Cryptogr. Commun. (2017) 9:647–664
DOI 10.1007/s12095-016-0207-4

A class of hyper-bent functions and Kloosterman sums

Chunming Tang[1] · Yanfeng Qi[2]

Received: 10 May 2016 / Accepted: 29 September 2016 / Published online: 10 October 2016

Abstract This paper is devoted to the characterization of hyper-bent functions. Several classes of hyper-bent functions have been studied, such as Charpin and Gong's family $\sum_{r\in R} \mathrm{Tr}_1^n(a_r x^{r(2^m-1)})$ and Mesnager's family $\sum_{r\in R} \mathrm{Tr}_1^n(a_r x^{r(2^m-1)}) + \mathrm{Tr}_1^2(bx^{\frac{2^n-1}{3}})$. In this paper, we generalize these results by considering the following class of Boolean functions over $\mathbb{F}_{2^n}$:

$$\sum_{r\in R}\sum_{i=0}^{2} Tr_1^n(a_{r,i}x^{r(2^m-1)+\frac{2^n-1}{3}i}) + Tr_1^2(bx^{\frac{2^n-1}{3}}),$$

where $n = 2m$, m is odd, $b \in \mathbb{F}_4$, and $a_{r,i} \in \mathbb{F}_{2^n}$. With the restriction of $a_{r,i} \in \mathbb{F}_{2^m}$, we present a characterization of hyper-bentness of these functions in terms of crucial exponential sums. For some special cases, we provide explicit characterizations for some hyper-bent functions in terms of Kloosterman sums and cubic sums. Finally, we explain how our results on binomial, trinomial and quadrinomial hyper-bent functions can be generalized to the general case where the coefficients $a_{r,i}$ belong to the whole field $\mathbb{F}_{2^n}$.

Keywords Bent functions · Hyper-bent functions · Walsh-Hadmard trasform · Dickson polynomials · Kloosterman sums

Mathematics Subject Classification (2010) 06E75 · 94A60

✉ Chunming Tang
tangchunmingmath@163.com

Yanfeng Qi
qiyanfeng07@163.com

[1] School of Mathematics and Information, China West Normal University, Sichuan Nanchong, 637002, China

[2] School of Science, Hangzhou Dianzi University, Hangzhou, Zhejiang, 310018, China

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 [29] as interesting combinatorial objects have been extensively studied for their applications not only in cryptography, but also in coding theory [3, 25, 31] and combinatorial 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 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. Hyper-bent functions as a subclass of bent functions [15, 35] achieve the maximal minimum distance to all the coordinate functions of all bijective monomials (i.e., functions of the form $\mathrm{Tr}_1^n(ax^i) + \epsilon$, $\gcd(i, 2^n - 1) = 1$). It is still elusive to completely characterize bent and hyper-bent functions. Much research on bent and hyper-bent functions on $\mathbb{F}_{2^n}$ can be found in [1, 5, 7–10, 14, 17, 18, 22, 24–26, 36].

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

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

where $n = 2m$, R is a set of representations of the cyclotomic cosets modulo $2^m + 1$ of maximal size n [1] and $a_r \in \mathbb{F}_{2^m}$. The characterization of these hyper-bent functions was presented by the exponential sums on $\mathbb{F}_{2^m}$. Lisoněk [20] presented another characterization of Charpin and Gong's hyper-bent functions in terms of the number of rational points on certain hyper-elliptic curves. He provided an algorithm for determining such hyper-bent functions with time complexity and space complexity $O(r_{max}^a m^b)$, 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 functions are monomial functions via Dillon-like exponent. Many authors have proved that the monomial function $Tr_1^n(ax^{r(2^m-1)})(a \in \mathbb{F}_{2^m})$ is hyper-bent if and only if $K_m(a) = 0$ (a proof can be found for instance in [17]).

In [22–25], Mesnager studied and characterized the hyper-bentness of the functions of the form (which are distinct from those of Charpin and Gong's functions)

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

She exhibited firstly binomial hyper-bent functions in [22, 23] and studied the case of multiple trace terms in [24, 25].

Afterward, Mesnager and Flori [27] considered a general class of Boolean functions and characterized the hyper-bentness of these 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 $b \in \mathbb{F}_{2^t}$. The so-called Mesnager's functions correspond then to the case where $t = 2$ and $s = \frac{2^m+1}{3}$. For the case: $t = 4$ and $s = \frac{2^m+1}{5}$, explicit characterizations were given in [32–34]. When r_{max} is small, Flori and Mesnager [11, 12] used the number of rational points on hyper-elliptic curves to determine those classes of hyper-bent functions.

[1] Later, Flori and Mesnager [11] have shown that the condition of maximality is not necessary.

Next, Li et al. [19] characterized a class of Boolean functions of the form

$$f(x) = \sum_{i=0}^{q-1} Tr_1^n(a_i x^{i(q-1)}) + Tr_1^l(\epsilon x^{\frac{q^2-1}{e}}),$$

where $n = 2m$, $q = p^m$ (p is a prime), $e|(q+1)$, $a_i \in \mathbb{F}_{q^2}$, $\epsilon \in \mathbb{F}_{p^l}$, and l is the smallest positive integer satisfying $l|n$ and $e|p^l - 1$.

