两类多输出逻辑函数的关系

金栋梁[1],赵亚群[1,2]
JIN Dong-liang[1],ZHAO Ya-qun[1,2]

1.信息工程大学 信息工程学院,郑州 450002
2.中国科学院 研究生院 信息安全国家重点实验室,北京 100039
1.Information Engineering Institute,Information Engineering University,Zhengzhou,Henan 450002,China
2.State Kay Laboratory of Information Security,Graduate of Chinese Academy of Sciences,Beijing 100039,China
E-mail:jindongliang0709@163.com

JIN Dong-liang,ZHAO Ya-qun.Relationship between multi-output generalized partially Bent functions and multi-output generalized Bent functions.Computer Engineering and Applications,2008,44(13):54-56.

Abstract: The definition and existence of multi-output generalized partially Bent functions are discussed,then the criterion of multi-output generalized partially Bent functions is presented,and the relationship between multi-output p-valued generalized partially Bent functions and multi-output p-valued generalized Bent functions is obtained,which includes the generalized Chrestenson spectrum expression and function expression,meanwhile a method of constructing multi-output p-valued generalized partially Bent functions is provided.

Key words: multi-output generalized partially Bent functions;multi-output generalized Bent functions;generalized Chrestenson spectrum;criterion

摘 要:首次给出了多输出广义部分 Bent 函数的定义并论证了其的存在,得到了多输出广义部分 Bent 函数的等价判别条件,给出了多输出 p 值广义部分 Bent 函数与多输出 p 值广义 Bent 函数的关系,并讨论了这两者的广义一阶 Chrestenson 谱的关系,为多输出 p 值广义部分 Bent 函数的构造提供了一种方法。

关键词:多输出广义部分 Bent 函数;多输出广义 Bent 函数;广义一阶 Chrestenson 谱;等价判别条件
DOI:10.3778/j.issn.1002-8331.2008.13.016 **文章编号**:1002-8331(2008)13-0054-03 **文献标识码**:A **中图分类号**:TN918.1

1 引言

当前分组密码受到人们的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之中,多输出的逻辑函数常常扮演重要角色。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,Bent 函数[1]在密码设计中发挥了重要作用。为了弥补 Bent 函数不具有平衡性、相关免疫性等特点,C.carlet 对 Bent 函数作了推广,提出了部分 Bent 函数[2]的概念。后来文献[3]将此概念进行了推广,提出了多输出部分 Bent 函数的概念。依据实际应用的需要,近年来人们在密码学中对多值逻辑函数的性质和构造给予了更多的关注,将布尔函数的许多研究成果都拓广到多值逻辑函数中。1991 年,Nyberg 在文献[4]中将二元域上的向量 Bent 函数的概念推广到素域上广义向量 Bent 函数。将向量函数称为多输出函数。且在文献[5]中讨论了多输出 Bent 函数与多输出部分 Bent 函数的关系。本文在广义 Bent 函数[6]及广义部分 Bent 函数[7]的基础上,提出了多输出广义部分 Bent 函数的定义并论证了其的存在,得到了多输出广义部分 Bent 函数的等价判别条件,给出了多输出 p 值广义部分 Bent 函数与多输出 p 值广义 Bent 函数的关系,并讨论了这两者的广义一阶 Chrestenson 谱的关系,为多输出 p 值广义部分 Bent 函数的构造提供了一种方法。将文献[5]的结果推广到了 p 值逻辑函数。

下面给出几个要用到的基本概念,另外有关逻辑函数的概念见文献[8,9]。

设 $m\geqslant 2$ 是任一取定的正整数,以 $Z_m=Z/(m)$ 为整数模 m 的剩余类环,又设 n 为任一正整数,Z_m^n 为 n 个 Z_m 笛卡儿积。$X=(X_1,\cdots,X_n)$ 中的 $X_1,\cdots,X_n$ 都是定义在某概率空间 (Ω,F,P) 上相互独立,且都具有均匀分布的 m 值随机变量,记 m 次本原单位根为 $u_m=e^{2\pi i/m}$,$i=\sqrt{-1}$。

