Pure Mathematics 理论数学, 2013, 3, 120-125
http://dx.doi.org/10.12677/pm.2013.32019 Published Online March 2013 (http://www.hanspub.org/journal/pm.html)

A Generalization of One Class of Semi-Bent Functions with Polynomial Trace Form

Hao Chen, Xiwang Cao

College of Science, Nanjing University of Aeronautics and Astronautics, Nanjing
Email: chenhao246@sina.cn, xwcao@nuaa.edu.cn

Received: Dec. 22nd, 2012; revised: Feb. 5th, 2013; accepted: Feb. 21st, 2013

Abstract: This paper is devoted to generalize a class of semi-Bent functions with even number of variables on the finite filed F_{2^n}. We define the functions $g_{a,b,c,d}^{(r,s)}(x)=Tr_1^n\left(ax^{r\left(2^m-1\right)}\right)+Tr_1^2\left(bx^{\left(2^n-1\right)/3}\right)+Tr_1^n\left(cx^{\left(2^m-1\right)/2+1}\right)+Tr_1^n\left(dx^{\left(2^m-1\right)s+1}\right)$ and $f_{a,b}^{(r)}(x)=Tr_1^n\left(ax^{r\left(2^m-1\right)}\right)+Tr_1^2\left(bx^{\left(2^n-1\right)/3}\right)$, where $n=2m$ with m odd, r is a positive integer and $s\in\{0,1/4,1/6,3\}$, $a\in F_{2^n}^*, b\in F_4^*, c\in F_{2^n}$ and $d\in F_2, x\in F_{2^n}$. In the paper [1], S. Mesnager has discussed whether $g_{a,b,c,d}^{(r,s)}$ could be semi-Bent function under the situations $r=3$ and $\left(r,2^m+1\right)=1$. In this paper, we will give a further investigation on the function $g_{a,b,c,d}^{(r,s)}$ by removing the restrictions on r. We need to note that Kloosterman sums and cubic sums are essential to this paper.

Keywords: Boolean Functions; Semi-Bent Functions; Walsh-Hadamard Transformation; Kloosterman Sums; Cubic Sums

一类带有多项式迹形式的 Semi-Bent 函数的推广

陈　浩，曹喜望

南京航空航天大学理学院，南京
Email: chenhao246@sina.cn, xwcao@nuaa.edu.cn

收稿日期：2012 年 12 月 22 日；修回日期：2013 年 2 月 5 日；录用日期：2013 年 2 月 21 日

摘　要：本文的主要是对一类已知的 semi-Bent 函数作进一步的推广。首先，我们来定义下列两个位于有限域上的具有多项式迹形式的布尔函数 $g_{a,b,c,d}^{(r,s)}(x)=Tr_1^n\left(ax^{r\left(2^m-1\right)}\right)+Tr_1^2\left(bx^{\left(2^n-1\right)/3}\right)+Tr_1^n\left(cx^{\left(2^m-1\right)/2+1}\right)+Tr_1^n\left(dx^{\left(2^m-1\right)s+1}\right)$ 及 $f_{a,b}^{(r)}(x)=Tr_1^n\left(ax^{r\left(2^m-1\right)}\right)+Tr_1^2\left(bx^{\left(2^n-1\right)/3}\right)$，其中 $n=2m$ 且 m 为奇数，r 是一个正整数且 $s\in\{0,1/4,1/6,3\}$，$a\in F_{2^n}^*, b\in F_4^*, c\in F_{2^n}$ 及 $d\in F_2, x\in F_{2^n}$。在文献[1]中，S. Mesnager 已经讨论了当 $r=3$ 或者 $\left(r,2^m+1\right)=1$ 时，函数 $g_{a,b,c,d}^{(r,s)}$ 可能成为 semi-Bent 的情形。在本文中，我们将取消对 r 的任何的限制条件，进一步的讨论函数 $g_{a,b,c,d}^{(r,s)}$ 成为 semi-Bent 函数的条件。在推广结论的过程中，我们要借助于 Kloosterman 和以及 Cubic 和这两样工具。