The coefficients a_r in these above Boolean function are restricted to the subfield $\mathbb{F}_{2^m}$. This paper considers a class of Boolean functions of the form

$$\sum_{r\in R}\sum_{i=0}^{2} Tr_1^n(a_{r,i} x^{r(2^m-1)+\frac{2^n-1}{3}i}) + Tr_1^2(bx^{\frac{2^n-1}{3}}),$$

where $n = 2m$, m is odd, $b \in \mathbb{F}_4$, and $a_{r,i} \in \mathbb{F}_{2^n}$. We first characterize the hyper-bentness of this class of Boolean functions in terms of exponential sums on $\mathbb{F}_{2^m}$. Using these results, we exhibit some hyper-bent functions via the so-called *Dillon-like exponent* in terms of the well-known *cubic sums* and *Kloosterman sums*. Further, our characterizations can also be applied in the general case for $a_{r,i} \in \mathbb{F}_{2^n}$.

The following paper is organized as follows: Section 2 introduces some notations and background. Section 3 considers a class of Boolean functions and presents the characterization of hyper-bentness of these functions with exponential sums on $\mathbb{F}_{2^m}$. Section 4 gives an explicit characterization of some special hyper-bent functions with multiple trace terms in terms of Kloosterman sums and cubic sums. Section 5 provides a conclusion.

2 Preliminaries

2.1 Boolean functions

Let n be a positive integer, $\mathbb{F}_{2^n}$ be a finite field with 2^n elements, $\mathbb{F}_{2^n}^*$ be the multiplicative group of $\mathbb{F}_{2^n}$, and $\mathbb{F}_{2^k}$ be a subfield of $\mathbb{F}_{2^n}$. The trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^k}$ is denoted by $\mathrm{Tr}_k^n(x) = \sum_{i=0}^{n/k-1} x^{2^{ik}}$. When $k = 1$, $\mathrm{Tr}_1^n(\cdot)$ is called the *absolute trace function*.

A Boolean function over $\mathbb{F}_{2^n}$ can be represented by

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

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 $\mathrm{wt}(f) := \#\{x \in \mathbb{F}_{2^n} | f(x) = 1\}$.

The "sign" function of a Boolean function f is defined by $\chi(f) := (-1)^f$. The Walsh-Hadamard transform of f over $\mathbb{F}_{2^n}$ 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, $\deg(f) \leq \frac{n}{2}$ [2]. 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.

It has been proved in [3] and [35] that if f is a hyper-bent function, then $\deg(f) = \frac{n}{2}$. 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 3 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 $x, y \in \mathbb{F}_{2^m}$, 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 $\beta \in \mathbb{F}_{2^m}^*$ and $z \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$. Youssef and Gong [35] 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, [3] 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 $f(x) = g(\delta x)$.*

Charpin and Gong [5] 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 $\{i \,|\, f(\xi^i) = 1, 0 \leq i \leq 2^m\}$ is 2^{m-1}.*

2.2 Dickson polynomials

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

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

with initial values $D_0(x) = 0$ and $D_1(x) = x$.

Some properties of Dickson polynomials are given below.

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

More results on Dickson polynomials over $\mathbb{F}_2$ can be found in [28].

2.3 Kloosterman sums and cubic sums

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

Definition 4 The binary Kloosterman sums associated with a are

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

When $x = 0$, we set $\frac{1}{x} = 0$.

Some properties of binary Kloosterman sums are given in the following propositions [16].

Proposition 4 *Let $a \in \mathbb{F}_{2^m}$, then $K_m(a) \in [-2^{(m+2)/2} + 1, 2^{(m+2)/2} + 1]$ and $K_m(a) \equiv 0 \mod 4$.*

Another property of Kloosterman sums is stated in the following proposition [6].

Proposition 5 *Let $m \geq 3$ be an odd integer and $a \in \mathbb{F}_{2^m}$. Then*

$$K_m(a) \equiv 1 \mod 3 \text{ if and only if } Tr_1^m(a^{1/3}) = 0.$$

Definition 5 The binary cubic sums on $\mathbb{F}_{2^m}$ are

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

Carlitz [4] computed the exact values of the cubic sums in the following proposition.

Proposition 6 *Let m be a positive 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 $C_m(1, c) = \chi(Tr_1^m(\gamma^3 + \gamma))(\frac{2}{m})2^{(m+1)/2}$, where $c = \gamma^4 + \gamma + 1$, $(\frac{2}{m})$ is the Jacobi symbol , and $\gamma \in \mathbb{F}_{2^m}$.*

From Proposition 5 and Proposition 6, we have the following corollary.

Corollary 1 *Let m be odd and $a \in \mathbb{F}_{2^m}^*$, the following results are equivalent:*

(1) $K_m(a) \equiv 1 \mod 3$;
(2) $C_m(a, a) = 0$;
(3) $Tr_1^m(a^{\frac{1}{3}}) = 0$.

2.4 Exponential sums

Let m be an odd integer, $U = \{u : u^{2^m+1} = 1, u \in \mathbb{F}_{2^n}\}$ and $V = U^3 = \{u^3 : u \in U\}$. Let ξ be a generator of U and $w = \xi^{\frac{2^m+1}{3}}$. Let R be a set of representations of the cyclotomic cosets modulo $2^m + 1$ and $a_r \in \mathbb{F}_{2^m}$. For simplicity, some notations on exponential sums are defined below.

