)} = \begin{bmatrix} h_j \circ I(X_0, E^{(i)}) \\ h_j \circ I(X_1, E^{(i)}) \\ \vdots \\ h_j \circ I(X_{N_1-1}, E^{(i)}) \end{bmatrix}, \ \widetilde{\boldsymbol{Y}}^{(ij)} = \begin{bmatrix} h_j \circ I(Y_0, E^{(i)}) \\ h_j \circ I(Y_1, E^{(i)}) \\ \vdots \\ h_j \circ I(Y_{N_1-1}, E^{(i)}) \end{bmatrix} \tag{9}$$

其中 $h_i \circ I(B,E)$ 定义为 $[h_{i0} L^{e_0}(B), h_{i1} L^{e_1}(B), \cdots, h_{i(N-1)} \cdot L^{e_{N-1}}(B)]$。

由此可以得到 MN 个体积为 $N_1 \times NN_2$ 的阵列偶 $P^{(0,0)}, P^{(0,1)}, \cdots, P^{(M-1,N-1)}$。对任意两个序列偶 $P^{(k,m)}$ 和 $P^{(l,n)}$，它们在 $\tau = (s,t)$，$0 \le s < N_1$，$0 \le t < NN_2$ 的相关值为

$$C_{P^{(k,m)}, P^{(l,n)}}(s,t) = \sum_{i=0}^{N_1-1} C_{h_m \circ I(X_i, E^{(k)}), h_n \circ I(Y_{i+s}, E^{(l)})}(t) \tag{10}$$

记 $t=N\tau_1+\tau_2, 0\le\tau_1<N_2, 0\le\tau_2<N$，则由式(6)知

$$C_{P^{(k,m)},P^{(l,n)}}(s,t)=\sum_{j=0}^{N-\tau_2-1}h_{m,j}h_{n,j+\tau_2}C_{X,Y}(s,\ e_{j+\tau_2}^{(l)}-e_j^{(k)}+\tau_1)+\sum_{j=N-\tau_2}^{N-1}h_{m,j}h_{n,j+\tau_2}C_{X,Y}(s,\ e_{j+\tau_2}^{(l)}-e_j^{(k)}+\tau_1+1)\quad(11)$$

易见，若 $\boldsymbol{P}=\{\boldsymbol{X},\boldsymbol{Y}\}$ 是最佳二进阵列偶，$s\ne0$ 或 $e_j^{(k)}-e_{j+\tau_2}^{(l)}-1\ne\tau_1$，且 $e_j^{(k)}-e_{j+\tau_2}^{(l)}\ne\tau_1$，则 $C_{P^{(k,m)},P^{(l,n)}}(s,t)=0$。

由式(11)可以看出，要使得构造得到的阵列偶集具有较好的相关性，则其移位序列集必须满足一定的条件。类似文献[13]中的定义，我们引入如下记号：

定义 5

$$\boldsymbol{D}_{E^{(i)},E^{(j)}}=\begin{bmatrix}e_0^{(i)}-e_0^{(j)} & e_1^{(i)}-e_1^{(j)} & \cdots\\ e_0^{(i)}-e_1^{(j)} & e_1^{(i)}-e_2^{(j)} & \cdots\\ \vdots & \vdots & \\ e_0^{(i)}-e_{N-1}^{(j)} & e_1^{(i)}-e_0^{(j)}-1 & \cdots\\ e_{N-2}^{(i)}-e_{N-2}^{(j)} & e_{N-1}^{(i)}-e_{N-1}^{(j)} & \\ e_{N-2}^{(i)}-e_{N-1}^{(j)} & e_{N-1}^{(i)}-e_0^{(j)}-1 & \\ \vdots & \vdots & \\ e_{N-2}^{(i)}-e_{N-3}^{(j)}-1 & e_{N-1}^{(i)}-e_{N-2}^{(j)}-1 &\end{bmatrix}\quad(12)$$

