Bent 互补函数偶族的充分必要条件

靳慧龙[①②] 许成谦[②]
[①](河北师范大学电子系 石家庄 050031)
[②](燕山大学信息科学与工程学院 秦皇岛 066004)

摘 要：该文在研究 Bent 互补函数偶族性质的基础上，证明了 Bent 互补函数偶族与 Hadamard 互补矩阵偶族等价关系，即 Bent 互补函数偶族的构造充分必要条件，给出了 Bent 互补函数偶族的一种构造方法。根据等价关系，该文实质上也给出了 Hadamard 互补矩阵偶族的性质、构造方法，这些表明 Bent 互补函数偶族在最佳信号设计方面有广阔的应用前景。

关键词：编码理论；Bent 函数；Bent 互补函数偶族；充要条件
中图分类号：TN911.22 **文献标识码**：A **文章编号**：1009-5896(2008)06-1397-03

The Necessary and Sufficient Condition of the Families of Bent Complementary Function Pairs

Jin Hui-long[①②] Xu Cheng-qian[②]
[①](*The Faculty of Electronic*, *Hebei Normal University*, *Shijiazhuang* 050031, *China*)
[②](*The College of Information Science and Engineering*, *Yanshan University*, *Qinhuangdao* 066004, *China*)

Abstract: Based on analysis of some characters of the families of Bent Complementary Function Pairs (BCFPF), the equivalence relations of BCFPF with the families of Hadamard complementary matrix pairs is studied. The equivalence relation is the necessary and sufficient condition for constructions of BCFPF。A sort of construction method of BCFPF is provided. The families of Hadamard complementary matrix pairs and can be constructed correspondingly by using the equivalent relationships.

Key words: Coding theory; Bent function; Families of Bent complementary function pairs; Necessary and sufficient condition

1 引言

Bent 函数是 Rothaus 于 1976 年提出[1]的一类特殊的布尔函数，人们利用 Bent 函数构造出了具有良好的循环自相关和循环互相关性质以及较大线性复杂度的最佳离散信号——Bent 序列[2]。在码分多址通信、雷达、同步等许多系统中都要求具有较低的异相自相关函数值和互相关函数值的最佳离散信号。Bent 序列被认为是这些系统理想的候选信号。文献[3]将 Bent 函数的概念做了推广，提出了 Bent 互补函数的概念，给出了 Bent 互补函数与并元互补码和 Hadamard 互补矩阵的等价关系。

近年来在最佳信号的研究中，“偶”的概念越来越体现出其本身的优良性能[4,5] 。文献[6]提出了一类新的类 Bent 函数——Bent 互补函数偶族。本文在此基础上，研究 Bent 互补函数偶族性质，证明了 Bent 互补函数偶族与 Hadamard 互补矩阵偶族的等价关系，最后给出了 Bent 互补函数偶族的一种构造方法。应用 Bent 互补函数偶族的构造方法，可以构造出许多单值并元相关函数互补码偶族。

2006-11-24 收到，2007-05-28 改回
河北省师范大学重点课程基金(123939)资助课题

2 定义

定义 1[6] 设 $\left\{f_i(x)=f_i(x_0,x_1,\cdots,x_{n-1})\middle|0\le i\le P-1\right\}$ 和 $\left\{g_i(x)=g_i(x_0,x_1,\cdots,x_{n-1})\middle|0\le i\le P-1\right\}$ 分别是容量为 P 的 n 元布尔函数族， 函数 $(-1)^{f_i(x)}$ ， $(-1)^{g_i(x)}$ 的 Walsh-Hadamard 变换分别是

$$F_i(u)=\sum_{x=0}^{2^n-1}(-1)^{x\cdot u+f_i(x)},\ G_i(u)=\sum_{x=0}^{2^n-1}(-1)^{x\cdot u+g_i(x)},\quad 0\le i\le P-1,\quad u\in\{0,1\}^n \tag{1}$$

若

$$\sum_{i=0}^{p-1}(F_i(u)G_i(u))=P2^n-2\sum_{i=0}^{P-1}d(f_i,g_i),\ u\in\{0,1\}^n \tag{2}$$

则称 $\left\{(f_i(x),g_i(x))\middle|0\le i\le P-1\right\}$ 为 Bent 互补 n 元函数偶族。记为 $\mathrm{BCFPF}_P^n(f_i(x),g_i(x))$，其中 $d(f_i,g_i)$ 表示 x 取 $0\sim 2^n-1$ 时，n 元布尔函数 $f_i(x)$ 和 $g_i(x)$ 取值序列之间的汉明距离。