$$S_i((a_r)_{r\in R}) = \sum_{v\in V} \chi(Tr_1^n(\sum_{r\in R} a_r(\xi^i v)^{r(2^m-1)})); \; T_i((a_r)_{r\in R}) = \sum_{x\in\mathbb{F}_{2^m}, Tr_1^m(x^{-1})=i} \chi(Tr_1^m(\sum_{r\in R} a_r D_r(x))).$$

$$T_i^3((a_r)_{r\in R}) = \sum_{x\in\mathbb{F}_{2^m}, Tr_1^m(x^{-1})=i} \chi(Tr_1^m(\sum_{r\in R} a_r D_r(D_3(x)))); \; \Xi((a_r)_{r\in R}) = \sum_{x\in\mathbb{F}_{2^m}} \chi(Tr_1^m(\sum_{r\in R} a_r D_r(x)));$$

$$\overline{\Xi}((a_r)_{r\in R}) = \sum_{x\in\mathbb{F}_{2^m}} \chi(Tr_1^m(\frac{1}{x} + \sum_{r\in R} a_r D_r(x))); \; \Xi^3((a_r)_{r\in R}) = \sum_{x\in\mathbb{F}_{2^m}} \chi(Tr_1^m(\sum_{r\in R} a_r D_r(D_3(x)))).$$

$$\overline{\Xi}^3((a_r)_{r\in R}) = \sum_{x\in\mathbb{F}_{2^m}} \chi(Tr_1^m(\frac{1}{x} + \sum_{r\in R} a_r D_r(D_3(x)))).$$

In all evidence, if $i \equiv j \mod 2^m + 1$, then $S_i((a_r)_{r\in R}) = S_j((a_r)_{r\in R})$. Some relationships of these exponential sums are given in the following proposition [27].

Proposition 7

(1) $S_0((a_r)_{r\in R}) = \frac{1}{3}(1 + 2T_1^3((a_r)_{r\in R})) = \frac{1}{3}[1 + 2\Xi^3((a_r)_{r\in R}) - 2T_0((a_r)_{r\in R})]$; $S_1((a_r)_{r\in R}) = S_2((a_r)_{r\in R})$; $S_0((a_r)_{r\in R}) + S_1((a_r)_{r\in R}) + S_2((a_r)_{r\in R}) = 1 + 2T_1((a_r)_{r\in R})$.

(2) $T_0^3((a_r)_{r\in R}) = T_0((a_r)_{r\in R})$; $T_1^3((a_r)_{r\in R}) = \Xi^3((a_r)_{r\in R}) - T_0((a_r)_{r\in R})$; $T_i((a_r)_{r\in R}) = \frac{1}{2}[\Xi((a_r)_{r\in R}) + (-1)^i\overline{\Xi}((a_r)_{r\in R})]$; $T_i^3((a_r)_{r\in R}) = \frac{1}{2}[\Xi^3((a_r)_{r\in R}) + (-1)^i\overline{\Xi}^3((a_r)_{r\in R})]$.

When $\#R = 1$, we write $(a)_R$ for $(a)_{r\in R}$ and a for $(a)_{\{1\}}$. From the definitions and Proposition 7, we have the following lemma.

Lemma 1 *Let $a \in \mathbb{F}_{2^m}$ and $gcd(r, \frac{2^m+1}{3}) = 1$, then*

(1) $S_0((a)_{\{r\}}) = S_0(a)$;

(2) *If $3 \nmid r$, $S_1((a)_{\{r\}}) = S_1(a)$; If $3 \mid r$, $S_1((a)_{\{r\}}) = S_0(a)$.*

Actually, $S_0(a)$ and $S_1(a)$ can be expressed by cubic sums and Kloosterman sums [22].

Lemma 2 *Let $a \in \mathbb{F}_{2^m}^*$, then*

(1) $S_0(a) = \frac{1}{3}[-K_m(a) + 2C_m(a, a) + 1]$;

(2) $S_1(a) = \frac{1}{3}[-K_m(a) - C_m(a, a) + 1]$.

Obviously, when $a \in \mathbb{F}_{2^m}$, we have $S_i(a) = S_i(a^2)$. From Lemma 2, Corollary 1, Proposition 4, and Proposition 6, we have the following lemma.

Lemma 3 *Let $m \geq 5$, $m \equiv 1 \mod 2$, and $a \in \mathbb{F}_{2^m}^*$. The following four conditions are equivalent:*

(1) $K_m(a) = 4$;
(2) $-S_0(a) = 1$;
(3) $-2S_0(a) + S_1(a) = 1$;
(4) $S_0(a) - 2S_1(a) = 1$.

3 A class of hyper-bent functions with multiple trace terms

In this section, we will consider a class of Boolean functions of the form

$$f_{a,b}(x) = \sum_{r\in R}\sum_{i=0}^{2} Tr_1^n(a_{r,i}x^{r(2^m-1)+\frac{2^n-1}{3}i}) + Tr_1^2(bx^{\frac{2^n-1}{3}}), \tag{1}$$

where $n = 2m$, m is odd, $a_{r,i} \in \mathbb{F}_{2^n}$ and $b \in \mathbb{F}_4$. With notations given in the previous section, we present the characterization of hyper-bent functions in (1).

