第 26 卷第 7 期
2004 年 7 月

电子与信息学报
Journal of Electronics & Information Technology

Vol.26No.7
July 2004

具有良好并元相关特性的序列 [1]

贾彦国　　许成谦

(燕山大学信息工程学院　秦皇岛　066004)

摘　要：　该文对并元互补码偶族作出进一步的研究．首先提出了新的区组设计的概念——并元加族偶，然后给出了并元互补码偶族与区组设计的等价关系，应用这一等价关系给出了并元互补码偶族存在的必要条件，最后给出了并元互补码偶族的若干构造方法．

关键词：　区组设计，并元相关函数，序列

中图分类号：　TN911.2　　**文献标识码**：　A　　**文章编号**：　1009-5896(2004)07-1024-06

Families of Sequence Pairs with Good Dyadic Correlation Properties

Jia Yan-guo　　Xu Cheng-qian

(*The College of Info. Sci. & Eng., Yanshan Univ., Qinhuangda* 066004, *China*)

Abstract　This paper does more research on families of dyadic complementary codes pairs. Firstly, a new block design(dyadic addition set pairs) is presented. Secondly, the equivalent relationship between families of dyadic complementary code pairs and the new block design is given. Finally, families of dyadic complementary code pairs are constructed.

Key words　Block design, Dyadic correlation function, Sequences

1 引言

在最佳离散信号的设计过程中如何使信号的相关函数尽可能地逼近脉冲函数是一个十分重要的问题．从物理意义上讲，使相关函数逼近脉冲函数的主要目的是使我们能够很容易地将信号与它的移位信号区分开来．信号的移位是多种多样的，除了最常见的循环移位和非循环移位外，还有诸如并元移位和 Walsh 移位 [1] 等．并元移位是并元理论的基础，它也是信号变换的一种形式．并元码是基于元理论的一类并元移位数字信号，这类信号的并元相关函数为脉冲函数，它能将信号本身与其并元移位信号很好地区分开来，这些性质使得它可以在信号处理和保密通信等方面得到应用 [1−4]．文献 [5] 对二元并元码作了深入的研究，由文献 [5] 可知，二元并元码的长度只能是 2^{2t+2}(t 为非负整数)，这就限制了并元码的数量．文献 [6] 提出了并元互补码偶，并给出一些相关的性质，它不但具有与并元码类似的相关特性，而且在数量上要比并元码多得多．本文在此基础上对并元互补码偶族作出进一步的研究．首先提出了新的区组设计的概念——并元加族偶，然后给出了并元互补码偶族与区组设计的等价关系，应用这一等价关系给出了并元互补码偶族存在的必要条件，最后给出了并元互补码偶族的若干构造方法．

2 并元互补码偶族的定义

定义 1　设 $a=(a(0),a(1),\cdots,a(2^n-1))$ 和 $b=(b(0),b(1),\cdots,b(2^n-1))$ 是两个长度为 2^n 的二元序列 $a(i),b(i)=\pm1(i=0,1,\cdots,2^n-1)$．对任意 $u=0,1,\cdots,2^n-1$，若

[1] 2003-03-27 收到，　2003-08-12 改回
国家自然科学基金资助课题 (No.60272026)

$R_{(a,b)}(u)=\sum_{i=0}^{2^n-1}a(i)b(i\oplus u)$ 则称 $R_{(a,b)}(u)$ 为序列偶 (a,b) 的并元相关函数. 其中 $i\oplus u$ 为整数 i 与 u 的并元和，即若 $i=\sum_{k=0}^{n-1}i_k2^k$, $u=\sum_{k=0}^{n-1}u_k2^k$, i_k, $u_k\in\{0,1\}(k=(0,1,\cdots,n-1)$, 则$i\oplus u=\sum_{k=0}^{n-1}((i_k+u_k)\mathrm{mod}2)2^k$.

