代数次数为2的Bent函数的性质及其应用

张文英,李世取
(郑州信息工程学院信息研究系,河南郑州 450002)

摘 要: 本文证明了任意代数次数为2的 n 元 Bent 函数都与形式为 $x_1x_2+x_3x_4+\cdots+x_{n-1}x_n$ 的 Bent 函数线性等价;给出了以任意已知代数次数为2的 n 元 Bent 函数为分量的多维 Bent 函数的构造法;利用本文所给的方法,对任一主对角线上元素全为0的 n 阶可逆对称矩阵 M_1,都可以构造 $k-1$ 个主对角线上元素全为0的 n 阶可逆对称矩阵 $M_2\cdots,M_k$,使得 $M_1,M_2\cdots,M_k$ 的任意非零线性组合仍是主对角线上元素全为0的阶可逆对称矩阵.

关键词: Bent函数; 多维Bent函数; Bent互补函数族; 线性等价; 可逆对称矩阵
中图分类号: TN918.1 **文献标识码:** A **文章编号:** 0372-2112 (2004) 04-0654-03

The Characteristic of Quadratic Bent Functions and Its Applications

ZHANG Wen-ying, LI Shi-qu
(*Dept. of Information Research, Institute of Information Engineering, Zhengzhou 450002, China*)

Abstract: This paper gives a proof that all Bent functions of degree 2 are linearly equivalent each other and presents a method for constructing *multi—dimension Bent* functions when one output variable is of degree 2. For a given reversible symmetrical matrix with the elements of its diagonal is 0, it provides a method for constructing $k-1$'s reversible symmetrical matrixes, such that every non-zero linear combination of these k's matrixes is also a reversible symmetrical matrix.

Key words: Bent function; multi-dimension Bent function; The families of Bent complementary functions; linear equivalent; reversible symmetrical matrix

1 引言

如文[1]所述,由于"加密算法标准化的需要"和"多级安全的需要"与"网络安全通信的需要",当前分组密码"受到了广泛关注并且成为密码学研究的热点之一".在分组密码的实际设计中,多输出的布尔函数常常扮演重要角色,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 $GF^6(2)$到 $GF^4(2)$的多输出布尔函数,因此如何构造更多具有良好密码性质的多输出布尔函数是值得研究的重要课题.由于具有抗"差分攻击"和"最优仿射逼近"的能力以及具有最高的非线性度和高度的"稳定性"[2],Bent函数[3]在密码设计中发挥了重要作用,如澳大利亚加密标准HAVAL算法[4]的设计中所用到的5个布尔函数无一例外都是由Bent函数演化而来.另外,1997年许成谦,杨义先,胡正名在文[5]中所提出的"Bent互补函数族"是一类与Bent函数的概念有关的函数族,文[5]的研究结果表明,"Bent互补函数族"在区分初始信号及其并元移位信号方面有着重要的应用,而多维Bent函数[6]——每个分量以及各分量的所有非零线性组合都是Bent函数的多输出函数(m 个输出时称为 m 维Bent函数)正是一类特殊的"Bent互补函数族".综上,多维Bent函数的构造方法是一个十分有意义的课题.

本文通过变量替换的方法证明了任意代数次数为2的 n 元Bent函数都与形式为 $x_1x_2+x_3x_4+\cdots+x_{n-1}x_n$ 的Bent函数线性等价,即在线性等价的意义下,代数次数为2的 n 元Bent函数只有一个;据之给出了以某个已知代数次数为2的Bent函数为分量的多维Bent函数的构造法;最后结合每个仅含有二次项的Bent函数都与主对角线上元素全为0的某可逆对称布尔矩阵相对应的事实,用我们上面的结论和方法解决了矩阵论中的一个问题.在本文将函数变为标准型的过程中只须做一系列的递归运算便可得到一个可逆线性变换,求做多维Bent函数的运算可以借助线性移位寄存器理论[7],所以上述过程都便于快速实现.本文中约定:n 是不小于2的偶数;$n=2k$.;$GF(2)=\{0,1\}$表示二元域.

