基于特殊阵列递归构造 Bent 互补函数族 [1]

许成谦

(燕山大学信息科学与工程学院 秦皇岛 066004)

摘 要 本文进一步研究 Bent 互补函数族的构造，给出分别应用列正交矩阵和列并元最佳阵列递归地构造 Bent 互补函数族的方法.

关键词 信号设计， Bent 函数， Bent 互补函数族

中图号 TN918.1

1 引 言

若 n 元布尔函数 $f(x)$ 的 $(-1)^{f(x)}$ 的 Walsh-Hadamard 变换谱值的平方等于 2^n, 则称函数 $f(x)$ 为 Bent 函数 [1] 。 Bent 函数在密码设计，编码理论和扩频通信等领域中有重要的应用。例如由 Bent 函数构造的 Bent 序列具有良好的自相关和互相关特性，并且具有大的线性复杂度，是适合于扩频通信，特别是保密通信的理想序列 [2-5] 。在文献 [6] 中，我们将 Bent 函数的概念作了推广提出了 Bent 互补函数族的概念。由文献 [6] 可知， Bent 互补函数族具有与 Bent 函数类似的性质。但是在数量上要比 Bent 函数多得多。列正交矩阵和列并元最佳阵列都是具有特殊性质的矩阵. 文献 [5,7] 给出了很多这类矩阵。本文进一步研究 Bent 互补函数族的构造，给出了分别应用列正交矩阵和列并元最佳阵列递归地构造 Bent 互补函数族的方法。

2 定义、记号和引理

定义 1 设 $\{f_i(x)=f_i(x_0,...,x_{n-1})|0\le i\le P-1\}$ 是容量为 P 的 n 元布尔函数族，若函数 $(-1)^{f_i(x)}$ 的 Walsh-Hadamard 变换 $F_i(u),0\le i\le P-1$, 满足

$$\sum_{i=0}^{P-1}(F_i(u))^2=P2^n, u\in\{0,1\}^n,$$

则称 $\{f_i(x)|0\le i\le P-1\}$ 为 Bent 互补 n 元函数族。记为 $\mathrm{BCF}_P^n(f_i(x))$, 简记 BCF_P^n 。

在本文中， $(-1)^{f(x)}\leftrightarrow F(u)$ 表示 $F(u)$ 是 $(-1)^{f(x)}$ 的 Walsh-Hadamard 变换。 $x\oplus y$ 表示 x 和 y 的并元和 [5] 。 $x\oplus_Q y$ 表示 x 与 y 的模 Q 和。

定义 2 设 $[h(j,i)]$ 是 $P\times Q$ 阶矩阵。若对于 $0\le i,k\le Q-1$ 和 $i\ne k$,

$$\sum_{j=0}^{P-1}h(j,i)h(j,k)=0,$$

则称矩阵 $[h(j,i)]$ 为 $P\times Q$ 阶列正交矩阵。

[1] 1998-12-04 收到， 1999-06-05 定稿
国家自然科学基金和河北省自然科学基金资助课题

定义 3 设 $A=[a(i,j)]$ 是 $2^r\times 2^s$ 阶阵列，其中 r,s 为非负整数。若

$$\sum_{i=0}^{2^r-1}\sum_{j=0}^{2^s-1}a(i,j)a(i\oplus_{2^r}\sigma,j\oplus\tau)=\begin{cases}2^{r+s}, & (\sigma,\tau)=(0,0);\\ 0, & (\sigma,\tau)\neq(0,0);\end{cases}$$

则称 $A=[a(i,j)]$ 是列并元最佳阵列。

引理 1 设 $\{f_i(x)|0\le i\le 2^r-1\}$ 是 n 元布尔函数族。若 $A=[a(i,j)]=[(-1)^{f_i(j)}]$ 是 $2^r\times 2^n$ 阶列并元最佳阵列，并且 $(-1)^{f_i(x)}\leftrightarrow F_i(u),i=0,\cdots,2^r-1$，则对于 $\forall u\in\{0,1\}^n$，有

$$\sum_{i=0}^{2^r-1}F_i(u)F_{i\oplus_{2^r}\sigma}(u)=\begin{cases}2^{r+n}, & \sigma=0;\\ 0, & \sigma\neq 0.\end{cases}$$

