广义向量 Bent 函数

张文英[***]　武传坤[**]　黄晓英[*]　李世取[*]

[*](郑州信息工程学院信息研究系　郑州　450002)

[**](中国科学院软件所信息安全国家重点实验室　北京　100080)

摘 要： 该文完善并拓展了 Nyberg(1991)的关于广义向量 Bent 函数性质的结论，相应于 Nyberg 给出的正则广义向量 Bent 函数，提出了“负则的广义向量 Bent 函数”的概念；得到有偶数个输入的负则的广义向量 Bent 函数输出维数也不大于输入维数的一半；证明了奇数个输入的正则和负则的广义向量 Bent 函数都不存在，这些结果的给出，可使密码设计者避免一味去寻找某类不存在的函数。该文还给出了广义向量 Bent 函数的一种递归构造法。

关键词： 广义 Bent 函数，广义向量 Bent 函数， Chrestenson 循环谱

中图分类号： TN918.1　　**文献标识码：** A　　**文章编号：** 1009-5896(2005)01-0119-04

Generalized Vector Bent Functions

Zhang Wen-ying[***]　Wu Chuan-kun[**]　Huang Xiao-ying[*]　Li Shi-qu[*]

[*](*Dept ot Info. Research, Information Engineering Institute*, *Zhengzhou* 450002, *China*)

[**](*The State Key Lab of Info.Security, Institude of Software, Chinese Academy of Sciences, Beijing* 100080, *China*)

Abstract This paper generalizes the conclusion of Perfect nonlinear S-boxes by Nyberg(1991), and introduces the conception of inverse regular generalized vector Bent function. It shows that for inverse regular generalized vector Bent function $f^{(m)}(x)$ with even variables, m is no more than half of n. It also shows that when the input dimension n is odd, the regular generalized vector Bent function and the inverse regular generalized vector Bent function do not exist. This may prevent the cryptology designer from seeking the inexistent function. A method for recursively constructing vector generalized Bent function is presented.

Key words Generalized Bent functions, Generalized vector Bent functions, Chrestenson spectrum

1 引言

如文献[1]所述，由于“加密算法标准化的需要”、“多级安全的需要”和“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，多输出的逻辑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。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，97 年许成谦，杨义先，胡正名在文献[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，文献[5]的研究结果表明，“Bent 互补函数族”在区分初始信号及并元移位信号方面有着重要的应用，而向量 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 维向量 Bent 函数）正是一类特殊的“Bent 互补函数族”。综上，向量 Bent 函数的性质及构造方法是一个十分有意义的课题。

随着计算机及通信技术的发展，密码更多地用到了有限域上的逻辑函数，所以对有限域上逻辑函数密码性质的研究也是一件很有意义的事情。1985 年，Kuma 在文献[7]中把 Bent 函数的概念推广为有限域上的广义 Bent 函数，继之，1991 年，Nyberg 在文献[8]中将二元域上向量 Bent 函数的概念推广为素域上广义向量 Bent 函数，并得到：当输入维数 n 为偶数时，若 $\boldsymbol{f}^{(m)}(\boldsymbol{x})=[f_1(\boldsymbol{x})\cdots f_m(\boldsymbol{x})]$， $\boldsymbol{x}\in Z_p^n$ 是 m 维广义向量 Bent 函数，且对任意的 $\mathbf{0}\neq\boldsymbol{\lambda}\in Z_p^m$，都存在 Z_p^m 上的 p 值逻辑函数 $g(\boldsymbol{y})$，使得 $S_{(\lambda\cdot f^{(m)})}(\mathbf{0})=p^{-n/2}u^{g(\lambda)}$（此时，称 $\boldsymbol{f}^{(m)}(\boldsymbol{x})$为正则的[8]），那么 $2m\le n$．本文将上述结论加以推广得到了：当 n 为偶数时，若 $\boldsymbol{f}^{(m)}(\boldsymbol{x})$， $\boldsymbol{x}\in Z_p^n$ 是 m 维广义向量 Bent 函数，且满足对任意的 $\mathbf{0}\neq\boldsymbol{\lambda}\in Z_p^m$，都存在 Z_p^m

