一类多输出 Bent函数的构造

刘志高[1,2], 张福泰[1], 徐 倩[1]

(1.南京师范大学 数学与计算机科学学院, 江苏 南京 210097;
2.安徽工业大学 职业技术学院, 安徽 马鞍山 243001)

[摘要] 推广了半 Bent函数的概念, 提出了多输出半 Bent函数的概念, 并由此给出了多输出 Bent函数的一种构造方法. 该方法通过级联两个多输出半 Bent函数得到多输出 Bent函数. 与原有的方法相比, 该方法具有结构简单、使用方便的优点. 用此方法可构造具有任意偶数个变元的多输出 Bent函数. 此外, 还给出了多输出半 Bent函数的一种构造方法. 除了可用于构造多输出 Bent函数外, 多输出半 Bent函数还可应用于多输出前馈网等方面.

[关键词] Bent函数, 半 Bent函数, 多输出 Bent函数, 多输出半 Bent函数, Walsh谱
[中图分类号]TN918 [文献标识码]A, [文章编号]1672-1292(2005)02-0046-04

Construction of a Class of Multi-output Bent Functions

LIU Zhigao[1,2], ZHANG Futai[1], XU Qian[1]

(1. School of Mathematics and Computer Science, Nanjing Normal University, Jiangsu Nanjing 210097, China;
2. School of Vocational Technology, Anhui University of Technology, Anhui Maanshan 243002, China)

Abstract The concept of semi-bent functions is generalized. Meanwhile, the concept of multi-output semi-bent functions is introduced. Based on the new concept, a method of constructing multi-output Bent functions is presented. In the method, a multi-output Bent function is constructed by concatenating two multi-output semi-Bent functions. Compared with the existing methods, our newly proposed method has a simple structure and is convenient to use. With this new method, multi-output Bent functions with arbitrary even variables can be constructed. Moreover, a method of constructing multi-output semi-Bent functions is proposed. Besides, applications in the construction of multi-output Bent functions, multi-output semi-Bent functions can also be applied in multi-output feedforward networks.

Key words Bent function, semi-Bent function, multi-output Bent function, multi-output semi-Bent function, Walsh spectrum

0 引言

Bent函数是由 Rothaus于 1976年提出的一类特殊的布尔函数[1]. 它在展频通信、编码理论、密码学等领域中有着广泛的应用. Bent函数的主要优点是它具有最高的非线性度和差分分布的均匀性, 用于非线性组合器可以很好的抗击相关攻击、最佳线性逼近攻击差分分析攻击. 1982年, Olsen, Scholtz和 Welch利用 Bent函数构造出一类循环相关特性很好的二进制序列(称为 Bent序列)[2], 从此, Bent函数的研究受到人们的广泛重视, 已取得了许多较深入的研究成果[1~6].

在密码设计中, 为了提高序列密码中密钥流的生成速度和分组密码的安全性, 常常采用具有良好密码性质的多输出布尔函数. 例如, 分组密码的典型代表—美国数据加密标准 DES算法的核心是 8个"S盒", 而其每一个 S盒都可以看作一个 $GF^6(2) \rightarrow GF^4(2)$的多输出布尔函数. 众所周知, S盒的构造是分组密码设计中的重要环节, 它的好坏直接影响到密码体制的安全性. 而 S盒的构造实质上就是具有良好密码性质的多输出布尔函数的构造. 多输出 Bent函数[7]就是一类具有良好密码性质的

收稿日期: 2004-11-23
基金项目: 江苏省高校自然科学研究计划重点资助项目(03KJA520066)和教育部网络与信息安全重点实验室(西安电子科技大学)开放课题资助项目.
作者简介: 刘志高(1975–), 硕士研究生, 讲师, 主要从事密码学与网络安全的学习与研究. E-mail: zhigaoliu@126.com
通讯联系人: 张福泰(1965–), 博士, 教授, 主要从事密码学与信息安全的教学与研究. E-mail: zhangfuta@njnu.edu.cn

多输出布尔函数, 它的每个分量以及各分量的所有非零线性组合都是 Bent函数. 关于多输出 Bent函数的构造, 目前已经有了一些较好的结果, Kaisa Nyberg在文献[8]中证明了 $2n$ 元多输出 Bent函数的输出维数至多是 n, 并且同时给出了一种基于 m 序列状态转移矩阵的多输出 Bent函数的构造法; 张文英等在文献[9]中运用布尔函数的谱分解式给出了二输出 Bent函数的一种构造方法; 其他一些结果参见文献[7, 10~12].

