

PS 类 Bent 函数的一种构造方法

常祖领^{1,2}, 陈鲁生², 符方伟²

(1. 北京邮电大学理学院, 北京 100876; 2. 南开大学数学科学学院, 天津 300071)

摘 要: PS 类 bent 函数类是所有 $2^{(n/2)-1}$ 或 $2^{(n/2)-1}+1$ 个 F_2^n 的/ 不交的 $0 \frac{n}{2}$ 维子空间的指示函数的模 2 和所组成的函数的集合. 这些函数具有很好的代数结构并在密码学中有很多应用. 如何来刻画 PS bent 函数的代数范式一直是公开的难题. 构造 PS 类 bent 函数关键在于如何将 F_2^n 划分为 $2^{n/2}+1$ 个 $\frac{n}{2}$ 维子空间. 本文给出一种划分的方法, 从而构造出 PS 类 bent 函数, 并给出了对应的代数范式.

关键词: Bent 函数; 代数范式; Galois 域; 线性化多项式

中图分类号: TN9181.1 **文献标识码:** A **文章编号:** 0372-2112 (2004) 10-1642-05

One Method for Constructing Bent Functions of Class PS

CHANG Zu2ling^{1,2}, CHEN Lu2sheng², FU Fang2wei²

(1. School of Science, Beijing University of Posts and Telecommunications, Beijing 100876, China;

2. College of Mathematical Science, Nankai University, Tianjin 300071, China)

Abstract: The class of PS bent functions is one interesting class of bent functions, they have good algebraic structure and have many applications in cryptography. They are also useful for studying the general structure of bent functions. Unfortunately, the construction of PS bent functions is theoretic, it is still an open problem to characterize the algebraic normal forms of PS bent functions. In this paper we study the properties of such functions, and one method to construct PS bent functions and the corresponding algebraic normal forms are provided.

Key words: bent function; algebraic normal form; Galois field; linearized polynomial

1 引言

我们用 F_2 表示元素为 0 和 1 的有限域, 其中的加法运算用 $\oplus$ 来表示, 一个布尔函数 $f(x)$ 是从 F_2^n 到 F_2 的函数, 其中 $x = (x_1, \dots, x_n)$. 函数 $f(x)$ 可以表示成一个 n 变量的多项式

$$f(x_1, \dots, x_n) = a_0 \oplus \left(\bigoplus_{i=1}^n a_i x_i \right) \oplus \left(\bigoplus_{1 \leq i < j \leq n} a_{ij} x_i x_j \right) \oplus \dots \oplus a_{12 \dots n} x_1 x_2 \dots x_n,$$

其中的系数 $a_0, a_{ij}, \dots, a_{12 \dots n} \in F_2$. $f(x)$ 的这种表示称为 $f(x)$ 的代数范式 (algebraic normal form). 这个多项式的次数就是这个函数的次数. $f(x)$ 在 $XI \ F_2^n$ 处的 Walsh 变换定义如下:

$$W_f(X) = \sum_{x \in F_2^n} (-1)^{f(x) \oplus Xx}$$

其中 Xx 表示 X 和 x 的内积. 若函数 $f(x)$ 的 Walsh 变换满足 $|W_f(X)| = 2^{n/2}(-1)^{f(X)}$

也是 bent 函数. 我们称 f 是 f 的对偶函数. f 的对偶函数就是 f 本身.

Bent 函数有许多很好的性质, 并且也有许多应用^[3-6], 因此 bent 函数的构造就非常有意义. 我们至今所知道的直接构造出的 bent 函数 (而不是由已知的 bent 函数来构造另外的 bent 函数) 并经常使用的主要有两类, 一种是 M (Maiorana-Mc

Farland) 类^[1,7]. 我们令 $p = \frac{n}{2}$, 则有 $F_2^n = \{(x, y), x, y \in F_2^p\}$.

M 类中的 bent 函数具有如下形式:

$$f(x, y) = x \# P(y) \oplus g(y)$$

其中 P 是 F_2^p 上任意的置换, 而 g 是 F_2^p 上任意的布尔函数. 另一类是 PS (Partial Spread) 类^[1]. F_2^n 的子空间 E 的指示函数定义为

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

PS 类是所有 2^{p-1} 或 $2^{p-1}+1$ 个 F_2^n 的/ 不交的 $0p$ 维子空间的指示函数的模 2 和所组成的函数的集合, 其中/ 不交的 0 表示任意两个这样的子空间只交于 0 元素, 所以任意两个这样的子空间的直和是 F_2^n . 这类函数的对偶函数具有同样的形式, 把所有的 p 维子空间用它们的对偶空间代替即可. 文[1]中用 PS^- (PS^+) 来表示所有 2^{p-1} ($2^{p-1}+1$) 个 F_2^n 的不交的 p 维子空间的指示函数的模 2 和所组成的函数的集合. PS 类的构造只是理论性的, 如何来刻画这类 bent 函数的代数范式一直是公开的难题. 从 PS 类 bent 函数的定义我们可以看出, 构造这类 bent 函数的关键在于如何将 F_2^n 划分成 2^p+1 个不相交的 p 维子空间. 我们下面就根据这种思想给出一种构造这类 bent 函数的方法, 并给出了对应 bent 函数的代数范式.

收稿日期: 20021217; 修回日期: 200408208

基金项目: 国家自然科学基金 (No. 60373059, 60172060); 教育部跨世纪人才培养基金; 教育部优秀教师基金

2 子空间的构造

以后我们令 n 是偶数, 且 $p = \frac{n}{2}$. 在这一节中我们来把空间 F_2^n 划分成 $2^p + 1$ 个不相交的子空间.