2003-08-12 收到，2003-12-25 改回

上 p 的值逻辑函数 $g(y)$，使得 $S_{(\lambda\cdot f^{(m)})}(\mathbf{0}) = -p^{-n/2}u^{g(\lambda)}$，那么也有 $2m \le n$，与 Nyberg 提出的正则广义向量 Bent 函数的概念相对应，在此称这类函数为“负则的广义向量 Bent 函数”，为了说明负则的广义向量 Bent 函数的存在性，文中给出了这类函数的具体例子。文章还运用二次 Gauss 和的有关性质证明了：当输入变量的个数 n 为奇数时，正则和负则的多维广义向量 Bent 函数都不存在。这就完善并拓展了 Nyberg 关于正则广义向量 Bent 函数的性质的相关结论。在文章的最后我们还给出了广义向量 Bent 函数的一种递归构造法。

本文中约定：p 是素数，$u = \exp[(2\pi i)/p]$ 是 p 次本原单位根，Z_p 表示整数模 p 的剩余类域，亦称为素域，Z_p^n 表示 Z_p 上的 n 维向量空间。

2 一类广义向量 Bent 函数的变元个数与维数之间的制约关系

定义 1[7] 设 $f(\boldsymbol{x}): Z_p^n \to Z_p$，$\boldsymbol{x} \in Z_p^n$ 是 p 值逻辑函数，$S_{(f)}(\boldsymbol{w}) = p^{-n}\sum_{x\in Z_p^n} u^{(f(x)-\boldsymbol{w}\cdot\boldsymbol{x})}$，$\boldsymbol{w} \in Z_p^n$ 是 $f(\boldsymbol{x})$ 的 Chrestenson 循环谱，若对任意的 $\boldsymbol{w} \in Z_p^n$，都有 $|S_{(f)}(\boldsymbol{w})| = p^{-n/2}$，则称 $f(\boldsymbol{x})$ 是广义 Bent 函数。

定义 2[8] 设 $\boldsymbol{f}^{(m)}(\boldsymbol{x}) = [f_1(\boldsymbol{x}),\cdots,f_m(\boldsymbol{x})]$，$\boldsymbol{x} \in Z_p^n$ 是向量逻辑函数，若对任意的 $\mathbf{0} \ne \boldsymbol{\lambda} \in Z_p^m$，函数 $\boldsymbol{\lambda}\cdot\boldsymbol{f}^{(m)}(\boldsymbol{x}) = \lambda_1 f_1(\boldsymbol{x}) + \cdots + \lambda_m f_m(\boldsymbol{x})$ 都是广义 Bent 函数，则称 $\boldsymbol{f}^{(m)}(\boldsymbol{x})$ 是广义向量 Bent 函数。

仿照 Nyberg 所提出的正则广义向量 Bent 函数的概念，我们提出“负则广义向量 Bent 函数”的概念。

定义 3 $\boldsymbol{f}^{(m)}(\boldsymbol{x})$，$\boldsymbol{x} \in Z_p^n$ 是向量逻辑函数。若对任意的 $\mathbf{0} \ne \boldsymbol{\lambda} \in Z_p^m$，都有 $S_{(\boldsymbol{\lambda}\cdot\boldsymbol{f}^{(m)})}(\mathbf{0}) = -p^{-n/2}u^k$ 或 $S_{(\boldsymbol{\lambda}\cdot\boldsymbol{f}^{(m)})}(\mathbf{0}) = -ip^{-n/2}u^k$ 其中 $k = 0,1,\cdots,p-1$，则称 $\boldsymbol{f}^{(m)}(\boldsymbol{x})$ 是负则的广义向量 Bent 函数。

引理 1[7] 设 $f(\boldsymbol{x})$，$\boldsymbol{x} \in Z_p^n$ 是 p 值逻辑函数，则 $f(\boldsymbol{x})$ 是广义 Bent 函数的充要条件是：

(1) 当 n 为偶数，或 n 为奇数且 $p \equiv 1 \bmod 4$ 时，

$$S_{(f)}(\boldsymbol{w}) \in \left\{\pm\frac{1}{p^{n/2}}, \pm\frac{u}{p^{n/2}}, \cdots, \pm\frac{u^{p-1}}{p^{n/2}}\right\},\quad \boldsymbol{w} \in Z_p^n;$$