注意：本文以下出现的 $d(f_i,g_i)$ 的含义与以上所述相同，文中任意向量 $\boldsymbol{x}=(x_0,x_1,\cdots,x_{n-1})$ 均满足 $\boldsymbol{x}=\sum_{j=0}^{n-1}x_j2^j$ ，即 $\boldsymbol{x}=(x_0,x_1,\cdots,x_{n-1})$ 表示二进制向量， $(-1)^{f(x)}\leftrightarrow F(u)$ 表

示 $F(u)$ 是 $(-1)^{f(x)}$ 的 Walsh-Hadamard 变换。

定义 2 设 $\boldsymbol{A}_i$ 和 $\boldsymbol{B}_i$ 是两个 $2^n\times 2^n$ 阶二维矩阵，α_j 和 β_j 分别表示 $\boldsymbol{A}_i$ 和 $\boldsymbol{B}_j$ 的第 j 行，$j=0,\cdots,2^n-1$。若 $d(\alpha_{i,0},\beta_{i,0})=d(\alpha_{i,1},\beta_{i,1})=\cdots=d(\alpha_{i,2^n-1},\beta_{i,2^n-1})=rd_i$，其中 rd_i 是常量，则称矩阵 $\boldsymbol{A}_i$ 和 $\boldsymbol{B}_i$ 互为行等距。

在定义了行等距后，本文利用矩阵中存在的这种性质，给出了下面的定义，另外需要说明的是本文以下出现的 rd_i 的含义如定义 2。

定义 3 设 $\{\boldsymbol{A}_i=[a_i(x,y)]|0\le x,y\le 2^n-1,\ a_i(x,y)=\pm 1,\ 0\le i\le P-1\}$ (3)

$\{\boldsymbol{B}_i=[b_i(x,y)]|0\le x,y\le 2^n-1,\ b_i(x,y)=\pm 1,\ 0\le i\le P-1\}$ (4)

分别是容量为 $\boldsymbol{P}$ 的 $2^n\times 2^n$ 阶二维矩阵族，且 $\boldsymbol{A}_i$ 和 $\boldsymbol{B}_i$ 互为行等距，$i=0,\cdots,P-1$，若

$$\sum_{i=0}^{P-1}\boldsymbol{A}_i\boldsymbol{B}_i^{\mathrm{T}}=(P2^n-2\sum_{i=0}^{P-1}rd_i)\boldsymbol{I} \tag{5}$$

则称 $\{(\boldsymbol{A}_i,\boldsymbol{B}_i)|0\le i\le P-1\}$ 是 Hadamard 互补矩阵偶族。其中 $\boldsymbol{B}_i^{\mathrm{T}}$ 表示矩阵 $\boldsymbol{B}_i$ 的转置，$\boldsymbol{I}$ 表示 $2^n\times 2^n$ 阶单位矩阵。

定义 4 设 $[h(l,j)]$ 是 $p\times r$ 阶矩阵，若 $\sum_{l=0}^{p-1}h(l,i)\cdot h(l,j)=0$，则称 $[h(l,j)]$ 的两列 $h(l,i)$ 和 $h(l,j)$ 是正交的，其中 $0\le i,j\le r-1, i\ne j$。

3 Bent 互补函数偶族的性质

可证得，若 $\{(f_i(x),g_i(x))|0\le i\le P-1\}$ 是一个 $\mathrm{BCFPF}_P^n(f_i(x),g_i(x))$，则函数偶族作下列变换后，所得仍为 Bent 互补 n 元函数偶族。

(1) $f_i^l(x)=a_n+a\cdot x+f_i(x)$，$g_i^l(x)=a_n+a\cdot x+g_i(x)$，$i=0,\cdots,P-1$，则 $\{(f_i^l(x),\ g_i^l(x))|0\le i\le P-1\}$ 是 Bent 互补 n 元函数偶族。其中 $a_n\in\{0,1\}$，$a=(a_0,a_1,\cdots,a_{n-1})\in\{0,1\}^n$。

(2) $f_i^{<s>}(x)=f_i(x\oplus s)$，$g_i^{<s>}(x)=g_i(x\oplus s)$，$i=0,\cdots,P-1$，$s=0,\cdots,2^n-1$，那么 $\{(f_i^{\langle s\rangle}(x),g_i^{\langle s\rangle}(x)|0\le i\le P-1,\ 0\le s\le 2^n-1\}$ 也是一个 Bent 互补 n 元函数偶族。

