International Journal of Engineering, Mathematical and Physical Sciences
ISSN: 2517-9934
Vol:8, No:5, 2014

The Bent and Hyper-Bent Properties of a Class of Boolean Functions

Yu Lou, Chunming Tang, Yanfeng Qi, Maozhi Xu

Abstract—This paper considers the bent and hyper-bent properties of a class of Boolean functions. For one case, we present a detailed description for them to be hyper-bent functions, and give a necessary condition for them to be bent functions for another case.

Keywords—Boolean functions, bent functions, hyper-bent functions, character sums.

I. Introduction

BENT function is a class of Boolean functions with even variables and with the maximal distance to all affine functions. In fact, the distance of an n-variable bent function to any affine function equals $2^{n-1} - 2^{\frac{n}{2}-1}$. Bent function was introduction by Rothaus [9] in 1976, later in 2001 Youssef et al [10] found a subclass of bent functions with even better cryptographic properties, which was named as hyper-bent functions. Thanks to their applications in cryptography, coding theory and combinatorial design, many interests have been put in bent and hyper-bent functions recently[2], [3], [4], [6], [7], [8].

In this paper, we consider a class of Boolean functions defined on $\mathbb{F}_{2^n}$ of the form:

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

where $n = 2m$, $m \equiv 2k \pmod 4$, $k \in \{0, 1\}$, $a \in \mathbb{F}_{2^n}$ and $b \in \mathbb{F}_{16}$. When $m = 2 \pmod 4$, with the help of the factorization of x^5+x+a^{-1} and Kloosterman sums, this paper characterizes the cases for $f_{a,b}^{(r)}$ to be hyper-bent. Further more , for $a \in \mathbb{F}_{2^{\frac{m}{2}}}$, we list all the hyper-bent functions of the form of $f_{a,b}^{(r)}$. When $m = 0 \pmod 4$, we give a necessary condition for $f_{a,b}^{(r)}$ to be bent.

The rest of paper is organized as follows. In Section II, we give some notations and recall some basic knowledge for this paper. Then we describe the hyper-bent properties of $f_{a,b}^{(r)}$ when $m \equiv 2 \pmod 4$ and study the bent properties of $f_{a,b}^{(r)}$ when $m \equiv 0 \pmod 4$ in Section III and Section IV respectively. Finally, we conclude our work in Section V.

II. Preliminaries

The ***sign*** function of Boolean function f is $\chi(f) := (-1)^f$.

Definition 1: A Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is called a bent function, if $\widehat{\chi}_f(w) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{Tr}_1^n(wx)} = \pm 2^{\frac{n}{2}}$ $(\forall w \in \mathbb{F}_{2^n})$, where Tr_1^n is the absolute trace function defined as $\mathrm{Tr}_1^n(x) := x + x^2 + x^{2^2} + \cdots + x^{2^{n-1}}$.

Hyper-bent function is an important subclass of bent functions defined as

Definition 2: A bent function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is called a hyper-bent function, if, for any i satisfying $(i, 2^n - 1) = 1$, $f(x^i)$ is also a bent function.

Charpin and Gong [4] gave the following property to determine a hyper-bent function.

Proposition 1: Let $n = 2m$, α be a primitive element of $\mathbb{F}_{2^n}$ and f be a Boolean function over $\mathbb{F}_{2^n}$ satisfying $f(\alpha^{2^{m+1}}x) = f(x)$ $(\forall x \in \mathbb{F}_{2^n})$ and $f(0) = 0$. Let ξ be a primitive $2^m + 1$-th root in $\mathbb{F}_{2^n}^*$. Then f is a hyper-bent function if and only if the cardinality of the set $\{i | f(\xi^i) = 1, 0 \le i \le 2^m\}$ is 2^{m-1}.

Kloosterman sum is a powerful tool to study the hyper-bent properties of some classes of boolean functions.

Kloosterman sums on $\mathbb{F}_{2^n}$ are defined as

$$K_m(a) := \sum_{x\in\mathbb{F}_{2^m}} \chi(\mathrm{Tr}_1^m(ax + \frac{1}{x})), \quad a \in \mathbb{F}_{2^m}.$$

Some properties of Kloosterman sums are given by the following proposition.

Proposition 2: ([5],Theorem 3.4]) Let $a \in \mathbb{F}_{2^m}$. Then $K_m(a) \in [1 - 2^{(m+2)/2}, 1 + 2^{(m+2)/2}]$ and $4 \mid K_m(a)$.

Quintic Weil sums on $\mathbb{F}_{2^m}$ are

$$Q_m(a) := \sum_{x\in\mathbb{F}_{2^m}} \chi(\mathrm{Tr}_1^m(a(x^5 + x^3 + x))), \quad a \in \mathbb{F}_{2^m}.$$

And the value of $Q_m(a)$ is related to the factorization of the polynomial $P(x) = x^5 + x + a^{-1}$ [1].

When $a \in \mathbb{F}_{2^{m_1}}^*$, $m = 2m_1$, $K_m(a)$ and $Q_m(a)$ have the following properties

Proposition 3: (Lemma 3 [1]) If $a \in \mathbb{F}_{2^{m_1}}^*$, $m = 2m_1$,

(1) $1 - K_m(a) = (1 - K_{m_1}(a))^2 - 2 \cdot 2^{m_1}$.

(1) if $m_1 \equiv 1 \pmod 2$, then $Q_m(a) \in \{0,\ 2 \cdot 2^{m/2}, -4 \cdot 2^{m/2}\}$.

Proposition 4: [11] The Ramanujan-Nagell equation $x^2 - D = 2^{n+2}$ has at most 4 solutions (x, n), which are

$$(x, n) := (2^k-3, 1),\ (2^k-1, k),\ (2^k+1, k+1),\ (3\cdot2^k-1, 2k+1),$$

where $k \in \mathbb{N}$ and $D \in \mathbb{N}$ is odd.

With the help of the solutions of Ramanujan-Nagell equation,

Lemma 1: If $a \in \mathbb{F}_{2^{m_1}}$, $m = 2m_1$, $m_1 > 1$, then $K_m(a) \neq -4$.

Proof: By Propostion 3, if $K_m(a) = -4$,

$$(1 - K_{m_1}(a))^2 = 2 \cdot 2^{m_1} + 5. \tag{2}$$

Y. Lou, is with the School of Mathematical Sciences, Peking University, Beijing, 100871, China. (e-mail: windtker@163.com).
C. Tang is with School of Mathematics and Information, China West Normal University, Sichuan Nanchong,China.
Y. Qi is with Hangzhou Dianzi University, Zhejiang HangZhou, China.

It is easy to check that when $m_1 < 5$, $2\cdot 2^{m_1}+5$ is not a square. By Propostion 4, (2) has at most 4 solutions $(\mid (1-K_{m_1}(a)) \mid, n)$, which are

$$(\mid (1-K_{m_1}(a)) \mid, m_1-1) =$$
$$(2^k-3,1),\ (2^k-1,k),\ (2^k+1,k+1),\ (3\cdot 2^k-1,2k+1),$$

where $k \in \mathbb{N}$. We can check all the 4 solutions can not satisfy (2). For example, if $(\mid (1-K_{m_1}(a)) \mid, m_1-1) = (3\cdot 2^k-1, 2k+1)$, then

$$(3\cdot 2^k-1)^2 = 2^{2k+1+2}+5. \tag{3}$$

When $k=1,2$, $(3\cdot 2^k-1)^2 \neq 2^{2k+1+2}+5$. When $k\geq 3$, $(3\cdot 2^k-1)^2 > 2^{2k+1+2}+5$. Thus (3) has no integral solution, therefore (2) has no integral solution either, which concludes the proof. ■

III. The hyper-bent property of $f_{a,b}^{(r)}$ when $m=2 \pmod 4$

In the this section, we consider the Boolean function $f_{a,b}^{(r)}$ defined by (1), where $n=2m$, $m\equiv 2 \pmod 4$, $a\in\mathbb{F}_{2^n}$ and $b\in\mathbb{F}_{16}$. As the cyclotomic coset of 2 module 2^n-1 containing $\frac{2^n-1}{5}$ is

$$\{\frac{2^n-1}{5}, 2\cdot\frac{2^n-1}{5}, 2^2\cdot\frac{2^n-1}{5}, 2^3\cdot\frac{2^n-1}{5}\}.$$

Its size is 4, or $o(\frac{2^n-1}{5})=4$, which means $f_{a,b}^{(r)}$ is neither in the class considered by Charpin and Gong [4] nor in the class studied by Mesanager [6], [7].

