三类 Semi-Bent 函数的构造

何业锋[1,2],马文平[1]
(1.西安电子科技大学计算机网络与信息安全教育部重点实验室,陕西西安 710071;
2.西安邮电学院通信与信息工程学院,陕西西安 710121)

摘 要: Semi-bent 函数是一种具有高非线性度的布尔函数,它们在密码和通信领域中都有重要的应用价值.本文构造了三类由迹函数表示的 semi-bent 函数.证明了当限制某些参数的取值范围时,这些新构造函数的 semi-bent 性与 Kloosterman 和密切相关.并且证明了每一类新构造的含有 n 个变元的 semi-bent 函数,都存在一个 semi-bent 函数的子类,它们的代数次数是 $n/2$.利用 Kloosterman 和的零点,也给出了小域上 semi-bent 函数的例子.

关键词: 布尔函数; semi-bent 函数; Hadamard 变换; Kloosterman 和
中图分类号: TN918.1 **文献标识码:** A **文章编号:** 0372-2112 (2011) 01-0233-04

Constructions of Three Classes of Semi-Bent Functions

HE Ye-feng[1,2], MA Wen-ping[1]
(1. *Ministry of Education Key Laboratory of Computer Network and Information Security, Xidian University, Xi'an, Shaanxi* 710071, *China*;
2. *School of Communication and Information Engineering, Xi'an Institute of Post & Telecommunications, Xi'an, Shaanxi* 710121, *China*)

Abstract: Semi-bent functions are a kind of Boolean functions with high nonlinearity. They have important applications in cryptography and communications. This paper gives three classes of semi-bent functions represented by trace. It is shown that the semi-bentness of the new functions is closely related to Kloosterman sums when the values of some parameters are restricted. It is also proved there exists a subclass of semi-bent functions with degree $n/2$ in each class of the new semi-bent functions on n variables. Several examples of the semi-bent functions in a small field are given by using the zeros of some Kloosterman sums.

Key words: Boolean function; semi-bent function; Hadamard transform; Kloosterman sums

1 引言

有限域 F_{2^n} 上的 semi-bent 函数[1,2]具有非常低的 Hadamard 变换值,因此它们拥有很高的非线性度.特别当 n 是偶数时,semi-bent 函数的非线性度仅次于 bent 函数[3].由于高非线性度的密码函数能很好的抵抗线性密码分析[4],因此 semi-bent 函数一直都受到密码工作者的高度关注.另一方面,semi-bent 函数也相应于一些有趣的序列,这些序列和 m 序列之间有很低的互相关值.并且,有些 semi-bent 函数也可以直接用来构造拥有三值互相关谱的序列簇.例如,Gold 序列[5]和 Gold-like 序列[6],它们都是已知的具有最优相关函数的二元序列簇.因此,semi-bent 函数在通信领域也有很广泛的应用.目前,研究者在寻找 semi-bent 函数方面已经做了很多工作[1,2,5~8].然而,现有的由基本构造得到的 semi-bent 函数大多数是低次布尔函数.因此,并不适合用于流密码的滤波生成器中.在本文中,我们构造了三类具有较高代数次数的 semi-bent 函数.并且在某些限制条件下,这些函数的 semi-bent 性与 Kloosterman 和[9]密切相关.

2 基础知识

令 F_{2^n} 是含有 2^n 个元素的有限域,$F_{2^n}^*$ 是它的乘法群.根据有限域 F_{2^n} 的基底可知,从 F_{2^n} 到 F_2 的函数 $f(x)$ 等价于从 F_2^n 到 F_2 的布尔函数.函数 $f(x)$ 的汉明重量定义为 $wt(f)=|\{x\in F_{2^n}|f(x)=1\}|$.若函数 $f(x)$ 的汉明重量为 2^{n-1},则称 $f(x)$ 是平衡函数.任意一个函数 $f(x)$ 都可以表示成一些迹函数的和.当正整数 m 整除 n 时,一个从 F_{2^n} 到 F_{2^m} 的迹函数记为 $Tr_m^n(x)$,即

$$Tr_m^n(x)=x+x^{2^m}+\cdots+x^{2^{(\frac{n}{m}-1)m}}.$$

当 $m=1$ 时,称它为绝对迹函数.迹函数有下面的性质:

(1) $\forall x\in F_{2^n}$,有 $Tr_m^n(x^{2^m})=Tr_m^n(x)$.