若设 $d(a,b)$ 为序列 a 与 b 的汉明距离，则由定义 1 可知 $R_{(a,b)}(0)=2^n-2d(a,b)$.

定义 2　设 $\{(a_i,b_i)|0\le i\le Q-1\}$ 是一个由 Q 个二元序列偶组成的集合，其中每个序列的长度为 2^n ，序列的每个元素为 ±1 . 若

$$\sum_{i=0}^{Q-1}R_{(a_i,b_i)}(u)=\begin{cases}Q2^n-s\sum\limits_{i=0}^{Q-1}d(a_i,b_i), & u=0\\ 0, & u\ne 0\end{cases}$$

则称 $\{(a_i,b_i)|0\le i\le Q-1\}$ 为并元相关函数互补码偶族，简称并元互补码偶族，记作

$$\mathrm{DCSPF}_Q^{2^n}(a_i,b_i)$$

3 并元互补码偶族与并元加族偶的等价关系

定义 3　设 $S=\{D_0,D_1,\cdots,D_{p-1}\}$ 和 $S'=\{D'_1,D'_2,\cdots,D'_{p-1}\}$ 为整数集 $\{0,1,\cdots,2^n-1\}$ 上的两个 P 元子集族，并且 $D_l=\{d_{l,0},d_{l,1},\cdots,d_{l,k_l-1}\}$ 是整数集 $\{0,1,\cdots,2^n-1\}$ 上的 k_l 阶子集， $D'_l=\{d'_{l,0},d'_{l,1},\cdots,d'_{l,k'_l-1}\}$ 是整数集 $\{0,1,\cdots,2^n-1\}$ 上的 k'_l 阶子集，设 $K=\{k_0,k_1,\cdots,k_{p-1}\}$ 和 $K'=\{k'_0,k'_1,\cdots,k'_{p-1}\}$ 为对应于子集族 S 和 S' 中每个子集的长度的集合. 设集合 $E=\{e_0,e_1,\cdots,e_{Q-1}\}$ ，其中 $e_l=|D_l\cap D'_l|, l=0,1,\cdots P-1$. 那么把 (S,S') 称作一个 $(2^n,K,K',E,\lambda)$ ——并元加族偶，当且仅当对于整数集 $\{0,1,\cdots,2^n-1\}$ 中任意元素 $\alpha\ne0$ ，使

$$\sum_{l=0}^{P-1}(d_{l,i}\oplus d'_{l,j})=\alpha \tag{1}$$

其中 $d_{l,i}\in D_l, d'_{l,j}\in D'_l, D_l\in S, D'_l\in S', l=0,1,\cdots,Q-1$ ，存在 λ 组 $(d_{l,i},d'_{l,j})$ 解.

定理 1　若存在 $(2^n,K,K',E,\lambda)$ ——并元加族偶 (S,S') ，则

$$\sum_{l=0}^{P-1}(k_lk'_l-e_l)=\lambda(2^n-1) \tag{2}$$

证明　从式 (1) 可知，对于等式的左侧，集合

$$\{(d_{l,i},d'_{l,j})|d_{l,i}\ne d'_{l,j},\ 0\le l\le P-1,\ 0\le i\le k_l-1,\ 0\le j\le k'_l-1\}$$

存在 $\sum_{l=0}^{P-1}(k_lk'_l-e_l)$ 个元素；对于等式的右侧，任意 $\alpha\in(1,2,\cdots,2^n)$ 存在 λ 组解，则对于所有的 α 存在有 $\lambda(2^n-1)$ 个解，所以等式 (2) 成立.　　证毕

