密码学报 ISSN 2095-7025 CN 10-1195/TN
Journal of Cryptologic Research,2015,2(5):404–438

E-mail: jcr@cacrnet.org.cn
http://www.jcr.cacrnet.org.cn
Tel/Fax: +86-10-81033101

Bent 函数构造方法研究*

杨小龙[1,2], 胡红钢[1,2]

1. 中国科学技术大学 电子工程与信息科学系, 合肥 230027
2. 中国科学院 电磁空间信息重点实验室, 合肥 230027
通讯作者: 胡红钢, E-mail: hghu2005@ustc.edu.cn

摘 要: Bent 函数的概念由 Rothaus 在 1976 年提出. 因为 Bent 函数既是非线性度最优的布尔函数, 又达到了一阶 Reed-Muller 码的覆盖半径, 并且与 Hadamard 矩阵、差集等组合对象有紧密联系, 所以其应用涉及密码、编码、组合数学等多个领域. 对 Bent 函数的研究一直是热门方向, 其中包含了大量的关于 Bent 函数构造的结果. 除了布尔 Bent 函数, 在不同的应用背景下还定义了 Bent 函数的各类推广形式, 比如: 广义 Bent 函数、*p* 值 Bent 函数、向量 Bent 函数、超 Bent 函数等. 本文对 Bent 函数的构造方法做一个系统的综述, 介绍 Bent 函数及其各类推广形式的构造, 包括广义 Bent 函数、*p* 值 Bent 函数、向量 Bent 函数和超 Bent 函数. 在每一部分的介绍中, 着重介绍最具有代表形式的 Bent 函数, 如 Maiorana-McFarland 类、PS (Partial Spread)类、二次型以及一些特殊的指数形式.

关键词: 布尔 Bent 函数; 广义 Bent 函数; *p* 值 Bent 函数; 向量 Bent 函数; 超 Bent 函数
中图法分类号: TP309.7 **文献标识码**: A DOI: 10.13868/j.cnki.jcr.000089

中文引用格式: 杨小龙, 胡红钢. Bent 函数构造方法研究[J]. 密码学报, 2015, 2(5): 404–438.
英文引用格式: Yang X L, Hu H G. A survey of constructions on Bent functions[J]. Journal of Cryptologic Research, 2015, 2(5): 404–438.

A Survey of Constructions on Bent Functions

YANG Xiao-Long[1,2], HU Hong-Gang[1,2]

1. Department of Electronic Engineering and Information Science, University of Science and Technology of China, Hefei 230027, China
2. Key Laboratory of Electromagnetic Space Information, Chinese Academy of Science, Hefei 230027, China
Corresponding author: HU Hong-Gang, E-mail: hghu2005@ustc.edu.cn

Abstract: The concept of Bent functions was proposed by Rothaus in 1976. Bent functions are Boolean functions with best nonlinearity, and also achieve the coverage radius of the first-order Reed-Muller codes. Furthermore, they are closely related to several combinatorial objects, such as Hadamard matrices, difference sets. Thus, Bent functions can be applied to the fields of cryptography, coding theory, combinatorics etc. The construction of Bent functions is an attractive research topic. There are many approaches to construct Bent functions. In addition to Boolean Bent functions, some generalizations of this concept have also been defined in different cases, such as generalized Bent functions, *p*-ary Bent functions, vectorial Bent functions, and hyper-Bent functions. In this paper, we provide a compresensive survey of construction methods of Bent functions and their generalized forms, including generalized Bent functions, *p*-ary Bent functions, vectorial Bent functions, and

* 基金项目: 国家自然科学基金项目(61271271, 61522210); 中国科学院百人计划经费; 中央高校基本科研业务费专项资金(WK2101020005)
收稿日期: 2015-06-30 定稿日期: 2015-09-11

hyper-Bent functions. In each part of description, we highlight Bent functions with the most representative forms, such as the Maiorana-McFarland class, the PS (Partial Spread) class, quadratic forms, and some special exponential forms.

Key words: Boolean Bent functions; generalized Bent functions; *p*-ary Bent functions; vectorial Bent function; hyper-Bent function

1 引言

随着信息化时代的来临, 信息安全的重要性越来越突出, 而密码学作为实现信息安全的重要手段一直发挥着重要作用. 对一个密码系统而言, 密码函数是其重要的组要部分. 密码系统的安全性, 即密码系统抵抗各种攻击的能力, 是与系统所用密码函数的各类密码学指标密切相关的. 密码函数可以分为布尔函数和向量值函数两大类, 布尔函数和向量值函数广泛用于序列密码和分组密码的设计, 比如: 滤波序列和非线性组合序列所用的滤波函数和组合函数, 分组密码所用的 S 盒.

序列密码和分组密码都面临着各种各样的攻击, 其中主要的攻击方法有 Berlekamp-Massey 攻击[1]、相关攻击[2,3]、代数攻击[4,5]、差分攻击[6]和线性攻击[7]. 密码算法抵抗上述攻击的能力与其所用密码函数相应的密码学指标有关, 包括非线性度、相关免疫阶、代数免疫阶和差分均匀度等. 在这些指标中, Bent 函数是非线性度最优的布尔函数, 完全非线性函数是差分均匀度最优的函数.

对单项密码学性质最优的密码函数的研究, 如Bent函数、完全非线性函数、代数免疫阶最优函数, 或者对同时具有多个良好密码学性质的密码函数的研究一直是近年来本领域的热点问题, 取得了丰富的成果. Rothaus 于 1976 年提出 Bent 函数概念[8], 此后 Bent 函数在密码、编码以及组合数学领域受到了广泛的关注. 在密码学方面, 它是非线性度最优的布尔函数, 在序列密码的设计中有重要作用; 在编码学方面, 它达到了一阶 Reed-Muller 码的覆盖半径[8]; 在组合数学方面, 它与 Hadamard 矩阵、差集等有着密切的联系[9]. 不仅如此, 它的一类推广形式—广义 Bent 函数在 CDMA(Code-Division Multiple Access)通信系统中也具有重要应用[10]. 故本文着眼于 Bent 函数, 对 Bent 函数的构造方法做一个系统的综述: 首先介绍 Bent 函数的概念及相关的密码学性质, 然后着重介绍 Bent 函数的各类构造, 包括布尔 Bent 函数, 广义 Bent 函数和 p 值 Bent 函数三种不同形式下的构造, 随后介绍向量值 Bent 函数, 最后介绍 Bent 函数的一个特殊子类—超 Bent 函数.

2 Bent 函数及其密码学性质

2.1 Bent函数

一个 n 元布尔函数 $f(x)$ 是从 F_2^n 到 F_2 的一个映射, 记为 $f(x): F_2^n \to F_2$. 布尔函数有多种表示方式, 最常用的是代数正规型表示:

$$f(x_1, x_2, \cdots, x_n) = \sum_{I \subseteq \{1,\cdots,n\}} a_I \left(\prod_{i \in I} x_i \right)$$

其中 $a_I \in F_2$. 每一个 $\prod_{i \in I} x_i$ 被称为一个单项式, 布尔函数 $f(x)$ 的代数次数定义为所有具有非零系数的单项式的次数的最大值, 记为 $\deg(f)$. 记 B_n 为所有 n 元布尔函数构成的集合. 代数次数不超过 1 的布尔函数称为仿射函数, 全体 n 元仿射函数构成的集合记为 A_n, 即

$$A_n = \left\{ f \in B_n \mid f(x_1, x_2, \cdots x_n) = \sum_{i=1}^{n} a_i x_i + a_0, a_0, \cdots, a_n \in F_2 \right\}$$

常数项为 0 的仿射函数称为线性函数, 全体 n 元线性函数的集合记为 L_n, 即

$$L_n=\left\{f\in B_n \mid f\left(x_1,x_2,\cdots x_n\right)=\sum_{i=1}^{n}a_ix_i,a_1,\cdots,a_n\in F_2\right\}$$

布尔函数的 Walsh 变换是研究布尔函数密码学性质的重要数学工具. 布尔函数 f 的循环 Walsh 变换定义如下

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

其中 $\boldsymbol{\omega}\in F_2^n$, "·"表示两个向量的内积, 为 $\boldsymbol{\omega}\cdot\boldsymbol{x}=\sum_{1\leqslant i\leqslant n}\omega_ix_i$. 同时还可以定义布尔函数的线性 Walsh 谱, 但是两种 Walsh 谱之间可以相互唯一确定, 故后文一直使用循环 Walsh 谱.

两个布尔函数 $f\left(\boldsymbol{x}\right),l\left(\boldsymbol{x}\right)$ 的距离定义为

$$d_H\left(f\left(\boldsymbol{x}\right),l\left(\boldsymbol{x}\right)\right)=\left|\left\{\boldsymbol{x}\in F_2^n\,\middle|\,f\left(\boldsymbol{x}\right)\neq l(\boldsymbol{x})\right\}\right|$$

函数 f 的非线性度定义为 f 与所有仿射函数距离的最小值, 为

$$\mathrm{NL}\left(f\right)=\min_{l(\boldsymbol{x})\in A_n}d_H\left(f\left(\boldsymbol{x}\right),l\left(\boldsymbol{x}\right)\right)$$

根据布尔函数的非线性度和 Walsh 谱的定义, 可以得到两者具有如下关系:

$$\mathrm{NL}\left(f\right)=2^{n-1}-\frac{1}{2}\max_{\boldsymbol{a}\in F_2^n}\left|W_f\left(\boldsymbol{a}\right)\right|$$

从上式中可以看到, f 要具有高的非线性度, 就需要 f 的 Walsh 谱绝对值的最大值要尽量小. 根据 Parseval 等式

$$\sum_{\boldsymbol{a}\in F_2^n}W_f^2\left(\boldsymbol{a}\right)=2^{2n}$$

得到 $\max_{\boldsymbol{a}\in F_2^n}\left|W_f\left(\boldsymbol{a}\right)\right|\geqslant 2^{n/2}$, 进而可以得到布尔函数 f 的非线性度的一个上界 $\mathrm{NL}\left(f\right)\leqslant 2^{n-1}-2^{n/2-1}$.

定义 1 如果 n 元布尔函数 f 的非线性度为 $\mathrm{NL}\left(f\right)=2^{n-1}-2^{n/2-1}$, 则 f 称为 Bent 函数.

因为布尔函数的非线性度肯定是一个正整数, 所以 Bent 函数只有在 n 为正偶数的情况下才存在. 在 n 为正偶数的情况下, 根据非线性度与 Walsh 谱谱值的关系, 可得到 $f\left(\boldsymbol{x}\right)$ 为 Bent 函数的一个充要条件.

定理 1 n 元布尔函数 f 为 Bent 函数当且仅当对于任意的 $\boldsymbol{a}\in F_2^n$, $W_f\left(\boldsymbol{a}\right)=\pm 2^{n/2}$.

当 n 元布尔函数 $f\left(\boldsymbol{x}\right)$ 为 Bent 函数时, 可知 $W_f\left(\boldsymbol{a}\right)=\pm 2^{n/2}=2^{n/2}\left(-1\right)^{\tilde{f}(\boldsymbol{x})}$, 则 $\tilde{f}\left(\boldsymbol{x}\right)$ 称为 $f\left(\boldsymbol{x}\right)$ 的对偶函数, 且满足 $\tilde{\tilde{f}}=f$.

2.2 Bent函数的密码学性质

由定义可知, Bent 函数具有最优的非线性度. 下面考察 Bent 函数在平衡性、相关免疫、代数次数、自相关和扩散性等方面的密码学性质.

布尔函数 f 为平衡函数的充要条件为 f 的 Walsh 谱谱值在 $\boldsymbol{x}=0$ 处等于 0, 即 $W_f\left(\boldsymbol{0}\right)=0$, 而 Bent 函数的 Walsh 谱谱值在 $\boldsymbol{x}=0$ 处取值不为 0, 故 Bent 函数不是平衡函数.

对于布尔函数相关免疫方面的研究, 有如下著名的 Xiao-Massey 定理[11].

定理 2 布尔函数 f 是 m 阶相关免疫的当且仅当对于任意的 $\boldsymbol{a}\in F_2^n$, $1\leqslant \mathrm{wt}\left(\boldsymbol{a}\right)\leqslant m$, 都有 $W_f\left(\boldsymbol{a}\right)=0$.

根据 Bent 函数的 Walsh 谱谱值特点与 Xiao-Massey 定理可知 Bent 函数不具有任何阶的相关免疫性质. 此外, Bent 函数并不具有特别高的代数次数, 其代数次数上界由如下定理给出.

定理 3[8] f 是 n 元布尔函数, $n\geqslant 4$. 如果 f 为 Bent 函数, 则 f 的代数次数至多为 $n/2$.

下面考虑 Bent 函数的自相关性质, 首先给出自相关函数的定义:

定义 2 n 元布尔函数 f 的自相关函数定义为

$$A_f(\boldsymbol{a})=\sum_{\boldsymbol{x}\in F_2^n}(-1)^{f(\boldsymbol{x}+\boldsymbol{a})+f(\boldsymbol{x})}$$

定理 4 n 元布尔函数 f 是 Bent 函数当且仅当

$$A_f(\boldsymbol{a})=\begin{cases}2^n, & \boldsymbol{a}=0\\ 0, & \boldsymbol{a}\neq 0\end{cases}$$

根据定理 4 可知 Bent 函数具有最优的自相关性质.

定义 3 n 元布尔函数 f, 如果对于任意的 $\boldsymbol{a}\in F_2^n$, $1\leqslant \mathrm{wt}(\boldsymbol{a})\leqslant k$, 函数 $f(\boldsymbol{x}+\boldsymbol{a})+f(\boldsymbol{x})$ 都是平衡函数, 则称 f 满足 k 阶扩散准则.

定理 5 n 元布尔函数 f 是 Bent 函数当且仅当 f 满足 n 阶扩散准则.

根据上文对 Bent 函数各项密码学性质的研究可以知道, Bent 函数具有一些明显的优点[12]: 一是具有最优的非线性度, 使得它是抵抗最佳仿射逼近攻击最优的函数; 二是 Bent 函数的 Walsh 谱取值非常特殊, 在每一点的取值均为 $\pm 2^{n/2}$, 根据流密码的稳定性理论, 如果用 Bent 函数作为流密码系统的非线性组合函数或者滤波函数, 则所得到的密钥流序列具有稳定的线性复杂度[13]. 但 Bent 函数也具有一些明显的缺点[12]: 一是 Bent 函数不是平衡的; 二是 Bent 函数不具有任何阶的相关免疫性; 三是 Bent 函数的代数次数不高.

3 布尔 Bent 函数

Bent 函数的构造一直是 Bent 函数研究中的热点问题. 自从 1976 年 Bent 函数概念提出以来, 已有大量的 Bent 函数构造方法. 这些方法可以分为两类: 直接构造法和间接构造法. 直接构造法就是在不依赖已有 Bent 函数的情况下, 按照某些特定的方式得到 Bent 函数. 间接构造法是利用已有的 Bent 函数来得到新的 Bent 函数. 下面主要介绍布尔 Bent 函数的各类直接或间接构造方法, 此部分结果读者也可参见文献[14,15]等相关章节.

3.1 直接构造法

直接构造法的代表性方法有 Maiorana-McFarland 构造法、Dillon 构造法和迹函数复合构造法(此类方法在 3.3 节专门介绍)等.

首先介绍 Bent 函数的第一种直接构造方法——Maiorana-McFarland 构造法[9,16].

定义 4 n 为偶数, $F_2^n=\left\{(\boldsymbol{x},\boldsymbol{y})\middle|\boldsymbol{x},\boldsymbol{y}\in F_2^{n/2}\right\}$, n 元布尔函数如果具有如下形式

$$f(\boldsymbol{x},\boldsymbol{y})=\boldsymbol{x}\cdot\pi(\boldsymbol{y})+g(\boldsymbol{y})$$

其中 π 为定义在 $F_2^{n/2}$ 上的任意置换, g 为 $F_2^{n/2}$ 上的任意布尔函数. 则称函数 f 是 Maiorana-McFarland 型函数, 简称为 M-M 型函数.

定理 6 如果 f 为 F_2^n 上的 M-M 型函数, 则 f 为 Bent 函数. 此外, f 的对偶函数为

$$\tilde{f}(\boldsymbol{x},\boldsymbol{y})=\boldsymbol{y}\cdot\pi^{-1}(\boldsymbol{x})+g\left(\pi^{-1}(\boldsymbol{x})\right)$$

也是 M-M 型 Bent 函数.

下面介绍 Bent 函数的另一种重要的直接构造方法——Dillon 构造, 该方法是 Dillon 在他的博士论文[9]中提出的.

设 E 为 F_2^n 上的一个线性子空间, 定义 E 的指标函数为

$$1_E(\boldsymbol{x})=\begin{cases}1, & \boldsymbol{x}\in E\\ 0, & \boldsymbol{x}\notin E\end{cases}$$

定义 $E^{\perp}=\left\{\boldsymbol{x}\in F_2^n \middle| \text{对任意}\boldsymbol{y}\in E,\text{都有}\boldsymbol{x}\cdot\boldsymbol{y}=0\right\}$. 给定 F_2^n 的两个线性子空间 E_1 和 E_2, 如果 $E_1\cap E_2=\{\boldsymbol{0}\}$, 则称 E_1 与 E_2 是“不相交”的. 当 n 为偶数时, 向量空间 F_2^n 中所包含的两两不相交的 $n/2$ 维子空间恰有 $2^{n/2}+1$ 个[15].

Dillon 在博士论文中构造的 Bent 函数被称为 PS (Partial Spread)函数, 包括 PS⁻ 和 PS⁺. PS⁻ 函数和 PS⁺ 函数分别是由 F_2^n 中任意 $2^{n/2-1}$ 或 $2^{n/2-1}+1$ 个不相交的 $n/2$ 维子空间的指标函数模 2 和所组成的函数集合.

定理 7 PS 类函数是 Bent 函数[9].

PS 类所包含的两类函数 PS⁻ 和 PS⁺ 各自具有特别的性质: PS⁻ 函数的代数次数一定为 $n/2$, 而 PS⁺ 类函数都是正规的, 即存在一个 $n/2$ 维子空间, 使得函数限制在这个子空间上为一个常数.

在 PS⁻ 类函数中, 有一类更为特殊的函数, 称为 $\mathrm{PS}_{\mathrm{ap}}$ 函数. 考虑向量空间 $F_2^n\approx F_{2^{n/2}}\times F_{2^{n/2}}$, 可以看作是 2 维的 $F_{2^{n/2}}$ 向量空间, 由通过原点的不相交的 $2^{n/2}+1$ 条线的并构成, 其中每一条线都对应 F_2^n 的一个 $n/2$ 维子空间. 从这 $2^{n/2}+1$ 条线中选择 $2^{n/2-1}$ 条线(不包括 $x=0$ 和 $y=0$), 所得到的函数就是 $\mathrm{PS}_{\mathrm{ap}}$ 函数. 对于一般的 PS 类函数, 要想写出它的精确表达式比较困难, 但对于 $\mathrm{PS}_{\mathrm{ap}}$ 函数, 它具有明确的表达式

$$f(x,y)=\begin{cases}0, & y=0\\ g\left(\dfrac{x}{y}\right), & y\neq 0\end{cases}$$

其中 $x,y\in F_{2^{n/2}}$, g 是定义在 $F_{2^{n/2}}$ 上的平衡布尔函数且满足 $g(0)=0$. $\mathrm{PS}_{\mathrm{ap}}$ 函数 $f(x,y)$ 的对偶函数为 $f(y,x)$, $f(x,y)$ 的补函数 $f(x,y)+1$ 属于 PS⁺.

Carlet 在文献[17]中提出了广义局部扩散类, 简记为 GPS 类, 并证明了所有的 Bent 函数都属于 GPS 类.

定理 8[17] n 为偶数, f 为 n 元布尔函数, f 是 Bent 函数当且仅当存在 k 个 F_2^n 的 $n/2$ 维子空间 $E_1,E_2,\cdots,E_k$ 和整数 $m_1,m_2,\cdots,m_k$ 使得对于任意的 $\boldsymbol{x}\in F_2^n$,

$$f(\boldsymbol{x})\equiv\sum_{i=1}^{k}m_i 1_{E_i}(\boldsymbol{x})-2^{\frac{n}{2}-1}\delta_0(\boldsymbol{x})\bmod 2^{n/2}$$

如果

$$f(\boldsymbol{x})=\sum_{i=1}^{k}m_i 1_{E_i}(\boldsymbol{x})-2^{\frac{n}{2}-1}\delta_0(\boldsymbol{x})$$

是 Bent 函数, 则 f 的对偶函数为

$$\tilde{f}(\boldsymbol{x})=\sum_{i=1}^{k}m_i 1_{E_i^{\perp}}(\boldsymbol{x})-2^{\frac{n}{2}-1}\delta_0(\boldsymbol{x})$$

除了 M-M 类和 PS 类这两类基本构造, 还有一些其它的构造方法, 列举其中部分结果如下.

