Bent 函数的一种迭代构造

曾祥勇[1,2],胡 磊[2]
(1.湖北大学数学与计算机科学学院,湖北武汉 430062; 2.中国科学院研究生院信息安全国家重点实验室,北京 100049)

摘 要: 对于不小于 4 的偶数 n,建立了由 4 个 n-元 Bent 函数构造 $(n+2)$-元 Bent 函数的一个充要条件.提出了由 n-元 Bent 函数构造 $(n+2)$-元 Bent 函数的一种迭代构造方法,也对所构造的 Bent 函数的代数次数进行了分析.这种迭代方法统一并推广了以前的两种 Bent 函数的构造.

关键词: Bent 函数; Walsh 谱; 非线性度; 代数次数
中图分类号: TN918.1; TN918.2 **文献标识码:** A **文章编号:** 0372-2112 (2010) 12-2724-05

An Iterative Construction of Bent Functions

ZENG Xiang-yong[1,2], HU Lei[2]
(1. *Faculty of Mathematics and Computer Science, Hubei University, Wuhan, Hubei* 430062, *China*;
2. *The State Key Laboratory of Information Security, Graduate School of Chinese Academy of Sciences, Beijing* 100049, *China*)

Abstract: For an even integer n not less than 4, a sufficient and necessary condition was established for constructing a Bent function in $n+2$ variables from 4 Bent functions in n variables. An iterative construction of Bent functions was proposed to construct $(n+2)$-variable Bent functions from n-variable Bent functions. The algebraic degree of some Bent functions constructed by the proposed method was also analyzed. The iterative method unifies and generalizes two previous constructions of Bent functions.

Key words: Bent function; Walsh spectrum; nonlinearity; algebraic degree

1 引言

布尔函数在密码学和编码学等领域有着重要的应用,非线性度高的布尔函数常用于设计流密码的密钥流生成器和分组密码的 S-盒[1~6].Bent 函数作为达到非线性度极大值的一类布尔函数,受到了人们的普遍关注[7].同时,这类函数在组合学上也有重要的研究价值[8~10].尽管如此,目前已知的 Bent 函数的构造还很有限,其分类问题还远未能解决.

M-M 构造[11]和 PS 构造[8,12]是设计 Bent 函数的两种重要方法,在此基础上,其它的一些方法也被人们提出[13,14].同时,人们也十分关注从幂函数、二项式函数以及二次函数中寻找 Bent 函数[15~19].另一种研究 Bent 函数的思路是运用已知的 Bent 函数来构造新的 Bent 函数,如 Hou 和 Langevin 提出了一种由 Bent 函数构造相同变元 Bent 函数的方法[20].还有一种由 n-元 Bent 函数迭代构造 $(n+2)$-元 Bent 函数的方法,较为人们所熟悉,即通过级联两个 n-元 Bent 函数 $f(x)$和 $g(x)$,可获得 $(n+2)$-元 Bent 函数

$$f(x)\|f(x)\|g(x)\|g(x)+1 \tag{1}$$

这种构造也被 Carlet 等人用来研究 Bent 函数的正规扩张[21].最近,Climent 等人也对这种构造进行了仔细的分析,并考虑了由此生成的 Bent 函数的计数问题[22],同时提出了由存在二阶离散导函数 $(D_b(D_af))(x)$恒等于 1 的 n-元 Bent 函数 $f(x)$构造 $(n+2)$-元 Bent 函数

$$f(x)\|f(x+a)\|f(x+b)\|f(x+a+b)+1 \tag{2}$$

的方法[23].限制 Bent 函数在余维数为 2 的仿射子空间上也可能得到 Bent 函数,基于此想法 Canteaut 和 Charpin 利用 Bent 函数的对偶函数的性质刻画了一个 $(n+2)$-元 Bent 函数分解成 4 个 n-元 Bent 函数的充要条件[24],其中的讨论涉及到对偶函数的二阶离散导函数.另外,一些启发式的搜索算法也常用于设计 Bent 函数[25].

文献[24]的研究表明,一个 $(n+2)$-元 Bent 函数可以由 4 个具有至多 5 个不同谱值的 n-元布尔函数级联而成.本文的主要目的是研究 4 个 n-元 Bent 函数在什么情况下能级联成一个 $(n+2)$-元 Bent 函数,我们首先建立了由 4 个 n-元 Bent 函数迭代构造 $(n+2)$-元 Bent 函数的一个充要条件;然后在此基础上,我们提出了对

收稿日期:2009-11-12;修回日期:2010-02-27
基金项目:国家自然科学基金(No.60973130,No.60773134,No.10990011);国家重点基础研究发展规划(973 计划)项目(No.2007CB311201);湖北省自然科学基金重点项目(杰出青年人才)(No.2009CDA147)

任意向量 $\boldsymbol{a}\in F_2^n$,由 n-元 Bent 函数 $f(\boldsymbol{x})$和 $g(\boldsymbol{x})$构造($n+2$)-元 Bent 函数

$$f(\boldsymbol{x})\,\|\,f(\boldsymbol{x}+\boldsymbol{a})\,\|\,g(\boldsymbol{x})\,\|\,g(\boldsymbol{x}+\boldsymbol{a})+1 \qquad (3)$$

的方法.当 $\boldsymbol{a}=0$ 时,这就是等式(1)中的构造;当 $g(\boldsymbol{x})=f(\boldsymbol{x}+\boldsymbol{b})$且$(D_b(D_af))(\boldsymbol{x})\equiv 1$ 时,这就是等式(2)中的构造.在我们的构造中不需要对$(D_b(D_af))(\boldsymbol{x})$的性质作任何限制.我们的方法统一了上述两种构造,而且等式(3)中的向量 $\boldsymbol{a}$ 可以取任意值.