定义 4　设 $\{(a_i,b_i)|0\le i\le Q-1\}$ 是一个由 Q 个二元序列偶组成的集合，其中 $\{a_i=(a_i(0),a_i(1),\cdots,a_i(2^n-1))|0\le i\le Q-1\}$ 和 $\{b_i=(b_i(0),b_i(1),\cdots,b_i(2^n-1))|0\le i\le Q-1\}$ 是两个由 Q 个长度为 2^n 的二元序列族， $S=\{D_0,D_1,\cdots,D_{Q-1}\}$ 和 $S'=\{D'_1,D'_2,\cdots,D'_{Q-1}\}$ 是两个由整数集 $\{0,1,\cdots,2^n-1\}$ 的 Q 个子集组成的子集族，其中 $D_l=\{d_{l,0},d_{l,1},\cdots,d_{l,k_l-1}\}$,

$D'_l=\{d'_{l,0},d'_{l,1},\cdots,d'_{k'_l-1}\}$ ， $l=0,1,\cdots,Q-1$. 若存在 $a_i(j)=\begin{cases}-1, & j\in D_l\\ +1, & j\notin D_l\end{cases}$ ， $b_i(j)=\begin{cases}-1, & j\in D'_l\\ +1, & j\notin D'_l\end{cases}$ ，则称 $\{(a_i,b_i)|0\le i\le Q-1\}$ 为子集偶族 (S,S') 的特征序列族，子集偶族 (S,S') 为二元序列偶族 $\{(a_i,b_i)|0\le i\le Q-1\}$ 的关联区组设计.

定理 2 二元序列偶族 $\{(a_i,b_i)|0\le i\le Q-1\}$ $(a_i,b_i$ 为长度为 2^n 的二元序列) 的关联区组设计 (S,S') 是 $(2^n,K,K',E,\lambda)$ ——并元加族偶的充分必要条件为

$$Q2^n-2\sum_{i=0}^{Q-1}(k_i+k'_i-2\lambda)=0$$

证明 设 $a_i(j)=1-2c_i(j),\ b_i(j)=1-2c'_i(j)$ ，则 $a_i(j)=\begin{cases}-1, & j\in D_l\\ +1, & j\notin D_l\end{cases}$, $b_i(j)=\begin{cases}-1, & j\in D'_l\\ +1, & j\notin D'_l\end{cases}$ 等价于 $c_i(j)=\begin{cases}1, & j\in D_l\\ 0, & j\notin D_l\end{cases}$, $c'_i(j)=\begin{cases}1, & j\in D'_l\\ 0, & j\notin D'_l\end{cases}$. 因为

$$\sum_{i=0}^{Q-1}R_{(a_i,b_i)}(u)=\sum_{i=0}^{Q-1}\sum_{j=0}^{2^n-1}(1-2c_i(j)-2c'_i(j\oplus u)+4c_i(j)c'_i(j\oplus u)) \tag{3}$$

当 $u=0$ 时，显然式 (3) $\sum_{i=0}^{Q-1}R_{(a_i,b_i)}(u)=P2^n-2\sum_{i=0}^{p-1}d(a_i,b_i)$. 当 $u\ne 0$ 时，由于 $\{(a_i,b_i)|0\le i\le Q-1\}$ 是二元序列偶族，那么式 (3) 成为

$$\sum_{i=0}^{Q-1}R_{(a_i,b_i)}(u)=Q2^n-2\sum_{i=0}^{Q-1}(k_i+k'_i)-2k_ik'_i-2\lambda)=0$$ 证毕

定理 3 若存在并元互补码偶族 $\mathrm{DCSPF}_Q^{2^n}(a_i,b_i)$ ，设 k_i 为序列 a_i 中 -1 的个数，设 k'_i 为序列 b_i 中 -1 的个数， $i=0,1,\cdots,Q-1$ ，则

$$Q2^n(2^n-1)=2\sum_{i=0}^{Q-1}=2^n(k_i+k'_i)-2k_ik'_i$$

证明 若存在并元互补码偶族 $\mathrm{DCSPF}_Q^{2^n}(a_i,b_i)$ ，则有

$$\sum_{i=0}^{Q-1}R_{(a_i,b_i)}(u)=\begin{cases}Q2^n-2\sum\limits_{i=0}^{Q-1}d(a_i,b_i), & u=0\\ 0, & u\ne 0\end{cases}$$