(2) $\forall x,y\in F_{2^n}$, $\forall a,b\in F_{2^m}$,有 $Tr_m^n(ax+by)=aTr_m^n(x)+bTr_m^n(y)$.

收稿日期:2009-11-28;修回日期:2010-04-12
基金项目:国家自然科学基金(No.60773002);国家 863 高技术研究发展计划(No.2007AA01Z472);大唐移动通信资助基金

设 e 是一个整数且 $0\leqslant e\leqslant 2^n-1$,则 e 的 2 - 重指的是它的 2 元表示的系数和,记为 $\omega_2(e)$. 利用 $\omega_2(e)$ 可以定义由迹函数表示的布尔函数的代数次数. 例如,函数 $Tr_1^n(x^e)$ 的代数次数可以定义为 $\omega_2(e)$. 函数 $f(x)$ 的 Hadamard 变换是 F_{2^n} 上的一个实值函数,其定义为

$$\hat{f}(\lambda)=\sum_{x\in F_{2^n}}(-1)^{f(x)+Tr_1^n(\lambda x)},\lambda\in F_{2^n}$$

利用 Hadamard 变换值,可以方便地给出 semi-bent 函数的定义.

定义 1 设 n 是偶数,$f(x)$是一个从 F_{2^n}到 F_2 的函数. 若对于 $\forall\lambda\in F_{2^n}$,都有 $\hat{f}(\lambda)\in\{0,\pm 2^{(n+2)/2}\}$,则称 $f(x)$是 semi-bent 函数.

Kloosterman 和也是有限域 F_{2^n}上的实值函数,它的定义如下:

定义 2 有限域 F_{2^n}上的 Kloosterman 和为

$$K_n(a)=\sum_{x\in F_{2^n}}(-1)^{Tr_1^n(ax+x^{-1})},a\in F_{2^n}$$

其中 $Tr_1^n(0^{-1})=0$.

在接下来的论文中,我们假设 $n=2m$. 设 $U=\{u\in F_{2^n}\mid u^{2^m+1}=1\}$, 则 U 是一个由所有 2^m+1 次单位根构成的群,且 $|U|=2^m+1$. 显然,$U\bigcap F_{2^m}=\{1\}$. 根据有限域的知识知,$F_{2^n}^*$中的每一个元素 x 都有唯一的分解:$x=uy$,其中 $u\in U$ 且 $y\in F_{2^m}^*$.

下面介绍 F_{2^n}上的三个函数[10],这三个函数在群 U 上根的个数均为 0 或 2.

引理 1[10] 设 $\lambda\in F_{2^n}$,定义 F_{2^n}上的函数为:

$g_{i,\lambda}(u)=u^{1-2s_i}+(u^{1-2s_i})^{2^m}+\lambda u+(\lambda u)^{2^m}+1(i=1,2,3)$,其中 $s_1=3,s_2=1/4,s_3=1/6$,而 1/4 和 1/6 分别为 4 和 6 模 2^m+1 的逆元. 则有下述结论成立:

(1)对于任意 m,等式 $g_{1,\lambda}(u)=0$ 在群 U 上解的个数为 0 或 2.

(2)当 m 是奇数时,等式 $g_{2,\lambda}(u)=0$ 在群 U 上解的个数为 0 或 2.

(3)当 m 是偶数时,等式 $g_{3,\lambda}(u)=0$ 在群 U 上解的个数为 0 或 2.

在本文中,我们可以利用这些特殊函数来构造 semi-bent 函数.

3 Semi-Bent 函数的构造

设 $d_i=(2^m-1)\cdot s_i+1(i=1,2,3)$,其中 s_i 与引理 1 中的定义相同. 下面给出三类 semi-bent 函数的构造.

