Noname manuscript No.
(will be inserted by the editor)

A generalization of the class of hyper-bent Boolean functions in binomial forms

Chunming Tang · Yu Lou · Yanfeng Qi · Baocheng Wang · Yixian Yang

Received: date / Accepted: date

Abstract Bent functions, which are maximally nonlinear Boolean functions with even numbers of variables and whose Hamming distance to the set of all affine functions equals $2^{n-1} \pm 2^{\frac{n}{2}-1}$, were introduced by Rothaus in 1976 when he considered problems in combinatorics. Bent functions have been extensively studied due to their applications in cryptography, such as S-box, block cipher and stream cipher. Further, they have been applied to coding theory, spread spectrum and combinatorial design. Hyper-bent functions, as a special class of bent functions, were introduced by Youssef and Gong in 2001, which have stronger properties and rarer elements. Many research focus on the construction of bent and hyper-bent functions. In this paper, we consider functions defined over $\mathbb{F}_{2^n}$ by $f_{a,b}^{(r)} := \mathrm{Tr}_1^n(ax^{r(2^m-1)}) + \mathrm{Tr}_1^4(bx^{\frac{2^n-1}{5}})$, where $n = 2m$, $m \equiv 2 \pmod 4$, $a \in \mathbb{F}_{2^m}$ and $b \in \mathbb{F}_{16}$. When $r \equiv 0 \pmod 5$, we characterize the hyper-bentness of $f_{a,b}^{(r)}$. When $r \not\equiv 0 \pmod 5$, $a \in \mathbb{F}_{2^m}$ and $(b+1)(b^4+b+1) = 0$, with the help of Kloosterman sums and the factorization of $x^5 + x + a^{-1}$, we present a characterization of hyper-bentness of $f_{a,b}^{(r)}$. Further, we give all the hyper-bent functions of $f_{a,b}^{(r)}$ in the case $a \in \mathbb{F}_{2^{\frac{m}{2}}}$.

Chunming Tang, Yu Lou and Yanfeng Qi acknowledge support from the Natural Science Foundation of China (Grant No.10990011 & No.60763009). Baocheng Wang and Yixian Yang acknowledge support from National Science Foundation of China Innovative Grant (70921061), the CAS/SAFEA International Partnership Program for Creative Research Teams.

Chunming Tang, Yu Lou and Yanfeng Qi
Laboratory of Mathematics and Applied Mathematics, School of Mathematical Sciences, Peking University, Beijing, 100871, China
Chunming Tang's e-mail: tangchunmingmath@163.com

Baocheng Wang and Yixian Yang
Information Security Center, Beijing University of Posts and Telecommunications and Research Center on fictitious Economy and Data Science, Chinese Academy of Sciences, Beijing, 100871, China

Keywords Boolean functions · bent functions · hyper-bent functions · Walsh-Hadamard transformation · Kloosterman sums

1 Introduction

Bent functions are maximally nonlinear Boolean functions with even numbers of variables whose Hamming distance to the set of all affine functions equals $2^{n-1} \pm 2^{\frac{n}{2}-1}$. These functions introduced by Rothaus [30] as interesting combinatorial objects have been extensively studied for their applications not only in cryptography, but also in coding theory [4,27] and combinatorial design. Some basic knowledge and recent results on bent functions can be found in [3,12,27]. A bent function can be considered as a Boolean function defined over $\mathbb{F}_2^n$, $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ $(n = 2m)$ or $\mathbb{F}_{2^n}$. Thanks to the different structures of the vector space $\mathbb{F}_2^n$ and the Galois field $\mathbb{F}_{2^n}$, bent functions can be well studied. Although some algebraic properties of bent functions are well known, the general structure of bent functions on $\mathbb{F}_{2^n}$ is not clear yet. As a result, much research on bent functions on $\mathbb{F}_{2^n}$ can be found in [2,7,8,10,11,13,14, 21,22,25–29,32]. Youssef and Gong [31] introduced a class of bent functions called hyper-bent functions, which achieve the maximal minimum distance to all the coordinate functions of all bijective monomials (i.e., functions of the form $\mathrm{Tr}_1^n(ax^i) + \epsilon$, $\gcd(i, 2^n - 1) = 1$). However, the definition of hyper-bent functions was given by Gong and Golomb [15] by a property of the extend Hadamard transform of Boolean functions. Hyper-bent functions as special bent functions with strong properties are hard to characterize and many related problems are open. Much research give the precise characterization of hyper-bent functions in certain forms.