Let α be a primitive element of $\mathbb{F}_{2^n}$, $\beta=\alpha^{\frac{2^n-1}{5}}$, $\xi=\alpha^{2^m-1}$, $U=<\xi>$, $V=<\xi^5>$. Since $5|(2^m+1)$, V is the subgroup of U and $\#V=\frac{2^m+1}{5}$.

For any $i\in\mathbb{F}_{2^m}$, define

$$\begin{aligned} S_i &= \sum_{v\in V}\chi(\mathrm{Tr}_1^n(a\xi^{i(2^m-1)}v)) \\ &= \sum_{v\in V}\chi(\mathrm{Tr}_1^n(a\xi^{-2i}v)) = \sum_{v\in V}\chi(\mathrm{Tr}_1^n(a\xi^{-5i+3i}v)) \\ &= \sum_{v\in V}\chi(\mathrm{Tr}_1^n(a\xi^{3i}v)). \qquad (as\ \xi^{-5i}\in V) \end{aligned}$$

From the definition of S_i,

$$S_i = S_{i \pmod 5}. \tag{4}$$

To study the hyper-bent properties of $f_{a,b}^{(r)}$, we define the following character sum

$$\Lambda_r(a,b) := \sum_{u\in U}\chi(f_{a,b}^{(r)}(u)). \tag{5}$$

Similar to the proof of Proposition 9 in [1], the hyper-bent properties of $f_{a,b}^{(r)}$ can be described as

Proposition 5: $f_{a,b}^{(r)}$ is a hyper-bent function if and only if $\Lambda_r(a,b)=1$.

Before our work on $f_{a,b}^{(r)}$, let us consider a *general* case of $f_{a,b}^{(r)}$ which is defined as

$$f_{a,b}^{(r,k)} := \mathrm{Tr}_1^n(ax^{r(2^m-1)}) + \mathrm{Tr}_1^4(bx^{k\frac{2^n-1}{5}}), \tag{6}$$

where a,b is defined as above and $k\in\mathbb{N}$.

When $k\equiv 0 \pmod 5$, $f_{a,b}^{(r,k)} = \mathrm{Tr}_1^n(ax^{r(2^m-1)}) + \mathrm{Tr}_1^4(b)$ is a special case studied by Charpin and Gong in [4]. In this paper we only consider the case of $k\not\equiv 0 \pmod 5$.

Proposition 6: The hyper-bent properties of $f_{a,b}^{(r,k)}$ can be represented by that of $f_{a,b}^{(r)}$ efficiently, where $a\in\mathbb{F}_{2^n}$, $b\in\mathbb{F}_{16}$, $k\not\equiv 0 \pmod 5$.

Proof: For $b\in\mathbb{F}_{16}^*$, b can be written as $b=\omega\beta^j$, where $\omega^3=1$, $0\leq j\leq 4$. Thus

$$\mathrm{Tr}_1^4(bx^{k\frac{2^n-1}{5}}) = \mathrm{Tr}_1^4(\omega\beta^j x^{k\frac{2^n-1}{5}}) = \mathrm{Tr}_1^4(\omega(\beta^{\frac{j}{k}}x^{\frac{2^n-1}{5}})^k).$$

It is easy to check,

$$\begin{aligned} \mathrm{Tr}_1^4(\omega x^{\frac{2^n-1}{5}}) &= \mathrm{Tr}_1^4(\omega^2 x^{2\frac{2^n-1}{5}}) \\ &= \mathrm{Tr}_1^4(\omega x^{4\frac{2^n-1}{5}}) = \mathrm{Tr}_1^4(\omega^2 x^{3\frac{2^n-1}{5}}). \end{aligned}$$

Then $\mathrm{Tr}_1^4(bx^{k\frac{2^n-1}{5}}) = \mathrm{Tr}_1^4(b' x^{\frac{2^n-1}{5}})$, where $b'\in\mathbb{F}_{16}^*$.

Hence the result stands. ■

A step further, $f_{a,b}^{(r)}$ has following proposition.

Proposition 7: Let $f_{a,b}^{(r)}$ be defined as (1) and $(r,5)=1$, then $f_{a,b}^{(r)}$ is a hyper-bent function if and only if $f_{a',b'}^{(r)}$ is a hyper-bent one, where $a=a'\xi^i\in\mathbb{F}_{2^n}$, $a'\in\mathbb{F}_{2^m}$, b, $b'=b\alpha^{-\frac{i}{r}\frac{2^n-1}{5}}\in\mathbb{F}_{16}$.

Proof: Notice that $\forall a\in\mathbb{F}_{2^n}$, $a=a'\xi^i$, where $a'\in\mathbb{F}_{2^m}$, $\xi=\alpha^{2^m-1}$ is a primitive 2^m+1-th root of unity in $\mathbb{F}_{2^n}$ and $0\leq i\leq 2^m$. We have

$$\begin{aligned} f_{a,b}^{(r)}(x) &= \mathrm{Tr}_1^n(ax^{r(2^m-1)}) + \mathrm{Tr}_1^4(bx^{\frac{2^n-1}{5}}) \\ &= \mathrm{Tr}_1^n(a'(\alpha^{\frac{i}{r}}x)^{r(2^m-1)}) + \mathrm{Tr}_1^4(b\alpha^{-\frac{i}{r}\frac{2^n-1}{5}}(\alpha^{\frac{i}{r}}x)^{\frac{2^n-1}{5}}) \\ &= f_{a',b'}^{(r)}(\alpha^{-\frac{i}{r}}x), \end{aligned}$$

where $b'=b\alpha^{-\frac{i}{r}\frac{2^n-1}{5}}\in\mathbb{F}_{16}$.

Thus $f_{a,b}^{(r)}$ is linearly equivalent to $f_{a',b'}^{(r)}$, that is to say, $f_{a,b}^{(r)}$ is a hyper-bent function if and only if $f_{a',b'}^{(r)}$ is a hyper-bent one. ■

By Proposition 7, if $a=a'\xi^i$, and $\beta=\alpha^{\frac{2^n-1}{5}}$, we have the following results

- $f_{a,b}^{(1)}$ is linearly equivalent to $f_{a',b\beta^{4i}}^{(1)}$.
- $f_{a,b}^{(2)}$ is linearly equivalent to $f_{a',b\beta^{2i}}^{(2)}$.
- $f_{a,b}^{(3)}$ is linearly equivalent to $f_{a',b\beta^{3i}}^{(3)}$.
- $f_{a,b}^{(4)}$ is linearly equivalent to $f_{a',b\beta^{i}}^{(4)}$.

By Proposition 7 and Proposition 6, when $a\in\mathbb{F}_{2^n}, k\in\mathbb{N}$, $b\in\mathbb{F}_{16}$, the hyper-bent properties of $f_{a,b}^{(r,k)}$ can be fully represented by that of $f_{a,b}^{(r)}$, where $a\in\mathbb{F}_{2^m}$, $b\in\mathbb{F}_{16}$. Since the hyper-bent properties of $f_{a,b}^{(1)}$ had been studied elaborately in [1], in the following parts of this Section we only consider the rest cases of r.