其中 $d(a_i,b_i)$ 为序列 a_i 与 b_i 的汉明距离，那么 $\sum_{u=1}^{2^n-1}\sum_{i=0}^{Q-1}R_{(a_i,b_i)}(u)=0$ ，由于 $R_{(a_i,b_i)}(u)=0$ 是有 2^n 个值为“ $+1$ ”或“ -1 ”项的积组成. 因此 $\sum_{u=1}^{2^n-1}\sum_{i=0}^{Q-1}R_{(a_i,b_i)}(u)=0$ 是由 $Q2^n(2^n-1)$ 个值为“ $+1$ ”或“ -1 ”的积组成. 由于 $\sum_{u=1}^{2^n-1}\sum_{i=0}^{Q-1}R_{(a_i,b_i)}(u)=0$ ，因此在 $\sum_{u=1}^{2^n-1}\sum_{i=0}^{Q-1}R_{(a_i,b_i)}(u)$ 中有 $Q2^n(2^n-1)/2$ 个积为“ -1 ”. 因此在 $\sum_{i=0}^{Q-1}R_{(a_i,b_i)}(u)$ 中值为“ -1 ”的积的个数为

$$k_i(2^n-k'_i)+(2^n-k_i)k'_i=2^n(k_i+k'_i)-2k_ik'_i$$

所以在 $\sum_{u=1}^{2^n-1}\sum_{i=0}^{Q-1}R_{(a_i,b_i)}(u)$ 中值为“ -1 ”的积的个数为 $\sum_{i=0}^{Q-1}2^n(k_i+k_i')-2k_ik_i'$. 这样有

$$Q2^n(2^n-1)=2\sum_{i=0}^{Q-1}2^n(k_i+k_i')-2k_ik_i'$$ 证毕

定义 5 若并元互补码偶族 $\mathrm{DCSPF}_Q^{2^n}(a_i,b_i)$ 中，每个 a_i, b_i 中 -1 的个数相同，则称 $\mathrm{DCSPF}_Q^{2^n}(a_i,b_i)$ 为并元等重互补码偶族.

定理 4 若存在并元等重互补码偶族 $\mathrm{DCSPF}_Q^{2^n}(a_i,b_i)$ ，则 n 为偶数，序列 a_i, b_i 中“ -1 ”的个数 $k=2^{n/2-1}(2^{n/2}\pm1)$.

证明 由定理 3 可知 $Q2^n(2^n-1)=Q4k(2^n-k)$ ，解方程有

$$2^n=\frac{1}{2}(4k+1\pm\sqrt{8k+1}) \tag{4}$$

因为 2^n 为整数，所以 $\sqrt{8k+1}$ 为奇数. 设

$$\sqrt{8k+1}=2t+1 \tag{5}$$

由式 (4), (5) 得

$$2^n=\frac{1}{2}(2t(t+1)+1\pm(2t+1))=\begin{cases}t^2\\(t+1)^2\end{cases}$$

所以 n 必为偶数. 若 $2^n=t^2$ ，则 $t=2^{n/2}$ ，将其带入式 (5) 得 $k=2^{n/2-1}(2^{n/2}+1)$. 若 $2^n=(t+1)^2$ ，则同理得 $k=2^{n/2-1}(2^{n/2}+1)$ ，这样 $k=2^{n/2-1}(2^{n/2}\pm1)$ 证毕

4 并元互补码偶族的构造方法

定义 6 设 $a=(a(0),a(1),\cdots,a(2^n-1))$ 是长度为 N 的二元序列，那么

(1) $-a=(-a(0),-a(1),\cdots,-a(2^n-1))$;