我们首先来考虑 Galois 域^[4] F_{2^p} . 设 $f(x)$ 是 F_2 上的一个次数为 p 的本原多项式, 而 B 是 $f(x)$ 的一个根, 即 $f(B) = 0$, 则 B 是 F_{2^p} 的一个本原元, $F_{2^p} = \{0, 1, B, B^2, \dots, B^{2^p-2}\}$, 同时 F_{2^p} 中的元素可以表示成 $b_0 B^0 + b_1 B^1 + \dots + b_{p-1} B^{p-1}, b_i \in F_2$. 令

$$E_{C_i} = \{(A, AB^i), AI F_{2^p}\}, i = 0, 1, \dots, 2^p - 2,$$

$$E_{C_{2^p-1}} = \{(A, 0), AI F_{2^p}\}, E_{C_{2^p}} = \{(0, A), AI F_{2^p}\}$$

设 $a_1 = (A_1, A_2), a_2 = (B_1, B_2)$ 为某个 E_{C_i} 中的两个元素, 定义加法 $a_1 + a_2 = (A_1 + B_1, A_2 + B_2)$, 可以验证 $E_{C_i}, i = 0, 1, \dots, 2^p$ 是 Abel 群, 且 $E_{C_i} \cap E_{C_j} = \{(0, 0)\}, i \neq j$.

现在我们来把 $E_{C_i}, i = 0, 1, \dots, 2^p$ 中的元素转换成 F_2^n 中的元素. 对于 E_{C_i} 中的元素 (A, AB^i) , 它还可以表示成

$$(a_0 B^0 + a_1 B^1 + \dots + a_{p-1} B^{p-1}, b_0 B^0 + b_1 B^1 + \dots + b_{p-1} B^{p-1})$$

我们令它对应的 F_2^n 中的元素为

$$(a_0, a_1, \dots, a_{p-1}, b_0, b_1, \dots, b_{p-1})$$

易知这种转换是一一对应的. 我们把 E_{C_i} 中元素对应的 F_2^n 中的元素组成的集合记为 E_i , 由于 E_{C_i} 是 Abel 群, 所以 E_i 对于加法是封闭的, 即 E_i 是 F_2^n 的子空间. 又由于 $E_{C_i} \cap E_{C_j} = \{(0, 0), i \neq j\}$, 则 $E_i \cap E_j = \{(0, \dots, 0)\}, i \neq j$. 所以 $E_0, \dots, E_{2^p}$ 正是我们想要的 $2^p + 1$ 个/ 不交的子空间.

这时我们还可以求出这些子空间的基. 对于子空间 $E_i, i = 0, 1, \dots, 2^p - 2$, 它的基其实就是由 $(1, B^i), (B, B^{i+1}), \dots, (B^{p-1}, B^{i+p-1})$ 对应于 F_2^n 中向量所组成的, 具有如下形式:

$$(0, 0, \dots, 0, s_{i,1}^1, \dots, b_{i,p}^1), \dots, (0, \dots, 0, 1, b_{i,p-1}^1, \dots, b_{i,p}^1), b_{i,k}^1 \in F_2$$

子空间 E_{2^p-1} 的基是由 $(1, 0), (B, 0), \dots, (B^{p-1}, 0)$ 对应于 F_2^n 中向量所组成的, 即

$$(1, 0, \dots, 0, 0, \dots, 0), \dots, (0, \dots, 0, 1, 0, \dots, 0)$$

子空间 E_{2^p} 的基是由 $(0, 1), (0, B), \dots, (0, B^{p-1})$ 对应于 F_2^n 中向量所组成的, 即

$$(0, \dots, 0, 1, 0, \dots, 0), \dots, (0, \dots, 0, 0, \dots, 0, 1)$$

我们构造的子空间类似于仿射平面 $AP(F_{2^p})$ 的不同斜率的直线上的点组成的集合. 事实上, 我们就是从利用仿射平面 $AP(F_{2^p})$ 的 $2^p - 1$ 个非 0 斜率的平行直线类来生成正交拉丁方的方法受到启发的. 关于仿射平面和正交拉丁方的内容, 请参考文献[8].

例 1 我们来考虑 $n = 8$ 的情形, 这时 $p = 4$. 我们首先表示 Galois 域 F_{16} . $f(x) = x^4 + x + 1$ 是一个本原多项式. 令 B 是 $f(x)$ 的一个根, 则

$$F_{16} = \{0, 1, B, B^2, \dots, B^{14}\}$$

同时还可把 F_{16} 中元素表示成 B 的次数小于等于 3 的多项式:

$$0, 1, B, B+1, B^2, B^2+1, B^2+B, B^2+B+1$$

$$B^3, B^3+1, B^3+B, B^3+B+1, B^3+B^2,$$

$$B^3+B^2+1, B^3+B^2+B, B^3+B^2+B+1$$

下面我们来构造 $E_{C_0}, \dots, E_{14}, E_{15}, E_{16}$:

$$E_{C_i} = \{(A, AB^i), AI F_{16}\}, i = 0, 1, \dots, 14.$$

$$E_{15} = \{(A, 0), AI F_{16}\}, E_{16} = \{(0, A), AI F_{16}\}$$

接着我们把 E_{C_i} 转换成 F_2^8 的子空间 E_i ,

$$E_i = \{(a_0, \dots, a_3, b_0, \dots, b_3) | (a_0 B^0 + \dots + a_3 B^3, b_0 B^0 + \dots + b_3 B^3) \in E_{C_i}\}$$

这样我们就把 F_2^8 分成了 17 个不相交的子空间. 为了简单起见, 我们只列出这些子空间的基.