关键词：布尔函数；Semi-Bent 函数；Walsh-Hadamard 转换；Kloosterman 和；Cubic 和

1. 引言

Bent 函数是 Rothus[2]于 1976 年提出的一类特殊的布尔函数，它满足到所有的仿射函数的汉明距离都等于 $2^{n-1}\pm 2^{n/2-1}$，Bent 函数仅存在于变量个数为偶数的情形。Bent 函数由于其在代数及组合学方面的良好性质以及在密码和编码理论及序列等方面的多重应用而被广泛研究。Bent 函数的定义是比较简单的，但是需要特别强调的是，在当前的数学水平下想要对它们进行明确的分类是不可行的。因此，想要尽可能多的了解它们，找出构造方法就显得尤为重要。

Semi-Bent 函数的概念于 1994 年由 Chee、Lee 及 Kim[3]在亚洲的一个重要的密码学会议 Asiacrypt 上提出。和 Bent 函数一样，semi-Bent 函数也由于其拥有的一系列优异的性质而被广泛的研究[4]。但是与 bent 函数不同的是，semi-Bent 函数对于变量个数的奇偶性没有限制。当 n 取奇数的时候，semi-Bent 函数的 Walsh-Hadamard 转换的值为 0 或者 $\pm 2^{(n+1)/2}$；当 n 取偶数的时候，semi-Bent 函数的 Walsh-Hadamard 转换的值为 0 或者 $\pm 2^{(n+2)/2}$。在本文中，我们只研究变量个数为偶数的 semi-Bent 函数。Semi-Bent 函数都是平衡函数并且在平衡且达到稳定的函数中具有极大非线性性[5,6]。读者可以阅读文献[7]去了解平衡布尔函数的更多的性质。迄今为止，几乎所有的 semi-Bent 函数都是由选择合适的 d 的幂多项式 $Tr_1^n\left(x^d\right)$ 导出的[8,9]。

本文的主要结构如下：第二节介绍一下必要的基础知识；第三节明确一些特定的记号以及归纳总结一些基本定理；在第四节中，我们将对一类含有多项式迹形式的 semi-Bent 函数进行推广。

2. 背景知识简介

令 F_{2^n} 是含有 2^n 个元素的有限域，$F_{2^n}^*$ 是它的所有非零元素构成的乘法群。在本文中我们主要讨论位于 F_{2^n} 或者是 F_{2^n} 的子域上的布尔函数。

2.1. 布尔函数的迹表示

设 m， n 是正整数并且满足 m 整除 n 时，我们用 Tr_m^n 表示从 F_{2^n} 到 F_{2^m} 的迹函数，即

$$Tr_m^n\left(x\right)=x+x^2+\cdots+x^{2^{n-m}},\forall x\in F_{2^n}$$

特别地，当 $m=1$ 时，称为绝对迹函数，它满足性质 $Tr_1^n=Tr_1^m\cdot Tr_m^n$。

有限域 F_{2^n} 上的每个非零布尔函数 $f\left(x\right)$ 都有如下形式的迹表示：

$$f\left(x\right)=\sum_{j\in\Gamma_n}Tr_1^{o(j)}\left(a_jx^j\right)+e\left(1+x^{2^n-1}\right),\forall x\in F_{2^n}.$$

其中，Γ_n 表示从 2 模 2^n-1 的每个分圆陪集中选取一个代表元所形成的整数的集合，$o\left(j\right)$ 表示包含元素 j 的上述分圆陪集的大小且 $a_j\in F_{2^{o(j)}}$，e 的值为 0 或 1。因为布尔函数的迹表示是唯一的，所以它又被称为布尔函数的多项式形式。

2.2. Walsh 变换，Semi-Bent 函数的定义

定义 2.2.1 有限域 F_{2^n} 上的布尔函数 $f\left(x\right)$ 的 Walsh 变换定义为

$$\hat{\chi}_f\left(\omega\right)=\sum_{x\in F_{2^n}}\chi\left(f\left(x\right)+Tr_1^n\left(\omega x\right)\right),\forall\omega\in F_{2^n}$$