矩阵中元素的运算均为模 N_2，即取值为 $\{0,1,\cdots,N_2-1\}$，称其为移位序列 $E^{(i)}$ 和 $E^{(j)}$ 的差矩阵。

记 $\boldsymbol{D}_{e^{(i)},e^{(j)}}$ 的第 i 行为 $\boldsymbol{D}_i$，$0\le i\le N-1$，且 $\min^0(\boldsymbol{D}_{E^{(i)},E^{(j)}})=\min\boldsymbol{D}_0$

$$\min{}^*(\boldsymbol{D}_{E^{(i)},E^{(j)}})=\min\{\boldsymbol{D}_1,\boldsymbol{D}_2,\cdots,\boldsymbol{D}_{N-1}\}$$

$$\mathrm{Index}\left\{\boldsymbol{D}_{E^{(i)},E^{(j)}}\right\}=\min_{1\le i<N}\left\{i:\min\boldsymbol{D}_i=\min{}^*\left(\boldsymbol{D}_{E^{(i)},E^{(j)}}\right)\right\}$$

定理 1　设 $P=\{X,Y\}$ 是体积为 $N_1\times N_2$ 的最佳阵列偶，$\{E^{(0)},E^{(1)},\cdots,E^{(M-1)}\}$ 是 M 个移位序列，则 $P^{(0,0)},P^{(0,1)},\cdots,P^{(M-1,N-1)}$ 是一个 $(N_1\times NN_2,MN,(T_1,T_2))$-ZCZ 阵列偶集，其中

$$T_1=N_1$$

$$T_2=\min\left\{\min_{i\ne j}\left\{N\cdot\min{}^0\left\{\boldsymbol{D}_{E^{(i)},E^{(j)}}\right\}\right\},\ \min\left\{N\cdot\min{}^*\left\{\boldsymbol{D}_{E^{(i)},E^{(j)}}\right\}+\mathrm{Index}\left\{\boldsymbol{D}_{E^{(i)},E^{(j)}}\right\}\right\}\right\}$$

证明

(1)对该阵列偶集中的任意一个阵列偶 $P^{(k,m)}$，计算其非零移位的自相关函数。

对任意的 (s,t)，$0\le s<N_1, 0\le t=N\tau_1+\tau_2<T_2,(s,t)\ne(0,0)$，由式(11)

$$C_{P^{(k,m)}}(s,t)=\sum_{j=0}^{N-\tau_2-1}h_{m,j}h_{m,j+\tau_2}C_{X,Y}(s,e_{j+\tau_2}^{(k)}-e_j^{(k)}+\tau_1)+\sum_{j=N-\tau_2}^{N-1}h_{m,j}h_{m,j+\tau_2}C_{X,Y}(s,e_{j+\tau_2}^{(k)}-e_j^{(k)}+\tau_1+1)$$

(a)若 $s\ne0$，易知 $C_{P^{(k,m)}}(s,t)=0$。

(b)若 $s=0$，$\tau_2=0$，但 $\tau_1\ne0$，则

$$C_{P^{(k,m)}}(s,t)=\sum_{j=0}^{N-1}C_{X,Y}(s,\tau_1)=0$$

(c)若 $s=0,\tau_2\ne0$，则由 $0\le t=N\tau_1+\tau_2<T_2$，及 T_2 的定义知，$\tau_1<\min^*\{\boldsymbol{D}_{E^{(k)},E^{(k)}}\}$ 或 $\tau_1=\min^*\{\boldsymbol{D}_{E^{(k)},E^{(k)}}\}$，$\tau_2<\mathrm{Index}\{\boldsymbol{D}_{E^{(i)},E^{(j)}}\}$，从而，$e_{j+\tau_2}^{(k)}-e_j^{(k)}+\tau_1\ne0, 0\le j<N-\tau_2-1$，且 $e_{j+\tau_2}^{(k)}-e_j^{(k)}+\tau_1+1\ne0, N-\tau_2\le j<N-1$。进而，$C_{P^{(k,m)}}(s,t)=0$。