$$A_0 = \{(1, 0, 0, 0, 1, 0, 0, 0), (0, 1, 0, 0, 0, 1, 0, 0), (0, 0, 1, 0, 0, 0, 1, 0), (0, 0, 0, 1, 0, 0, 0, 1)\}$$

$$A_1 = \{(1, 0, 0, 0, 0, 1, 0, 0), (0, 1, 0, 0, 0, 0, 1, 0), (0, 0, 1, 0, 0, 0, 0, 1), (0, 0, 0, 1, 1, 1, 0, 0)\}$$

$$A_2 = \{(1, 0, 0, 0, 0, 0, 1, 0), (0, 1, 0, 0, 0, 0, 0, 1), (0, 0, 1, 0, 1, 1, 0, 0), (0, 0, 0, 1, 0, 0, 1, 0)\}$$

$$A_3 = \{(1, 0, 0, 0, 0, 0, 0, 1), (0, 1, 0, 0, 1, 1, 0, 0), (0, 0, 1, 0, 0, 1, 1, 0), (0, 0, 0, 1, 0, 0, 1, 1)\}$$

$$A_4 = \{(1, 0, 0, 0, 1, 1, 0, 0), (0, 1, 0, 0, 0, 1, 1, 0), (0, 0, 1, 0, 0, 0, 1, 1), (0, 0, 0, 1, 1, 1, 0, 1)\}$$

$$A_5 = \{(1, 0, 0, 0, 0, 1, 1, 0), (0, 1, 0, 0, 0, 0, 1, 1), (0, 0, 1, 0, 1, 1, 0, 1), (0, 0, 0, 1, 1, 0, 1, 0)\}$$

$$A_6 = \{(1, 0, 0, 0, 0, 0, 1, 1), (0, 1, 0, 0, 1, 1, 0, 1), (0, 0, 1, 0, 1, 0, 1, 0), (0, 0, 0, 1, 0, 1, 0, 1)\}$$

$$A_7 = \{(1, 0, 0, 0, 1, 1, 0, 1), (0, 1, 0, 0, 1, 0, 1, 0), (0, 0, 1, 0, 0, 1, 0, 1), (0, 0, 0, 1, 1, 1, 1, 0)\}$$

$$A_8 = \{(1, 0, 0, 0, 1, 0, 1, 0), (0, 1, 0, 0, 0, 1, 0, 1), (0, 0, 1, 0, 1, 1, 1, 0), (0, 0, 0, 1, 0, 1, 1, 1)\}$$

$$A_9 = \{(1, 0, 0, 0, 0, 1, 0, 1), (0, 1, 0, 0, 1, 1, 1, 0), (0, 0, 1, 0, 0, 1, 1, 1), (0, 0, 0, 1, 1, 1, 1, 1)\}$$

$$A_{10} = \{(1, 0, 0, 0, 1, 1, 1, 0), (0, 1, 0, 0, 0, 1, 1, 1), (0, 0, 1, 0, 1, 1, 1, 1), (0, 0, 0, 1, 1, 0, 1, 1)\}$$

$$A_{11} = \{(1, 0, 0, 0, 0, 1, 1, 1), (0, 1, 0, 0, 1, 1, 1, 1), (0, 0, 1, 0, 1, 0, 1, 1), (0, 0, 0, 1, 1, 0, 0, 2)\}$$

$$A_{12} = \{(1, 0, 0, 0, 1, 1, 1, 1), (0, 1, 0, 0, 1, 0, 1, 1), (0, 0, 1, 0, 1, 0, 0, 1), (0, 0, 0, 1, 1, 0, 0, 0)\}$$

$$A_{13} = \{(1, 0, 0, 0, 1, 0, 1, 1), (0, 1, 0, 0, 1, 0, 0, 1), (0, 0, 1, 0, 1, 0, 0, 0), (0, 0, 0, 1, 0, 1, 0, 0)\}$$

$$A_{14} = \{(1, 0, 0, 0, 1, 0, 0, 1), (0, 1, 0, 0, 1, 0, 0, 0), (0, 0, 1, 0, 0, 1, 0, 0), (0, 0, 0, 1, 0, 0, 1, 0)\}$$

$$A_{15} = \{(1, 0, 0, 0, 0, 0, 0, 0), (0, 1, 0, 0, 0, 0, 0, 0), (0, 0, 1, 0, 0, 0, 0, 0), (0, 0, 0, 1, 0, 0, 0, 0)\}$$

$$A_{16} = \{(0, 0, 0, 0, 1, 0, 0, 0), (0, 0, 0, 0, 0, 1, 0, 0), (0, 0, 0, 0, 0, 0, 1, 0), (0, 0, 0, 0, 0, 0, 0, 1)\}$$

3 子空间的指示函数

在上一节中我们求出了 F_2^n 的 $2^p + 1$ 个不相交的子空间, 现在我们来求这些子空间的指示函数. 事实上, 直接求这些子空间的指示函数并不是一件容易的事, 但是我们可以换一种

角度来考虑它.

对于子空间 $E_a, i=0, 1, \dots, 2^p$, 设它的基是 $\{A_1, \dots, A_p\}$. 我们构造一个齐次线性方程组

$$F_i(x) = \begin{cases} f_{i1}(x) = A_1 \# x = 0 \\ f_{i2}(x) = A_2 \# x = 0 \\ \vdots \\ f_{ip}(x) = A_p \# x = 0 \end{cases}$$

由于 $A_1, \dots, A_p$ 是 p 个相互无关的向量, 根据线性代数的知识, 齐次线性方程组 $F_i(x)$ 的解空间为 F_2^n 的一个维数为 p 的线性子空间, 我们令这个线性子空间为 S_i . 容易证明 S_i 是 E_i 的对偶空间. 对于任两个子空间 $E_i, E_j, i \neq j$, 它们的基分别为 $\{A_1, \dots, A_p\}$ 和 $\{A_1, \dots, A_p\}$. 由于 E_i 和 E_j 的直和是 F_2^n , 所以 $\{A_1, \dots, A_p, A_1, \dots, A_p\}$ 也是 F_2^n 的基, 维数是 n , 所以它对应的齐次线性方程组 ($F_i(x) = 0, F_j(x) = 0$) 的解只有 0 向量. 这说明子空间 $S_i, i=0, 1, \dots, 2^p$ 相互之间也是不交的, 也满足我们的要求.

