A New Class of Hyper-bent Boolean Functions with Multiple Trace Terms

Baocheng Wang, Chunming Tang, Yanfeng Qi, Yixian Yang, Maozhi Xu

***Abstract*—Introduced by Rothaus in 1976 as interesting combinatorial objects, bent functions are maximally nonlinear Boolean functions with even numbers of variables whose Hamming distance to the set of all affine functions equals $2^{n-1} \pm 2^{\frac{n}{2}-1}$. Not only bent functions are applied in cryptography, such as applications in components of S-box, block cipher and stream cipher, but also they have relations to coding theory. Hence a lot of research have been paid on them. Youssef and Gong introduced a new class of bent functions the so-called hyper-bent functions which have stronger properties and rarer elements. It seems that hyper-bent functions are more difficult to generate. Moreover, (hyper)-bent functions are not classified. Charpin and Gong studied a class of hyper-bent functions f defined on $\mathbb{F}_{2^n}$ by $f = \sum_{r\in R} \mathrm{Tr}_1^n(a_r x^{r(2^m-1)})$, $n = 2m$ and $a_r \in \mathbb{F}_{2^n}$, where R is a subset of a set of representatives of the cyclotomic cosets modulo 2^m+1 for which each coset has the full size n. Further, Mesnager contributed to the knowledge of a class of hyper-bent functions f_b defined over $\mathbb{F}_{2^n}$ by $f_b = \sum_{r\in R} \mathrm{Tr}_1^n(a_r x^{r(2^m-1)}) + \mathrm{Tr}_1^2(bx^{\frac{2^n-1}{3}})$, $b \in \mathbb{F}_4$, $n = 2m$ and $a_r \in \mathbb{F}_{2^m}$. In this paper, we study a new class of the hyper-bent functions f_b defined over $\mathbb{F}_{2^n}$ by $f_b = \sum_{r\in R} \mathrm{Tr}_1^n(a_r x^{r(2^m-1)}) + \mathrm{Tr}_1^4(bx^{\frac{2^n-1}{5}})$, $b \in \mathbb{F}_{16}$, $n = 2m$ and $a_r \in \mathbb{F}_{2^m}$.**

***Index Terms*—Boolean functions, bent functions, hyper-bent functions, Walsh-Hadamard tranformation, Dickson polynomials.**

I. Introduction

Bent functions with even numbers of variables are maximally nonlinear Boolean functions, that is, their hamming distance to the set of all affine functions equals $2^{n-1} \pm 2^{\frac{n}{2}-1}$. Bent functions were defined and named by Rothaus [28] in the study of combinatorial objects. They have been extensively studied for their applications in cryptography, but have also been applied to spread spectrum, coding theory [3], [24] and combinatorial design. The recent study of bent functions along with properties and constructions of bent functions can be found in [2], [11], [24]. A bent function can be seemed as a function defined on $\mathbb{F}_2^n$, $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, or $\mathbb{F}_{2^n}$ $(n = 2m)$. Thanks to the different structures of the vectorspace $\mathbb{F}_2^n$ and the Galois field $\mathbb{F}_{2^n}$, bent functions can be well studied. However, it is not yet clear on the general structure of bent functions over $\mathbb{F}_{2^n}$. Further, it seems impossible to classify bent functions. As a result, many research works are devoted to the description of new class of bent functions [1], [6], [7], [9], [10], [12], [13], [18], [19], [25], [23], [22], [24], [26], [30]. Youssef and Gong [29] 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 $\mathrm{Tr}_1^n(ax^i) + \epsilon$, $\gcd(c, 2^n - 1) = 1$). Actually, it is Gong and Golomb [14] who, based on a property of the extended Hadamard transform of Boolean functions, presented the definition of hyper-bent functions. The classification of hyper-bent function has not been achieved yet.

Many related problems are still open. Many research focus on the characterization of bentness of Boolean functions. The monomial bent functions in the form $\mathrm{Tr}_1^n(ax^s)$ are considered in [1], [18]. Leander [18] 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 [6], [9], [18]. 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 [8], [15], [16], [17], [20], [30]. Dobbertin et al. [12] constructed a class of binomial bent functions of the form $\mathrm{Tr}_1^n(a_1 x^{s_1} + a_2 x^{s_2}), (a_1, a_2) \in (\mathbb{F}_{2^n}^*)^2$ with Niho power functions. Garlet and Mesanager [5] studied the duals of the Niho bent functions in [12]. In [22], [23], [26], 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 [19] generalized one of the constructions proven by Dobbertin et al. [12] and presented a new primary construction of bent functions consisting of a linear combination of 2^r Niho exponents. Carlet et al. [4] computed the dual of the Niho bent function with 2^r exponents found by Leander and Kholosha [19] and showed that this new bent function is not of the Niho type. Charpin and Gong [6] 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. [24], [25] generalized the results of Charpin and Gong [6] and considered the bentness of Boolean functions over $\mathbb{F}_{2^n}$ of the

B. Wang and Y, Yang are with Information Security Center, Beijing University of Posts and Telecommunications and Research Center on fictitious Economy and Data Science, Chinese Academy of Sciences, Beijing, 100088, China

C. Tang, Y. Qi and M. Xu are with Laboratory of Mathematics and Applied Mathematics, School of Mathematical Sciences , Peking University, 100871, China

C. Tang's e-mail: tangchunmingmath@163.com

form $\sum\limits_{r\in R}\mathrm{Tr}_1^n(a_rx^{r(2^m-1)})+\mathrm{Tr}_1^2(bx^{\frac{2^n-1}{3}})$, 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 over $\mathbb{F}_{2^n}$ in $\mathcal{D}_n$. These Boolean functions are given by the form $\sum\limits_{r\in R}\mathrm{Tr}_1^n(a_rx^{r(2^m-1)})+\mathrm{Tr}_1^4(bx^{\frac{2^n-1}{5}})$, where $n=2m$, $m\equiv 2 \pmod 4$, $a_r\in\mathbb{F}_{2^m}$ and $b\in\mathbb{F}_{16}$. When $b=0$, Charpin and Gong [6] described the bentness and hyper-bentness of these functions with some character sums involving Dickson polynomial. Generally, it is elusive to give a characterization of bentness and hyper-bentness of Boolean functions in $\mathcal{D}_n$. This paper presents the bentness and hyper-bentness of functions in $\mathcal{D}_n$ in two cases: (1) $b=1$ and $b^4+b+1=0$; (2) $a_r\in\mathbb{F}_{\frac{m}{2}}$.

The rest of the paper is organized as follows. In Section II, we give some notations and review some knowledge on bent functions. In Section III, we consider the bentness and hyper-bentness of Boolean functions in $\mathcal{D}_n$ in two cases: (1) $b=1$ and $b^4+b+1=0$; (2) $a_r\in\mathbb{F}_{\frac{m}{2}}$. The bentness and hyper-bentness of these functions for the two cases are related to some character sums involving Dickson polynomials and some equations on the weights of some Boolean functions. In Section IV, we list some examples. Finally, Section V makes a conclusion for the paper.

II. Preliminaries

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 in $\mathbb{F}_2^n$ $x=(x_1,\cdots,x_n)$ and $y=(y_1,\cdots,x_n)$. Their dot product is defined by

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

$\mathbb{F}_{2^n}$ 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 $\prod\limits_{i\in I}=1$. The terms $\prod\limits_{i\in I}x_i$ 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

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

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

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

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 its binary expansion. Then

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

The "sign" function of 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 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, $\deg(f)\leq\frac{n}{2}$ [2]. Hyper-bent functions are an important subclass of bent functions. The definition of hyper-bent functions is given below.

