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

Constructing hyper-bent functions from Boolean functions with the Walsh spectrum taking the same value twice

Chunming Tang · Yanfeng Qi

Received: date / Accepted: date

Abstract Hyper-bent functions as a subclass of bent functions attract much interest and it is elusive to completely characterize hyper-bent functions. Most of known hyper-bent functions are Boolean functions with Dillon exponents and they are often characterized by special values of Kloosterman sums. In this paper, we present a method for characterizing hyper-bent functions with Dillon exponents. A class of hyper-bent functions with Dillon exponents over $\mathbb{F}_{2^{2m}}$ can be characterized by a Boolean function over $\mathbb{F}_{2^m}$, whose Walsh spectrum takes the same value twice. Further, we show several classes of hyper-bent functions with Dillon exponents characterized by Kloosterman sum identities and the Walsh spectra of some common Boolean functions.

Keywords Bent function · hyper-bent function · Dillon exponents · Walsh-Hadamard transform · 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 [26] as interesting combinatorial objects have been extensively studied for their applications not only in cryptography, but also in coding theory [4,22] and combinatorial

Chunming Tang
School of Mathematics and Information, China West Normal University, Sichuan Nanchong, 637002, China

Yanfeng Qi
School of Science, Hangzhou Dianzi University, Hangzhou, Zhejiang, 310018, China; Part of this work was done when he was a postdoctor in Peking University and Aisino Corporation Inc.
E-mail: qiyanfeng07@163.com

design. 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 good structures and properties of the finite field $\mathbb{F}_{2^n}$, bent functions can be well studied. Much research on bent functions on $\mathbb{F}_{2^n}$ can be found in [2,3,5,6,8–11,14,16,17,20–24,31]. Youssef and Gong [30] 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 extended 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, such as hyper-bent functions with Dillon exponents and hyper-bent functions with Niho exponents.

Charpin and Gong [5] studied the hyper-bent functions with multiple trace terms of the form

$$f(x)=\sum_{r\in R}\mathrm{Tr}_1^n(a_rx^{r(2^m-1)}),$$

where $n=2m$, R is a set of representations of the cyclotomic cosets modulo 2^m+1 of full size n and $a_r\in\mathbb{F}_{2^m}$. The characterization of these hyper-bent functions was presented by the character sums on $\mathbb{F}_{2^m}$. Lisonek [18] presented another characterization of Charpin and Gong's hyper-bent functions in terms of the number of rational points on certain hyperelliptic curves. And they proved that there exists an algorithm for determining such hyper-bent functions with time complexity and space complexity $O(r_{max}^am^b)$, where r_{max} is the biggest element in R, and a,b are some positive constants irrelevant to r_{max} and m. In particular, when $R=r$ and $(r,2^m+1)=1$, these hyper-bent function are monomial functions via Dillon-like exponents. Dillon [8] proved that $Tr_1^n(ax^{r(2^m-1)})$ $(a\in\mathbb{F}_{2^m})$ is hyper-bent if and only if $K_m(a)=0$.

Mesnager [22] generalized Charpin and Gong's hyper-bent functions and presented the characterization of hyper-bent functions of the form

$$f(x)=\sum_{r\in R}\mathrm{Tr}_1^n(a_rx^{r(2^m-1)})+Tr_1^2(bx^{\frac{2^n-1}{3}}),$$

where $b\in\mathbb{F}_4$ and $a_r\in\mathbb{F}_{2^m}$. In the case $\#R=1$, explicit characterization in [21] by Mesnager is presented. With the similar approach, Wang et al. [29] characterized the hyper-bentness of a class of Boolean functions of the form

$$f(x)=\sum_{r\in R}\mathrm{Tr}_1^n(a_rx^{r(2^m-1)})+Tr_1^4(bx^{\frac{2^n-1}{5}}),$$

where $b\in\mathbb{F}_{16}$ and $a_r\in\mathbb{F}_{2^m}$. In [27,28], explicit characterization for the case $\#R=1$ is given. When r_{max} is small, Flori and Mesnager[12,13] used the number of rational points on hyper-elliptic curves to determine those classes of Wang et al.'s hyper-bent functions. Mesnager and Flori [25] generalized the above results and characterized the hyper-bentness of Boolean functions of the form

$$f(x)=\sum_{r\in R}\mathrm{Tr}_1^n(a_r x^{r(2^m-1)})+Tr_1^t(bx^{s(2^m-1)}),$$

where $s|(2^m+1)$, $t=o(s(2^m-1))$, i.e., t is the size of the cyclotomic coset of s modulo 2^m+1, $a_r\in\mathbb{F}_{2^m}$, and $b\in\mathbb{F}_{2^t}$.

Li et al. [19] considered a class of Boolean functions of the form

$$f(x)=\sum_{i=0}^{q-1}Tr_1^n(ax^{(ri+s)(q-1)})+Tr_1^2(bx^{\frac{q^2-1}{3}}),$$

where $n=2m$, $q=2^m$, m is odd, $gcd(r,q+1)=1$, $a\in\mathbb{F}_{q^2}$, and $b\in\mathbb{F}_4$. The hyper-bentness of these functions is characterized by Kloosterman sums.