A. The Case of $r=5$

1) The hyper-bent properties of $f_{a,b}^{(5)}$, where $a\in\mathbb{F}_{2^m}$:

Proposition 8: Let $n=2m$ and $m\equiv\pm2,\pm6 \pmod{20}$, If $b\in\{0\}\bigcup\{\beta^i|i=0,1,2,3,4\}$, then the Boolean function

$f_{a,b}^{(5)}$ is not a hyper-bent function. Further, if $b \in \mathbb{F}_{16}^{*} \backslash \{\beta^i | 0 \leq i \leq 4\}$, $f_{a,b}^{(5)}$ is a hyper-bent function if and only if

$$\sum_{v \in V} \chi(\mathrm{Tr}_1^n(av)) = 1.$$

Proof: By (5),

$$\begin{aligned}\Lambda_5(a,b) &= \sum_{u \in U} \chi(f_{a,b}^{(5)}(u)) \\ &= \sum_{u \in U} \chi(\mathrm{Tr}_1^n(au^{5(2^m-1)}))\chi(\mathrm{Tr}_1^4(bu^{\frac{2^n-1}{5}})).\end{aligned}$$

Notice that $U =< \xi >$, $V =< \xi^5 >$ and $U = \xi^0 V \bigcup \xi^1 V \bigcup \xi^2 V \bigcup \xi^3 V \bigcup \xi^4 V$. Then,

$$\Lambda_5(a,b) = \qquad (7)$$

$$\sum_{i=0}^{4} \sum_{v \in V} \chi(\mathrm{Tr}_1^4(b(\xi^i v)^{\frac{2^n-1}{5}}))\chi(\mathrm{Tr}_1^n(a(\xi^i v)^{5(2^m-1)}))$$

$$= \sum_{i=0}^{4} \sum_{v \in V} \chi(\mathrm{Tr}_1^4(b(\xi^i v)^{\frac{2^n-1}{5}}))\chi(\mathrm{Tr}_1^n(a(\xi^{5i})^{2^m-1} v^{5(2^m-1)})) \qquad (8)$$

Since $(\xi^{5i})^{2^m-1} \in V$ and $m \equiv \pm 2, \pm 6 \pmod{20}$, $(5(2^m-1), \#V) = (5, \frac{2^m+1}{5}) = 1$. Then $v \longmapsto (\xi^{5i})^{2^m-1} v^{5(2^m-1)}$ is a permutation of V. Hence,

$$\begin{aligned}\Lambda_5(a,b) &= \sum_{i=0}^{4} \sum_{v \in V} \chi(\mathrm{Tr}_1^4(b(\xi^i v)^{\frac{2^n-1}{5}}))\chi(\mathrm{Tr}_1^n(av)) \\ &= (\sum_{i=0}^{4} \chi(\mathrm{Tr}_1^4(b\xi^{i\frac{2^n-1}{5}})))(\sum_{v \in V} \chi(\mathrm{Tr}_1^n(av))).\end{aligned}$$

As $\xi^{\frac{2^n-1}{5}} = (\alpha^{2^m-1})^{\frac{(2^m-1)(2^m+1)}{5}} = \beta^{2^m-1} = \beta^{2^m+1-2} = \beta^3$,

$$\begin{aligned}\Lambda_5(a,b) &= (\sum_{i=0}^{4} \chi(\mathrm{Tr}_1^4(b\beta^{3i}))(\sum_{v \in V} \chi(\mathrm{Tr}_1^n(av))) \\ &= (\sum_{i=0}^{4} \chi(\mathrm{Tr}_1^4(b\beta^{i}))(\sum_{v \in V} \chi(\mathrm{Tr}_1^n(av))). \qquad (9)\end{aligned}$$

By (9), when $b = 0$, $\Lambda_5(a,0) = 5 \sum_{v \in V} \chi(\mathrm{Tr}_1^n(av))$, and thus $\Lambda_5(a,0) \neq 1$. By Proposition 5, $f_{a,0}^{(5)}$ is not a hyper-bent function.

When $b \neq 0$, b can be represented as $b = \omega\beta^j$, where $\omega^3 = 1$ and $0 \leq j \leq 4$. Then

$$\sum_{i=0}^{4} \chi(\mathrm{Tr}_1^4(b\beta^i)) = \sum_{i=0}^{4} \chi(\mathrm{Tr}_1^4(\omega\beta^{i+j})) = \sum_{i=0}^{4} \chi(\mathrm{Tr}_1^4(\omega\beta^i)). \qquad (10)$$

Since $\omega^3 = 1$ and $\omega^4 = \omega$, we have

$$\mathrm{Tr}_1^4(\omega\beta^i) = \mathrm{Tr}_1^4(\omega^4\beta^{4i}) = \mathrm{Tr}_1^4(\omega\beta^{4i}).$$

If $\omega = 1$, $\sum_{i=0}^{4} \chi(\mathrm{Tr}_1^4(b\beta^i) = \sum_{i=0}^{4} \chi(\mathrm{Tr}_1^4(\beta^i))$. As β satisfies $\beta^4 + \beta^3 + \beta^2 + \beta + 1 = 0$, $\mathrm{Tr}_1^4(\beta^i) = 1, i \neq 0$. Then $\sum_{i=0}^{4} \chi(\mathrm{Tr}_1^4(b\beta^i)) = -3$. Therefore,

$$\Lambda_5(a,b) = -3 \sum_{v \in V} \chi(\mathrm{Tr}_1^n(av)), b = \beta^j, 0 \leq j \leq 4.$$

By Proposition 5, $f_{a,\beta^j}^{(5)}$ is not a hyper-bent function. When $\omega \neq 1$, we have

$$\begin{aligned}&\mathrm{Tr}_1^4(\omega\beta) + \mathrm{Tr}_1^4(\omega\beta^2) = \mathrm{Tr}_1^4(\omega(\beta + \beta^2)) \\ &= \omega(\beta + \beta^2 + \beta^3 + \beta^4) + \omega^2(\beta + \beta^2 + \beta^3 + \beta^4) \\ &= 1.\end{aligned}$$

Then $\chi(\mathrm{Tr}_1^4(\omega\beta)) + \chi(\mathrm{Tr}_1^4(\omega\beta^2)) = 0$. Similarly, $\chi(\mathrm{Tr}_1^4(\omega\beta^3)) + \chi(\mathrm{Tr}_1^4(\omega\beta^4)) = 0$. Therefore,

$$\Lambda_5(a,b) = \sum_{v \in V} \chi(\mathrm{Tr}_1^n(av)), b = \omega\beta^j, 0 \leq j \leq 4, \omega^3 = 1, \omega \neq 1.$$

By Proposition 5, the second part of this proposition follows. ■

In Proposition 8, we consider the hyper-bent properties of the Boolean function $f_{a,b}^{(5)}$ for $m \equiv \pm 2, \pm 6 \pmod{20}$. The proposition below discusses the hyper-bent properties of $f_{a,b}^{(5)}$ for $m \equiv 10 \pmod{20}$.

Proposition 9: Let $n = 2m$, $m \equiv 10 \pmod{20}$, $a \in \mathbb{F}_{2^m}$, $b \in \mathbb{F}_{16}$. then the Boolean function $f_{a,b}^{(5)}$ is not a hyper-bent function.