Dobbertin 在文献[18]中构造出了一类 Bent 函数, 此类函数包含了已知的 $\mathrm{PS}_{\mathrm{ap}}$ 类和 M-M 类函数.

定理 9[18] 具有如下形式的布尔函数

$$f(x,\phi(y))=g\left(\frac{x+\psi(y)}{y}\right)$$

是 Bent 函数. 其中 g 是 $F_{2^{n/2}}$ 上的平衡布尔函数, ϕ,ψ 是 $F_{2^{n/2}}$ 到 $F_{2^{n/2}}$ 的映射, ϕ 必须是一一映射, T 是由 g 的 Walsh 谱的支集 $\left\{x\in F_{2^{n/2}}\middle| W_g(x)\neq 0\right\}$ 支撑扩张成的 $F_{2^{n/2}}$ 的仿射子空间, 对任意的 $a\in F_{2^{n/2}}$, ϕ,ψ 都是

$aT=\{ax|x\in T\}$ 上的仿射函数.

Dillon 和 McGuire 在文献[19]中指出, 可以通过将 F_{2^n} 上的函数限制在其上的超平面来得到 Bent 函数. 文中给出了通过此方法得到的两类构造.

定理 10[19] 奇数 $n=3k\pm1$, 考虑 Kasami 函数 $f(x)=\mathrm{Tr}\left(x^{2^{2k}-2^k+1}\right)$, 超平面为 $H=\{x\in F_{2^n}|\mathrm{Tr}(x)=0\}$, 则 $f(x)$ 限制在超平面 H 上为 Bent 函数, 并且限制在其它超平面上都不为 Bent 函数.

定理 11[19] n 为奇数, $\gcd(n,k)=1$, 考虑 Gold 函数 $f(x)=\mathrm{Tr}\left(x^{2^k+1}\right)$, 超平面为 $H_\alpha=\{x\in F_{2^n}|\mathrm{Tr}(\alpha x)=0\}$. 则 $f(x)$ 限制在超平面 H_α 上为 Bent 函数当且仅当 $\mathrm{Tr}(\alpha)=1$.

Carlet 在文献[20]中提出了利用几乎 Bent 函数构造 Bent 函数的方法. 当 $n/2$ 为奇数时, 能够通过 $F_{2^{n/2}}\to F_{2^{n/2}}$ 的几乎 Bent 函数得到 $F_{2^n}\to F_2$ 的 Bent 函数.

Leander 和 McGuire 在文献[21]提出了用 Semi-Bent 函数构造 Bent 函数的方法, 利用 $2m-1$ 元的 Semi-Bent 函数得到 $2m$ 元的 Bent 函数.

3.2 间接构造法

本节主要介绍 Bent 函数的间接构造方法, 即通过已有 Bent 函数来构造新 Bent 函数的方法. 根据是否改变函数变量个数可以将该方法分为两类. 首先介绍改变变量个数的间接构造方法, 其中最简单的一种方法就是直和构造法[8,9].

定理 12 f 是 n 元 Bent 函数(n 为偶数), g 是 m 元 Bent 函数(m 为偶数), 则 $n+m$ 元布尔函数 $h(\boldsymbol{x},\boldsymbol{y})=f(\boldsymbol{x})+g(\boldsymbol{y})$ 也是 Bent 函数.

注 1 此类间接构造得到的 Bent 函数从密码学的观点来看具有明显的缺点, 因为 $h(\boldsymbol{x},\boldsymbol{y})$ 可以分解为变量间没有关系的两个函数之和, 这样的性质会导致此类函数容易遭受分别征服攻击.

除了最简单的直和构造法以外, Rothaus 在文献[8]中给出了一类 Bent 函数的间接构造, 在文中用来证明对于所有的正偶数 n, 都存在 n 元 Bent 函数.

定理 13 n 为偶数, $g,h,k,g+h+k$ 均为 n 元 Bent 函数, 那么 $n+2$ 元布尔函数

$$f(x_1,x_2,\boldsymbol{y})=g(\boldsymbol{y})h(\boldsymbol{y})+g(\boldsymbol{y})k(\boldsymbol{y})+h(\boldsymbol{y})k(\boldsymbol{y})+\big(g(\boldsymbol{y})+h(\boldsymbol{y})\big)x_1+\big(g(\boldsymbol{y})+k(\boldsymbol{y})\big)x_2+x_1x_2$$

也是 Bent 函数, 其中 $x_1, x_2\in F_2, \boldsymbol{y}\in F_2^n$.

Carlet 在文献[22]中给出了一类一般性构造, 包含定理 13 中的构造.

定理 14 n 和 m 是两个正偶数. f 是定义在 $F_2^{n+m}=F_2^n\times F_2^m$ 上的布尔函数, 并满足对于任意的 $\boldsymbol{y}\in F_2^m$, 定义在 F_2^n 上的函数 $f_y:\boldsymbol{x}\to f(\boldsymbol{x},\boldsymbol{y})$ 是 Bent 的. 那么 f 是 Bent 函数当且仅当对于任意的 $\boldsymbol{s}\in F_2^n$, 函数 $\varphi_s:\boldsymbol{y}\to\tilde{f}_y(\boldsymbol{s})$ 是 F_2^m 上的 Bent 函数. 如果这个条件满足, 那么 f 的对偶为 $\tilde{f}(\boldsymbol{s},\boldsymbol{t})=\tilde{\varphi}_s(\boldsymbol{t})$.

随后 Carlet 在文献[23]和[24]中各给出一类间接构造, 都属于定理 14 中构造的特例.

推论 1[23] n 和 m 为偶数, f_1,f_2 为 n 元 Bent 函数, g_1,g_2 为 m 元 Bent 函数, 那么 $n+m$ 元函数

$$h(\boldsymbol{x},\boldsymbol{y})=f_1(\boldsymbol{x})+g_1(\boldsymbol{y})+(f_1+f_2)(\boldsymbol{x})\cdot(g_1+g_2)(\boldsymbol{y})$$

为 Bent 函数.

推论 2[24] 设 π 是 $F_2^{n/2}$ 上的置换, $f_{\pi,g}(\boldsymbol{x},\boldsymbol{y})=\boldsymbol{x}\cdot\pi(\boldsymbol{y})+g(\boldsymbol{y})$ 是一个 M-M 型 Bent 函数. 如果对于任意正偶数 m 和任意 $\boldsymbol{y}\in F_2^{n/2}$, h_y 都是 m 元 Bent 函数, 那么 $k(\boldsymbol{x},\boldsymbol{y},\boldsymbol{z})=h_y(\boldsymbol{z})+f_{\pi,g}(\boldsymbol{x},\boldsymbol{y})$ 为 Bent 函数.

除此之外, 在直接构造部分已经提到 Bent 函数可以通过 Semi-Bent 函数来构造, Charpin 等在文献[25]

中以 Semi-Bent 函数为桥梁, 给出了一个使用低次 Bent 函数迭代构造高次 Bent 函数的方法.

定理 15 n 为偶数, $\boldsymbol{x}=(x_0,x_1,\cdots,x_{n-1})\in F_2^n$, $f_1(\boldsymbol{x})$ 和 $f_2(\boldsymbol{x})$ 都是 $F_2^n\to F_2$ 的 Bent 函数. 则

$$s_1(\boldsymbol{x},x_n)=s_1(x_0,\cdots,x_n)=f_1\,\|\,f_2=x_nf_1(\boldsymbol{x})+(1+x_n)f_2(\boldsymbol{x})$$

$$s_2(\boldsymbol{x},x_n)=s_2(x_0,\cdots,x_n)=(1+f_1)\,\|\,f_2=x_n(1+f_1(\boldsymbol{x}))+(1+x_n)f_2(\boldsymbol{x})$$

是 $F_2^{n+1}\to F_2$ 的 Semi-Bent 函数.

$$b(\boldsymbol{x},x_n,x_{n+1})=b(x_0,\cdots,x_n,x_{n+1})=s_1\,\|\,s_2=x_{n+1}s_1(\boldsymbol{x},x_n)+(1+x_{n+1})s_2(\boldsymbol{x},x_n)$$

是 $F_2^{n+2}\to F_2$ 的 Bent 函数, 并且 $s_1(\boldsymbol{x},x_n)$, $s_2(\boldsymbol{x},x_n)$, $b(\boldsymbol{x},x_n,x_{n+1})$ 代数次数的关系为

$$\deg(s_1(\boldsymbol{x},x_n))=\deg(s_2(\boldsymbol{x},x_n))=\deg(b(\boldsymbol{x},x_n,x_{n+1}))=\max(\deg(f_1),\deg(f_2))+1$$

上面介绍的几种 Bent 的间接构造方法都改变了函数变量的个数, 下面给出的三种构造方法都能保持函数变量个数不变.

Carlet 在文献[26]中给出如下的一般性 Bent 函数的间接构造方法以及相应的特例.

定理 16 E 是 F_2^n 的线性子空间, $\boldsymbol{b}+E$ 是 F_2^n 上的任一仿射平面. f 是 n 元 Bent 函数. 函数 $f^*=f+1_{\boldsymbol{b}+E}$ 是 Bent 函数当且仅当下面任一条件成立

(1) 对于任意的 $\boldsymbol{a}\in F_2^n\setminus E$, 函数 $D_a(f)$ 在仿射平面 $\boldsymbol{b}+E$ 上是平衡的;

(2) 函数 $\tilde{f}(\boldsymbol{x})+\boldsymbol{b}\cdot\boldsymbol{x}$ 限制在 $E^\perp$ 的任意陪集上要么是常数, 要么是平衡的.

如果 f 和 f^* 都是Bent函数, 那么E的维度一定大于等于 $n/2$, 同时 f 在 $\boldsymbol{b}+E$ 上限制所得函数的代数次数至多为 $\dim(E)-n/2+1$. 如果 f 是Bent函数, E的维度为 $n/2$, 并且 f 在 $\boldsymbol{b}+E$ 上限制所得函数的代数次数至多为 $\dim(E)-n/2+1=1$, 即为仿射函数, 则 f^* 也为 Bent 函数.

推论 3 n 为偶数, n 元布尔函数 f 定义为

$$f(\boldsymbol{x},\boldsymbol{y})=\boldsymbol{x}\cdot\pi(\boldsymbol{y})+1_{E_1}(\boldsymbol{x})1_{E_2}(\boldsymbol{x})$$

其中 $\boldsymbol{x},\boldsymbol{y}\in F_2^{n/2}$, π 是 $F_2^{n/2}$ 上的置换, E_1 和 E_2 为 $F_2^{n/2}$ 的两个线性子空间, 且满足 $\pi(E_2)=E_1^\perp$, 那么 f 为 Bent 函数.

随后, Canteaut 等在文献[27]中给出了如下构造, 也属于定理 16 的特殊形式.

推论 4 n 为偶数, n 元布尔函数 f 定义为

$$f(\boldsymbol{x},\boldsymbol{y})=\boldsymbol{x}\cdot\pi(\boldsymbol{y})+1_L(\boldsymbol{x})$$

其中 $\boldsymbol{x},\boldsymbol{y}\in F_2^{n/2}$, L 是 $F_2^{n/2}$ 的一个线性子空间, π 是 $F_2^{n/2}$ 上的置换, 并且满足对任意 $\boldsymbol{a}\in F_2^{n/2}$, $\pi^{-1}(\boldsymbol{a}+L^\perp)$ 是一个平面, 那么 f 为 Bent 函数.

下面介绍Hou和Langevin在文献[28]中提出的不改变变量个数的一般性构造方法及满足此方法条件的特例.

定理 17 n 为偶数, f 是 n 元布尔函数. σ 是 F_2^n 上的置换, 记它的分支函数为 $\sigma_1,\sigma_2,\cdots,\sigma_n$. 如果对任意的 $\boldsymbol{a}\in F_2^n$ 有

$$d_H(f,\oplus_{i=1}^n a_i\sigma_i)=2^{n-1}\pm 2^{\frac{n}{2}-1}$$

那么 $f\circ\sigma^{-1}$ 是 Bent 函数.

推论 5 n 为偶数, 取 f_1, f_2 和 g 为 n 元布尔函数, h 为 n 元仿射函数. 构造 $n+2$ 元布尔函数

$$f(x_1,x_2,\boldsymbol{x})=x_1x_2h(\boldsymbol{x})+x_1f_1(\boldsymbol{x})+x_2f_2(\boldsymbol{x})+g(\boldsymbol{x})$$

其中 $x_1,x_2\in F_2$, $\boldsymbol{x}\in F_2^n$. 如果具有上述表述形式的函数 f 是 Bent 函数, 那么函数

$$f(x_1,x_2,\boldsymbol{x})+(h(\boldsymbol{x})+1)f_1(\boldsymbol{x})f_2(\boldsymbol{x})+f_1(\boldsymbol{x})+(x_1+h(\boldsymbol{x})+1)f_2(\boldsymbol{x})+x_2h(\boldsymbol{x})$$

也是 Bent 函数.

推论 6 如果 n 元Bent函数 f 的代数次数至多为3, σ 是 F_2^n 上的置换, 并且满足对任意 $i\in\{1,2,\cdots,n\}$, 都存在 F_2^n 的子集 U_i 以及仿射函数 h_i, 使得

$$\sigma_i(\boldsymbol{x})=\sum_{\boldsymbol{u}\in U_i}(f(\boldsymbol{x})+f(\boldsymbol{x}+\boldsymbol{u}))+h_i(\boldsymbol{x})$$

那么 $f\circ\sigma^{-1}$ 是 Bent 函数.

随后 Hou 在文献[29]中给出了一类构造, 也为定理 17 的特殊形式.

推论 7 $f(\boldsymbol{x},\boldsymbol{y})=\boldsymbol{x}\cdot\boldsymbol{y}+g(\boldsymbol{y})$ 是一个 M-M 型的 Bent 函数, 如果 $\sigma_1,\sigma_2,\cdots,\sigma_n$ 都是形如

$$\sum_{1\leqslant i<j\leqslant n/2}a_{i,j}x_iy_j+\boldsymbol{b}\cdot\boldsymbol{x}+\boldsymbol{c}\cdot\boldsymbol{y}+h(\boldsymbol{y})$$

的布尔函数, 那么 $f\circ\sigma^{-1}$ 是 Bent 函数.

Carlet 在文献[30]中也给出了一个不改变变量个数的间接构造.

定理 18 f_1,f_2 和 f_3 是三个 n 元 Bent 函数, n 为偶数. 定义 $s_1=f_1+f_2+f_3$, $s_2=f_1f_2+f_2f_3+f_3f_1$, 那么:

(1) 如果 s_1 是 Bent 函数, 并且 $\tilde{s}_1=\tilde{f}_1+\tilde{f}_2+\tilde{f}_3$, 那么 s_2 是 Bent 函数, 且 $\tilde{s}_2=\tilde{f}_1\tilde{f}_2+\tilde{f}_2\tilde{f}_3+\tilde{f}_3\tilde{f}_1$;

(2) 如果对任意的 $\boldsymbol{a}\in F_2^n$, $W_{s_2}(\boldsymbol{a})$ 可以被 $2^{n/2}$ 整除, 那么 s_1 是 Bent 函数.

后来 Mesnager 在文献[31]中, 对上述定理的反向情况作了进一步研究, 得到如下定理.

定理 19 n 为偶数, f_1,f_2 和 f_3 是三个两两不同的 n 元 Bent 函数. 定义 $s_1=f_1+f_2+f_3$ 为 Bent 函数, $s_2=f_1f_2+f_2f_3+f_3f_1$, 则 s_2 为 Bent 函数当且仅当 $\tilde{s}_1=\tilde{f}_1+\tilde{f}_2+\tilde{f}_3$. 此外, 如果 s_2 为 Bent 函数, 那么 $\tilde{s}_2=\tilde{f}_1\tilde{f}_2+\tilde{f}_2\tilde{f}_3+\tilde{f}_3\tilde{f}_1$.

3.3 多项式型Bent函数

因为向量空间 F_2^n 与有限域 F_{2^n} 是同构的, 布尔函数在有限域 F_{2^n} 上可以用迹函数来表示. 为了给出布尔函数的迹表示, 我们首先给出迹函数的定义. 假设 F_{2^k} 是 F_{2^n} 的一个子域, 其中 $k|n$. 从 F_{2^n} 到 F_{2^k} 的迹函数定义为

$$\mathrm{Tr}_k^n(x)=\sum_{i=0}^{n/k-1}x^{2^{ik}}=x+x^{2^k}+x^{2^{2k}}+\cdots+x^{2^{n-k}},x\in F_{2^n}$$

迹函数 Tr_k^n 满足以下性质:

(1) $\mathrm{Tr}_k^n(x+y)=\mathrm{Tr}_k^n(x)+\mathrm{Tr}_k^n(y)$, 其中 $x,y\in F_{2^n}$;

(2) $\mathrm{Tr}_k^n(cx)=c\mathrm{Tr}_k^n(x)$, 其中 $c\in F_{2^k},x\in F_{2^n}$;

(3) $\mathrm{Tr}_k^n(x^{2^k})=\mathrm{Tr}_k^n(x)$, 其中 $x\in F_{2^n}$;

(4) $\mathrm{Tr}_k^n(x)=\mathrm{Tr}_k^r(\mathrm{Tr}_r^n(x))$, 其中 $x\in F_{2^n},F_{2^k}\subseteq F_{2^r}\subseteq F_{2^n}$.

由性质(1)(2)可知, 迹函数 Tr_k^n 是 F_{2^n} 到 F_{2^k} 上的线性映射.

在给定 F_{2^n} 的一组基 $(\alpha_1,\alpha_2,\cdots,\alpha_n)$ 后, F_{2^n} 中元素 x 与 F_2^n 中的向量 $(x_1,x_2,\cdots,x_n)$ 有如下一一对应关系:

$$x = x_1\alpha_1 + x_2\alpha_2 + \cdots + x_n\alpha_n \in F_{2^n}$$

因此布尔函数 $f(x_1, x_2, \cdots, x_n)$ 可以写成一个单变量的多项式函数

$$f(x) = \sum_{i=0}^{2^n-1} c_i x^i$$

其中 $c_i \in F_{2^n}$. 此形式下, 多项式函数 f 是布尔函数的充要条件为

(1) $c_0, c_{2^n-1} \in F_2$;

(2) $c_{2j} = c_j^2$, 对于任意的 $j \neq 0$ 和 $j \neq 2^n - 1$, 其中下标 $2j$ 模 $2^n - 1$.

对于 $0 \leqslant s \leqslant 2^n - 2$, 定义含 s 的分圆陪集为

$$C_s = \left\{s, 2s, 2^2 s, \cdots, 2^{n_s-1} s\right\} \bmod \left(2^n - 1\right)$$

其中 n_s 是使得 $s = 2^{n_s} s \bmod \left(2^n - 1\right)$ 成立的最小正整数. 一般选取分圆陪集 C_s 中最小的整数作为此陪集的代表元, 称作陪集首.

根据前面提到的迹函数和分圆陪集的定义, 我们可以得到布尔函数的迹表示:

$$f(x) = \sum_{j \in \Gamma_n} \mathrm{Tr}_1^{o(j)}\left(c_j x^j\right) + \epsilon\left(1 + x^{2^n-1}\right)$$

其中

(1) Γ_n 表示模 $2^n - 1$ 的所有分圆陪集的陪集首构成的集合;

(2) $o(j)$ 表示含 j 的分圆陪集的大小;

(3) $c_j \in F_{2^{o(j)}}$;

(4) $\epsilon = \mathrm{wt}(f) \bmod 2$.

此形式下, 单项式 x^j 的次数为 j 的二进制展开中 1 的个数, 记为 $\mathrm{wt}(j)$. $f(x)$ 的代数次数为迹表示中所有具有非零系数的单项式的次数的最大值. 当 $\epsilon = 1$ 时, $\deg(f) = n$; 当 $\epsilon = 0$ 时, $\deg(f) < n$. 如果 $f(x)$ 中仅包含一项, 则称 $f(x)$ 为单项式, 否则称为多项式.