定理 1 设 r 是一个正整数且 $\gcd(r,2^m+1)=1$. 设 $a,b\in F_{2^n}^*$且 $b+b^{2^m}=1$. 定义 F_{2^n}上的函数为

$$f_i(x)=Tr_1^n(ax^{r(2^m-1)})+Tr_1^n(bx^{2^{m-1}(2^m+1)})+Tr_1^n(x^{d_i})$$

其中 $i=1,2,3$. 令 $h(u)=Tr_1^n(au^{r(2^m-1)})$,则有下述结论成立:

(1)对于任意 m,$f_1(x)$是 semi-bent 函数当且仅当 $|\{u\in U\mid h(u)=1\}|=2^{m-1}$.

(2)当 m 是奇数时,$f_2(x)$是 semi-bent 函数当且仅当 $|\{u\in U\mid h(u)=1\}|=2^{m-1}$.

(3)当 m 是偶数时,$f_3(x)$是 semi-bent 函数当且仅当 $|\{u\in U\mid h(u)=1\}|=2^{m-1}$.

证明 显然有 $f_i(0)=0$. 既然 $F_{2^n}^*$中的每一个元素 x 都可以唯一的分解为 $x=uy$,其中 $u\in U$ 而 $y\in F_{2^m}^*$,因此我们能计算 $f_i(x)$的 Hadamard 变换如下:

$$\begin{aligned}\hat{f}_i(\lambda)&=\sum_{x\in F_{2^n}}(-1)^{Tr_1^n(ax^{r(2^m-1)})+Tr_1^n(bx^{2^{m-1}(2^m+1)})}\\&\quad\cdot(-1)^{Tr_1^n(x^{d_i})+Tr_1^n(\lambda x)}\\&=1+\sum_{x\in F_{2^n}^*}(-1)^{Tr_1^n(ax^{r(2^m-1)})+Tr_1^n(bx^{2^{m-1}(2^m+1)})}\\&\quad\cdot(-1)^{Tr_1^n(x^{d_i})+Tr_1^n(\lambda x)}\\&=1+\sum_{u\in U}\sum_{y\in F_{2^m}^*}(-1)^{Tr_1^n(a(uy)^{r(2^m-1)})}\\&\quad\cdot(-1)^{Tr_1^n(b(uy)^{2^{m-1}(2^m+1)})+Tr_1^n((uy)^{d_i})+Tr_1^n(\lambda uy)}\\&=1+\sum_{u\in U}\sum_{y\in F_{2^m}^*}(-1)^{Tr_1^n(au^{r(2^m-1)})+Tr_1^n(by)}\\&\quad\cdot(-1)^{Tr_1^n(u^{1-2s_i}y)+Tr_1^n(\lambda uy)}\\&=1-\sum_{u\in U}(-1)^{h(u)}+\sum_{u\in U}(-1)^{h(u)}\\&\quad\cdot\sum_{y\in F_{2^m}}(-1)^{Tr_1^n(by)+Tr_1^n(u^{1-2s_i}y)+Tr_1^n(\lambda uy)}\\&=1-\sum_{u\in U}(-1)^{h(u)}+\sum_{u\in U}(-1)^{h(u)}\\&\quad\cdot\sum_{y\in F_{2^m}}(-1)^{Tr_1^m[Tr_m^n(b+u^{1-2s_i}+\lambda u)\cdot y]}\end{aligned}$$

如果 $g_{i,\lambda}(u)=Tr_m^n(b+u^{1-2s_i}+\lambda u)\neq 0$,则 $Tr_1^m[Tr_m^n(b+u^{1-2s_i}+\lambda u)\cdot y]$是域 F_{2^m}上关于变元 y 的平衡函数. 因此,

$$\hat{f}_i(\lambda)=1-\sum_{u\in U}(-1)^{h(u)}+2^m\cdot\sum_{u\in U,g_{i,\lambda}(u)=0}(-1)^{h(u)}$$