The complete classification of bent and hyper-bent functions is not yet achieved. The monomial bent functions in the form $\mathrm{Tr}_1^n(ax^s)$ are considered in [2,21]. Leander [21] described the necessary conditions for s such that $\mathrm{Tr}_1^n(ax^s)$ is a bent function. In particular, when $s = r(2^m - 1)$ and $(r, 2^m + 1) = 1$, the monomial functions $\mathrm{Tr}_1^n(ax^s)$ (i.e., the Dillon functions) were extensively studied in [7,10,21]. A class of quadratic functions over $\mathbb{F}_{2^n}$ in polynomial form $\sum_{i=1}^{\frac{n}{2}-1} a_i \mathrm{Tr}_1^n(x^{1+2^i}) + a_{\frac{n}{2}} \mathrm{Tr}_1^{\frac{n}{2}}(x^{\frac{n}{2}+1})$ $(a_i \in \mathbb{F}_2)$ was described and studied in [9,17–19,23,32]. Dobbertin et al. [13] constructed a class of binomial bent functions of the form $\mathrm{Tr}_1^n(a_1x^{s_1} + a_2x^{s_2}), (a_1, a_2) \in (\mathbb{F}_{2^n}^*)^2$ with Niho power functions. Garlet and Mesanager [6] studied the duals of the Niho bent functions in [13]. In [25,26,29], Mesnager considered the binomial functions of the form $\mathrm{Tr}_1^n(ax^{r(2^m-1)}) + \mathrm{Tr}_1^2(bx^{\frac{2^n-1}{3}})$, where $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_4^*$. Then he gave the link between the bentness property of such functions and Kloosterman sums. Leander and Kholosha [22] generalized one of the constructions provided by Dobbertin et al. [13] and presented a new primary construction of bent functions consisting of a linear combination of 2^r Niho exponents. Carlet et al. [5] computed the dual of the Niho bent function with 2^r exponents found by Leander and Kholosha [22] and showed that this new bent function is not of the Niho type. Charpin and Gong [7] presented a characterization of bentness of Boolean functions over $\mathbb{F}_{2^n}$ of the form $\sum_{r\in R} \mathrm{Tr}_1^n(a_r x^{r(2^m-1)})$, where R is a subset of the set of representatives of the cyclotomic cosets modulo 2^m+1 of maximal size n. These functions include the well-known monomial functions with the Dillon exponent as a special case. Then they described the bentness of these functions with the Dickson polynomials. Mesnager et al. [27, 28] generalized the results of Charpin and Gong [7] and considered the bentness of Boolean functions over $\mathbb{F}_{2^n}$ of the form $\sum_{r\in R} \mathrm{Tr}_1^n(a_r x^{r(2^m-1)}) + \mathrm{Tr}_1^2(bx^{\frac{2^n-1}{3}})$, where $n=2m$, $a_r \in \mathbb{F}_{2^m}$ and $b \in \mathbb{F}_4$. Further, they presented the link between the bentness of such functions and some exponential sums (involving Dickson polynomials).

In this paper, we consider a class of Boolean functions defined over $\mathbb{F}_{2^n}$ by 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 $n=2m$, $m \equiv 2 \pmod 4$, $a \in \mathbb{F}_{2^m}$ and $b \in \mathbb{F}_{16}$. When $r=1$, this class of Boolean functions is studied in [1]. Generally, it is elusive to give a characterization of bentness and hyper-bentness of Boolean functions. When $r \equiv 0 \pmod 5$, the hyper-bentness of $f_{a,b}^{(r)}$ is characterized in this paper. When $r \not\equiv 0 \pmod 5$ and $(b+1)(b^4+b+1=0)=0$, this paper presents the hyper-bentness of $f_{a,b}^{(r)}$ by the factorization of x^5+x+a^{-1} and Kloosterman sums. For $a \in \mathbb{F}_{2^{\frac{m}{2}}}$, we give all the hyper-bent functions $f_{a,b}^{(r)}$.

The rest of paper is organized as follows. In Section 2, we give some notations and recall some basic knowledge for this paper. In Section 3, we study the hyper-bentness of the Boolean functions $f_{a,b}^{(r)}$ for two cases (1) $(b+1)(b^4+b+1)=0$; (2) $a \in \mathbb{F}_{2^{\frac{m}{2}}}$. Finally, Section 4 makes a conclusion.

2 Preliminaries

2.1 Boolean functions

Let n be a positive integer. $\mathbb{F}_2^n$ is a n-dimensional vector space defined over finite field $\mathbb{F}_2$. Take two vectors $x=(x_1,\cdots,x_n)$ and $y=(y_1,\cdots,x_n)$ in $\mathbb{F}_2^n$. Their dot product is defined by

$$\langle x,y\rangle := \sum_{i=1}^{n} x_i y_i.$$

$\mathbb{F}_{2^n}$ is a finite field with 2^n elements and $\mathbb{F}_{2^n}^*$ is the multiplicative group of $\mathbb{F}_{2^n}$. Let $\mathbb{F}_{2^k}$ be a subfield of $\mathbb{F}_{2^n}$. The trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^k}$, denoted by Tr_k^n, is a map defined as

$$\mathrm{Tr}_k^n(x) := x + x^{2^k} + x^{2^{2k}} + \cdots + x^{2^{n-k}}.$$

When $k=1$, Tr_1^n is called the absolute trace. The trace function Tr_k^n satisfies the following properties.