人们在研究过程中发现, 某些多项式形式的Bent函数的存在条件与一些经典的指数和有关. 下面给出Kloosterman和与立方和的定义.

定义 5 F_{2^n} 上的 Kloosterman 和定义为 $K_n(\mathrm{a}) = \sum_{x \in F_{2^n}} (-1)^{\left(\mathrm{Tr}_1^n(ax+1/x)\right)}$, 其中 $a \in F_{2^n}$, 并假设 $\mathrm{Tr}_1^n\left(\frac{1}{0}\right) = 0$.

定义 6 F_{2^n} 上的立方和定义为 $C_n(a,b) = \sum_{x \in F_{2^n}} (-1)^{\left(\mathrm{Tr}_1^n\left(ax^3+bx\right)\right)}$, 其中 $a \in F_{2^n}^*, b \in F_{2^n}$.

3.3.1 幂函数型

如果函数 $f(x)$ 的单变量表示形式仅包含一项, 则构造所得的 Bent 函数就被称为幂函数型 Bent 函数. 幂函数型函数一般的表示形式为 $f(x) = \mathrm{Tr}\left(\alpha x^d\right)$. 如果对于特定的指数 d, 存在 $\alpha \in F_{2^n}$ 使得 $f(x)$ 为 Bent 函数, 则称 d 为 Bent 指数. 目前已知的幂函数型 Bent 函数有 Gold 函数、Dillon 函数、Kasami 函数、Leander 函数和 Canteaut-Charpin-Kyureghyan 函数五类.

定理 20(Gold 函数)[9] $\alpha \in F_{2^n}$, $r \in N$, $d = 2^r + 1$. 函数 $f(x) = \mathrm{Tr}\left(\alpha x^d\right)$ 是 Bent 函数当且仅当 $\alpha \notin \left\{x^d \middle| x \in F_{2^n}\right\}$.

定理 21(Dillon 函数)[9,32] $\alpha\in F_{2^n}$, $n=2k$, $d=2^r+1$. 函数 $f(x)=\mathrm{Tr}(\alpha x^d)$ 是 Bent 函数当且仅当 $K_k\left(\alpha^{2^k+1}\right)=0$, 并且在这种情况下 f 的对偶恰为它自身.

推论 8 同定理 21 中条件, 对于任意与 2^k+1 互素的整数 s, 函数 $f'(x)=\mathrm{Tr}(\alpha x^{sd})$ 是 Bent 函数当且仅当 $K_k\left(\alpha^{2^k+1}\right)=0$.

定理 22(Kasami 函数)[32,33] n 为偶数, $\alpha\in F_{2^n}$, $d=2^{2r}-2^r+1$, $\gcd(r,n)=1$. 函数 $f(x)=\mathrm{Tr}(\alpha x^d)$ 是 Bent 函数当且仅当 $\alpha\notin\left\{x^3\middle|x\in F_{2^n}\right\}$.

定理 23(Leander 函数)[34,35] $n=4r$, r 为奇数, $\alpha\in F_{2^n}$, $d=\left(2^r+1\right)^2$, 函数 $f(x)=\mathrm{Tr}(\alpha x^d)$ 是 Bent 函数当且仅当 $\alpha\in\omega\cdot F_{2^r}$, 其中 $\omega\in F_4\setminus F_2$.

定理 24(Canteaut-Charpin-Kyureghyan 函数)[36] $n=6r$, $\alpha\in F_{2^n}$, $d=2^{2r}+2^r+1$, 函数 $f(x)=\mathrm{Tr}(\alpha x^d)$ 是 Bent 函数当且仅当 $\alpha\in F_{2^{3r}}$, 且 $\mathrm{Tr}_k^{3k}(\alpha)=0$.

3.3.2 多项式型

多项式型 Bent 函数的构造, 人们研究的热点主要集中于两类特殊的指数——Niho 指数和 Dillon 指数以及特殊的多项式型——二次型, 得到了很多结果.

我们首先介绍 Niho 指数的研究成果. 如果 x^d 限制在 $F_{2^{n/2}}$ 上是线性的, 即 $d\equiv 2^i \bmod\left(2^{n/2}-1\right)$, 则称指数 d 为 Niho 指数. 不失一般性, 取 $i=0$, 则 $d=\left(2^{n/2}-1\right)s+1$, 其中 $2\leqslant s\leqslant 2^{n/2}$.

Dobbertin 等在文献[37]研究了两项 Niho 指数在三种特殊取值下的情况, 得到如下定理.

定理 25 $n=2m$, f 是定义在 F_{2^n} 上的布尔函数

$$f(x)=\mathrm{Tr}_1^n\left(\alpha_1 x^{\frac{2^m-1}{2}+1}+\alpha_2 x^{d_2}\right)$$

其中 $\alpha_1,\alpha_2\in F_{2^n}^*$. 假设有 $\alpha_2^{\left(2^m+1\right)/2}=\alpha_1+\alpha_1^{2^m}$,

(1) 取 $d_2=\left(2^m-1\right)3+1$, 如果 $\alpha_2=\gamma^5$ 对一些 $\gamma\in F_{2^n}^*$ 成立, 则 f 是次数为 m 的 Bent 函数.

(2) m 是奇数, $d_2=\left(2^m-1\right)/4+1$, 则 f 是次数为 3 的 Bent 函数.

(3) m 是偶数, $d_2=\left(2^m-1\right)/6+1$, 则 f 是次数为 m 的 Bent 函数.

随后, Leander 和 Kholosha 在文献[38]中将上述两项的形式推广到多项, 得到了新的 Bent 函数, Budaghyan 等在文献[39]中给出了新函数的对偶函数.

定理 26[38,39] $n=2m$, $r>1$, 且 $\gcd(r,m)=1$. $\alpha\in F_{2^n}$ 满足 $\alpha+\alpha^{2^m}=1$, 对于 $i=1,2,\cdots,2^{r-1}-1$, 取 $s_i=i/2^r \bmod\left(2^m+1\right)$, $d_i=\left(2^m-1\right)s_i+1$ 是 Niho 指数. 则定义在 F_{2^n} 上的函数 $f(x)=\mathrm{Tr}_1^n\left(\alpha x^{2^m+1}+\sum_{i=1}^{2^{r-1}-1}x^{d_i}\right)$ 是 Bent 函数. 取 $u\in F_{2^n}$ 满足 $u+u^{2^k}=1$. $f(x)$ 的对偶函数为

$$\hat{f}(\omega)=\mathrm{Tr}_1^m\left(\left(u\left(1+\omega+\omega^{2^m}\right)+u^{2^{n-r}}+\omega^{2^m}\right)\times\left(1+\omega+\omega^{2^m}\right)^{\frac{1}{2^r-1}}\right)$$

进一步, 如果 $d<m$ 由 $dr\equiv 1 \bmod m$ 唯一确定, 则 $\hat{f}(\omega)$ 的代数次数为 $d+1$.

关于 Niho Bent 函数的研究还有另一种思路, 是由 Carlet 和 Mesnager 在 2011 年给出的[40]. 为了介绍此结果, 先介绍相关的 Bent 函数集合 H 以及 o-多项式(oval polynomial)等概念.

Dillon 在其博士论文[9]中给出了一类 Bent 函数集合, 记为 H. H 中函数的双变量表示形式为 $f(x,y)=\mathrm{Tr}_1^m\left(y+xF\left(yx^{2^m-2}\right)\right)$, 其中 $x,y\in F_{2^m}$, F 是 F_{2^m} 上的置换并满足 $F(x)+x$ 不为 0, 并且对于任意的 $\beta\in F_{2^m}^*$, 函数 $F(x)+\beta x$ 是 2 到 1 的. (条件 $F(x)+x$ 不为 0 不是函数 $f(x,y)$ 为 Bent 函数的必要条件, 而是 $f(x,y)$ 属于 PS 类函数的必要条件.)

函数 $f,g:F_2^n\to F_2$ 如果存在 F_2^n 上的仿射置换 L 及仿射函数 $l:F_2^n\to F_2$ 满足 $g(x)=(f\circ L)(x)+l(x)$, 则称函数 f 和 g 是 EA 等价(Extended-Affine Equivalent)的.

o-多项式是来源于有限几何中的记号, 其定义如下:

定义 7 m 为正整数, F_{2^m} 上的置换多项式 G 被叫做 o-多项式, 如果满足对于每个 $\mu\in F_{2^m}$, 函数

$$z\in F_{2^m}\to\begin{cases}\left(G(z+\mu)+G(\mu)\right)/z, & z\neq 0\\ 0, & z=0\end{cases}$$

单变量表示形式只有一项的o-多项式叫做o-单项式. 线性的o-单项式只有Frobenius映射 $G(z)=z^{2^i}$, 其中 $\gcd(i,m)=1$. 文献[41]证明了三次 o-单项式仅有一个, 为 $G(z)=z^{3\cdot 2^k+4}$, 其中 $m=2k-1$. 所有已知的二次 o-单项式列举如下[42]:

(1) $G(z)=z^{2^i}$, 其中 $\gcd(i,m)=1$;

(2) $G(z)=z^6$, 其中 m 为奇数;

(3) $G(z)=z^{2^{2k}+2^k}$, 其中 $m=4k-1$;

(4) $G(z)=z^{2^{3k+1}+2^{2k+1}}$, 其中 $m=4k+1$;

(5) $G(z)=z^{2^k+2}$, 其中 $m=2k-1$;

(6) $G(z)=z^{2^{m-1}+2^{m-2}}$, 其中 m 为奇数.

其他关于 o-多项式的结果可以参见文献[43,44].

2011 年 Carlet 和 Mesnager[40]将 Dillon 提出的 Bent 函数集 H 做了推广, 得到 Bent 函数集 $\mathcal{H}$. $\mathcal{H}$ 中函数的形式为

$$g(x,y)=\begin{cases}\mathrm{Tr}_1^m\left(xG\left(\frac{y}{x}\right)\right), & x\neq 0\\ \mathrm{Tr}_1^m(\mu y), & x=0\end{cases}$$

其中 $\mu\in F_{2^m}$, G 为 F_{2^m} 到自身的映射且满足对于任意 $\beta\in F_{2^m}^*$, 函数 $G(x)+\beta x$ 在 F_{2^m} 上是 2 到 1 的.

Carlet 和 Mesnager 发现 $\mathcal{H}$ 中函数的单变量表示恰好对应于之前文献[37,38]所研究的 Niho Bent 函数, 从而对集合 $\mathcal{H}$ 的研究等同对 Niho Bent 函数的研究. 文章随后给出了集合 $\mathcal{H}$ 与 o-多项式的关系, 结果如下.

定理 27 上式定义的函数 $g(x,y)$ 属于 Bent 函数集 $\mathcal{H}$, 当且仅当函数 G 为 o-多项式.

Carllet 和 Mesnager 利用定理 27 和已有的 o-多项式函数, 得到了一些新的 Niho Bent 函数, 具体结果可以参见文献[40].

2014 年, Budaghyan 等在文献[45]中沿着文献[40]的思路, 证明了任意的单变量 Niho Bent 函数可由如下特殊形式的函数(Leander-Kholosha 型[38])求和得到, 结果如下.

定理 28 任何单变量形式的 Niho Bent 函数, 在 EA 等价的意义下, 可由具有以下形式的函数求和得到.

$$\mathrm{Tr}_1^n\left(A_{2^{r-1}}t^{2^m+1}+\sum_{i=1}^{2^{r-1}-1}A_i t^{\left(2^m-1\right)\left(2^{m-r}i+1\right)+1}\right)$$

每一个上述形式的函数都是由 Bent 函数所对应 o-多项式所含的每个单项决定, 其中 A_i, $i=1,2,\cdots,2^{r-1}$ 为非零系数集合, 参数 $m-r$ 表示这个单项式所含指数二进制展开后数字 1 的最低位置, 并且满足 $0<m-r<m$.

同时 Budaghyan 还给出了所有已知的二次和三次 o-单项式所对应的 Niho Bent 函数的精确的双变量表示形式, 具体结果可以参见文献[45].

下面我们介绍 Dillon 指数的一些研究结果. 首先是 Mesnager 在文献[46]中考虑的二项式情况.

定理 29 $n=2m$, m 为奇数且 $m>3$, $\gcd\left(r,2^m+1\right)=1$. $a\in F_{2^m}^*$ 且 $b\in F_4^*$. 定义在 F_{2^n} 上的函数 $f_{a,b}^{(r)}$ 形式为

$$f_{a,b}^{(r)}(x)=\mathrm{Tr}_1^n\left(ax^{r\left(2^m-1\right)}\right)+\mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right)$$

则可得到下述性质

(1) $f_{a,b}^{(r)}$ 是 Bent 函数当且仅当 $f_{a,b}^{(1)}$ 是 Bent 函数当且仅当 $K_m(a)=4$;

(2) 如果 $f_{a,b}^{(r)}$ 是 Bent 函数, 则它属于 PS^- 类, 如果进一步有 $b=1\left(b\neq 1\right)$, 则它属于 $\mathrm{PS}_{\mathrm{ap}}\left(\mathrm{PS}_{\mathrm{ap}}^{\#}\right)$;

(3) 如果 $f_{a,b}^{(r)}$ 是 Bent 函数, 则它的对偶函数为 $f_{a^{2^m},b^2}^{(r)}$.

注 2 函数类 $\mathrm{PS}_{\mathrm{ap}}^{\#}$ 是由 $\mathrm{PS}_{\mathrm{ap}}$ 函数通过变换 $x\to\delta x\left(\delta\in F_{2^n}^*\right)$ 以及添加常函数得到的函数类. 显然有 $\mathrm{PS}_{\mathrm{ap}}\subseteq\mathrm{PS}_{\mathrm{ap}}^{\#}$.

定理 29 给出的是 m 为奇数的情况, 若 m 为偶数, 只有如下的必要条件.

定理 30 $n=2m$, m 为偶数且 $m>2$, $\gcd\left(r,2^m+1\right)=1$. $a\in F_{2^m}^*$ 且 $b\in F_4^*$. 函数 $f_{a,b}^{(r)}$ 定义同定理 29, 则 $f_{a,b}^{(r)}$ 是 Bent 函数当且仅当 $f_{a,b}^{(1)}$ 是 Bent 函数, 并且如果 $f_{a,b}^{(r)}$ 是 Bent 函数, 则 $K_m(a)=4$.

随后, Mesnager 在文献[47]中研究了 $r=3$ 特殊情况. 在 m 为奇数时, $\gcd\left(r,2^m+1\right)\neq 1$, 可知此情况不属于定理 29.

定理 31 $n=2m$, m 为奇数. $a\in F_{2^m}^*$ 且 $b\in F_4^*$, β 是 F_4 的本原元, U 表示 $F_{2^n}^*$ 的阶为 2^m+1 的循环子群. ζ 为 U 的生成元. F_{2^n} 上的函数 $g_{a,b}$ 为

$$g_{a,b}(x)=\mathrm{Tr}_1^n\left(ax^{3\left(2^m-1\right)}\right)+\mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right)$$

如果 $g_{a,b}$ 是 Bent 函数, 则它属于类 PS^-, 并且它的对偶函数为 $g_{a^{2^m},b^2}$. 如果进一步有 $b=1\left(b\neq 1\right)$, 则它属于 $\mathrm{PS}_{\mathrm{ap}}\left(\mathrm{PS}_{\mathrm{ap}}^{\#}\right)$.

更进一步当 $m\neq 3\bmod 6$ 时,

(1) 如果 $\mathrm{Tr}_1^m\left(a^{1/3}\right)=0$, 则对于每个 $(i,j)\in\{0,1,2\}^2$, $g_{a\zeta^i,\beta^j}$ 是 Bent 函数当且仅当 $K_m(a)=4$.

(2) 如果 $\mathrm{Tr}_1^m\left(a^{1/3}\right)=1$, 则① g_{a,β^j} 对于所有的 $j\in\{0,1,2\}$ 都不是 Bent 函数; ②对于每个 $i\in\{1,2\}$, $j\in\{0,1,2\}$, $g_{a\zeta^i,\beta^j}$ 是 Bent 函数当且仅当 $K_m(a)+C_m(a,a)=4$.

而当 $m=3 \bmod 6$ 时, 对于所有的 $i \in \{0,1,2\}$, $g_{a\zeta^i,b}$ 都不是 Bent 函数.

前面研究的都是二项式的情况, Li 等在文献[48]中考虑多项式的情况, 对 $p=2$ 和 p 为奇素数的情况都有讨论.

定理 32[48] p 为任意素数, $q=p^m>3$, $n=2m$, $e\left|(q+1)\right.$, $a_i \in F_{q^2}$, $\epsilon \in F_{p^l}$, l 是最小的正整数满足 $l\left|n\right.$ 和 $e\left|p^l-1\right.$, $U=\left\{x \in F_{q^2}: x^{q+1}=1\right\}$. 函数

$$f(x)=\sum_{i=0}^{q-1}\mathrm{Tr}_1^n\left(a_i x^{i(q-1)}\right)+\mathrm{Tr}_1^l\left(\epsilon x^{\frac{q^2-1}{e}}\right)$$

是 Bent 函数当且仅当

$$\omega^{f(0)}=\sum_{z\in U}\omega^{\mathrm{Tr}_1^n\left(\sum_{i=0}^{q-1}a_i z^i\right)+\mathrm{Tr}_1^l\left(\epsilon z^{(q+1)/e}\right)}$$

文章在 $p=2$ 时讨论了以下两种形式的函数, 给出了它们为 Bent 函数的等价条件, 并在更特殊条件下给出更精细的刻画, 具体可参见文献[48].

$$f(x)=\mathrm{Tr}_1^n\left(ax^{l(q-1)}\right)+bx^{\left(\frac{q+1}{e}-l\right)(q-1)}+cx^{\left(\frac{q+1}{e}+l\right)(q-1)}+\mathrm{Tr}_1^l\left(\epsilon x^{\frac{q^2-1}{e}}\right)$$

$$f(x)=\sum_{i\in D}\mathrm{Tr}_1^n\left(ax^{(ri+s)(q-1)}\right)+\mathrm{Tr}_1^l\left(\epsilon x^{\frac{q^2-1}{e}}\right)$$

下面介绍二次型的部分研究结果. 关于二次型 Bent 函数有如下定理.

定理 33[49] n 为偶数, F_{2^n} 上的二次函数 $f(x)$ 是 Bent 函数当且仅当 $f(x)$ 的秩为 n.

2006 年 Youssef 和 Gong[50]研究了如下形式的二次函数

$$f(x)=\sum_{i=1}^{n/2-1}c_i\mathrm{Tr}_1^n\left(x^{1+2^i}\right)+c_{\frac{n}{2}}\mathrm{Tr}_1^{\frac{n}{2}}\left(x^{1+2^{\frac{n}{2}}}\right)$$

其中 $c_i \in F_2$.

定理 34[51] n 为偶数, $f(x)$ 如上式所示, 则 $f(x)$ 是 Bent 函数当且仅当 $\gcd\left(c(x),x^n+1\right)=1$, 其中

$$c(x)=\sum_{i=1}^{n/2-1}c_i\left(x^i+x^{n-i}\right)+c_{\frac{n}{2}}x^{\frac{n}{2}}$$

进一步, 如果 $f(x)$ 是 Bent 函数, 则 $c_{n/2}=1$.

文章随后给出在 n 的三种特殊取值下, 函数为 Bent 函数的充要条件, 并给出了一些计数结果.

随后, Hu 和 Feng 在文献[52]中考虑如下形式的函数

$$f(x)=\sum_{i=1}^{m/2-1}c_i\mathrm{Tr}_1^n\left(\beta x^{1+2^{ei}}\right)+c_{\frac{m}{2}}\mathrm{Tr}_1^{\frac{n}{2}}\left(\beta x^{1+2^{\frac{n}{2}}}\right)$$

其中 $c_i \in F_2$, $i=1,2,\cdots,n/2-1$, $\beta \in F_{2^{n/2}}$, n 为偶数, e 为 n 的一个因子, 使得 $m=n/e$ 为偶数.

定理 35 函数 $f(x)$ 如上式定义, 则 $f(x)$ 为 Bent 函数当且仅当 $\gcd\left(c(x),x^m+1\right)=1$, 其中

$$c(x)=\sum_{i=1}^{m/2-1}c_i\left(x^i+x^{m-i}\right)+c_{\frac{m}{2}}x^{\frac{m}{2}}$$

特别的, 如果 $f(x)$ 是 Bent 函数, 则 $c_{m/2}=1$.