本文余下的部分在第二节中是一些预备知识;第三节我们描叙了由 4 个 n-元 Bent 函数迭代构造($n+2$)-元 Bent 函数的一个充要条件,并且提出了一种 Bent 函数的迭代构造;第四节为结论.

2　预备知识

记 F_2 是由 0 和 1 两个元素组成的有限域,F_2^n 表示由所有向量 $\boldsymbol{a}=(a_1,a_2,\cdots,a_n)$,$a_i\in F_2$ 组成的 n 维向量空间.向量 $\boldsymbol{a}=(a_1,a_2,\cdots,a_n)$的汉明权重被定义为自然数 $w(a)=\sum_{i=1}^{n}a_i$.一个 n-元布尔函数 f 是从 F_2^n 到 F_2 的一个函数,它有如下的多项式表示:

$$f(x_1,x_2,\cdots,x_n)=\sum_{u\in F_2^n}\lambda_u\Big(\prod_{i=1}^{n}x_i^{u_i}\Big)$$

其中 $\lambda_u\in F_2$, $u=(u_1,u_2,\cdots u_n)$.

这种表达式被称为 f 的代数正规型,它的代数次数 $\deg(f)$被定义为 $w(u)$的极大值,这里 u 取遍所有使得 $\lambda_u=1$ 的 n 维向量.

对每个整数 $i(0\leqslant i\leqslant 2^n-1)$,设 $\boldsymbol{e}^i=(e_1^i,e_2^i,\cdots,e_n^i)\in F_2^n$ 使得 $i=\sum_{j=1}^{n}e_j^i2^{j-1}$.那么每个 n-元布尔函数f 对应着唯一的长度为 2^n 的(0,1)序列

$$f(\boldsymbol{e}^0),f(\boldsymbol{e}^1),\cdots,f(\boldsymbol{e}^{2^n-1})$$

这个序列被称为 f 的真值表.两个 n-元布尔函数f 和g 的汉明距离等于向量

$$(f(\boldsymbol{e}^0)+g(\boldsymbol{e}^0),f(\boldsymbol{e}^1)+g(\boldsymbol{e}^1),\cdots,f(\boldsymbol{e}^{2^n-1})+g(\boldsymbol{e}^{2^n-1}))$$

的汉明权重,这里的加法在 F_2 中进行.两个 n-元布尔函数f 和g 的级联$f(x)\,\|\,g(x)$是一个$(n+1)$-元的布尔函数,这个级联函数的真值表为

$$f(\boldsymbol{e}^0),f(\boldsymbol{e}^1),\cdots,f(\boldsymbol{e}^{2^n-1}),g(\boldsymbol{e}^0),g(\boldsymbol{e}^1),\cdots,g(\boldsymbol{e}^{2^n-1}).$$

因此这个函数可表示为$(1+z)f(\boldsymbol{x})+zg(\boldsymbol{x})$,这里 $\boldsymbol{x}\in F_2^n,z\in F_2$.

两个向量 $\boldsymbol{x}=(x_1,x_2,\cdots,x_n)$和 $\boldsymbol{y}=(y_1,y_2,\cdots,y_n)$的点乘被定义为 $\boldsymbol{x}\cdot\boldsymbol{y}=\sum_{i=1}^{n}x_iy_i$,这里的加法为模 2 相加.$n$-元布尔函数$f$ 的 Walsh 变换 W_f 是从 F_2^n 到整数环的一个函数,即

$$W_f(\boldsymbol{\lambda})=\sum_{x\in F_2^n}(-1)^{f(x)+\boldsymbol{\lambda}\cdot x}.$$

$\boldsymbol{W}_f(\lambda)$称为 f 的谱值.函数 f 是平衡的,如果 $W_f(\boldsymbol{0})=0$,即 f 的支集$\{\boldsymbol{x}\in F_2^n\,|\,f(\boldsymbol{x})=1\}$由 2^{n-1}个向量组成.布尔函数 f 的非线性度 N_f 是它和所有仿射函数的汉明距离的极小值,也可表达为

$$N_f=2^{n-1}-2^{-1}\max_{\lambda\in F_2^n}|W_f(\boldsymbol{\lambda})|.$$

当 n 为偶数时,f 的非线性度 N_f 的最大可能值为 $2^{n-1}-2^{n/2-1}$.非线性度达到这个最大值的布尔函数 f 称为 Bent 函数,它的谱值 $W_f(\boldsymbol{\lambda})$对任意 $\boldsymbol{\lambda}\in F_2^n$ 取值为 $2^{n/2}$或 $-2^{n/2}$.Bent 函数在密码学和组合学等领域中有着重要的应用.