(2)对任意两个不同的阵列偶 $\boldsymbol{P}^{(k,m)}$ 和 $\boldsymbol{P}^{(l,n)}$，计算其互相关函数值。

对任意的 (s,t)，$0\le s<N_1, 0\le t=N\tau_1+\tau_2<T_2$，由式(11)

$$C_{P^{(k,m)},P^{(l,n)}}(s,t)=\sum_{j=0}^{N-\tau_2-1}h_{m,j}h_{n,j+\tau_2}C_{X,Y}(s,e_{j+\tau_2}^{(l)}-e_j^{(k)}+\tau_1)+\sum_{j=N-\tau_2}^{N-1}h_{m,j}h_{n,j+\tau_2}C_{X,Y}(s,e_{j+\tau_2}^{(l)}-e_j^{(k)}+\tau_1+1)$$

(a)若 $k=l$，则 $m\ne n$。此时，若 $(s,t)=(0,0)$，则由 $\boldsymbol{H}$ 是Hadamard矩阵知

$$C_{P^{(k,m)},P^{(l,n)}}(0,0)=\sum_{j=0}^{N-1}h_{mj}\cdot h_{nj}\cdot E=0$$

若 $(s,t)\ne(0,0)$，类似(1)可证。

(b)若 $k\ne l$，此时，如果 $(s,t)=(0,0)$，由 T_2 的定义知

$$\min\left\{N\cdot\min{}^\circ\left(\boldsymbol{D}_{E(k),E(l)}\right)\right\}>0$$

从而，$C_{P^{(k,m)},P^{(l,n)}}(0,0)=0$。

如果 $(s,t)\ne(0,0)$，类似(1)可证。　　证毕

显然，定理 1 构造的阵列偶集包含更多的阵列偶个数，而且此时零相关区的大小可由矩阵 $\{\boldsymbol{D}_{E^{(i)},E^{(j)}}\}_{0\le i,j<M}$ 得到。文献[11] 给出的构造可看成定理 1 的特殊情况，即只取一个移位序列，利用定理 1 容易给文献[11]的结果一个简单的证明。

推论 1[11]

(1) 当 $N\,|\,N_2$ 时，取 $e_i\equiv(N_2/N)i \bmod N_2$，则 $\boldsymbol{P}^{(0)},\boldsymbol{P}^{(1)},\cdots,\boldsymbol{P}^{(N-1)}$ 是 $(N_1\times NN_2,N,(N_1,N_2-1))$-ZCZ 阵列偶集。

(2)当 $N_2\,|\,N$ 时，取 $e_i\equiv i \bmod N_2$，则 $\boldsymbol{P}^{(0)},\boldsymbol{P}^{(1)},\cdots,\boldsymbol{P}^{(N-1)}$ 是 $(N_1\times NN_2,N,(N_1,N_2-1))$-ZCZ 阵列偶

集。

(3)当 $\gcd(N,N_2)=1$ 时，取 $e_i \equiv N^{-1}i \bmod N_2$，则 $\boldsymbol{P}^{(0)},\boldsymbol{P}^{(1)},\cdots,\boldsymbol{P}^{(N-1)}$ 是 $(N_1\times NN_2,N,(N_1,N_2-1))$-ZCZ 阵列偶集。

证明 由定理 1，只需证明 T_2 分别为 N_2-1，N_2-1 及 N_2 即可。

(1)当 $N\mid N_2$ 时，不妨设 $N_2=kN$，则

$$\boldsymbol{D}_{E,E}=\begin{bmatrix} 0 & 0 & \cdots & 0 \\ (N-1)k & (N-1)k & \cdots & (N-1)k-1 \\ \vdots & \vdots & & \vdots \\ 2k & 2k & \cdots & 2k-1 \\ k & k-1 & \cdots & k-1 \end{bmatrix}$$

易见，$\min^*\{\boldsymbol{D}_{E,E}\}=k-1$ 且 $\mathrm{Index}\{\boldsymbol{D}_{E,E}\}=N-1$。

从而，$T_2=(k-1)N+N-1=kN-1=N_2-1$。

(2)(3)的证明类似，限于篇幅不赘述。 证毕

推论 2 当 $N<N_2$ 时，取 $e_i\equiv\lfloor N_2/N\rfloor i \bmod N_2$，则 $\boldsymbol{P}^{(0)},\boldsymbol{P}^{(1)},\cdots,\boldsymbol{P}^{(N-1)}$ 是 $(N_1\times NN_2,N,(N_1,N\cdot\lfloor N_2/N\rfloor-1))$-ZCZ 阵列偶集。