Proof: Notice that $\Lambda_5(a,b) = \sum_{i=0}^4 \sum_{v \in V} \chi(\mathrm{Tr}_1^4(b\xi^{i\frac{2^n-1}{5}}))\chi(\mathrm{Tr}_1^n(a(\xi^{5i})^{2^m-1}v^{5(2^m-1)}))$. Since $m \equiv 10 \pmod{20}$, $25 | (2^m + 1)$ and $(5(2^m-1), \frac{2^m+1}{5}) = 5$. Then $v \longmapsto v^{5(2^m-1)}$ is a 5 to 1 morphism from V to $V^5 := \{v^5 | v \in V\}$. Therefore,

$$\Lambda_5(a,b) = 5 \sum_{i=0}^{4} \sum_{v \in V^5} \chi(\mathrm{Tr}_1^4(b\xi^{i\frac{2^n-1}{5}}))\chi(\mathrm{Tr}_1^n(a(\xi^{5i})^{2^m-1}v)).$$

Hence, $5 | \Lambda_5(a,b)$ and $\Lambda_5(a,b)$ is not equal to 1, By Proposition 5, $f_{a,b}^{(5)}$ is not a hyper-bent function. ■

By Proposition 8,

$$\sum_{v \in V} \chi(\mathrm{Tr}_1^n(av)) = \sum_{v \in V} \chi(\mathrm{Tr}_1^n(av^{2^m-1})).$$

Notice that $\sum_{v \in V} \chi(\mathrm{Tr}_1^n(av)) = S_0$ in [1]. By Proposition 15 in [1],

$$\sum_{v \in V} \chi(\mathrm{Tr}_1^n(av)) = \frac{1}{5}[1 - K_m(a) + 2Q_m(a)]. \qquad (11)$$

Further, By Proposition 16 and 18 in [1], we have the following results.

Proposition 10: Let $n = 2m$, $m \equiv \pm 2, \pm 6 \pmod{20}$, $m \geq 6$ and $b \in \mathbb{F}_{16}^{*} \backslash \{\beta^i | 0 \leq i \leq 4\}$, then $f_{a,b}^{(5)}$ is a hyper-bent function if and only if one of the assertions (1) and (2) holds.

(1) $Q_m(a) = 0$, $K_m(a) = -4$.

(2) $Q_m(a) = 2^{m_1}$, $K_m(a) = 2 \cdot 2^{m_1} - 4$.

International Journal of Engineering, Mathematical and Physical Sciences
ISSN: 2517-9934
Vol:8, No:5, 2014

2) The hyper-bent properties of $f^{(5)}_{a,b}$ where $a \in \mathbb{F}_{2^n}$: In this part, we always assume $n = 2m$, $m = 2m_1$, $m_1 \in \mathbb{N}$.

Lemma 2: Let $b \in \mathbb{F}^*_{16}$, $\gamma \in \{z \in \mathbb{F}_{2^n} : z^5 = 1, z \neq 1\} = <\alpha^{\frac{2^n-1}{5}}>$, then

$$\sum_{i=0}^{4} \chi(\mathrm{Tr}_1^4(b\gamma^i)) = \begin{cases} 1, & b^5 \neq 1 \\ -3, & b^5 = 1. \end{cases}$$

Proof: Firstly, if $b^5 = 1$,

$$\sum_{i=0}^{4} \chi(\mathrm{Tr}_1^4(b\gamma^i)) = \sum_{i=0}^{4} \chi(\mathrm{Tr}_1^4(\gamma^i)) = 1 + \sum_{i=0}^{3} \chi(\mathrm{Tr}_1^4(\gamma^{2^i})) = 1 + 4\chi(\mathrm{Tr}_1^4(\gamma)) = -3.$$

Secondly, if $b^5 \neq 1$,

$$\sum_{i=0}^{4} \chi(\mathrm{Tr}_1^4(b\gamma^i)) = \sum_{i=0}^{4} \chi(\mathrm{Tr}_1^4(b^2\gamma^{2i})) = \sum_{i=0}^{4} \chi(\mathrm{Tr}_1^4(b^2\gamma^i)).$$

Since $\forall b \in \mathbb{F}^*_{16}$, $b = \omega^j\gamma^i,\ 0 \leq j \leq 2,\ 0 \leq i \leq 4$, we have

$$\begin{aligned} &\sum_{b\in\mathbb{F}_{16}} \chi(\mathrm{Tr}_1^4(b)) = 1 + \sum_{b\in\mathbb{F}^*_{16}} \chi(\mathrm{Tr}_1^4(b)) \\ &= 1 + \sum_{j=0}^{2}\sum_{i=0}^{4} \chi(\mathrm{Tr}_1^4(\omega^j\gamma^i)) \\ &= 1 + \sum_{i=0}^{4} \chi(\mathrm{Tr}_1^4(\gamma^i)) + \sum_{i=0}^{4} \chi(\mathrm{Tr}_1^4(\omega\gamma^i)) + \sum_{i=0}^{4} \chi(\mathrm{Tr}_1^4(\omega^2\gamma^i)) \\ &= 1 + (-3) + 2\sum_{i=0}^{4} \chi(\mathrm{Tr}_1^4(\omega\gamma^i)). \end{aligned}$$

Notice that $\sum_{b\in\mathbb{F}_{16}} \chi(\mathrm{Tr}_1^4(b)) = 0$, hence $\sum_{i=0}^4 \chi(\mathrm{Tr}_1^4(b\gamma^i)) = 1$, and the conclusion stands. ■

Theorem 1: If $a = a'\xi^i$, $a' \in \mathbb{F}_{2^m}$, the hyper-bent properties of $f^{(5)}_{a,b}$ can be described as follows:

(1) when $m \equiv 10 \pmod{20}$, $f^{(5)}_{a,b}$ is not hyper-bent.

(2) when $m \equiv \pm 2, \pm 6 \pmod{20}$, $f^{(5)}_{a,b}$ is hyper-bent if and only if $S_{2i} = 1$.

Proof: To the character sum of $f^{(5)}_{a,b}$:

$$\begin{aligned} \Lambda(a'\xi^i, b) &= \sum_{u\in U} \chi(f^{(5)}_{a'\xi^i,b}(u)) \\ &= \sum_{u\in U} \chi(\mathrm{Tr}_1^n(a'\xi^i u^{5(2^m-1)}))\chi(\mathrm{Tr}_1^4(bu^{\frac{2^n-1}{5}})) \\ &= \sum_{j=0}^{4}\sum_{v\in V} \chi(\mathrm{Tr}_1^n(a'\xi^i(\xi^j v)^{5(2^m-1)}))\chi(\mathrm{Tr}_1^4(b(\xi^j v)^{\frac{2^n-1}{5}})) \\ &= \sum_{j=0}^{4}\sum_{v\in V} \chi(\mathrm{Tr}_1^4(b\xi^{j\frac{2^n-1}{5}}))\chi(\mathrm{Tr}_1^n(a'\xi^i\xi^{5j(2^m-1)}v^{5(2^m-1)})). \end{aligned} \tag{12}$$

If $m \equiv 10 \pmod{20}$, then $(5, \#V) = 5$. By (12), $\Lambda(a'\xi^i, b) = 5\sum_{j=0}^4 \sum_{v'\in V^5} \chi(\mathrm{Tr}_1^4(b\xi^{j\frac{2^n-1}{5}}))\chi(\mathrm{Tr}_1^n(a'\xi^i\xi^{5j(2^m-1)}v'))$, where $V^5 = \{v^5 \mid v \in V\}$, $v \mapsto v^{5(2^m-1)}$ is a 5 *to* 1 morphism from V to V^5 . Thus $\Lambda(a'\xi^i, b) \neq 1$, and $f^{(5)}_{a,b}$ is not a hyper-bent function.