本文给出了一种构造具有任意偶数个变元的多输出 Bent函数的方法, 该方法通过级联两个多输出半 Bent函数来得到多输出 Bent函数. 由于将级联的方法应用到多输出 Bent函数的构造中, 使得该方法与文献[7~12]中的方法相比, 具有结构简单明了、使用方便的优点. 本文将半 Bent函数的概念推广, 首次提出了多输出半 Bent函数的概念. 相应地, 半 Bent函数可看作是多输出半 Bent函数的特例——单输出半 Bent函数. 进一步, 还给出了多输出半 Bent函数的一种构造方法.

1 预备知识

定义 1 设 m, n 均为正整数, $m \leqslant n$, $f_i(x)$ 为 $F_2^n \to F_2$ 的布尔函数, 则称 $f(x) = (f_1(x), \cdots, f_m(x))$ 为 $F_2^n \to F_2^m$ 的 n 元 m 输出函数.

定义 2[7] 设 $f(x)$ 是 n 元 m 输出函数, 称 $S_{(f)}(u, v) = 2^{-n}\sum_{x\in F_2^n}(-1)^{u\cdot f(x)+v\cdot x}$ 为 $f(x)$ 的广义一阶 Walsh循环谱. 其中 $u \in F_2^m$, $v \in F_2^n$.

易知, 对于固定的 u, $S_{(f)}(u, v)$ 就是布尔函数 $u\cdot f(x)$ 的一阶 Walsh 循环谱, 即 $S_{(f)}(u, v) = S_{(u\cdot f)}(v)$.

定义 3[7] 设 $f(x)$ 是 n 元 m 输出函数, 若对一切 $0 \neq u \in F_2^m$, $v \in F_2^n$ 均有 $|S_{(f)}(u, v)| = 2^{-\frac{n}{2}}$, 则称 $f(x)$ 为多输出 Bent函数.

由定义 3易得如下引理:

引理 1 n 元 m 输出函数 $f(x)$ 是多输出 Bent函数的必要条件是 n 为偶数.

引理 2 设 $f(x)$ 是 n 元 m 输出函数, 则 $f(x)$ 是多输出 Bent函数的充要条件是 $\forall 0 \neq u \in F_2^m$, $u\cdot f(x)$ 是 n 元 Bent函数.

2 一类多输出 Bent函数的构造

文[13]给出了通过级联两个半 Bent函数得到 Bent函数的方法. 本文把该方法推广, 提出了多输出半 Bent函数的概念, 给出了一类多输出 Bent函数的构造方法, 即通过级联两个多输出半 Bent函数来得到多输出 Bent函数.

为叙述方便, 现给出多输出半 Bent函数的定义.

定义 4 设 $f(x)$ 是 n 元 m 输出函数, 若对一切固定的 $u \neq 0$, $u \in F_2^m$, $\forall v \in F_2^n$ 均有 $|S_{(f)}(u, v)| = 0$ 或 $2^{-\frac{n+1}{2}}$, 则称 $f(x)$ 为多输出半 Bent函数.

由定义 4易得如下结论:

结论 1 n 元 m 输出函数 $f(x)$ 是多输出半 Bent函数的必要条件是 n 为奇数.

结论 2 设 $f(x)$ 是 n 元 m 输出函数, 则 $f(x)$ 是多输出半 Bent函数的充要条件是 $\forall 0 \neq u \in F_2^m$, $u\cdot f(x)$ 是 n 元半 Bent函数.

设 $n = 2k$, 记 $X_1 = (x_1, x_2, \cdots, x_{n-1})$, $X = (X_1, x_n)$, 设 $g_1(X_1)$ 和 $g_2(X_1)$ 均是 $n-1$ 元布尔函数, 令

$$f(X) = g_1(X_1)(x_n + 1) + g_2(X_1)x_n \quad (1)$$

引理 3[13] 若 $g_1(X_1)$ 和 $g_2(X_1)$ 均是 $n-1$ 元半 Bent函数, 且 $\mathrm{supp}S_{(g_1)} \cap \mathrm{supp}S_{(g_2)} = \Phi$, 则由 (1) 式构造的 $f(X)$ 是 n 元 Bent函数.

设 $G_1(X_1)$ 和 $G_2(X_1)$ 均是 $n-1$ 元 m 输出函数, 令

$$F(X) = G_1(X_1)(x_n + 1) + G_2(X_1)x_n \quad (2)$$

定理 1 若 $G_1(X_1)$ 和 $G_2(X_1)$ 均是 $n-1$ 元多输出半 Bent函数, 且 $\forall 0 \neq u \in F_2^m$, $\mathrm{supp}S_{(uG_1)} \cap \mathrm{supp}S_{(uG_2)} = \Phi$, 则由 (2) 式构造的 $F(X)$ 是 n 元多输出 bent函数.