设偶数 $n\geqslant 4$,那么 n-元 Bent 函数 f 的代数次数至多为 $n/2$[8].当 f 的代数次数为 $n/2$ 时,我们称它为代数次数最优的 Bent 函数.

n-元布尔函数f 在向量 $\boldsymbol{a}\in F_2^n$ 处的离散导函数定义为:

$$(D_af)(x)=f(x)+f(x+a).$$

它也是一个 n-元布尔函数,其性质与 f 的谱值密切相关.对于 Bent 函数,能用其导函数进行如下等价刻画.

引理 1[8]　n-元布尔函数f 是 Bent 函数当且仅当 f 在任意非零向量 $\boldsymbol{a}\in F_2^n$ 处的导函数$(D_af)(\boldsymbol{x})$是平衡的.

3　Bent 函数的一种迭代构造

本节中我们总是假定 n 为偶数且 $n\geqslant 4$.

我们首先讨论了由 4 个 n-元 Bent 函数构造($n+2$)-元 Bent 函数的一个充要条件,然后提出了由 n-元 Bent 函数构造$(n+2)$-元 Bent 函数一种迭代方法,并讨论了所得函数的代数次数.

引理 2　设 $f(\boldsymbol{x})$和 $g(\boldsymbol{x})$是两个 n-元布尔函数,对于任何向量 $\boldsymbol{a}\in F_2^n$,布尔函数 $f(\boldsymbol{x})+g(\boldsymbol{x}+\boldsymbol{a})$和 $g(\boldsymbol{x})+f(\boldsymbol{x}+\boldsymbol{a})$的支集含有相同的向量数目.

证明　对任何给定的向量 $\boldsymbol{a}\in F_2^n$,$f(\boldsymbol{x}_0)+g(\boldsymbol{x}_0+\boldsymbol{a})=1$ 等价于 $f((\boldsymbol{x}_0+\boldsymbol{a})+\boldsymbol{a})+g(\boldsymbol{x}_0+\boldsymbol{a})=1$.

这说明向量 $\boldsymbol{x}_0$ 在 $f(\boldsymbol{x})+g(\boldsymbol{x}+\boldsymbol{a})$的支集中等价于 $\boldsymbol{x}_0+\boldsymbol{a}$ 在 $g(\boldsymbol{x})+f(\boldsymbol{x}+\boldsymbol{a})$的支集中.因此,$f(\boldsymbol{x})+g(\boldsymbol{x}+\boldsymbol{a})$和 $g(\boldsymbol{x})+f(\boldsymbol{x}+\boldsymbol{a})$的支集具有相同的向量数目.　　证毕

定理 1　设 f_1,f_2,f_3 和 f_4 是 n-元 Bent 函数.那么 $f_1(\boldsymbol{x})\,\|\,f_2(\boldsymbol{x})\,\|\,f_3(\boldsymbol{x})\,\|\,f_4(\boldsymbol{x})$是$(n+2)$-元 Bent 函数当且仅当对任意向量 $\boldsymbol{a}\in F_2^n$ 和集合$\{2,3,4\}$上的任一置换 σ,$(n+1)$-元布尔函数 $f_1(\boldsymbol{x})+f_{\sigma(2)}(\boldsymbol{x}+\boldsymbol{a})\,\|\,f_{\sigma(3)}(\boldsymbol{x})+f_{\sigma(4)}(\boldsymbol{x}+\boldsymbol{a})$是平衡的.

证明　布尔函数 $f_1(\boldsymbol{x})\,\|\,f_2(\boldsymbol{x})\,\|\,f_3(\boldsymbol{x})\,\|\,f_4(\boldsymbol{x})$的

表达式 $F(\boldsymbol{x},y,z)$可写为

$$F(\boldsymbol{x},y,z)=(1+y)(1+z)f_1(\boldsymbol{x})+y(1+z)f_2(\boldsymbol{x})+(1+y)zf_3(\boldsymbol{x})+yzf_4(\boldsymbol{x})$$

其中 $\boldsymbol{x}\in F_2^n, y,z\in F_2$.

由引理 1, $F(\boldsymbol{x},y,z)$是 Bent 函数当且仅当对任意的非零向量$(\boldsymbol{a},b,c)\in F_2^n\times F_2\times F_2$,布尔函数

$$\begin{aligned}(D_{(a,b,c)}F)(\boldsymbol{x},y,z)&=F(\boldsymbol{x},y,z)+F(\boldsymbol{x}+\boldsymbol{a},y+b,z+c)\\&=(1+y)(1+z)f_1(\boldsymbol{x})+y(1+z)\\&\cdot f_2(\boldsymbol{x})+(1+y)zf_3(\boldsymbol{x})+yzf_4(\boldsymbol{x})\\&+(1+y+b)(1+z+c)\cdot f_1(\boldsymbol{x}+\boldsymbol{a})\\&+(y+b)(1+z+c)f_2(\boldsymbol{x}+\boldsymbol{a})\\&+(1+y+b)(z+c)f_3(\boldsymbol{x}+\boldsymbol{a})\\&+(y+b)(z+c)f_4(\boldsymbol{x}+\boldsymbol{a})\end{aligned}$$

是平衡的.下面我们按照 $\boldsymbol{a},b,c$ 的取值分情况来讨论$(D_{(a,b,c)}F)(\boldsymbol{x},y,z)$是平衡函数的等价条件.