This paper characterizes hyper-bent functions with Dillon exponents $c(2^m-1)$ with a new method. A hyper-bent function with Dillon exponents over $\mathbb{F}_{2^{2m}}$ can be characterized by two elements in $\mathbb{F}_{2^m}$, which take the same Walsh-Hadamard coefficient of a Boolean function over $\mathbb{F}_{2^m}$. Further, Kloosterman sum identities and the Walsh spectra of some common Boolean functions are used to characterize several classes of hyper-bent functions.

This paper is organized as follows: Section 2 introduces some notations, hyper-bent functions, and results of exponential sums. Section 3 presents our main method for characterizing hyper-bent functions over $\mathbb{F}_{2^{2m}}$ from Boolean functions over $\mathbb{F}_{2^m}$. Then we give several classes of hyper-bent functions from some common Boolean functions over over $\mathbb{F}_{2^m}$. Kloosterman sum identities and the Walsh spectra of some common Boolean functions are of use in the characterization of these hyper-bent functions. Section 4 makes a conclusion for this paper.

2 Preliminaries

2.1 Boolean functions and bent functions

Let n be a positive integer, $n=2m$, and $q=2^m$. Let $\mathbb{F}_{2^n}$ be a finite field with 2^n elements and $\mathbb{F}_{2^n}^*$ the multiplicative group of $\mathbb{F}_{2^n}$. Let α be a primitive element of $\mathbb{F}_{2^n}$. Let U be a subgroup of $\mathbb{F}_{2^n}^*$ generated by $\xi=\alpha^{q-1}$. Then U is a cyclic group of $q+1$ elements.

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 $\mathrm{Tr}_k^n(x)$, is a map defined as $\mathrm{Tr}_k^n(x):=x+x^{2^k}+x^{2^{2k}}+\cdots+x^{2^{n-k}}$.

A Boolean function f over $\mathbb{F}_{2^n}$ is an $\mathbb{F}_2$-valued function. The "sign" function of f is defined by $\chi(f):=(-1)^f$. The Walsh-Hadamard transform of f is the discrete Fourier transform of χ_f, whose value at $\omega\in\mathbb{F}_{2^n}$ 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 as an important subclass of bent functions are defined 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.

Many hyper-bent Boolean functions are with Dillon exponents. A Boolean function is with Dillon exponents if the exponents of the trace representation of this function have the form $c(q-1)$, where c is a positive integer. Such functions satisfies that for any $y \in \mathbb{F}_q^*$ and $x \in \mathbb{F}_{2^n}$, $f(yx) = f(x)$. The characterization of hyper-bent functions with Dillon exponents is given in the following proposition [19,21].

Proposition 1 *Let $f(x)$ be a Boolean function with Dillon exponents defined over $\mathbb{F}_{2^{2m}}$. Then $f(x)$ is hyper-bent if and only if $\Lambda_f = \sum_{u \in U} (-1)^{f(u)} = (-1)^{f(0)}$.*

2.2 Exponential sums

In this subsection, we introduce some results for special exponential sums.

Definition 3 The binary Kloosterman sums associated with a on finite field $\mathbb{F}_{2^m}$ are

$$K_m(a) = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{Tr_1^m(\frac{1}{x} + ax)}, a \in \mathbb{F}_{2^m}.$$

Note that $\frac{1}{0} = 0$ for $x = 0$.

Definition 4 The cubic sums on $\mathbb{F}_{2^m}$ are

$$C_m(a, b) = \sum_{x \in \mathbb{F}_{2^m}} (-1)^{Tr_1^m(ax^3 + bx)}, a \in \mathbb{F}_{2^m}^*, b \in \mathbb{F}_{2^m}.$$

Carlitz computed the exact values of the cubic sums in the following two propositions [1].

Proposition 2 *Let m be an odd integer. Then*

(1) $C_m(1, 1) = (-1)^{(m^2-1)/8} 2^{(m+1)/2}$.

(2) If $Tr_1^m(c) = 0$, then $C_m(1, c) = 0$.

(3) If $Tr_1^m(c) = 1$ and $c \neq 1$, then $C_m(1, c) = (-1)^{Tr_1^m(\gamma^3 + \gamma)} (\frac{2}{m}) 2^{(m+1)/2}$, where $c = \gamma^4 + \gamma + 1$,$\gamma \in \mathbb{F}_{2^m}$, and $(\frac{2}{m})$ is the Jacobi symbol.

Proposition 3 *Let m be an even integer. Then,*

(1) $C_m(1, 0) = (-1)^{\frac{m}{2}+1} 2^{\frac{m}{2}+1}$;

(2) $C_m(1, \lambda) = \begin{cases} (-1)^{Tr_1^m(\gamma^3)} (-1)^{\frac{m}{2}+1} 2^{\frac{m}{2}+1}, & Tr_2^m(\lambda) = 0 \\ 0, & Tr_2^m(\lambda) \neq 0 \end{cases}$, where γ is a solution of $\gamma^4 + \gamma = \lambda^2$.