(2) 当 n 为奇数且 $p \equiv 3 \bmod 4$ 时，

$$S_{(f)}(\boldsymbol{w}) \in \left\{\pm\frac{i}{p^{n/2}}, \pm\frac{iu}{p^{n/2}}, \cdots, \pm\frac{iu^{p-1}}{p^{n/2}}\right\},\quad \boldsymbol{w} \in Z_p^n。$$

注：由引理 1 我们知道素域 Z_p 上任意广义 Bent 函数的 Chrestenson 循环谱都形如 $u^k p^{-n/2}$ 或 $iu^k p^{-n/2}$，$k = 0,1,\cdots,p-1$ 之前加一个正负号，且同一个函数在 Z_p^n 中各点的 Chrestenson 循环谱的“符号”总是同时为正或同时为负。所以在考察素域上一个广义 Bent 函数的 Chrestenson 循环谱的“符号”时，只须考察它在零向量处的符号。

引理 2[8] 设 $\boldsymbol{f}^{(m)}(\boldsymbol{x}) = [f_1(\boldsymbol{x}),\cdots,f_m(\boldsymbol{x})]$，$\boldsymbol{x} \in Z_p^n$，是 p 值多输出逻辑函数，若记 $a_0 = \#\{\boldsymbol{x} \mid \boldsymbol{x} \in Z_p^n, \boldsymbol{f}^{(m)}(\boldsymbol{x}) = [0,0,\cdots,0]\}$，则

$$\sum_{\lambda\ne 0} S_{(\boldsymbol{\lambda}\cdot\boldsymbol{f}^{(m)})}(\mathbf{0}) = p^{-n}(a_0 p^m - p^n) \tag{1}$$

引理 3[9] 设 p 是素数，u 是 p 次本原单位根，即 $u = \exp[(2\pi i)/p]$，则 $\sum_{i=0}^{p-1} b_i u^i = 0$ 的充要条件是 $b_0 = b_1 = \cdots = b_{p-1}$。

引理 4[8] 设 n 是偶数，$\boldsymbol{f}^{(m)}(\boldsymbol{x}) = [f_1(\boldsymbol{x}),\cdots,f_m(\boldsymbol{x})]$ 是 n 元 m 维广义向量 Bent 函数，若 $\boldsymbol{f}^{(m)}(\boldsymbol{x})$ 是正则的，那么 $2m \leqslant n$。

有了上述一系列的引理作准备，下面给出本节的一个主要结论：

定理 1 设 n 是偶数，$\boldsymbol{f}^{(m)}(\boldsymbol{x}) = [f_1(\boldsymbol{x}),\cdots,f_m(\boldsymbol{x})]$ 是 n 元 m 维广义向量 Bent 函数，若 $\boldsymbol{f}^{(m)}(\boldsymbol{x})$ 是负则的，那么也有 $2m \leqslant n$。

定理 1 的证明与引理 4 的证明类似，从略。

需要特别指出的是：满足定理 1 中条件的函数的确是存在的。

例 1 若设 $u = -(1/2) + (\sqrt{3}i/2)$ 是 3 次本原单位根. 经计算得下述 3 值 4 元 2 维广义向量 Bent 函数 $[f_1, f_2] = [x_1x_2 + x_1^2 + 2x_2^2 + x_3x_4,\ x_1x_2 + x_3^2 + 2x_4^2 + 2x_3x_4]$，$[x_1,x_2,x_3,x_4] \in Z_3^4$ 满足：对任意的 $\mathbf{0} \ne [\lambda_1,\lambda_2] \in Z_3^2$，$\lambda_1 f_1 + \lambda_2 f_2$ 的 Chrestenson 循环谱都形如 $-u^k/9$，$k = 0,1$ 或 2，所以 $[f_1, f_2]$ 就是一个满足定理 1 中的条件的 4 元 2 维 3 值广义向量 Bent 函数。