对任意 $A \in S_i$, 它都满足 $f_{i1}(A) = \dots = f_{ip}(A) = 0$. 根据指示函数的定义, S_i 的指示函数应为

$$I_{S_i}(x) = (f_{i1}(x) \odot 1) \odot (f_{ip}(x) \odot 1)$$

在 $E_i, i=0, \dots, 2^p$ 这些子空间中, 容易验证 E_0 与自身对偶, 所以 $S_0 = E_0$; E_{2^p-1} 与 E_{2^p} 互为对偶子空间, 所以我们有 $S_{2^p-1} = E_{2^p}, S_{2^p} = E_{2^p-1}$. 对于 $E_i, i=1, \dots, 2^p-2$, 设 E_i 的基为

$$(1, 0, \dots, 0, b_{1,1}^i, \dots, b_{1,p}^i), \dots, (0, \dots, 0, 1, b_{p,1}^i, \dots, b_{p,p}^i), \\ b_{j,k}^i \in F_2$$

我们可以得到对应的齐次线性方程组:

$$F(x) = \begin{cases} x_1 \odot b_{1,1}^i x_{p+1} \odot \dots \odot b_{1,p}^i x_{2p} = 0 \\ \vdots \\ x_p \odot b_{p,1}^i x_{p+1} \odot \dots \odot b_{p,p}^i x_{2p} = 0 \\ \left. \begin{cases} x_1 = b_{1,1}^i x_{p+1} \odot \dots \odot b_{1,p}^i x_{2p} \\ \vdots \\ x_p = b_{p,1}^i x_{p+1} \odot \dots \odot b_{p,p}^i x_{2p} \end{cases} \right\} s \end{cases}$$

经过计算, 这个齐次线性方程组的解空间 S_i 的基为

$$(b_{1,1}^i, \dots, b_{p,1}^i, 1, 0, \dots, 0), \dots, (b_{1,p}^i, \dots, b_{p,p}^i, 0, \dots, 0, 1)$$

由于一个空间的对偶空间的对偶空间是本身, 所以 S_i 的对偶空间就是 E_i . 同样根据上面的讨论, 我们可以得到子空间 E_i 的指示函数为

$$I_{E_0}(x) = I_{S_0}(x), I_{E_{2^p-1}}(x) = I_{S_{2^p}}(x), I_{E_{2^p}}(x) = I_{S_{2^p-1}}(x),$$

$$I_{E_i}(x) = (b_{1,1}^i x_1 \odot \dots \odot b_{p,1}^i x_p \odot x_{p+1} \odot \dots \odot x_{2p}),$$

$$(b_{p,1}^i x_1 \odot \dots \odot b_{p,p}^i x_p \odot x_{2p} \odot 1), i=1, \dots, 2^p-2$$

子空间 $E_i, i=0, 1, \dots, 2^p$ 的指示函数一共有 $2^{p+1}+1$ 个, 从中任取 2^{p-1} (或 $2^{p-1}+1$) 个, 把它们模 2 和, 而它的对偶函数则是这些子空间的对偶子空间的指示函数的模 2 和. 这样就得到了 PS^- (PS^+) 类 bent 函数的代数范式, 也就构造出了对应的 bent 函数, 当然, 如果 $f(x)$ 是一个 bent 函数, 对任意的仿射函数 $h(x) = A \# x \oplus a, A \in F_2^n, a \in F_2$ 和任意的从 F_2^n 到 F_2^n

的仿射同构 $W: f \mapsto W \circ f$ 仍旧是 bent 函数.

需要特别指出的是当 $n=4, p=2$ 时, 由于 E_0 的对偶子空间是本身, E_3 和 E_4 互对偶, 而经验证 E_1 和 E_2 也互对偶. 设它们的指示函数分别为 $I_{E_0}(x), \dots, I_{E_5}(x)$, 则下列 bent 函数的对偶函数是本身:

$$I_{E_1}(x) \odot I_{E_2}(x), I_{E_3}(x) \odot I_{E_4}(x),$$

$$I_{E_0}(x) \odot I_{E_1}(x) \odot I_{E_2}(x), I_{E_0}(x) \odot I_{E_3}(x) \odot I_{E_4}(x)$$

当 $n > 4$ 时, 我们构造出的 bent 函数的个数应该是 $2^{\binom{2^{p+1}}{2^{p-1}}}$, 其中一半是 PS^- 类, 一半是 PS^+ 类. 当然, 对偶函数的个数也是这么多.

在文献[1]中, Dillon 给出一种构造 PS^- 类 bent 函数的方法, 他称他构造出的函数为 PS_{ap} 类, 令 F_2^n 等同于 Galois 域 F_{2^p} , 则这类 bent 函数具有如下形式: $g(\frac{x}{y})$, 其中 g 是一个平衡函数, 且如果 $y=0$ 时, $\frac{x}{y}=0$. 其实这类 bent 函数是我们构造出的 bent 函数的一部分, 因为由我们的构造方法可以看出, 所有满足 $\frac{x}{y}$ 等于 Galois 域 F_{2^p} 中某元素的输入其实就是

我们构造出的某个子空间 E_i . 另外由于 Dillon 令 $y=0$ 时 $\frac{x}{y}=0$, 则与 $x=0$ 时对应的输出是一样的, 这时, 子空间 E_{2^p-1} 和 E_{2^p} 就同时被取或同时不取. 所以我们说 Dillon 构造的 PS_{ap} 类 bent 函数是我们构造出的 bent 函数的一部分.