既然有 $b+b^{2^m}=1$,故 $g_{i,\lambda}(u)=u^{1-2s_i}+(u^{1-2s_i})^{2^m}+\lambda u+(\lambda u)^{2^m}+1$. 由引理 1 知,对于任意 $\lambda\in F_{2^n}$,等式 $g_{i,\lambda}(u)=0$在群 U 上解的个数为 0 或 2(其中 m 在相应的限制条件下). 当 $g_{i,\lambda}(u)=0$ 的解的个数为 0 时,我们有

$$\hat{f}_i(\lambda)=1-\sum_{u\in U}(-1)^{h(u)}.$$

否则,当 $g_{i,\lambda}(u)=0$ 的解的个数为 2 时,分别记它的两个解为 u_1 和 u_2. 根据 $h(u_1)$和 $h(u_2)$的取值不同,$f_i(x)$的 Hadamard 变换值分为 3 种情况:

(1)若 $h(u_1)\neq h(u_2)$,则

$$\hat{f}_i(\lambda) = 1 - \sum_{u\in U}(-1)^{h(u)}.$$

(2)若 $h(u_1)=h(u_2)=0$,则

$$\hat{f}_i(\lambda) = 1 - \sum_{u\in U}(-1)^{h(u)} + 2^{m+1}.$$

(3)若 $h(u_1)=h(u_2)=1$,则

$$\hat{f}_i(\lambda) = 1 - \sum_{u\in U}(-1)^{h(u)} - 2^{m+1}.$$

因此,$\hat{f}_i(\lambda)\in\{0,\pm 2^{(n+2)/2}\}$ 当且仅当 $1-\sum_{u\in U}(-1)^{h(u)}=0$,即 $f_i(x)$ 是 semi-bent 函数当且仅当 $|\{u\in U\mid h(u)=1\}|=2^{m-1}$.

当参数 a 限制在 F_{2^n} 的子域上时,函数 $f_i(x)$ 的 semi-bent 性与 Kloosterman 和的取值密切相关.

推论 1　若 $a\in F_{2^m}^*$,则 $f_i(x)$ 是 semi-bent 函数当且仅当 $K_m(a)=0$,其中 m 的要求与定理 1 相同.

证明　根据定理 1 的证明知,$f_i(x)$ 是 semi-bent 当且仅当 $\sum_{u\in U}(-1)^{Tr_1^n(au^{r(2^m-1)})}=1$. 既然 $\gcd(r,2^m+1)=1$ 且 $\gcd(2^m-1,2^m+1)=1$,因此函数 $u\to u^{r(2^m-1)}$ 是群 U 到其自身的双射. 因此 $\sum_{u\in U}(-1)^{Tr_1^n(au^{r(2^m-1)})}=1$ 当且仅当 $\sum_{u\in U}(-1)^{Tr_1^n(au)}=1$. 当 $a\in F_{2^m}^*$ 时,文献[11]已经证明了 $\sum_{u\in U}(-1)^{Tr_1^n(au)}=1-K_m(a)$. 因此结论成立.

4　Semi-Bent 函数的代数次数与例子

本节主要讨论新构造的 semi-bent 函数的代数次数,并给出域 F_{2^6} 上 semi-bent 函数的具体例子.

定理 2　当 $r=1$ 时,定理 1 中定义的函数 $f_i(x)$ 是 m 次的布尔函数.

证明　计算相应指数的 2-重如下:

$$\omega_2(2^m-1)=\omega_2((2^m-1)\cdot 3+1)=m,$$

$$\omega_2(2^{m-1}(2^m+1))=2,$$

$$\omega_2((2^m-1)/4+1)=\omega_2(2^m+3)=3,$$

$$\omega_2((2^m-1)/6+1)=\omega_2((2^m-1)/3+2)$$

$$=\omega_2((1+4+16+\cdots+2^{m-2})+2)=m/2+1$$

因此结论成立.

根据定理 2 的证明知,新构造的三类 semi-bent 函数的代数次数都大于等于 3,分别至少为 m,3 和 $m/2+1$. 并且,每一类 semi-bent 函数都存在代数次数为 m 的子类. 与现有的 semi-bent 函数相比,代数次数有了一定程度的提高(主要指 m 是偶数的情况). 例如,文献[1,2,5~7]中的 semi-bent 函数都是 2 次的. 尽管文献[8]分别构造了 2 次、3 次和 $k+1$ 次 semi-bent 函数,但根据分析发现 $k+1\leqslant m$ 且此类 $k+1$ 次 semi-bent 函数仅在 m 是奇数时存在. 而本文可以在 m 是任意整数时得到 m 次 semi-bent 函数,丰富了高次 semi-bent 函数的选择源.