Definition 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.

[3] and [29] 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 on $\mathbb{F}_{2^{\frac{n}{2}}} \times \mathbb{F}_{2^{\frac{n}{2}}}$, then we have a class of bent functions.

Definition 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 $\mathcal{PS}_{ap}$ [3].

Definition 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 [29] studied these functions over $\mathbb{F}_{2^n}$ and gave the following property.

Proposition 2.1: 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, [3] proved the following result.

Proposition 2.2: Let f be a Boolean function defined in Proposition 2.1. 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 2.2 in a different version below.

Proposition 2.3: 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 [9] introduced a bigger class of bent functions the Partial Spreads class $\mathcal{PS}^-$ than $\mathcal{PS}_{ap}$ and $\mathcal{PS}_{ap}^{\#}$.

Theorem 2.4: 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 2.4 is defined by $\mathcal{PS}^-$.

Now we recall the knowledge of Dickson polynomials over $\mathbb{F}_2$. For $r > 0$, Dickson polynomials are given by

$$D_r(x) = \sum_{i=0}^{\lfloor \frac{r}{2} \rfloor} \frac{r}{r-i} \binom{r-i}{i} x^{r-2i}, r = 2, 3, \cdots.$$

Further, Dickson polynomials can be also defined by the following recurrence relation.

$$D_{i+2}(x) = xD_{i+1} + D_i(x)$$

with initial values

$$D_0(x) = 0, D_1(x) = x.$$

Some properties of Dickson polynomials are given below.

- $\deg(D_r(x)) = r$.
- $D_{rp}(x) = D_r(D_p(x))$.
- $D_r(x + x^{-1}) = x^r + x^{-r}$.

The first few Dickson polynomials with odd r are

$$\begin{aligned} &D_1(x) = x, \\ &D_3(x) = x + x^3, \\ &D_7(x) = x + x^5 + x^7, \\ &D_9(x) = x + x^5 + x^7 + x^9, \\ &D_{11}(x) = x + x^3 + x^5 + x^9 + x^{11}. \end{aligned}$$

III. The bentness of a new class of Boolean functions with multiple trace terms

A. Boolean functions in $\mathcal{D}_n$

Let $n = 2m$ and $m \equiv 2 \pmod 4$. Let E be the set of representing elements in each cyclotomic class of 2 module $2^n - 1$. Let $\mathcal{D}_n$ be the set of Boolean functions f_b over $\mathbb{F}_{2^n}$ of the form

$$f_b(x) := \sum_{r \in R} \mathrm{Tr}_1^n(a_r x^{r(2^m-1)}) + \mathrm{Tr}_1^4(bx^{\frac{2^n-1}{5}}) \tag{1}$$

where $R \subseteq E$, a_r is in $\mathbb{F}_{2^m}$ and $b \in \mathbb{F}_{16}$.

Note that the cyclotomic coset of 2 module $2^n - 1$ containing $\frac{2^n-1}{5}$ is $\{\frac{2^n-1}{5}, 2 \cdot \frac{2^n-1}{5}, 2^2 \cdot \frac{2^n-1}{5}, 2^3 \cdot \frac{2^n-1}{5}\}$. Then its size is 4, that is, $o(\frac{2^n-1}{5}) = 4$. Hence, the Boolean function f_b is not in the class considered by Charpin and Gong [6].

From $m \equiv 2 \pmod 4$, $2^m + 1 \equiv 0 \pmod 5$. Then every Boolean function f_b satisfies

$$f_b(\alpha^{2^m+1}x) = f_b(x), \forall x \in \mathbb{F}_{2^n},$$

where α is a primitive element of $\mathbb{F}_{2^n}$.

Note that $f_b(0) = 0$. Then the hyper-bentness of f_b can be characterized by the following proposition.

Proposition 3.1: Let $f_b \in \mathcal{D}_n$. Set the character sum of the form

$$\Lambda(f_b) := \sum_{u \in U} \chi(f_b(u)) \tag{2}$$

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

Proof: From Proposition 2.3, we have that f_b is a hyper-bent function if and only if its restriction to U has Hamming weight 2^{m-1}. From the definition of $\Lambda(f_b)$,

$$\begin{aligned}\Lambda(f_b) &= \sum_{x\in U}\chi(f_b(u)) \\ &= \#\{u\in U|f_b(u)=0\} - \#\{u|f_b(u)=1\} \\ &= \#U - 2\#\{u|f_b(u)=1\} \\ &= 2^m+1-2\#\{u|f_b(u)=1\}.\end{aligned}$$

Hence, the restriction of f_b to U has Hamming weight 2^{m-1} if and only if $\Lambda(f_b)=1$. As a result, f_b is a hyper-bent function if and only if $\Lambda(f_b)=1$.

As for the second part of the proposition, we compute

$$\begin{aligned}f_b(1) &= \sum_{r\in R}\mathrm{Tr}_1^n(a_r) + \mathrm{Tr}_1^4(b) \\ &= \sum_{r\in R}\mathrm{Tr}_1^m(a_r + a_r^{2^m}) + \mathrm{Tr}_1^4(b) \\ &= \mathrm{Tr}_1^4(b).\end{aligned}$$

Hence, $f_b(1)=0$ if and only if $\mathrm{Tr}_1^4(b)=0$. From Proposition 2.2, we have a hyper-bent function f_b lies in $\mathcal{PS}_{ap}$ if and only if $\mathrm{Tr}_1^4(b)=0$. ■

B. The characterization of Boolean functions in $\mathcal{D}_n$

Our goal is to present a characterization of hyper-bentness of Boolean functions f_b $(b\neq 0)$ in $\mathcal{D}_n$. In this section we analyze properties of $\Lambda(f_b)$ for the characterization. We now give some notations first.

Let α be a primitive element in $\mathbb{F}_{2^n}$. Then $\beta=\alpha^{\frac{2^n-1}{5}}$ is a primitive 5-th root of unity in U and U is a cyclic group generated by $\xi=\alpha^{2^m-1}$. Let V be a cyclic group generated by $\alpha^{5(2^m-1)}$. Then

$$U=\cup_{i=0}^4\xi^iV, \quad \mathbb{F}_{2^n}^* = \mathbb{F}_{2^m}^*\times U.$$

Next, we introduce the character sums

$$S_i=\sum_{v\in V}\chi(f_0(\xi^iv)).$$

Note that

$$S_0+S_1+S_2+S_3+S_4=\sum_{u\in U}\chi(f_0(u))=\Lambda(f_0). \qquad (3)$$

For any integer i, $S_i=S_{i \pmod 5}$. The following lemma gives the property of S_i.

Lemma 3.2: $S_1=S_4$, $S_2=S_3$.

Proof: Noth that $\mathrm{Tr}_1^n(x^{2^m})=\mathrm{Tr}_1^n(x)$, then

$$\begin{aligned}S_i &= \sum_{v\in V}\chi(\sum_{r\in R}\mathrm{Tr}_1^n(a_r(\xi^iv)^{r(2^m-1)})) \\ &= \sum_{v\in V}\chi(\sum_{r\in R}\mathrm{Tr}_1^n(a_r^{2^m}(\xi^{i2^m}v^{2^m})^{r(2^m-1)})).\end{aligned}$$

From $a_r\in\mathbb{F}_{2^m}$, $a_r^{2^m}=a_r$. Since $m\equiv 2 \pmod 4$ and $2^m\equiv -1 \pmod 5$, hence $i2^m\equiv -i \pmod 5$ and $\xi^{i2^m}v^{2^m}=\xi^{-i}(\xi^{i(2^m+1)}v^{2^m})$, where $\xi^{i(2^m+1)}\in V$. The map

$$v\longmapsto \xi^{i(2^m+1)}v^{2^m}$$

is a permutation of V. Consequently,

$$S_i=\sum_{v\in V}\chi(\sum_{r\in R}\mathrm{Tr}_1^n(a_r(\xi^{-i}v)^{r(2^m-1)}))=S_{-i}.$$

We just take $i=1,2$. Then this lemma follows. ■

From Lemma 3.2 and (3), the following corollary follows.