(2) $Fa=(F(a)(0),F(a)(1),\cdots,F(a)(2^n-1))$ 满足条件：

$$F(a)(j)=a(2^n-1-j),\qquad j=0,1,\cdots,2^n-1$$

(3) $L(a)=(L(a)(0),L(a)(1),\cdots,L(a)(2^n-1))$ 满足条件：

$$L(a)(j)=\begin{cases}a(j), & j=0\bmod2\\a(j-1), & j=1\bmod2\end{cases},\qquad j=0,1,\cdots,2^n-1$$

(4) $T^{(s)}(a)=(T^{(s)}(a)(0),T^{(s)}(a)(1),\cdots,T^{(s)}(a)(2^n-1))$ 满足条件：

$$T^{(s)}(a)(j)=a(s\oplus j),\qquad j=0,1,\cdots,2^n-1$$

(5) $D(a)=(D(a)(0),D(a)(1),\cdots,D(a)(2^n-1))$ 满足条件：

$$D(a)(j)=(-1)^ja(j),\qquad j=0,1,\cdots,2^n-1$$

定理 5 设 $\{(a_i,b_i)|0\le i\le Q-1\}$ 是一个 $\mathrm{DCSPF}_Q^{2^n}(a_i,b_i)$ ，那么

(1) $\{(-a_i,-b_i)|0\le i\le Q-1\}$, $\{(a_i,-b_i)|0\le i\le Q-1\}$, $\{(-a_i,b_i)|0\le i\le Q-1\}$ 是 $\mathrm{DCSPF}_Q^{2^n}(a_i,b_i)$；

(2) $\{(b_i,a_i)|0\le i\le Q-1\}$ 是一个 $\mathrm{DCSPF}_Q^{2^n}$；

(3) $\{(F(a_i),F(b_i))|0\le i\le Q-1\}$ 是一个 $\mathrm{DCSPF}_Q^{2^n}$；

(4) $\{(L(a_i),L(b_i))|0\le i\le Q-1\}$ 是一个 $\mathrm{DCSPF}_Q^{2^n}$；

(5) $\{(T^{(s)}(a_i),T^{(s)}(b_i))|0\le i\le Q-1\}$ 是一个 $\mathrm{DCSPF}_Q^{2^n}$；

(6) $\{(D(a_i),D(b_i))|0\le i\le Q-1\}$ 是一个 $\mathrm{DCSPF}_Q^{2^n}$．

证明　由定义 4 可直接得出．

定义 7　设两个并元互补码偶族 $\mathrm{DCSPF}_Q^{2^n}(a_i,b_i)$, $\mathrm{DCSPF}_Q^{2^n}(c_i,d_i)$，若对任意 $u\in\{0,1\}^{2^n}$ 有 $\sum_{i=0}^{Q-1}R_{(a_i,d_i)}(u)=0$，且 $\sum_{i=0}^{Q-1}R_{(b_i,c_i)}(u)=0$，则称 $\mathrm{DCSPF}_Q^{2^n}(a_i,b_i)$, $\mathrm{DCSPF}_Q^{2^n}(c_i,d_i)$ 为并元互补码偶侣．

并元互补码偶侣很容易由下面的定理构造出．

定理 6　设存在 $\mathrm{DCSPF}_Q^{2^n}(a_i,b_i)$，其中 $2|Q$．令 $z_{2k}=-a_{2k+1}$, $z_{2k+1}=a_{2k}$, $w_{2k}=-b_{2k+1}$, $w_{2k+1}=b_{2k}$, 则 $\{(w_i,z_i)|0\le i\le Q-1\}$ 为并元互补码偶族，$\mathrm{DCSPF}_Q^{2^n}(a_i,b_i)$ 与 $\mathrm{DCSPF}_Q^{2^n}(w_i,z_i)$ 为并元互补码偶侣．