定义 4 设 $x=(x_0,\cdots,x_{n-1})\in\{0,1\}^n$，$j=(j_0,\cdots,j_{r-1})\in\{0,1\}^r$，$z=(z_0,\cdots,z_{n+r-1})\in\{0,1\}^{n+r}$，并且 z 的分量是由 x 和 j 的分量任意排列而成。$f_0(x),f_1(x),\cdots,f_{2^r-1}(x)$ 是 2^r 个 n 元布尔函数。定义 $n+r$ 元布尔函数 $(\otimes\prod_{i=0}^{2^r-1}f_i)(z)$ 为

$$\left(\otimes\prod_{i=0}^{2^r-1}f_i\right)(z)=\begin{cases}f_0(x), & j=0;\\ f_1(x), & j=1;\\ \vdots & \\ f_{2^r-1}(x), & j=2^r-1.\end{cases}$$

设 $g(y)$ 是 m 元布尔函数，定义

$$\otimes\prod_{y=0}^{2^m-1}\prod_{i=0}^{2^r-1}(g(y)\oplus f_i)(z)=\otimes\prod_{y=0}^{2^m-1}\left(\otimes\prod_{i=0}^{2^r-1}(g(y)\oplus f_i)\right)(z).$$

3 应用列正交矩阵递归构造 Bent 互补函数族

本节我们应用列正交二元矩阵递归地构造元数更高的 Bent 互补函数族。

定理 1 $\{f_i(x)|0\le i\le P-1\}$ 是 BCF_P^n。$P=2^r$，$H=[h(j,i)]$ 是 $Q\times P$ 阶列正交 $(1,-1)$ 二元矩阵，则 $\{(\otimes\prod_{i=0}^{P-1}(\frac{1-h(j,i)}{2})\oplus f_i)(z)|0\le j\le Q-1\}$ 是 BCF_Q^{n+r}。

证明 设 $x\in\{0,1\}^n$，$i\in\{0,1\}^r$，$z=(z_0,\cdots,z_{n+r-1})\in\{0,1\}^{n+r}$，并且 z 的分量是由 x 和 i 的分量任意排列而成，$v=(v_0,\cdots,v_{n+r-1})\in\{0,1\}^{n+r}$，$v'\in\{0,1\}^n$，$v''\in\{0,1\}^r$，并且 v' 和 v'' 以 x 和 i 合成 z 相同的方法合成 v，$g_j(z)=(\otimes\prod_{i=0}^{P-1}(\frac{1-h(j,i)}{2})\oplus f_i)(z)$，$(-1)^{g_j(z)}\leftrightarrow G_j(v)$，$(-1)^{f_i(x)}\leftrightarrow F_i(v')$，$j=0,\cdots,Q-1,i=0,\cdots,P-1$，则

$$\begin{aligned}G_j(v) &= \sum_{z\in\{0,1\}^{n+r}}(-1)^{v\cdot z+g_j(z)}\\ &= \sum_{i=0}^{2^r-1}\sum_{x=0}^{2^n-1}(-1)^{v''\cdot i+v'\cdot x+(\frac{1-h(j,i)}{2})+f_i(x)}\\ &= \sum_{i=0}^{2^r-1}(-1)^{v''\cdot i}h(j,i)F_i(v').\end{aligned}$$

进而有

$$\begin{aligned}\sum_{j=0}^{Q-1} G_j^2(u) &= \sum_{j=0}^{Q-1}\sum_{k,l=0}^{2^r-1}(-1)^{v''\cdot(k+l)}h(j,k)h(j,l)F_k(v')F_l(v')\\ &= \sum_{j=0}^{Q-1}\sum_{i=0}^{2^r-1}(F_i(v'))^2\\ &+ \sum_{k,l=0,k\neq l}^{2^r-1}(-1)^{v''\cdot(k+l)}F_k(v')F_l(v')\sum_{j=0}^{Q-1}h(j,k)h(j,l).\end{aligned}$$

因为 $H=[h(j,i)]$ 是 $Q\times P$ 阶列正交 $(1,-1)$ 二元阵列，并且 $\{f_i(x)|0\le i\le P-1\}$ 是 BCF_P^n，所以上式左边第一项为 $Q2^{n+r}$，第二项为 0，即

$$\sum_{j=0}^{Q-1} G_j^2(u) = Q2^{n+r}.$$

故 $\{(\otimes\prod_{i=0}^{P-1}(\frac{1-h(j,i)}{2})\oplus f_i)(z)|0\le j\le Q-1\}$ 是 BCF_Q^{n+r} . 证毕

同理可以证明下面定理.