If $m \equiv \pm 2, \pm 6 \pmod{20}$, then $(5, \#V) = 1$. By (12) and (9),

$$\begin{aligned} \Lambda(a'\xi^i, b) &= \sum_{j=0}^{4}\sum_{v\in V} \chi(\mathrm{Tr}_1^4(b\beta^j))\chi(\mathrm{Tr}_1^n(a'\xi^i v)) \\ &= (\sum_{j=0}^{4} \chi(\mathrm{Tr}_1^4(b\beta^j)))(\sum_{v\in V} \chi(\mathrm{Tr}_1^n(a'(\xi^{\frac{i}{2^m-1}})^{2^m-1}v))), \end{aligned}$$

where $\beta = \alpha^{\frac{2^n-1}{5}}$, $\xi^{\frac{2^n-1}{5}} = \beta^3$. Since $\frac{1}{2^m-1} \equiv 2 \pmod{5}$, then by (4),

$$\begin{aligned} \Lambda(a'\xi^i, b) &= (\sum_{j=0}^{4} \chi(\mathrm{Tr}_1^4(b\beta^j)))(\sum_{v\in V} \chi(\mathrm{Tr}_1^n(a'(\xi^{2i})^{2^m-1}v))) \\ &= (\sum_{j=0}^{4} \chi(\mathrm{Tr}_1^4(b\beta^j)))S_{2i}. \end{aligned}$$

By Lemma 2,

$$\Lambda(a'\xi^i, b) = \begin{cases} S_{2i}, & b^5 \neq 1 \\ -3S_{2i}, & b^5 = 1. \end{cases}$$

If $b^5 = 1$, $3 \mid \Lambda(a'\xi^i, b)$. Thus $f^{(5)}_{a'\xi^i,b}$ is not a hyper-bent function.

If $b^5 \neq 1$, then $f^{(5)}_{a'\xi^i,b}$ is a hyper-bent function if and only if $S_{2i} = 1$. ■

B. The Case of $r = 2$

When $b = 0$, the hyper-bent propriety of $f^{(2)}_{a,0}$ has been studied by Canteaut et al in [2]. We consider the case of $b \neq 0$.

Proposition 11: Let $a \in \mathbb{F}_{2^m}$, $b \in \mathbb{F}^*_{16}$, we have

(1) if $b = 1$, then $\Lambda_2(a, b) = S_0 - 2(S_1 + S_2) = 2S_0 - \Lambda_2(a, 0)$.

(2) if $b \in \{\beta+\beta^2, \beta+\beta^3, \beta^2+\beta^4, \beta^3+\beta^4\}$, then $\Lambda_2(a, b) = S_0$.

(3) if $b = \beta$ or β^4, then $\Lambda_2(a, b) = -S_0 - 2S_2$.

(4) if $b = \beta^2$ or β^3, then $\Lambda_2(a, b) = -S_0 - 2S_1$.

(5) if $b = 1 + \beta$ or $1 + \beta^4$, then $\Lambda_2(a, b) = -S_0 + 2S_2$.

(6) if $b = 1 + \beta^2$ or $1 + \beta^3$, then $\Lambda_2(a, b) = -S_0 + 2S_1$.

(7) if $b = \beta + \beta^4$, then $\Lambda_2(a, b) = S_0 + 2S_2 - 2S_1$.

(8) if $b = \beta^2 + \beta^3$, then $\Lambda_2(a, b) = S_0 - 2S_2 + 2S_1$.

Proof: Similar to proof of Proposition 13 in [1] the results hold. ■

Corollary 1: Let $a \in \mathbb{F}_{2^m}$, $b \in \mathbb{F}^*_{16}$, we have

(1) $f^{(2)}_{a,b}$ holds the same hyper-bent propertyies as $f^{(1)}_{a,b^2}$.

(2) if b satisfies $(b+1)(b^4+b+1) = 0$, then $f^{(2)}_{a,b}$ holds the same hyper-bent properties as $f^{(1)}_{a,b}$.

Proof: (1) By Proposition 11 and Proposition 13 in [1],

$$\Lambda_2(a, b) = \Lambda_1(a, b^2).$$

Hence $f^{(2)}_{a,b}$ is a hyper-bent function if and only if $f^{(1)}_{a,b^2}$ is.

(2) Similarly, if b satisfying $(b+1)(b^4+b+1) = 0$, then,

$$\Lambda_2(a, b) = \Lambda_1(a, b).$$

Thus $f^{(2)}_{a,b}$ holds the same hyper-bent properties as $f^{(1)}_{a,b}$. ■

International Journal of Engineering, Mathematical and Physical Sciences
ISSN: 2517-9934
Vol:8, No:5, 2014

C. The General Case of r

Theorem 2: Let $n = 2m$, $m \equiv 2 \pmod 4$, $a \in \mathbb{F}_{2^m}$ and $b \in \mathbb{F}_{16}$. If $(r, \frac{2^m+1}{5}) > 1$, then $f_{a,b}^{(r)}$ is not a hyper-bent function. Further, if $(r, \frac{2^m+1}{5}) = 1$, then

(1) If $r \equiv 0 \pmod 5$, then $f_{a,b}^{(r)}$ and $f_{a,b}^{(5)}$ has the same hyper-bent properties.

(2) If $r \equiv \pm 1 \pmod 5$, then $f_{a,b}^{(r)}$ and $f_{a,b}^{(1)}$ has the same hyper-bent properties.

(3) If $r \equiv \pm 2 \pmod 5$, then $f_{a,b}^{(r)}$ and $f_{a,b}^{(2)}$ has the same hyper-bent properties.

Proof: Notice that

$$\Lambda_r(a,b) = \sum_{i=0}^{4}\sum_{v\in V}\chi(\mathrm{Tr}_1^4(b(\xi^i v)^{\frac{2^n-1}{5}}))\chi(\mathrm{Tr}_1^n(a(\xi^i v)^{r(2^m-1)}))$$
$$= \sum_{i=0}^{4}\sum_{v\in V}\chi(\mathrm{Tr}_1^4(b\xi^{i\frac{2^n-1}{5}}))\chi(\mathrm{Tr}_1^n(a\xi^{ri(2^m-1)}v^{r(2^m-1)})).$$

Let $d = (r(2^m-1), \#V) = (r, \frac{2^m+1}{5})$, then $\Lambda_r(a,b) = d\sum_{i=0}^{4}\chi(\mathrm{Tr}_1^4(b\xi^{i\frac{2^n-1}{5}}))\sum_{v\in V^d}\chi(\mathrm{Tr}_1^n(a\xi^{ri(2^m-1)}v^{r(2^m-1)}))$, where $V^d = \{v^d | v \in V\}$. If $d = (r, \frac{2^m+1}{5}) > 1$, $d|\Lambda_r(a,b)$ and $\Lambda_r(a,b) \neq 1$. Hence, $f_{a,b}^{(r)}$ is not a hyper-bent function.

When $d = (r, \frac{2^m+1}{5}) = 1$,

$$\Lambda_r(a,b) = \sum_{i=0}^{4}\chi(\mathrm{Tr}_1^4(b\xi^{i\frac{2^n-1}{5}}))\sum_{v\in V}\chi(\mathrm{Tr}_1^n(a\xi^{ri(2^m-1)}v)). \tag{13}$$

If $r \equiv 0 \pmod 5$, from $\xi^{\frac{2^n-1}{5}} = \beta^3$, we have

$$\Lambda_r(a,b) = \sum_{i=0}^{4}\chi(\mathrm{Tr}_1^4(b\beta^{3i}))\sum_{v\in V}\chi(\mathrm{Tr}_1^n(a\xi^{ri(2^m-1)}v))$$
$$= \sum_{i=0}^{4}\chi(\mathrm{Tr}_1^4(b\beta^{i}))\sum_{v\in V}\chi(\mathrm{Tr}_1^n(av)).$$

Then $\Lambda_r(a,b) = \Lambda_5(a,b)$. Therefore, $f_{a,b}^{(r)}$ and $f_{a,b}^{(5)}$ has the same hyper-bent properties.