证明　根据定义 7 可直接得出．

下面给出通过并元互补码偶侣构造高阶并元互补码偶族的方法．

定义 8　设 $x=(x(0),x(1),\cdots,x(N-1))$ 为长度为 N 的二元码，$\boldsymbol{A}=[a(i,j)]$ 为 $N_1\times N_2(N_1N_2=N)$ 阶矩阵，若 $a(i,j)=x(iN_2+j)$, $(0\le i\le N_1-1, 0\le j\le N_2-1)$，则称 $\boldsymbol{A}$ 为 x 的 $N_1\times N_2$ 阶矩阵表示形式，称 x 为矩阵 $\boldsymbol{A}$ 所表示的二元码．

定理 7　设 $\mathrm{DCSPF}_Q^{2^n}(a_i,b_i)$ 与 $\mathrm{DCSPF}_Q^{2^n}(c_i,d_i)$ 为并元互补码偶侣，$N_1\times N_2(N_1N_2=2^n)$ 阶矩阵 $\boldsymbol{A}_i=[a_i(j,k)]$, $\boldsymbol{B}_i=[b_i(j,k)]$, $\boldsymbol{C}_i=[c_i(j,k)]$, $\boldsymbol{D}_i=[d_i(j,k)]$ 分别为 a_i, b_i, c_i, d_i 的矩阵表示形式；$\overline{\boldsymbol{A}}_i=[-a_i(j,k)]$, $\overline{\boldsymbol{B}}_i=[-b_i(j,k)]$, $\overline{\boldsymbol{C}}_i=[-c_i(j,k)]$, $\overline{\boldsymbol{D}}_i=[-d_i(j,k)]$; 则

(1) 矩阵族 $\left\{\begin{bmatrix}\boldsymbol{A}_i\\ \boldsymbol{C}_i\end{bmatrix}|0\le i\le Q-1\right\}$ 和 $\left\{\begin{bmatrix}\boldsymbol{B}_i\\ \boldsymbol{D}_i\end{bmatrix}|0\le i\le Q-1\right\}$ 所表示的码偶族为 $\mathrm{DCSPF}_Q^{2^{n+1}}$

(2) 矩阵族 $\{[\boldsymbol{A}_i\boldsymbol{C}_i]|0\le i\le Q-1\}$ 和 $\{[\boldsymbol{B}_i\boldsymbol{D}_i]|0\le i\le Q-1\}$ 所表示的码偶族为 $\mathrm{DCSPF}_Q^{2^{n+1}}$;

(3) 矩阵族 $\left\{\begin{bmatrix}\boldsymbol{A}_i\\ \boldsymbol{C}_i\end{bmatrix}|0\le i\le Q-1\right\}$ 和 $\left\{\begin{bmatrix}\boldsymbol{B}_i\\ \boldsymbol{D}_i\end{bmatrix}|0\le i\le Q-1\right\}$ 所表示的码偶族为 $\mathrm{DCSPF}_Q^{2^{n+1}}$

(4) 矩阵族 $\{[\boldsymbol{A}_i\overline{\boldsymbol{C}}_i]|0\le i\le Q-1\}$ 和 $\{[\boldsymbol{B}_i\overline{\boldsymbol{D}}_i]|0\le i\le Q-1\}$ 所表示的码偶族为 $\mathrm{DCSPF}_Q^{2^{n+1}}$．