其中 χ 满足对于 $\forall x\in F_{2^n},\chi\left(x\right)=\left(-1\right)^x$。

利用 Walsh 变换，我们可以给出 semi-Bent 函数的定义[3,10]。

定义 2.2.2 设 $f\left(x\right)$ 是 F_{2^n} 到 F_2 的函数。当 n 为偶数时，若对于 $\forall\omega\in F_{2^n}$，都有 $\hat{\chi}_f\left(\omega\right)\in\left\{0,\pm 2^{(n+2)/2}\right\}$，则称 $f\left(x\right)$ 是 semi-Bent 函数；当 n 为奇数时，若对于 $\forall\omega\in F_{2^n}$ 都有 $\hat{\chi}_f\left(\omega\right)\in\left\{0,\pm 2^{(n+1)/2}\right\}$，则也称 $f\left(x\right)$ 是 semi-Bent

函数。

2.3. 极分解、Kloosterman 和、Cubic 和

设 $U=\left\{x\in F_{2^n}^*\,\middle|\,x^{2^m+1}=1\right\}$，则 U 是有限域 F_{2^n} 的循环群的一个阶为 2^m+1 的子群。根据有限域的知识可知，F_{2^n} 的每一个非零元素 x 都有唯一的分解：$x=uy$，其中 $u\in U, y\in F_{2^m}^*$。

定义 2.3.1 有限域 F_{2^n} 上的 Kloosterman 和定义为

$$K_m(a)=\sum_{x\in F_{2^m}}\chi\left(Tr_1^m\left(ax+\frac{1}{x}\right)\right),\ a\in F_{2^m}$$

其中，当 $x=0$ 时，我们规定 $\chi\left(Tr_1^m\left(\frac{1}{x}\right)\right)=1$。

Lachaud 和 Wolfman 已经计算出了 F_{2^m} 上的 Kloosterman 和取值范围。

引理 1[11] 对于 $\forall a\in F_{2^m}$，$K_m(a)$ 的值 s 满足 $s\in\left[-2^{m/2+1}+1,2^{m/2+1}+1\right]$ 及 $s\equiv 0\pmod 4$。

定义 2.3.2 有限域 F_{2^m} 上的 Cubic 和定义为

$$C_m(a,b)=\sum_{x\in F_{2^m}}\chi\left(Tr_1^m\left(ax^3+bx\right)\right),\ a\in F_{2^m}, b\in F_4。$$

读者可以参考文献[12]去了解更多的关于 Cubic 和的取值问题。

3. 循环群 U 上的特征和

在本文中，我们总是假设 $n=2m$, m 为奇数。设 α 是 $F_{2^n}^*$ 的一个本原元，则 U 是由 $\varsigma=\alpha^{2^m-1}$ 生成的一个循环群并且 $\beta=\alpha^{\frac{2^n-1}{3}}$ 是 U 的一个 3 次单位根。设 $V=\left\{u^3\,\middle|\,u\in U\right\}$，则 U 可以表示为如下形式：$U=\bigcup_{i=0}^{2}\varsigma_i V$。

函数 $f_{a,b}^{(r)}(x)=Tr_1^n\left(ax^{r\left(2^m-1\right)}\right)+Tr_1^2\left(bx^{\frac{2^n-1}{3}}\right)$，$a\in F_{2^n}^*, b\in F_4$，$x\in F_{2^n}$ 我们定义如下形式的记号：

$$\Lambda_r\left(f_{a,b}\right)=\sum_{u\in U}\chi\left(f_{a,b}^{(r)}(u)\right),\quad S_i^r=\sum_{v\in V}\chi\left(f_{a,0}^{(r)}\left(\varsigma^i v\right)\right),$$

则有

$$S_0^r+S_1^r+S_2^r=\sum_{u\in U}\chi\left(f_{a,0}^{(r)}(u)\right)=\Lambda_r\left(f_{a,0}\right).$$