2 代数次数为2的Bent函数的性质

定义1 设 $w=(w_1,\cdots,w_n)\in GF^n(2)$, $w\cdot x=w_1x_1+\cdots+w_nx_n$ 表示通常的内积(其中加法是模2加), $S_{(f)}(w)=\frac{1}{2^n}\sum_{x\in GF^n(2)}(-1)^{f(x)+w\cdot x}$, $w\in GF^n(2)$是 $f(x)$的Walsh循环谱,若对任意的 $w\in GF^n(2)$,都有 $S_{(f)}(w)=\pm 2^{-n/2}$,则称 $f(x)$是Bent函数.

收稿日期:2002-11-14;修回日期:2003-11-19

定义 2　设 $f(x)$、$\varphi(x)$, $x\in GF^n(2)$是布尔函数,若存在 $GF(2)$上的 n 阶可逆矩阵 A、n 维列向量 a 以及 $b\in GF(2)$,使得 $f(x)=\varphi(Ax+a)+b$,则称 f 和 φ 线性等价,记为 $f\sim\varphi$.

定理 1　代数次数为 2 的 n 元布尔函数

$$f(x_1,x_2,\cdots,x_n)=\sum_{1\le i\le j\le n}a_{ij}x_ix_j+\sum_{i=1}^{n}a_ix_i+c,x\in GF^n(2)\quad(1)$$

为 Bent 函数的充分必要条件是它和 n 元 Bent 函数

$$\varphi(x_1,x_2,\cdots,x_n)=x_1x_2+x_3x_4+\cdots+x_{n-1}x_n,x\in GF^n(2)$$

线性等价.从而所有代数次数为 2 的 n 元 Bent 函数都相互线性等价.

证明　充分性显然.下证必要性:当 $n=2$ 时,2 元 Bent 函数必定形为

$$f(x_1,x_2)=x_1x_2+a_1x_1+a_2x_2+c=(x_1+a_2)(x_2+a_1)+a_1a_2+c,(x_1,x_2)\in GF^2(2)\quad(2)$$

定理结论显然成立.

设对于代数次数为 2 的 $n-2$ 元 Bent 函数定理中必要性成立,若式(1)中的 $f(x)$是 Bent 函数,这等价于 $\sum_{1\le i<j\le n}a_{ij}x_ix_j$ 是 Bent 函数,由于任一 Bent 函数都是非退化的,故至少存在一个 $2\le j\le n$,使得 $a_{1j}=1$,不妨设 $j=2$,于是可有

$$\begin{aligned}f(x_1,x_2,\cdots,x_n)&=(x_1+a_{23}x_3+\cdots+a_{2n}x_n)\\&\quad\cdot(x_2+a_{13}x_3+\cdots+a_{1n}x_n)\\&\quad+(a_{13}x_3+\cdots+a_{1n}x_n)\\&\quad\cdot(a_{23}x_3+\cdots+a_{2n}x_n)\\&\quad+\sum_{3\le i<j\le n}a_{ij}x_ix_j+\sum_{i=1}^{n}a_ix_i+c\\&=(y_1+a_2)(y_2+a_1)+g(x_3,\cdots,x_n)\end{aligned}$$

其中 $y_1=x_1+a_{23}x_3+\cdots+a_{2n}x_n$, $y_2=x_2+a_{13}x_3+\cdots+a_{1n}x_n$,

$$\begin{aligned}g(x_3,x_4,\cdots,x_n)&=(a_{13}x_3+\cdots+a_{1n}x_n)(a_{23}x_3+\cdots+a_{2n}x_n)\\&\quad+\sum_{3\le i<j\le n}a_{ij}x_ix_j+a_1a_{23}x_3+\cdots+a_1a_{2n}x_n\\&\quad+a_2a_{13}x_3+\cdots+a_2a_{1n}x_n+\sum_{i=3}^{n}a_ix_i+c\end{aligned}$$

由于$(y_1+a_2)(y_2+a_1)$是关于 y_1、y_2 的 Bent 函数,且易知 y_1、y_2、x_3、$\cdots$、x_n 是独立取值于 $GF(2)$的,再对 $g(x_3,x_4,\cdots,x_n)$进行归纳假设可得定理结论成立.