Corollary 3.3: $S_0+2(S_1+S_2)=\Lambda(f_0)$.

Generally, $\Lambda(f_b)$ is a linear combination of S_0, S_1 and S_2.

Proposition 3.4: $\Lambda(f_b)$ can be expressed by a linear combination of S_0, S_1 and S_2, that is,

$$\begin{aligned}\Lambda(f_b) = &\chi(\mathrm{Tr}_1^4(b))S_0 + (\chi(\mathrm{Tr}_1^4(b\beta^2))+\chi(\mathrm{Tr}_1^4(b\beta^3)))S_1 \\ &+ (\chi(\mathrm{Tr}_1^4(b\beta))+\chi(\mathrm{Tr}_1^4(b\beta^4)))S_2.\end{aligned}$$

Proof: From (2), we have

$$\begin{aligned}\Lambda(f_b) &= \sum_{u\in U}\chi(f_0(u)+\mathrm{Tr}_1^4(bu^{\frac{2^n-1}{5}})) \\ &= \sum_{u\in U}\chi(\mathrm{Tr}_1^4(bu^{\frac{2^n-1}{5}}))\chi(f_0(u)) \\ &= \sum_{i=0}^4\sum_{v\in V}\chi(\mathrm{Tr}_1^4(b(\xi^iv)^{\frac{2^n-1}{5}}))\chi(f_0(\xi^iv)) \quad \text{(From (3))} \\ &= \sum_{i=0}^4\sum_{v\in V}\chi(\mathrm{Tr}_1^4(b(\alpha^{i(2^m-1)})^{\frac{2^n-1}{5}}))\chi(f_0(\xi^iv)) \ (\xi=\alpha^{2^m-1}) \\ &= \sum_{i=0}^4\sum_{v\in V}\chi(\mathrm{Tr}_1^4(b\beta^{i(2^m-1)}))\chi(f_0(\xi^iv)) \quad (\beta=\alpha^{\frac{2^n-1}{5}})\end{aligned}$$

Since $2^m+1\equiv 0 \pmod 5$, hence $2^m-1\equiv 3 \pmod 5$. We have

$$\begin{aligned}\Lambda(f_b) &= \sum_{i=0}^4\sum_{v\in V}\chi(\mathrm{Tr}_1^4(b\beta^{3i}))\chi(f_0(\xi^iv)) \\ &= \sum_{i=0}^4\chi(\mathrm{Tr}_1^4(b\beta^{3i}))\sum_{v\in V}\chi(f_0(\xi^iv))\end{aligned}$$

From the definition of S_i, we obtain

$$\Lambda(f_b)=\sum_{i=0}^4\chi(\mathrm{Tr}_1^4(b\beta^{3i}))S_i.$$

From Lemma 3.2, this proposition follows. ■

Assume that $a_r\in\mathbb{F}_{2^{m_1}}$ for every $r\in R$, where $m_1=m/2$. Further, we have the following proposition.

Proposition 3.5: Assume $a_r\in\mathbb{F}_{2^{m_1}}$, where $r\in R$, $m_1=m/2$, then

$$S_1=S_2, S_0+4S_1=\Lambda(f_0).$$

Proof: From $a_r\in\mathbb{F}_{2^{m_1}}$, $\mathrm{Tr}_1^n(a_rx^{r(2^m-1)})=\mathrm{Tr}_1^n(a_rx^{2^{m_1}r(2^m-1)})$. Then we have

$$\begin{aligned}S_i &= \sum_{v\in V}\chi(\sum_{r\in R}\mathrm{Tr}_1^n(a_r(\xi^iv)^{r(2^m-1)})) \\ &= \sum_{v\in V}\chi(\sum_{r\in R}\mathrm{Tr}_1^n(a_r(\xi^{2^{m_1}i}v^{2^{m_1}})^{r(2^m-1)})).\end{aligned}$$

In particular, take $i=1$, then

$$S_1=\sum_{v\in V}\chi(\sum_{r\in R}\mathrm{Tr}_1^n(a_r(\xi^{2^{m_1}}v^{2^{m_1}})^{r(2^m-1)})).$$

Since $2^m + 1 \equiv 0 \pmod 5$, $(2^{m_1})^2 \equiv -1 \pmod 5$ and $2^{m_1} \equiv \pm 2 \pmod 5$.

When $2^{m_1} \equiv 2 \pmod 5$, then

$$S_1 = \sum_{v\in V} \chi(\sum_{r\in R} \mathrm{Tr}_1^n(a_r(\xi^2 \xi^{2^{m_1}-2} v^{2^{m_1}})^{r(2^m-1)})).$$

The map

$$v \longmapsto \xi^{2^{m_1}-2} v^{2^{m_1}}$$

is a permutation of V. Consequently,

$$S_1 = \sum_{v\in V} \chi(\sum_{r\in R} \mathrm{Tr}_1^n(a_r(\xi^2 v)^{r(2^m-1)})) = S_2.$$

When $2^{m_1} \equiv -2 \pmod 5$, we can similarly obtain $S_1 = S_3$.

As a result, $S_1 = S_2$. From Corollary 3.3, $S_0 + 4S_1 = \Lambda(f_0)$. ■

For $\Lambda(f_b)$, the proposition below gives some properties.

Proposition 3.6: $\Lambda(f_b)$ satisfies the following properties.

(1) $\Lambda(f_{b^4}) = \Lambda(f_b)$.

(2) If b a primitive element in $\mathbb{F}_{2^{16}}$ and $\mathrm{Tr}_1^4(b) = 0$, then $\Lambda(f_{b^2}) = \Lambda(f_b) = S_0$.

Proof: From $b \in \mathbb{F}_{16}$, $\mathrm{Tr}_1^4(b^4) = \mathrm{Tr}_1^4(b)$. Further,

$$\mathrm{Tr}_1^4(b(\beta^2+\beta^3)) = \mathrm{Tr}_1^4(b^4(\beta^8+\beta^{12})) = \mathrm{Tr}_1^4(b^4(\beta^2+\beta^3))$$

and

$$\mathrm{Tr}_1^4(b(\beta+\beta^4)) = \mathrm{Tr}_1^4(b^4(\beta^4+\beta^{16})) = \mathrm{Tr}_1^4(b^4(\beta+\beta^4)).$$

From the expressions of $\Lambda(f_{b^4})$ and $\Lambda(f_b)$ in Proposition 3.4, $\Lambda(f_{b^4}) = \Lambda(f_b)$.

(2) For an element b in $\mathbb{F}_{16}$ such that $\mathrm{Tr}_1^4(b) = 0$, it is easy to verify that b satisfies the following equation.

$$b^4 + b + 1 = 0.$$

Hence, we have

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

The minimal polynomial of β over $\mathbb{F}_2$ is $\beta^4+\beta^3+\beta^2+\beta+1 = 0$. Hence,

$$\mathrm{Tr}_1^2(\beta^2+\beta^3) = \beta^2+\beta^3+\beta^4+\beta^6 = 1.$$

Then we have $\mathrm{Tr}_1^4(b(\beta^2+\beta^3)) = 1$. Similarly, $\mathrm{Tr}_1^4(b(\beta+\beta^4)) = 1$.