这样我们又得到了另一类输出维数不大于输入维数一半的广义向量 Bent 函数。

引理 4 和定理 1 中提到了两类很特殊的广义向量 Bent 函数—对任意的 $(0,\cdots,0) \ne \boldsymbol{\lambda} \in Z_p^m$，$S_{(\boldsymbol{\lambda}\cdot\boldsymbol{f}^{(m)})}(\mathbf{0})$ 的表达式中 $p^{-2/n}u^k$ 的“符号”恒为正或恒为负，我们不禁会问：如果当 $\boldsymbol{\lambda}$ 取遍 Z_p^m 时，$S_{(\boldsymbol{\lambda}\cdot\boldsymbol{f}^{(m)})}(\mathbf{0})$ 的“符号”有正有负，$\boldsymbol{f}^{(m)}(\boldsymbol{x})$ 满足什么条件时，也有 $2m \leqslant n$？下面的定理 2 回答了这个问题，首先介绍一些记号：

设 n 为偶数，$\boldsymbol{f}^{(m)}(\boldsymbol{x}) = [f_1(\boldsymbol{x}) \cdots f_m(\boldsymbol{x})]$，$\boldsymbol{x} \in Z_p^n$ 是广义向量 Bent 函数，由引理 1，对任意的 $\boldsymbol{\lambda} \ne \mathbf{0}$，存在 $k \in Z_p$，使得：$S_{(\boldsymbol{\lambda}\cdot\boldsymbol{f}^{(m)})}(\mathbf{0})$ 等于 $p^{-n/2}u^k$ 或 $-p^{-n/2}u^k$，若记：

$$r_k^+ = \#\{\boldsymbol{\lambda} \mid \boldsymbol{\lambda} \ne \mathbf{0}, S_{(\boldsymbol{\lambda}\cdot\boldsymbol{f}^{(m)})}(\mathbf{0}) = p^{-n/2}u^k\}, r_k^- = \#\{\boldsymbol{\lambda} \mid \boldsymbol{\lambda} \ne \mathbf{0}, S_{(\boldsymbol{\lambda}\cdot\boldsymbol{f}^{(m)})}(\mathbf{0})$$

$=-p^{-n/2}u^k\}$，则

$$\sum_{\lambda\neq 0} S_{(\lambda\cdot f^{(m)})}(\mathbf{0}) = p^{-n/2}\sum_{k\in Z_p}(r_k^+ - r_k^-)\,u^k \tag{2}$$

定理 2　设 n 为偶数，$f^{(m)}(x)$，$x\in Z_p^n$ 是广义向量 Bent 函数，如果 $p\mid\sum_{i\in Z_p} r_i^-$，那么 $2m\leqslant n$.

证明　由引理 2 及式(2)得

$$p^{-n}(a_0p^m - p^n) = p^{-2/n}\sum_{i\in Z_p}(r_i^+ - r_i^-)\,u^i$$

故 $a_0p^{m-n/2} - p^{n/2} = \sum_{i\in Z_p}(r_i^+ - r_i^-)u^i$，由引理 3 得：上式中除了 u^0 的系数外，其他 u^i，$1\leq i\leq p-1$ 的系数应该都相等，即 $r_1^+ - r_1^- = r_2^+ - r_2^- = \cdots = r_{p-1}^+ - r_{p-1}^-$，而 $(r_0^+ - r_0^-) - (r_i^+ - r_i^-) = a_0p^{m-n/2} - p^{n/2}$, $1\leq i\leq p-1$，所以 $r_i^+ = r_i^- + (r_0^+ - r_0^-) - a_0p^{m-n/2} - p^{n/2}$, $1\leq i\leq p-1$。又

$$\begin{aligned} p^m - 1 &= \sum_{i\in Z_p}(r_i^+ + r_i^-) = r_0^+ + r_0^- + r_1^+ + r_1^- + \cdots + r_{p-1}^+ + r_{p-1}^- \\ &= p(r_0^+ - r_0^-) + 2\sum_{i\in Z_p} r_i^- - (p-1)(a_0p^{m-n/2} - p^{n/2}) \end{aligned} \tag{3}$$

因 $p\nmid p^m-1$，从而 p 不整除式(3)右边，于是若 $p\mid\sum_{i\in Z_p} r_i^-$，则 $p\nmid a_0p^{m-n/2} - p^{n/2}$，又因 n 是偶数时 $p\mid p^{n/2}$，所以 $p\nmid a_0p^{m-n/2}$，故 $m\leq n/2$，即 $2m\leqslant n$。　　证毕