Theorem 1 *Let $f_{a,b}$ be a Boolean function defined in (1) and $a'_{r,i}$ be defined by*

$$\begin{pmatrix} a'_{r,0} \\ a'_{r,1} \\ a'_{r,2} \end{pmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & w & w^2 \\ 1 & w^2 & w \end{bmatrix} \begin{pmatrix} a_{r,0} \\ a_{r,1} \\ a_{r,2} \end{pmatrix}. \tag{2}$$

where w is a primitive 3rd root of unity. Then $f_{a,b}$ is hyper-bent if and only if

$$\Lambda(f_{a,b}) = \sum_{u\in U} \chi(f_{a,b}(u)) = 1.$$

Further, we have that

$$\Lambda(f_{a,b}) = \chi(Tr_1^2(b))S_0((a'_{r,0})_{r\in R}) + \chi(Tr_1^2(bw))S_1((a'_{r,1})_{r\in R}) + \chi(Tr_1^2(bw^2))S_2((a'_{r,2})_{r\in R}).$$

If $a'_{r,2} \in \mathbb{F}_{2^m}$, then

$$\Lambda(f_{a,b}) = \chi(Tr_1^2(b))S_0((a'_{r,0})_{r\in R}) + \chi(Tr_1^2(bw))S_1((a'_{r,1})_{r\in R}) + \chi(Tr_1^2(bw^2))S_1((a'_{r,2})_{r\in R}).$$

Proof Let α be a primitive element in $\mathbb{F}_{2^n}$. From the definition of $f_{a,b}$, for $x \in \mathbb{F}_{2^m}$ we have that

$$f_{a,b}(\alpha^{2^m+1}x) = f_{a,b}(x), \quad f(0) = 0,$$

From Proposition 3, $f_{a,b}(x)$ is hyper-bent if and only if $\Lambda(f_{a,b}) = 1$ [24, 25]. Since $U = V \cup \xi V \cup \xi^2 V$,

$$\Lambda(f_{a,b}) = \sum_{u\in U} \chi(f_{a,b}(u)) = \sum_{v\in V} \chi(f_{a,b}(v)) + \sum_{v\in V} \chi(f_{a,b}(\xi v)) + \sum_{v\in V} \chi(f_{a,b}(\xi^2 v)).$$

For any $v \in V$, $v^{\frac{2^n-1}{3}} = 1$. Hence

$$\begin{aligned}\Lambda(f_{a,b}) &= \chi(Tr_1^2(b)) \sum_{v\in V} \chi(\sum_{r\in R}\sum_{i=0}^{2} Tr_1^n(a_{r,i} v^{r(2^m-1)})) \\ &+ \chi(Tr_1^2(b\xi^{\frac{2^n-1}{3}})) \sum_{v\in V} \chi(\sum_{r\in R}\sum_{i=0}^{2} Tr_1^n(a_{r,i}\xi^{\frac{2^n-1}{3}i}(\xi v)^{r(2^m-1)})) \\ &+ \chi(Tr_1^2(b\xi^{\frac{2^n-1}{3}\cdot 2})) \sum_{v\in V} \chi(\sum_{r\in R}\sum_{i=0}^{2} Tr_1^n(a_{r,i}\xi^{\frac{2^n-1}{3}\cdot 2i}(\xi^2 v)^{r(2^m-1)})).\end{aligned}$$

Note that $\xi^{\frac{2^n-1}{3}} = (\xi^{\frac{2^m+1}{3}})^{2^m-1} = w^{2^m+1-2} = w$. We have that

$$\begin{aligned}\Lambda(f_{a,b}) &= \chi(Tr_1^2(b)) \sum_{v\in V} \chi(\sum_{r\in R} Tr_1^n((\sum_{i=0}^{2} a_{r,i}) v^{r(2^m-1)})) \\ &+ \chi(Tr_1^2(bw)) \sum_{v\in V} \chi(\sum_{r\in R} Tr_1^n((\sum_{i=0}^{2} a_{r,i} w^i)(\xi v)^{r(2^m-1)})) \\ &+ \chi(Tr_1^2(bw^2)) \sum_{v\in V} \chi(\sum_{r\in R} Tr_1^n((\sum_{i=0}^{2} a_{r,i} w^{2i})(\xi^2 v)^{r(2^m-1)})).\end{aligned}$$

From the definitions of $S_i((.)_{r\in R})$ and $a'_{r,i}$,

$$\begin{aligned}\Lambda(f_{a,b}) &= \chi(Tr_1^2(b))S_0((a'_{r,0})_{r\in R}) + \chi(Tr_1^2(bw))S_1((a'_{r,1})_{r\in R}) \\ &+\chi(Tr_1^2(bw^2))S_2((a'_{r,2})_{r\in R}).\end{aligned}$$

Note that if $a'_{r,2} \in \mathbb{F}_{2^m}$, $S_2((a'_{r,2})_{r\in R}) = S_1((a'_{r,2})_{r\in R})$. Then we have

$$\begin{aligned}\Lambda(f_{a,b}) &= \chi(Tr_1^2(b))S_0((a'_{r,0})_{r\in R}) + \chi(Tr_1^2(bw))S_1((a'_{r,1})_{r\in R}) \\ &+\chi(Tr_1^2(bw^2))S_1((a'_{r,2})_{r\in R}).\end{aligned}$$

The result follows. □

The values of $S_0((a'_{r,0})_{r\in R})$ and $S_1((a'_{r,1})_{r\in R})$ can be computed by means of exponential sums on $\mathbb{F}_{2^m}$. From Proposition 7, the following result is obtained.