Therefore, we obtain $\chi(\mathrm{Tr}_1^4(b\beta^2)) + \chi(\mathrm{Tr}_1^4(b\beta^3)) = 0$ and $\chi(\mathrm{Tr}_1^4(b\beta)) + \chi(\mathrm{Tr}_1^4(b\beta^4)) = 0$. From Proposition 3.4, $\Lambda(f_b) = S_0$.

If b is a primitive element in $\mathbb{F}_{2^{16}}$ such that $\mathrm{Tr}_1^4(b) = 0$, b^2 is also a primitive element in $\mathbb{F}_{2^{16}}$ such that $\mathrm{Tr}_1^4(b) = 0$. Naturally, we obtain $\Lambda(f_{b^2}) = \Lambda(f_b) = S_0$. ■

In fact, we have more explicit results on $\Lambda(f_b)$.

Proposition 3.7: Let $b \in \mathbb{F}_{16}^*$, then

(1) If $b = 1$, then $\Lambda(f_b) = S_0 - 2(S_1+S_2) = 2S_0 - \Lambda(f_0)$.

(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 such that $\mathrm{Tr}_1^4(b) = 0$, then $\Lambda(f_b) = S_0$.

(3) If $b = \beta$ or β^4, then $\Lambda(f_b) = -S_0 - 2S_1$.

(4) If $b = \beta^2$ or β^3, then $\Lambda(f_b) = -S_0 - 2S_2$.

(5) If $b = 1+\beta$ or $1+\beta^4$, then $\Lambda(f_b) = -S_0 + 2S_1$.

(6) If $b = 1+\beta^2$ or $1+\beta^3$, then $\Lambda(f_b) = -S_0 + 2S_2$.

(7) If $b = \beta+\beta^4$, then $\Lambda(f_b) = S_0 + 2S_1 - 2S_2$.

(8) If $b = \beta^2+\beta^3$, then $\Lambda(f_b) = S_0 - 2S_1 + 2S_2$.

Proof: From the expression of $\Lambda(f_b)$ in Proposition 3.4, these results follows. ■

Assume that $a_r \in \mathbb{F}_{2^{m_1}}$ for every $r \in R$. We have more simplified results than Proposition 3.7.

Proposition 3.8: Assume that $a_r \in \mathbb{F}_{2^{m_1}}$, where $r \in R$, then

(1) If $b = 1$, then $\Lambda(f_b) = 2S_0 - \Lambda(f_0)$.

(2) If $b \in \{\beta, \beta^2, \beta^3, \beta^4\}$, then $\Lambda(f_b) = -S_0 - 2S_1 = -\frac{S_0+\Lambda(f_0)}{2}$.

(3) If $b \in \{1+\beta, 1+\beta^2, 1+\beta^3, 1+\beta^4\}$, then $\Lambda(f_b) = -S_0 + 2S_1 = -\frac{3S_0-\Lambda(f_0)}{2}$.

(4) If $b \in \{\beta+\beta^2, \beta+\beta^3, \beta^2+\beta^4, \beta^3+\beta^4, \beta+\beta^4, \beta^2+\beta^3\}$, then $\Lambda(f_b) = S_0$.

Proof: Proposition 3.5 gives that $S_1 = S_2$. From Proposition 3.7, these results in Proposition 3.8 follow. ■

Corollary 3.9: Assume $a_r \in \mathbb{F}_{2^{m_1}}$, where $r \in R$, then $\Lambda(f_{b^2}) = \Lambda(f_b)$.

Proof: From Proposition 3.8, this corollary follows. ■

To characterize the hyper-bentness of f_b with character sums over $\mathbb{F}_{2^m}$, we now introduce some results on the character sums by Mesnager [25].

Lemma 3.10: Let $n = 2m$. f_0 is the function over $\mathbb{F}_{2^n}$ defined by (1) with $b = 0$. Let g_0 be a Boolean function defined on $\mathbb{F}_{2^m}$ by

$$g_0(x) = \sum_{r\in R} \mathrm{Tr}_1^m(a_r D_r(x)),$$

where $D_r(x)$ is the Dickson polynomial of degree r. U is the group of 2^m+1-th roots of unity in $\mathbb{F}_{2^n}^*$. Then for any positive integer p, we have

$$\sum_{u\in U} \chi(f_0(u^p)) = 1 + 2 \sum_{x\in\mathbb{F}_{2^m}^*, \mathrm{Tr}_1^m(x^{-1})=1} \chi(g_0(D_p(x))).$$

From Lemma 3.10, we have the following proposition.

Proposition 3.11: f_b is the function defined by (1). Let g_0 be a Boolean function defined on $\mathbb{F}_{2^m}$ by

$$g_0(x) = \sum_{r\in R} \mathrm{Tr}_1^m(a_r D_r(x)), \tag{4}$$

where $D_r(x)$ is the Dickson polynomial of degree r. Then

(1) If b is a primitive element in $\mathbb{F}_{16}$ such that $\mathrm{Tr}_1^4(b) = 0$, then

$$\Lambda(f_b) = \frac{1}{5}[1 + 2 \sum_{x\in\mathbb{F}_{2^m}^*, \mathrm{Tr}_1^m(x^{-1})=1} \chi(g_0(D_5(x)))].$$

(2) If $b = 1$, then

$$\begin{aligned}\Lambda(f_b) =& \frac{1}{5}[4 \sum_{x\in\mathbb{F}_{2^m}^*, \mathrm{Tr}_1^m(x^{-1})=1} \chi(g_0(D_5(x)))\\ &- 10 \sum_{x\in\mathbb{F}_{2^m}^*, \mathrm{Tr}_1^m(x^{-1})=1} \chi(g_0(x)) - 3].\end{aligned}$$

Proof: (1) From Proposition 3.7, when b is the primitive element such that $\mathrm{Tr}_1^4(b)=0$, we have

$$\Lambda(f_b)=S_0=\sum_{v\in V}\chi(f_0(v))=\frac{1}{5}\sum_{u\in U}\chi(f_0(u^5)).$$

From Lemma 3.10, we obtain

$$\Lambda(f_b)=\frac{1}{5}[1+2\sum_{x\in\mathbb{F}_{2^m}^*,\mathrm{Tr}_1^m(x^{-1})=1}\chi(g_0(D_5(x)))].$$

(2) From Proposition 3.7, when $b=1$, we have

$$\begin{aligned}\Lambda(f_b)=&2S_0-\Lambda(f_0)\\=&2\sum_{v\in V}\chi(f_0(v))-\sum_{u\in U}\chi(f_0(u))\\=&\frac{2}{5}\sum_{u\in U}\chi(f_0(u^5))-\sum_{u\in U}\chi(f_0(u)).\end{aligned}$$

From Lemma3.10, we obtain

$$\begin{aligned}\Lambda(f_b)\;=\;&\frac{2}{5}[1+2\sum_{x\in\mathbb{F}_{2^m}^*,\mathrm{Tr}_1^m(x^{-1})=1}\chi(g_0(D_5(x)))]\\&-[1+2\sum_{x\in\mathbb{F}_{2^m}^*,\mathrm{Tr}_1^m(x^{-1})=1}\chi(g_0(x))]\\=\;&\frac{1}{5}[4\sum_{x\in\mathbb{F}_{2^m}^*,\mathrm{Tr}_1^m(x^{-1})=1}\chi(g_0(D_5(x)))\\&-10\sum_{x\in\mathbb{F}_{2^m}^*,\mathrm{Tr}_1^m(x^{-1})=1}\chi(g_0(x))-3].\end{aligned}$$

■

To have another version of Proposition 3.11, we first introduce the following lemma.