定理 2 $\{f_i(x),g_i(x),\cdots,h_i(x)|0\le i\le P-1\}$ 是 Bent 互补 n 元函数族. $P=2^r$,$H=[h(j,i)]$ 是 $Q\times P$ 阶列正交 $(1,-1)$ 二元阵列,则 $\{(\otimes\prod_{i=0}^{P-1}(\frac{1-h(j,i)}{2})\oplus f_i)(z),(\otimes\prod_{i=0}^{P-1}(\frac{1-h(j,i)}{2})\oplus g_i)(z),\cdots,(\otimes\prod_{i=0}^{P-1}(\frac{1-h(j,i)}{2})\oplus h_i)(z)|0\le j\le Q-1\}$ 是 Bent 互补 $n+r$ 元函数族.

定理 3 设 $\{f_0(x),f_1(x)\}$ 是 BCF_2^n，$\{g_0(y),g_1(y)\}$ 是 BCF_2^m . 若

$$h_0(z)=\left(\otimes\prod_{j=0}^{2^m-1}(g_0(j)\oplus f_0)\right)\otimes\left(\otimes\prod_{k=0}^{2^m-1}(g_1(k)\oplus f_1)\right)(z),$$

$$h_1(z)=\left(\otimes\prod_{j=0}^{2^m-1}(g_1(j)\oplus f_0)\right)\otimes\left(\otimes\prod_{k=0}^{2^m-1}(\overline{g}_0(k)\oplus f_1)\right)(z),$$

则 $\{h_0(z),h_1(z)\}$ 是 BCF_2^{n+m+1} .

证明 设 $(-1)^{f_i(x)}\leftrightarrow F_i(v')$, $(-1)^{g_i(y)}\leftrightarrow G_i(v'')$, $(-1)^{h_i(z)}\leftrightarrow H_i(v)$, i=0,1 . 因为

$$H_0(v)=\sum_{l=0}^{1}(-1)^{v'''\cdot l}F_l(v')G_l(v''),$$

$$H_1(v)=\sum_{l=0}^{1}(-1)^{v'''\cdot l+l}F_l(v')G_{1-l}(v''),$$

所以

$$\begin{aligned}H_0^2(v)+H_1^2(v) &= (F_0(v')G_0(v'')+(-1)^{v'''}F_1(v')G_1(v''))^2\\ &\quad+(F_0(v')G_1(v'')+(-1)^{v'''+1}F_1(v')G_0(v''))^2\\ &= (F_0^2(v')+F_1^2(v'))(G_0^2(v')+G_1^2(v'))\\ &= 22^n22^m=22^{n+m+1}.\end{aligned}$$

故 $\{h_0(z), h_1(z)\}$ 是 BCF_2^{n+m+1} 。 证毕

定理 3 可以作如下推广：

定理 4 设 $\{f_l(x)|0 \le l \le 2^r-1\}$ 是 $\mathrm{BCF}_{2^r}^n$, $\{g_0(y), g_1(y)\}$ 是 BCF_2^m, $H=[h(i,j)]$ 是 $(1,-1)$ 二元 $Q \times 2^r$ 阶列正交矩阵， Q 为偶数。若

$$d_i(z) = \otimes \prod_{j=0}^{2^r-1} \prod_{k=0}^{2^m-1} \left((\frac{1-h(i,j)}{2}) \oplus g_{i\oplus_2 j}(k) \oplus f_j \right)(z), 0 \le i \le Q-1,$$

则 $\{d_i(z)|0 \le i \le Q-1\}$ 是 BCF_Q^{n+m+r} 。

证明 设 $(-1)^{d_i(z)} \leftrightarrow D_i(v)$, $(-1)^{f_l(x)} \leftrightarrow F_l(v')$, $(-1)^{g_j(y)} \leftrightarrow G_j(v'')$ 。因为

$$\begin{aligned} D_i(v) &= \sum_{w=0}^{2^r-1} \sum_{y=0}^{2^m-1} \sum_{x=0}^{2^n-1} (-1)^{v'''\cdot w + v'\cdot x + v''\cdot y + f_w(x) + g_{w\oplus_2 i}(y) + (1-h(i,w))/2} \\ &= \sum_{w=0}^{2^r-1} (-1)^{u'''\cdot w} h(i,w) F_w(v') G_{w\oplus_2 i}(v'') \end{aligned}$$

和 $H=[h(i,j)]$ 是 $(1,-1)$ 二元 $Q \times 2^r$ 阶列正交矩阵，所以

$$\begin{aligned} \sum_{i=0}^{Q-1} D_i^2(v) &= \sum_{i=0}^{Q-1} \sum_{w=0}^{2^r-1} F_w^2(v') G_{w\oplus_2 i}^2(v'') \\ &= \sum_{w=0}^{2^r-1} F_w^2(v') \sum_{i=0}^{Q-1} G_{w\oplus_2 i}^2(v'') \\ &= Q 2^{n+m+r}. \end{aligned}$$