由定理 1 的证明过程可以看出一个代数次数为 2 的布尔函数是 Bent 函数当且仅当可以通过每次标准化两个变量,逐步将其变成

$$x_1x_2+x_3x_4+\cdots+x_{n-1}x_n+c$$

的形式.

例 1　如

$$\begin{aligned}f(x)&=x_1x_2+x_1x_3+x_1x_6+x_2x_3+x_3x_4+x_5x_6\\&=(x_1+x_3)(x_2+x_3+x_6)+x_3(x_4+x_6+1)+x_5x_6\end{aligned}$$

做线性变换

$$y_1=x_1+x_3,y_2=x_2+x_3+x_6,y_3=x_3,$$

$$y_4=x_4+x_6+1,y_5=x_5,y_6=x_6$$

易见上述变换是可逆的,若设 $\varphi(y)=y_1y_2+y_3y_4+y_5y_6$,且将上述变换记为 $y=Ax+a$,则 $f(x)=\varphi(Ax+a)$,所以 $f\sim\varphi$,且由定理 1 知 $f(x)$是 Bent 函数.

3　代数次数为 2 的多维 Bent 函数的构造

定义 3　每个分量以及各分量的所有非零线性组合都是 Bent 函数的多输出函数称为多维 Bent 函数,m 个输出时称为 m 维 Bent 函数.

引理 1[8]　对于代数次数为 2 的 n 元 Bent 函数

$$\varphi(x_1,x_2,\cdots,x_n)=x_1x_2+x_3x_4+\cdots+x_{n-1}x_n,x\in GF^n(2),$$

一定存在 $GF(2)$上的 n 阶可逆矩阵 B_j, $1\le j\le k-1$,使得当 $\varphi_j(x)=\varphi(B_jx)$时,$(\varphi(x),\varphi_1(x),\cdots,\varphi_{k-1}(x))$是一个 k 维 Bent 函数.

定理 1 表明任意代数次数为 2 的 n 元 Bent 函数 $f(x)$都可以经可逆线性变换变成形式为 $x_1x_2+x_3x_4+\cdots+x_{n-1}x_n$ 的 Bent 函数,引理 1 说明以 $x_1x_2+x_3x_4+\cdots+x_{n-1}x_n$ 为一个分量的 n 元 k 维 Bent 函数一定存在,将二者结合起来,就可以得到以某个代数次数为 2 的 n 元 Bent 函数 $f_1(x)$为分量的多维 Bent 函数的构造法.

定理 2　对于每个代数次数为 2 的 $n(n\ge4)$元 Bent 函数 $f_1(x)$, $x\in GF^n(2)$,一定可以找到 $k-1$ 个代数次数为 2 的 n 元 Bent 函数 $f_2(x),\cdots,f_k(x)$,使得

$$(f_1(x),f_2(x),\cdots,f_k(x))$$

是 n 元 k 维 Bent 函数.