3 A class of hyper-bent functions with Dillon exponents

Let n be a positive integer, $n = 2m$, and $q = 2^m$. In this section, we present our new method for characterizing hyper-bent functions over $\mathbb{F}_{2^n}$ by a Boolean function over $\mathbb{F}_q$, whose Walsh spectrum takes the same value twice.

Note that $\frac{1}{0} = 0$. Let $g(y)$ be a Boolean function defined over $\mathbb{F}_q$. Then we define a Boolean function over $\mathbb{F}_{q^2}$ of the form

$$f(x) = g(\frac{1}{\lambda_1 + \lambda_2} \cdot \frac{1}{x^{q-1} + x^{-(q-1)}}) + Tr_1^m(\frac{\lambda_i}{\lambda_1 + \lambda_2} \cdot \frac{1}{x^{q-1} + x^{-(q-1)}}) \quad (1)$$

where $\lambda_i \in \mathbb{F}_q$ ($i = 1$ or 2) and $\lambda_1 \neq \lambda_2$. Note that $x^{q-1} + x^{-(q-1)} \in \mathbb{F}_q$. Then $f(x)$ is well defined. The hyper-bentness of $f(x)$ is characterized by the same Walsh-Hadamard coefficient of $g(y)$ in the following theorem.

Theorem 1 *Let $f(x)$ be defined in (1). Let $g(0) = 0$. Then $f(x)$ is hyper-bent if and only if $\widehat{\chi}_g(\lambda_1) = \widehat{\chi}_g(\lambda_2)$, where $\widehat{\chi}_g(\lambda)$ is the Walsh-Hadamard transform of $g(y)$.*

Proof Note that $f(x)$ is a function with Dillon exponents $c(q-1)$. When $y \neq 0$ and $Tr_1^n(y) = 1$, the equation $\frac{1}{u+u^{-1}} = y$ has two solutions. Then $u \mapsto \frac{1}{u+u^{-1}}$ is a 2-to-1 map from $U \setminus \{1\}$ to $\{y \in \mathbb{F}_q : Tr_1^n(y) = 1\}$ [21]. The map $u \mapsto u^{q-1}$ is a permutation of U. Then

$$\begin{aligned} \Lambda_f &= \sum_{u \in U} (-1)^{g(\frac{1}{\lambda_1+\lambda_2} \cdot \frac{1}{u+u^{-1}}) + Tr_1^m(\frac{\lambda_i}{\lambda_1+\lambda_2} \cdot \frac{1}{u+u^{-1}})} \\ &= (-1)^{g(0)} + 2 \sum_{y \in \mathbb{F}_q, Tr_1^m(y)=1} (-1)^{g(\frac{y}{\lambda_1+\lambda_2}) + Tr_1^m(\frac{\lambda_i}{\lambda_1+\lambda_2} y)}. \end{aligned}$$

Further, we have

$$\begin{aligned} \Lambda_f =& (-1)^{g(0)} + \sum_{y \in \mathbb{F}_q} (-1)^{g(\frac{y}{\lambda_1+\lambda_2}) + Tr_1^m(\frac{\lambda_i}{\lambda_1+\lambda_2} y)} - \sum_{y \in \mathbb{F}_q} (-1)^{g(\frac{y}{\lambda_1+\lambda_2}) + Tr_1^m(\frac{\lambda_i}{\lambda_1+\lambda_2} y) + Tr_1^m(y)} \\ =& (-1)^{g(0)} + \sum_{y \in \mathbb{F}_q} (-1)^{g(\frac{y}{\lambda_1+\lambda_2}) + Tr_1^m(\frac{\lambda_i}{\lambda_1+\lambda_2} y)} - \sum_{y \in \mathbb{F}_q} (-1)^{g(\frac{y}{\lambda_1+\lambda_2}) + Tr_1^m(\frac{\lambda_{3-i}}{\lambda_1+\lambda_2} y)}. \end{aligned}$$

Note that $y \mapsto \frac{y}{\lambda_1+\lambda_2}$ is a permutation of $\mathbb{F}_q$ and $g(0) = 0$. Then $\Lambda_f = 1 + \sum_{y \in \mathbb{F}_q} (-1)^{g(y) + Tr_1^m(\lambda_i y)} - \sum_{y \in \mathbb{F}_q} (-1)^{g(y) + Tr_1^m(\lambda_{3-i} y)}$. From Proposition 1, $f(x)$ is hyper-bent if and only if $\sum_{y \in \mathbb{F}_q} (-1)^{g(y) + Tr_1^m(\lambda_i y)} = \sum_{y \in \mathbb{F}_q} (-1)^{g(y) + Tr_1^m(\lambda_{3-i} y)}$, i.e, $\widehat{\chi}_g(\lambda_1) = \widehat{\chi}_g(\lambda_2)$. Hence, this theorem follows.