例 2 承接例 1, 根据 17 个子空间的基, 我们可以列出对应的齐次线性方程组的解空间即对偶空间的指示函数如下:

$$I_{S_0}(x) = (x_1 \odot x_5 \odot 1)(x_2 \odot x_6 \odot 1)(x_3 \odot x_7 \odot 1)(x_4 \odot x_8 \odot 1)$$

$$I_{S_1}(x) = (x_1 \odot x_6 \odot 1)(x_2 \odot x_7 \odot 1)(x_3 \odot x_8 \odot 1)$$

$$(x_4 \odot x_5 \odot x_6 \odot 1)$$

$$I_{S_2}(x) = (x_1 \odot x_7 \odot 1)(x_2 \odot x_8 \odot 1)(x_3 \odot x_5 \odot x_6 \odot 1)$$

$$(x_4 \odot x_6 \odot x_7 \odot 1)$$

$$I_{S_3}(x) = (x_1 \odot x_8 \odot 1)(x_2 \odot x_5 \odot x_6 \odot 1)(x_3 \odot x_6 \odot x_7 \odot 1)$$

$$(x_4 \odot x_7 \odot x_8 \odot 1)$$

$$I_{S_4}(x) = (x_1 \odot x_5 \odot x_6 \odot 1)(x_2 \odot x_6 \odot x_7 \odot 1)(x_3 \odot x_7 \odot x_8 \odot 1)$$

$$(x_4 \odot x_5 \odot x_6 \odot x_8 \odot 1)$$

$$I_{S_5}(x) = (x_1 \odot x_6 \odot x_7 \odot 1)(x_2 \odot x_7 \odot x_8 \odot 1)$$

$$(x_3 \odot x_5 \odot x_6 \odot x_8 \odot 1)(x_4 \odot x_5 \odot x_7 \odot 1)$$

$$I_{S_6}(x) = (x_1 \odot x_7 \odot x_8 \odot 1)(x_2 \odot x_5 \odot x_6 \odot x_8 \odot 1)$$

$$(x_3 \odot x_5 \odot x_7 \odot 1)(x_4 \odot x_6 \odot x_8 \odot 1)$$

$$I_{S_7}(x) = (x_1 \odot x_5 \odot x_6 \odot x_8 \odot 1)(x_2 \odot x_5 \odot x_7 \odot 1)$$

$$(x_3 \odot x_6 \odot x_8 \odot 1)(x_4 \odot x_5 \odot x_6 \odot x_7 \odot 1)$$

$$I_{S_8}(x) = (x_1 \odot x_5 \odot x_7 \odot 1)(x_2 \odot x_6 \odot x_8 \odot 1)$$

$$(x_3 \odot x_5 \odot x_6 \odot x_7 \odot 1)(x_4 \odot x_6 \odot x_7 \odot x_8 \odot 1)$$

$$I_{S_9}(x) = (x_1 \odot x_6 \odot x_8 \odot 1)(x_2 \odot x_5 \odot x_6 \odot x_7 \odot 1)$$

$$(x_3 \odot x_6 \odot x_7 \odot x_8 \odot 1)(x_4 \odot x_5 \odot x_6 \odot x_7 \odot x_8 \odot 1)$$

$$I_{S_{10}}(x) = (x_1 \odot x_5 \odot x_6 \odot x_7 \odot 1)(x_2 \odot x_6 \odot x_7 \odot x_8 \odot 1)$$

$$\begin{aligned}
& (x_3^{\odot} x_5^{\odot} x_6^{\odot} x_7^{\odot} x_8^{\odot} 1)(x_4^{\odot} x_5^{\odot} x_7^{\odot} x_8^{\odot} 1) \\
I_{S_{11}}(x) &= (x_1^{\odot} x_6^{\odot} x_7^{\odot} x_8^{\odot} 1)(x_2^{\odot} x_5^{\odot} x_6^{\odot} x_7^{\odot} x_8^{\odot} 1) \\
& (x_3^{\odot} x_5^{\odot} x_7^{\odot} x_8^{\odot} 1)(x_4^{\odot} x_5^{\odot} x_8^{\odot} 1) \\
I_{S_{12}}(x) &= (x_1^{\odot} x_5^{\odot} x_6^{\odot} x_7^{\odot} x_8^{\odot} 1)(x_2^{\odot} x_5^{\odot} x_7^{\odot} x_8^{\odot} 1) \\
& (x_3^{\odot} x_5^{\odot} x_8^{\odot} 1)(x_4^{\odot} x_5^{\odot} 1) \\
I_{S_{13}}(x) &= (x_1^{\odot} x_5^{\odot} x_7^{\odot} x_8^{\odot} 1)(x_2^{\odot} x_5^{\odot} x_8^{\odot} 1)(x_3^{\odot} x_5^{\odot} 1) \\
& (x_4^{\odot} x_6^{\odot} 1) \\
I_{S_{14}}(x) &= (x_1^{\odot} x_5^{\odot} x_8^{\odot} 1)(x_2^{\odot} x_5^{\odot} 1)(x_3^{\odot} x_6^{\odot} 1) \\
& (x_4^{\odot} x_7^{\odot} 1) \\
I_{S_{15}}(x) &= (x_1^{\odot} 1)(x_2^{\odot} 1)(x_3^{\odot} 1)(x_4^{\odot} 1) \\
I_{S_{16}}(x) &= (x_5^{\odot} 1)(x_6^{\odot} 1)(x_7^{\odot} 1)(x_8^{\odot} 1)
\end{aligned}$$