当 $r=1$ 时，记 $S_i^1=S_i$。特别的，对于任意的整数 i，我们有 $S_i^{(r)}=S_{i(\bmod 3)}^{(r)}$。

由定理[1,11,13]，我们可以总结出下面的结论。

引理 3 设 r 是一个正整数且满足 $\left(r,2^m+1\right)=1$。设 $a\in F_{2^m}$，则

1) $\Lambda_r\left(f_{a,0}\right)=1-K_m(a)$；

2) $S_0^r=S_0=\left(1+C_m(a,a)-K_m(a)\right)/3$；

3) $S_1^r=S_2^r=\left(1-C_m(a,a)-K_m(a)\right)/3$。

4. 主要结论

本节中，我们主要讨论 r 在没有任何限制条件的情形下 $\Lambda_r\left(f_{a,b}\right)$ 的取值情况。

引理 4.1 设 $n=2m$, m 为奇数。设 $b\in F_4^*$，$a\in F_{2^m}^*$ 且 ς 是 U 的生成元。如果 $\left(r,\left(2^m+1\right)/3\right)\neq 1$，那么

$\Lambda_r\left(f_{a,b}\right)\neq 1$。

证明：假设$\left(r,\left(2^m+1\right)/3\right)=d\neq 1$，那么映射$u\mapsto u^d$是$U$上的一个$d$对1映射。因为$\left(2^m-1,2^m+1\right)=1$，所以

$$\begin{aligned}\Lambda_r\left(f_{a,b}\right)&=\sum_{u\in U}\chi\left(Tr_1^n\left(au^r\right)+Tr_1^2\left(bu^{\left(2^m+1\right)/3}\right)\right)\\&=d\sum_{u\in U}\chi\left(Tr_1^n\left(au^{r/d}\right)+Tr_1^2\left(bu^{\left(2^m+1\right)/3d}\right)\right).\end{aligned}$$

由于$\sum_{u\in U}\chi\left(Tr_1^n\left(au^{r/d}\right)+Tr_1^2\left(bu^{\left(2^m+1\right)/3d}\right)\right)$的值为正整数且$d$为整数，所以$\Lambda_r\left(f_{a,b}\right)\neq 1$。

假设$\left(r,\left(2^m+1\right)/3\right)=1$，我们继续讨论$\wedge_r\left(f_{a,b}\right)$的取值情况。

定理 4.2 设$n=2m$, m为奇数。设ς是U的生成元。设$b\in F_4^*$，$a\in F_{2^n}^*$满足$a=a'\varsigma^j v'$，其中$a'\in F_{2^m}^*$，$v'\in V$且$j\in\{0,1,2\}$。当$\left(r,\left(2^m+1\right)/3\right)=1$时，下述结论成立。

1) 若$r\equiv 0\left(\mathrm{mod}3\right)$，则$\Lambda_r\left(f_{a,b}\right)=-S_j$。

2) 若$r\equiv 1\left(\mathrm{mod}3\right)$，则下列结论成立：

a) $j=0$，$b\neq 1$时，$\Lambda_r\left(f_{a,b}\right)=-S_0$；

当$j=0$，$b=1$时，$\Lambda_r\left(f_{a,b}\right)=S_0-2S_1$。

b) $j=1, b\neq\beta$时，$\Lambda_r\left(f_{a,b}\right)=-S_0$；当$j=1, b=\beta$时，$\Lambda_r\left(f_{a,b}\right)=S_0-2S_1$。

c) $j=2$，$b\neq\beta^2$时，$\Lambda_r\left(f_{a,b}\right)=-S_0$；当$j=2$，$b=\beta^2$时，$\Lambda_r\left(f_{a,b}\right)=S_0-2S_1$。

3)若$r\equiv 2\left(\mathrm{mod}3\right)$，则下列结论成立：

a) $j=0$，$b\neq 1$时，$\Lambda_r\left(f_{a,b}\right)=-S_0$；当$j=0, b=1$时，$\Lambda_r\left(f_{a,b}\right)=S_0-2S_1$。

b) $j=1$，$b\neq\beta^2$时，$\Lambda_r\left(f_{a,b}\right)=-S_0$；当$j=1$，$b=\beta^2$时，$\Lambda_r\left(f_{a,b}\right)=S_0-2S_1$。

c) $j=2$，$b\neq\beta$时，$\Lambda_r\left(f_{a,b}\right)=-S_0$；当$j=2$，$b=\beta$时，$\Lambda_r\left(f_{a,b}\right)=S_0-2S_1$。