(3) $\boldsymbol{A}$ 为 $n\times n$ 阶可逆的 0、1 矩阵，$\boldsymbol{B}$ 为任意 n 维 0、1 向量，则设 $f_i^e(x)=f_i(x\boldsymbol{A}+\boldsymbol{B})$，$g_i^e(x)=g_i(x\boldsymbol{A}+\boldsymbol{B})$，$i=0,1\cdots,P-1$，那么 $\{(f_i^e(x),g_i^e(x))|0\le i\le P-1\}$ 也是一个 Bent 互补 n 元函数偶族。

(4) $\overline{f}_i(x)=f_i(x)\oplus 1$，$i=0,\cdots,P-1$，则 $\{(\overline{f}_i(x),g_i(x)|0\le i\le P-1\}$ 也是一个 Bent 互补 n 元函数偶族。

(5) $\overline{g}_i(x)=g_i(x)\oplus 1$，$i=0,\cdots,P-1$，则 $\{(f_i(x),\overline{g}_i(x))|0\le i\le P-1\}$ 是一个 Bent 互补 n 元函数偶族。

(6) $\overline{f}_i(x)=f(x)\oplus 1$，$\overline{g}_i(x)=g(x)\oplus 1$，$i=0,\cdots,P-1$，则 $\{(\overline{f}_i(x),\overline{g}_i(x))\ |0\le i\le P-1\}$ 是一个 Bent 互补 n 元函数偶族。

4 Bent 互补函数偶族的充分必要条件

定理 1 设 $\{f_i(x)=f_i(x_0,x_1,\cdots,x_{n-1})|0\le i\le P-1\}$ 和 $\{g_i(x)=g_i(x_0,x_1,\cdots,x_{n-1})|0\le i\le P-1\}$ 分别是 n 元布尔函数族，其中 $p=2^n$；$\{\boldsymbol{A}_i|0\le i\le P-1\}$，$\{\boldsymbol{B}_i|0\le i\le P-1\}$ 分为 $2^n\times 2^n$ 阶二维矩阵族，其中 $\{\boldsymbol{A}_i=[a_i(x,y)]=|(-1)^{f_i(x\oplus y)}|\ |0\le i\le P-1\}$，$\{\boldsymbol{B}_i=[b_i(x,y)]=|(-1)^{g_i(x\oplus y)}|\ |0\le i\le P-1\}$，那么 $\{(f_i(x),g_i(x))|0\le i\le P-1\}$ 为 Bent 互补 n 元函数偶族的充分必要条件是：$\{(\boldsymbol{A}_i,\boldsymbol{B}_i)|0\le i\le P-1\}$ 是 Hadamard 互补矩阵偶族。

证明 设 $f_i(x)\leftrightarrow F_i(u)$，$g_i(x)\leftrightarrow G_i(u)$。

必要性：因为 $\{(f_i(x),g_i(x))|0\le i\le P-1\}$ 是一个 Bent 互补 n 元函数偶族，所以 $\sum_{i=0}^{p-1}(F_i(u)G_i(u))=P2^n-2\cdot\sum_{i=0}^{P-1}d(f_i,g_i)$。

设 $\phi(y)=\sum_{i=0}^{P-1}\sum_{x=0}^{2^n-1}(-1)^{f_i(x)+g_i(x\oplus y)}$，对 $\phi(y)$ 作 Walsh-Hadamard 变换有

$$\begin{aligned}\phi(u)&=\sum_{y=0}^{2^n-1}(-1)^{u\cdot y}\phi(y)\\&=\sum_{y=0}^{2^n-1}(-1)^{u\cdot y}\sum_{i=0}^{P-1}\sum_{x=0}^{2^n-1}(-1)^{f_i(x)+g_i(x\oplus y)}\\&=\sum_{i=0}^{P-1}\sum_{x=0}^{2^n-1}(-1)^{f_i(x)+u\cdot x}\sum_{y=0}^{2^n-1}(-1)^{g_i(x\oplus y)+u\cdot(x\oplus y)}\\&=\sum_{i=0}^{p-1}(F_i(u)G_i(u))\\&=P2^n-2\sum_{i=0}^{P-1}d(f_i,g_i)\end{aligned} \tag{6}$$

对 $\phi(u)$ 作 Walsh-Hadamard 逆变换有

$$\begin{aligned}\phi(y)&=(1/2^n)\sum_{u=0}^{2^n-1}(-1)^{u\cdot y}\phi(u)\\&=\left(\left(P2^n-2\sum_{i=0}^{P-1}d(f_i,g_i)\right)/2^n\right)\sum_{u=0}^{2^n-1}(-1)^{u\cdot y}\\&=\left(P2^n-2\sum_{i=0}^{P-1}d(f_i,g_i)\right)\delta(y)\end{aligned} \tag{7}$$