If $r \equiv 1 \pmod 5$, then

$$\Lambda_r(a,b) = \sum_{i=0}^{4}\chi(\mathrm{Tr}_1^4(b\xi^{i\frac{2^n-1}{5}}))\sum_{v\in V}\chi(\mathrm{Tr}_1^n(a\xi^{i(2^m-1)}v)).$$

By Proposition 10 in [1], $\Lambda_r(a,b) = \Lambda_1(a,b)$. Hence, $f_{a,b}^{(r)}$ and $f_{a,b}^{(1)}$ has the same hyper-bent properties.

If $r \equiv 2 \pmod 5$, then

$$\Lambda_r(a,b) = \sum_{i=0}^{4}\chi(\mathrm{Tr}_1^4(b\xi^{i\frac{2^n-1}{5}}))\sum_{v\in V}\chi(\mathrm{Tr}_1^n(a\xi^{2i(2^m-1)}v))$$
$$= \sum_{i=0}^{4}\chi(\mathrm{Tr}_1^4(b\beta^{3i}))S_{2i}$$
$$= \sum_{i=0}^{4}\chi(\mathrm{Tr}_1^4(b\beta^{9i}))S_{6i} = \sum_{i=0}^{4}\chi(\mathrm{Tr}_1^4(b\beta^{4i}))S_i.$$

By Lemma 1 in [1],

$$\Lambda_r(a,b) = \chi(\mathrm{Tr}_1^4(b))S_0 + (\chi(\mathrm{Tr}_1^4(b\beta)) + \chi(\mathrm{Tr}_1^4(b\beta^4)))S_1 + (\chi(\mathrm{Tr}_1^4(b\beta^2)) + \chi(\mathrm{Tr}_1^4(b\beta^3)))S_2. \tag{14}$$

Hence, $\Lambda_r(a,b) = \Lambda_2(a,b)$. $f_{a,b}^{(r)}$ and $f_{a,b}^{(2)}$ has the same hyper-bent properties.

If $r \equiv 3 \pmod 5$,

$$\Lambda_r(a,b) = \sum_{i=0}^{4}\chi(\mathrm{Tr}_1^4(b\xi^{i\frac{2^n-1}{5}}))\sum_{v\in V}\chi(\mathrm{Tr}_1^n(a\xi^{3i(2^m-1)}v))$$
$$= \sum_{i=0}^{4}\chi(\mathrm{Tr}_1^4(b\beta^{3i}))S_{3i} = \sum_{i=0}^{4}\chi(\mathrm{Tr}_1^4(b\beta^{i}))S_i.$$

From Lemma 1 in [1],

$$\Lambda_r(a,b) = \chi(\mathrm{Tr}_1^4(b))S_0 + (\chi(\mathrm{Tr}_1^4(b\beta)) + \chi(\mathrm{Tr}_1^4(b\beta^4)))S_1 + (\chi(\mathrm{Tr}_1^4(b\beta^2)) + \chi(\mathrm{Tr}_1^4(b\beta^3)))S_2. \tag{15}$$

Hence, $\Lambda_r(a,b) = \Lambda_3(a,b)$. From (14) and (15), we have $\Lambda_2(a,b) = \Lambda_3(a,b)$. Thus, $f_{a,b}^{(r)}$ and $f_{a,b}^{(2)}$ have the same hyper-bent properties.

Similarly, if $r \equiv 4 \pmod 5$, then $\Lambda_r(a,b) = \Lambda_4(a,b) = \Lambda_1(a,b)$. Thus, $f_{a,b}^{(r)}$ and $f_{a,b}^{(1)}$ have the same hyper-bent properties.

Above all, the results stand. ■

From the above discussion, we have the following results on $f_{a,b}^{(r)}$.

Proposition 12: Let $a \in \mathbb{F}_{2^m}$ and $(r, \frac{2^m+1}{5}) = 1$, then

(1) If $\frac{1}{5}[1 - K_m(a) + 2Q_m(a)] = 1$, then the following Boolean functions

(a) $f_{a,b}^{(r)}$, $b \in \mathbb{F}_{16}^* \backslash \{\beta^i | i = 0,1,2,3,4\}$, $r \equiv 0 \pmod 5$.

(b) $f_{a,b}^{(r)}$, $r \not\equiv 0 \pmod 5$, $b^4 + b + 1 = 0$.

are hyper-bent functions.

(2) If $-\frac{1}{5}[3(1 - K_m(a)) - 4Q_m(a)] = 1$, then the Boolean function $f_{a,1}^{(r)}$ $(r \not\equiv 0 \pmod 5)$ is a hyper-bent function.

Proof: By Theorem 2, (11), Proposition 8 and Proposition 16 in [1], this proposition follows. ■

With Proposition 12, we can generalize Theorem 3 in [1] to the following theorem.

Theorem 3: Let $n = 2m$, $m = 2m_1$, $m_1 \equiv 1 \pmod 2$, $m_1 \geq 3$ and $(r, \frac{2^m+1}{5}) = 1$, If one of two assertions (1) and (2) holds,

(1) $p(x) = x^5 + x + a^{-1}$ over $\mathbb{F}_{2^m}$ is $(1)(2)^2$ and $K_m(a) = -4$.

(2) $p(x) = x^5 + x + a^{-1}$ is irreducible over $\mathbb{F}_{2^m}$. The quadratic form $\mathfrak{q}(x) = \mathrm{Tr}_1^m(x(ax^4 + ax^2 + a^2x))$ over $\mathbb{F}_{2^m}$ is even. $K_m(a) = 2 \cdot 2^{m_1} - 4$.

Then the Boolean functions

(a) $f_{a,b}^{(r)}$, $b \in \mathbb{F}_{16}^* \backslash \{\beta^i | i = 0,1,2,3,4\}$, $r \equiv 0 \pmod 5$.

(b) $f_{a,b}^{(r)}$, $r \not\equiv 0 \pmod 5$, $b^4 + b + 1 = 0$.

are hyper-bent functions.

Proof: By Proposition 16 and Theorem 3 in [1] and Proposition 12, this theorem follows. ■

By Proposition 16 , Proposition 12 and Theorem 2 in [1], we have the following results for the hyper-bent properties of $f_{a,b}^{(r)}$:

Theorem 4: Let $n = 2m$, $m = 2m_1$, $m_1 \equiv 1 \pmod 2$, $m_1 \geq 3$, $(r, \frac{2^m+1}{5}) = 1$ and $r \not\equiv 0 \pmod 5$, then $f_{a,1}^{(r)}$ is a hyper-bent function if and only if the following assertions holds.

(1) $p(x) = x^5 + x + a^{-1}$ is irreducible over $\mathbb{F}_{2^m}$.

(2) The quadratic form $\mathfrak{q}(x) = \mathrm{Tr}_1^m(x(ax^4 + ax^2 + a^2x))$ over $\mathbb{F}_{2^m}$ is even.

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

If $a \in \mathbb{F}_{2^{\frac{m}{2}}}$, the hyper-bent properties of $f_{a,b}^{(r)}$ is

Theorem 5: Let $n = 2m$, $m = 2m_1$, $m_1 \equiv 1 \pmod 2$ and $m_1 \geq 3$. If $n \neq 12, 28$, any Boolean function in

$$\{f_{a,b}^{(r)} | a \in \mathbb{F}_{2^{\frac{m}{2}}}, b \in \mathbb{F}_{16}\} \tag{16}$$

is not a hyper-bent function. Further, if $n = 12$, all the hyper-bent functions in (16) are $\mathrm{Tr}_1^{12}(ax^{r(2^6-1)}) + \mathrm{Tr}_1^4(bx^{\frac{2^{12}-1}{5}})$, where $r \not\equiv 0 \pmod 5$, $(r, \frac{2^m+1}{5}) = 1$, $(a+1)(a^3 + a^2 + 1) = 0$ and $b = \beta^i, i = 1, 2, 3, 4$. If $n = 28$, all the hyper-bent functions in (16) are $\mathrm{Tr}_1^{28}(ax^{r(2^{14}-1)}) + \mathrm{Tr}_1^4(bx^{\frac{2^{28}-1}{5}})$, where $r \not\equiv 0 \pmod 5$, $(r, \frac{2^m+1}{5}) = 1$, $(a+1)(a^7+a^6+a^5+a^4+a^3+a^2+1) = 0$ and $b = \beta^i, i = 1, 2, 3, 4$.