根据此定理, 文章进而得到在一些特殊情况下, 函数为 Bent 函数的条件, 并与已有结果作了比较, 并

彻底解决了文献[50]中的计数问题.

推论 9 对任意 $\beta\in F_{2^e}^*$, 定义在 F_{2^n} 上的函数 $f(x)$ 形式为

$$f(x)=\sum_{i=1}^{m/2-1}\mathrm{Tr}_1^n\left(\beta x^{1+2^{ei}}\right)+\mathrm{Tr}_1^{\frac{n}{2}}\left(\beta x^{1+2^{\frac{n}{2}}}\right)$$

是 Bent 函数. 特别的, 对任意 $\beta\in F_{2^{n/2}}^*$, 函数 $f(x)=\mathrm{Tr}_1^{n/2}\left(\beta x^{1+2^{n/2}}\right)$ 是一个 Bent 函数.

注 3 上式中, 如果取 $e=1,\beta=1$, 则结果同文献[53], 如果取 $e\geqslant 2,\beta=1$, 则结果同文献[54].

注 4 取 $\{\alpha_1,\alpha_2,\cdots,\alpha_e\}$ 为 F_{2^e} 在 F_2 上的一组基, $i=1,2,\cdots,e$,

$$f_i(x)=\sum_{j=1}^{m/2-1}\mathrm{Tr}_1^n\left(\alpha_i x^{1+2^{ej}}\right)+\mathrm{Tr}_1^{\frac{n}{2}}\left(\alpha_i x^{1+2^{\frac{n}{2}}}\right)$$

则对于任意 $(a_1,a_2,\cdots,a_e)\in F_2^e$, $(a_1,a_2,\cdots,a_e)\neq(0,0,\cdots,0)$, 函数 $a_1f_1(x)+a_2f_2(x)+\cdots+a_ef_e(x)$ 都是 Bent 函数.

除了上述构造, Wu 等在文献[55]中也给出了一类新构造.

定理 36 n 为偶数, $a\in F_{2^n}$, $a^{\left(2^n-1\right)/3}\neq 1$. 选择 T 的任意子集 I, 令 $J=n-(T\setminus I)=\{n-i\,|\,i\in T\setminus I\}$, $S=I\cup J$, 其中

$$T=\begin{cases}\left\{2i+1\,\middle|\,0\leqslant i\leqslant\dfrac{n}{4}-1\right\}, & n\equiv 0\bmod 4\\ \left\{2i+1\,\middle|\,0\leqslant i\leqslant\dfrac{n-6}{4}\right\}, & n\equiv 2\bmod 4\end{cases}$$

则

$$f(x)=\begin{cases}\displaystyle\sum_{i\in S}\mathrm{Tr}_1^n\left(a^{\frac{2^n-2^{2i+1}-2}{3}}x^{1+2^{2i+1}}\right), & n\equiv 0\bmod 4\\ \displaystyle\sum_{i\in S}\mathrm{Tr}_1^n\left(a^{\frac{2^n-2^{2i+1}-2}{3}}x^{1+2^{2i+1}}\right)+\mathrm{Tr}_1^{\frac{n}{2}}\left(a^{\frac{2^n-2^{\frac{n}{2}}-2}{3}}x^{1+2^{\frac{n}{2}}}\right), & n\equiv 2\bmod 4\end{cases}$$

是 Bent 函数.

除了直接证明函数的 Bent 性质, 还可以通过 Bent 函数与广义 Bent 函数的关系来得到新的 Bent 函数. Li 等在文献[56]中首先研究新的广义 Bent 函数, 进而给出新的 Bent 函数的构造. 文章考察如下所示的二次函数

$$f_Q(x)=p(x)+\sum_{i=1}^{\lfloor(n-1)/2\rfloor}\mathrm{Tr}_1^n\left(c_ix^{1+2^{ki}}\right)$$

其中 $c_i\in F_2$, $x\in F_{2^n}$,

$$p(x)=\begin{cases}\displaystyle\sum_{i=1}^{(n-1)/2}\mathrm{Tr}_1^n\left(x^{1+2^i}\right), & m\text{为奇数}\\ \displaystyle\sum_{i=1}^{n/2-1}\mathrm{Tr}_1^n\left(x^{1+2^i}\right)+\mathrm{Tr}_1^{\frac{m}{2}}\left(x^{1+2^{\frac{m}{2}}}\right), & m\text{为偶数}\end{cases}$$

定理 37[56] m 为偶数, k 为正整数, $f_Q(x)$ 是 Bent 函数当且仅当 $\gcd\left(c\left(x^k\right),x^n-1\right)=1$, 其中

$$c(x)=1+\sum_{i=1}^{\lfloor (n-1)/2\rfloor}\left(c_i x^i+c_i x^{m-i}\right)\in F_2[x]$$

除了使用文章中新构造的广义 Bent 函数, 文章还根据文献[57]中得到的广义 Bent 函数来构造新的布尔 Bent 函数.

定理 38[56,57] $f_{a,b}(x)=\mathrm{Tr}_1^n\left(ax+2bx^{1+2^k}\right)$, n 为偶数, k 为正整数满足 $n/\gcd(n,k)$ 是奇数, $a\in L, b\in L$ 使得 $f_{a,b}(x)$ 为广义 Bent 函数, 则函数 $p(\bar{a}x)+\mathrm{Tr}_1^n\left(\bar{b}x^{1+2^k}\right)$ 是 Bent 函数, 其中 $\bar{x}$ 表示从 R 到 F_{2^n} 的模 2 约化, R 为特征为 4 阶为 4^n 的 Galois 环.

在多项式型的构造中, 除了之前介绍的两类指数以及特殊的二次型, 还有一些其他的研究工作, 比如研究较特殊的旋转对称函数. Gao 等[58]研究了如下两类旋转对称函数为 Bent 函数的条件.

$$f_c(x)=\sum_{i=1}^{m-1}c_i\left(\sum_{j=0}^{n-1}x_j x_{i+j}\right)+c_m\left(\sum_{j=0}^{m-1}x_j x_{m+j}\right)$$

$$f_t(x)=\sum_{i=0}^{n-1}\left(x_i x_{t+i}x_{m+i}+x_i x_{t+i}\right)+\sum_{i=0}^{m-1}x_i x_{m+i}$$

其中 $n=2m$, $c_i\in\{0,1\}$, $0<t<m$.

定理 39[58] $n=2m$, $m\geqslant 2$, $f_c(x)$ 如上定义. $R=F_2[X]/(X^n+1)$ 是 F_2 上多项式环, $F_c(X)=\sum_{i=1}^{m-1}c_i\left(X^i+X^{n-i}\right)+c_m X^m\in R$. 则 $f_c(x)$ 是 Bent 函数当且仅当 $\gcd\left(F_c(X),X^n+1\right)=1$.

定理 40[58] $n=2m$, $m\geqslant 2$, $0<t<m$, $r=m/\gcd(m,t)$. 则立方旋转对称函数 $f_t(x)$ 是 Bent 函数当且仅当 r 是奇数.

除了本节所介绍的, 其他的关于布尔 Bent 函数的相关研究可以参见[40,59–74]等文献.

4 广义 Bent 函数

布尔函数有多种推广形式, 我们首先考虑形式为 $Z_2^n\to Z_p$ 的函数, 这一类函数被称作广义布尔函数, 是由 Schmidt 在文献[10]中率先考虑的.

广义布尔函数 $f:Z_2^n\to Z_p$ 的 Walsh 变换定义如下:

$$\hat{f}(\boldsymbol{\lambda})=\sum_{\boldsymbol{x}\in F_2^n}\omega^{f(\boldsymbol{x})}(-1)^{\boldsymbol{\lambda}\cdot\boldsymbol{x}}$$

其中 $\boldsymbol{\lambda}\in Z_2^n$, ω 是 p 次本原单位根, 即 $\omega=e^{2\pi i/p}$.

定义 8 f 是广义 Bent 函数当且仅当对所有的 $\boldsymbol{\lambda}\in Z_2^n$, 都有 $\left|\hat{f}(\boldsymbol{\lambda})\right|=2^{n/2}$.

注 5 广义 Bent 函数的存在性不对 n 的奇偶性有要求.

若 f 是广义 Bent 函数，并且满足对于任意的 $\boldsymbol{\lambda}\in Z_2^n$ 都有 $\hat{f}(\boldsymbol{\lambda})=2^{n/2}\omega^{k_\lambda}$, 其中 $0\leqslant k_\lambda<p$, 则存在广义布尔函数 $g:Z_2^n\to Z_p$ 使得 $\hat{f}(\boldsymbol{\lambda})=2^{n/2}\omega^{g}$. 称函数 g 为函数 f 的对偶函数，记为 $g=\tilde{f}$，此时函数 g 也为广义 Bent 函数，且有 $\tilde{g}=f$.

注 6 只有部分广义 Bent 函数存在对偶函数.

Schmidt 在文献[10]中首先对广义布尔函数 $f:Z_2^n\to Z_p$ 在 $p=4$ 的情况下进行了研究, 主要得到了三类构造, 其中第一个构造可看成布尔函数 M-M 类的推广.

定理 41 n 变量广义布尔函数 $f(\boldsymbol{x},\boldsymbol{y})=2\boldsymbol{x}\cdot\pi(\boldsymbol{y})+g(\boldsymbol{y})$ 是广义 Bent 函数, 其中 $\boldsymbol{x},\boldsymbol{y}\in Z_2^{n/2}$, π 是 $Z_2^{n/2}$ 上的置换, g 为 $n/2$ 个变量的任意广义布尔函数.

定理 42 假设 $n\geqslant 3$. R_n 表示特征为 4 的大小为 4^n 的 Galois 环, R_n^x 表示 $R_n\setminus 2R_n$. T_n 表示 R_n 的 Teichmuller 集, Tr 表示 R_n 上的迹函数. 定义在 $x\in T_n$ 上的 n 变量广义布尔函数

$$f(x)=\epsilon+\mathrm{Tr}(sx)$$

是 Bent 函数, 其中 $\epsilon\in Z_4$, $s\in R_n^x$.

定理 43 与定理 42 记号一致. μ 表示从 R_n 到 F_{2^n} 的模 2 约化. 定义在 $x\in T_n$ 上的 n 变量广义布尔函数

$$f(x)=\epsilon+\mathrm{Tr}(sx+2tx^3)$$

是 Bent 函数, 其中 $\epsilon\in Z_4$, $s\in R_n$, $t\in T_n\setminus\{0\}$. 当且仅当 $\mu(s)=0$, 并且方程 $\mu(t)z^3+1=0$ 在 F_{2^n} 上没有解, 或者 $\mu(s)\neq 0$, 并且方程 $z^3+z+\mu(t)^2/\mu(t)^6=0$ 在 F_{2^n} 上没有解.

在文献[75]中, Solé 和 Tokareva 也是在 $p=4$ 的特殊情况下进行研究. 他们讨论了布尔 Bent 函数与广义 Bent 函数的关系, 有如下结果.

定理 44[75] $f:Z_2^{2n}\to Z_4$ 是广义布尔函数, 可以表示为 $f(\boldsymbol{x},\boldsymbol{y})=a(\boldsymbol{x},\boldsymbol{y})+2b(\boldsymbol{x},\boldsymbol{y})$, 其中 $\boldsymbol{x},\boldsymbol{y}\in Z_2^n$, $a,b:Z_2^{2n}\to Z_2$ 为布尔函数, 则 f 是广义 Bent 函数当且仅当 b 和 $a+b$ 都是 Bent 函数.

随后, Stănică等在文献[76]中对广义布尔函数进行了研究, 得到了三类广义 Bent 函数的构造方法, 这些构造方法可以看作是布尔 Bent 函数构造方法的推广.

下面首先介绍的是将 M-M 类进行推广得到的广义 M-M 类, 简记为 GMMF.

定理 45[76] p 是偶数, π 是 $Z_2^{n/2}$ 上的置换, g 为任意 $Z_2^{n/2}$ 到 Z_p 的函数, $f:Z_2^n\to Z_p$ 定义为

$$f(\boldsymbol{x},\boldsymbol{y})=\frac{p}{2}\boldsymbol{x}\cdot\pi(\boldsymbol{y})+g(\boldsymbol{y})$$

其中 $\boldsymbol{x},\boldsymbol{y}\in Z_2^{n/2}$. 则 $f(\boldsymbol{x},\boldsymbol{y})$ 是广义 Bent 函数, 并且其对偶为 $\tilde{f}(\boldsymbol{x},\boldsymbol{y})=g(\pi^{-1}(\boldsymbol{x}))+\frac{p}{2}\boldsymbol{y}\cdot(\pi^{-1}(\boldsymbol{x}))$.

Stănică在文章中还给出了 Dillon 的 PS 类 Bent 函数的推广构造—广义 Dillon 类, 简记为 GD.

假设 $n=2k$, $E_i\ (i=1,2,\cdots,2^k+1)$ 是 Z_2^n 的 2^k+1 个两两不相交 k 维子空间, 并且满足

$$Z_2^n=\bigcup_{i=1}^{2^k+1}E_i=\bigcup_{i=1}^{2^k+1}E_i^{\perp}$$

定理 46[76] $n=2k$, t, $\omega=e^{2\pi i/p}$, $m_1,m_2,\cdots,m_{2^k+1}$ 满足等式 $\sum_{i=1}^{2^k+1}\omega^{m_i}=\omega^t$. $F:Z_2^n\to C$ 定义为

$$F(\boldsymbol{x})=\sum_{i=1}^{2^k+1}\omega^{m_i}\Phi_{E_i}(\boldsymbol{x})$$

则函数 $f:Z_2^n\to Z_p$ 定义为 $w^{f(x)}=F(\boldsymbol{x})$ 是广义 Bent 函数.

文献[76]也将 Carlet 所提出的 GPS 类也进行了推广, 构造了类 GS.

假设 $n=2k$, 取 $E_1,E_2,\cdots,E_t$ 是 Z_2^n 的 t 个 k 维子空间满足

$$\bigcup_{i=1}^{t}E_i=\bigcup_{i=1}^{t}E_i^{\perp}=Z_2^n$$

对每一个 $\boldsymbol{x}\in Z_2^n$, 定义两个集合 $\varepsilon_x=\{E_i:\boldsymbol{x}\in E_i\}$, $\varepsilon_x{}^{\perp}=\{E_i^{\perp}:\boldsymbol{x}\in E_i^{\perp}\}$.

定理 47[76] $m_1,m_2,\cdots,m_t$ 为整数, $F:Z_2^n\to C$ 定义为

$$F(\boldsymbol{x})=\sum_{i=1}^{t}\omega^{m_i}\Phi_{E_i}(\boldsymbol{x})$$

如果有 $\sum_{i:E_i\in\varepsilon_x}\omega^{m_i}$, $\sum_{i:E_i^{\perp}\in\varepsilon_x^{\perp}}\omega^{m_i}\in\{\omega^j:j=0,1,\cdots p-1\}$, 则函数 $f:Z_2^n\to Z_p$ 定义为 $w^{f(x)}=F(\boldsymbol{x})$ 是广义 Bent 函数.

注 7 Carlet 所提出的 GPS 类包含所有的 Bent 函数. 文章[76]中所构造的类 GS 已知包含类 GMMF 和类 GD, 即 GD$\bigcup$GMMF$\subseteq$GS, 但不知道是否包含所有的广义 Bent 函数, 这仍是一个公开问题.

4.1 多项式型广义Bent函数

与布尔 Bent 函数的情况类似, 我们同样可以从有限域的角度去考虑广义布尔函数. 本节主要讨论在 $p=4$ 的情况下, 特殊的二次型的一些研究结果.

首先给出 Z_4 值二次型的定义. 考虑 $R=\mathrm{GR}(4,n)=Z_4[x]/h(x)$, $h(x)$ 为 $Z_4[x]$ 上代数次数为 n 的首一本原不可约多项式, R 为特征为 4 阶为 4^n 的 Galois 环. 取 $h(x)$ 的一个根 ξ, 则 $\xi^{2^n-1}=1$, R 可以记为 $Z_4[\xi]$, R 中的每个元素 $z\in R$ 可以唯一的表示为 $z=x+2y$, $x,y\in L$. L 为 R 的 Teichhmuller 集, 定义为 $\{0,1,\xi,\xi^2,\cdots,\xi^{2^n-2}\}$. 对于 $x,y\in L$, 定义 $x\oplus y=x+y+2\sqrt{xy}$.

一个对称的双线性映射 $B:L\times L\to Z_2$ 具有如下两条性质

(1) $B(x,y)=B(y,x)$;

(2) $B(x\oplus y,z)=B(x,z)\oplus B(y,z)$.

B 的秩定义为 $\mathrm{Rank}(B)=m-\dim_{Z_2}(\mathrm{rad}(B))$, 其中 $\mathrm{rad}(B)=\{x\in L:B(x,y)=0,\forall y\in L\}$.

定义 9[77] Z_4 值二次型 $F:L\to Z_4$ 是满足下面两个条件的映射

(1) $Q(ax)=a^2Q(x)$, $a\in Z_4$;

(2) $Q(x\oplus y)=Q(x)+Q(y)+2B(x,y)$.

Q 的秩定义为 $\mathrm{Rank}(Q)=\mathrm{Rank}(B)$. .

Schmidt 在文献[78]给出了二次型广义函数为广义 Bent 函数的条件.

定理 48 对于 Z_4 值二次型 $Q(x)$, $Q(x)$ 是广义 Bent 函数当且仅当 $Q(x)$ 是满秩的

Li 等在文献[57]中考虑了一项为 Gold 指数的双项式情况.

定理 49 n,k 为正整数满足 $n/\gcd(n,k)$ 是奇数, $a\in R$, $b\in L$, $\bar{x}$ 表示从 R 到 F_{2^n} 的模 2 约化, 其中 R 和 L 同本节开始处定义. 函数 $f_{a,b}(x)=\mathrm{Tr}_1^n\left(ax+2bx^{1+2^k}\right)$ 是广义 Bent 函数当且仅当下面条件都成立

(1) $\bar{a}\neq 0,\bar{b}\neq 0$;

(2) $\bar{a}\bar{b}\neq 0$, $\bar{b}^{2^k}x^{1+2^k}+\bar{a}^{2^{k+1}}x+\bar{b}=0$ 在 F_{2^m} 上要么没有根, 要么有两个根.

但是当 $n/\gcd(n,k)$ 为偶数时并没有类似的结论.

2014 年, Li 等在文献[56]中考虑了如下多项的二次型函数

$$Q(x)=\mathrm{Tr}_1^n\left(x+2\sum_{i=1}^{\lfloor (n-1)/2\rfloor}c_ix^{1+2^{ki}}\right)$$

其中 $c_i\in Z_2$, $x\in L$.

定理 50 n 和 k 为正整数. 广义布尔函数 $Q(x)$ 为 Bent 函数当且仅当 $\gcd\left(c\left(x^k\right),x^n-1\right)=1$, $c(x)$ 定义

如下

$$c(x)=1+\sum_{i=1}^{\lfloor (n-1)/2\rfloor}\left(c_i x^i+c_i x^{n-i}\right)\in F_2[x]$$

文中同时给出了定理 50 的一些特殊情况作为推论, 以推论 10 为例.

推论 10 n 和 k 为正整数, $x\in L$. 函数 $Q(x)=\mathrm{Tr}_1^n\left(x+2x^{1+2^{2k}}+2x^{1+2^{3k}}\right)$ 是 Bent 函数当且仅当 $\gcd(n,3k)=\gcd(n,k)$.

除了本节介绍之外, 更多的关于广义 Bent 函数的研究结果可以参见文献[79,80]等.

5 *p* 值 Bent 函数

下面介绍 Bent 函数的另一类推广形式 $f:Z_p^n\to Z_p$, 称为 p 值函数. Kumar 等在 1985 年的文献[81]中率先考虑此类推广. 此种情况下 $f(\boldsymbol{x})$ 的 Walsh 变换定义如下:

$$\hat{f}(\boldsymbol{\lambda})=\sum_{\boldsymbol{x}\in Z_p^n}\omega^{f(\boldsymbol{x})-\boldsymbol{\lambda}\cdot\boldsymbol{x}}$$

其中 $\omega=e^{2\pi i/p}$ 为 p 次单位根, $\boldsymbol{\lambda}\in Z_p^n$.