Lemma 3.12: For any Boolean function $g(x)$ over $\mathbb{F}_{2^m}$,

$$\begin{aligned}\sum_{x\in\mathbb{F}_{2^m}^*,\mathrm{Tr}_1^m(x^{-1})=1}\chi(g(x))\;=\;&\frac{1}{2}[\sum_{x\in\mathbb{F}_{2^m}}\chi(g(x))-\\&\sum_{x\in\mathbb{F}_{2^m}}\chi(\mathrm{Tr}_1^m(x^{-1})+g(x))].\end{aligned}$$

Proof: For any $x,y\in\mathbb{F}_2$, $\chi(x+y)=\chi(x)+\chi(y)$. Then we have

$$\begin{aligned}&\sum_{x\in\mathbb{F}_{2^m}}\chi(g(x))-\sum_{x\in\mathbb{F}_{2^m}}\chi(\mathrm{Tr}_1^m(x^{-1})+g(x))\\=\;&\sum_{x\in\mathbb{F}_{2^m}}\chi(g(x))-\sum_{x\in\mathbb{F}_{2^m}}\chi(\mathrm{Tr}_1^m(x^{-1}))\chi(g(x))\\=\;&\sum_{x\in\mathbb{F}_{2^m}}\chi(g(x))-(\sum_{x\in\mathbb{F}_{2^m},\mathrm{Tr}_1^m(x^{-1})=0}\chi(g(x))\\&+\sum_{x\in\mathbb{F}_{2^m}^*,\mathrm{Tr}_1^m(x^{-1})=1}(-1)\chi(g(x)))\\=\;&2\sum_{x\in\mathbb{F}_{2^m}^*,\mathrm{Tr}_1^m(x^{-1})=1}\chi(g(x)).\end{aligned}$$

Hence, this lemma follows. ■

Proposition 3.13: f_b and g_0 are functions defined by (1) and (4) respectively. Then,

(1) If b is a primitive element in $\mathbb{F}_{16}$ such that $\mathrm{Tr}_1^4(b)=0$, then

$$\begin{aligned}\Lambda(f_b)\;=\;&\frac{1}{5}[1+\sum_{x\in\mathbb{F}_{2^m}}\chi(g_0(D_5(x)))\\&-\sum_{x\in\mathbb{F}_{2^m}}\chi(\mathrm{Tr}_1^m(x^{-1})+g_0(D_5(x)))].\end{aligned}$$

(2) If $b=1$, then

$$\begin{aligned}\Lambda(f_b)\;=\;&\frac{1}{5}[2\sum_{x\in\mathbb{F}_{2^m}}\chi(g_0(D_5(x)))-2\sum_{x\in\mathbb{F}_{2^m}}\chi(\mathrm{Tr}_1^m(x^{-1})\\&+g_0(D_5(x)))-5\sum_{x\in\mathbb{F}_{2^m}}\chi(g_0(x))\\&+5\sum_{x\in\mathbb{F}_{2^m}}\chi(\mathrm{Tr}_1^m(x^{-1})+g_0(x))-3].\end{aligned}$$

Proof: From Proposition 3.11 and 3.12, this proposition follows. ■

Note that for any Boolean function $g(x)$ over $\mathbb{F}_{2^m}$, $\sum_{x\in\mathbb{F}_{2^m}}\chi(g(x))=2^m-2\mathrm{wt}(g(x))$. Hence, we have the following corollary.

Corollary 3.14: f_b and g_0 are functions defined by (1) and (4) respectively. Then,

(1) If b is a primitive element in $\mathbb{F}_{16}$ such that $\mathrm{Tr}_1^4(b)=0$, then

$$\Lambda(f_0)=\frac{1}{5}[1+2\mathrm{wt}(\mathrm{Tr}_1^m(x^{-1})+g_0(D_5(x)))-2\mathrm{wt}(g_0(D_5(x)))].$$

(2) If $b=1$, then

$$\begin{aligned}\Lambda(f_0)=&\frac{1}{5}[4\mathrm{wt}(\mathrm{Tr}_1^m(x^{-1})+g_0(D_5(x)))-4\mathrm{wt}(g_0(D_5(x)))\\&+10\mathrm{wt}(g_0(x))-10\mathrm{wt}(\mathrm{Tr}_1^m(x^{-1})+g_0(x))-3].\end{aligned}$$

Proof: From Proposition 3.13, this corollary follows. ■

C. The hyper-bentness of Boolean functions in $\mathcal{D}_n$

In this subsection, we give a characterization of hyper-bentness of Boolean functions in $\mathfrak{D}_n$.

Theorem 3.15: Let $n=2m$ and $m\equiv 2\pmod 4$. Let b is a primitive element in $\mathbb{F}_{16}$ such that $\mathrm{Tr}_1^4(b)=0$, that is, $b^4+b+1=0$. f_b is the function defined on $\mathbb{F}_{2^n}$ by (1). Let g_0 be a Boolean function defined on $\mathbb{F}_{2^m}$ by $g_0(x)=\sum_{x\in R}\mathrm{Tr}_1^m(a_rD_r(x))$, where $D_r(x)$ is the Dickson polynomial of degree r. Then, the following assertions are equivalent.

(1) f_b is hyper-bent.

(2) $\sum_{x\in\mathbb{F}_{2^m}^*,\mathrm{Tr}_1^m(x^{-1})=1}\chi(g_0(D_5(x)))=2.$

(3) $\mathrm{wt}(\mathrm{Tr}_1^m(x^{-1})+g_0(D_5(x)))-\mathrm{wt}(g_0(D_5(x)))=2$, where $\mathrm{Tr}_1^m(x^{-1})+g_0(D_5(x))$ and $g_0(D_5(x))$ are functions over $\mathbb{F}_{2^m}$.

Proof: From Proposition 3.1, Proposition 3.11 and Corollary 3.14, this theorem follows. ■

When $b=1$, we have the following theorem.

Theorem 3.16: Let $n=2m$ and $m\equiv 2\pmod 4$. f_1 is the function defined on $\mathbb{F}_{2^n}$ by (1) with $b=1$. Let g_0 be a Boolean function defined on $\mathbb{F}_{2^m}$ by $g_0(x)=\sum_{x\in R}\mathrm{Tr}_1^m(a_rD_r(x))$, where $D_r(x)$ is the Dickson polynomial of degree r. Then, the following assertions are equivalent.

(1) f_1 is hyper-bent.

(2) $2 \sum_{x\in\mathbb{F}_{2^m}^*,\mathrm{Tr}_1^m(x^{-1})=1} \chi(g_0(D_5(x))) - 5 \sum_{x\in\mathbb{F}_{2^m}^*,\mathrm{Tr}_1^m(x^{-1})=1} \chi(g_0(x)) = 4$.

(3) $2\mathrm{wt}(\mathrm{Tr}_1^m(x^{-1}) + g_0(D_5(x))) - 2\mathrm{wt}(g_0(D_5(x))) + 5\mathrm{wt}(g_0(x)) - 5\mathrm{wt}(\mathrm{Tr}_1^m(x^{-1}) + g_0(x)) = 4$.

Proof: From Proposition 3.1, Proposition 3.11 and Corollary 3.14, this theorem follows. ■

The following proposition gives relations of the hyper-bentness of different functions in $\mathcal{D}_n$.