当 $\boldsymbol{a}=\boldsymbol{0}$且 $b=1,c=0$时,$(D_{(0,1,0)}F)(\boldsymbol{x},y,z)=(1+z)(f_1(\boldsymbol{x})+f_2(\boldsymbol{x}))+z(f_3(\boldsymbol{x})+f_4(\boldsymbol{x}))$作为$(n+2)$-元函数是平衡的当且仅当 $f_1(\boldsymbol{x})+f_2(\boldsymbol{x})\|f_3(\boldsymbol{x})+f_4(\boldsymbol{x})$是$(n+1)$-元平衡布尔函数.

当 $\boldsymbol{a}=\boldsymbol{0}$且 $b=0,c=1$时,$(D_{(0,0,1)}F)(\boldsymbol{x},y,z)=(1+y)(f_1(\boldsymbol{x})+f_3(\boldsymbol{x}))+y(f_2(\boldsymbol{x})+f_4(\boldsymbol{x}))$是平衡的,当且仅当 $f_1(\boldsymbol{x})+f_3(\boldsymbol{x})\|f_2(\boldsymbol{x})+f_4(\boldsymbol{x})$是$(n+1)$-元平衡布尔函数.

当 $\boldsymbol{a}=\boldsymbol{0}$且 $bc=1$时,

$$\begin{aligned}(D_{(0,1,1)}F)(\boldsymbol{x},y,z)&=(1+y+z)(f_1(\boldsymbol{x})+f_4(\boldsymbol{x}))\\&+(y+z)(f_2(\boldsymbol{x})+f_3(\boldsymbol{x}))\end{aligned}$$

是平衡的,当且仅当 $f_1(\boldsymbol{x})+f_4(\boldsymbol{x})\|f_2(\boldsymbol{x})+f_3(\boldsymbol{x})$是$(n+1)$-元平衡布尔函数.

当 $\boldsymbol{a}\neq\boldsymbol{0}$且 $b=c=0$时,

$$\begin{aligned}&(D_{(a,0,0)}F)(\boldsymbol{x},y,z)\\&=F(\boldsymbol{x},y,z)+F(\boldsymbol{x}+a,y,z)\\&=(1+y)(1+z)(D_af_1)(\boldsymbol{x})+y(1+z)(D_af_2)(\boldsymbol{x})\\&+(1+y)z(D_af_3)(\boldsymbol{x})+yz(D_af_4)(\boldsymbol{x}).\end{aligned}$$

因为 $f_i(i=1,2,3,4)$是 Bent 函数,又由引理 1 可知,对任意的非零向量 $\boldsymbol{a}\neq\boldsymbol{0}$,$(D_af_i)(\boldsymbol{x})$是平衡的.因此函数$(D_{(a,0,0)}F)(\boldsymbol{x})=(D_af_1)(\boldsymbol{x})\|(D_af_2)(\boldsymbol{x})\|(D_af_3)(\boldsymbol{x})\|(D_af_4)(\boldsymbol{x})$也是平衡的.

当 $\boldsymbol{a}\neq\boldsymbol{0}$且 $b=1,c=0$时,

$$\begin{aligned}(D_{(a,1,0)}F)(\boldsymbol{x},y,z)&=(1+y)(1+z)(D_af_1)(\boldsymbol{x})\\&+(1+z)f_1(\boldsymbol{x}+\boldsymbol{a})\\&+y(1+z)(D_af_2)(\boldsymbol{x})+(1+z)f_2(\boldsymbol{x}+\boldsymbol{a})\\&+(1+y)z(D_af_3)(\boldsymbol{x})+zf_3(\boldsymbol{x}+\boldsymbol{a})\\&+yz(D_af_4)(\boldsymbol{x})+zf_4(\boldsymbol{x}+\boldsymbol{a}).\end{aligned}$$

因此 $f_1(\boldsymbol{x})+f_2(\boldsymbol{x}+\boldsymbol{a})\|f_2(\boldsymbol{x})+f_1(\boldsymbol{x}+\boldsymbol{a})\|f_3(\boldsymbol{x})+f_4(\boldsymbol{x}+\boldsymbol{a})\|f_4(\boldsymbol{x})+f_3(\boldsymbol{x}+\boldsymbol{a})$是$(n+2)$-元平衡布尔函数.由引理 2 知,这等价于 $f_1(\boldsymbol{x})+f_2(\boldsymbol{x}+\boldsymbol{a})\|f_3(\boldsymbol{x})+f_4(\boldsymbol{x}+\boldsymbol{a})$是$(n+1)$-元平衡布尔函数,也等价于 $f_1(\boldsymbol{x})+f_2(\boldsymbol{x}+\boldsymbol{a})\|f_4(\boldsymbol{x})+f_3(\boldsymbol{x}+\boldsymbol{a})$是$(n+1)$-元平衡布尔函数.