定义 1[8,10] 称 $Z_m^n\to Z_m^k$ 的任一映射 $F(x)$,$x\in Z_m^n$ 为 Z_m^n 上的 k(多)输出 n 元 m 值逻辑函数,$k\leqslant m$。若 $f_i(x)$ 为 Z_m^n 上的 n 元 m 值逻辑函数,$i=1,\cdots,k$,则 $F(x)=(f_1(x),\cdots,f_k(x))$ 是 Z_m^n 上的 n 元 k(多)输出 m 值逻辑函数,记为 $F(x)=(f_1(x),\cdots,f_k(x)):Z_m^n$

基金项目:信息安全国家重点实验室开放基金资助课题(01-02)(the State Kay Laboratory of Information Security Opening Foundation(01-02))。
作者简介:金栋梁(1983-),男,硕士研究生,主要研究方向为密码基础理论及概率统计应用;赵亚群(1961-),女,副教授,硕士生导师,主要研究方向为密码基础理论及概率统计应用。
收稿日期:2007-08-22 **修回日期**:2007-10-23

$\to Z_m^k$ 易知 $F(X)=(f_1(X),\cdots,f_k(X))$为$(\Omega,F,P)$上的 k 维 m 值随机向量。

定义 2[8] 设 $F(x)=(f_1(x),\cdots,f_k(x)):Z_m^n\to Z_m^k$,$k\leqslant m$,称 $S_{(F)}(v,w)=\frac{1}{m^n}\sum_{x\in Z_m^n}u_m^{v\cdot F(x)-w\cdot x}$,$v\in Z_m^k$,$w\in Z_m^n$为 $F(x)$的广义一阶 Chrestenson 循环谱。特别,当 $k=1$,$v=1$ 时,广义一阶 Chrestenson 循环谱是 m 值逻辑函数的 Chrestenson 循环谱。

定义 3[10] 设 $F(x)=(f_1(x),\cdots,f_k(x)):Z_m^n\to Z_m^k$,$k\leqslant m$,称 $r_F(v,s)=\frac{1}{m^n}\sum_{x\in Z_m^n}u_m^{v\cdot(F(x+s)-F(x))}$,$v\in Z_m^k$,$s\in Z_m^n$为 $F(x)$的广义自相关函数。

2 多输出广义部分 Bent 函数的等价判别条件

定义 4[4] 设 $F(x)=(f_1(x),\cdots,f_k(x))$,$x\in Z_m^n$为 n 元多输出 m 值逻辑函数,$1\leqslant k\leqslant m$,若对任意的 $0\neq v\in Z_m^k$,$v\cdot F(x)$都是广义 Bent 函数,则称 $F(x)$为 Z_m^n上的 n 元多输出广义 Bent 函数。

定义 5 设 $F(x)=(f_1(x),\cdots,f_k(x))$,$x\in Z_m^n$为 n 元多输出 m 值逻辑函数,对任意的,$v\in Z_m^k$,记

$$N_{r(v)}=|\{s:s\in Z_m^n,r_F(v,s)=0\}|$$

$$N_{s(v)}=|\{w:w\in Z_m^n,S_{(F)}(v,w)=0\}|$$

若有$(m^n-N_{r(v)})(m^n-N_{s(v)})=m^n$,则称 $F(x)$为 Z_m^n上的 n 元多输出广义部分 Bent 函数。

又可知,$F(x)=((x_1+x_2)(x_1+x_3),(x_1+x_2)(x_1+x_3)+(x_1+x_4)(x_3+x_5))$,$x\in Z_m^5$是 5 元二输出广义部分 Bent 函数,其分量函数均不是广义 Bent 函数,因此 $F(x)$不是多输出广义 Bent 函数。

注意到:对任意的 $v\in Z_m^k$,$S_{(F)}(v,w)=S_{(v\cdot F)}(w)$,$r_F(v,s)=r_{v\cdot F}(s)$,易得以下定理:

定理 1 设 $F(x)$是 n 元多输出 m 值逻辑函数,则 $F(x)$是多输出广义部分 Bent 函数的充分必要条件是对任意的 $0\neq v\in Z_m^k$,$v\cdot F(x)$是广义部分 Bent 函数。

注:由定理 1 可知,多输出 m 值仿射函数必为多输出广义部分 Bent 函数。

以上讨论表明, 多输出广义部分 Bent 函数是存在和有意义的,其分量函数皆是广义部分 Bent 函数。

引理 1[9] 设 $f(x)$,$x\in Z_m^n$是 m 值逻辑函数,则 $f(x)$是 Z_m^n上的广义部分 Bent 函数的充分必要条件是存在 $t\in Z_m^n$,使得 $f(x)$的 Chrestenson 谱具有下述性质:

$$|S_{(f)}(w)|^2=\begin{cases}\frac{|E_f|}{m^n},w\in t+E_f^{\perp}\\0,w\notin t+E_f^{\perp}\end{cases}$$

其中 $E_f=\{s\in Z_m^n:r_f(s)=u^{t-s}\}$为 Z_m^n的 Z_m-子模。

对任给定的 $v\in Z_m^k$,$t_v\in Z_m^n$,记

$$E_F(v)=\{s\in Z_m^n:r_F(v,s)=u_m^{t_v-s}\}=\{s\in Z_m^n:r_{v\cdot F}(s)=u_m^{t_v-s}\}=E_{v\cdot F}$$

定理 2 设 $F(x)$,$x\in Z_m^n$是多输出 m 值逻辑函数,则 $F(x)$是 Z_m^n上的多输出广义部分 Bent 函数的充分必要条件是对任意的 $0\neq v\in Z_m^k$,存在 $t_v\in Z_m^n$,使得 $F(x)$广义一阶 Chrestenson 谱具有下述性质:

$$|S_{(F)}(v,w)|^2=\begin{cases}\frac{|E_F(v)|}{m^n},w\in t+[E_F(v)]^{\perp}\\0,w\notin t+[E_F(v)]^{\perp}\end{cases}$$

其中 $E_F(v)$为 Z_m^n的 Z_m-子模。

证明 由定理 1 可知,$F(x)$是 Z_m^n上的多输出广义部分 Bent 函数的充分必要条件是对任意的 $0\neq v\in Z_m^k$,$v\cdot F(x)$是广义部分 Bent 函数。再由引理 1 可知,对任意的 $0\neq v\in Z_m^k$,$v\cdot F(x)$是广义部分 Bent 函数的充分必要条件是存在 $t_v\in Z_m^n$使得

$$|S_{(v\cdot F)}(w)|^2=\begin{cases}\frac{|E_{v\cdot F}|}{m^n},w\in t+[E_{v\cdot F}]^{\perp}\\0,w\notin t+[E_{v\cdot F}]^{\perp}\end{cases}$$

而 $S_{(v\cdot F)}(w)=S_{(F)}(v,w)$,$E_{v\cdot F}=E_F(v)$。可有

$$|S_{(F)}(v,w)|^2=\begin{cases}\frac{|E_F(v)|}{m^n},w\in t+[E_F(v)]^{\perp}\\0,w\notin t+[E_F(v)]^{\perp}\end{cases}$$

其中 $E_F(v)$为 Z_m^n的 Z_m-子模。

3 多输出 p 值广义部分 Bent 函数与多输出 p 值广义 Bent 函数的关系

当 $m=p$(p 为素数)时,由文献[9]可知对任意的 $0\neq v\in Z_p^k$,$E_F(v)$为 Z_p^n的线性子空间。设 A 是一个集合,记

$$I_A(x)=\begin{cases}1,x\in A\\0,x\notin A\end{cases}$$

在此记号下定理 2 可以改写为:

定理 3 $F(x)$,$x\in Z_p^n$是 n 元多输出 p 值广义部分 Bent 函数的充分必要条件是对任意的 $0\neq v\in Z_p^k$,存在 Z_p^n的 $l(v)$维线性子空间 $E_{l(v)}$及 $t_v\in Z_p^n$使得 $F(x)$广义一阶 Chrestenson 谱具有下述性质:

$$|S_{(F)}(v,t_v+w)|^2=\frac{1}{p^{l(v)}}I_{E_{l(v)}}(w),w\in Z_p^n$$

定义 6 设 $F(x)$,$x\in Z_p^n$是 n 元多输出 p 值广义部分 Bent 函数。若存在线性空间 E_l(l 为 E_l 的维数),满足对任意的 $0\neq v\in Z_p^k$,存在 $t_v\in Z_p^n$,使得

$$|S_{(F)}(v,t_v+w)|^2=\frac{1}{p^l}I_{E_l}(w),w\in Z_p^n$$

则称 $F(x)$为(n,k,l,E_l)多输出 p 值广义部分 Bent 函数。

记 $F(n,k,l,E_l)$={全体(n,k,l,E_l)多输出 p 值广义部分 Bent 函数}。

定义 7 设 $F(x)\in F(n,k,l,E_l)$,且对任意的 $0\neq v\in Z_p^k$满足$|S_{(F)}(v,w)|^2=\frac{1}{p^l}I_{E_l}(w)$,$w\in Z_p^n$,则称 $F(x)$为 $F(n,k,l,E_l)$的核函数。

定理 4 (1)$F(x)$为 $F(n,k,l,E_l)$的核函数的充分必要条件是对任意的 $0\neq v\in Z_p^k$,$v\cdot F(x)$是 $F(n,1,l,E_l)$的核函数。

(2)$F(x)\in F(n,k,l,E_l)$的充分必要条件是对任意的$0\neq v\in Z_p^k$,$v\cdot F(x)\in F(n,k,l,E_l)$。

证明 由文献[5]的证明思路易知结论成立。

又对正整数l,记$L_l=\{E_l:E_l$为Z_p^n的l维线性子空间$\}$。

引理 2[11] 设$E_l\in L_l,w^{(1)},w^{(2)},\cdots,w^{(l)}$是$E_l$的一组基,则

(1)$f(x)$为$F(n,1,l,E_l)$的核函数的充分必要条件是存在Z_p^l上的l元广义 Bent 函数$g(y)$,使得,

$$f(x)=g(w^{(1)}\cdot x,w^{(2)}\cdot x,\cdots,w^{(l)}\cdot x),x\in Z_p^n$$

或等价的

$$S_{(f)}(w)=\begin{cases}S_{(g)}(a_1,a_2,\cdots,a_l),w=a_1w^{(1)}+\cdots+a_lw^{(l)}\in E_l,\\ \qquad\qquad (a_1,a_2,\cdots,a_l)\in Z_p^l\\ 0,w\notin E_l\end{cases}$$

(2)$F(n,1,l,E_l)$的核函数总存在,且其个数即为Z_p^l上的广义 Bent 函数的个数。

引理 3[9] 设$f(x),g(x),x\in Z_m^n$都是n元m值逻辑函数,则 Chrestenson 谱有如下性质:

$$S_{(f+g)}(w)=\sum_{v\in Z_m^n}S_{(f)}(v)S_{(g)}(w-v),w\in Z_m^n$$

定理 5 设$E_l\in L_l,w^{(1)},\cdots,w^{(l)}$是$E_l$的一组基,则$F(x)$为$F(n,k,l,E_l)$的核函数的充分必要条件是存在$Z_p^l$上的$l$元多输出广义 Bent 函数$G(y)$,使得$F(x)=G(w^{(1)}\cdot x,\cdots,w^{(l)}\cdot x),x\in Z_p^n$,或等价的,对任意的$0\neq v\in Z_p^k$,

$$S_{(F)}(v,w)=\begin{cases}S_{(G)}(v,(a_1,\cdots,a_l)),w=a_1w^{(1)}+\cdots+a_lw^{(l)}\in E_l,\\ \qquad\qquad (a_1,\cdots,a_l)\in Z_p^l\\ 0,w\notin E_l\end{cases}$$