Proposition 3.17: Let $n = 2m$ and $m \equiv 2 \pmod 4$. Let d be a positive integer coprime to $\frac{2^m+1}{5}$. Let b be a primitive element in $\mathbb{F}_{16}$ such that $\mathrm{Tr}_1^4(b) = 0$, that is, $b^4+b+1 = 0$. f_b is the function defined by (1). Let h_b be a Boolean function defined by

$$\sum_{r\in R} \mathrm{Tr}_1^n(a_r x^{dr(2^m-1)}) + \mathrm{Tr}_1^4(b x^{\frac{2^n-1}{5}}),$$

where $a_r \in \mathbb{F}_{2^m}$. Then, h_b is hyper-bent if and only if f_b is hyper-bent.

Proof: From Proposition 3.1 and (2) in Proposition 3.7, h_b is hyper-bent if and only if $\sum_{v\in V} \chi(h_0(v)) = 1$ for the function $h_0 = \sum_{r\in R} \mathrm{Tr}_1^n(a_r x^{dr(2^m-1)})$. Since d and the cardinality of V $\frac{2^m+1}{5}$ are coprime, the map $v \mapsto v^d$ is a permutation of V. Therefore,

$$\begin{aligned}\sum_{v\in V} \chi(h_0(v)) &= \sum_{v\in V} \chi(\sum_{r\in R} \mathrm{Tr}_1^n(a_r v^{dr(2^m-1)}))\\ &= \sum_{v\in V} \chi(\sum_{r\in R} \mathrm{Tr}_1^n(a_r v^{r(2^n-1)}))\\ &= \sum_{v\in V} \chi(f_0(v)).\end{aligned}$$

Consequently, $\sum_{v\in V} \chi(h_0(v)) = 1$ if and only if $\sum_{v\in V} \chi(f_0(v)) = 1$. From Proposition 3.1 and (2) in Proposition 3.7, h_b is hyper-bent if and only if f_b is hyper-bent. ■

When $b = 1$, we have the following proposition.

Proposition 3.18: Let $n = 2m$ and $m \equiv 2 \pmod 4$. Let d be a positive integer coprime to $2^m + 1$. f_1 is the function defined by (1) with $b = 1$. Let h_1 be a Boolean function defined by

$$\sum_{r\in R} \mathrm{Tr}_1^n(a_r x^{dr(2^m-1)}) + \mathrm{Tr}_1^4(x^{\frac{2^n-1}{5}}),$$

where $a_r \in \mathbb{F}_{2^m}$. Then, h_1 is hyper-bent if and only if f_1 is hyper-bent.

Proof: Set $h_0 = \sum_{r\in R} \mathrm{Tr}_1^n(a_r x^{dr(2^n-1)})$. From Proposition 3.1 and (1) in Proposition 3.7, h_1 is hyper-bent if and only if $2\sum_{v\in V} \chi(h_0(v)) - \sum_{u\in U} \chi(h_0(u)) = 1$. From the process of proof in Proposition 3.17, $\sum_{v\in V} \chi(h_0(v)) = \sum_{v\in V} \chi(f_0(v))$. Since $(d, 2^m + 1) = 1$, we can have

$$\sum_{u\in U} \chi(h_0(u)) = \sum_{u\in U} \chi(f_0(u)).$$

Therefore, h_1 is hyper-bent if and only if f_1 is hyper-bent. ■

Further, we assume $5|d$ in Proposition 3.17. Then we can get the following proposition.

Proposition 3.19: Let $n = 2m$ and $m \equiv 2 \pmod 4$. Let d be a positive integer coprime to $\frac{2^m+1}{5}$ and $5|d$. Let b be a primitive element in $\mathbb{F}_{16}$ such that $\mathrm{Tr}_1^4(b) = 0$, that is, $b^4+b+1 = 0$. f_b is the function defined by (1). Let $h_{b'}$ be a Boolean function defined by

$$\sum_{r\in R} \mathrm{Tr}_1^n(a_r x^{dr(2^m-1)}) + \mathrm{Tr}_1^4(b' x^{\frac{2^n-1}{5}}), \qquad (5)$$

where $b' \in \mathbb{F}_{16}$. Then

(1) h_0 and $h_{\beta^i} (i = 0, 1, 2, 3, 4)$ are not bent functions, where β is the primitive 5-th root of unity in $\mathbb{F}_{16}$.

(2) $h_{b'}$ $(b' \in \mathbb{F}_{16}\backslash\{0, 1, \beta, \beta^2, \beta^3, \beta^4\})$ have the same hyper-bentness. Further, they are hyper-bent if and only if f_b is hyper-bent.

Proof: Set $h_0(x) = \sum_{r\in R} \mathrm{Tr}_1^n(a_r x^{d(2^m-1)})$. Let $S_i^{'} := \sum_{v\in V} \chi(h_0(\xi^i v))$. Then

$$S_i^{'} = \sum_{v\in V} \chi(\sum_{r\in R} \mathrm{Tr}_1^n(a_r(\xi^{id} v^d)^{r(2^m-1)})).$$

Since $5|d$ and $(d, \frac{2^m+1}{5}) = 1$, the map $v \mapsto \xi^{id} v^d$ is a permutation of V. Therefore,

$$S_i^{'} = \sum_{v\in V} \chi(\sum_{r\in R} \mathrm{Tr}_1^n(a_r v^{r(2^m-1)})) = \sum_{v\in V} \chi(f_0(v)) = S_0.$$

From (3), $\Lambda(h_0) = 5S_i^{'} = 5S_0$. From (1), (3) and (4) in Proposition 3.7, $\Lambda(h_{\beta^i}) = -3S_0$. Obviously, $5S_0$ and $-3S_0$ are not equal to 1. Since S_0 is odd. From Proposition 3.1, h_0 and $h_{\beta^i} (i = 0, 1, 2, 3, 4)$ are not bent functions.

From $(2), (5), (6), (7)$ and (8) in Proposition 3.7, when $b' \in \mathbb{F}_{16}\backslash\{0, 1, \beta, \beta^2, \beta^3, \beta^4\}$, $\Lambda(h_{b'}) = S_0^{'} = S_0$. Then from Proposition 3.1 and (2) in 3.7, (2) in this proposition follows. ■

Assume $a_r \in \mathbb{F}_{2^{m_1}}$ for any $r \in R$. We have the hyper-bentness of f_b $(b \in \{\beta, \beta^2, \beta^3, \beta^4\})$ in the following theorem.

Theorem 3.20: Let $n = 2m$, $m \equiv 2 \pmod 4$ and $m = 2m_1$. Let $b \in \{\beta, \beta^2, \beta^3, \beta^4\}$. f_b is the function defined on $\mathbb{F}_{2^n}$ by (1), where $a_r \in \mathbb{F}_{2^{m_1}}$ and $r \in R$. Let g_0 be a Boolean function over $\mathbb{F}_{2^m}$ defined by

$$g_0(x) = \sum_{r\in R} \mathrm{Tr}_1^m(a_r D_r(x)),$$

where $D_r(x)$ is the Dickson polynomial of degree r. Then the following assertions are equivalent.

(1) f_b is hyper-bent.

(2) $\sum_{x\in\mathbb{F}_{2^m}^*,\mathrm{Tr}_1^m(x^{-1})=1} \chi(g_0(D_5(x))) + 5 \sum_{x\in\mathbb{F}_{2^m}^*,\mathrm{Tr}_1^m(x^{-1})=1} \chi(g_0(x)) = -8$.