证明：因为$\left(r,\left(2^m+1\right)/3\right)=1$，所以映射$v\mapsto v^{r\left(2^m-1\right)}$是$V$上的一个置换。由于$2^m+1\equiv 0\left(\mathrm{mod}3\right)$，我们有$2^m-1\equiv 1\left(\mathrm{mod}3\right)$。又因为$\varsigma=\alpha^{2^m-1}$，$\beta=\alpha^{\left(2^n-1\right)/3}$，则$\varsigma^{r\left(2^m-1\right)}=\varsigma^{-3r}\cdot\varsigma^r=v_1\varsigma^r$，其中$v_1\in V$。我们有

$$\begin{aligned}&\Lambda_r\left(f_{a,b}\right)\\&=\sum_{i=0}^{2}\sum_{v\in V}\chi\left(Tr_1^n\left(a\left(\varsigma^i v\right)^{r\left(2^m-1\right)}\right)+Tr_1^2\left(b\left(\varsigma^i v\right)^{\frac{2^n-1}{3}}\right)\right)=\sum_{i=0}^{2}\chi\left(Tr_1^2\left(b\beta^i\right)\right)\sum_{v\in V}\chi\left(Tr_1^n\left(a\varsigma^{ir\left(2^m-1\right)}v^r\right)\right)\\&=\sum_{i=0}^{2}\chi\left(Tr_1^2\left(b\beta^i\right)\right)\sum_{v\in V}\chi\left(Tr_1^n\left(a\varsigma^{ir}v\right)\right)=\sum_{i=0}^{2}\chi\left(Tr_1^2\left(b\beta^i\right)\right)\sum_{v\in V}\chi\left(Tr_1^n\left(a'\varsigma^{ir+j}v\right)\right)\end{aligned}$$

1) 若$r\equiv 0\left(\mathrm{mod}3\right)$，则$\varsigma^r\in V$且$v\mapsto\varsigma^r v$是$V$上的一个置换。由特征的正交关系可得$\sum_{i=0}^{2}\chi\left(Tr_1^2\left(b\beta^i\right)\right)=-1$。所以，

$$\Lambda\left(f_{a,b}\right)=\sum_{i=0}^{2}\chi\left(Tr_1^2\left(b\beta^i\right)\right)\sum_{v\in V}\chi\left(Tr_1^n\left(a'\varsigma^j v\right)\right)=-S_j.$$

2) 若$r\equiv 1\left(\mathrm{mod}3\right)$，则假设$r=3k+1$，那么有$\varsigma^{ir}=v'\varsigma^j$，$v'\in V$。因此，

$$\Lambda_r\left(f_{a,b}\right)=\sum_{i=0}^{2}\chi\left(Tr_1^2\left(b\beta^i\right)\right)\sum_{v\in V}\chi\left(Tr_1^n\left(a'\varsigma^{i+j}v\right)\right)$$

因为 $\beta=\alpha^{\left(2^n-1\right)/3}$ 且 $\beta^2+\beta+1=0$，所以当 $b=1$ 时，我们有 $\chi\left(Tr_1^n\left(b\beta\right)\right)=\chi\left(Tr_1^n\left(b\beta^2\right)\right)=-1$ 且 $\chi\left(Tr_1^n\left(b\right)\right)=1$；当 $b\neq 1$ 时，$\chi\left(Tr_1^n\left(b\right)\right)=-1$ 以及 $\chi\left(Tr_1^n\left(b\beta\right)\right)+\chi\left(Tr_1^n\left(b\beta^2\right)\right)=0$。

因此，1) 当 $j=0$ 时，

$$\Lambda_r\left(f_{a,b}\right)=\sum_{i=0}^{2}\chi\left(Tr_1^2\left(b\beta^i\right)\right)\sum_{v\in V}\chi\left(Tr_1^n\left(a'\varsigma^i v\right)\right)$$