证明　设 $\varphi(x)=x_1x_2+x_3x_4+\cdots+x_{n-1}x_n$,由定理 1 知道:对于本定理中所给的 Bent 函数 $f_1(x)$,存在可逆矩阵 A,使得 $f_1(x)=\varphi(Ax+a)+b$,若 $n\ge4$,又由引理 1 知一定存在 $GF(2)$上的 $k-1$ 个 n 阶可逆矩阵 B_j, $1\le j\le k$,使得

$$(\varphi(x),\varphi(B_1x),\cdots,\varphi(B_{k-1}x))$$

是 k 维 Bent 函数,再用 $Ax+a$ 代替上面的 x,即得到 k 维 Bent 函数:

$$(\varphi(Ax+a)+b,\varphi(B_1(Ax+a)),\cdots,\varphi(B_{k-1}(Ax+a)))=(f_1(x),f_2(x),\cdots,f_k(x))$$

定义 4[5]　称 m 个 n 元布尔函数 $\{f_1(x),f_2(x),\cdots,f_m(x)\}$为容量是 m 的 n 元 Bent 互补函数族,如果

$$\sum_{i=1}^{m}S^2_{(f_i)}(w)=\frac{m}{2^n},w\in GF^n(2)$$

显然,当$(f_1(x),f_2(x),\cdots,f_m(x))$是 n 元 m 维 Bent 函数的时候,$\{f_1(x),f_2(x),\cdots,f_m(x)\}$必定是容量为 m 的 n 元"Bent 互补函数族".所以定理 2 也给出了以某个代数次数为 2 的 Bent 函数为一个分量的容量是 k 的 n 元 Bent 互补函数族的构造法.又多维 Bent 函数各分量的所有非零线性组合都是 Bent 函数,所以多维 Bent 函数还是一类性质很好的特殊的"Bent 互补函数族".

例 2　$f_1(x)$同例 1 中的 $f(x)$,下面构造以 $f_1(x)$为一个分量的 3 维 Bent 函数.设 $\varphi(x)=x_1x_2+x_3x_4+x_5x_6$、$B=\begin{pmatrix}1&0&0&0&0&0\\0&0&0&1&0&0\\0&0&1&0&0&0\\0&0&0&0&0&1\\0&0&0&0&1&0\\0&1&0&1&0&0\end{pmatrix}$,令 $B_j=B^j$, $j=1,2$,则

$\varphi(\boldsymbol{Bx}) = x_1x_4 + x_3x_6 + x_2x_5 + x_4x_5$, $\varphi(\boldsymbol{B}^2x) = x_1x_6 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_6$,且$(\varphi(x), \varphi(\boldsymbol{Bx}), \varphi(\boldsymbol{B}^2x))$是3维Bent函数,再用例1中的$\boldsymbol{Ax} + a$代替此处的$x$,便得到3维Bent函数

$$\begin{aligned}(f_1(x), f_2(x), f_3(x)) &= (\varphi(\boldsymbol{Ax} + a), \varphi(\boldsymbol{B}(\boldsymbol{Ax} + a)), \varphi(\boldsymbol{B}^2 \cdot (\boldsymbol{Ax} + a))) = (x_1x_2 + x_1x_3 + x_1x_6 \\ &+ x_2x_3 + x_3x_4 + x_5x_6, x_1x_6 + x_2x_3 \\ &+ x_3x_6 + x_4x_5 + x_5x_6, x_1x_4 + x_1x_6 \\ &+ x_2x_5 + x_3x_5 + x_3x_6)\end{aligned}$$

易知$(f_1(x), f_2(x), f_3(x))$还是一个容量是3的6元Bent互补函数族.

4 可逆对称布尔矩阵的一条性质

引理 2[2] 设$f(x_1, \cdots, x_n) = \sum_{1 \le i < j \le n} a_{ij}x_ix_j + \sum_{i=1}^{n} b_ix_i + c$, $x = (x_1, \cdots, x_n) \in GF^n(2)$,则$f(x)$是Bent函数的充分必要条件是对角线上元素全为0的对称布尔矩阵$\boldsymbol{M} = (m_{ij})$是可逆的.其中$m_{ij} = a_{ij}, i < j$.