Theorem 1 offers a new method to present hyper-bent funtions of the form (1). On the Walsh spectra of $g(y)$, there are many exisiting results, which can be used to find two different elements λ_1 and λ_2 satisfying $\widehat{\chi}_g(\lambda_1) = \widehat{\chi}_g(\lambda_2)$. From the proper choice of a Boolean function $g(y)$, λ_1, and λ_2, a lot of hyper-bent functions $f(x)$ can be given.

For further consideration, we give the following lemma.

Lemma 1 *Let $x \in \mathbb{F}_{q^2}$, $u = x^{q-1}$, $\lambda \in \mathbb{F}_q$, and $m \geq t \geq 1$. Then*

(1) $\frac{1}{u+u^{-1}} = \sum_{i=1}^{2^{m-2}} (u^{2(2i-1)} + u^{-2(2i-1)})$;
(2) $Tr_1^m(\lambda \frac{1}{x^{q-1}+x^{-(q-1)}}) = \sum_{i=1}^{2^{m-2}} Tr_1^n(\lambda^{2^{m-1}} x^{(2i-1)(q-1)})$;
(3) $(\frac{1}{u+u^{-1}})^{2^{t-1}-1} = \sum_{i=1}^{2^{m-t}} (u^{2^{t-1}(2i-1)} + u^{-2^{t-1}(2i-1)})$;
(4) $Tr_1^m(\lambda(\frac{1}{x^{q-1}+x^{-(q-1)}})^{2^{t-1}-1}) = \sum_{i=1}^{2^{m-t}} Tr_1^n(\lambda^{2^{m-t+1}} x^{(2i-1)(q-1)})$;
(5) $(u+u^{-1})^{2^t-1} = \sum_{i=1}^{2^{t-1}} (u^{2i-1} + u^{-(2i-1)})$;
(6) $Tr_1^m(\lambda(x^{q-1} + x^{-(q-1)})^{2^t-1}) = \sum_{i=1}^{2^{t-1}} Tr_1^n(\lambda x^{(2i-1)(q-1)})$;
(7) $(u+u^{-1})^{2^t+1} = u^{2^t-1} + u^{-(2^t-1)} + u^{2^t+1} + u^{-(2^t+1)}$;
(8) $Tr_1^m(\lambda(x^{q-1} + x^{-(q-1)})^{2^t+1}) = Tr_1^n(\lambda(x^{(2^t-1)(q-1)} + x^{(2^t+1)(q-1)}))$.

Proof This lemma can be easily verified.

In the rest of this section, some common classes of Boolean functions over $\mathbb{F}_q$ are used to characterize hyper-bent functions over $\mathbb{F}_{2^n}$. Kloosterman sum identities and cubic sums are linked with the characterization of hyper-bent functions.

3.1 Hyper-bent functions from $g(y) = Tr_1^m(ay^{-d})$

From Theorem 1, we have the following proposition.

Proposition 4 *Let d be an odd integer such that $q-3 \geq d \geq 1$ and $gcd(d, q-1) = e > 1$. Let $a \in \mathbb{F}_q$, $\rho \in \mathbb{F}_q^*$, $\rho^e = 1$, and $\rho \neq 1$. Then, the Boolean function $f(x) = \sum_{j=0}^{\frac{d-1}{2}} \binom{d}{j} Tr_1^n(ax^{(d-2j)(q-1)}) + \sum_{j=1}^{2^{m-2}} Tr_1^n(\frac{\rho^i}{1+\rho} x^{(2j-1)(q-1)}) \in \mathbb{F}_2[x]$ is hyper-bent, where $i = 0$ or $i = 1$.*

Proof Let $g(y) = Tr_1^m(ay^{-d})$. For any $\lambda \in \mathbb{F}_q^*$, we have

$$\widehat{\chi}_g(\lambda) = \sum_{y \in \mathbb{F}_q} (-1)^{Tr_1^m(ay^{-d}+\lambda y)} = \sum_{y \in \mathbb{F}_q} (-1)^{Tr_1^m(a(\rho y)^{-d}+\lambda(\rho y))} = \sum_{y \in \mathbb{F}_q} (-1)^{Tr_1^m(ay^{-d}+\lambda \rho y)},$$

i.e., $\widehat{\chi}_g(\lambda) = \widehat{\chi}_g(\lambda\rho)$. From Theorem 1, we have the hyper-bent function

$$f(x) = Tr_1^m(a\lambda^d(1+\rho)^d(x^{q-1} + x^{-(q-1)})^d) + Tr_1^m(\frac{\rho^i}{1+\rho} \frac{1}{x^{q-1} + x^{-(q-1)}}).$$