定义 10 函数 $f:Z_p^n\to Z_p$ 是 Bent 函数当且仅当对于任意的 $\boldsymbol{\lambda}\in Z_p^n$, $\left|\hat{f}(\boldsymbol{\lambda})\right|=p^{n/2}$ 都成立.

定义 11 Bent 函数 f 叫做正则的, 如果对任意的 $\boldsymbol{\lambda}\in Z_p^n$, 都有 $p^{-n/2}\hat{f}(\boldsymbol{\lambda})=\omega^{f^*(\boldsymbol{\lambda})}$, 其中 f^* 为 Z_p^n 到 Z_p 的函数. Bent 函数 f 叫做弱正则的, 如果存在复数 u, $|u|=1$, 对任意的 $\boldsymbol{\lambda}\in Z_p^n$, 都有 $up^{-n/2}\hat{f}(\boldsymbol{\lambda})=\omega^{f^*(\boldsymbol{\lambda})}$.

关于 p 值 Bent 函数代数次数有如下结论.

定理 51[82] 如果 f 是 n 元 p 值 Bent 函数, 则 $\deg(f)\leqslant(p-1)n/2+1$. 进一步, 如果 f 是一个弱正则 Bent 函数, 并且 $(p-1)n\geqslant 4$, 则 $\deg(f)\leqslant(p-1)n/2$.

在文献[81]中, Kumar 等研究了 p 值 Bent 函数的存在性情况, 关于存在性和不存在性, 都得到了一些结果.

定理 52 p 值函数 $f:Z_p^n\to Z_p$, 当 n 为偶数或者 $p\neq 2\bmod 4$ 时, p 值 Bent 函数都存在.

Kumar 通过对上述所有情况都给出 p 值 Bent 函数的构造来证明此定理, 从而给出了不同条件下 p 值 Bent 函数的构造方法, 其中比较重要的是如下 M-M 形式的推广构造, 其余的构造形式可以参见文献[81].

定理 53 p 和 k 为任意正整数, $n=2k$, 函数

$$f(\boldsymbol{x})=\boldsymbol{x}_2\cdot\pi(\boldsymbol{x}_1)+g(\boldsymbol{x}_1)$$

其中 $\boldsymbol{x}=(\boldsymbol{x}_1,\boldsymbol{x}_2)$, π 是 Z_p^k 上的置换, g 是任意的 $Z_p^k\to Z_p$ 的函数, 则 $f(\boldsymbol{x})$ 为 p 值 Bent 函数.

Kumar 在文中也给出了 p 值 Bent 函数不存在性的研究结果.

定理 54 n 是奇数, 且 $p\equiv 2\bmod 4$, 如果 p 满足以下任何一个条件

(1) $p=2$;

(2) $p\neq 2$, 并且存在一个整数 b 满足 $2^b=-1\bmod(p/2)$.

则不存在 $Z_p^n\to Z_p$ 的 p 值 Bent 函数.

但对于 n 为奇数, p 不满足以上两个条件时, 是否存在 $Z_p^n\to Z_p$ 的 p 值 Bent 函数依然是一个公开问题. 近年来的研究证明了在其中很多情况下都不存在 p 值 Bent 函数, 但此问题仍没有完全解决. 我们简要

介绍下此部分的研究成果, 前置条件为 $2\nmid n\geqslant 1,\ p=2N,\ 2\nmid N\geqslant 3$, 此类函数记为 $[n,p]$ 函数.

首先 Pei 在文献[83]中证明了 $n=1,\ N=7$ 时 $[1,14]$ Bent 函数不存在. 随后 Akyildiz 等在文献[84]中给出了一类 Bent 函数不存在的条件, 要求 $n=1,\ N=q^e,\ e\geqslant 1,\ q$ 为素数且满足 $q\equiv 7 \bmod 8$ 并且 $q\neq 7$.

Ikeda 在文献[85]中也得到了一类不存在性结果:

定理 55 当 $n=1,\ p=2N,\ N=\prod_{i=1}^{t} q_i^{e_i}$ 为 N 的素因子分解. 如果对于每一个 i, 都存在 $s_i\leqslant 1$ 满足

$$q_i^{s_i}\equiv -1 \bmod \frac{N}{q_i^{e_i}}$$

则此时 Bent 函数不存在。

Feng 等学者也对此问题做了一系列研究，得到了很多不存在结果[86–90], 列举如下(所有 q_i 都是素数, n 满足与第一种情况类似的条件):

(1) $N=q^e,\ e\geqslant 1,\ q\equiv 7 \bmod 8,\ f$ 是 2 模 N 的阶, $s=\phi(n)/(2f)$ 为奇数, 取 m 为使得方程 $x^2+qy^2=2^{m+2}$ 有整数解 (x,y) 的最小的奇整数, $n<m/s$.

(2) $N=q_1^{e_1}q_2^{e_2},\ q_1\equiv 3 \bmod 4,\ q_2\equiv 5 \bmod 8,\ \left(\frac{q_1}{q_2}\right)=-1.$

(3) $N=q_1^{e_1}q_2^{e_2},\ q_1\equiv 3 \bmod 4,\ q_2\equiv \left(2^{\lambda}+1\right) \bmod 2^{\lambda+1},\ \left(\frac{q_1}{q_2}\right)=-1,\ \left(\frac{2}{q_2}\right)_4=1.$

(4) $N=q_1q_2,\ q_1\equiv q_2\equiv 7 \bmod 8,\ \left(\frac{q_1}{q_2}\right)=-1.$

(5) $N=q_1q_2,\ q_1\equiv 3 \bmod 8,\ q_2\equiv 7 \bmod 8,\ \left(\frac{q_1}{q_2}\right)=-1.$

(6) $N=q_1q_2,\ q_1\equiv 3 \bmod 8,\ q_2\equiv 7 \bmod 8,\ \left(\frac{q_2}{q_1}\right)=-1.$

(7) $N=q_1q_2,\ q_1\equiv 2^{\lambda}+1 \bmod 2^{\lambda+1},\ \lambda\geqslant 3,\ q_2\equiv 7 \bmod 8,\ \left(\frac{q_1}{q_2}\right)=1,\ \left(\frac{q_2}{q_1}\right)_4\neq 1,\ \left(\frac{2}{q_2}\right)\neq 1.$

(8) $N=q_1q_2,\quad q_1\equiv 5 \bmod 8,\ q_2\equiv 3 \bmod 4,\ \left(\frac{q_1}{q_2}\right)=1,\ \left(\frac{q_2}{q_1}\right)_4\neq 1.$

(9) $N=q_1q_2q_3,\ q_1\equiv 3 \bmod 8,\ q_2\equiv 7 \bmod 8,\ q_3\equiv 5 \bmod 8,\ \left(\frac{q_3}{q_1}\right)=\left(\frac{q_3}{q_2}\right)=-1,\ \left(\frac{q_1}{q_2}\right)=1.$

随后 Jiang 和 Deng 在文献[91]中给出了两类不存在性结果. 第一类结果是将上述 $N=q_1q_2$ 的一些情况做推广, 通过额外增加一些条件, 则能够得到不存在 $\left[n,2q_1^{e_1}q_2\right]$ 类 Bent 函数, 如果进一步满足更强的条件, 可以得到不存在 $\left[n,2q_1^{e_1}q_2^{\ n}\right]$ Bent 函数. 另外文章证明了不存在 $\left[n,2\cdot(23)^e\right]$ 类 Bent 函数, 其中 $n=1,3$.

更多的相关研究结果可以参见文献[92,93].

5.1 多项式型*p*值Bent函数

我们同样可以考虑多项式型 p 值函数 $f:F_{p^n}\to F_p$, 在本小节中都要求 p 为奇素数. 首先给出需要用到的指数和的定义.

定义 12 对于任意的非平凡加法特征 χ，任意 $a,b\in F_{p^k}$，定义 Kloosterman 和如下

$$K(\chi;a,b)=\sum_{c\in F_{p^k}^*}\chi\left(ac+bc^{-1}\right)$$

首先介绍单项式型的一些研究结果. 2006 年, Helleseth 和 Kholosha[94]研究了 Dillon 指数和 Gold 指数这两类单项式的情况. 首先考虑 Dillon 指数的情况.

定理 56[94] $n=2k$, p 为奇素数, 为正整数满足 $\gcd\left(t,p^k+1\right)=1$, $p^k>3$. 对于任意的 $a\in F_{p^n}^*$, 函数 $f(x)=\mathrm{Tr}_1^n\left(ax^{t\left(p^k-1\right)}\right)$ 是 Bent 函数当且仅当 $K\left(\chi_1;1,a^{p^k+1}\right)=-1$, 其中 χ_1 是 F_{p^k} 上典型加法特征. 进一步, 如果 $f(x)$ 是 Bent 函数, 则 $f(x)$ 是正则的, 并且 Walsh 谱系数为 $\hat{f}(b)=p^k\omega^{-\mathrm{Tr}_1^n\left(a^{p^k}b^{t\left(p^k-1\right)}\right)}$.

文章随后给出了 Gold 指数的 Bent 条件, 所得结果包含了文献[49,95,96]等文章中关于二次单项式的研究结果.

定理 57[94] $a\in F_{p^n}^*$, p 为奇素数. 对于任意的 $j\in\{1,2,\cdots,n\}$, 二次函数 $f(x)=\mathrm{Tr}_1^n\left(ax^{p^j+1}\right)$ 是 Bent 函数当且仅当

$$p^{\gcd(2j,n)}-1\nmid\frac{p^n-1}{2}-i_0\left(p^j-1\right)$$

其中 $\mathrm{a}=\zeta^{i_0}$, ζ 是 F_{p^n} 的本原元. 如果 $f(x)$ 是 Bent 函数, 则 $f(x)$ 是弱正则的.

Kim 等在文献[97]中考虑多个 Gold 指数的情况.

定理 58 p 为奇素数, 取 $I\subseteq\{1,2,\cdots,(n-1)/2\}$, $f:F_{p^n}\to F_p$ 定义为

$$f(x)=\sum_{i\in I}\mathrm{Tr}_1^n\left(x^{p^i+1}\right)$$

如果 $|I|$ 与 n 和 p 都互素, 则 $f(x)$ 是 Bent 函数.

Khoo 等在文章[98]中同样考虑多个 Gold 指数的情况.

定理 59 p,n 都为素数, $p\neq n$. 假设 $\mathrm{ord}_n(p)=n-1$, 则

$$f(x)=\sum_{i=1}^{(n-1)/2}c_i\mathrm{Tr}_1^n\left(x^{p^i+1}\right)$$

为 Bent 函数, 其中 $c_i\in F_p$.

而对于一般的二次型函数, Helleseth 和 Kholosha 给出了如下的 Bent 条件.

定理 60[94] 任何二次 p 值函数 $f(x):F_{p^n}\to F_p$ 是 Bent 的当且仅当与 $f(x)$ 所关联的二次型是非退化的. 进一步, 所有二次型 p 值 Bent 函数都是弱正则的.

当我们给定 $f(x)$ 的形式时, 可得到对应的函数为 Bent 函数的条件.

定理 61[98]

$$f(x)=\begin{cases}\displaystyle\sum_{i=1}^{(n-1)/2}c_i\mathrm{Tr}_1^n\left(x^{p^i+1}\right), & n\text{是奇数}\\ \displaystyle\sum_{i=1}^{n/2-1}c_i\mathrm{Tr}_1^n\left(x^{p^i+1}\right)+c_{n/2}\mathrm{Tr}_1^{n/2}\left(x^{p^{n/2}+1}\right), & n\text{是偶数}\end{cases}$$

$$c(x)=\begin{cases}\sum_{i=1}^{(n-1)/2} c_i\left(x^i+x^{n-i}\right), & n\text{是奇数}\\ \sum_{i=1}^{n/2-1} c_i\left(x^i+x^{n-i}\right)+c_{n/2}x^{n/2}, & n\text{是偶数}\end{cases}$$

其中 $x\in F_{p^n}$, $c_i\in F_p$, p 为奇素数. 则 $f(x)$ 是 Bent 函数当且仅当 $\gcd\left(c(x),x^n-1\right)=1$.

Li 等[99]考虑了上述形式的函数, 在 n 的多种取值条件下($n=p^vq^r$, $n=2p^vq^r$, $v\geqslant 0$, $r\geqslant 1$, q 是奇素数, p 是模 q^2 的本原根)研究函数的 Bent 条件, 并在大部分情况下给出 Bent 函数的计数结果.

2014 年文献[56]考虑了如下形式的二次型函数

$$g(x)=\sum_{i=0}^{\lfloor (n-1)/2\rfloor}\mathrm{Tr}_1^n\left(c_ix^{1+p^{ki}}\right)$$

$c_i\in F_p$, p 为奇素数.

定理 62 n,k 为正整数, p 是奇素数. 函数 $g(x)$ 如上式所定义, 则 $g(x)$ 是 p 值 Bent 函数当且仅当 $\gcd\left(c_p\left(x^k\right),x^n-1\right)=1$, $c_p(x)$ 定义如下

$$c_p(x)=\sum_{i=0}^{\lfloor (n-1)/2\rfloor}\left(c_ix^i+c_ix^{n-i}\right)\in F_p[x]$$

除了二次型的研究结果, 还有一些对其它情况的研究. Hou 在文献[82]确定了 F_p 上的 Bent 函数, 并且讨论了三值函数为弱正则 Bent 函数的条件.

定理 63 p 为奇素数, $f:F_p\to F_p$ 是 Bent 函数当且仅当 $\deg(f)=2$, 并且所有这些 Bent 函数都是弱正则的.

定理 64 $f:F_{3^n}\to F_3$, f 是一个弱正则 Bent 函数当且仅当 $v_3\left(\hat{f}(0)\right)=n/2$, $v_3\left(\hat{f}(c)-\hat{f}(0)\right)>n/2$ 对于所有的 $c\in F_3^n$ 都成立, 其中 v_3 表示求三进制下的阶.

2006 年, Helleseth 和 Kholosha 在文献[94]中考虑一类特殊的三值函数, 猜想其为弱正则 Bent 函数和其对应的对偶函数的形式.

猜想 1[94] $n=2k,k$ 为奇数. 三值函数 $f:F_{3^n}\to F_3$ 具有如下形式:

$$f(x)=\mathrm{Tr}_1^n\left(ax^{\frac{3^n-1}{4}+3^k+1}\right)$$

则当 $a=\zeta^{(3^k+1)/4}$, ζ 为 F_{3^n} 的本原元时, 函数 $f(x)$ 是弱正则 Bent 函数. 并且函数 $f(x)$ 在点 $\lambda\in F_{3^n}$ 处的 Walsh 谱谱值为

$$\hat{f}(\lambda)=-3^k\omega^{\pm\mathrm{Tr}_1^k\left(\frac{b^{3^k+1}}{a(I+1)}\right)}$$

其中 $\omega=e^{2\pi i/3}$, I 是 F_{3^n} 的 4 次本原单位根.

2009 年, Helleseth 等在文献[100]中解决上猜想 1 的前一部分, 即证明了在 $a=\zeta^{(3^k+1)/4}$ 的条件下, 猜想 1 中定义函数为弱正则 Bent 函数. 2012 年, Gong 等在文献[101]中解决了猜想 1 的后一部分, 并给出了对偶函数的精确形式.

定理 65[101] 定义 $c=\lambda^{3^k+1}/a_1\in F_{3^k}$, 其中 $a_1=a\left(\zeta^{(3^n-1)/4}+1\right)\in F_{3^k}^*$, $a=\zeta^{(3^k+1)/4}$, ζ 是 F_{3^n} 的本原元. $\gamma=\zeta^4$,

定义 $C_i=\left\{\zeta^i\gamma^j\,\middle|\,j=0,1,\cdots,\left(3^n-1\right)/4-1\right\}$, 其中 $i=0,1,2,3$. 则猜想 2 中定义函数 $f(x)$ 的对偶函数 g 满足 $g(0)=0$, 对于 $\lambda\neq 0$,

$$g(\lambda)=(-1)^s\,\mathrm{Tr}_1^k(c)\sum_{\substack{0\leqslant b\leqslant 3^n-2\\ W(b)=n}}\left(\sigma(b)c^b\right)^{-1}$$

其中当 $\lambda\in C_0\bigcup C_3$ 时, $s=0$, 否则 $s=1$.

$$W(b)=\mathrm{wt}(b)+\mathrm{wt}\left(-\left(3^k+1\right)b-\frac{3^n-1}{4}\right)$$
$$\mathrm{wt}(b)=b_0+b_1+\cdots+b_{n-1}$$
$$\sigma(b)=b_0!b_1!\cdots b_{n-1}!$$

其中 $b=b_0+b_1 3+\cdots+k_{n-1}3^{n-1}$.

2010 年, Helleseth 和 Kholosha 在文献[102]中考虑了一类特别的 p 值函数 $f:F_{p^{4k}}\to F_p$

$$f(x)=\mathrm{Tr}_1^{4k}\left(x^{p^{3k}+p^{2k}-p^k+1}+x^2\right)$$

定理 66 $n=4k$, $f:F_{p^n}\to F_p$ 如上式所定义, 则 f 为弱正则 Bent 函数. 并且对于 $b\in F_{p^n}$, $\hat{f}(b)=-p^{2k}\omega^{\mathrm{Tr}_1^k(x_0)/4}$, x_0 是下述多项式在 F_{p^k} 中唯一的根.

$$b^{p^{2k}+1}+\left(b^2+X\right)^{\frac{p^{2k}+1}{2}}+b^{p^k\left(p^{2k}+1\right)}+\left(b^2+X\right)^{\frac{p^k\left(p^{2k}+1\right)}{2}}$$

前面已经介绍了 Li 等在 2013 年文献[48]中关于 Bent 函数部分的工作, 同时文章中考虑了如下形式的两类 Dillon 指数型的 p 值 Bent 函数, 其中 p 为奇素数.

$$f(x)=\mathrm{Tr}_1^n\left(ax^{l(q-1)}+bx^{\left(\frac{q+1}{e}+l\right)(q-1)}+cx^{\left(\frac{q+1}{e}-l\right)(q-1)}\right)+\mathrm{Tr}_1^l\left(\epsilon x^{\frac{q^2-1}{e}}\right)$$

$$f(x)=\sum_{i\in D}\mathrm{Tr}_1^n\left(ax^{(ri+s)(q-1)}\right)+\mathrm{Tr}_1^l\left(\epsilon x^{\frac{q^2-1}{e}}\right)$$

其中 $n=2m$, $q=p^m$, $a,b,c\in F_{p^n}$, $\epsilon\in F_{p^l}$, $e\left|\left(p^m+1\right)\right.$, $\gcd\left(l,p^m+1\right)=1$, l 是最小的正整数满足 $l\left|n\right.$, $e\left|\left(p^l-1\right)\right.$, D 是集合 $\{0,1,\cdots,q-1\}$ 的子集.

除了本节所介绍的工作外, 其他的一些 p 值 Bent 函数相关研究工作可以参见[79,103–117]等文献.

6 向量值函数

本节我们考虑如下形式的向量值函数 $F:F_2^n\to F_2^m$, 简称为 (n,m)-函数. 首先给出 (n,m)-函数非线性度的定义.

定义 13 (n,m)-函数 F 的非线性度定义为

$$\mathrm{NL}(F)=\min_{\boldsymbol{v}\in\left(F_2^m\right)^*}NL\left(\boldsymbol{v}\cdot F(\boldsymbol{x})\right)$$

其中 $\left(F_2^m\right)^*=F_2^m\setminus\{0\}$, $\mathrm{NL}\left(\boldsymbol{v}\cdot F(x)\right)$ 表示 $\boldsymbol{v}\cdot F(\boldsymbol{x})$ 的非线性度.

从定义可以看出, (n,m)-函数 F 的非线性度是由 F 分量函数的所有非零线性组合与所有 n 元仿射函

数的 Hamming 距离的最小值来决定的.

为了更一步研究, 考虑 (n,m)-函数的扩展 Walsh 变换

$$\hat{F}(\boldsymbol{u},\boldsymbol{v})=\sum_{\boldsymbol{x}\in F_2^n}(-1)^{\boldsymbol{v}\cdot F(\boldsymbol{x})+\boldsymbol{u}\cdot\boldsymbol{x}}$$

其中 $\boldsymbol{v}\in\left(F_2^m\right)^*$, $\boldsymbol{u}\in F_2^n$. 根据函数非线性度和 Walsh 变换之间的关系, 可以得到

$$\mathrm{NL}(F)=2^{n-1}-\frac{1}{2}\max_{\boldsymbol{v}\in\left(F_2^m\right)^*,\boldsymbol{u}\in F_2^n}\left|\sum_{\boldsymbol{x}\in F_2^n}(-1)^{\boldsymbol{v}\cdot F(\boldsymbol{x})+\boldsymbol{u}\cdot\boldsymbol{x}}\right|$$

根据 Parseval 恒等式可得到, (n,m)-函数 F 的非线性度要满足限制 $\mathrm{NL}(F)\leqslant 2^{n-1}-2^{n/2-1}$.