a) 当 $b=1$ 时，根据 1)中的讨论内容，有 $\Lambda_r\left(f_{a,b}\right)=S_0-S_1-S_2=S_0-2S_1$；

b) 类似地，当 $b=\beta$ 时，我们有 $\Lambda_r\left(f_{a,b}\right)=-S_0-S_1+S_2=-S_0$；

c) 当 $b=\beta^2$ 时，$\Lambda_r\left(f_{a,b}\right)=-S_0+S_1-S_2=-S_0$。

2) 当 $j=1$ 时，

$$\Lambda_r\left(f_{a,b}\right)=\sum_{i=0}^{2}\chi\left(Tr_1^2\left(b\beta^i\right)\right)\sum_{v\in V}\chi\left(Tr_1^n\left(a'\varsigma^{i+1} v\right)\right)$$

a) 若 $b=1$，则 $\Lambda_r\left(f_{a,b}\right)=S_1-S_2-S_0=-S_0$；

b) 若 $b=\beta$，则 $\Lambda_r\left(f_{a,b}\right)=-S_1-S_2+S_0=S-2S_1$；

c) 若 $b=\beta^2$，则 $\Lambda_r\left(f_{a,b}\right)=-S_1+S_2-S_0=-S_0$。

3) 当 $j=2$ 时，

$$\Lambda_r\left(f_{a,b}\right)=\sum_{i=0}^{2}\chi\left(Tr_1^2\left(b\beta^i\right)\right)\sum_{v\in V}\chi\left(Tr_1^n\left(a'\varsigma^{i+2} v\right)\right)$$

a) 若 $b=1$，则 $\Lambda_r\left(f_{a,b}\right)=S_2-S_1-S_0=-S_0$；

b) 若 $b=\beta$，则 $\Lambda_r\left(f_{a,b}\right)=-S_2-S_0+S_1=-S_0$；

c) 若 $b=\beta^2$，则 $\Lambda_r\left(f_{a,b}\right)=-S_2+S_0-S_1=S_0-2S_1$。

3) 若 $r\equiv 2\left(\mathrm{mod}3\right)$，则假设 $r=3k+2$，我们有 $\varsigma^{ir}=v''\varsigma^{2i}$，$v''\in V$。因此，$\Lambda_r\left(f_{a,b}\right)=\sum_{i=0}^{2}\chi\left(Tr_1^2\left(b\beta^i\right)\right)\sum_{v\in V}\chi\left(Tr_1^n\left(a'\varsigma^{2i+j} v\right)\right)$ 使用类似于 2)的讨论方法即可得出结论，在此我们省略具体步骤。

由文献[1]的推论 1、推论 2，以及本文的引理 3.1、定理 4.2，我们可以得到下面的结论。

推论 4.3 设 $n=2m$, m 为奇数。设 ς 是 U 的生成元。设 $b\in F_4^*$，$a\in F_{2^n}^*$ 满足 $a=a'\varsigma^j v'$，其中 $a'\in F_{2^m}^*$，$v'\in V$ 且 $j\in\{0,1,2\}$。当 $\left(r,\left(2^m+1\right)/3\right)=1$ 时，则 $\Lambda_r\left(f_{a,b}\right)=1$ 当且仅当

1) 若 $r\equiv 1\left(\mathrm{mod}3\right)$ 或者 $r\equiv 2\left(\mathrm{mod}3\right)$，则 $K_m\left(a'\right)=4$；

2) 若 $r\equiv 0\left(\mathrm{mod}3\right)$，则

a) 当 $j=0$ 时，$K_m\left(a'\right)=4$；

b) 当 $j\neq 0$ 时，$K_m\left(a'\right)+C_m\left(a',a'\right)=4$。

现在我们对文献[1]中的 semi-Bent 函数作推广，在此之前我们先定义一个位于有限域 F_{2^n} 上的布尔函数。这个布尔函数的表达式为

$$g_{a,b,c,d}^{(r,s)}\left(x\right)=Tr_1^n\left(ax^{r\left(2^m-1\right)}\right)+Tr_1^2\left(bx^{\left(2^n-1\right)/3}\right)+Tr_1^n\left(cx^{\left(2^m-1\right)/2+1}\right)+Tr_1^n\left(dx^{\left(2^m-1\right)s+1}\right)$$

其中，r 是整数，$a\in F_{2^n}^*, b\in F_4^*, c\in F_{2^n}$ 及 $d\in F_2$ $s\in\{0,1/4,1/6,3\}$。需要说明的是，在此我们只讨论 $d=0$ 时的情形，至于 $d=1$ 时的情形，推广的结果同样成立。