同样我们不以求出子空间 S_i 的基及 E_i 的指示函数. 下面只列出 E_i 的指示函数.

$$\begin{aligned}
I_{E_0}(x) &= I_{S_0}(x) \\
I_{E_1}(x) &= (x_4^{\odot} x_5^{\odot} 1)(x_1^{\odot} x_4^{\odot} x_6^{\odot} 1)(x_2^{\odot} x_7^{\odot} 1) \\
& (x_3^{\odot} x_8^{\odot} 1) \\
I_{E_2}(x) &= (x_3^{\odot} x_5^{\odot} 1)(x_3^{\odot} x_4^{\odot} x_6^{\odot} 1)(x_1^{\odot} x_4^{\odot} x_7^{\odot} 1) \\
& (x_2^{\odot} x_8^{\odot} 1) \\
I_{E_3}(x) &= (x_2^{\odot} x_5^{\odot} 1)(x_2^{\odot} x_3^{\odot} x_6^{\odot} 1)(x_3^{\odot} x_4^{\odot} x_7^{\odot} 1) \\
& (x_1^{\odot} x_4^{\odot} x_8^{\odot} 1) \\
I_{E_4}(x) &= (x_1^{\odot} x_4^{\odot} x_5^{\odot} 1)(x_1^{\odot} x_2^{\odot} x_4^{\odot} x_6^{\odot} 1) \\
& (x_2^{\odot} x_3^{\odot} x_7^{\odot} 1)(x_3^{\odot} x_4^{\odot} x_8^{\odot} 1) \\
I_{E_5}(x) &= (x_3^{\odot} x_4^{\odot} x_5^{\odot} 1)(x_1^{\odot} x_3^{\odot} x_6^{\odot} 1) \\
& (x_1^{\odot} x_2^{\odot} x_4^{\odot} x_7^{\odot} 1)(x_2^{\odot} x_3^{\odot} x_8^{\odot} 1) \\
I_{E_6}(x) &= (x_2^{\odot} x_3^{\odot} x_5^{\odot} 1)(x_2^{\odot} x_4^{\odot} x_6^{\odot} 1) \\
& (x_1^{\odot} x_3^{\odot} x_7^{\odot} 1)(x_1^{\odot} x_2^{\odot} x_4^{\odot} x_8^{\odot} 1) \\
I_{E_7}(x) &= (x_1^{\odot} x_2^{\odot} x_4^{\odot} x_5^{\odot} 1)(x_1^{\odot} x_3^{\odot} x_4^{\odot} x_6^{\odot} 1) \\
& (x_2^{\odot} x_4^{\odot} x_7^{\odot} 1)(x_1^{\odot} x_3^{\odot} x_8^{\odot} 1) \\
I_{E_8}(x) &= (x_1^{\odot} x_3^{\odot} x_5^{\odot} 1)(x_2^{\odot} x_3^{\odot} x_4^{\odot} x_6^{\odot} 1) \\
& (x_1^{\odot} x_3^{\odot} x_4^{\odot} x_7^{\odot} 1)(x_2^{\odot} x_4^{\odot} x_8^{\odot} 1) \\
I_{E_9}(x) &= (x_2^{\odot} x_4^{\odot} x_5^{\odot} 1)(x_1^{\odot} x_2^{\odot} x_3^{\odot} x_4^{\odot} x_6^{\odot} 1) \\
& (x_2^{\odot} x_3^{\odot} x_4^{\odot} x_7^{\odot} 1)(x_1^{\odot} x_3^{\odot} x_4^{\odot} x_8^{\odot} 1) \\
I_{E_{10}}(x) &= (x_1^{\odot} x_3^{\odot} x_4^{\odot} x_5^{\odot} 1)(x_1^{\odot} x_2^{\odot} x_3^{\odot} x_6^{\odot} 1) \\
& (x_1^{\odot} x_2^{\odot} x_3^{\odot} x_4^{\odot} x_7^{\odot} 1)(x_2^{\odot} x_3^{\odot} x_4^{\odot} x_8^{\odot} 1) \\
I_{E_{11}}(x) &= (x_2^{\odot} x_3^{\odot} x_4^{\odot} x_5^{\odot} 1)(x_1^{\odot} x_2^{\odot} x_6^{\odot} 1) \\
& (x_1^{\odot} x_2^{\odot} x_3^{\odot} x_7^{\odot} 1)(x_1^{\odot} x_2^{\odot} x_3^{\odot} x_4^{\odot} x_8^{\odot} 1) \\
I_{E_{12}}(x) &= (x_1^{\odot} x_2^{\odot} x_3^{\odot} x_4^{\odot} x_5^{\odot} 1)(x_1^{\odot} x_6^{\odot} 1) \\
& (x_1^{\odot} x_2^{\odot} x_7^{\odot} 1)(x_1^{\odot} x_2^{\odot} x_3^{\odot} x_8^{\odot} 1) \\
I_{E_{13}}(x) &= (x_1^{\odot} x_2^{\odot} x_3^{\odot} x_5^{\odot} 1)(x_4^{\odot} x_6^{\odot} 1)(x_1^{\odot} x_7^{\odot} 1) \\
& (x_1^{\odot} x_2^{\odot} x_8^{\odot} 1) \\
I_{E_{14}}(x) &= (x_1^{\odot} x_2^{\odot} x_5^{\odot} 1)(x_3^{\odot} x_6^{\odot} 1)(x_4^{\odot} x_7^{\odot} 1) \\
& (x_1^{\odot} x_8^{\odot} 1) \\
I_{E_{15}}(x) &= I_{S_1}(x)
\end{aligned}$$

$$I_{E_{16}}(x) = I_{S_2}(x)$$

根据这些指示函数, 从 $I_{E_i}(x)$ 中任选 8 个, 则它们的模 2 和就是 PS^- 类 bent 函数, 任选 9 个, 则它们的模 2 和就是 PS^+ 类 bent 函数. 这些 bent 函数的对偶函数是对应的 $I_{S_i}(x)$ 的模 2 和. 由于 $\begin{bmatrix} 17 \\ 8 \end{bmatrix} = \begin{bmatrix} 17 \\ 9 \end{bmatrix} = 24310$, 所以我们构造出的 PS^- 类和 PS^+ 类 bent 函数的个数都是 24310 个, 且它们的对偶函数个数也分别是 24310 个.