$$\mathrm{Tr}_k^n(ax+by) = a\mathrm{Tr}_k^n(x) + b\mathrm{Tr}_k^n(y), \quad a,b \in \mathbb{F}_{2^k}, x,y \in \mathbb{F}_{2^n}.$$
$$\mathrm{Tr}_k^n(x^{2^k}) = \mathrm{Tr}_k^n(x), \quad x \in \mathbb{F}_{2^n}.$$

When $\mathbb{F}_{2^k} \subseteq \mathbb{F}_{2^r} \subseteq \mathbb{F}_{2^n}$, the trace function Tr_k^n satisfies the following transitivity property.

$$\mathrm{Tr}_k^n(x) = \mathrm{Tr}_k^r(\mathrm{Tr}_r^n(x)), \quad x \in \mathbb{F}_{2^n}.$$

A Boolean function over $\mathbb{F}_2^n$ or $\mathbb{F}_{2^n}$ is an $\mathbb{F}_2$-valued function. The absolute trace function is a useful tool in constructing Boolean functions over $\mathbb{F}_{2^n}$. From the absolute trace function, a dot product over $\mathbb{F}_{2^n}$ is defined by

$$\langle x,y \rangle := \mathrm{Tr}_1^n(xy), \quad x,y \in \mathbb{F}_{2^n}.$$

A Boolean function over $\mathbb{F}_{2^n}$ is often represented by the algebraic normal form (ANF):

$$f(x_1,\cdots,x_n) = \sum_{I \subseteq \{1,\cdots,n\}} a_I(\prod_{i\in I} x_i), \quad a_I \in \mathbb{F}_2.$$

When $I=\emptyset$, let $\prod_{i\in I} = 1$. The terms $\prod_{i\in I} x_i$ are called monomials. The algebraic degree of a Boolean function f is the globe degree of its ANF, that is, $\deg(f) := \max\{\#(I) | a_I \neq 0\}$, where $\#(I)$ is the order of I and $\#(\emptyset)=0$.

Another representation of a Boolean function is of the form

$$f(x) = \sum_{j=0}^{2^n-1} a_j x^j.$$

In order to make f a Boolean function, we should require $a_0, a_{2^n-1} \in \mathbb{F}_2$ and $a_{2j} = a_j^2$, where $2j$ is taken modulo 2^n-1. This makes that f can be represented by a trace expansion of the form

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

called its polynomial form, where

- Γ_n is the set of integers obtained by choosing one element in each cyclotomic class of 2 module 2^n-1 (j is often chosen as the smallest element in its cyclotomic class, called the coset leader of the class);
- $o(j)$ is the size of the cyclotomic coset of 2 modulo 2^n-1 containing j;
- $a_j \in \mathbb{F}_{2^{o(j)}}$;
- $\epsilon = wt(f) \pmod 2$, where $\mathrm{wt}(f) := \#\{x \in \mathbb{F}_{2^n} | f(x) = 1\}$.

Let $\mathrm{wt}_2(j)$ be the number of 1's in the binary expansion of j. Then

$$\deg(f) = \begin{cases} n, & \epsilon = 1 \\ \max\{\mathrm{wt}_2(j) | a_j \neq 0\}, & \epsilon = 0. \end{cases}$$

2.2 Bent and hyper-bent functions

The "sign" function of a Boolean function f is defined by

$$\chi(f) := (-1)^f.$$

When f is a Boolean function over $\mathbb{F}_2^n$, the Walsh Hadamard transform of f is the discrete Fourier transform of $\chi(f)$, whose value at $w \in \mathbb{F}_2^n$ is defined by

$$\widehat{\chi}_f(w) := \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)+\langle w,x\rangle}.$$

When f is a Boolean function over $\mathbb{F}_{2^n}$, the Walsh Hadamard transform of f is defined by

$$\widehat{\chi}_f(w) := \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{Tr}_1^n(wx)},$$

where $w \in \mathbb{F}_{2^n}$. Then we can define the bent functions.

Definition 1 A Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is called a bent function, if $\widehat{\chi}_f(w) = \pm 2^{\frac{n}{2}}$ $(\forall w \in \mathbb{F}_{2^n})$.

If f is a bent function, n must be even. Further, $\deg(f) \leq \frac{n}{2}$ [3]. Hyper-bent functions are an important subclass of bent functions. The definition of hyper-bent functions is given below.

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.

[4] and [31] proved that if f is a hyper-bent function, then $\deg(f) = \frac{n}{2}$. For a bent function f, $\mathrm{wt}(f)$ is even. Then $\epsilon = 0$, that is,

$$f(x) = \sum_{j\in\Gamma_n} \mathrm{Tr}_1^{o(j)}(a_j x^j).$$

If a Boolean function f is defined over $\mathbb{F}_{2^{\frac{n}{2}}} \times \mathbb{F}_{2^{\frac{n}{2}}}$, then we have a class of bent functions[10, 24].