定义 14 如果 (n,m)-函数 F 的非线性度 $\mathrm{NL}(F)=2^{n-1}-2^{n/2-1}$, 则称 F 为向量 Bent 函数, 或者 (n,m)-Bent 函数.

定理 67 一个 (n,m)-函数 F 是向量 Bent 函数当且仅当对任意 $\boldsymbol{v}\in\left(F_2^m\right)^*$, 布尔函数 $\boldsymbol{v}\cdot F$ 是 Bent 函数.

定理 68 一个 (n,m)-函数 F 是向量 Bent 函数当且仅当对任意非零的 $\boldsymbol{a}\in F_2^n$, 差分函数 $D_{\boldsymbol{a}}F(\boldsymbol{x})=F(\boldsymbol{x}+\boldsymbol{a})+F(\boldsymbol{x})$ 是平衡的.

从上述定理可以知道, (n,m)-Bent 函数与 $F_2^n\to F_2^m$ 的 PN 函数是一致的. 关于向量 Bent 函数的一些其他研究结果, 读者可以参见文献[15,118].

Nyberg 首先在文献[119]中研究 (n,m)-Bent 函数的存在性.

定理 69[119] 如果 (n,m)-函数 F 是向量 Bent 函数, 那么 $2\mid n$, 且 $m\leqslant n/2$.

通过上述定理可知, 当 $m>n/2$ 时, (n,m)-Bent 函数是不存在的. 当 $m\leqslant n/2$ 时, (n,m)-Bent 函数的存在性由以下构造证明.

定理 70[119] 设 n 为正偶数, $m\leqslant n/2$, $\varphi_1,\varphi_2,\cdots,\varphi_m$ 为从 $F_2^{n/2}$ 到 $F_2^{n/2}$ 的映射且满足对任意 $0\neq\boldsymbol{v}\in F_2^m$, $\sum_{i=1}^m v_i\varphi_i$ 均为 $F_2^{n/2}$ 上的置换, 构造如下的向量值函数

$$F(\boldsymbol{x},\boldsymbol{y})=\left(f_1(\boldsymbol{x},\boldsymbol{y}),f_2(\boldsymbol{x},\boldsymbol{y}),\cdots,f_m(\boldsymbol{x},\boldsymbol{y})\right)$$

其中 $f_i(\boldsymbol{x},\boldsymbol{y})=\boldsymbol{x}\cdot\varphi_i(\boldsymbol{y})+h_i(\boldsymbol{y})$, $\boldsymbol{x},\boldsymbol{y}\in F_2^{n/2}$, $h_i(\boldsymbol{y})$ 为 m 元布尔函数, $1\leqslant i\leqslant m$, 则 $F(\boldsymbol{x},\boldsymbol{y})$ 为 (n,m)-Bent 函数.

上述定理中的构造也是 Nyberg 在文献[119]中给出的, 其构造依赖于已有的 M-M 型 Bent 函数. 在 Nyberg 的工作之后, Satoh 等在文献[120]中同样考虑 M-M 型 Bent 函数, 通过给定置换的形式得到了一类新的 (n,m)-Bent 函数并且使得输出变量个数和代数次数同时达到最大, 即 $m=n/2$, $\deg(F)=n/2$.

定理 71[120] $n=2m$, $\boldsymbol{x}=(x_1,x_2,\cdots,x_m)$, $\boldsymbol{y}=(y_1,y_2,\cdots,y_m)$, α 是 F_{2^m} 的本原元. 考虑 $F(\boldsymbol{x},\boldsymbol{y})=(f_1,f_2,\cdots,f_m)$, 每个 f_i 的形式为 $f_i(\boldsymbol{x},\boldsymbol{y})=\varphi_i(\boldsymbol{y})\cdot\boldsymbol{x}+g_i(\boldsymbol{y})$, 其中

$$\varphi_i(\boldsymbol{y})\triangleq\begin{cases}0, & \boldsymbol{y}=(0,\cdots,0)\\ \alpha^{|\boldsymbol{y}|+i-1}, & \text{其他}\end{cases}$$

$|\boldsymbol{y}|=2^{m-1}y_1+2^{m-2}y_2+\cdots+y_m$ 表示 y 的十进制数值, g_i 是任意的 F_2^m 上的布尔函数. 则 $F(\boldsymbol{x},\boldsymbol{y})$ 为 (n,m)-Bent 函数, 并且 $\deg(F)=n/2$.

除了利用 M-M 型函数来构造向量 Bent 函数, Nyberg 也给出了基于 PS 类函数的 (n,m)-Bent 函数构造.

定理 72[119] f_i, $i=1,2,\cdots,m$, 都是 F_2^n 上由 Dillon 方法构造出的 Bent 函数. 函数 h_i 是 f_i 的赋值函数.

则函数

$$F(x)=\left(f_1(x),f_2(x),\cdots,f_m(x)\right)$$

是 (n,m)-Bent 函数当且仅当对任意非 0 的 $\boldsymbol{c}=(c_1,c_2,\cdots,c_m)\in F_2^m$, 函数 $c_1h_1+c_2h_2+\cdots+c_mh_m$ 是平衡的.

类似的, Dong 等在文献[121]中给出了从 F_{2^n} 到 $F_{2^{n/2}}$ 的一种基于 PS Bent 函数的向量 Bent 函数构造方法.

假设 $n=2m$, 空间 F_2^n 可以分为 2^m+1 个不相交的 m 维子空间 $E_0,E_1,\cdots,E_{2^m}$, 对应的指标函数分别为 $1_{E_0},1_{E_1},\cdots 1_{E_{2^m}}$. 记 S 为所有指标函数构成的集合, 从 S 中选取任意的 2^m+1 个指标函数然后重新排列为 $1_{U_0},1_{U_1},\cdots,1_{U_{2^m-2}}$. 记 $k=(k_0,k_1,\cdots,k_{m-1})$, 同时也使用记号 $k=\sum_{i=0}^{n-1}k_i2^i$, 则可得到如下定理.

定理 73[121] 函数 $F(x)=(f_0,f_1,\cdots,f_{m-1})$, 其中 $f_i(x)=\oplus_{k_i=0}1_{U_k}(x)$, $0\leqslant k\leqslant 2^m-2$, $0\leqslant i\leqslant m-1$, 是向量 Bent 函数, 并且 $\deg(F(x))=m$. 当 2^m+1 个不相交的 m 维子空间选定时, 定理所构造的 (n,m)-Bent 函数的个数为 $(2^m+1)!/2$.

除了基于已有的 M-M 和 PS Bent 函数类构造向量函数, 人们也研究了基于其他形式 Bent 函数的构造.

Pasalic 和 Zhang[122]考虑幂函数型 Bent 函数 $f(x)=\mathrm{Tr}_1^n(\alpha x^d)$, 研究当参数如何选取时能够使对应的函数 $F(x)=\mathrm{Tr}_m^n(\alpha x^d)$ 为向量 Bent 函数.

定理 74 $n\geqslant 4$, n 为偶数, $m|n$. x^d 是 F_{2^m} 上的置换, 但不是 F_{2^n} 上的置换. 如果 $f(x)=\mathrm{Tr}_1^n(\alpha x^d)$ 是 Bent 函数, 则函数 $F(x)=\mathrm{Tr}_m^n(\alpha x^d)$ 为向量 Bent 函数.

推论 11 $n=2m\geqslant 8$, $r\geqslant 3$ 为奇数, $k\geqslant 3$ 为奇数, $\gcd(r,n)=1$ 以及 $3\nmid n$. 则考虑 Kasami 指数 $d=2^{2r}-2^r+1$, 当 $\alpha\notin\{x^3:x\in F_{2^n}\}$ 时函数 $\mathrm{Tr}_m^n(\alpha x^d)$ 为向量 Bent 函数.

推论 12 $n=4r$, $r\geqslant 3$ 为奇数, $d=(2^r+1)^2$. 则对任意的 $\alpha\in F_{2^r}^*\setminus F_{2^2}$, 函数 $\mathrm{Tr}_r^n(\alpha x^d)$ 是向量 Bent 函数.

推论 13 $n=6r$, $r\geqslant 3$ 为奇数, $d=2^{2r}+2^r+1$. 则当 $\alpha\in F_{2^r}^*$, 且满足 $\mathrm{Tr}_r^{3r}(\alpha^3)=0$ 时, 函数 $\mathrm{Tr}_{2r}^{6r}(\alpha x^d)$ 与函数 $\mathrm{Tr}_r^{6r}(\alpha x^d)$ 都是向量 Bent 函数.

Dong 等在文献[121]给出了从 F_{2^n} 到 $F_{2^{n/2}}$ 的两种基于单项式 Bent 函数的向量 Bent 函数的构造方法.

定理 75 函数 $F(x)=\mathrm{Tr}_m^n(\alpha x^{2^r+1})$ 是一个向量 Bent 函数, 如果以下条件满足:

(1) 整数 r, $1\leqslant r\leqslant n-1$ 满足 $2|n/\gcd(r,n)$, $t|2^m+1$, 其中 $t=\gcd(2^r+1,2^n-1)\neq 1$;

(2) $\alpha\in F_{2^n}$, 满足 $\alpha\notin\{x^t,x\in F_{2^n}\}$.

下述定理是对推论 11 中 Kasami 指数结果的进一步推广.

定理 76 函数 $F(x)=\mathrm{Tr}_m^n(\alpha x^{2^{2r}-2^r+1})$ 是一个向量 Bent 函数如果以下条件满足:

(1) 整数 r, $1\leqslant r\leqslant n-1$ 满足 $\gcd(r,n)=1$, $t|2^m+1$, 其中 $t=\gcd(2^{2r}-2^r+1,2^n-1)\neq 1$;

(2) $\alpha\in F_{2^n}$, 满足 $\alpha\notin\{x^t,x\in F_{2^n}\}$.

Muratović-Ribić 等在文献[123]中证明了单项式 Dillon 指数 Bent 函数不能直接推广得到向量 Bent 函数.

定理 77 $n=2k$, $f(x)=\mathrm{Tr}_1^n(\lambda x^{2^k-1})$ 对于合适的 $\lambda\in F_{2^k}^*$ 是布尔 Bent 函数. 但函数 $F(x)=\mathrm{Tr}_k^n(\lambda x^{2^k-1})$ 不

可能是 F_{2^k} 上的向量 Bent 函数.

除了单项式情况下, Muratović-Ribić 在文献[123]还研究了多个 Niho 指数和的情况.

定理 78 $n\geqslant 4$, n 为偶数, $m|n$, $m\leqslant n/2$. x^{d_1} 是 F_{2^m} 上的置换, $f(x)=\mathrm{Tr}_1^n\left(\sum_{i=1}^{r}\lambda_i x^{d_i}\right)$ 是一个布尔 Bent 函数, 其中 $d_i=d_1+v_i\left(2^m-1\right)$, $i=2,\cdots,r$, $v_i\geqslant 0$ 为整数, $m|n/2$. 则函数 $F(x)=\mathrm{Tr}_m^n\left(\sum_{i=1}^{r}\lambda_i x^{d_i}\right)$ 是向量 Bent 函数. 特别的, 当 $m=n/2$ 时, 此时函数输出空间的维数达到最大.

文中同时给出了一类函数为向量 Bent 函数的三个等价条件.

定理 79 $n=2k$, $F(x)=\mathrm{Tr}_k^n\left(P(x)\right)$, 其中 $P(x)=\sum_{i=1}^{t}a_i x^{r_i\left(2^k-1\right)}$. 下面的条件等价:

(1) F 是维度为 k 的向量 Bent 函数;

(2) $\sum_{u\in U}(-1)^{\mathrm{Tr}_1^k(\lambda F(u))}=1$ 对于任意的 $\lambda\in K^*$;

(3) 有两个 $u\in U$ 使得 $F(u)=0$, 进一步如果有 $F(u_0)=0$, 则 F 是从 $U_0=U\setminus u_0$ 到 K 的一一映射;

(4) 初等对称多项式 σ_e, 是 $\prod_{u\in U}\left(x-F(u)\right)$ 展开式的系数, 对于任意奇数 e, $1\leqslant e\leqslant 2^k+1$, 满足 $\sigma_{2^k-1}=1$, 其他值 $\sigma_e=0$.

特别的, 本文利用线性化多项式的性质, 给出了一类特殊形式的向量 Bent 函数.

推论 14[123] 如果 $\mathrm{Tr}_1^n\left(\lambda_1 x^{d_1}\right)$ 是 Bent 函数, 则 $\mathrm{Tr}_1^n\left(\lambda_1 x^{d_1}+\lambda_2 x^{2^j}\right)$ 也是 Bent 函数, 对于任意的 $\lambda_2\in L$, $j\in Z$. 特别的, 如果 x^{d_1} 是 F_{2^k} 上的置换, 存在 $j,v>0$ 使得 $2^j=d_1+v\left(2^{n/2}-1\right)$, 则 $\mathrm{Tr}_k^n\left(\lambda_1 x^{d_1}+\lambda_2 x^{2^j}\right)$ 是向量 Bent 函数.

除此之外, 更多的关于向量值 Bent 函数的研究结果可以参见文献[124–127]等.

7 超 Bent 函数

超 Bent 函数在 2001 年由 Youssef 和 Gong 在文献[128]中正式提出, 但其思想在文献[129]中已有体现. 当我们研究 Bent 函数的时候, 要求函数与所有仿射函数的距离尽量小. 但在有限域 F_{2^n} 上考虑此问题的时候, 我们会进一步要求所使用的密码函数不能够被一个双射的单项式函数来近似. 因为对于一般的单项式函数 $\mathrm{Tr}(\zeta_j x^c)$, 当满足 $\gcd\left(c,2^n-1\right)=1$ 时, 其与函数 $\mathrm{Tr}(\lambda x)$ 都是 m 序列并且具有相同的线性复杂度, 所以应进一步考虑函数与所有双射单项式函数的距离.

定义 15 f 是从 F_{2^n} 到 F_2 的函数, 定义

$$\hat{f}(\lambda,c)=\sum_{x\in F_{2^n}}(-1)^{f(x)+\mathrm{Tr}\left(\lambda x^c\right)}$$

其中 $\lambda\in F_{2^n}$, c 是与 2^n-1 互素的模 2^n-1 的陪集首. 称 $\hat{f}(\lambda,c)$ 为函数 f 的扩展变换.

此类情况下函数非线性度定义为

$$\mathrm{NLG}(f)=2^{n-1}-\frac{1}{2}\max_{\substack{\lambda\in F_{2^n}\\ c:\gcd\left(c,2^n-1\right)=1}}\left|\hat{f}(\lambda,c)\right|$$

定义 16 $f:F_{2^n}\to F_2$, $n=2k$ 是超 Bent 函数当且仅当 $\mathrm{NLG}(f)=2^{n-1}-2^{k-1}$.

定理 80 $f:F_{2^n}\to F_2$, $n=2k$ 是超 Bent 函数当且仅当对所有的 $\lambda\in F_{2^n}$ 和所有的 c, $\gcd\left(c,2^n-1\right)=1$ 都有:

$$\hat{f}(\lambda,c)=\sum_{x\in F_{2^n}}(-1)^{f(x)+\mathrm{Tr}(\lambda x^c)}=\pm 2^k$$

根据 Bent 函数与超 Bent 函数的关系, 可以得到 f 是超 Bent 函数当且仅当对于所有的 c, $\gcd(c,2^n-1)=1$, $f(x^c)$ 是 Bent 函数.

Youssef 和 Gong 率先给出超 Bent 函数的一个构造方法.

定理 81[128] $n=2m$, α 是 F_{2^n} 的本原元. f 是定义在 F_{2^n} 上的函数且对所有的 $x\in F_{2^n}$ 都有 $f(\alpha^{2^m+1}x)=f(x)$ 且 $f(0)=0$. 则 f 是超 Bent 函数当且仅当向量 $(f(1),f(\alpha),\cdots,f(\alpha^{2^m}))$ 的 Hamming 重量为 2^{m-1}. 此时 F 的代数次数为 m.

注 8 上述定理可以得到 $\binom{2^k+1}{2^{k-1}}$ 个超 Bent 函数, 再考虑到补函数的话, 共可得到 $2\binom{2^k+1}{2^{k-1}}$ 个超 Bent 函数.

其后, Carlet 和 Gaborit 在文献[130]对超 Bent 函数进行了深入的研究, 考虑超 Bent 函数与循环码之间的关系, 在文章中给出一些很有用的结果:

定理 82 所有 n 元超 Bent 函数代数次数都为 $n/2$. 所有 $\mathrm{PS}_{\mathrm{ap}}$ 函数都是超 Bent 的.

在文中, Carlet 等还定义了一个函数类 $\mathrm{PS}_{\mathrm{ap}}^{\#}$, 它是由 $\mathrm{PS}_{\mathrm{ap}}$ 函数通过变换 $x\to\delta x$ ($\delta\in F_{2^n}^*$)以及添加常函数得到的函数类, 显然 $\mathrm{PS}_{\mathrm{ap}}\subseteq\mathrm{PS}_{\mathrm{ap}}^{\#}$. 并且 Carlet 等证明了, 在 n 的某些特殊取值(如 $n=4$)下存在的超 Bent 函数一定属于 $\mathrm{PS}_{\mathrm{ap}}^{\#}$ 类.

定理 83 定理 81 中构造的函数如果满足 $f(1)=0$ 则属于 $\mathrm{PS}_{\mathrm{ap}}$ 类. 满足 $f(1)=1$ 则属于 $\mathrm{PS}_{\mathrm{ap}}^{\#}$, 并且函数的形式为 $f(x)=g(\delta x)$, 其中 $g\in\mathrm{PS}_{\mathrm{ap}}$, $\delta\in F_{2^n}^*$, 且 $g(\delta)=1$.

2008 年, Charpin 和 Gong 在文献[131]研究了具有如下形式函数的超 Bent 性质

$$f(x)=\sum_{r\in R}\mathrm{Tr}_1^n\left(a_r x^{r(2^m-1)}\right)$$

其中 $n=2m$, R 是 r 模 2^m+1 所得的大小为 n 的分圆类, $a_r\in F_{2^m}$. $\gcd(r,2^m+1)=1$. 先给出单项式情况的结果.

定理 84[131] $n=2m$, $a\in F_{2^m}^*$, $\gcd(r,2^m+1)=1$, $f_a^{(r)}(x)=\mathrm{Tr}_1^n\left(ax^{r(2^m-1)}\right)$. 则 $f_a^{(r)}$ 是超 Bent 函数当且仅当 $f_a^{(r)}$ 是 Bent 函数, 当且仅当 $f_a^{(1)}$ 是 Bent 函数, 当且仅当 $K_m(\alpha)=0$.

文章还研究了多项式的情况. 为了给出下面的结果, 我们首先介绍 Dickson 多项式.

定义 17 对于 $r>0$, Dickson 多项式定义为

$$D_r(x)=\sum_{i=0}^{\lfloor r/2\rfloor}\frac{r}{r-i}\binom{r-i}{i}x^{r-2i},r=2,3,\cdots$$

除了定义式, Dickson 多项式满足递归公式: $D_{i+2}(x)=xD_{i+1}(x)+D_i(x)$, 初始值为 $D_0(x)=0$, $D_1(x)=x$.

Dickson 多项式有如下性质:

(1) $\deg(D_r(x))=r$;

(2) $D_{2r}(x)=(D_r(x))^2$;

(3) $D_{rp}(x)=D_r(D_p(x))$;

(4) $D_r\left(x+x^{-1}\right)=x^r+x^{-r}$.

定理 85[131] $n=2m$, 定义在 F_{2^n} 上的函数 $f(x)=\sum_{r\in R}\mathrm{Tr}_1^n\left(a_r x^{r\left(2^m-1\right)}\right)$, 定义在 F_{2^m} 上的函数 $g(x)=\sum_{r\in R}\mathrm{Tr}_1^m\left(a_r D_r(x)\right)$, 其中 $a_r\in F_{2^m}$, $D_r(x)$ 是次数为 r 的 Dickson 多项式. 则 $f(x)$ 是超 Bent 函数当且仅当 $\sum_{x\in F_{2^m}}\chi\left(\mathrm{Tr}_1^m\left(x^{-1}\right)+g(x)\right)=2^m-2\mathrm{wt}(g)$.