Lemma 4 *Let $a_r \in \mathbb{F}_{2^m}$, then (1) $S_0((a_r)_{r\in R}) = \frac{1}{3}[2\Xi^3((a_r)_{r\in R}) - \Xi((a_r)_{r\in R}) - \overline{\Xi}((a_r)_{r\in R}) + 1]$; (2) $S_1((a_r)_{r\in R}) = \frac{1}{3}[-\Xi^3((a_r)_{r\in R}) + 2\Xi((a_r)_{r\in R}) - \overline{\Xi}((a_r)_{r\in R}) + 1]$.*

For the function $f_{a,b}$ with coefficients $a_r \in \mathbb{F}_{2^m}$, we can compute $\Lambda(f_{a,b})$ with exponential sums on $\mathbb{F}_{2^m}$. Note that $\chi(Tr_1^2(0)) = \chi(Tr_1^2(1)) = 1$ and $\chi(Tr_1^2(w)) = \chi(Tr_1^2(w^2)) = -1$. From Theorem 1 and Lemma 4, the value of $\Lambda(f_{a,b})$ can be computed by exponential sums $\Xi^3((a'_{r,0})_{r\in R})$, $\Xi((a'_{r,0})_{r\in R})$, $\overline{\Xi}((a'_{r,0})_{r\in R})$, $\Xi^3((a'_{r,1})_{r\in R})$, $\Xi((a'_{r,1})_{r\in R})$, $\overline{\Xi}((a'_{r,1})_{r\in R})$, $\Xi^3((a'_{r,2})_{r\in R})$, $2\Xi((a'_{r,2})_{r\in R})$, and $\overline{\Xi}((a'_{r,2})_{r\in R})$.

4 Hyper-bent functions and Kloosterman sums

In this section, we charcterize the hyper-bentness of certain functions in some particular cases by means of Kloosterman sums and cubic sums. Further, we try to generalize the characterization of some special hyper-bent functions for general cases: $a_{r,i} \in \mathbb{F}_{2^n}$.

4.1 Explicit characterization of hyper-bent functions with coefficients in $\mathbb{F}_{2^m}$

Theorem 2 *Let $gcd(r_i, \frac{2^m+1}{3}) = 1, a, c, d \in \mathbb{F}_{2^m}$ and w be a primitive 3rd root of unity. Let $f(x)$ be defined by*

$$\begin{aligned} f(x) &= Tr_1^n(a(x^{r_0(2^m-1)} + x^{r_0(2^m-1)+\frac{2^n-1}{3}} + x^{r_0(2^m-1)+2\frac{2^n-1}{3}})) \\ &+ Tr_1^n(c(x^{r_1(2^m-1)} + w^2x^{r_1(2^m-1)+\frac{2^n-1}{3}} + wx^{r_1(2^m-1)+2\frac{2^n-1}{3}})) \\ &+ Tr_1^n(d(x^{r_2(2^m-1)} + wx^{r_2(2^m-1)+\frac{2^n-1}{3}} + w^2x^{r_2(2^m-1)+2\frac{2^n-1}{3}})) \\ &+ Tr_1^2(bx^{\frac{2^n-1}{3}}). \end{aligned} \tag{3}$$

Then

(1) *If $b = 0$, $f(x)$ is hyper-bent if and only if $S_0(a) + S_1((c)_{\{r_1\}}) + S_1((d)_{\{r_2\}}) = 1$;*
(2) *If $b = 1$, $f(x)$ is hyper-bent if and only if $S_0(a) - S_1((c)_{\{r_1\}}) - S_1((d)_{\{r_2\}}) = 1$;*
(3) *If $b = w$, $f(x)$ is hypre-bent if and only if $-S_0(a) - S_1((c)_{\{r_1\}}) + S_1((d)_{\{r_2\}}) = 1$;*
(4) *If $b = w^2$, $f(x)$ is hyper-bent if and only if $-S_0(a) + S_1((c)_{\{r_1\}}) - S_1((d)_{\{r_2\}}) = 1$.*

Proof Let $R = \{r_0, r_1, r_2\}$. Take $a_{r_0,0} = a_{r_0,1} = a_{r_0,2} = a$, $a_{r_1,0} = c$, $a_{r_1,1} = cw^2$, $a_{r_1,2} = cw$, $a_{r_2,0} = d$, $a_{r_2,1} = dw$, and $a_{r_2,2} = dw^2$. Then

$$\begin{aligned} a'_{r_0,0} &= a, a'_{r_1,0} = 0, a'_{r_2,0} = 0, a'_{r,0} = 0 (r \notin R), \\ a'_{r_0,1} &= 0, a'_{r_1,1} = c, a'_{r_2,1} = 0, a'_{r,1} = 0 (r \notin R), \\ a'_{r_0,2} &= 0, a'_{r_1,2} = 0, a'_{r_2,2} = d, a'_{r,2} = 0 (r \notin R), \end{aligned}$$

From Lemma 1, we have

$$S_0((a'_{r,0})_{r\in R}) = S_0((a)_{\{r_0\}}) = S_0(a);\ S_1((a'_{r,1})_{r\in R}) = S_1((c)_{\{r_1\}});\ S_2((a'_{r,2})_{r\in R}) = S_2((a)_{\{r_2\}}).$$

From $Tr_1^2(w) = Tr_1^2(w^2) = 1, Tr_1^2(1) = 0$, and Theorem 1, this theorem can be immediately obtained. □

Corollary 2 *Let $gcd(r_i, \frac{2^m+1}{3}) = 1 (i = 1, 2)$, $a, c, d \in \mathbb{F}_{2^m}$, $Tr_1^m(a^{\frac{1}{3}}) = Tr_1^m(c^{\frac{1}{3}}) = Tr_1^m(d^{\frac{1}{3}}) = 0$, w be a primitive 3rd root of unity, and $f(x)$ be defined by (3). Then*

(1) *If $b = 0$, $f(x)$ is hyper-bent if and only if $K_m(a) + K_m(c) + K_m(d) = 0$;*
(2) *If $b = 1$, $f(x)$ is hyper-bent if and only if $-K_m(a) + K_m(c) + K_m(d) = 4$;*
(3) *If $b = w$, $f(x)$ is hyper-bent if and only if $K_m(a) + K_m(c) - K_m(d) = 4$;*
(4) *If $b = w^2$, $f(x)$ is hyper-bent if and only if $K_m(a) - K_m(c) + K_m(d) = 4$.*