From Result (2) in Lemma 1, we have

$$f(x) = \sum_{j=0}^{d} Tr_1^m(a\lambda^d(1+\rho)^d \binom{d}{j} x^{(2j-d)(q-1)}) + \sum_{j=1}^{2^{m-2}} Tr_1^n((\frac{\rho^i}{1+\rho})^{2^{m-1}} x^{(2j-1)(q-1)}),$$

$$= \sum_{j=0}^{\frac{d-1}{2}} Tr_1^m(a\lambda^d(1+\rho)^d \binom{d}{j} (x^{(2j-d)(q-1)} + x^{(d-2j)(q-1)})) + \sum_{j=1}^{2^{m-2}} Tr_1^n((\frac{\rho^i}{1+\rho})^{2^{m-1}} x^{(2j-1)(q-1)}),$$

$$= \sum_{j=0}^{\frac{d-1}{2}} \binom{d}{j} Tr_1^n(a\lambda^d(1+\rho)^d x^{(d-2j)(q-1)}) + \sum_{j=1}^{2^{m-2}} Tr_1^n((\frac{\rho^i}{1+\rho})^{2^{m-1}} x^{(2j-1)(q-1)}).$$

We can replace a by $\frac{a}{\lambda^d(1+\rho)^d}$ and ρ by $\rho^{2^{m-1}}$ and get that $f(x)$ is still hyper-bent. Hence, this proposition holds.

The coefficient $\binom{d}{j} \mod 2$ can be determined by Lucas's theorem. We will give the hyper-bent function $f(x)$ for cases $d = 2^s-1$ and $d = 2^s+1$ correspondingly in the following corollary.

Corollary 1 *Let $a \in \mathbb{F}_q$ and s be a positive integer.*

(1) Let $gcd(m,s) > 1$, $e = 2^{gcd(m,s)} - 1$, $\rho \in \mathbb{F}_q \setminus \mathbb{F}_2$, $\rho^e = 1$, and $i \in \{0,1\}$. Then the Boolean function $f(x) = \sum_{j=0}^{2^{s-1}} Tr_1^n(ax^{(2j-1)(q-1)}) + \sum_{j=1}^{2^{m-2}} Tr_1^n(\frac{\rho^i}{1+\rho}x^{(2j-1)(q-1)})$ is hyper-bent.

(2) Let $\frac{m}{gcd(m,s)}$ be even, $e = 2^{gcd(m,s)} + 1$, $\rho \in \mathbb{F}_q \setminus \mathbb{F}_2$, $\rho^e = 1$, and $i \in \{0,1\}$. Then the Boolean function $f(x) = Tr_1^n(a(x^{(2^s-1)(q-1)} + x^{(2^s+1)(q-1)})) + \sum_{j=1}^{2^{m-2}} Tr_1^n(\frac{\rho^i}{1+\rho}x^{(2j-1)(q-1)})$ is hyper-bent.

Proof Take $d = 2^s-1$. Then $e = 2^{gcd(m,s)}-1 = gcd(d, q-1)$. From Proposition 4, we have the hyper-bent function

$$f(x) = \sum_{j=0}^{2^{s-1}-1} \binom{2^s-1}{j} Tr_1^n(ax^{(d-2j)(q-1)}) + \sum_{j=1}^{2^{m-2}} Tr_1^n(\frac{\rho^i}{1+\rho}x^{(2j-1)(q-1)}).$$

From Lucas's Theorem, when $2^{s-1} - 1 \geq j \geq 0$, $\binom{2^s-1}{j} \equiv 1 \mod 2$. We have the hyper-bent function

$$f(x) = \sum_{j=1}^{2^{s-1}} Tr_1^n(ax^{(2j-1)(q-1)}) + \sum_{j=1}^{2^{m-2}} Tr_1^n(\frac{\rho^i}{1+\rho}x^{(2j-1)(q-1)}).$$

Result (1) holds.

Take $d = 2^s + 1$. Since $\frac{m}{gcd(m,s)}$ is even, $e = 2^{gcd(m,s)} + 1 = gcd(d, q-1)$. From Proposition 4, we have the hyper-bent function

$$f(x) = \sum_{j=0}^{2^{s-1}} \binom{2^s+1}{j} Tr_1^n(ax^{(d-2j)(q-1)}) + \sum_{j=1}^{2^{m-2}} Tr_1^n(\frac{\rho^i}{1+\rho}x^{(2j-1)(q-1)}).$$

From Lucas's Theorem, when $2^{s-1} \geq j \geq 0$, $\binom{2^s+1}{j} \equiv 1 \mod 2$ holds only for $j = 0, 1$. Then we have the hyper-bent function

$$f(x) = Tr_1^n(a(x^{(2^s-1)(q-1)} + x^{(2^s+1)(q-1)})) + \sum_{j=1}^{2^{m-2}} Tr_1^n(\frac{\rho^i}{1+\rho}x^{(2j-1)(q-1)}).$$

Result (2) holds.