同理可得,当 $\boldsymbol{a}\neq\boldsymbol{0}$且 $b=0,c=1$时,我们需要 $f_1(\boldsymbol{x})+f_3(\boldsymbol{x}+\boldsymbol{a})\|f_2(\boldsymbol{x})+f_4(\boldsymbol{x}+\boldsymbol{a})$是$(n+1)$-元平衡布尔函数,或者 $f_1(\boldsymbol{x})+f_3(\boldsymbol{x}+\boldsymbol{a})\|f_4(\boldsymbol{x})+f_2(\boldsymbol{x}+\boldsymbol{a})$是$(n+1)$-元平衡布尔函数;当 $\boldsymbol{a}\neq\boldsymbol{0}$且 $bc=1$时,我们需要 $f_1(\boldsymbol{x})+f_4(\boldsymbol{x}+\boldsymbol{a})\|f_2(\boldsymbol{x})+f_3(\boldsymbol{x}+\boldsymbol{a})$是$(n+1)$-元平衡布尔函数,或者 $f_1(\boldsymbol{x})+f_4(\boldsymbol{x}+\boldsymbol{a})\|f_3(\boldsymbol{x})+f_2(\boldsymbol{x}+\boldsymbol{a})$是$(n+1)$-元平衡布尔函数.

综上所述,对任意非零向量$(a,b,c)\in F_2^n\times F_2\times F_2$,布尔函数$(D_{(a,b,c)}F)(\boldsymbol{x},y,z)$是平衡的等价于对集合$\{2,3,4\}$的任一置换 σ 和任意向量 $\boldsymbol{a}\in F_2^n$, $f_1(\boldsymbol{x})+f_{\sigma(2)}(\boldsymbol{x}+\boldsymbol{a})\|f_{\sigma(3)}(\boldsymbol{x})+f_{\sigma(4)}(\boldsymbol{x}+\boldsymbol{a})$是平衡的.因此定理得证. 证毕

注:(1)设 $n\geqslant 4,\boldsymbol{u},\boldsymbol{v}\in F_2^n$ 是两个线性独立的非零向量,$U=<\boldsymbol{u},\boldsymbol{v}>^{\perp}$表示 $\boldsymbol{u},\boldsymbol{v}$ 生成的 F_2 上的二维子空间的对偶空间.文献[24]的定理 7 证明了 n-元 Bent 函数 f 关于空间 U 分解成 4 个具有至多 5 个谱值的布尔函数;而且每个函数都是 Bent 的当且仅当 $D_u(D_v\tilde{f})\equiv 1$,其中 $\tilde{f}$ 为 f 的对偶函数.这里的刻画需要借助对偶函数 $\tilde{f}$ 的性质.文献[24]还证明了的确存在 n-元 Bent 函数不能分解成 4 个$(n-2)$-元 Bent 函数的情形,即这种函数不能由任何 4 个$(n-2)$-元 Bent 函数级联而成;(2)设 f_1,f_2 和 f_3 是 n-元 Bent 函数.文献[26]定理 1 给出了 $f_1(\boldsymbol{x})\|f_2(\boldsymbol{x})\|f_2(\boldsymbol{x})\|f_3(\boldsymbol{x})$是 Bent 函数的两个充要条件.在本文定理 1 中令 $f_2(\boldsymbol{x})=f_3(\boldsymbol{x})$,立即可得到文献[26]定理 1.因此它可看作本文定理 1 的一个特例.

根据定理 1,我们提出下面的级联 Bent 函数生成 Bent 函数的迭代构造.

推论 1 设 $f(\boldsymbol{x})$和 $g(\boldsymbol{x})$是 n-元 Bent 函数,向量$\boldsymbol{a}\in F_2^n$.那么$(n+2)$-元布尔函数

$$f(\boldsymbol{x})\|f(\boldsymbol{x}+\boldsymbol{a})\|g(\boldsymbol{x})\|g(\boldsymbol{x}+\boldsymbol{a})+1$$

是 Bent 函数.

证明 由定理 1,要证明$(n+2)$-元布尔函数$f(\boldsymbol{x})\|f(\boldsymbol{x}+\boldsymbol{a})\|g(\boldsymbol{x})\|g(\boldsymbol{x}+\boldsymbol{a})+1$是 Bent 函数,只需证明对任意向量 $\boldsymbol{b}\in F_2^n$,$(n+1)$-元布尔函数

$$f(\boldsymbol{x})+f(\boldsymbol{x}+\boldsymbol{a}+\boldsymbol{b})\|g(\boldsymbol{x})+g(\boldsymbol{x}+\boldsymbol{a}+\boldsymbol{b})+1,$$

$$f(\boldsymbol{x})+g(\boldsymbol{x}+\boldsymbol{b})\|f(\boldsymbol{x}+\boldsymbol{a})+g(\boldsymbol{x}+\boldsymbol{a}+\boldsymbol{b})+1$$

和 $f(\boldsymbol{x})+g(\boldsymbol{x}+\boldsymbol{a}+\boldsymbol{b})+1\|f(\boldsymbol{x}+\boldsymbol{a})+g(\boldsymbol{x}+\boldsymbol{b})$

都是平衡的.