随后, 有很多学者研究双项式形式. Mesnager 考虑了如下形式的函数.

定理 86[132] $n=2m$, m 为奇数且 $m>3$, $\gcd\left(r,2^m+1\right)=1$. $a\in F_{2^m}^*$ 且 $b\in F_4^*$. 定义在 F_{2^n} 上的函数 $f_{a,b}^{(r)}$ 形式为

$$f_{a,b}^{(r)}(x)=\mathrm{Tr}_1^n\left(ax^{r\left(2^m-1\right)}\right)+\mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right)$$

则 $f_{a,b}^{(r)}$ 是超 Bent 函数当且仅当 $f_{a,b}^{(r)}$ 是 Bent 函数, 当且仅当 $f_{a,b}^{(1)}$ 是 Bent 函数, 当且仅当 $K_m(a)=4$.

在文献[47]中, Mesnager 研究了 $r=3$ 的特殊情况.

定理 87 $n=2m$, m 为奇数. $a\in F_{2^m}^*$ 且 $b\in F_4^*$, β 是 F_4 的本原元, U 表示 $F_{2^n}^*$ 的阶为 2^m+1 的循环子群. ζ 为 U 的生成元. 定义在 F_{2^n} 上的函数 $g_{a,b}$ 形式为

$$g_{a,b}(x)=\mathrm{Tr}_1^n\left(ax^{3\left(2^m-1\right)}\right)+\mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right)$$

则 $g_{a,b}$ 是超 Bent 函数当且仅当 $g_{a,b}$ 是 Bent 的.

在文献[133]中, Tang 等考虑了另一种形式的二项式情况.

$n=2m$, $m\equiv 2 \bmod 4$, $a\in F_{2^m}$, $b\in F_{16}$,

$$f_{a,b}(x)=\mathrm{Tr}_1^n\left(ax^{2^m-1}\right)+\mathrm{Tr}_1^4\left(bx^{\frac{2^n-1}{5}}\right)$$

文章考虑了 $b=1$ 以及 $\mathrm{Tr}_1^4(b)=0$, 即 $b^4+b+1=0$ 两种情形, 得到了如下结果.

定理 88[133] $n=2m$, $m=2m_1$, $m_1=1 \bmod 2$, $m_1\geqslant 3$. 函数

$$f_{a,1}=\mathrm{Tr}_1^n\left(ax^{2^m-1}\right)+\mathrm{Tr}_1^4\left(x^{\frac{2^n-1}{5}}\right)$$

是超 Bent 函数当且仅当下面的条件成立.

(1) $p(x)=x^5+x+a^{-1}$ 在 F_{2^m} 上是不可约的;

(2) 二次型 $q(x)=\mathrm{Tr}_1^m\left(x\left(ax^4+ax^2+a^2x\right)\right)$ 是偶的, 即集合 $\left\{i\middle|q\left(e_i\right)=q\left(e_{m_1+i}\right)=1,1\leqslant i\leqslant m_1\right\}$ 元素个数为偶数个;

(3) $K_m(a)=4\left(2-2^{m_1}\right)/3$.

定理 89[133] $n=2m$, $m=2m_1$, $m_1=1 \bmod 2$, $m_1\geqslant 3$. b 是 F_{16}^* 的本原元并且满足 $\mathrm{Tr}_1^4(b)=0$. 函数

$$f_{a,b}=\mathrm{Tr}_1^n\left(ax^{2^m-1}\right)+\mathrm{Tr}_1^4\left(bx^{\frac{2^n-1}{5}}\right)$$

是超 Bent 函数当且仅当下面任意一个条件成立.

(1) $p(x)=x^5+x+a^{-1}$ 在 F_{2^m} 上的分解形式为 $(1)(2)^2$,即分解为一个一次不可约多项式和两个二次不可约多项式的乘积, 以及 $K_m(a)=-4$;

(2) $p(x)=x^5+x+a^{-1}$ 在 F_{2^m} 上是不可约的. 二次型 $q(x)=\mathrm{Tr}_1^m\left(x\left(ax^4+ax^2+a^2x\right)\right)$ 是偶的. $K_m(a)=2\cdot 2^{m_1}-4$.

随后 Mesnager 和 Flori 在文献[134]中首先对 Charpin 和 Gong 研究的函数的条件作了弱化, 其次将上述的二项式的结果作了推广, 研究更一般的情形

$$f(x)=\sum_{r\in R}\mathrm{Tr}_1^n\left(a_r x^{r\left(2^m-1\right)}\right)+\mathrm{Tr}_1^t\left(bx^{s\left(2^m-1\right)}\right)$$

其中 $t=o\left(s\left(2^m-1\right)\right)$, 为 s 模 2^m+1 所得分圆陪集的大小. 最后文章提出一个算法来产生此类超 Bent 函数.

在二项式的基础上, 人们将二项式的结果推广到多项. Mesnager 在文献[135]中有如下结论

定理 90 $n=2m$, m 为奇数. $a_r\in F_{2^m}$, $b\in F_4^*$, β 是 F_4 的本原元, 定义在 F_{2^n} 上的函数

$$f_{a_r,b}(x)=\sum_{r\in R}\mathrm{Tr}_1^n\left(a_r x^{r\left(2^m-1\right)}\right)+\mathrm{Tr}_1^2\left(bx^{\frac{2^n-1}{3}}\right)$$

$g_{a_r}(x)$ 是对应的定义在 F_{2^m} 上的函数

$$g_{a_r}(x)=\sum_{r\in R}\mathrm{Tr}_1^m\left(a_r D_r(x)\right)$$

则可得到下述性质

(1) $f_{a_r,b}$ 是超 Bent 函数当且仅当 $f_{a_r,b}$ 是 Bent 的;

(2) 如果 $f_{a_r,b}$ 是 Bent, 则它属于类 PS^-, 如果进一步有 $b=1(b\neq 1)$, 则它属于 $\mathrm{PS}_{\mathrm{ap}}\left(\mathrm{PS}_{\mathrm{ap}}^{\#}\right)$;

(3) 下面三个断言是等价的:

(a) $f_{a_r,b}$ 是超 Bent 函数;

(b) $\sum_{x\in F_{2^m}^*,\mathrm{Tr}_1^m\left(x^{-1}\right)=1}\chi\left(g_{a_r}\left(D_3(x)\right)\right)=-2$;

(c) $\sum_{x\in F_{2^m}^*}\chi\left(\mathrm{Tr}_1^m\left(x^{-1}\right)+g_{a_r}\left(D_3(x)\right)\right)=2^m-2\mathrm{wt}\left(g_{a_r}\circ D_3\right)+4$;

(4) $f_{a_r,1}$ 是超 Bent 函数当且仅当

$$2\sum_{x\in F_{2^m}^*,\mathrm{Tr}_1^m\left(x^{-1}\right)=1}\chi\left(g_{a_r}\left(D_3(x)\right)\right)-3\sum_{x\in F_{2^m}^*,\mathrm{Tr}_1^m\left(x^{-1}\right)=1}\chi\left(g_{a_r}(x)\right)=2$$

文献[136]中也将之前二项式的研究结果推广得到多项式情况, 考虑 $b=1$ 以及 $\mathrm{Tr}_1^4(b)=0$ 两种情形.

$n=2m$, $m\equiv 2\bmod 4$, $a_r\in F_{2^m}$, $b\in F_{16}$, R 是 r 模 2^m+1 所得的分圆类

$$f_{a_r,b}(x)=\sum_{r\in R}\mathrm{Tr}_1^n\left(a_r x^{r\left(2^m-1\right)}\right)+\mathrm{Tr}_1^4\left(bx^{\frac{2^n-1}{5}}\right)$$

定理 91[136] $n=2m$, $m\equiv 2\bmod 4$. b 是 F_{16} 的本原元并且满足 $\mathrm{Tr}_1^4(b)=0$, 即 $b^4+b+1=0$. 定义在 F_{2^n} 上的函数为

$$f_{a_r,b}(x)=\sum_{r\in R}\mathrm{Tr}_1^n\left(a_r x^{r\left(2^m-1\right)}\right)+\mathrm{Tr}_1^4\left(bx^{\frac{2^n-1}{5}}\right)$$

定义 F_{2^m} 上的函数 $g_{a_r}(x)=\sum_{r\in R}\mathrm{Tr}_1^m\left(a_rD_r(x)\right)$. 则下面的条件等价.

(1) $f_{a_r,b}$ 是超 Bent 函数;

(2) $\sum_{x\in F_{2^m}^*,\mathrm{Tr}_1^m\left(x^{-1}\right)=1}\chi\left(g_{a_r}\left(D_5(x)\right)\right)=2$;

(3) $\mathrm{wt}\left(\mathrm{Tr}_1^m\left(x^{-1}\right)+g_{a_r}\left(D_5(x)\right)\right)-\mathrm{wt}\left(g_{a_r}\left(D_5(x)\right)\right)=2$.

定理 92[136] $n=2m$, $m\equiv 2\bmod 4$. 定义在 F_{2^n} 上的函数为

$$f_{a_r,1}(x)=\sum_{r\in R}\mathrm{Tr}_1^n\left(a_rx^{r\left(2^m-1\right)}\right)+\mathrm{Tr}_1^4\left(x^{\frac{2^n-1}{5}}\right)$$

定义 F_{2^m} 上的函数 $g_{a_r}(x)=\sum_{r\in R}\mathrm{Tr}_1^m\left(a_rD_r(x)\right)$. 则下面的条件等价.

(1) $f_{a_r,1}$ 是超 Bent 函数;

(2) $2\sum_{x\in F_{2^m}^*,\mathrm{Tr}_1^m\left(x^{-1}\right)=1}\chi\left(g_{a_r}\left(D_5(x)\right)\right)-5\sum_{x\in F_{2^m}^*,\mathrm{Tr}_1^m\left(x^{-1}\right)=1}\chi\left(g_{a_r}(x)\right)=4$;

(3) $2\mathrm{wt}\left(\mathrm{Tr}_1^m\left(x^{-1}\right)+g_{a_r}\left(D_5(x)\right)\right)-2\mathrm{wt}\left(g_{a_r}\left(D_5(x)\right)\right)+5\mathrm{wt}\left(g_{a_r}(x)\right)-5\mathrm{wt}\left(\mathrm{Tr}_1^m\left(x^{-1}\right)+g_{a_r}(x)\right)=4$

在这些研究之外, Mesnager 在文献[137]中对已有的工作进行了总结, 并提出了两个猜想, 并根据这两个猜想分别构造了两类超 Bent 函数

定义 18 $I:=\left\{x\in F_{2^m}^*\,\middle|\,x=c^3+c,\mathrm{Tr}_1^m\left(c^{-1}\right)=1\right\}$, 对于 $a,a'\in F_{2^m}$,

$$S(a,a')=\sum_{x\in I}(-1)^{\mathrm{Tr}_1^m\left(a\left(x+x^3\right)+a'x^5\right)}$$

猜想 2 对于 $a\in F_{2^m}^*$, 集合 $\Gamma_a=\left\{a'\in F_{2^m}^*\,\middle|\,S(a,a')=-1\right\}$ 非空.

定理 93 $n=2m$, m 为奇数. 假设猜想 2 成立, $a\in F_{2^m}^*$, $a'\in\Gamma_a(\neq\varnothing)$, β 是 F_4 的本原元. 定义在 F_{2^n} 上的函数

$$f(x)=\mathrm{Tr}_1^n\left(\left(a+a'\right)x^{3\left(2^m-1\right)}\right)+\mathrm{Tr}_1^n\left(a'x^{5\left(2^m-1\right)}\right)+\mathrm{Tr}_1^2\left(\beta x^{\frac{2^n-1}{3}}\right)$$

是超 Bent 函数.

定义 19 对于 $(a,a')\in F_{2^m}^*$, 以及 $a''\in F_{2^m}$,

$$S'(a,a',a'')=\sum_{x\in I}(-1)^{\mathrm{Tr}_1^m\left(ax+a'x^3+a''x^5\right)}$$

猜想 3 集合 $\Gamma'=\left\{(a,a',a'')\in F_{2^m}^*\times F_{2^m}^*\times F_{2^m}\,\middle|\,S'(a,a',a'')=-1\right\}$ 非空.

定理 94 $n=2m$, m 为奇数. 假设猜想 3 成立, $(a,a',a'')\in\Gamma'(\neq\varnothing)$, β 是 F_4 的本原元. 定义在 F_{2^n} 上的函数

$$f(x)=\mathrm{Tr}_1^n\left(\left(a+a'\right)x^{2^m-1}\right)+\mathrm{Tr}_1^n\left(\left(a'+a''\right)x^{3\left(2^m-1\right)}\right)+\mathrm{Tr}_1^n\left(a''x^{5\left(2^m-1\right)}\right)+\mathrm{Tr}_1^2\left(\beta x^{\frac{2^n-1}{3}}\right)$$

是超 Bent 函数.

7.1 向量超Bent函数

下面考虑向量超 Bent 函数, Youssef 和 Gong 在 2001 年文献[128]中给出了一类构造.

α 是 F_{2^n} 的本原元, $d=2^k+1$, 令 $\gamma=\alpha^d$, 则 γ 是 F_{2^k} 的本原元. 取 $\{\beta_0,\beta_1,\cdots,\beta_{k-1}\}$ 是 $\left\{1,\gamma,\cdots,\gamma^{k-1}\right\}$ 的对

偶基. π 是 F_{2^k} 上的置换. 定义

$$b_{i,j}^{\pi}=\begin{cases}\mathrm{Tr}\left(\beta_j\pi\left(\gamma^i\right)\right), & 0\leqslant i\leqslant 2^k-2\\ \mathrm{Tr}\left(\beta_j\pi\left(0\right)\right), & i=2^k-1\\ 0, & i=2^k\end{cases}$$

记 $\underline{\boldsymbol{b}}_j^{\pi}=\left(b_{i,j}^{\pi}\right)_{i\geqslant 0}$, 其中 $b_{i,j}^{\pi}=b_{s,j}^{\pi}$ 对于 $i=kd+s,\ 0\leqslant s<d$. 通过构造容易得到 $\mathrm{Per}\left(\underline{\boldsymbol{b}}_j^{\pi}\right)=d$.

定理 95[128] 记号如上所述. Π 是 F_{2^k} 上所有置换构成的集合,

$$P=\left\{h(x):F_{2^n}\to F_{2^k}\left|h(x)=\sum_{j=0}^{k-1}h_j(x)\gamma^j,h_j(x)\leftrightarrow\underline{\boldsymbol{b}}_j^{\pi},\pi\in\Pi\right.\right\}$$

则任意函数 $h\in P$ 都是向量超 Bent 函数, 同时具有有 $|P|=2^n!$.

在 2014 年, Muratović-Ribić 等在文献[138]中基于已有的向量 Bent 函数的等价条件得到了向量超 Bent 函数的等价条件.

定理 96[138] 如果 $F(x)=\mathrm{Tr}_k^n\left(\sum_{i=1}^{t}a_ix^{i\left(2^k-1\right)}\right)$ 是向量 Bent 函数, 则对任意 j, 只要 $\gcd\left(j,2^n-1\right)=1$, $F\left(x^j\right)$ 是向量 Bent 函数, 也就是说 $F(x)$ 是向量超 Bent 函数.

除此之外, 关于超 Bent 函数以及向量超 Bent 函数的其他相关研究可以参见文献[139]等.

8 总结

本文从密码函数的非线性度说起, 简单的介绍了各种形式下的 Bent 函数的构造情况, 其中包括布尔 Bent 函数、广义 Bent 函数、p 值 Bent 函数、向量 Bent 函数和超 Bent 函数. 而关于 Bent 函数的研究并不仅限于此, 其它方面的研究也很多, 比如 Bent 函数的其它推广: 考虑函数的高阶非线性度或者是考虑对 Bent 函数的修改使之适用于密码系统等方面也都有大量的研究工作. 总结来说, Bent 函数作为一个在密码、编码和组合数学等多个领域都有重要应用的组件, 仍然存在大量的问题等待人们的进一步研究.

References

[1] Massey J L. Shift-register synthesis and BCH decoding[J]. IEEE Transactions on Information Theory, 1969, 15(1): 122–127.

[2] Siegenthaler T. Decrypting a class of stream ciphers using ciphertext only[J]. IEEE Transactions on Computers, 1985, 100(1): 81–85

[3] Meier W, Staffelbach O. Fast correlation attacks on stream ciphers[C]. In: Advances in Cryptology—EUROCRYPT '88. Springer Berlin Heidelberg, 1988: 301–314.

[4] Courtois N T, Meier W. Algebraic attacks on stream ciphers with linear feedback[C]. In: Advances in Cryptology—EUROCRYPT 2003. Springer Berlin Heidelberg, 2003: 345–359.

[5] Courtois N T. Fast algebraic attacks on stream ciphers with linear feedback[C]. In: Advances in Cryptology—CRYPTO 2003. Springer Berlin Heidelberg, 2003: 176–194.

[6] Meier W, Staffelbach O. Nonlinearity criteria for cryptographic functions[C]. In: Advances in Cryptology—EUROCRYPT '89. Springer Berlin Heidelberg, 1990: 549–562.

[7] Matsui M. Linear cryptanalysis method for DES cipher[C]. In: Advances in Cryptology—EUROCRYPT '93. Springer Berlin Heidelberg, 1994: 386–397.

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

[9] Dillon J F. Elementary Hadamard difference sets[D]. University of Maryland, 1974.

[10] Schmidt K. Quaternary constant-amplitude codes for multicode CDMA[J]. IEEE Transactions on Information Theory, 2009, 55(4): 1824–1832.

[11] Xiao G Z, Massey J L. A spectral characterization of correlation-immune combining functions[J]. IEEE Transactions on Information Theory, 1988, 34(3): 569–571.