3.2 Hyper-bent functions from $g(y) = Tr_1^m(y)$

Take $g(y) = Tr_1^m(y)$. Note that $\sum_{y\in\mathbb{F}_q}(-1)^{Tr_1^m(\mu y)} = 0 \quad (\mu \neq 0)$. Thus, for any $\lambda \in \mathbb{F}_q \setminus \mathbb{F}_2$, we have $\widehat{\chi}_g(0) = \widehat{\chi}_g(\lambda) = 0$. From Theorem 1, we have the

Corollary 2 *Let $b \in \mathbb{F}_q$ and $\epsilon \in \mathbb{F}_2$. The following Boolean functions $Tr_1^n((b^2+b)x^{q-1})+\sum_{i=1}^{2^{m-2}} Tr_1^n((b+\epsilon)x^{(2i-1)(q-1)})$ $(b \notin \mathbb{F}_2)$, $Tr_1^n((b^2+b)x^{q-1})+\sum_{i=1}^{2^{m-2}} Tr_1^n((b^2+\epsilon)x^{(2i-1)(q-1)})$ $(b \notin \mathbb{F}_2)$, and $Tr_1^n((b^4+b)x^{q-1})+\sum_{i=1}^{2^{m-2}} Tr_1^n((b^4+\epsilon)x^{(2i-1)(q-1)})$ $(b \notin \mathbb{F}_4)$ are all hyper-bent.*

Proof From [7], when $b \in \mathbb{F}_q \setminus \mathbb{F}_2$, we have the following Kloosterman sum identities: $K_m(b^3(1+b)) = K_m((1+b)^3 b)$, $K_m(b^5(1+b)) = K_m((1+b)^5 b)$, and $K_m(b^8(b^4+b)) = K_m((1+b)^8(b^4+b))$. Consider the following three cases:

(1) $\lambda_1 = b^3(1+b)$ and $\lambda_2 = (1+b)^3 b$, where $b \in \mathbb{F}_q \setminus \mathbb{F}_2$. Then $\lambda_1 \neq \lambda_2$;

(2) $\lambda_1 = b^5(1+b)$ and $\lambda_2 = (1+b)^5 b$, where $b \in \mathbb{F}_q \setminus \mathbb{F}_2$. Then $\lambda_1 \neq \lambda_2$;

(3) $\lambda_1 = b^8(b^4+b)$ and $\lambda_2 = (1+b)^8(b^4+b)$, where $b \in \mathbb{F}_q \setminus \mathbb{F}_4$. Then $\lambda_1 \neq \lambda_2$;

From Theorem 2, this corollary can be obtained immediately.

3.4 Hyper-bent functions from $g(y) = Tr_1^m(y^{2^{t-1}-1})$

Take $g(y) = Tr_1^m(y^{2^{t-1}-1})$, $t \geq 1$, $\lambda_i \in \mathbb{F}_q$ $(i = 1, 2)$, and $\lambda_1 \neq \lambda_2$. From Result (2) and Result (4) in Lemma 1, the Boolean function defined in (1) over $\mathbb{F}_{q^2}$ is

$$f(x) = \sum_{j=1}^{2^{m-t}} Tr_1^n((\lambda_1+\lambda_2)^{2^{m-t+1}-1} x^{(2j-1)(q-1)}) + \sum_{j=1}^{2^{m-2}} Tr_1^n((\frac{\lambda_i}{\lambda_1+\lambda_2})^{2^{m-1}} x^{(2j-1)(q-1)}). \tag{2}$$

From Theorem 1, we have the following theorem.

Theorem 3 *Let $f(x)$ be defined in (2). Then $f(x)$ is hyper-bent if and only if $\sum_{y\in\mathbb{F}_q}(-1)^{Tr_1^m(y^{2^{t-1}-1}+\lambda_1 y)} = \sum_{y\in\mathbb{F}_q}(-1)^{Tr_1^m(y^{2^{t-1}-1}+\lambda_2 y)}$.*

If $gcd(t-1, m) = 1$, then $gcd(2^{t-1}-1, 2^m-1) = 1$ and $y \mapsto y^{2^{t-1}-1}$ is a permutation of $\mathbb{F}_q$, and $\sum_{y\in\mathbb{F}_q}(-1)^{Tr_1^m(y^{2^{t-1}-1})} = 0$. Hence, we have the following corollary.

Corollary 3 *Let $gcd(t-1, m) = 1$, $\lambda \in \mathbb{F}_q^*$, and $\epsilon \in \mathbb{F}_2$. The Boolean function*

$$f(x) = \sum_{j=1}^{2^{m-t}} Tr_1^n(\lambda^{2^{m-t+1}-1} x^{(2j-1)(q-1)}) + \epsilon \sum_{j=1}^{2^{m-2}} Tr_1^n(x^{(2j-1)(q-1)})$$

is hyper-bent if and only if $\sum_{y\in\mathbb{F}_q}(-1)^{Tr_1^m(y^{2^{t-1}-1}+\lambda y)} = 0$.

This corollary generalizes Theorem 6 in [19]. It is easy to verify that when $t = 1, 2$, the hyper-bent function defined in (2) is just the hyper-bent function in Remark 1. In the following subsection, we discuss the case $t = 3$. When $t = 3$, $\widehat{\chi}_g(\lambda)$ is just the cubic sum $C_m(1, \lambda)$.