Definition 3 The Maiorana-McFarland class $\mathcal{M}$ is the set of all the Boolean functions f defined on $\mathbb{F}_{2^{\frac{n}{2}}} \times \mathbb{F}_{2^{\frac{n}{2}}}$ of the form $f(x, y) = \langle x, \pi(y)\rangle + g(y)$, where $x, y \in \mathbb{F}_{2^{\frac{n}{2}}}$, π is a permutation of $\mathbb{F}_{2^{\frac{n}{2}}}$ and $g(x)$ is a Boolean function over $\mathbb{F}_{2^{\frac{n}{2}}}$.

For Boolean functions over $\mathbb{F}_{2^{\frac{n}{2}}} \times \mathbb{F}_{2^{\frac{n}{2}}}$, we have a class of hyper-bent functions $\mathcal{PS}_{ap}$ [4].

Definition 4 Let $n = 2m$, the $\mathcal{PS}_{ap}$ class is the set of all the Boolean functions of the form $f(x, y) = g(\frac{x}{y})$, where $x, y \in \mathbb{F}_{2^m}$ and g is a balanced Boolean functions (i.e., $\mathrm{wt}(f) = 2^{m-1}$) and $g(0) = 0$. When $y = 0$, let $\frac{x}{y} = xy^{2^n-2} = 0$.

Each Boolean function f in $\mathcal{PS}_{ap}$ satisfies $f(\beta z) = f(z)$ and $f(0) = 0$, where $\beta \in \mathbb{F}_m^*$ and $z \in \mathbb{F}_m \times \mathbb{F}_m$. Youssef and Gong [31] studied these functions over $\mathbb{F}_{2^n}$ and gave the following property.

Proposition 1 *Let $n = 2m$, α be a primitive element in $\mathbb{F}_{2^n}$ and f be a Boolean function over $\mathbb{F}_{2^n}$ such that $f(\alpha^{2^m+1}x) = f(x)(\forall x \in \mathbb{F}_{2^n})$ and $f(0) = 0$, then f is a hyper-bent function if and only if the weight of $(f(1), f(\alpha), f(\alpha^2), \cdots, f(\alpha^{2^m}))$ is 2^{m-1}.*

Further, [4] proved the following result.

Proposition 2 *Let f be a Boolean function defined in Proposition 1. If $f(1) = 0$, then f is in $\mathcal{PS}_{ap}$. If $f(1) = 1$, then there exists a Boolean function g in $\mathcal{PS}_{ap}$ and $\delta \in \mathbb{F}_{2^n}^*$ satisfying $f(x) = g(\delta x)$.*

Let $\mathcal{PS}_{ap}^{\#}$ be the set of hyper-bent functions in the form of $g(\delta x)$, where $g(x) \in \mathcal{PS}_{ap}$, $\delta \in \mathbb{F}_{2^n}^*$ and $g(\delta) = 1$. Charpin and Gong expressed Proposition 2 in a different version below.

Proposition 3 *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}.*

In fact, Dillon [10] introduced the Partial Spreads class $\mathcal{PS}^-$, which is a bigger class of bent functions than $\mathcal{PS}_{ap}$ and $\mathcal{PS}_{ap}^{\#}$.

Theorem 1 *Let $E_i (i = 1, 2, \cdots, N)$ be N subspaces in $\mathbb{F}_{2^n}$ of dimension m such that $E_i \cap E_j = \{0\}$ for all $i, j \in \{1, \cdots, N\}$ with $i \neq j$. Let f be a Boolean function over $\mathbb{F}_{2^n}$. If the support of f is given by $supp(f) = \bigcup_{i=1}^{N} E_i^*$, where $E_i^* = E_i \backslash \{0\}$, then f is a bent function if and only if $N = 2^{m-1}$.*

The set of all the functions in Theorem 1 is defined by $\mathcal{PS}^-$.

2.3 Kloosterman sums and Weil sums

The Kloosterman sums on $\mathbb{F}_{2^n}$ are:

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

Some properties of Kloosterman sums are given by the following proposition[16, 20].

Proposition 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:

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

To determine the value of $Q_m(a)$, we should consider the factorization of the polynomial $P(x) = x^5 + x + a^{-1}$. We write that $P(x) = (n_1)^{r_1}(n_2)^{r_2} \cdots (n_t)^{r_t}$

to indicate that r_i of the irreducible factors of $P(x)$ have degree n_i. When $P(x) = x^5 + x + a^{-1}$ is irreducible over $\mathbb{F}_{2^m}$, the value of $Q_m(a)$ is related to the parity of the quadratic form $\mathfrak{q}(x) = \mathrm{Tr}_1^m(x(ax^4 + ax^2 + a^2x))$. $\mathfrak{q}(x)$ is the quadratic form associated to the simplectic form:

$$< x, y >_{\mathfrak{q}} := \mathrm{Tr}_1^m(x(ay^4 + ay^2 + a^2y) + y(ax^4 + ax^2 + a^2x)),$$