Proof From $Tr_1^m(a^{\frac{1}{3}}) = 0$ and Corollary 1, we have $C_m(a, a) = 0$. From Lemma 2, we obtain $S_0(a) = S_1(a) = \frac{1}{3}(-K_m(a) + 1)$. Similarly, $S_0(c) = S_1(c) = \frac{1}{3}(-K_m(c) +$

1) and $S_0(d) = S_1(d) = \frac{1}{3}(-K_m(d) + 1)$. The corollary follows from Lemma 1 and Theorem 2. □

Example 1 Let $m = 23$, $\mathbb{F}_{2^m} \cong \mathbb{F}_2[x]/(x^{23} + x^5 + 1)$. Consider positive integers r_i such that $gcd(r_i, \frac{2^m+1}{3}) = 1 (i = 1, 2)$. Set

$$\begin{aligned} a &= a_0^3 = x^{23} + x^{16} + x^{15} + x^{13} + x^9 + x^8 + x^7 + x^6 + x^5 + x^3 + x^2 + x + 1, \\ c &= c_0^3 = x^{23} + x^{21} + x^{20} + x^{17} + x^{14} + x^{12} + x^{11} + x^{10} + x^7 + x^5 + 1, \\ d &= d_0^3 = x^{23} + x^{21} + x^{19} + x^{17} + x^{12} + x^{11} + x^{10} + x^8 + x^6 + x^4 + x^2 + x + 1, \\ b &= 0; \end{aligned}$$

where $a_0 = x^{23}+x^{21}+x^{19}+x^{16}+x^{14}+x^{12}+x^{11}+x^{10}+x^8+x^6+x^5+x^3+x^2+x+1$, $c_0 = x^{23}+x^{21}+x^{18}+x^{13}+x^{12}+x^8+x^7+x^4+x^3+x+1$, $d_0 = x^{23}+x^{21}+x^{19}+x^{18}+x^{17}+x^{13}+x^{12}+x^{10}+x^7+x^6+x^3+x^2+1$. Then $Tr_1^m(a_0) = 0$, $Tr_1^m(c_0) = 0$, $Tr_1^m(d_0) = 0$, and $K_m(a) = 1120$, $K_m(c) = 2920$, $K_m(d) = -4040$, $K_m(a) + K_m(c) + K_m(d) = 0$. Hence, $f(x)$ in (3) is a hyper-bent function with nine trace terms.

Many hyper-bent functions of the form (3) exist. From an exhaustive search, when $m = 5, 7$, the number of the hyper-bent functions in Result (1) in Corollary 2 are 1500 and 58653 respectively, and the number of the hyper-bent functions in Result (2) in Corollary 2 are 1500 and 57624 respectively.

For some special cases, from Lemma 1, Lemma 2, Lemma 3, Theorem 1, and Theorem 2, we can straightforwardly obtain the following theorem on the explicit characterization of hyper-bent functions $f_{a,b}$ in (3).

Theorem 3 *Let $gcd(r_i, \frac{2^m+1}{3}) = 1$, $a \in \mathbb{F}_{2^m}$, and w be a primitive 3rd root of unity. Let $f(x)$ be defined by (3) with $a = c = d$. Then*

(1) *If $b = 0$ and $3 | r_i (i = 1, 2)$, $f(x)$ is not hyper-bent;*
(2) *If $b = 0$ and $3 \nmid r_i (i = 1, 2)$, $f(x)$ is hyper-bent if and only if $K_m(a) = 0$;*
(3) *If $b = 0$ and $\#\{r_i : r_i \equiv 0 \mod 3, i = 1, 2\} = 1$, $f(x)$ is hyper-bent if and only if $K_m(a) = C_m(a, a)$;*
(4) *For the following cases: i) $b = 1$, $\#\{r_i : r_i \equiv 0 \mod 3, i = 1, 2\} = 1$; ii) $b = w$, $3 \nmid r_1$, $3 \mid r_2$; and iii) $b = w^2$, $3 \mid r_1$, $3 \nmid r_2$; $f(x)$ is hyper-bent if and only if $K_m(a) = -C_m(a, a) + 4$;*
(5) *For the rest cases, $f(x)$ is hyper-bent if and only if $K_m(a) = 4$.*

Remark 1 The value a such that $K_m(a) = 0, 4$ or $-C_m(a, a) + 4$ can be used to construct monomial hyper-bent functions [5, 8, 13, 17] or binomial hyper-bent functions by Mesnager [22, 26]. From the above theorem, the value a such that $K_m(a) = C_m(a, a)$ can be used to construct hyper-bent functions. From Corollary 1, if $K_m(a) = C_m(a, a)$, then $Tr_1^m(a^{1/3}) = 1$. Obviously, if a satisfies $K_m(a) = C_m(a, a)$, any Frobenius conjugate a^{2^i} of a also satisfies $K_m(a^{2^i}) = C_m(a^{2^i}, a^{2^i})$. Actually, If $m = 5, 7, 9$, just one conjugacy class satisfies $K_m(a) = C_m(a, a)$, and if $m = 11, 13, 15$, there are 3,8,9 conjugacy classes.

Take $R = \{r_0, r_1\}$, $a_{r_0,0} = a_{r_0,1} = a_{r_0,2} = a$, $a_{r_1,0} = 0$, and $a_{r_1,1} = a_{r_1,2} = c$. From Lemma 1 and Theorem 1, the theorem comes straightforwardly.