When m is odd, from Proposition 2, we have $\widehat{\chi}_g(\lambda) \in \{0, \pm(\frac{2}{m})2^{(m+1)/2}\}$. Define $H_{1,0} = \{\lambda \in \mathbb{F}_q : \widehat{\chi}_g(\lambda) = 0\}$, $H_{1,1} = \{\lambda \in \mathbb{F}_q : \widehat{\chi}_g(\lambda) = (\frac{2}{m})2^{(m+1)/2}\}$, and $H_{1,-1} = \{\lambda \in \mathbb{F}_q : \widehat{\chi}_g(\lambda) = -(\frac{2}{m})2^{(m+1)/2}\}$. Further, from Proposition 2, we have $H_{1,0} = \{\lambda \in \mathbb{F}_q : Tr_1^m(\lambda) = 0\}$, $H_{1,1} = \{\gamma^4 + \gamma + 1 : Tr_1^m(\gamma^3 + \gamma) = 0\} \cup \{1\}$, and $H_{1,-1} = \{\gamma^4 + \gamma + 1 : Tr_1^m(\gamma^3 + \gamma) = 1\}$.

From Theorem 1, we have the following corollary.

Corollary 4 *Let m be odd, $\lambda_i \in \mathbb{F}_q (i = 1, 2)$, and $\lambda_1 \neq \lambda_2$. Then, the Boolean function*

$$f(x) = \sum_{j=1}^{2^{m-3}} Tr_1^n((\lambda_1+\lambda_2)^{2^{m-2}-1}x^{(2j-1)(q-1)}) + \sum_{j=1}^{2^{m-2}} Tr_1^n((\frac{\lambda_i}{\lambda_1 + \lambda_2})^{2^{m-1}} x^{(2j-1)(q-1)})$$

is hyper-bent if and only if there exists $j \in \{0, 1, -1\}$ such that $\lambda_1, \lambda_2 \in H_{1,j}$.

Remark 2 Note that the cardinality of $\{\widehat{\chi}_g(\lambda) | \lambda \in \mathbb{F}_q\}$ is 3. If we suppose $q = 2^m > 3$ and take four elements in $\mathbb{F}_q$, then there exists two elements $\lambda_1, \lambda_2 \in \mathbb{F}_q$ lying in some $H_{1,j}$. Hence we can get a corresponding hyper-bent function.

Note that $0 \in H_{1,0}$. Then we have the following corollary.

Corollary 5 *Let m be odd, $\lambda \in \mathbb{F}_q^*$, and $\epsilon \in \mathbb{F}_2$. The Boolean function $f(x) = \sum_{j=1}^{2^{m-3}} Tr_1^n(\lambda^{2^{m-2}-1}x^{(2j-1)(q-1)}) + \epsilon \sum_{j=1}^{2^{m-2}} Tr_1^n(x^{(2j-1)(q-1)})$ is hyper-bent if and only if $Tr_1^m(\lambda) = 0, \lambda \neq 0$.*

These corollaries generalize Result (3) in Corollary 6 in [19].

When m is even, from Proposition 3, $\widehat{\chi}_g(\lambda) \in \{0, \pm(-1)^{\frac{m}{2}+1}2^{\frac{m}{2}+1}\}$. Define $H_{0,0} = \{\lambda \in \mathbb{F}_q : \widehat{\chi}_g(\lambda) = 0\}$, $H_{0,1} = \{\lambda \in \mathbb{F}_q : \widehat{\chi}_g(\lambda) = (-1)^{\frac{m}{2}+1}2^{\frac{m}{2}+1}\}$, and $H_{0,-1} = \{\lambda \in \mathbb{F}_q : \widehat{\chi}_g(\lambda) = -(-1)^{\frac{m}{2}+1}2^{\frac{m}{2}+1}\}$. From Proposition 3, we have $H_{0,0} = \{\lambda \in \mathbb{F}_q : Tr_2^m(\lambda) \neq 0\}$, $H_{0,1} = \{(\gamma^4 + \gamma)^{2^{m-1}} : \gamma \in \mathbb{F}_q, Tr_1^m(\gamma^3) = 0\}$, and $H_{0,-1} = \{(\gamma^4 + \gamma)^{2^{m-1}} : \gamma \in \mathbb{F}_q, Tr_1^m(\gamma^3) = 1\}$. Obviously, $0 \in H_{0,1}$.

Lemma 2 $1 \in H_{0,1}$ *if and only if* $8|m$.

Proof From the definition of $H_{0,1}$, we have $1 \in H_{0,1}$ if and only if there exists $\gamma \in \mathbb{F}_q$ satisfying $\gamma^4 + \gamma + 1 = 0$ and $Tr_1^m(\gamma^3) = 0$. It is easy to verify that $\gamma^4 + \gamma + 1 = 0$ is irreducible over $\mathbb{F}_2$. Thus, $4|m$. Further, $Tr_1^m(\gamma^3) = Tr_1^4(Tr_4^m(\gamma^3)) = \frac{m}{4} = 0$. Hence, this theorem follows.

From Theorem 1, we have the following corollary.