which is non-degenerate. Then there exists a normal simplectic basis e_1, e_{m_1+1}, $\cdots$, e_{m_1}, e_{2m_1} $(2m_1 = m)$. If $i \not\equiv j (\mod m_1)$, $< e_i, e_j >_{\mathfrak{q}} = 0$. For any i $(1 \leq i \leq m_1)$, $< e_i, e_{m_1+i} >_{\mathfrak{q}} = 1$. If $\#\{i|\mathfrak{q}(e_i) = \mathfrak{q}(e_{m_1+i}) = 1, 1 \leq i \leq m_1\}$ is even, then the quadratic form $\mathfrak{q}(x)$ is called an even quadratic form and $Q_m(a) = 2^{m_1}$. If $\#\{i|\mathfrak{q}(e_i) = \mathfrak{q}(e_{m_1+i}) = 1, 1 \leq i \leq m_1\}$ is odd, then the quadratic form $\mathfrak{q}(x)$ is called a odd quadratic form and $Q_m(a) = -2^{m_1}$.

3 A generalization of the class of hyper-bent functions in binomial forms

In this section, we will discuss the hyper-bentness of $f_{a,b}^{(r)}(x)$. We introduce some notations on character sums in [1]. Let $\xi = \alpha^{2^m-1}$, then $U =< \xi >$. Let $V =< \xi^5 >$. Since $5|(2^m + 1)$, V is the subgroup of U and $\#V = \frac{2^m+1}{5}$. Let $\beta = \alpha^{\frac{2^n-1}{5}}$.

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

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

From the definition of S_i, $S_i = S_j$ when $i \equiv j \pmod 5$. Further, $S_i = S_{-i}$(Lemma 1 [1]).

3.1 The hyper-bentness of Boolean functions $f_{a,b}^{(5)}(x)$

In this subsection, we consider the hyper-bentness of $f_{a,b}^{(r)}(x)$ with $r = 5$ of the form

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

where $n = 2m$, $m \equiv 2 \pmod 4$, $a \in \mathbb{F}_{2^m}$ and $b \in \mathbb{F}_{16}$.

Since $m \equiv 2 \pmod 4$, $2^m + 1 \equiv 0 \pmod 5$. For any $y \in \mathbb{F}_{2^m}$, $y^{2^m-1} = 1$. Then

$$f_{a,b}^{(5)}(\alpha^{2^m+1}x) = f_{a,b}^{(5)}(x), \quad x \in \mathbb{F}_{2^n},$$

where α is a primitive element of $\mathbb{F}_{2^n}$. Further, $f_{a,b}^{(5)}(0) = 0$. Then, from Proposition 3, we have the following proposition on the hyper-bentness of $f_{a,b}^{(5)}(x)$.

Proposition 5 *Let $f_{a,b}^{(5)}$ be the Boolean function defined by* (1)*, where $a \in \mathbb{F}_{2^m}$ and $b \in \mathbb{F}_{16}$. Define the following character sum*

$$\Lambda_5(a,b) := \sum_{u \in U} \chi(f_{a,b}^{(5)}(u)) \tag{2}$$

where U is the group of all the 2^m+1-th root of unity in $\mathbb{F}_{2^n}$, that is, $U = \{x \in \mathbb{F}_{2^n} | x^{2^m+1} = 1\}$. Then $f_{a,b}^{(5)}$ is a hyper-bent function if and only if $\Lambda_5(a,b) = 1$. Further, the hyper-bent function $f_{a,b}^{(5)}$ lies in $\mathcal{PS}_{ap}$ if and only if $\mathrm{Tr}_1^4(b) = 0$.

Proof Similar to the proof of Proposition 9 in [1], this proposition follows.

Proposition 6 *Let $n = 2m$ and $m \equiv \pm 2, \pm 6 \pmod{20}$, If $b \in \{0\} \bigcup \{\beta^i | i = 0,1,2,3,4\}$, then the Boolean function $f_{a,b}^{(5)}$ in* (1) *is not a hyper-bent function. Further, if $b \in \mathbb{F}_{16}^* \backslash \{\beta^i | 0 \le i \le 4\}$, $f_{a,b}^{(5)}$ is a hyper-bent function if and only if*

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

Proof From (2),

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

Note that $U = <\xi>$, $V = <\xi^5>$ and

$$U = \xi^0 V \bigcup \xi^1 V \bigcup \xi^2 V \bigcup \xi^3 V \bigcup \xi^4 V. \tag{3}$$

Then,

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

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,

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

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

$$\begin{aligned}\Lambda_5(a,b) &= (\sum_{i=0}^{4}\chi(\mathrm{Tr}_1^4(b\beta^{3i}))(\sum_{v\in V}\chi(\mathrm{Tr}_1^n(av))) \\ &= (\sum_{i=0}^{4}\chi(\mathrm{Tr}_1^4(b\beta^{i}))(\sum_{v\in V}\chi(\mathrm{Tr}_1^n(av))). \qquad (5)\end{aligned}$$