Theorem 4 *Let $a, c \in \mathbb{F}_{2^m}$, $b \in \mathbb{F}_4$, and $gcd(r_i, \frac{2^m+1}{3}) = 1$. Let $f(x)$ be defined by*

$$\begin{aligned} f(x) &= Tr_1^n(a(x^{r_0(2^m-1)} + x^{r_0(2^m-1)+\frac{2^n-1}{3}} + x^{r_0(2^m-1)+2\frac{2^n-1}{3}})) \\ &+ Tr_1^n(c(x^{r_1(2^m-1)+\frac{2^n-1}{3}} + x^{r_1(2^m-1)+2\frac{2^n-1}{3}})) + Tr_1^2(bx^{\frac{2^n-1}{3}}), \end{aligned} \tag{4}$$

Then

(1) *If $b = 0$, $f(x)$ is hyper-bent if and only if $S_0(a) + 2S_1((c)_{\{r_1\}}) = 1$;*
(2) *If $b = 1$, $f(x)$ is hyper-bent if and only if $S_0(a) - 2S_1((c)_{\{r_1\}}) = 1$;*
(3) *If b is a primitive 3rd root of unity, $f(x)$ is hyper-bent if and only if $S_0(a) = -1$.*

From Corollary 1, Lemma 2, Lemma 1, and Theorem 4, the following corollary can be obtained straightforwardly.

Corollary 3 *Let $a, c \in \mathbb{F}_{2^m}$, $Tr_1^m(a^{\frac{1}{3}}) = Tr_1^m(c^{\frac{1}{3}}) = 0$, $b \in \mathbb{F}_4$, $gcd(r_i, \frac{2^m+1}{3}) = 1$, and $f(x)$ be defined by (4). Then*

(1) *If $b = 0$, $f(x)$ is hyper-bent if and only if $K_m(a) + 2K_m(c) = 0$;*
(2) *If $b = 1$, $f(x)$ is hyper-bent if and only if $-K_m(a) + 2K_m(c) = 4$;*
(3) *If b is a primitive 3rd root of unity, $f(x)$ is hyper-bent if and only if $K_m(a) = 4$.*

Example 2 Let $m = 23$, $\mathbb{F}_{2^m} \cong \mathbb{F}_2[x]/(x^{23} + x^5 + 1)$. Take positive integers r_i such that $gcd(r_i, \frac{2^m+1}{3}) = 1 (i = 0, 1)$. Take

$$\begin{aligned} a &= a_0^3 = x^{23} + x^{21} + x^{14} + x^{13} + x^{11} + x^{10} + x^9 + x^4 + x^2 + x + 1, \\ c &= c_0^3 = x^{23} + x^{22} + x^{20} + x^{18} + x^{17} + x^{16} + x^{15} + x^{13} + x^{10} + x^8 + x^7 + x^5 + x^3 + x + 1, \\ b &= 0; \end{aligned}$$

where $a_0 = x^{23} + x^{21} + x^{19} + x^{18} + x^{17} + x^{15} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^7 + x^4 + x^3 + x^2 + x + 1$, $c_0 = x^{23} + x^{20} + x^{19} + x^{17} + x^{15} + x^{12} + x^9 + x^7 + x^6 + x^5 + x^4 + x^3 + 1$. Then $Tr_1^m(a_0) = 0$, $Tr_1^m(c_0) = 0$, and $K_m(a) = 1768$, $K_m(c) = -884$, $K_m(a) + 2K_m(c) = 0$. Hence, $f(x)$ in (4) is a hyper-bent function with 5 trace terms.

From an exhaustive search, when $m = 5, 7, 9$, the number of hyper-bent functions in Result (1) in Corollary 3 are 50, 735 and 5346 respectively, and the number of hyper-bent functions in Result (2) in Corollary 3 are 100, 588 and 5103 respectively.

Take $R = \{r_0, r_1\}$, $a_{r_0,0} = 0$, $a_{r_0,1} = aw$, $a_{r_0,2} = aw^2$, $a_{r_1,0} = c$, $a_{r_1,1} = cw$, $a_{r_1,2} = cw^2$. From Lemma 1 and Theorem 1, we get straightforwardly the following result.

Theorem 5 *Let $a, c \in \mathbb{F}_{2^m}$, $b \in \mathbb{F}_4$, $gcd(r_i, \frac{2^m+1}{3}) = 1$. Let $f(x)$ be defined by*

$$\begin{aligned} f(x) &= Tr_1^n(a(wx^{r_0(2^m-1)+\frac{2^n-1}{3}} + w^2x^{r_0(2^m-1)+2\frac{2^n-1}{3}})) \\ &+ Tr_1^n(c(x^{r_1(2^m-1)} + wx^{r_1(2^m-1)+\frac{2^n-1}{3}} + w^2x^{r_1(2^m-1)+2\frac{2^n-1}{3}})) + Tr_1^2(bx^{\frac{2^n-1}{3}}), \end{aligned} \tag{5}$$

Then

(1) *If $b = 0$, $f(x)$ is hyper-bent if and only if $S_0(a) + S_1((a)_{\{r_0\}}) + S_1((c)_{\{r_1\}}) = 1$;*
(2) *If $b = 1$, $f(x)$ is hyper-bent if and only if $S_0(a) - S_1((a)_{\{r_0\}}) - S_1((c)_{\{r_1\}}) = 1$;*

(3) *If* $b = w$, $f(x)$ *is hyper-bent if and only if* $-S_0(a) - S_1((a)_{\{r_0\}}) + S_1((c)_{\{r_1\}}) = 1$;
(4) *If* $b = w^2$, $f(x)$ *is hyper-bent if and only if* $-S_0(a) + S_1((a)_{\{r_0\}}) - S_1((c)_{\{r_1\}}) = 1$.