证明　由定义 8 和文献 [7] 中定理 1 可直接得出．

定理 8　设 $\mathrm{DCSPF}_Q^{2^n}(a_i,b_i)$ 与 $\mathrm{DCSPF}_Q^{2^n}(c_i,d_i)$ 为并元互补码偶侣，$N_1\times N_2(N_1N_2=2^n)$ 阶矩阵 $\boldsymbol{A}_i=[a_i(j,k)]$, $\boldsymbol{B}_i=[b_i(j,k)]$, $\boldsymbol{C}_i=[c_i(j,k)]$, $\boldsymbol{D}_i=[d_i(j,k)]$ 分别为 a_i, b_i, c_i, d_i 的矩阵表示形式，$\overline{\boldsymbol{A}}_i=[-a_i(j,k)]$, $\overline{\boldsymbol{B}}_i=[-b_i(j,k)]$, $\overline{\boldsymbol{C}}_i=[-c_i(j,k)]$, $\overline{\boldsymbol{D}}_i=[-d_i(j,k)]$．当 $0\le i\le Q-1$ 时，$Z_i^+=[\boldsymbol{A}_i\boldsymbol{C}_i]$, $W_i^+=[\boldsymbol{B}_i\boldsymbol{D}_i]$, $Z_i^-=[\overline{\boldsymbol{A}}_i\boldsymbol{C}_i]$, $W_i^-=[\overline{\boldsymbol{B}}_i\boldsymbol{D}_i]$, $S_i^+=[\boldsymbol{C}_i\boldsymbol{A}_i]$, $T_i^+=[\boldsymbol{D}_i\boldsymbol{B}_i]$, $S_i^-=[\overline{\boldsymbol{C}}_i\boldsymbol{A}_i]$, $T_i^-=[\overline{\boldsymbol{D}}_i\boldsymbol{B}_i]$；当 $Q\le i\le 2Q-1$ 时，$Z_i^+=[\boldsymbol{A}_{i-Q}\overline{\boldsymbol{C}}_{i-Q}]$, $W_i^+=[\boldsymbol{B}_{i-Q}\overline{\boldsymbol{D}}_{i-Q}]$, $Z_i^-=[\overline{\boldsymbol{A}}_{i-Q}\boldsymbol{C}_{-Qi}]$, $W_i^-=[\overline{\boldsymbol{B}}_{i-Q}\boldsymbol{D}_{i-Q}]$, $S_i^+=[\boldsymbol{C}_{i-Q}\overline{\boldsymbol{A}}_{i-Q}]$, $T_i^+=[\boldsymbol{D}_i\overline{\boldsymbol{B}}_{i-Q}]$, $S_i^-=[\boldsymbol{C}_{i-Q}\boldsymbol{A}_{i-Q}]$, $T_i^-=[\boldsymbol{D}_{i-Q}\boldsymbol{B}_{i-Q}]$，则矩阵偶族 $\{(Z_i^+,W_i^+)|0\le i\le 2Q-1\}$, $\{(Z_i^+,W_i^+)|0\le i\le 2Q-1\}$, $\{(Z_i^-,W_i^-)|0\le i\le 2Q-1\}$, $\{(S_i^+,T_i^+)|0\le i\le 2Q-1\}$，

$\{(S_i^-, T_i^-)|0 \le i \le 2Q-1\}$ 所表示的码偶族为 $\mathrm{DCSPF}_{2Q}^{2^{n+1}}$，并且前两个所表示的码偶族互为并元互补码偶侣，后两个所表示的码偶族互为并元互补码偶侣.

证明 根据定义 7 及定理 7 可直接得出.

参 考 文 献

[1] 哈尔姆斯 HF 著，张其善译．序率理论基础与应用．北京：人民邮电出版社，1980: 340–420.

[2] AhamedN 等著，胡正名等译．数字信号处理中的正交变换．北京：人民邮电出版社，1979: 210–290.

[3] 胡正名．矩阵方法．北京：人民邮电出版社，1986: 442–491.

[4] 胡正名，杨义先．并元码的进一步研究． 通信学报, 1989, 10(5): 42–46.

[5] 许成谦，杨义先，胡正名．并元加集与二元并元码． 通信学报, 1996, 17(5): 49–55.

[6] 许成谦．单值并元相关函数互补码偶的研究． 系统工程与电子技术. 2001, 23(11): 25–27.

[7] 许成谦，杨义先，胡正名．具有良好并元相关特性的序列族． 通信学报, 1997, 18(7): 28–33.

贾彦国： 男，1971 年生，博士生，讲师，主要研究方向：信道编码理论、密码学、扩频序列设计、软件工程.

许成谦： 男，1961 年生，教授，博士生导师，主要研究方向：信道编码理论、密码学、扩频序列设计.