(3) $\mathrm{wt}(\mathrm{Tr}_1^m(x^{-1}) + g_0(D_5(x))) - \mathrm{wt}(g_0(D_5(x))) + 5\mathrm{wt}(\mathrm{Tr}_1^m(x^{-1}) + g_0(x)) - 5\mathrm{wt}(g_0(x)) = -8$.

Proof: From (2) in Proposition 3.8, $\Lambda(f_b) = -\frac{1}{2}(S_0 + \Lambda(f_0)) = -\frac{1}{2}(2S_0 - \Lambda(f_0)) - \frac{3}{2}S_0$. From (1) in Proposition

3.7 and (2) Proposition 3.11,

$$\begin{aligned}2S_0 - \Lambda(f_0) =& \frac{1}{5}[4 \sum_{x\in\mathbb{F}_{2^m}^*, \mathrm{Tr}_1^m(x^{-1})=1} \chi(g_0(D_5(x))) \\ & - 10 \sum_{x\in\mathbb{F}_{2^m}^*, \mathrm{Tr}_1^m(x^{-1})=1} \chi(g_0(x)) - 3].\end{aligned} \tag{6}$$

From (2) in Proposition 3.7 and (1) in 3.11,

$$S_0 = \frac{1}{5}[1 + 2 \sum_{x\in\mathbb{F}_{2^m}^*, \mathrm{Tr}_1^m(x^{-1})=1} \chi(g_0(D_5(x)))]. \tag{7}$$

Hence,

$$\begin{aligned}\Lambda(f_b) =& -\frac{1}{5}[\sum_{x\in\mathbb{F}_{2^m}^*, \mathrm{Tr}_1^m(x^{-1})=1} \chi(g_0(D_5(x))) \\ & + 5 \sum_{x\in\mathbb{F}_{2^m}^*, \mathrm{Tr}_1^m(x^{-1})=1} \chi(g_0(x)) + 3].\end{aligned}$$

Then from Proposition 3.1, f_b is hyper-bent if and only if (2) in this theorem holds.

Further, from Proposition 3.11 and Corollary 3.14,

$$\begin{aligned}\sum_{x\in\mathbb{F}_{2^m}^*, \mathrm{Tr}_1^m(x^{-1})=1} \chi(g_0(D_5(x))) =& \mathrm{wt}(\mathrm{Tr}_1^m(x^{-1}) + g_0(D_5(x))) \\ & - \mathrm{wt}(g_0(D_5(x)))\end{aligned} \tag{8}$$

and

$$\begin{aligned}\sum_{x\in\mathbb{F}_{2^m}^*, \mathrm{Tr}_1^m(x^{-1})=1} \chi(g_0(x)) =& \mathrm{wt}(\mathrm{Tr}_1^m(x^{-1}) + g_0(x)) \\ & - \mathrm{wt}(g_0(x))\end{aligned} \tag{9}$$

Consequently, assertions (2) and (3) in this theorem are equivalent. Hence, this theorem follows. ■

If $b \in \{1+\beta, 1+\beta^2, 1+\beta^3, 1+\beta^4\}$, we have the following theorem corresponding to Theorem 3.20.

Theorem 3.21: Let $n = 2m$, $m \equiv 2 \pmod 4$ and $m = 2m_1$. Let $b \in \{1+\beta, 1+\beta^2, 1+\beta^3, 1+\beta^4\}$, that is, b is the primitive element in $\mathbb{F}_{16}$ such that $\mathrm{Tr}_1^4(b) = 1$. f_b is the function over $\mathbb{F}_{2^n}$ by (1), where $a_r \in \mathbb{F}_{2^{m_1}}$ and $r \in R$. Let g_0 be a Boolean function defined on $\mathbb{F}_{2^m}$ by

$$g_0(x) = \sum_{r\in R} \mathrm{Tr}_1^m(a_r D_r(x)),$$

where $D_r(x)$ is the Dickson polynomial of degree r. Then the following assertions are equivalent.

(1) f_b is hyper-bent.

(2) $3 \sum_{x\in\mathbb{F}_{2^m}^*, \mathrm{Tr}_1^m(x^{-1})=1} \chi(g_0(D_5(x))) - 5 \sum_{x\in\mathbb{F}_{2^m}^*, \mathrm{Tr}_1^m(x^{-1})=1} \chi(g_0(x)) = -4$.

(3) $3\mathrm{wt}(\mathrm{Tr}_1^m(x^{-1}) + g_0(D_5(x))) - 3\mathrm{wt}(g_0(D_5(x))) - 5\mathrm{wt}(\mathrm{Tr}_1^m(x^{-1}) + g_0(x)) + 5\mathrm{wt}(g_0(x)) = -4$.

Proof: From (3) in Proposition 3.8,

$$\Lambda(f_b) = -\frac{1}{2}(3S_0 - \Lambda(f_0)) = -\frac{1}{2}(2S_0 - \Lambda(f_0)) - \frac{1}{2}S_0.$$

Then from (6) and (7),

$$\begin{aligned}\Lambda(f_b) =& -\frac{1}{5}[3 \sum_{x\in\mathbb{F}_{2^m}^*, \mathrm{Tr}_1^m(x^{-1})=1} \chi(g_0(D_5(x))) \\ & - 5 \sum_{x\in\mathbb{F}_{2^m}^*, \mathrm{Tr}_1^m(x^{-1})=1} \chi(g_0(x)) - 1].\end{aligned}$$

From Proposition 3.1, f_b is hyper-bent if and only if (2) in this theorem holds. Further, from (8) and (9), f_b is hyper-bent if and only if (3) in this theorem holds. Hence, this theorem follows. ■

If $b \in \{\beta+\beta^2, \beta+\beta^3, \beta^2+\beta^4, \beta^3+\beta^4, \beta+\beta^4, \beta^2+\beta^3\}$, we have the following theorem corresponding to Theorem 3.20.

Theorem 3.22: Let $n = 2m$, $m \equiv 2 \pmod 4$ and $m = 2m_1$. Let $b \in \{\beta+\beta^2, \beta+\beta^3, \beta^2+\beta^4, \beta^3+\beta^4, \beta+\beta^4, \beta^2+\beta^3\}$, that is, b is the primitive element such that $\mathrm{Tr}_1^m(b) = 1$ or a primitive 3-th root of unity. f_b is the function over $\mathbb{F}_{2^n}$ by (1), where $a_r \in \mathbb{F}_{2^{m_1}}$ and $r \in R$. Let g_0 be a Boolean function defined on $\mathbb{F}_{2^m}$ by

$$g_0(x) = \sum_{r\in R} \mathrm{Tr}_1^m(a_r D_r(x)),$$

where $D_r(x)$ is the Dickson polynomial of degree r. Then f_b is hyper-bent if and only if (2) and (3) in Theorem 3.15 hold.

Proof: From (4) in Proposition 3.8, $\Lambda(f_b) = S_0$. Hence, from Theorem 3.15, this theorem follows. ■

IV. Examples of hyper-bent functions in $\mathcal{D}_n$

In this section, we list some instances of hyper-bent functions in $\mathfrak{D}_n$.

Let $m_1 = 3$, then $m = 6$ and $n = 12$. $\mathbb{F}_6 = \mathbb{F}_2[x]/(x^6 + x^4 + x^3 + x + 1)$, $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^4 + x + 1)$, Let α_6 be a root of $x^6 + x^4 + x^3 + x + 1 = 0$. Let α_4 be a root of $x^4 + x + 1 = 0$.