定理 4.4 设 $n=2m$, m 为奇数。设 ς 是 U 的生成元。设 $c\in F_{2^n}^*\setminus F_{2^m}$，$b\in F_4^*$，$a\in F_{2^n}^*$ 满足 $a=a'\varsigma^j v'$，其中

$a' \in F_{2^m}^*$， $v' \in V$ 且 $j \in \{0,1,2\}$。

1) 若 $\left(r,\left(2^m+1\right)/3\right) \neq 1$，则 $g_{a,b,c,d}^{(r,s)}$ 不是 semi-Bent 函数。

2) 若 $\left(r,\left(2^m+1\right)/3\right) = 1$，则 $g_{a,b,c,0}^{(r,s)}$ 是 semi-Bent 函数的充要条件是

①若 $r \equiv 1 \pmod 3$ 或者 $r \equiv 2 \pmod 3$，则 $K_m(a') = 4$；

②若 $r \equiv 0 \pmod 3$，则

a) 当 $j = 0$ 时， $K_m(a') = 4$；

b) 当 $j \neq 0$ 时， $K_m(a') + C_m(a', a') = 4$。

5. 结束语

本文主要是对一类含有多项式迹形式的位于有限域 F_{2^n} 中的 semi-Bent 函数作进一步的推广，使得这一类的 semi-Bent 函数具有更广泛的形式及更少的限制条件，这样更有助于具有此类形式的 semi-Bent 函数在编码理论等方面的应用。

参考文献 (References)

[1] S. Mesnager. Semi-Bent functions from Dillon and Niho exponnets, Kloosterman sums and Dickson polynomials. IEEE Transactions on Information Theory, 2011, 57(11): 7443-7458.

[2] O. S. Rothus. On “bent” functions. Journal of Combinatorial Theory, Series A, 1976, 20: 300-305.

[3] S. Chee, S. Lee and K. Kim. Semi-Bent functions. Advances in cryptology-Asiacrypt 94. In: J. Pieprzyk, R. Safavi-Naini, Eds., Proceedings of the 4th International Conference on the Theory and Applications of Cryptology, Wollongong, Australia. Lecture Notes on Computer Science, 1994, 917: 107-118.

[4] X. Y. Zeng, C. Carlet, J. Y. Shan and L. Hu. More balanced Boolean functions with optimal algebraic immunity and nonlinearity and resistance to fast algebraic attacks. IEEE Transactions on Information Theory, 2011, 57(9): 6310-6320.

[5] Y. Zheng, X. M. Zhang. Plateaued functions. Advances in Cryptology-ICICS Lecture Notes in Computer Science. Berlin, Germany: Springer-Verlag, 1999, 1726: 284-300.

[6] Y. Zheng, X. M. Zhang. Relationships between bent functions and complementary plateaued functions. Lecture Notes on Computer Science, 1999, 1787: 60-67.

[7] X. Y. Zeng, L. Hu. Constructing Boolean functions by modifying Maiorana-McFarland's superclass functions. IEICE Transactions on Fundamentals, 2005, 88(1): 59-66.

[8] P. Charpin, E. Pasalic and C. Tavernier. On bent and semi-Bent quadratic Boolean functions. IEEE Transactions on Information Theory, 2005, 51(12): 4286-4298.

[9] G. Sun, C. Wu. Construction of semi-Bent Boolean functions in even number of variables. Chinese Journal of Electronics, 2009, 18(2): 231-237.

[10] J. H. Cheon, S. Chee. Elliptic curves and resilient functions. Lecture Notes on Computer Science, 2000, 2015: 386-397.

[11] G. Lachaud, J. Wolfmann. The weights of the orthogonals of the extended quadratic binary Goppa codes. IEEE Transaction s on Information Theory, 1990, 36(3): 686-692.

[12] L. Carlitz. Explicit evaluation of certain exponential sums. Mathematica Scandinavica, 1979, 44(1): 5-16.

[13] P. Charpin, T. Helleseth and V. Zinoviev. Divisibility properties of Kloosterman sums over finite fields of characteristic two. Toronto: In ISIT, 2008: 2608-2612.