4 PS 类 bent 函数的一般构造

下面来讨论 PS 类 bent 函数的一般构造方法. 由于构造这类 bent 函数最主要的工作在于将空间 F_2^n 划分成 $2^p + 1$ 个 / 不交的 $0p$ 维子空间, 所以首先讨论划分空间 F_2^n 的方法.

为了说明方便, 我们下面用子空间的生成矩阵: $A_0, A_1, \dots, A_{2^p}$, 来代表对应的子空间. 这样的生成矩阵 A_i 为 $p \times n$ 的矩阵, 可以表示为 $A_i = (S_{i1}, S_{i2})$, 其中 S_{i1}, S_{i2} 都是 $p \times p$ 矩阵, 且 A_i 的秩为 p . 因为任意两个子空间都不交, 它们的直和是整个空间 F_2^n , 则对任意 $i, j \in \{0, 1, \dots, 2^p\}$

$$\begin{bmatrix} A_i \\ A_j \end{bmatrix} = \begin{bmatrix} S_{i1} & S_{i2} \\ S_{j1} & S_{j2} \end{bmatrix}$$

是一个 $n \times n$ 满秩矩阵. 令 C 是 F_2 上的任意 $n \times n$ 的满秩矩阵, 则

$$\begin{bmatrix} A_i @ C \\ A_j @ C \end{bmatrix} = \begin{bmatrix} A_i \\ A_j \end{bmatrix} @ C$$

仍是满秩矩阵, 且分别以 $A_0 @ C, \dots, A_{2^p} @ C$ 为生成矩阵的子空间仍是维数为 p 的不相交的子空间. 这样我们就可以得到下面结果.

引理 1 如果 $f(x)$ 是 F_2^n 上的 PS 类 bent 函数, C 是任意 F_2 上的 $n \times n$ 满秩矩阵, 则 $f(C @ x)$ 仍是 PS 类 bent 函数.

这样对于 $A_0, A_1, \dots, A_{2^p}$, 我们令

$$C = \begin{bmatrix} A_0 \\ A_1 \end{bmatrix}^{-1},$$

则 $A_0 @ C = (E_p, 0)$, $A_0 @ C = (0, E_p)$, 其中 E_p 为 p 阶单位矩阵. 因此我们总可以假设划分 F_2^n 所得到的 $2^p + 1$ 个 / 不交的子空间对应的生成矩阵包括 $A_0 = (E_p, 0)$ 和 $A_1 = (0, E_p)$ 在内.

对于 $A_0 = (E_p, 0)$, $A_1 = (0, E_p)$, $A_2, \dots, A_{2^p}$, 由于其中的 $A_i = (S_{i1}, S_{i2})$, $i = 2, \dots, 2^p$, 必须与 A_0 和 A_1 不交, 则 S_{i1} 和 S_{i2} 的秩都为 p . 如果其中一个的秩小于 p , 不妨假设 S_{i2} 的秩小于 p , 因为它与 A_0 不交, 则

$$W_{n @ n} = \begin{bmatrix} E_p & 0 \\ S_{i1} & S_{i2} \end{bmatrix}$$

对应的行列式的值等于

$$|W_{n @ n}| = |E_p| @ |S_{i2}|.$$

因为 S_{i2} 的秩小于 p , 则它对应行列式的值为 0, 所以 $|W| = 0$. 根据线性代数的知识, 得到矩阵 W 的秩小于 n , 则由它为生成矩阵生成的空间一定不是 F_2^n , 因此就与它和 A_0 不交这个事实矛盾, 所以 S_{i2} 的秩必为 p . 同理还可证明 S_{i1} 的秩也为 p .

这样我们就对子空间的结构有了清醒的认识. 如果把 $A_i, i = 2, \dots, 2^p$, 对应子空间中元素表示成有限域中元素的话, 则 A_i 中元素有如下形式:

$$(A, B), A, B \in F_{2^p}$$

且 A 和 B 都取遍 F_{2^p} 中的值. 令 $H(x)$ 是 F_{2^p} 上的一个置换函数, 则 A_i 中元素还可表示成

$$(A, H(A)), A \in F_{2^p}$$

因为 A_i 是一个子空间, 满足加法封闭, 所以置换 $H(x)$ 应满足

$$(1) (0) = 0; \quad (2) H(A) + H(B) = H(A+B), A, B \in F_{2^p}$$

可见, 转换 $H(x)$ 应是 F_{2^p} 上一个线性变换, 即线性转换.

因此划分 $F_{2^p}^2$ 的工作就集中在寻找 F_{2^p} 上的线性置换上了.

需要注意的是, 这时的线性置换其实就是线性变换. 但是我们所需要的线性变换必须不是零变换, 所以我们采用了线性置换这个术语.

因为有限域 F_{2^p} 的特征是 2, 我们首先来考虑 F_{2^p} 上的指数函数 $H(x) = x^{2^h}$, 其中 h 是一个非负整数. 根据有限域中的知识, 对于 F_{2^p} 中任意两个元素 A, B , 我们总有

$$(A+B)^{2^h} = A^{2^h} + B^{2^h}, (A-B)^{2^h} = A^{2^h} - B^{2^h},$$

因此我们可以判断 $H(x)$ 是 F_{2^p} 上的置换函数, 并且还满足我们要求的两条, 因此它是一个线性置换.