Proof: Notice that $a \in \mathbb{F}_{2^{\frac{m}{2}}}$. By Theorem 2, if $f_{a,b}^{(r)}$ is a hyper-bent function, $(r, \frac{2^m+1}{5}) = 1$.

Suppose $(r, \frac{2^m+1}{5}) = 1$. we first prove that $f_{a,0}^{(r)}$ is not a hyper-bent function when $r \equiv 0 \pmod 5$. By Theorem 2, $f_{a,b}^{(r)}$ is a hyper-bent function if and only if $f_{a,b}^{(5)}$ is a hyper-bent function. If $b = 0$,

$$\Lambda_5(a, 0) = \sum_{u \in U} \chi(\mathrm{Tr}_1^n(au^{5(2^m-1)})) = 5 \sum_{v \in V} \chi(\mathrm{Tr}_1^n(av^{2^m-1})).$$

Hence, $5 | \Lambda_5(a, 0)$ and $\Lambda_5(a, 0) \neq 1$. Therefore, $f_{a,0}^{(5)}$ is not a hyper-bent function. Then $f_{a,0}^{(r)}$ is not a hyper-bent function.

When $b \neq 0$, by Theorem 3, $f_{a,b}^{(r)}$ is a hyper-bent function if and only if $f_{a,b'}^{(1)}$ $(b'^4 + b' + 1 = 0)$ is a hyper-bent function. By Theorem 5 in [1], $f_{a,b'}^{(1)}$ $(b'^4 + b' + 1 = 0)$ is not a hyper-bent function. Hence, $f_{a,b}^{(r)}$ is not a hyper-bent function when $r \equiv 0 \pmod 5$.

Now we discuss the case $r \equiv \pm 1 \pmod 5$ and $(r, \frac{2^m+1}{5}) = 1$. By Theorem 2, $f_{a,b}^{(r)}$ is a hyper-bent function if and only if $f_{a,b}^{(1)}$ is a hyper-bent function. By Theorem 5 in [1], there are only two cases. The first case is $n = 12$, where a and b satisfy

$$(a+1)(a^3 + a^2 + 1) = 0, b = \beta^i, i = 1, 2, 3, 4.$$

The second case is $n = 28$, where a and b satisfy

$$(a+1)(a^7+a^6+a^5+a^4+a^3+a^2+1) = 0, b = \beta^i, i = 1, 2, 3, 4.$$

When $r \equiv \pm 2 \pmod 5$ and $(r, \frac{2^m+1}{5}) = 1$, we have similar results.

Above all, this theorem follows. ■

IV. The bent property of $f_{a,b}^{(r)}$ when $m = 0 \pmod 4$

In this section we consider the bent properties of $f_{a,b}^{(r)}$, where $m \equiv 0 \pmod 4$, $a \in \mathbb{F}_{2^n}$, $b \in \mathbb{F}_{16}$.

Proposition 13: Let $a = a'\xi^k \in \mathbb{F}_{2^n}^*$, $b \in \mathbb{F}_{16}^*$, $a' \in \mathbb{F}_{2^m}^*$, $0 \leq k \leq 2^m$, $m \equiv 0 \pmod 4$, $m = 2m_1$. One necessary condition for $f_{a,b}^{(r)}$ to be a bent function is: $(r, 2^m + 1) = 1$, $a' \in \mathbb{F}_{2^m} \setminus \mathbb{F}_{2^{m_1}}$, $b^5 \neq 1$, $\widehat{\chi}_{f_{a,b}^{(r)}}(0) = 2^m$ and $K_m(a') = -4$.

Proof: Notice that $\forall x \in \mathbb{F}_{2^n}^*$, $x = yu$, where $y \in \mathbb{F}_{2^m}^*$, $u \in U =< \alpha^{2^m-1} >$. Since $m \equiv 0 \pmod 4$, $5 \mid 2^m - 1$. Thus $u^{\frac{2^n-1}{5}} = (u^{2^m+1})^{\frac{2^m-1}{5}} = 1$. Now, consider the Walsh spectrum of $f_{a,b}^{(r)}$ at 0, which is

$$\begin{aligned}\widehat{\chi}_{f_{a,b}^{(r)}}(0) &= \sum_{x \in \mathbb{F}_{2^n}} \chi(f_{a,b}^{(r)}(x)) = 1 + \sum_{u \in U} \sum_{y \in \mathbb{F}_{2^m}^*} \chi(f_{a,b}^{(r)}(yu)) \\ &= 1 + \sum_{u \in U} \sum_{y \in \mathbb{F}_{2^m}^*} \chi(\mathrm{Tr}_1^n(a(yu)^{r(2^m-1)}))\chi(\mathrm{Tr}_1^4(b(yu)^{\frac{2^n-1}{5}})) \\ &= 1 + \sum_{u \in U} \chi(\mathrm{Tr}_1^n(au^{r(2^m-1)})) \sum_{y \in \mathbb{F}_{2^m}^*} \chi(\mathrm{Tr}_1^4(by^{\frac{2^n-1}{5}}))\end{aligned} \tag{17}$$

$\mathbb{F}_{2^m}^*$ can be written as $\mathbb{F}_{2^m}^* = \bigcup_{i=0}^{4} \beta^i V$, where $V = \{z^5 \mid z \in \mathbb{F}_{2^m}^*\}$, $\beta \in \mathbb{F}_{2^m}^* \setminus V$.

If $(r(2^m - 1), 2^m + 1) = 1$, by (17),

$$\begin{aligned}&\widehat{\chi}_{f_{a,b}^{(r)}}(0) = \\ &1 + \sum_{u \in U} \chi(\mathrm{Tr}_1^n(a'\xi^k u^{r(2^m-1)})) \sum_{i=0}^{4} \sum_{v \in V} \chi(\mathrm{Tr}_1^4(b(v\beta^i)^{\frac{2^n-1}{5}})) \\ &= 1 + \sum_{u \in U} \chi(\mathrm{Tr}_1^n(a'u)) \sum_{i=0}^{4} \sum_{v \in V} \chi(\mathrm{Tr}_1^4(b\beta^{i\frac{2^n-1}{5}})) \\ &= 1 + \sum_{u \in U} \chi(\mathrm{Tr}_1^n(a'u)) \sum_{v \in V} \sum_{i=0}^{4} \chi(\mathrm{Tr}_1^4(b\gamma^i)) \\ &= 1 + (1 - K_m(a'))\frac{2^m - 1}{5} \sum_{i=0}^{4} \chi(\mathrm{Tr}_1^4(b\gamma^i)),\end{aligned} \tag{18}$$

$(r(2^m-1), 2^m+1) = 1$, $u \mapsto \xi^k u^{r(2^m-1)}$ is a permutation in U, $\sum_{u \in U} \chi(\mathrm{Tr}_1^n(au^{2^m-1})) = 1 - K_m(a)$. $\gamma = \beta^{\frac{2^n-1}{5}} \neq 1$ is a 5-th primitive root of unity in $\mathbb{F}_{2^n}$. If $f_{a,b}^{(r)}$ is a bent function,

$$\widehat{\chi}_{f_{a,b}^{(r)}}(0) = 1 + (K_m(a') - 1)(\frac{2^m - 1}{5}) \sum_{i=0}^{4} \chi(\mathrm{Tr}_1^4(b\gamma^i)) = \pm 2^m.$$

By Lemma 2,

(1) if $\sum_{i=0}^{4} \chi(\mathrm{Tr}_1^4(b\gamma^i)) = -3$, then $K_m(a') = \frac{8}{3}$ or $3(2^m - 1)(K_m(a') - 1) = -5(2^m + 1)$. Since $K_m(a')$ is an integer, however $(\frac{2^m-1}{5}, 2^m + 1) = 1$, Neither of the two equations stands, thus $f_{a,b}^{(r)}$ is not a bent function.