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

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

$$\sum_{i=0}^{4}\chi(\mathrm{Tr}_1^4(b\beta^i)) = \sum_{i=0}^{4}\chi(\mathrm{Tr}_1^4(\omega\beta^{i+j})) = \sum_{i=0}^{4}\chi(\mathrm{Tr}_1^4(\omega\beta^i))). \qquad (6)$$

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

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

In particular, we take $i = 1, 2$. Then

$$\mathrm{Tr}_1^4(\omega\beta) = \mathrm{Tr}_1^4(\omega\beta^4), \qquad (7)$$
$$\mathrm{Tr}_1^4(\omega\beta^2) = \mathrm{Tr}_1^4(\omega\beta^3). \qquad (8)$$

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

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

From Propsition 5, $f^{(5)}_{a,\beta^j}$ is not a hyper-bent function. When $\omega \neq 1$, we have

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

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,

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

From Proposition 5, the second part of this proposition follows.

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

Proposition 7 *Let $n = 2m$, $m \equiv 10 \pmod{20}$, $a \in \mathbb{F}_{2^m}$, $b \in \mathbb{F}_{16}$. then the Boolean function $f^{(5)}_{a,b}$ in (1) is not a hyper-bent function.*

Proof Note 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 5 to 1 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, From Proposition 5, $f^{(5)}_{a,b}$ is not a hyper-bent function.

From Proposition 6,

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

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

$$\sum_{v\in V} \chi(\mathrm{Tr}_1^n(av)) = \frac{1}{5}[1 - K_m(a) + 2Q_m(a)]. \quad (9)$$

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

Proposition 8 *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 $f^{(5)}_{a,b}$ 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) $Q_m(a) = 2^{m_1}$, $K_m(a) = 2 \cdot 2^{m_1} - 4$.

From Theorem 3 in [1], we have the following theorem.

Theorem 2 *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 following 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. $K_m(a) = 2 \cdot 2^{m_1} - 4$.

3.2 The hyper-bentness of $f_{a,b}^{(r)}(x)$

In the rest of the paper, we consider the Boolean function

$$f_{a,b}^{(r)}(x) := \mathrm{Tr}_1^n(ax^{r(2^m-1)}) + \mathrm{Tr}_1^4(bx^{\frac{2^n-1}{5}}), \tag{10}$$

where $n = 2m$, $m \equiv 2 \pmod 4$, $a \in \mathbb{F}_{2^m}$ and $b \in \mathbb{F}_{16}$. Then we define the character sum

$$\Lambda_r(a,b) := \sum_{u \in U} \chi(f_{a,b}^{(r)}(u)). \tag{11}$$

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

Theorem 3 *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 $f_{a,b}^{(5)}$ have the same hyper-bentness.

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

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

Proof Note that

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

Let $d := (r(2^m - 1), \#V) = (r, \frac{2^m+1}{5})$, then

$$\Lambda_r(a,b) = d \sum_{i=0}^{4} \chi(\mathrm{Tr}_1^4(b\xi^{i\frac{2^n-1}{5}})) \sum_{v \in V^d} \chi(\mathrm{Tr}_1^n(a\xi^{ri(2^m-1)}v^{r(2^m-1)})), \tag{12}$$

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

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

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

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

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

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

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

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

From Lemma 1 in [1], then

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

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

If $r \equiv 3 \pmod 5$,

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

From Lemma 1 in [1],

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

Hence, $\Lambda_r(a,b) = \Lambda_3(a,b)$. From (14) and (15),

$$\Lambda_2(a,b) = \Lambda_3(a,b).$$

$f_{a,b}^{(r)}$ and $f_{a,b}^{(2)}$ have the same hyper-bentness.

Similarly, if $r \equiv 4 \pmod 5$,

$$\Lambda_r(a,b) = \Lambda_4(a,b) = \Lambda_1(a,b).$$

$f_{a,b}^{(r)}$ and $f_{a,b}^{(1)}$ have the same hyper-bentness.

Above all, this theorem follows.

From Theorem 3, to characterize the hyper-bentness of $f_{a,b}^{(r)}$, we just consider the hyper-bentness of $f_{a,b}^{(1)}$, $f_{a,b}^{(2)}$ and $f_{a,b}^{(5)}$. The hyper-bentness of $f_{a,b}^{(1)}$ is considered in [1]. And the hyper-bentness of $f_{a,b}^{(5)}$ is discussed before. Next, we just study the hyper-bentness of $f_{a,b}^{(2)}$.

When $b = 0$, the hyper-bentness of $f_{a,0}^{(2)}$ is given in [2]. Then we just consider the case $b \neq 0$. We first give properties of $\Lambda_2(a,b)$ in the following proposition.