证明 因为 $G_1(X_1)$ 和 $G_2(X_1)$ 均是 $n-1$ 元多输出半 Bent函数, 所以, 由结论 4可知, $\forall 0 \neq u \in F_2^m$, $u\cdot G_1(X_1)$ 和 $u\cdot G_2(X_1)$ 均是 $n-1$ 元半 Bent函数. 而 $u\cdot F(X) = (u\cdot G_1(X_1))(x_n + 1) + (u\cdot G_2(X_1))x_n$, 即 $u\cdot F(X)$ 可看成是由 $u\cdot G_1(X_1)$ 和 $u\cdot G_2(X_1)$ 级联而成的. 又因为 $\forall 0 \neq u \in F_2^m$, $\mathrm{supp}S_{(uG_1)} \cap \mathrm{supp}S_{(uG_2)} = \Phi$, 所以, 由引理 3可得, $\forall 0 \neq u \in F_2^m$, $u\cdot F(X)$ 是 n 元 Bent函数. 再由引理 2知, $F(X)$ 是 n 元多输出 bent函数.

文[13]中指出引理 3的逆命题也成立, 则由上述证明过程易得, 定理 1的逆命题也成立.

3 一类多输出半 Bent函数的构造

文[13]给出了一类半 Bent函数的构造方法, 具体如下:

设 n 是奇数, $n = 2k-1$, 构造 n 元半 Bent函数如下, 令 $X_1 = (x_1, x_2, \cdots, x_{k-1})$, $X_2 = (x_k, x_{k+1},$

…, x_n), $X = (X_1, X_2)$, 再令 τ 是 $F_2^{k-1} \to F_2^k$ 的单射, $\tau(X_1) = (\tau_1(X_1), \cdots, \tau_k(X_1))$, 其中 τ_i 是 $k-1$ 元布尔函数. 令

$$f(X) = \tau(X_1) \cdot X_2 = \tau_1(X_1)\, x_k + \tau_2(X_1)\, x_{k+1} + \cdots + \tau_k(X_1)\, x_{2k-1} \quad (3)$$

引理 **4**[13]　由(3)式定义的 $f(X)$ 是 n 元半 bent函数, 并且

$$|S_{(f)}(W)| = \begin{cases} 2^{-\frac{n-1}{2}} & \text{若 } w_2 \in \mathrm{Im}(\tau) \\ 0 & \text{否则} \end{cases}$$

其中, $W = (W_1, W_2)$, $W_1 = (w_1, \cdots, w_{k-1})$, $W_2 = (w_k, w_{k+1}, \cdots, w_n)$

定理 **2**　设 n 是奇数, $n = 2k-1$, 记 $X_1 = (x_1, x_2, \cdots, x_{k-1})$, $X_2 = (x_k, x_{k+1}, \cdots, x_n)$, $X = (X_1, X_2)$, 设 π_i: $F_2^{k-1} \to F_2^k$ 是满足下列条件的 m 个单射: 对任意的 $1 \leqslant i_1 \leqslant i_2 \leqslant \cdots \leqslant i_j \leqslant m$, $\pi_{i_1} \oplus \pi_{i_2} \oplus \cdots \oplus \pi_{i_j}$ 仍是单射. 设 f_i: $F_2^n = F_2^{k-1} \times F_2^k \to F_2$, 令 $f_i(X) = \pi_i(X_1) \cdot X_2$ ($1 \leqslant i \leqslant m$), 则 $f(X) = (f_1(X), f_2(X), \cdots, f_m(X))$ 是 n 元多输出半 Bent 函数.

证明　$\forall\, 0 \neq u \in F_2^m$, 设 u 的汉明重量 $W_H(u) = j$ ($1 \leqslant j \leqslant m$), 于是 $u \cdot f(X) = (\pi_{i_1}(X_1) \oplus \pi_{i_2}(X_1) \oplus \cdots \oplus \pi_{i_j}(X_1)) \cdot X_2$, 由定理的条件知 $\pi_{i_1} \oplus \pi_{i_2} \oplus \cdots \oplus \pi_{i_j}$ 是单射, 再由引理 4可知 $u \cdot f(X)$ 是 n 元半 bent函数, 根据结论 2可得 $f(X)$ 是 n 元多输出半 Bent函数.