3　一类正则或负则广义向量 Bent 函数的不存在性

前面我们讨论了 n 为偶数时，正则或负则的广义向量 Bent 函数的输出维数 m 不大于输入维数 n 的一半，当输入变量的维数 n 为奇数时，结论又如何？下面的定理表明当 n 为奇数时，正则或负则的广义向量 Bent 函数根本就不存在。首先考虑 p=3 的情形：

定理 3　设 n 是奇数，$m\geqslant 2$，则不存在满足条件："对任意的 $\mathbf{0}\neq\lambda\in Z_3^m$，恒有 $S_{(\lambda\cdot f^{(m)})}(\mathbf{0}) = i3^{-n/2}u^k$（或 $S_{(\lambda\cdot f^{(m)})}(\mathbf{0}) = -i3^{-n/2}u^k$），$k=0,1,2$" 的 n 元广义向量 Bent 函数。

证明　用反证法. 设 $f^{(m)}(x) = [f_1(x),\cdots,f_m(x)]$，$x\in Z_3^n$ 是广义向量 Bent 函数且对任意的 $\lambda\in Z_3^m, \lambda\neq[0,\cdots,0]$ 恒有 $S_{(\lambda\cdot f^{(m)})}(\mathbf{0}) = i3^{-n/2}u^k$，$k=0,1,2$，一方面由引理 2 有 $\sum_{\lambda\neq 0} S_{(\lambda\cdot f^{(m)})}(\mathbf{0}) = 3^{-n}(a_03^m - 3^n)$，另一方面，因

$$\begin{aligned} \sum_{\lambda\neq 0} S_{(\lambda\cdot f^{(m)})}(\mathbf{0}) &= i3^{-n/2}\left[r_0 + r_1\left(-\frac{1}{2}+\frac{\sqrt{3}}{2}i\right) + r_2\left(-\frac{1}{2}-\frac{\sqrt{3}}{2}i\right)\right] \\ &= i3^{-n/2}\left[r_0 - \frac{r_1+r_2}{2} - \frac{\sqrt{3}}{2}i(r_2-r_1)\right] \end{aligned}$$

故 $a_03^{m-n/2} - 3^{n/2} = i[r_0 - (r_1+r_2)/2] + (\sqrt{3}/2)(r_2-r_1)$，进而有 $r_0 - (r_1+r_2)/2 = 0$，$2r_0 = r_1 + r_2$，又 $r_0 + r_1 + r_2 = 3^m - 1$，故 $3r_0 = 3^m - 1$，$m=0$，这不可能. 同样可以证明不存在对任意的 $[0,\cdots,0]\neq\lambda\in Z_3^m$，恒有 $S_{(\lambda\cdot f^{(m)})}(\mathbf{0}) = -i3^{-n/2}u^k$，$k$=0，1，2 的 3 值广义向量 Bent 函数。所以定理结论正确。

证毕

关于 p=3 的情形的结论启发我们去探讨 p 为一般的素数时，是否也会有相应的结论？

引理 5[9]　设 p 是素数，若 p=1 mod 4，则有二次 Guass 和[9]：$\sqrt{p} = \sum_{j=1}^{p-1}\left(\frac{j}{p}\right)u^j$；若 p=3 mod 4，则有二次 Guass 和：$i\sqrt{p} = \sum_{j=1}^{p-1}\left(\frac{j}{p}\right)u^j$。其中 $\left(\frac{j}{p}\right)$ 为 Legendre 符号：当 j 为 p 的二次剩余时，有 $\left(\frac{j}{p}\right)=1$；当 j 为 p 的非二次剩余时，有 $\left(\frac{j}{p}\right)=-1$。

定理 4　设 n 是奇数，p 是素数，i 是纯虚数，当 p=1 mod 4 时，不存在满足条件："对任意的 $\mathbf{0}\neq\lambda\in Z_p^m$，都有 $S_{(\lambda\cdot f^{(m)})}(\mathbf{0}) = p^{-n/2}u^{g(\lambda)}$（或 $S_{(\lambda\cdot f^{(m)})}(\mathbf{0}) = -p^{-n/2}u^{g(\lambda)}$）" 的广义向量 Bent 函数；当 p=3 mod 4 时，不存在满足条件："对任意的 $\mathbf{0}\neq\lambda\in Z_p^m$，都有 $S_{(\lambda\cdot f^{(m)})}(\mathbf{0}) = ip^{-n-2}u^{g(\lambda)}$（或 $S_{(\lambda\cdot f^{(m)})}(\mathbf{0}) = -ip^{-n/2}u^{g(\lambda)}$）" 的广义向量 Bent 函数。