由于 $f(\boldsymbol{x})$和 $g(\boldsymbol{x})$是 Bent 函数,对任何向量 $\boldsymbol{b}\in F_2^n\setminus\{a\}$,$f(\boldsymbol{x})+f(\boldsymbol{x}+\boldsymbol{a}+\boldsymbol{b})$和 $g(\boldsymbol{x})+g(\boldsymbol{x}+\boldsymbol{a}+\boldsymbol{b})$都是平衡的,因此 $f(\boldsymbol{x})+f(\boldsymbol{x}+\boldsymbol{a}+\boldsymbol{b})\|g(\boldsymbol{x})+g(\boldsymbol{x}+\boldsymbol{a}+\boldsymbol{b})+1$ 是平衡的.当 $\boldsymbol{a}=\boldsymbol{b}$ 时$f(\boldsymbol{x})+f(\boldsymbol{x}+\boldsymbol{a}+\boldsymbol{b})\equiv 0$且 $g(\boldsymbol{x})+g(\boldsymbol{x}+\boldsymbol{a}+\boldsymbol{b})+1\equiv 1$,因此在这种情形下 $f(\boldsymbol{x})+f(\boldsymbol{x}+\boldsymbol{a}+\boldsymbol{b})\|g(\boldsymbol{x})+g(\boldsymbol{x}+\boldsymbol{a}+\boldsymbol{b})+1$ 也是平衡的.

设 $V=\{\boldsymbol{x}\in F_2^n \mid f(\boldsymbol{x})+g(\boldsymbol{x}+\boldsymbol{b})=1\}$,则 $\{\boldsymbol{x}\mid f(\boldsymbol{x}+\boldsymbol{a})+g(\boldsymbol{x}+\boldsymbol{a}+\boldsymbol{b})+1=0\}=\{\boldsymbol{a}+\boldsymbol{x}\mid \boldsymbol{x}\in V\}$. 这表明 $f(\boldsymbol{x})+g(\boldsymbol{x}+\boldsymbol{b})$和 $f(\boldsymbol{x}+\boldsymbol{a})+g(\boldsymbol{x}+\boldsymbol{a}+\boldsymbol{b})+1$ 的支集所含向量的数目之和为 2^n,也就是说$(n+1)$-元布尔函数$f(\boldsymbol{x})+g(\boldsymbol{x}+\boldsymbol{b})\,\|\, f(\boldsymbol{x}+\boldsymbol{a})+g(\boldsymbol{x}+\boldsymbol{a}+\boldsymbol{b})+1$ 是平衡的.

同理可证 $f(\boldsymbol{x})+g(\boldsymbol{x}+\boldsymbol{a}+\boldsymbol{b})+1\,\|\, f(\boldsymbol{x}+\boldsymbol{a})+g(\boldsymbol{x}+\boldsymbol{b})$也是平衡的. 证毕

在推论 1 中令 $\boldsymbol{a}=\boldsymbol{0}$,可得下面结论.这种构造方法曾被用来研究 Bent 函数的正规扩张.

推论 2[21]　设 $f(\boldsymbol{x})$和 $g(\boldsymbol{x})$是 n-元 Bent 函数.那么$(n+2)$-元布尔函数

$$f(\boldsymbol{x})\,\|\, f(\boldsymbol{x})\,\|\, g(\boldsymbol{x})\,\|\, g(\boldsymbol{x})+1$$

是 Bent 函数.

文献[22]也讨论了推论 2 中的构造,并且考虑了生成的 Bent 的计数问题.

在推论 1 中令 $g(\boldsymbol{x})=f(\boldsymbol{x}+\boldsymbol{b})$,$\boldsymbol{b}\in F_2^n$,得到下面函数的构造.

推论 3　设 $f(\boldsymbol{x})$是 n-元 Bent 函数,向量 $\boldsymbol{a},\boldsymbol{b}\in F_2^n$.那么$(n+2)$-元布尔函数

$$f(\boldsymbol{x})\,\|\, f(\boldsymbol{x}+\boldsymbol{a})\,\|\, f(\boldsymbol{x}+\boldsymbol{b})\,\|\, f(\boldsymbol{x}+\boldsymbol{a}+\boldsymbol{b})+1$$

是 Bent 函数.

文献[23]定理 3.6 在向量 $\boldsymbol{a},\boldsymbol{b}\in F_2^n$ 满足

$$f(\boldsymbol{x})+f(\boldsymbol{x}+\boldsymbol{a})+f(\boldsymbol{x}+\boldsymbol{b})+f(\boldsymbol{x}+\boldsymbol{a}+\boldsymbol{b})=1$$

时,即 $f(\boldsymbol{x})$的二阶导函数满足$(D_b(D_af))(\boldsymbol{x})=1$ 的条件下,证明了推论 3 中构造的$(n+2)$-元布尔函数是 Bent 的.这是一个较强的限制,有很多 n-元 Bent 函数并不满足这个性质,如文献[24]中引理 3 给出的变元数 $n\geqslant 8$ 的 Bent 函数类,这些函数的所有的二阶离散导函数都不是常数.因此文献[23]定理 3.6 不能用这些 n-元 Bent 函数构造$(n+2)$-元 Bent 函数,但是推论 3 却可以用它们来构造$(n+2)$-元 Bent 函数.这说明文献[23]中定理 3.6 只是推论 3 的一个特例.