用上述定理 2的方法构造多输出半 Bent函数的关键在于如何构造满足下列条件的 m 个单射 $\{\pi_i\}_{i=1}^m$: (1)π_i: $F_2^{k-1} \to F_2^k$ ($1 \leqslant i \leqslant m$); (2)对任意的 $1 \leqslant i_1 \leqslant i_2 \leqslant \cdots \leqslant i_j \leqslant m$, $\pi_{i_1} \oplus \pi_{i_2} \oplus \cdots \oplus \pi_{i_j}$ 仍是单射.

下面给出构造这种单射集的一种具体方法.

引理 **5**[7]　设 $h(x)$ 是 F_2 上的一个 n 次本原多项式, 记由 $h(x)$ 产生的 m 序列的全体为 $G(h)$, 令

$$\beta = \left\{ \boldsymbol{A} \,\middle|\, \boldsymbol{A} = \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_1 & a_2 & \cdots & a_n \\ \cdots & \cdots & \cdots & \cdots \\ a_{n-1} & a_n & \cdots & a_{2n-2} \end{pmatrix}, (a_0, a_1, a_2, \cdots) \in G(h) \right\}$$

则(1)集合 $\mathscr{B}$ 中的元素均为 F_2 上的非奇异 $n \times n$ 矩阵, 且满足条件: 若 $\boldsymbol{A}_1, \boldsymbol{A}_2 \in \mathscr{B}$ 且 $\boldsymbol{A}_1 \neq \boldsymbol{A}_2$ 则 $\boldsymbol{A}_1 \oplus \boldsymbol{A}_2 \in \mathscr{B}$;

(2) $\mathscr{B} \cup \{\boldsymbol{0}\}$ 在运算 $\oplus$ 之下形成 F_2 上的一个 n 维线性子空间. 在 $\mathscr{B}$ 中选择 m 个线性无关的元素, 记为 $\{\boldsymbol{A}_i\}_{i=1}^m$. 令 $\pi_i(x) = x\boldsymbol{A}_i$, $1 \leqslant i \leqslant m$, $x \in F_2^n$, 则这 m 个置换满足条件: 对任意的 $1 \leqslant i_1 \leqslant i_2 \leqslant \cdots \leqslant i_j \leqslant m$, $\pi_{i_1} \oplus \pi_{i_2} \oplus \cdots \oplus \pi_{i_j}$ 仍是置换.

注: 关于引理 5详见文[7].

由引理 5易得如下定理:

定理 **3**　设 $h(x)$ 是 F_2 上的一个 n 次本原多项式, 记由 $h(x)$ 产生的 m 序列的全体为 $G(h)$, 令

$$\alpha = \left\{ \boldsymbol{B} \,\middle|\, \boldsymbol{B} = \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-2} & a_{n-1} \\ a_1 & a_2 & \cdots & a_{n-1} & a_n \\ \cdots & \cdots & \cdots & \cdots & \\ a_{n-2} & a_{n-1} & \cdots & a_{2n-4} & a_{2n-3} \end{pmatrix}, (a_0, a_1, a_2, \cdots) \in G(h) \right\}$$

则(1)集合 $\mathscr{A}$ 中的元素均为 F_2 上的 $n-1 \times n$ 矩阵, 且满足条件: 若 $\boldsymbol{B}_1, \boldsymbol{B}_2 \in \mathscr{A}$ 并且 $\boldsymbol{B}_1 \neq \boldsymbol{B}_2$ 则 $\boldsymbol{B}_1 \oplus \boldsymbol{B}_2 \in \mathscr{A}$;

(2) $\mathscr{A} \cup \{\boldsymbol{0}\}$ 在运算 $\oplus$ 之下形成 F_2 上的一个 $n-1$ 维线性子空间. 在 α 中选择 m 个线性无关的元素, 记为 $\{\boldsymbol{B}_i\}_{i=1}^m$. 令 $\pi_i(x) = x\boldsymbol{B}_i$, $1 \leqslant i \leqslant m$, $x \in F_2^{n-1}$, 则这 m 个单射满足条件: 对任意的 $1 \leqslant i_1 \leqslant i_2 \leqslant \cdots \leqslant i_j \leqslant m$, $\pi_{i_1} \oplus \pi_{i_2} \oplus \cdots \oplus \pi_{i_j}$ 仍是单射.

4　结束语

本文提出了多输出半 Bent函数的概念, 并给出了多输出半 Bent函数的一种构造方法, 给出了用多输出半 Bent函数构造多输出 Bent函数的一种方法, 除了可用于构造多输出 Bent函数外, 多输出半 Bent函数还可应用于多输出前馈网[14,15]等方面.