由引理2,仅含有二次项的Bent函数与主对角线上元素全为0的可逆对称矩阵一一对应,所以再由定理2,可以得到布尔矩阵的一条性质:

定理 3 对任一主对角线上元素全为0的n, $n \ge 4$阶可逆对称布尔矩阵$\boldsymbol{M}_1$,一定存在$k-1$个主对角线上元素全为0的n阶可逆对称布尔矩阵$\boldsymbol{M}_2, \cdots, \boldsymbol{M}_k$,使得$\boldsymbol{M}_1, \boldsymbol{M}_2, \cdots, \boldsymbol{M}_k$中的任意$i(i \le k)$个之和仍然是主对角线上元素全为0的$n$阶可逆对称布尔矩阵.

证明 以$\boldsymbol{M}_1$所决定的仅含有二次项的Bent函数$f(x)$为一个分量,按照定理2中的方法做代数次数为2的n元k维Bent函数$(f_1(x), f_2(x), \cdots, f_k(x))$,则与$f_2(x), \cdots, f_k(x)$相对应的可逆对称布尔矩阵$\boldsymbol{M}_2, \cdots, \boldsymbol{M}_k$即为所求.

5 结束语

本文在证明了所有代数次数为2的n元Bent函数都与$x_1x_2 + x_3x_4 + \cdots + x_{n-1}x_n$线性等价的基础上,给出了以某个代数次数为2的Bent函数为分量的多维Bent函数的构造法,需要指出的是:由于这类函数的代数次数太低及在线性等价的意义下只有一个,设计者不宜直接采用,但根据本文的方法和文献[3]、[8]的结论,当$n \ge 6$,且是偶数时,对任意取定的线性无关的n维布尔向量$W_i \in GF^n(2), 1 \le i \le n$,和任意一个$k$元布尔函数$g(y_1, \cdots, y_k)$,对形如

$$\begin{aligned}f(x) &= (W_1 \cdot x)(W_2 \cdot x) + (W_3 \cdot x)(W_4 \cdot x) + \cdots \\ &+ (W_{n-1} \cdot x)(W_n \cdot x) + g(W_2 \cdot x, W_4 \cdot x, \cdots, W_n \cdot x)\end{aligned}$$

的n元布尔函数,用本文第三部分中的方法都可以构造出形如$f(x)$的$f_2(x), f_3(x), \cdots, f_k(x)$,使得

$$(f_1(x), f_2(x), \cdots, f_k(x))$$

是k维Bent函数,这样,$f_2(x), f_3(x), \cdots, f_k(x)$的代数次数就不一定限制为2了,其实各自都可以达到最高——$n/2$.

参考文献:

[1] 冯登国,吴文玲.分组密码的设计与分析[M].北京:清华大学出版社,2000.1-2.

[2] 丁存生,肖国镇.流密码学及其应用[M].北京:国防工业出版社,1994.136-142.

[3] Rothaus O S. On Bent functions [J]. J Combinatorial Theory (Ser A), 1976, 20: 300-305.

[4] Yuliang Zheng, Josef Pieprzyk, Jennifer Seberry. HAVAL—A One Way Hashing Algorithm with Variable Length Output [A]. Advances in Crytology-AUSCRYPT'92 [C]. Heidelberg, Springer-Verlag, 1993. 83-104.

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

[6] 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,2000.118-132.

[7] 丁石孙.线性移位寄存器序列[M].上海:上海科技出版社,1980.10-24.

[8] Kaisa Nyberg. Perfect nonlinear S-boxes [A]. Advances in Crytology-Eurocrypt'91 [C]. Heidelberg, Springer-Verlag, 1992.378-383.

作者简介:

张文英 1970年6月出生于山东鄄城县,1994年毕业于曲阜师范大学数学系,获理学硕士学位,现为解放军信息工程学院博士生,主要研究方向为概率论及其在密码学中的应用.

李世取 1945年出生于重庆市,解放军信息工程学院教授,博士生导师,曾在国内外重要学术刊物上发表论文数篇,主要研究方向为概率论及其在密码学中的应用.