我们在推论 1 中提出的 Bent 函数的迭代构造方法统一并推广了以前的两个迭代构造(即推论 2 和文献[23]定理 3.6).

下面我们将讨论推论 1 生成的 Bent 函数的代数次数.

命题 1　当 n-元 Bent 函数 $f(\boldsymbol{x})$和 $g(\boldsymbol{x})$中仅有一个函数的代数次数达到最优时,由推论 1 构造的$(n+2)$-元 Bent 函数也具有最优的代数次数.

证明　构造的$(n+2)$-元 Bent 函数可表示为

$$\begin{aligned}&(1+y)(1+z)f(\boldsymbol{x})+y(1+z)f(\boldsymbol{x}+\boldsymbol{a})+(1+y)zg(\boldsymbol{x})\\&+yz(g(\boldsymbol{x}+\boldsymbol{a})+1)=f(\boldsymbol{x})+z(f(\boldsymbol{x})+g(\boldsymbol{x}))+yD_af(\boldsymbol{x})\\&\qquad+yz(D_af(\boldsymbol{x})+D_ag(\boldsymbol{x})+1)\end{aligned}$$

其中 $\boldsymbol{x}\in F_2^n$,$y,z\in F_2$.不失一般性,我们假设 Bent 函数 $f(\boldsymbol{x})$和 $g(\boldsymbol{x})$满足 $\deg(f)=n/2$ 且 $\deg(g)<n/2$ 时,则

$$\begin{aligned}&\deg(f(\boldsymbol{x})+g(\boldsymbol{x}))=n/2,\\&\deg(D_af)(\boldsymbol{x})\leqslant n/2-1,\\&\deg(D_ag)(\boldsymbol{x})<n/2-1.\end{aligned}$$

从上面的表达式可以看出,所构造的$(n+2)$-元 Bent 函数的代数次数为 $n/2+1$. 证毕

一般地,我们并不一定要求 $f(\boldsymbol{x})$和 $g(\boldsymbol{x})$中仅有一个函数的代数次数达到最优,在 $f(\boldsymbol{x})+g(\boldsymbol{x})$的代数次数等于 $n/2$ 时同样能证明命题 1 中的结论成立.然而,由推论 3 生成的任何 Bent 函数的代数次数都不可能达到最优.这是因为

$$\begin{aligned}&(1+y)(1+z)f(\boldsymbol{x})+y(1+z)f(\boldsymbol{x}+\boldsymbol{a})+(1+y)zf(\boldsymbol{x}+\boldsymbol{b})\\&+yz(f(\boldsymbol{x}+\boldsymbol{a}+\boldsymbol{b})+1)=f(\boldsymbol{x})+z(D_bf)(\boldsymbol{x})+y(D_af)(\boldsymbol{x})\\&\qquad+yz(D_a(D_bf))(\boldsymbol{x})+yz\end{aligned}$$

其中 $\deg((D_bf)(\boldsymbol{x}))\leqslant n/2-1$,$\deg((D_af)(\boldsymbol{x}))\leqslant n/2-1$ 和 $\deg(D_a(D_bf))(\boldsymbol{x})\leqslant n/2-2$,因此推论 3 构造的$(n+2)$-元 Bent 函数代数次数不超过 $n/2$.

4　结束语

本文研究了级联 4 个 n-元 Bent 函数构造$(n+2)$-元 Bent 函数的相关问题,建立了由 4 个 n-元 Bent 函数构造$(n+2)$-元 Bent 函数的一个充要条件.提出了一种 Bent 函数的迭代构造方法,这种方法统一并推广了以前的两种 Bent 函数的构造.反复运用这种方法,可以由低变元的代数次数最优 Bent 函数构造高变元的代数次数最优 Bent 函数.本文所构造的 Bent 函数与其它方法构造的 Bent 函数的关系如不等价性是下一步的一个研究方向.

参考文献:

[1] 冯登国,裴定一.密码学导引[M].北京:科学出版社,1999.

[2] 温巧燕,钮心忻,杨义先.现代密码学中的布尔函数[M].北京:科学出版社,2000.

[3] 李世取,曾本胜,廉玉忠.密码学中的逻辑函数[M].北京:中软电子出版社,2003.

[4] Xiao G,Massey J.A spectral characterization of correlation immunity functions[J].IEEE Transactions on Information Theory,1988,34(3):569 – 571.