下面我们就用 $H(x) = x^{2^h}$ 来把划分 $F_{2^p}^2$ 成 $2^p + 1$ 个不交的子空间. 显然, A_0 和 A_1 是其中的两个, 其余的子空间如下构造: 令 B 是 F_{2^p} 的一个生成元, 子空间 $A_i, i = 2, \dots, 2^p$, 满足

$$A_i = \{(A, B^{i-2}H(A)) | A \in F_{2^p}\}$$

根据 $H(x)$ 的特性, 我们可以验证 $A_i, i = 2, \dots, 2^p$, 确实是子空间, 且这些子空间互不相交, 且它们与 A_0 和 A_1 也是互不相交的, 因此 $A_0, A_1, A_2, \dots, A_{2^p}$ 就是我们所希望的 $F_{2^p}^2$ 的一种划分. 根据前面的方法, 我们还可求出子空间的指示函数, 然后就可构造出 PS 类 bent 函数的方法其实是这里讨论的一种, 它对应的线性置换函数是 $H(x) = x = x^{2^0}$, 即 $h = 0$.

我们还可把上述方法进行更进一步的推广来得到更一般的结果. F_{2^p} 上的线性化多项式是具有如下形式的多项式:

$$L(x) = \sum_{s=0}^{p-1} A_s x^{2^s}, A_s \in F_{2^p}$$

显然上面考虑的置换函数 $H(x) = x^{2^h}$ 是线性化多项式对应函数的一个特例. 容易验证线性化函数满足线性性, 但遗憾的是在一般情况下它不是 F_{2^p} 上的置换. 文献[9]证明了线性化函数 $L(x)$ 是 F_{2^p} 上的置换当且仅当由它的系数构成的矩阵

$$A = \begin{pmatrix} A_0 & A_{p-1}^2 & A_{p-2}^2 & \dots & A_1^{2^{p-1}} \\ A_1 & A_0^2 & A_{p-1}^2 & \dots & A_2^{2^{p-1}} \\ A_2 & A_1^2 & A_0^2 & \dots & A_3^{2^{p-1}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ A_{p-1} & A_{p-2}^2 & A_{p-3}^2 & \dots & A_0^{2^{p-1}} \end{pmatrix}$$

满足 $|A| \neq 0$. 根据这个事实, 我们可以首先构造出线性化多

项式函数 $L(x)$, 然后再检验它的系数构成的矩阵是否满足 $|A| \neq 0$. 如果满足, 则它就是 F_{2^p} 上的置换, 则我们就可以根据它按照上面的方法来划分 $F_{2^p}^2$, 从而构造出 PS 类 bent 函数.

综合上面分析, 我们可以得到下面定理.

定理 1 对于 F_{2^p} 上的线性化多项式

$$L(x) = \sum_{s=0}^{p-1} A_s x^{2^s}, A_s \in F_{2^p},$$

如果它的系数构成的矩阵 A 对应的行列式的值不等于 0, 则我们就可以根据它划分空间并构造出一组 PS 类 bent 函数.

根据有限域的知识我们知道对应矩阵 A 的行式不为 0 的线性化多项式与满秩矩阵是一一对应的^[9]. 因此我们完全可以用线性代数的语言来描述上述有限域的结果.

5 结论

在这篇文章中, 我们主要讨论了 PS 类 bent 函数的构造方法. 我们首先给出一种特殊的构造方法, 详细讨论了如何利用这种方法来进行空间的划分、子空间的指示函数的表示和构造 PS 类 bent 函数. 在例子中我们列出了 $n = 8$ 时我们构造出的 bent 函数. 最后我们讨论了 PS 类 bent 函数的一般构造方法, 说明如何根据线性置换来构造 PS 类 bent 函数, 指出了线性化多项式在构造 PS 类 bent 函数中的作用. 我们在这里构造出的部分 PS 类 bent 函数没有出现于其它文献中.

参考文献:

- [1] Dillon JF. Elementary hadamard difference sets[D]. Ph D Thesis, University of Maryland, 1974.
- [2] Rothaus OS. On bent functions[J]. Journal of Combinatorics Theory, Series A, 1976, 20: 300- 305.
- [3] Meier W, Staffelbach. Nonlinearity criteria for cryptographic functions[A]. in Advances in Cryptology EUROCRYPTO. 89 (Lecture Notes in Computer Science, 434) [C]. Berlin, Germany: Springer-Verlag, 1992. 549- 562.
- [4] F J MacWilliams, N J A Sloane. The Theory of Error Correcting Codes[M]. Amsterdam, Netherlands: North Holland, 1977.
- [5] Olsen JD, Scholtz RA, Welch LR. Bent function sequences[J]. IEEE Transactions on Information Theory, 1982, 28(6): 858- 864.
- [6] Assmus EF, J D Key. Designs and Their Codes[M]. Cambridge University Press, 1992.
- [7] McFarland RL. A family of noncyclic difference sets[J]. Journal of Combinatorics Theory, Series A, 1973, 15: 1- 10.
- [8] R A Brualdi. Introductory Combinatorics[M]. Elsevier North-Holland, Inc. 1977.
- [9] R Lidl, H Niederreiter. Finite Fields. Encyclopedia of Mathematics and Its Applications[M]. vol. 20, Addison-Wesley Publishing Company, 1983.

作者简介:

常祖领 男, 1976 年出生于河南新乡, 现为北京邮电大学理学院博士后, 主要研究方向是密码学和编码理论. Email: zhang@you. com