引理 2　当 $m=3$ 且 $a+a^2+a^4=0$ 时,有 $K_m(a)=0$.

证明　显然有 $y^{-1}=y^{2^3-2}=(y^3)^2$. 因此

$$K_3(a)=\sum_{y\in F_{2^3}}(-1)^{Tr_1^3(ay+y^{-1})}=\sum_{y\in F_{2^3}}(-1)^{Tr_1^3(ay+y^3)}$$

众所周知,函数 $y\to Tr_1^3(ay+y^3)$ 是平衡函数当且仅当 $Tr_1^3(a)=a+a^2+a^4=0$. 所以当 $a+a^2+a^4=0$ 时,有 $K_m(a)=0$.

利用此引理的结论即可得 semi-bent 函数的具体例子.

例　设 $a\in F_{2^3}^*$ 且 $a+a^2+a^4=0$. 设 $b\in F_{2^6}^*$ 且 $b+b^{2^3}=1$. 则下面的函数

$$f_1(x)=Tr_1^6(ax^{2^3-1})+Tr_1^6(bx^{2^2(2^3+1)})+Tr_1^6(x^{(2^3-1)\cdot 3+1}),$$

$$f_2(x)=Tr_1^6(ax^{2^3-1})+Tr_1^6(bx^{2^2(2^3+1)})+Tr_1^6(x^{(2^3-1)\cdot 7+1})$$

是域 F_{2^6} 上的 semi-bent 函数,其中 $1/4\bmod(2^3+1)=7$.

5　结束语

利用迹函数,我们构造了三类 semi-bent 函数. 证明了在某些限制条件下,这些函数的 semi-bent 性与 Kloosterman 和密切相关. 并且,新构造的 semi-bent 函数中有大量的函数具有很高的代数次数. 因此,这为流密码滤波生成器的设计提供了更多同时具有高代数次数和高非线性度的布尔函数.

参考文献:

[1] K Khoo, G. Gong, D R Stinson. A new characterization of semi-bent and bent functions on finite fields[J]. Designs, Codes and Cryptography, 2006, 38(2): 279 – 295.

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

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

[4] M Matsui. Linear cryptanalysis method for DES cipher[A]. Proceedings of Workshop on the theory and application of cryptographic techniques on Advances in cryptology[C]. Springer-Verlag New York, 1994. 386 – 397.

[5] R Gold. Maximal recursive sequences with 3-valued recursive cross-correlation functions[J]. IEEE Transactions on Information Theory, 1968, IT – 14(1): 154 – 156.

[6] S Boztas, P V Kumar. Binary sequences with Gold-like correlation but large linear span[J]. IEEE Transactions on Information

Theory,1994,40(2):532 – 537.
[7] K Khoo,G.Gong,D R Stinson. A new family of gold-like sequences[A]. Proceedings of IEEE International Symposium on Information Theory[C]. Switzerland:Lausanne,2002.181.
[8] G Sun,C Wu. Construction of semi-bent Boolean functions in even number of variables[J]. Chinese Journal of Electronics,2009,18(2):231 – 237.
[9] I Shparlinski. On the values of Kloosterman sums[J]. IEEE Transactions on Information Theory,2009,55(6):2599 – 2601.
[10] H Dobbertin,G Leander,A Canteaut,et al. Construction of bent functions via Niho power functions[J]. Journal of Combinatorial Theory,Series A,2006,113(5):779 – 798.
[11] P Charpin,T Helleseth,V Zinoviev. The divisibility modulo 24 of Kloosterman sums on GF(2^m),m odd[J]. Journal of Combinatorial Theory,Series A,2007,114(2):322 – 338.

作者简介:

何业锋 女,1978 年 2 月生于山东淄博.西安电子科技大学博士研究生,研究方向为密码学.
E-mail:yefenghe2004@163.com

马文平 男,1966 年 5 月生于陕西省,西安电子科技大学教授,博士生导师,主要研究方向为:编码和密码学.