证明　只证 p=3 mod 4 的情形，p=1 mod 4 时，类似可证。

假设对任意的 $\lambda\in Z_p^m$，$\lambda\neq[0,\cdots,0]$，都有 $S_{(\lambda\cdot f^{(m)})}(\mathbf{0}) = ip^{-n/2}u^k$，$k\in Z_p$，由引理 3 得

$$p^{-n}(a_0p^m - p^n) = \sum_{\lambda\neq 0} S_{(\lambda\cdot f^{(m)})}(\mathbf{0}) = ip^{-n/2}\sum_{k\in Z_p} r_k u^k \tag{4}$$

其中 $r_k = \#\{\lambda \mid \mathbf{0}\neq\lambda\in Z_p^m, S_{(\lambda\cdot f^{(m)})}(\mathbf{0}) = ip^{-n/2}u^k\}$，$k\in Z_p$。

对式（4）进行恒等变形得

$$i\sqrt{p}(p^{(n-1)/2} - a_0p^{m-(n+1)/2}) = \sum_{k\in Z_p} r_k u^k \tag{5}$$

由引理 5

$$i\sqrt{p} = \sum_{j=1}^{p-1}\left(\frac{j}{p}\right)u^j \tag{6}$$

将之代入式（5）得

$$\sum_{j=1}^{p-1}\left(\frac{j}{p}\right)(p^{(n-1)/2} - a_0p^{m-(n+1)/2})\,u^j = \sum_{k\in Z_p} r_k u^k \tag{7}$$

把式（7）合并同类项得

$$r_0 + \sum_{k=1}^{p-1}\left[r_k - \left(\frac{k}{p}\right)\left(p^{(n-1)/2} - a_0p^{m-(n+1)/2}\right)\right]u^k = 0 \tag{8}$$

再由引理 3 得 $r_0 = r_k - (k/p)(p^{(n-1)/2} - a_0p^{m-(n+1)/2})$，$k=1,\cdots,p-1$，于是

$$r_k = r_0 + (k/p)(p^{(n-1)/2} - a_0 p^{m-(n+1)/2}), \quad k = 1, \cdots, p-1 \tag{9}$$

$$\begin{aligned} p^m - 1 &= r_0 + r_1 + \cdots + r_{p-1} \\ &= pr_0 + (p^{(n-1)/2} - a_0 p^{m-(n+1)/2}) \sum_{j=1}^{p-1} \left(\frac{j}{p}\right) \\ &= pr_0 + (p^{(n-1)/2} - a_0 p^{m-(n+1)/2}) \cdot i\sqrt{p} \end{aligned}$$

所以 $pr_0 = p^m - 1$，此为矛盾。同样可以证明不存在对任意的 $\boldsymbol{\lambda} \in Z_p^m$，$\boldsymbol{\lambda} \neq [0, \cdots, 0]$，恒有 $S_{(\boldsymbol{\lambda} \cdot f^{(m)})}(\mathbf{0}) = -ip^{-n/2} u^k$，$k \in Z_p$ 的 3 值广义向量 Bent 函数。 证毕

上面的定理表明：若 n 是奇数，不存在这样的 n 元广义向量 Bent 函数 $f^{(m)}(x)$，使得对任意 $\boldsymbol{\lambda} \in Z_p^m, \boldsymbol{\lambda} \neq [0, \cdots, 0]$，都有 $S_{(\boldsymbol{\lambda} \cdot f^{(m)})}(\mathbf{0})$ 的表达式中 $p^{-n/2} u^{g(\boldsymbol{\lambda})}$（或 $ip^{n/2} u^{g(\boldsymbol{\lambda})}$）的系数全为正或全为负。

推论 对于任一关于奇数个变元的广义 Bent 函数 $f(x)$，$x \in Z_p^n$，总存在不为 0 的 k_1，$k_2 \in Z_p$ 及 $w, v \in Z_p^n$ 使得 $S_{(k_1 f)}(w)$，$w \in Z_p^n$ 与 $S_{(k_2 f)}(v)$，$v \in Z_p^n$ 的“符号”相反。