Proposition 9 *Let $a \in \mathbb{F}_{2^m}$ and $b \in \mathbb{F}_{16}^*$, then*

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

(2) *If $b \in \{\beta+\beta^2, \beta+\beta^3, \beta^2+\beta^4, \beta^3+\beta^4\}$, that is, b is a primitive element satisfying $\mathrm{Tr}_1^4(b) = 0$, 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 From (14) and the similar proof of Proposition 13 in [1], this proposition follows.

Corollary 1 *Let $a \in \mathbb{F}_{2^m}$ and $b \in \mathbb{F}_{16}^*$, then*

(1) $f_{a,b}^{(2)}$ and $f_{a,b^2}^{(1)}$ have the same hyper-bentness.

(2) If b satisfies $(b+1)(b^4+b+1)=0$, then $f_{a,b}^{(2)}$ and $f_{a,b}^{(1)}$ have the same hyper-bentness.

Proof (1) From Proposition 13 in [1] and Proposition 9,

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

Hence, $f_{a,b}^{(2)}$ and $f_{a,b^2}^{(1)}$ have the same hyper-bentness.

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

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

Hence, $f_{a,b}^{(2)}$ and $f_{a,b}^{(1)}$ have the same hyper-bentness.

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

Proposition 10 *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.

In fact, the converse proposition still holds.

Proof From Proposition 16 in [1] and Theorem 3, (9) and Proposition 6, this proposition follows.

We generalize Theorem 3 in [1] and get the following theorem.

Theorem 4 *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

In fact, the converse theorem still holds.

Proof From Proposition 16 and Theorem 3 in [1] and Proposition 10, this theorem follows.

Similar to Theorem 2 in [1], we have the following result.

Theorem 5 *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) $K_m(a) = \frac{4}{3}(2 - 2^{m_1})$.

In fact, the converse theorem still holds.

Proof From Proposition 16 and Theorem 2 in [1] and Proposition 10, this theorem follows.

If $a \in \mathbb{F}_{2^{\frac{m}{2}}}$, we have the hyper-bentness of $f_{a,b}^{(r)}$ in the theorem below.

Theorem 6 *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 Note that $a \in \mathbb{F}_{2^{\frac{m}{2}}}$. From Theorem 3, 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 $r \equiv 0 \pmod 5$. From Theorem 3, $f_{a,b}^{(r)}$ 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 $b \neq 0$, from Theorem 4, $f_{a,b}^{(r)}$ is a hyper-bent function if and only if $f_{a,b'}^{(1)}$ $(b'^4 + b' + 1 = 0)$ is a hyper-bent function. From 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 $r \equiv 0 \pmod 5$.

Then we discuss the case $r \equiv \pm 1 \pmod 5$ and $(r, \frac{2^m+1}{5}) = 1$. From Theorem 3, $f_{a,b}^{(r)}$ is a hyper-bent function if and only if $f_{a,b}^{(1)}$ is a hyper-bent function. From 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.

4 Conclusion

This paper considers the hyper-bentness 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 $n = 2m$, $m = 2 \pmod 4$, $a \in \mathbb{F}_{2^m}$ and $b \in \mathbb{F}_{16}$. When $r \equiv 0 \pmod 5$, we give the characterization of hyper-bentness of $f_{a,b}^{(r)}$. If $r \not\equiv 0 \pmod 5$ and $b = 1$ or b is a primitive element in $\mathbb{F}_{16}$ such that $\mathrm{Tr}_1^4(b) = 0$, the hyper-bentness of $f_{a,b}^{(r)}$ can be characterized by Kloosterman sums and the factorization of $x^5 + x + a^{-1}$. If $a \in \mathbb{F}_{2^{\frac{m}{2}}}$, with the results of [1], we prove that $f_{a,b}^{(r)}$ is not a hyper-bent function unless $n = 12$ or $n = 28$. Further, we give all the hyper-bent functions for $n = 12$ or $n = 28$.

References

1. Chunming Tang, Yanfeng Qi, Maozhi Xu, Baocheng Wang, Yixian Yang, A new class of hyper-bent Boolean functions in binomial forms, arXiv:1112.0062, http://eprintweb.org/S/article/cs/1112.0062.
2. Canteaut A., Charpin P., Kyureghyan G.: A new class of monomial bent functions, Finite Fields Applicat., vol. 14, no. 1, pp 221-241, 2008.
3. Carlet C.: Boolean functions for cryptography and error correcting codes, in Chapter of the Monography Boolean Models and Method in Mathematics, Computer Science, and Engineering, Y. Crama and P. L. Hammer, Eds. Cambridge, U.K.: Cambridge Univ. Press, 2010 pp. 257-397.
4. Carlet C., Gaborit P.: Hyperbent functions and cyclic codes, J Combin. Theory, ser. A, vol. 113, no. 3, pp. 466-482, 2006.
5. Carlet C., Helleseth T., Kholosha A., Mesnager S.: On the Dual of the Niho Bent Functions with 2^r Exponents, 2011, to be published.
6. Carlet C., Mesnager S.: On Dillon's Class H of Bent Functions Niho Bent Functions and O-Polynomials Cryptology ePrint Archive Report no 567.
7. Charpin P., Gong G.: Hyperbent functions, Kloosterman sums and Dickson polynomials, IEEE Trans. Inf. Theory, vol. 9, no. 54, pp 4230-4238, 2008.
8. Charpin P., Kyureghyan G.: Cubic monomial bent functions: A subclass of $\mathcal{M}$, SIAM J. Discr. Math., vol. 22, no. 2, pp. 650-665 2008.
9. Charpin P., Pasalic E., Tavernier C., On bent and semi-ben quadratic Boolean functions, IEEE Trans. Inf. Theory, vol. 51, no 12, pp. 4286-4298, 2005.
10. Dillon J.:, Elementary Hadamard Difference Sets, Ph.D., Univ.Mary- land, 1974.