[5] 常祖领,柯品惠,张▮,温巧燕.高非线性度多输出布尔函数的构造[J].电子学报,2008,36 (1):141 – 145.
CHANG Zu-ling, KE Pin-hui, ZHANG Jie, WEN Qiao-yan. Constructions of multi-output Boolean functions with high nonlinearity[J]. Acta Electronica Sinica, 2008, 36 (1): 141 – 145. (in Chinese)

[6] 李超,屈龙江. Bent 函数和弹性函数的最小距离[J]. 电子学报,2008,36(1):136 – 140.
LI Chao, QU Long-jiang. Minimum distance between Bent and resilient Boolean functions[J]. Acta Electronica Sinica, 2008, 36(1):136 – 140. (in Chinese)

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

[8] Dillion J. Elementary Hadamard Difference Sets[D]. Baltimore: Univ Maryland, 1974.

[9] Weng G, Feng R, Qiu W, Zheng Z. The ranks of Maiorana-McFarland bent functions[J]. Science in China Series A, 2008, 51(9):1726 – 1731.

[10] Weng G, Feng R, Qiu W. On the ranks of Bent functions[J]. Finite Fields and Their Applications, 2007, 13(4): 1096 – 1116.

[11] McFarland R L. A family of difference sets in noncyclic groups[J]. Journal of Combinatorial Theory Series A, 1973, 15(1):1 – 10.

[12] 常祖领,陈鲁生,符方伟. PS 类 Bent 函数的一种构造方法[J]. 电子学报,2004,32(10):1649 – 1653.
CHANG Zu-ling, CHEN Lu-sheng, FU Fang-wei. One method for constructing Bent functions of class PS[J]. Acta Electronica Sinica, 2004, 32(10):1649 – 1653. (in Chinese)

[13] Carlet C. Generalized partial spreads[J]. IEEE Transactions on Information Theory, 1995, 41(5):1482 – 1487.

[14] Dobbertin H. Construction of Bent functions and highly nonlinear balanced Boolean functions[A]. Preneel B. Lecture Notes on Computer Science 1008[C]. Berlin: Springer-Verlag, 1995. 61 – 74.

[15] Leander G. Monomial Bent functions[J]. IEEE Transactions on Information Theory, 2006, 52(2):738 – 743.

[16] Canteaut A, Charpin P, Kyureghyan G. A new class of monomial Bent functions[J]. Finite Fields and Their Applications, 2008, 14(1):221 – 241.

[17] Dobbertin H, Leander G, Canteaut A, Carlet C, Felke P, Gaborit P. Construction of Bent functions via Niho power functions[J]. Journal of Combinatorial Theory Series A, 2006, 113(5):779 – 798.

[18] Hu H, Feng D. On quadratic Bent functions in polynomial forms[J]. IEEE Transactions on Information Theory, 2007, 53(7):2610 – 26.

[19] 张文英,李世取. 代数次数为 2 的 Bent 函数的性质及其应用[J]. 电子学报,2004,32(4):654 – 656.
ZHANG Wen-ying, LI Shi-qu. The characteristic of quadratic Bent functions and its applications[J]. Acta Electronica Sinica, 2004, 32(4):654 – 656. (in Chinese)

[20] Hou X, Langevin P. Results on Bent functions[J]. Journal of Combinatorial Theory Series A, 1997, 80(2):232 – 246.

[21] Carlet C, Dobbertin H, Leander G. Normal extensions of Bent functions[J]. IEEE Transactions on Information Theory, 2004, 50(11):2880 – 2885.

[22] Climent J, Garcia F, Requena V. On the construction of Bent functions of $n+2$ variables from Bent functions of n variables [J]. Advances in Mathematics of Communications, 2008, 2(4):421 – 431.

[23] Climent J, Garcia F, Requena V. Some constructions of Bent functions of $n+2$ variables from Bent functions of n variables [A]. Michon J F, Valacher P, Yunès J B. Proceedings of the 3rd International Conference on Boolean Functions: Cryptography and Applications[C]. Paris: Publication des Universtés de Rouen et du Havre, 2007. 57 – 72.

[24] Canteaut A, Charpin P. Decomposing Bent functions[J]. IEEE Transactions on Information Theory, 2003, 49(8): 2004 – 2019.

[25] 孟庆树,张焕国,王张宜,覃中平,彭文灵. Bent 函数的演化设计[J]. 电子学报,2004,32(11):1901 – 1903.
MENG Qing-shu, ZHANG Huang-guo, WANG Zhang-yi, QIN Zhong-ping, PENG Wen-ling. Designing Bent functions using evolving method[J]. Acta Electronica Sinica, 2004, 32(11):1901 – 1903. (in Chinese)

[26] 孙光洪,武传坤. 级联函数的密码学性质[J]. 电子学报,2009,37(4):884 – 888.
SUN Guang-hong, WU Chuan-kun. Some cryptographic properties of Boolean functions by concatenation[J]. Acta Electronica Sinica, 2009, 37(4):884 – 888. (in Chinese)

作者简介:

曾祥勇 男,1973 年 11 月出生于湖北省仙桃市. 现为湖北大学教授、硕士生导师. 主要研究方向为密码学和编码学.
E-mail: xiangyongzeng@yahoo.com.cn

胡 磊 男,1967 年 3 月出生于湖北省麻城市. 现为中国科学院研究生院教授、博士生导师. 主要研究方向为密码学、信息安全和编码理论.
E-mail: hu@is.ac.cn