证明 在定理 4 中令 $m = 1$，再利用引理 1 之后的“注”便得结论。

例 2 可以验证 $f(x) = x_1^2 + x_2^2 + x_3^2, x = (x_1, x_2, x_3) \in Z_3^3$，是 3 元 1 维广义 Bent 函数，$S_{(f)}(\mathbf{0}) = -i/(3\sqrt{3})$, $S_{(2f)}(\mathbf{0}) = i/(3\sqrt{3})$，即 $S_{(f)}(\mathbf{0})$ 与 $S_{(2f)}(\mathbf{0})$ 的“符号”相反。

4 广义向量 Bent 函数的构造

关于正则广义向量 Bent 函数的构造，文献[8]中曾经给出了一种基于 m 序列的状态转移矩阵的典型构造法，作者也曾经对广义向量 Bent 函数的构造进行过一系列的探讨，见文献[10]，下面只给出广义向量 Bent 函数的一种递归构造法。

定理 5 设 $[f_1(x^{(1)}), f_2(x^{(1)}), \cdots, f_m(x^{(1)})]$，$x^{(1)} \in Z_p^{n_1}$ 和 $[g_1(x^{(2)}), g_2(x^{(2)}), \cdots, g_m(x^{(2)})]$，$x^{(2)} \in Z_p^{n_2}$ 都是 m 维广义向量 Bent 函数，则下述 $n_1 + n_2$ 元向量逻辑函数：

$$f_1(x^{(1)}) + g_1(x^{(2)}), f_2(x^{(1)}) + g_2(x^{(2)}), \cdots, f_m(x^{(1)}) + g_m(x^{(2)}) \tag{10}$$

也是 m 维广义向量 Bent 函数. 并且若 $[f_1, f_2, \cdots, f_m]$，$[g_1, g_2, \cdots, g_m]$ 两者之中有一组是正则的，另一组是负则的，那么式(10)中逻辑函数是负则的。

例 3 根据文献[8]，$[g_1(y), g_2(y)] = [y_1 y_2 + y_3 y_4, y_1 y_4 + y_2 y_3]$，$y = [y_1, y_2, y_3, y_4] \in Z_3^4$ 是正则的二维广义 Bent 函数，再由例 1：$[f_1, f_2] = [x_1 x_2 + x_1^2 + 2x_2^2 + x_3 x_4, x_1 x_2 + x_3^2 + 2x_4^2 + 2x_3 x_4]$，$x = [x_1, x_2, x_3, x_4] \in Z_3^4$ 是负则的二维广义 Bent 函数，所以由定理 5 可以得到 $[f_1(x) + g_1(y), f_2(x) + g_2(y)]$ 是负则的 8 元 2 维广义向量 Bent 函数。

参 考 文 献

[1] 冯登国, 吴文玲. 分组密码的设计与分析. 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. 北京: 国防工业出版社, 1994, 第六章.

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

[4] Zheng Y, Pieprzyk J, Seberr J Y. HAVAL—A one way hashing algorithm with variable length output, Advances in Cryptology-AUSCRYPT'92, Queens land: 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. 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. 北京: 科学出版社, 2000: 118 – 120.

[7] Kumar P, Scholtz R, Welch L. Generalized Bent functions and their properties. *J. Combinatorial Theory*, 1985, 40(A): 90 – 107.

[8] Nyberg K. Perfect nonlinear S-boxes, Advances in Cryptology-Eurocrypt'91, Brighton: Springer-Verlag, 1991: 378 – 383.

[9] 柯召, 孙琦. 数论讲义. 北京: 高等教育出版社, 1987,第四章.

[10] 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]. 第三届中国信息和通信安全学术会议论文集 CCICS 2003, 武汉, 科学出版社, 2003: 290 – 296.

张文英： 女，1970 年生，副教授，博士，研究方向为密码学.

武传坤： 男，1964 年生，教授，博士生导师，研究方向为密码学和网络安全.

黄晓英： 女，1962 年生，副教授，博士，研究方向为密码学.

李世取： 男，1945 年生，教授，博士生导师，研究方向为密码学.