证明 必要性:设$F(x)=(f_1(x),\cdots,f_k(x)),x\in Z_p^n$,由定理 4 可知,对任意的$0\neq v\in Z_p^k$,$v\cdot F(x)$是$F(n,1,l,E_l)$的核函数。特别地$f_i(x)(i=1,\cdots,k)$是$F(n,1,l,E_l)$的核函数。则由引理 2,必然存在$Z_p^l$上的$l$元广义 Bent 函数$g_i(y)(i=1,\cdots,k)$,使得

$$f_i(x)=g_i(w^{(1)}\cdot x,\cdots,w^{(l)}\cdot x)\triangleq g_i(y),x\in Z_p^n$$

且

$$S_{(f_i)}(w)=\begin{cases}S_{(g_i)}(a_1,\cdots,a_l),w=a_1w^{(1)}+\cdots+a_lw^{(l)}\in E_l,\\ \qquad\qquad (a_1,\cdots,a_l)\in Z_p^l\\ 0,w\notin E_l\end{cases}$$

令$G(y)=(g_1(y),\cdots,g_k(y))$显然有$F(x)=G(w^{(1)}\cdot x,\cdots,w^{(l)}\cdot x)$。

下面来证明:对任意的$0\neq v\in Z_p^k$,有

$$S_{(v\cdot F)}(w)=\begin{cases}S_{(v\cdot G)}(a_1,\cdots,a_l),w=a_1w^{(1)}+\cdots+a_lw^{(l)}\in E_l,\\ \qquad\qquad (a_1,\cdots,a_l)\in Z_p^l\\ 0,w\notin E_l\end{cases}$$

首先考虑$k=2$时的情形。

当$v=(a,0),v=(0,a),a\in Z_p\backslash\{0\}$时,由(1)知结论成立;当$v=(a,b),a,b\in Z_p\backslash\{0\}$时:

(1)$w=a_1w^{(1)}+\cdots+a_lw^{(l)}\in E_l$时,若$s\in E_l$,不妨设$s=b_1w^{(1)}+\cdots+b_lw^{(l)},(b_1,\cdots,b_l)\in Z_p^l$,则$w-s=(a_1-b_1)w^{(1)}+\cdots+(a_l-b_l)w^{(l)}\in E_l$;

若$s\notin E_l$,则$w-s\notin E_l$,由引理 3 可得:

$$S_{(v\cdot F)}(w)=S_{(af_1+bf_2)}(v)=\sum_{s\in F_2^n}S_{(af_1)}(s)S_{(bf_2)}(w-s)=$$

$$\sum_{s\in E_l}S_{(af_1)}(s)S_{(bf_2)}(w-s)+\sum_{s\notin E_l}S_{(af_1)}(s)S_{(bf_2)}(w-s)=$$

$$\sum_{(b_1,\cdots,b_l)\in Z_p^l}S_{(ag_1)}(b_1,\cdots,b_l)S_{(bg_2)}(a_1-b_1,\cdots,a_l-b_l)=$$

$$\sum_{(b_1,\cdots,b_l)\in Z_p^l}S_{(ag_1)}(b_1,\cdots,b_k)S_{(bg_2)}((a_1,\cdots,a_l)-(b_1,\cdots,b_l))=$$

$$S_{(ag_1+bg_2)}(a_1,\cdots,a_l)$$

(2)$w=a_1w^{(1)}+\cdots+a_lw^{(l)}\notin E_l$时,因为$af_1+bf_2$是核函数,所以$S_{(af_1+bf_2)}(w)=0$。故

$$S_{(af_1+bf_2)}(v)=\begin{cases}S_{(ag_1+bg_2)}(a_1,\cdots,a_l),v=a_1w^{(1)}+\cdots+a_lw^{(l)}\in E_l\\ 0,v\notin E_l\end{cases}$$