11. Dillon J. F., Dobbertin H.: New cyclic difference sets with Singer parameters, Finite Fields Applicat., vol. 10, no. 3, pp. 342-389, 2004.
12. Dobbertin H., Leander G.: 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.
13. Dobbertin H., Leander G., Canteaut A., Carlet C., Felke P., Gaborit P.: Construction of bent functions via Niho power functions, J. Combin. Theory, ser. A, vol. 113, pp. 779-798, 2006.
14. Gold R.: Maximal recursive sequences with 3-valued recursive crosscorrelation functions, IEEE Trans. Inf. Theory, vol. 14, no. 1, pp. 154-156, 1968.
15. Gong G., Golomb S. W.: Transform domain analysis of DES, IEEE Trans. Inf. Theory, vol. 45, no. 6, pp. 2065-2073, 1999.
16. Helleseth T., Zinoviev V.A.: On Z_4-Linear Goethals Codes and Kloosterman Sums, Designs, Codes and Cryptography, vol. 17, no. 1-3, pp. 246-262, 1999.
17. Hu H., Feng D.: On quadratic bent functions in polynomial forms, IEEE Trans. Inf. Theory, vol. 53, no. 7, pp. 2610-2615, 2007.
18. Kasami T.: Weight enumerators for several classes of subcodes of the 2nd-order Reed-CMuller codes, Inf. Contr., vol. 18, pp. 369-394, 1971.
19. Kim S. H., No J. S.: New families of binary sequences with low correlation, IEEE Trans. Inf. Theory, vol. 49, no. 11, pp. 3059-3065, 2003.
20. Lachaud G., Wolfmann J.: The weights of the orthogonal of the extended quadratic binary Goppa codes, IEEE Trans. Inform. Theory, 36 (1990), pp. 686-692
21. Leander G.: Monomial bent functions, IEEE Trans. Inf. Theory, vol. 2, no. 52, pp. 738-743, 2006.
22. Leander G., Kholosha A.: Bent functionswith Niho exponents, IEEE Trans. Inf. Theory, vol. 52, no. 12, pp. 5529-5532, 2006.
23. Ma W., Lee M., Zhang F.: A new class of bent functions, IEICE Trans. Fund., vol. E88-A, no. 7, pp. 2039-2040, 2005.
24. McFarland R. L.: A family of noncyclic difference sets, J. Combin. Theory, ser. A, no. 15, pp. 1-10, 1973.
25. Mesnager S.: A new class of bent boolean functions in polynomial forms, in Proc. Int. Workshop on Coding and Cryptography, WCC 2009, 2009, pp. 5-18.
26. Mesnager S.: A new class of bent and hyper-bent boolean functions in polynomial forms, Des. Codes Cryptography, 59(1-3):265-279, 2011
27. Mesnager S.: Bent and Hyper-Bent Functions in Polynomial Form and Their Link With Some Exponential Sums and Dickson Polynomials, IEEE Trans. Inf. Theory, vol. 57, no. 9, pp. 5996-6009, 2011
28. Mesnager S.: Hyper-bent boolean functions with multiple trace terms. In M. Anwar Hasan and Tor Helleseth, editors, WAIFI, volume 6087 of Lecture Notes in Computer Science, pages 97-113. Springer, 2010.
29. Mesnager S.: A new family of hyper-bent Boolean functions in polynomial form. Proceedings of Twelfth International Conference on Cryptography and Coding, Cirencester, United Kingdom. M. G. Parker (Ed.): IMACC 2009, LNCS 5921, pp 402-417, Springer, Heidelberg (2009).
30. Rothaus O. S.: On bent functions, J. Combin. Theory, ser. A, vol. 20, pp. 300-305, 1976.
31. Youssef A. M., Gong G.: Hyper-bent functions, in Advances in CrypologyCEurocrypt01, 2001, LNCS, pp. 406-419.
32. Yu N. Y., Gong G.: Construction of quadratic bent functions in polynomial forms, IEEE Trans. Inf. Theory, vol. 7, no. 52, pp. 3291-3299, 2006.