故 $\{d_i(z)|0 \le i \le Q-1\}$ 是 BCF_Q^{n+m+r} 。 证毕

4 应用列并元最佳阵列递归构造 Bent 互补函数族

下面我们应用列并元最佳阵列递归地构造 Bent 互补函数族。

定理 5 设 $\{f_i(x)|0 \le i \le 2^r-1\}$ 是 $\mathrm{BCF}_{2^r}^n$ 。若 $A=[a(i,j)]=[(-1)^{f_i(j)}]$ 是 $2^r \times 2^n$ 阶列并元最佳阵列，则 $\{(\otimes \prod_{i=0}^{2^r-1} f_{i\oplus_{2^r} j})(z)|0 \le j \le 2^r-1\}$ 是 $\mathrm{BCF}_{2^r}^{n+r}$ 。

证明 设 $g_j(z)=(\otimes \prod_{i=0}^{2^r-1} f_{i\oplus_{2^r} j})(z)$, $(-1)^{g_j(z)} \leftrightarrow G_j(v)$ 。 $z \in \{0,1\}^{n+r}$,$x \in \{0,1\}^n$,$i \in \{0,1\}^r$,z 的分量是由 x 和 i 的分量排列而成，则

$$\begin{aligned} G_j(v) &= \sum_{z\in\{0,1\}^{n+r}} (-1)^{v\cdot z + g_j(z)} \\ &= \sum_{i=0}^{2^r-1} \sum_{x=0}^{2^r-1} (-1)^{v'\cdot x + v''\cdot i + f_{i\oplus_{2^r} j}(x)} \\ &= \sum_{i=0}^{2^r-1} (-1)^{v''\cdot i} F_{i\oplus_{2^r} j}(v'). \end{aligned}$$

进而有

$$\sum_{j=0}^{2^r-1} G_j^2(v) = \sum_{l,k=0}^{2^r-1} (-1)^{v''\cdot(l\oplus k)} \sum_{j=0}^{2^r-1} F_{l\oplus_{2^r} j}(v') F_{k\oplus_{2^r} j}(v').$$

由引理 1 可知，

$$\sum_{j=0}^{2^r-1} G_j^2(v) = \sum_{k=0}^{2^r-1} (-1)^{v''\cdot(k\oplus k)} \sum_{j=0}^{2^r-1} F_{k\oplus_{2^r} j}^2(v') = 2^r 2^{n+r}.$$

故 $\{(\otimes\prod_{i=0}^{2^r-1} f_{i\oplus_{2^r} j})(z) | 0 \le j \le 2^r - 1\}$ 是 $\mathrm{BCF}_{2^r}^{n+r}$.　　证毕

参 考 文 献

[1] Rothaus O S. On Bent functions, J. of Combin. Theory, 1976, 20(A): 300-305.

[2] MacWilliams F J, Sloane N J A. The theory of error-corrorecting codes, Amsterdam, North-Holland: North-Holland Publishing Company, 1977, Chapter 14.

[3] Olsen J, Scholtz R, Welch L. Bent function sequences, IEEE Trans. on Inform. Theory, 1982, IT-28(6): 858-864.

[4] Kumar P V. Frequency-hopping code sequences designs having large linear span, IEEE Trans. on Inform. Theory, 1988, IT-34(1): 146-151.

[5] 杨义先，林须端，著. 编码密码学. 北京：人民邮电出版社，1992, 第一章，第三章.

[6] 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.

[7] Luke H, Bomer L, Antweiler M. Perfect binary array, Signal Processing, 1989, 17(1): 69-80.

RECURSIVE CONSTRUCTIONS BASED ON SPECIAL ARRAYS FOR THE FAMILIES OF BENT COMPLEMENTARY FUNCTIONS

Xu Chengqian

(*The College of Information Science and Engineering, Yanshan Univ., Qinhuangdao* 066004)

Abstract　In this paper, the constructions for the families of Bent complementary functions (BCF) are further studied. Recursive construction methods of BCFs are given by using matrices with orthogonal columns and perfect arrays.

Key words　Signal designs, Bent functions, The families of Bent complementary functions

许成谦：　男，1961 年生，副教授，主要研究方向：编码理论，密码学，扩频序列设计.