Corollary 6 *Let m be even, $\lambda_i \in \mathbb{F}_q (i = 1, 2)$, and $\lambda_1 \neq \lambda_2$. The Boolean function*

$$f(x) = \sum_{j=1}^{2^{m-3}} Tr_1^n((\lambda_1 + \lambda_2)^{2^{m-2}-1}x^{(2j-1)(q-1)}) + \sum_{j=1}^{2^{m-2}} Tr_1^n((\frac{\lambda_i}{\lambda_1 + \lambda_2})^{2^{m-1}} x^{(2j-1)(q-1)})$$

is hyper-bent if and only if there exists $j \in \{0, 1, -1\}$ satisfying $\lambda_1, \lambda_2 \in H_{0,j}$.

When $8|m$, from Lemma 2, we have $0, 1 \in H_{0,1}$. Hence, we have the following hyper-bent functions : $f_0(x) = \sum_{j=1}^{2^{m-3}} Tr_1^n(x^{(2j-1)(q-1)})$ and $f_1(x) = \sum_{j=2^{m-3}+1}^{2^{m-2}} Tr_1^n(x^{(2j-1)(q-1)})$.

4 Conclusion

In this paper, we characterize hyper-bent functions from Boolean functions with the Walsh spectrum taking the same value twice. From our method, many results on exponential sums can be used in the characterization of hyper-bent functions. We use some Kloosterman sum identities and the Walsh spectra of some common Boolean functions to characterize several classes of hyper-bent functions.

Acknowledgements This work was supported by the Natural Science Foundation of China (Grant No.10990011 & No. 61272499).

References

1. Carlitz, L.: Explicit evaluation of certain exponential sums. Math. Scand., vol. 44, pp. 5–16, 1979
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. Charpin, P., Gong, G.: Hyperbent functions, Kloosterman sums and Dickson polynomials. IEEE Trans. Inf. Theory, vol. 9, no. 54, pp 4230–4238, 2008
6. 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
7. Cao, X., Hollmann, H.D.L., Xiang Q.: New Kloosterman sum identities and equalities over finite fields. Finite Fields and Their Applications, vol. 14, 823–833, 2008
8. Dillon, J.: Elementary Hadamard Difference Sets. Ph.D., Univ. Maryland, 1974
9. Dillon, J. F., Dobbertin, H.: New cyclic difference sets with Singer parameters. Finite Fields Applicat., vol. 10, no. 3, pp. 342–389, 2004
10. Dobbertin, H., Leander, G.: A survey of some recent results on bent functions. In SETA 2004, vol. 3486, LNCS, pp. 1–29
11. 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
12. Flori, J. P., Mesnager, S.: An efficient characterization of a family of hyper-bent functions with multiple trace terms. Journal of Mathematical Cryptology. Vol 7 (1), pages 43–68, 2013
13. Flori, J.P., Mesnager, S.: Dickson polynomials, hyperelliptic curves and hyper-bent functions. Proceedings of 7-th International conference SEquences and Their Applications, SETA 2012, Waterloo, Canada. LNCS 7780, pages 40–52, Springer, 2012
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. Leander, G.: Monomial bent functions. IEEE Trans. Inf. Theory, vol. 2, no. 52, pp. 738–743, 2006
17. Leander, G., Kholosha, A.: Bent functionswith 2^r Niho exponents. IEEE Trans. Inf. Theory, vol. 52, no. 12, pp. 5529–5532, 2006
18. Lisonek, P.: An Efficient Characterization of a Family of Hyperbent Functions. IEEE Trans. Inf. Theory, vol. 57, no. 9, pp. 6010–6014, 2011
19. Li, N., Helleseth, T., Tang, X., Kholosha, A.: Several new classes of bent functions from Dillon exponents. IEEE Trans. Inf. Theory, 59(3), 1818–1831. 2013
20. 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.
21. Mesnager, S.: A new class of bent and hyper-bent Boolean functions in polynomial forms. Des. Codes Cryptography, 59(1-3):265–279, 2011
22. 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
23. Mesnager, S.: 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
24. Mesnager, S.: 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
25. Mesnager, S., Flori, J. P.: Hyper-bent functions via Dillon-like exponents, IEEE Trans. Inf. Theory. Vol. 59 No. 5, pages 3215-3232, 2013
26. Rothaus, O. S.: On bent functions. J. Combin. Theory, ser. A, vol. 20, pp. 300–305, 1976
27. Wang, B., Tang, C., Qi, Y., Yang, Y.: A generalization of the class of hyper-bent Boolean functions in binomial forms. Cryptology ePrint Archive, Report 2011/698, 2011. http://eprint.iacr.org/
28. Wang, B., Tang, C., Qi, Y., Yang, Y., Xu, M.: A new class of hyper-bent Boolean functions in binomial forms.CoRR, abs/1112.0062, 2011
29. Wang, B., Tang, C., Qi, Y., Yang, Y., Xu, M.: A new class of hyper-bent Boolean functions with multiple trace terms. Cryptology ePrint Archive, Report 2011/600, 2011. http://eprint.iacr.org/
30. Youssef, A. M., Gong, G.: Hyper-bent functions. In Advances in Crypology C Eurocrypt01, 2001, LNCS, pp. 406-419
31. 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