[12] 冯登国, 裴定一. 密码学导引[M]. 科学出版社, 1999.
[13] 丁存生, 肖国镇. 流密码学及其应用[M]. 国防工业出版社, 1994.
[14] Carlet C. Boolean functions for cryptography and error correcting codes[J]. Boolean Models and Methods in Mathematics, Computer Science, and Engineering, 2010, 134: 257.
[15] 李超, 屈龙江, 周悦. 密码函数的安全性指标分析[M]. 科学出版社, 2011.
[16] McFarland R L. A family of difference sets in non-cyclic groups[J]. Journal of Combinatorial Theory, Series A, 1973, 15(1): 1–10.
[17] Carlet C, Guillot P. A characterization of binary Bent functions[J]. Journal of Combinatorial Theory, Series A, 1996, 76(2): 328–335.
[18] Dobbertin H. Construction of Bent functions and balanced Boolean functions with high nonlinearity[C]. In: Fast Software Encryption. Springer Berlin Heidelberg, 1995: 61–74.
[19] Dillon J F, McGuire G. Near Bent functions on a hyperplane[J]. Finite Fields and Their Applications, 2008, 14(3): 715–720.
[20] Carlet C, Charpin P, Zinoviev V. Codes, Bent functions and permutations suitable for DES-like cryptosystems[J]. Designs, Codes and Cryptography, 1998, 15(2): 125–156.
[21] Leander G, McGuire G. Construction of Bent functions from near-Bent functions[J]. Journal of Combinatorial Theory, Series A, 2009, 116(4): 960–970.
[22] Carlet C. A construction of Bent function[C]. In: Proceedings of the 3rd International Conference on Finite Fields and Applications. Cambridge University Press, 1996: 47–58.
[23] Carlet C. On the secondary constructions of resilient and Bent functions[M]. In: Coding, Cryptography and Combinatorics. Birkhäuser Basel, 2004: 3–28.
[24] Carlet C, Dobbertin H, Leander G. Normal extensions of Bent functions[J]. IEEE Transactions on Information Theory, 2004, 50(11): 2880–2885.
[25] Charpin P, Pasalic E, Tavernier C. On Bent and Semi-Bent quadratic Boolean functions[J]. IEEE Transactions on Information Theory, 2005, 51(12): 4286–4298.
[26] Carlet C. Two new classes of Bent functions[C]. In: Advances in cryptology—EUROCRYPT '93. Springer Berlin Heidelberg, 1994: 77–101.
[27] Canteaut A, Daum M, Dobbertin H, et al. Normal and non normal Bent functions[C]. In: Workshop on Coding and Cryptography. 2003, 3: 91–100.
[28] Hou X D, Langevin P. Results on Bent functions[J]. Journal of Combinatorial Theory, Series A, 1997, 80: 232–246.
[29] Hou X D. New constructions of Bent functions[J]. J. Combin. Inform. System Sci, 2000, 25(1–4): 173–189.
[30] Carlet C. On Bent and highly nonlinear balanced/resilient functions and their algebraic immunities[C]. In: Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. Springer Berlin Heidelberg, 2006: 1–28.
[31] Mesnager S. Several new infinite families of Bent functions and their duals[J]. IEEE Transactions on Information Theory, 2014,60(7): 4397–4407.
[32] Langevin P, Leander G. Monomial Bent functions and Stickelberger's theorem[J]. Finite Fields and Their Applications, 2008, 14(3): 727–742.
[33] Dillon J F, Dobbertin H. New cyclic difference sets with Singer parameters[J]. Finite Fields and Their Applications, 2004, 10(3): 342–389.
[34] Leander N G. Monomial Bent functions[J]. IEEE Transactions on Information Theory, 2006, 52(2): 738–743.
[35] Charpin P, Kyureghyan G M. Cubic monomial Bent functions: a subclass of M[J]. SIAM Journal on Discrete Mathematics, 2008, 22(2): 650–665.
[36] Canteaut A, Charpin P, Kyureghyan G M. A new class of monomial Bent functions[J]. Finite Fields and Their Applications, 2008, 14(1): 221–241.
[37] Dobbertin H, Leander G, Canteaut A, et al. Construction of Bent functions via Niho power functions[J]. Journal of Combinatorial Theory, Series A, 2006, 113(5): 779–798.
[38] Leander G, Kholosha A. Bent functions with 2^r Niho exponents[J]. IEEE Transactions on Information Theory, 2006, 52(12): 5529–5532.
[39] Budaghyan L, Carlet C, Helleseth T, et al. Further results on Niho Bent functions[J]. IEEE Transactions on Information Theory, 2012, 58(11): 6979–6985.
[40] Carlet C, Mesnager S. On Dillon□s class H of Bent functions, Niho Bent functions and o-polynomials[J]. Journal of Combinatorial Theory, Series A, 2011, 118(8): 2392–2410.
[41] Vis T L. Monomial hyperovals in Desarguesian planes[D]. University of Colorado Denver, 2010.
[42] Cherowitzo W E, Storme L. α-flocks with oval herds and monomial hyperovals[J]. Finite fields and their Applications, 1998, 4(2): 185–199.
[43] Cherowitzo W, Penttila T, Pinneri I, et al. Flocks and ovals[J]. Geometriae Dedicata, 1996, 60(1): 17–37.

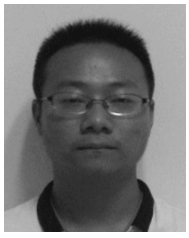
[44] Cherowitzo W E, O'Keefe C M, Penttila T. A unified construction of finite geometries associated with q-clans in characteristic 2[J]. Advances in Geometry, 2003, 3(1): 1–21.
[45] Budaghyan L, Kholosha A, Carlet C, et al. Univariate Niho Bent Functions from o-Polynomials[J]. arXiv preprint arXiv: 1411.2394, 2014.
[46] Mesnager S. A new class of Bent functions in Polynomial Forms[J]. IACR Cryptology ePrint Archive, 2008, 2008: 512.
[47] Mesnager S. A new family of hyper-Bent Boolean functions in polynomial form[C]. In: Cryptography and Coding. Springer Berlin Heidelberg, 2009: 402–417.
[48] Li N, Helleseth T, Tang X, et al. Several New Classes of Bent Functions From Dillon Exponents[J]. IEEE Transactions on Information Theory, 2013, 59(3): 1818–1831.
[49] Helleseth T, Kumer P V. Sequences with low correlation[M]. In: Handbook of Coding Theory, Pless V S and Huffman W C, Eds. Amsterdam, The Netherlands: North-Holland, 1998, vol.II, 1765–1853.
[50] Yu N Y, Gong G. Constructions of quadratic Bent functions in polynomial forms[J]. IEEE Transactions on Information Theory, 2006, 52(7): 3291–3299
[51] Ma W, MoonHo L, Zhang F. A new class of Bent functions[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2005, 88(7): 2039–2040.
[52] Hu H, Feng D. On quadratic Bent functions in polynomial forms[J]. IEEE Transactions on Information Theory, 2007, 53(7): 2610–2615.
[53] Udaya P. Polyphase and frequency hopping sequences obtained from finite rings[D]. Indian Inst. Technol., Kanpur, India, Ph. D. dissertation, 1992.
[54] Kim S H, No J S. New families of binary sequences with low correlation[J]. IEEE Transactions on Information Theory, 2003, 49(11): 3059–3065.
[55] Wu B, Zheng J, Liu Z. New classes of quadratic Bent functions in polynomial forms[J]. arXiv preprint arXiv:1305.3700, 2013.
[56] Li N, Tang X, Helleseth T,. New constructions of quadratic Bent functions in polynomial form[J]. IEEE Transactions on Information Theory, 2014, 60(9): 5760–5767.
[57] Li N, Tang X, Helleseth T. Several Classes of Codes and Sequences Derived From a Z_4-Valued Quadratic Form[J]. IEEE Transactions on Information Theory, 2011, 57(11): 7618–7628.
[58] Gao G, Zhang X, Liu W, et al. Constructions of quadratic and cubic rotation symmetric Bent functions[J]. IEEE Transactions on Information Theory, 2012, 58(7): 4908–4913.
[59] Tu Z, Deng Y. A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity[J]. Designs, Codes and Cryptography, 2011, 60(1): 1–14.
[60] Macwilliams F J, Sloane N J A. The Theory of Error-Correcting Codes[M]. Amsterdam: AMC, 1977.
[61] Hou X. Cubic Bent functions[J]. Discrete Mathematics, 1998, 189(1): 149–161.
[62] Carlet C. A larger class of cryptographic Boolean functions via a study of the Maiorana-McFarland construction[C]. In: Advances in Cryptology—CRYPTO 2002. Springer Berlin Heidelberg, 2002: 549–564.
[63] Carlet C, Prouff E. On plateaued functions and their constructions[C]. In: Fast Software Encryption. Springer Berlin Heidelberg, 2003: 54–73.
[64] Carlet C. Improving the algebraic immunity of resilient and nonlinear functions and constructing Bent functions[J]. IACR Cryptology ePrint Archive, 2004, 2004: 276.
[65] Carlet C. On the confusion and diffusion properties of Maiorana–McFarland's and extended Maiorana–McFarland's functions[J]. Journal of Complexity, 2004, 20(2): 182–204.
[66] Dobbertin H, Leander G. A survey of some recent results on Bent functions[C]. In: Sequences and Their Applications-SETA 2004. Springer Berlin Heidelberg, 2005: 1–29.
[67] Carlet C, Yucas J L. Piecewise constructions of Bent and almost optimal Boolean functions[J]. Designs, Codes and Cryptography, 2005, 37(3): 449–464
[68] Langevin P, Leander G. Classification of Boolean quartic forms in eight variables[J]. Boolean Functions in Cryptology and Information Security, 2008: 139.
[69] Meng Q, Yang M, Zhang H, et al. A novel algorithm enumerating Bent functions[J]. Discrete Mathematics, 2008, 308(23): 5576–5584.
[70] Carlet C, Helleseth T, Kholosha A, et al.. On the Dual of Bent Functions with 2^r Niho Exponents[C]. In: IEEE International Symposium on Information Theory Proceedings, 2011. IEEE, 2011: 703–707.
[71] Gupta K C, Nawaz Y, Gong G. Upper bound for algebraic immunity on a subclass of Maiorana McFarland class of Bent functions [J]. Information Processing Letters, 2011, 111(5): 247–249.
[72] Langevin P, Leander G. Counting all Bent functions in dimension eight 99270589265934370305785861242880[J]. Designs, Codes and Cryptography, 2011, 59(1–3): 193–205.
[73] Carlet C, Mesnager S. On Dillon's class H of Niho Bent functions and o-polynomials[C]. In: International Symposium on Artificial Intelligence and Mathematics. 2012.

[74] Kantor W M. Bent functions generalizing Dillon's partial spread functions[J]. arXiv preprint arXiv:1211.2600, 2012.
[75] Solé P, Tokareva N. Connections between Quaternary and Binary Bent Functions[J]. IACR Cryptology ePrint Archive, 2009, 2009: 544.
[76] Stănică P, Martinsen T, Gangopadhyay S, et al. Bent and generalized Bent Boolean functions[J]. Designs, codes and cryptography, 2013, 69(1): 77–94.
[77] Brown E H. Generalizations of the Kervaire invariant[J]. Annals of Mathematics, 1972: 368–383.
[78] Schmidt K. Z_4-valued quadratic forms and quaternary sequence families[J]. IEEE Transactions on Information Theory, 2009, 55(12): 5803–5810.
[79] Tokareva N N. Generalizations of Bent functions. A survey[J]. Journal of Applied and Industrial Mathematics, 2011, 5(1): 110–129.
[80] Stănică P, Gaangopadhyay S, Singh B K. Some results concerning generalized Bent functions[J]. 2012.
[81] Kumar P V, Scholtz R A, Welch L R. Generalized Bent functions and their properties[J]. Journal of Combinatorial Theory, Series A, 1985, 40(1): 90–107.
[82] Hou X D. p-Ary and q-ary versions of certain results about Bent functions and resilient functions[J]. Finite Fields and Their Applications, 2004, 10(4): 566–582.
[83] Pei D Y. On non-existence of generalized Bent functions[J]. LN in pure and applied math, 1993, 141: 165–172.
[84] Akyildiz E, Gülo□lu I Ş. A note of generalized Bent functions[J]. Journal of Pure and Applied Algebra, 1996, 106(1): 1–9.
[85] Ikeda M. A remark on the non-existence of generalized Bent functions[J]. Number Theory and Its Applications (Ankara, 1996), 1998: 109–119.
[86] Feng K. Generalized Bent functions and class group of imaginary quadratic fields[J]. Science in China Series A: Mathematics, 2001, 44(5): 562–570.
[87] Feng K Q, Liu F M. New results on the nonexistence of generalized Bent functions[J]. IEEE Transactions on Information Theory, 2003, 49(11): 3066–3071.
[88] Liu F, Ma Z, Feng K. New results on non-existence of generalized Bent functions (II)[J]. Science in China Series A: Mathematics, 2002, 45(6): 721–730.
[89] Feng K Q, Liu F M. Non-existence of some generalized Bent functions [J]. Acta Mathematica Sinica, 2003, 19(1): 39–50.
[90] Liu F M, Yue Q. A relationship between the nonexistence of generalized Bent functions and class groups[J]. Science in China Series A: Mathematics, 2010, 53(1): 213–222.
[91] Jiang Y, Deng Y. New results on nonexistence of generalized Bent functions[J]. Designs, Codes and Cryptography, 2015, 75(3): 375–385.
[92] Feng K Q, Liu F M, Ma Z. Generalized Bent function and the class group of imaginary Abel fields[J]. Progress in Natural Science, 2002, 12: 1080–1082.
[93] Feng K Q, Liu F M. Non-existence of some special generalized Bent function[J]. Chinese Annals of Mathematics Series A, 2003, 24(4): 445–452.
[94] Helleseth T, Kholosha A. Monomial and quadratic Bent functions over the finite fields of odd characteristic[J]. IEEE Transactions on Information Theory, 2006, 52(5): 2018–2032.
[95] Kumar P V, Moreno O. Prime-phase sequences with periodic correlation properties better than binary sequences[J]. IEEE Transactions on Information Theory, 1991, 37(3): 603–616.
[96] Liu S C, Komo J J. Nonbinary Kasami sequences over GF(*p*)[J]. IEEE Transactions on Information Theory, 1992, 38(4): 1409–1412.
[97] Kim Y S, Jang J W, No J S, et al. On p-ary Bent functions defined on finite fields[C]. In: Mathematical Properties of Sequences and Other Combinatorial Structures. Springer US, 2003: 65–76.
[98] Khoo K, Gong G, Stinson D R. A New Characterization of Semi-Bent and Bent Functions on Finite Fields*[J]. Designs, Codes and Cryptography, 2006, 38(2): 279–295.
[99] Li S, Hu L, Zeng X. Constructions of p-ary quadratic Bent functions[J]. Acta Applicandae Mathematicae, 2008, 100(3): 227–245.
[100] Helleseth T, Hollmann H, Kholosha A, et al. Proofs of two conjectures on ternary weakly regular Bent functions[J]. IEEE Transactions on Information Theory, 2009, 55(11): 5272–5283.
[101] Gong G, Helleseth T, Hu H, et al. On the dual of certain ternary weakly regular Bent functions[J]. IEEE Transactions on Information Theory, 2012, 58(4): 2237–2243.
[102] Helleseth T, Kholosha A. New binomial Bent functions over the finite fields of odd characteristic[C]. In: IEEE International Symposium on Information Theory Proceedings, 2010. IEEE, 2010: 1277–1281.
[103] Chung H, Kumar P V. A new general construction for generalized Bent functions[J]. IEEE Transactions on Information Theory, 1989, 35(1): 206–209.
[104] Coulter R S, Matthews R W. Planar functions and planes of Lenz-Barlotti class II[J]. Designs, Codes and Cryptography, 1997, 10(2): 167–184.
[105] Hou X. q-Ary Bent functions constructed from chain rings[J]. Finite Fields and Their Applications, 1998, 4(1): 55–61.

[106] Carlet C, Dubuc S. On generalized Bent and q-ary perfect nonlinear functions[J]. Finite Fields and Applications. Springer Berlin Heidelberg, 2001: 81–94.
[107] Kim S, Gil G M, Kim K H, et al. Generalized Bent functions constructed from partial spreads[C]. In: IEEE International Symposium on Information Theory, 2002. IEEE, 2002: 41.
[108] Canteaut A, Daum M, Dobbertin H, et al. Finding nonnormal Bent functions[J]. Discrete Applied Mathematics, 2006, 154(2): 202–218.
[109] Helleseth T, Kholosha A. On the dual of monomial quadratic p-ary Bent functions[C]. In: Sequences, subsequences, and consequences. Springer Berlin Heidelberg, 2007: 50–61.
[110] Helleseth T, Kholosha A. Sequences, Bent functions and Jacobsthal sums[C]. In: Sequences and Their Applications–SETA 2010. Springer Berlin Heidelberg, 2010: 416–429.
[111] Helleseth T, Kholosha A. On generalized Bent functions[C]. In: Information Theory and Applications Workshop (ITA), 2010. IEEE, 2010: 1–6.
[112] Tan Y, Yang J, Zhang X. A recursive construction of p-ary Bent functions which are not weakly regular[C]. In: IEEE International Conference on Information Theory and Information Security (ICITIS), 2010. IEEE, 2010: 156–159.
[113] Xia Y. A New Class of p-Ary Quadratic Bent Functions[J]. Journal of South-Central University for Nationalities (Natural Science Edition), 2011, 4: 027.
[114] Zheng D, Zeng X, Hu L. A family of p-ary binomial Bent functions[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2011, 94(9): 1868–1872.
[115] Budaghyan L, Carlet C, Helleseth T, et al. Generalized Bent functions and their relation to Maiorana-McFarland class[C]. In: IEEE International Symposium on Information Theory Proceedings, 2012. IEEE, 2012: 1212–1215.
[116] Jia W, Zeng X, Helleseth T, et al. A class of binomial Bent functions over the finite fields of odd characteristic[J]. IEEE Transactions on Information Theory, 2012, 58(9): 6054–6063.
[117] Cesmelioglu A, Meidl W, Pott A. On the normality of *p*-ary Bent functions[J]. Pre-proceedings of the InternationalWorkshop on Coding and Cryptography WCC 2013, 2013.
[118] Carlet C. Vectorial Boolean functions for cryptography[J]. Boolean Models and Methods in Mathematics, Computer Science, and Engineering, 2010, 134: 398–469.
[119] Nyberg K. Perfect nonlinear S-boxes[C]. In: Advances in Cryptology—EUROCRYPT '91. Springer Berlin Heidelberg, 1991: 378–386.
[120] Satoh T, Iwata T, Kurosawa K. On cryptographically secure vectorial Boolean functions[C]. In: Advances in Cryptology—ASIACRYPT '99. Springer Berlin Heidelberg, 1999: 20–28.
[121] Dong D, Zhang X, Qu L, et al. A note on vectorial Bent functions[J]. Information Processing Letters, 2013, 113(22): 866–870.
[122] Pasalic E, Zhang W G. On multiple output Bent functions[J]. Information Processing Letters, 2012, 112(21): 811–815.
[123] Muratovic-Ribic A, Pasalic E, Bajric S. Vectorial Bent functions from multiple terms trace functions[J]. IEEE Transactions on Information Theory, 2014, 60(2): 1337–1347.
[124] Feng K, Yang J. Vectorial Boolean functions with good cryptographic properties[J]. International Journal of Foundations of Computer Science, 2011, 22(06): 1271–1282.
[125] Carlet C, Khoo K, Lim C W, et al. Generalized correlation analysis of vectorial Boolean functions[C]. In: Fast Software Encryption—FSE 2007. Springer Berlin Heidelberg, 2007: 382–398.
[126] Budaghyan L, Carlet C. CCZ-equivalence of Bent vectorial functions and related constructions[J]. Designs, Codes and Cryptography, 2011, 59(1–3): 69–87.
[127] Carlet C. Relating three nonlinearity parameters of vectorial functions and building APN functions from Bent functions[J]. Designs, Codes and Cryptography, 2011, 59(1–3): 89–109.
[128] Youssef A M, Gong G. Hyper-Bent Functions[C]. In: Advances in cryptology—EUROCRYPT 2001. Springer Berlin Heidelberg, 2001: 406–419.
[129] Gong G, Golomb S W. Transform domain analysis of DES[J]. Information Theory, IEEE Transactions on, 1999, 45(6): 2065–2073.
[130] Carlet C, Gaborit P. Hyper-Bent functions and cyclic codes[J]. Journal of Combinatorial Theory, Series A, 2006, 113(3): 466–482.
[131] Charpin P, Gong G. HyperBent Functions, Kloosterman Sums, and Dickson Polynomials[J]. IEEE Transactions on Information Theory, 2008, 54(9): 4230–4238.
[132] Mesnager S. A new class of Bent and hyper-Bent Boolean functions in polynomial forms[J]. Designs, Codes and Cryptography, 2011, 59(1–3): 265–279.
[133] Tang C M, Qi Y F, Xu M Z, et al. A new class of hyper-Bent Boolean functions in binomial forms[J]. arXiv preprint arXiv:1112.0062, 2011.
[134] Mesnager S, Flori J P. HyperBent functions via Dillon-like exponents[J]. IEEE Transactions on Information Theory, 2013, 59(5):3215–3232.

[135] Mesnager S. Hyper-Bent Boolean functions with multiple trace terms[C]. In: Arithmetic of Finite Fields. Springer Berlin Heidelberg, 2010: 97–113.
[136] Wang B, Tang C, Qi Y, et al. A New Class of Hyper-Bent Boolean Functions with Multiple Trace Terms[J]. IACR Cryptology ePrint Archive, 2011, 2011: 600.
[137] Mesnager S. Bent and hyper-Bent functions in polynomial form and their link with some exponential sums and Dickson polynomials[J]. IEEE Transactions on Information Theory, 2011, 57(9): 5996–6009.
[138] Muratovic-Ribic A, Pasalic E, Ribic S. Vectorial HyperBent Trace Functions From the PS_{ap} Class—Their Exact Number and Specification[J]. IEEE Transactions on Information Theory, 2014, 60(7): 4408–4413.
[139] Wang B, Tang C, Qi Y, et al. A generalization of the class of hyper-Bent Boolean functions in binomial forms[J]. IACR Cryptology ePrint Archive, 2011, 2011: 698.

作者信息



杨小龙(1991–), 安徽阜阳人, 博士生. 主要研究领域为密码学.
E-mail: yxl@mail.ustc.edu.cn

胡红钢(1978–), 博士, 教授, 博士生导师, 中科院百人计划. 主要研究领域为密码学与信息安全.
E-mail: hghu2005@ustc.edu.cn