即

$$\begin{aligned}\phi(y)&=\sum_{i=0}^{P-1}\sum_{x=0}^{2^n-1}(-1)^{f_i(x)+g_i(x\oplus y)}\\&=\left(P2^n-2\sum_{i=0}^{P-1}d(f_i,g_i)\right)\delta(y)\end{aligned} \tag{8}$$

其中 $\delta(y)=\begin{cases}1, & y=0\\0, & y\ne 0\end{cases}$，$\sum_{i=0}^{P-1}\boldsymbol{A}_i\boldsymbol{B}_i^{\mathrm{T}}=\left(P2^n-2\sum_{i=0}^{P-1}\cdot d(f_i,g_i)\right)\boldsymbol{I}=\left(P2^n-2\sum_{i=0}^{P-1}rd_i\right)\boldsymbol{I}$。

充分性：因为 $\{(\boldsymbol{A}_i,\boldsymbol{B}_i)|0\le i\le P-1\}$ 是 Hadamard 互补矩阵偶族，所以 $\sum_{i=0}^{P-1}\boldsymbol{A}_i\boldsymbol{B}_i^{\mathrm{T}}=\left(P2^n-2\sum_{i=0}^{P-1}rd_i\right)\boldsymbol{I}=\left(P2^n-2\sum_{i=0}^{P-1}d(f_i,g_i)\right)\boldsymbol{I}$。

即

$$\begin{aligned}&\sum_{i=0}^{P-1}\sum_{x=0}^{2^n-1}(-1)^{f_i(x)+g_i(x\oplus y)}\\&\quad=\left(P2^n-2\sum_{i=0}^{P-1}d(f_i,g_i)\right)\delta(y)\end{aligned} \tag{9}$$

对上式两端作 Walsh-Hadamard 变换有

$$\begin{aligned}\text{左边}&=\sum_{y=0}^{2^n-1}(-1)^{u\cdot y}\sum_{i=0}^{P-1}\sum_{x=0}^{2^n-1}(-1)^{f_i(x)+g_i(x\oplus y)}\\&=\sum_{i=0}^{P-1}\sum_{x=0}^{2^n-1}(-1)^{f_i(x)+u\cdot x}\sum_{y=0}^{2^n-1}(-1)^{g_i(x\oplus y)+u\cdot(x\oplus y)}\\&=\sum_{i=0}^{p-1}(F_i(u)G_i(u))\end{aligned}\tag{10}$$

$$\begin{aligned}\text{右边}&=\sum_{y=0}^{2^n-1}(-1)^{u\cdot y}\left(P2^n-2\sum_{i=0}^{P-1}d(f_i,g_i)\right)\delta(y)\\&=P2^n-2\sum_{i=0}^{P-1}d(f_i,g_i)\end{aligned}\tag{11}$$

所以 $\sum_{i=0}^{p-1}(F_i(u)G_i(u))=P2^n-2\sum_{i=0}^{P-1}d(f_i,g_i)$，即 $\{(f_i(x),g_i(x))|0\le i\le P-1\}$ 为 Bent 互补 n 元函数偶族。　　证毕

5　Bent 互补函数偶族的构造

除了用性质(1)− 性质(6)由已知 Bent 互补函数偶族构造新的 Bent 互补函数偶族外，本节给出另外一种 Bent 互补函数偶族的构造方法。

定理 2　若 $\{(f_i(x),g_i(x))|0\le i\le P-1\}$ 是一个 Bent 互补 n 元函数偶族，其中 P=2^r，$\boldsymbol{H}=[(j,i)]$ 是 $Q\times P$ 阶列正交(1，−1)二元阵列，设 $s_j(z)=\left(\otimes\prod_{i=0}^{P-1}\left(\frac{1-h(j,i)}{2}\right)\oplus f_i\right)(z)$，$t_j(z)=\left(\otimes\prod_{i=0}^{P-1}\left(\frac{1-h(j,i)}{2}\right)\oplus g_i\right)(z)$，$i=0,1,\cdots,P-1$，$j=0,1,\cdots,Q-1$，那么 $\{(s_j(z),\ t_j(z))|0\le j\le Q-1\}$ 是一个 Bent 互补 n+r 元函数偶族。