[参考文献]

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

[2] Olsen J, Scholtz R, Welch L. Bent function sequences [J]. IEEE Transactions on Information Theory, 1982, 28(6): 858-864.

[3] Kumar P. Bounds on the linear span of bent sequences [J]. IEEE Transactions on Information Theory, 1983, 29(6): 854-862.

[4] Adams C, Tavares S. Generating and counting binary bent sequences [J]. IEEE Transactions on Information Theory, 1990, 36(5): 1170-1173.

[5] 郭宝安, 蔡长年. 一类即非 Bent基又非线性基的二元 Bent序列的产生与计数[J]. 科学通报, 1991, 36(2): 810-811.

[6] 欧洁,罗铸楷. 关于 Bent函数的一些研究[J]. 湘潭大学自然科学学报, 1999, 21(1): 7-11.
[7] 冯登国. 频谱理论及其在密码学中的应用[M]. 北京: 科学出版社, 2000. 65-100.
[8] Kaisa Nyberg. Perfect nonlinear S-boxed[A]. Advances in cryptology Eurocrypt' 91[C]. Berlin: Springer Verlag, 1992. 378-383.
[9] 张文英,滕吉红,李世取. 布尔函数的谱分解式及其在多维 Bent函数构造中的应用[A]. 张焕国. 第三届中国信息和通信安全学术会议论文集 CCICS[C]. 北京: 科学出版社, 2003. 290-296.
[10] Kaisa Nyberg. New Bent Mappings Suitable for Fast Implementation[A]. Fast Software Encryption[C]. Berlin: Springer-Verlag, 1994. 179-184.
[11] 张文英,李世取. 2维 2次 Bent函数的性质及构造[J]. 曲阜师范大学学报(自然科学版), 2003, 29(3): 22-24.
[12] 张文英,李世取,傅培利. 具有最高代数次数的 $2n$ 元 n 维 Bent函数的构造[J]. 应用数学, 2004, 17(3): 444-449.
[13] 胡磊,裴定一,冯登国. 一类 Bent函数的构造[J]. 中国科学院研究生院学报, 2002, 19(2): 103-106.
[14] 杨义先,胡正名. 抗熵漏前馈网络的研究[J]. 电子与信息学报, 1991, 13(6): 232-241.
[15] 胡一平,冯登国. 多输出前馈函数的一种相关分析方法[J]. 电子与信息学报, 1998, 20(6): 787-793.

[责任编辑: 刘健]

(上接第 30页)

(2) 与其余 3种扰流柱相比,水滴形扰流柱的强化换热效果略逊,其恒热流壁面的平均对流换热系数相对于前三者而言分别降低了 18.5%、12.4%和 3.8%.

(3) 用特殊压力损失系数来权衡,水滴形扰流柱的特殊压力损失系数分别是圆形、准水滴形和椭圆形扰流柱的 52.1%、82.0%和 84.7%,是一种具有较高综合性能的新型扰流柱.

[参考文献]

[1] Metzger D E, Berry R A, Bronson J P. Developing heat transfer in rectangular duct with staggered array of short pin fins[J]. Journal of Heat Transfer, 1982, 104: 700-706.
[2] Li Q. Heat transfer and pressure drop characteristics in rectangular channels with elliptic pin fins[J]. International Journal of Heat and Fluid Flow, 1998, 19: 245-250.
[3] Sparrow E M, Grannis V B. Pressure drop characteristics of heat exchangers consisting of arrays of diamond-shaped pin fins[J]. International Journal of Heat and Mass Transfer, 1991, 34(3): 589-600.
[4] Uzol Q, Camci C. Elliptical pin fins as an alternative to circular pin fins for gas turbine blade cooling applications[R]. (part 1: endwall heat transfer and total pressure loss characteristics). ASME Paper 2001-GT-0180, 2001.
[5] Chen Z, Li Q, Meier D. Convective heat transfer and pressure loss in rectangular ducts with drop-shaped pin fins[J]. Heat and Mass Transfer, 1997, 33: 219-224.
[6] 李庆领,丛培军. 矩形通道内扰流柱形状对阻力特性的影响[J]. 石油化工技术设备, 1997, 18(6): 42-44.
[7] 苏红桢,刘松龄. 扰流柱排内部流场的实验研究[J]. 航空动力学报, 1997, 12(2): 175-179.
[8] 苏红桢,刘松龄,许都纯. 叉排形扰流柱排内部流场的实验研究[J]. 推进技术, 1998, 18(2): 51-55.

[责任编辑: 刘健]