(2) if $\sum_{i=0}^{4} \chi(\mathrm{Tr}_1^4(b\gamma^i)) = 1$, which means $K_m(a') = -4$, $\widehat{\chi}_{f_{a,b}^{(r)}}(0) = 2^m$, or $(2^m - 1)(K_m(a') - 1) = 5(2^m + 1)$, $\widehat{\chi}_{f_{a,b}^{(r)}}(0) = -2^m$. Since $(\frac{2^m-1}{5}, 2^m + 1) = 1$, the last group of equations can not stand. By Lemma 1, if $a' \in \mathbb{F}_{2^{m_1}}$, then $K_m(a') \neq -4$.

If $(r(2^m-1), 2^m+1) = d > 1$. Since $5 \mid 2^m-1$, $5 \nmid d$. By (17),

$$\begin{aligned}
&\widehat{\chi}_{f_{a,b}^{(r)}}(0) = \\
&1 + \sum_{u\in U}\chi(\mathrm{Tr}_1^n(au^{r(2^m-1)}))\sum_{i=0}^{4}\sum_{v\in V}\chi(\mathrm{Tr}_1^4(b(v\beta^i)^{\frac{2^n-1}{5}})) \\
&= 1 + d\sum_{u'\in U^d}\chi(\mathrm{Tr}_1^n(au))\frac{2^m-1}{5}\sum_{i=0}^{4}\chi(\mathrm{Tr}_1^4(b\gamma^i)) \\
&= 1 + dh\frac{2^m-1}{5}\sum_{i=0}^{4}\chi(\mathrm{Tr}_1^4(b\gamma^i)),
\end{aligned}$$

where $U^d = \{u^d \mid u \in U\}$, $u \mapsto u^{r(2^m-1)}$ is a d *to* 1 morphism from U to U^d, $h = \sum_{u'\in U^d}\chi(\mathrm{Tr}_1^n(au))$. If $f_{a,b}^{(r)}$ is a bent function,

$$\widehat{\chi}_{f_{a,b}^{(r)}}(0) = 1 + dh(\frac{2^m-1}{5})\sum_{i=0}^{4}\chi(\mathrm{Tr}_1^4(b\gamma^i)) = \pm 2^m.$$

By Lemma 2,

(1) if $\sum_{i=0}^{4}\chi(\mathrm{Tr}_1^4(b\gamma^i)) = -3$, then $3dh = -5$ or $3dh(2^m-1) = 5(2^m+1)$.

(2) if $\sum_{i=0}^{4}\chi(\mathrm{Tr}_1^4(b\gamma^i)) = 1$, then $dh = 5$ or $dh(2^m-1) = -5(2^m+1)$.

Notice that $d > 1$, $5 \nmid d$, $3 \nmid 2^m+1$, $(2^m-1, 2^m+1) = 1$, all of the above equations can not stand.

Above all, the results follow. ∎

V. Conclusion

This paper considers the bent and hyper-bent properties of the Boolean functions $f_{a,b}^{(r)}$ of the form $f_{a,b}^{(r)} := \mathrm{Tr}_1^n(ax^{r(2^m-1)}) + \mathrm{Tr}_1^4(bx^{\frac{2^n-1}{5}})$, where $n = 2m$, $m = 2k \pmod 4$, $k \in \{0,1\}$, $a \in \mathbb{F}_{2^n}$ and $b \in \mathbb{F}_{16}$. When $m = 2 \pmod 4$, we give a detailed description of the hyper-bent properties of $f_{a,b}^{(r)}$, and prove that the hyper-bent properties of $f_{a,b}^{(r)}$ can be characterized by that of $f_{a',b'}^{(r)}$, where $a = a'\xi^i \in \mathbb{F}_{2^n}$, $a' \in \mathbb{F}_{2^m}$, b, $b' = b\alpha^{-\frac{i}{r}\frac{2^n-1}{5}} \in \mathbb{F}_{16}$. We also prove that $f_{a,b}^{(r)}$ is not a hyper-bent function unless $n = 12$ or $n = 28$ when $a \in \mathbb{F}_{2^{\frac{m}{2}}}$. Further, we give all the hyper-bent functions for $n = 12$ or $n = 28$. When $m = 0 \pmod 4$, we give a necessary condition for $f_{a,b}^{(r)}$ to be a bent function. To those strict restrictions, it seems $f_{a,b}^{(r)}$ can not be bent. In fact with the help of computer, we have checked all of the functions which satisfy Proposition 13 for $m = 4, 8$, and find that none of them is bent. Thus we guess when $m = 0 \pmod 4$, $f_{a,b}^{(r)}$ can not be bent.

References

[1] C. Tang, Y. Qi, M. Xu, B. Wang and Y. Yang, *A new class of hyper-bent Boolean functions in binomial forms*, http://eprintweb.org/S/article/cs/1112.0062.

[2] A. Canteaut, P. Charpin and G. Kyureghyan, *A new class of monomial bent functions*, Finite Fields Applicat., vol. 14, no. 1, pp 221-241, 2008.

[3] H. Dobbertin and G. Leander, *A survey of some recent results on bent functions*, in T. Helleseth et al. (eds.) Sequences and Their Applications, LNCS 3486, pp. 1-29, Springer, Heidelberg, 2004.

[4] P. Charpin and G. Gong , *Hyperbent functions, Kloosterman sums and Dickson polynomials*, IEEE Trans. Inf. Theory, vol. 9, no. 54, pp 4230-4238, 2008.

[5] G. Lachaud and J. Wolfmann, *The weights of the orthogonal of the extended quadratic binary Goppa codes*, IEEE Trans. Inform. Theory, 36, pp. 686-692, 1990.

[6] S. Mesnager, *A new class of bent boolean functions in polynomial forms*, in Proc. Int. Workshop on Coding and Cryptography, WCC 2009, 2009, pp. 5-18.

[7] S. Mesnager, *A new class of bent and hyper-bent boolean functions in polynomial forms*, Des. Codes Cryptography, 59(1-3), 265-279, 2011

[8] S. Mesnager, *A new family of hyper-bent Boolean functions in polynomial form*, IMACC 2009, LNCS 5921, pp 402-417, 2009.

[9] O. Rothaus, *On bent functions*, J. Combin. Theory, ser. A, vol. 20, pp. 300-305, 1976.

[10] A. Youssef and G. Gong, *Hyper-bent functions*, in Advances in Crypology-Eurocrypt'01, LNCS, pp. 406-419, 2001.

[11] M. Le, *On the number of solutions of the generalized Ramanujan-Nagell equation* $x^2 - D = 2^{n+2}$, ACTA ARITHMETICA, LX.2, pp. 149-167, 1991.

Yu Lou received his Ph.D. degree in School of Mathematical Sciences, Peking University, China in 2013. His research focuses on information security and applied cryptography.

Chunming Tang received his M.S. and Ph.D. degrees from Peking University, China in 2012. He is now in School of Mathematics and Information, China West Normal University, China. His research is in the fields of cryptography, coding theory and information security.

Yanfeng Qi received hishis M.S. and Ph.D. degrees from Peking University, China in 2012. He is now Hangzhou Dianzi University, China. His research interests include cryptography and information security

Maozhi Xu received his Ph.D. degree from Peking University, China in 1994. He is currently a Professor at Laboratory of Mathematics and Applied Mathematics, Chinese Ministry of Education, and School of Mathematical Sciences, Peking University. He is also the Vice-President of Chinese Association for Cryptologic research. His research fields are cryptography and information security.