综上所述可知$k=2$时,对任意的$0\neq v\in Z_p^2$,有

$$S_{(v\cdot F)}(w)=\begin{cases}S_{(v\cdot G)}(a_1,\cdots,a_l),w=a_1w^{(1)}+\cdots+a_lw^{(l)}\in E_l\\ \qquad\qquad (a_1,\cdots,a_l)\in Z_p^l\\ 0,v\notin E_l\end{cases}$$

即

$$S_{(F)}(u,v)=\begin{cases}S_{(G)}(u,(a_1,\cdots,a_k)),v=a_1v^{(1)}+\cdots+a_kv^{(k)}\in E_k\\ \qquad\qquad (a_1,\cdots,a_k)\in F_2^k\\ 0,v\notin E_k\end{cases}$$

且$F(x)=G(v^{(1)}\cdot x,\cdots,v^{(k)}\cdot x),x\in F_2^n$。

一般性结论由数学归纳法可得。

充分性:由于$S_{(F)}(v,w)=S_{(v\cdot F)}(w)$,且$S_{(G)}(v,(a_1,\cdots,a_l))=S_{(v\cdot G)}(a_1,\cdots,a_l)$,则由已知条件可得:

$$S_{(v\cdot F)}(w)=\begin{cases}S_{(v\cdot G)}(a_1,\cdots,a_l),w=a_1w^{(1)}+\cdots+a_lw^{(l)}\in E_l\\ \qquad\qquad (a_1,\cdots,a_l)\in Z_p^l\\ 0,w\notin E_l\end{cases}$$

且$v\cdot F(x)=v\cdot G(w^{(1)}\cdot x,\cdots,w^{(l)}\cdot x),x\in Z_p^n$。

由引理 2 得,$v\cdot F(x)$是$F(n,1,l,E_l)$的核函数,从而由定理 4 得,$F(x)$为$F(n,1,l,E_l)$的核函数。

引理 4[11] 设$E_l\in L_l,w^{(1)},w^{(2)},\cdots,w^{(l)}$是$E_l$的一组基,则$f(x)\in F(n,k,l,E_l)$的充分必要条件是存在$Z_p^l$上的广义 Bent 函数$g(y)$及$t\in Z_p^n$使得$f(x)=g(w^{(1)}\cdot x,w^{(2)}\cdot x,\cdots,w^{(l)}\cdot x)+t\cdot x,x\in Z_p^n$。

定理 6 设$E_l\in L_l,w^{(1)},w^{(2)},\cdots,w^{(l)}$是$E_l$的一组基,则$F(x)\in F(n,k,l,E_l)$的充分必要条件是存在$Z_p^l$上的$l$元多输出广义 Bent 函数$G(y)$及$t_i\in Z_p^n$,$i=1,\cdots,k$,使得$F(x)=G(w^{(1)}\cdot x,\cdots,w^{(l)}\cdot x)+(t_1\cdot x,\cdots,t_k\cdot x),x\in Z_p^n$。

证明 必要性:设$F(x)\in F(n,k,l,E_l)$,则对任意的$0\neq v\in Z_p^k$,存在$t_v\in Z_p^n$及l维线性子空间E_l使得

$$|S_{(F)}(v,t_v+w)|^2=\frac{1}{p^l}I_{E_l}(w),w\in Z_p^n$$

令$F^*(x)=F(x)-(t_1\cdot x,t_2\cdot x,\cdots,t_k\cdot x),t=(t_1,t_2,\cdots,t_k),t_i\in Z_p^n$,$i=1,\cdots,k$满足$t_v=v\cdot t$,则

$$|S_{(F^*)}(v,w)|^2=|S_{(v\cdot F^*)}(w)|^2=|S_{(v\cdot F)}(t_v+w)|^2=|S_{(F)}(v,t_v+w)|^2\frac{1}{p^l}I_{E_l}(w)$$

(下转 70 页)