证明　设 $x=(x_0,\cdots,x_{n-1})\in\{0,1\}^n$，$i=(i_0,\cdots,i_{r-1})\in\{0,1\}^r$，并且 $z=(z_0,\cdots,z_{n+r-1})\in\{0,1\}^{n+r}$，$z$ 的分量是由 x 和 i 的分量任意排列而成，$v=(v_0,\cdots,v_{n+r-1})\in\{0,1\}^{n+r}$，$v'\in\{0,1\}^n$，$v''\in\{0,1\}^r$，$v'$ 和 v'' 是以 x 和 i 合成 z 相同的方法合成 v，$(-1)^{s_j(z)}\leftrightarrow S_j(v)$，$(-1)^{t_j(z)}\leftrightarrow T_j(v)$，$j=0,\cdots,Q-1$，$(-1)^{f_i(x)}\leftrightarrow F_i(v')$，$(-1)^{g_i(x)}\leftrightarrow G_i(v')$，$i=0,\cdots,P-1$，则

$$\begin{aligned}S_j(v)&=\sum_{z\in\{0,1\}^{n+r}}(-1)^{v\cdot z+s_j(z)}\\&=\sum_{i=0}^{2^r-1}\sum_{x=0}^{2^n-1}(-1)^{v''i+v'x+\left(\frac{1-h(j,i)}{2}\right)+f_i(x)}\\&=\sum_{i=0}^{2^r-1}(-1)^{v''i}h(j,i)F_i(v')\end{aligned}\tag{12}$$

$$\begin{aligned}T_j(v)&=\sum_{z\in\{0,1\}^{n+r}}(-1)^{vz+t_j(z)}\\&=\sum_{i=0}^{2^r-1}\sum_{x=0}^{2^n-1}(-1)^{v''i+v'x+\left(\frac{1-h(j,i)}{2}\right)+g_i(x)}\\&=\sum_{i=0}^{2^r-1}(-1)^{v''i}h(j,i)G_i(v')\end{aligned}\tag{13}$$

进而有

$$\begin{aligned}&\sum_{j=0}^{Q-1}S_j(v)T_j(v)\\&=\sum_{j=0}^{Q-1}\sum_{k,l=0}^{2^r-1}(-1)^{v''(k+l)}h(j,k)h(j,l)F_k(v')G_l(v')\\&=\sum_{k,l=0}^{2^r-1}(-1)^{v''(k+l)}F_k(v')G_l(v')\sum_{j=0}^{Q-1}h(j,k)h(j,l)\end{aligned}\tag{14}$$

因为 $\boldsymbol{H}=[h(j,i)]$ 是 $Q\times P$ 阶列正交(1，−1)二元阵列，并且 $\{(f_i(x),g_i(x))|0\le i\le P-1\}$ 是一个 Bent 互补 n 元函数偶族，所以有

$$\begin{aligned}\sum_{j=0}^{Q-1}S_j(v)T_j(v)&=Q2^{n+r}-2\sum_{j=0}^{Q-1}\sum_{k=0}^{2^r-1}d(f_k,g_k)\\&=Q2^{n+r}-2\sum_{j=0}^{Q-1}d(s_j,t_j)\end{aligned}\tag{15}$$

故 $\{(s_j(z),t_j(z))|0\le j\le Q-1\}$ 是一个 Bent 互补 n+r 元函数偶族。　　证毕

从上面的定理可以得出，通过应用一个正交阵列和一个低维 Bent 互补函数偶族便能够构造出维数更高的 Bent 互补函数偶族。

6　结束语

本文研究了 Bent 互补函数偶族的性质和一些构造方法。特别是本文给出了 Bent 互补函数偶族与 Hadamard 矩阵偶族的等价关系，这样可以将对 Hadamard 矩阵偶族的研究统一为对 Bent 互补函数偶族的研究。例如本文提出的有关 Bent 互补函数偶族的构造方法可以视为 Hadamard 矩阵偶族的构造方法。

参 考 文 献

[1] Rothaus OS. On Bent functions. *J of Combin. Theory*, 1976, 20(A): 300−305.

[2] 杨义先, 许成谦, 胡正名著. 并元理论及其应用. 北京: 人民邮电出版社, 2002: 36−74.

[3] 许成谦, 杨义先, 胡正名. Bent 互补函数族的性质和构造方法. 电子学报, 1997, 25(10): 52−56.

[4] 赵晓群, 何文才, 王仲文等. 最佳二进阵列偶理论研究. 电子学报, 1999, 27(1): 34−35.

[5] 许成谦, 靳慧龙. 几乎最佳周期互补二元序列偶族. 系统工程与电子技术, 2003, 25(9): 1086−1089.

[6] 许成谦, 靳慧龙. 基于特殊阵列递归构造 Bent 互补函数偶族. 系统工程与电子技术, 2005, 27(1): 45−48.

靳慧龙：　男，1973 年生，讲师，主要从事信道编码、信号处理、DSP 等的研究.

许成谦：　男，1961 年生，教授，博士生导师，主要从事信道编码、密码学、扩频序列设计的研究.