Take $R = \{1\}$, $a_1 = \alpha_6^{23}$ and $b = \alpha_4$ in (1). From Theorem 3.15, we have a hyper-bent function of the form

$$\mathrm{Tr}_1^{12}(\alpha_6^{23} x^{2^m-1}) + \mathrm{Tr}_1^4(\alpha_4 x^{\frac{2^n-1}{5}}).$$

Take $R = \{1, 3\}$, $a_1 = 1$, $a_3 = \alpha_6^{17}$ and $b = \alpha_4$ in (1). From Theorem 3.15, we have a hyper-bent function of the form

$$\mathrm{Tr}_1^{12}(x^{2^m-1}) + \mathrm{Tr}_1^{12}(\alpha_6^{17} x^{3(2^m-1)}) + \mathrm{Tr}_1^4(x^{\frac{2^n-1}{5}}).$$

Take $R = \{1\}$, $a_1 = 1$ and $b = \beta$ in (1). From Theorem 3.20, we have a hyper-bent function of the form

$$\mathrm{Tr}_1^{12}(x^{2^m-1}) + \mathrm{Tr}_1^4(\beta x^{\frac{2^n-1}{5}}),$$

where β is a primitive 5-th root of unity in $\mathbb{F}_{16}$.

Finally, take $d = 5$, $R = \{1\}$ and $a_1 = \alpha_6^{11}$ in (5). From Proposition 3.19, we have a hyper-bent function of the form

$$\mathrm{Tr}_1^{12}(\alpha_6^{11} x^{5(2^n-1)}) + \mathrm{Tr}_1^4(b x^{\frac{2^n-1}{5}}),$$

where $b \in \mathbb{F}_{16} \backslash \{0, 1, \beta, \beta^2, \beta^3, \beta^4\}$.

V. Conclusion

In this paper, we consider a new class of Boolean functions with multiple trace terms $\mathcal{D}_n$. With some restrictions, we present the characterization of hyper-bentness of functions in $\mathcal{D}_n$. We give a link between hyper-bent functions of $\mathcal{D}_n$ and some character sums involving Dickson polynomials. Further, we relate hyper-bentness of functions in $\mathcal{D}_n$ to some equations on weights of Boolean functions involving Dickson polynomials. This characterization of hyper-bentness of functions in $\mathcal{D}_n$ provides more hyper-bent functions and enriches the theory of hyper-bent functions. Naturally, further study on the characterization is to investigate the hyper-bentness in other cases, such as (1) $a_r \in \mathbb{F}_{2^m}$ and $b \in \mathbb{F}_{16}^* \setminus \{b|(b+1)(b^4+b+1) = 0\}$; (2)for some of r, $a_r \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$.

Acknowledgment

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. Chungming Tang, Yanfeng Qi and Maozhi Xu acknowledge support from the Natural Science Foundation of China (Grant No.10990011 & No.60763009).

References

[1] 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.

[2] C. Carlet, 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.

[3] C. Carlet and P. Gaborit, Hyperbent functions and cyclic codes, J Combin. Theory, ser. A, vol. 113, no. 3, pp. 466-482, 2006.

[4] C. Carlet, T. Helleseth, A. Kholosha, and S. Mesnager, On the Dual of the Niho Bent Functions with 2^r Exponents, Information Theory Proceedings (ISIT), 2011 IEEE International Symposium on , vol., no., 2011 pp.703-707.

[5] C. Carlet and S. Mesnager, On Dillon's Class H of Bent Functions Niho Bent Functions and o-Polynomials, Journal of Combinatorial Theory, Series A Volume 118, Issue 8, November 2011, Pages 2392-2410.

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

[7] P. Charpin and G. Kyureghyan, Cubic monomial bent functions: A subclass of $\mathcal{M}$, SIAM J. Discr. Math., vol. 22, no. 2, pp. 650-665 2008.

[8] P. Charpin, E. Pasalic, and C. Tavernier, On bent and semi-ben quadratic Boolean functions, IEEE Trans. Inf. Theory, vol. 51, no 12, pp. 4286-4298, 2005.

[9] J. Dillon, Elementary Hadamard Difference Sets, Ph.D., Univ.Maryland, 1974.

[10] J. F. Dillon and H. Dobbertin, New cyclic difference sets with Singer parameters, Finite Fields Applicat., vol. 10, no. 3, pp. 342-389, 2004.

[11] H. Dobbertin and G. Leander, T. Helleseth, Ed. et al., A survey of some recent results on bent functions, in SETA 2004, 2005, vol. 3486, LNCS, pp. 1-29.

[12] H. Dobbertin, G. Leander, A. Canteaut, C. Carlet, P. Felke, and P. Gaborit, Construction of bent functions via Niho power functions, J. Combin. Theory, ser. A, vol. 113, pp. 779-798, 2006.

[13] R. Gold, Maximal recursive sequences with 3-valued recursive crosscorrelation functions, IEEE Trans. Inf. Theory, vol. 14, no. 1, pp. 154-156, 1968.

[14] G. Gong and S. W. Golomb, Transform domain analysis of DES, IEEE Trans. Inf. Theory, vol. 45, no. 6, pp. 2065-2073, 1999.

[15] H.Hu and D. Feng, On quadratic bent functions in polynomial forms, IEEE Trans. Inf. Theory, vol. 53, no. 7, pp. 2610-2615, 2007.

[16] T. Kasami, Weight enumerators for several classes of subcodes of the 2nd-order ReedCMuller codes, Inf. Contr., vol. 18, pp. 369-394, 1971.

[17] S. H. Kim and J. S. No, New families of binary sequences with low correlation, IEEE Trans. Inf.. Theory, vol. 49, no. 11, pp. 3059-3065, 2003.

[18] G. Leander, Monomial bent functions, IEEE Trans. Inf. Theory, vol. 2, no. 52, pp. 738-743, 2006.

[19] G. Leander and A.Kholosha, Bent functions with 2^r Niho exponents, IEEE Trans. Inf. Theory, vol. 52, no. 12, pp. 5529-5532, 2006.

[20] W. Ma, M. Lee, and F. Zhang, A new class of bent functions, IEICE Trans. Fund., vol. E88-A, no. 7, pp. 2039-2040, 2005.

[21] R. L. McFarland, A family of noncyclic difference sets, J. Combin. Theory, ser. A, no. 15, pp. 1-10, 1973.

[22] 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.

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

[24] S. Mesnager, 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

[25] S.Mesnager, M. A. Hasan and T. Helleseth, Eds., Hyper-bent boolean functions with multiple trace terms, in Proc. Int. Workshop on the Arithmetic of Finite Fields. WAIFI 2010, Heidelberg, 2010, vol. LNCS 6087, pp. 97-113.

[26] S. Mesnager, M. G. Parker, Ed., A new family of hyper-bent boolean functions in polynomial form, in Proc. Twelfth Int. Conf. Cryptography and Coding, Cirencester, United Kingdom. IMACC 2009, Heidelberg, Germany, 2009, vol. 5921, LNCS, pp. 402-417.

[27] G. L. Mullen, R. Lidl, and G. Turnwald, Dickson Polynomials. Reading, MA: Addison-Wesley, 1993, vol. 65, Pitman Monographs in Pure and Applied Mathematics.

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

[29] A. M. Youssef and G. Gong, Hyper-bent functions, in Advances in Crypology C Eurocrypt01, 2001, LNCS, pp. 406-419.

[30] N. Y. Yu and G. Gong, Construction of quadratic bent functions in polynomial forms, IEEE Trans. Inf. Theory, vol. 7, no. 52, pp. 3291-3299, 2006.