证明 由 $\boldsymbol{D}_{E,E}$ 的定义，$\boldsymbol{D}_{E,E}$ 中的元素恰好为

$$\{0,(e_i-e_j)\bmod N_2,(e_j-e_i-1)\bmod N_2 \mid 0\le i<j<N\}$$

记 $\lfloor N_2/N\rfloor=k$，由 $e_i\equiv\lfloor N_2/N\rfloor i \bmod N_2$ 知，有

$$\min^*\{\boldsymbol{D}_{E,E}\}=\min\{-k,-2k\cdots,-(N-1)k,k-1,2k-1,\cdots,(N-1)k-1\}$$

又由 $-ik=N_2-ik>(N-i)k,\ 1\le i\le N-1$，知 $\min^*\{\boldsymbol{D}_{E,E}\}=k-1$。此时，$i=N-1,\ j=0$，即 $\mathrm{Index}\{\boldsymbol{D}_{E,E}\}=N-1$。因此，$T_2=N(k-1)+N-1=Nk-1$，见定理 1。 证毕

当 $N\mid N_2$ 时，推论 2 即为推论 1 的情形(1)。但是，推论 2 更具有一般性，例如情形 $1<\gcd(N,N_2)<\min\{N,N_2\}$。例如，已知存在 1×20 最佳二进阵列偶，取 8 阶的 Hadamard 矩阵，即 $N=8,N_2=20$。由推论 2，可以得到 $(1\times 160,8,(1,15))$-ZCZ 阵列偶集。

当 $N=2$ 时，文献[10] 给出移位序列集的一种构造方法，从这个移位序列的构造方法可以看出，此时，零相关区域的大小和移位序列的条数(进而和阵列偶的个数)存在折衷的关系。关于一般情形，文献[13]给出了更多的移位序列集的构造，不过它们的表达式都比较复杂，读者可以参考相应文献，这里不再赘述。

4 结束语

通过选择适当的移位序列集，本文提出了基于交织方法的 ZCZ 阵列偶集的新的构造方法。为了计算阵列偶集的零相关区的大小，本文提出了移位序列集的差矩阵。利用差矩阵可以对已有的结果给予简单的证明，同时给出了一些新的构造。本文的方法可以平移到 ZCZ 屏蔽阵列偶集的情形，此时只须把构造中的最佳二进阵列偶换成最佳屏蔽阵列偶即可。

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.

[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.

[4] 蒋挺，毛飞，赵成林. 几乎最佳二进阵列偶理论研究[J]. 电子学报，2005, 33(10): 1817–1821.

[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] 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.

[7] Long B Q, Zhang P, and Hu J. A generalized Qs-CDMA system and the design of new sreading codes [J]. *IEEE Transactions on Vehicular Technology*, 1998, 47(6): 1268–1275.

[8] Tang X T and Fan P Z. Lower bounds on the maximum correlation of sequence set with low and zero correlation zone [J]. *Electron Letter*, 2000, 36: 551–552.

[9] Chung J H, Han Y K, and Yang K. New classes of optimal freqnency-hopping sequences by interleaving techniques [J]. *IEEE Transactions on Information Theory*, 2009, 55(12): 5783–5791.

[10] Zhang Z, Tang X H, and Gong G. A new class of sequences with zero or low correlation zone based on interleaving technique[J]. *IEEE Transactions on Information Theory*, 2008, 54(9): 4267–4273.

[11] 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.

[12] 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.

[13] Hu H and Gong G. New sequence families with zero or low correlation zone via interleaving techniques [J]. *IEEE Transactions on Information Theory*, 2010, 56(4): 1702–1712.

柯品惠： 男，1978 年生，副教授，研究兴趣包括最佳信号设计、现代密码学中的布尔函数.

王志华： 女，1983 年生，硕士生，研究兴趣为最佳信号设计.

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