From Corollary 1, Lemma 2, Lemma 1, and Theorem 5, this corollary can be obtained straightforwardly.

Corollary 4 *Let* $a, c \in \mathbb{F}_{2^m}$, $Tr_1^m(a^{\frac{1}{3}}) = Tr_1^m(c^{\frac{1}{3}}) = 0$, $b \in \mathbb{F}_4$, $gcd(r_i, \frac{2^m+1}{3}) = 1$, *and* $f(x)$ *be defined by* (5). *Then*

(1) *If* $b = 0$, $f(x)$ *is hyper-bent if and only if* $K_m(a) + 2K_m(c) = 0$;
(2) *If* $b \in \{1, w^2\}$, $f(x)$ *is hyper-bent if and only if* $K_m(c) = 4$;
(3) *If* $b = w$, $f(x)$ *is hyper-bent if and only if* $2K_m(a) - K_m(c) = 4$.

Theorem 6 *Let* $a, c_r \in \mathbb{F}_{2^m}$, $b \in \mathbb{F}_4$ *be a primitive 3rd root of unity, and* $gcd(r, \frac{2^m+1}{3}) = 1$. *Let* $f(x)$ *be defined by*

$$f(x) = Tr_1^n(ax^{r_0(2^m-1)}) + \sum_{r\in R} Tr_1^n(c_r(x^{r(2^m-1)+\frac{2^n-1}{3}} + x^{r(2^m-1)+2\frac{2^n-1}{3}})) + Tr_1^2(bx^{\frac{2^n-1}{3}}).$$

Then $f(x)$ *is hyper-bent if and only if* $K_m(a) = 4$.

Proof Let $r_0 \in R$. From the definition of $a'_{r,i}$, we have that

$$a'_{r_0,0} = a, a'_{r,0} = 0 (r \neq r_0),\ a'_{r,1} = 0, a'_{r,2} = 0 (r \in R).$$

From Lemma 1,

$$\begin{aligned} S_0((a'_{r,0})_{r\in R}) &= S_0((a)_{\{r_0\}}) = S_0(a), \\ S_1((a'_{r,1})_{r\in R}) &= S_1(0) = \frac{2^m+1}{3}, \\ S_2((a'_{r,2})_{r\in R}) &= S_2(0) = \frac{2^m+1}{3}. \end{aligned}$$

Note that $Tr_1^2(w) = Tr_1^2(w^2) = 1$, $Tr_1^2(1) = 0$. The result follows from Theorem 1. □

4.2 Explicit characterization of hyper-bent functions with coefficients in $\mathbb{F}_{2^n}$

From the previous characterization of hyper-bent functions, we recover some well-known results and generalize those results in the case where the coefficients $a_{r,i}$ belong to the whole field $\mathbb{F}_{2^n}$.

Some results on binomial, trinomial and quadrinomial hyper-bent functions for ($p = 2, e = 3$) are given by Li et al. [19]. Let $R = \{r\}$, $a_{r,0} = a + c + d$, $a_{r,1} = a + cw^2 + dw$, and $a_{r,2} = a + cw + dw^2$. From Lemma 1 and Theorem 1, we obtain the following results similar to Theorem 2 in [19].

Theorem 7 *Let* $a, c, d \in \mathbb{F}_{2^m}$, $b \in \mathbb{F}_4$, *and* $gcd(r, \frac{2^m+1}{3}) = 1$. *Let* $f(x)$ *be defined by*

$$\begin{aligned} f(x) &= Tr_1^n((a+c+d)x^{r(2^m-1)}) + Tr_1^n((a+cw^2+dw)x^{r(2^m-1)+\frac{2^n-1}{3}}) \\ &+ Tr_1^n((a+cw+dw^2)x^{r(2^m-1)+2\frac{2^n-1}{3}}) + Tr_1^2(bx^{\frac{2^n-1}{3}}), \end{aligned} \tag{6}$$

Then

(1) *If* $b = 0$, $f(x)$ *is hyper-bent if and only if* $S_0(a) + S_1((c)_{\{r\}}) + S_1((d)_{\{r\}}) = 1$;
(2) *If* $b = 1$, $f(x)$ *is hyper-bent if and only if* $S_0(a) - S_1((c)_{\{r\}}) - S_1((d)_{\{r\}}) = 1$;
(3) *If* $b = w$, $f(x)$ *is hyper-bent if and only if* $-S_0(a) - S_1((c)_{\{r\}}) + S_1((d)_{\{r\}}) = 1$;
(4) *If* $b = w^2$, $f(x)$ *is hyper-bent if and only if* $-S_0(a) + S_1((c)_{\{r\}}) - S_1((d)_{\{r\}}) = 1$.

From Corollary 1, Lemma 2, Lemma 1, and Theorem 7, this corollary can be obtained immediately.

Corollary 5 *Let* $a, c, d \in \mathbb{F}_{2^m}$, $Tr_1^m(a^{\frac{1}{3}}) = Tr_1^m(c^{\frac{1}{3}}) = Tr_1^m(d^{\frac{1}{3}}) = 0$, $b \in \mathbb{F}_4$, $gcd(r, \frac{2^m+1}{3}) = 1$, *and* $f(x)$ *be defined by* (6). *Then*

(1) *If* $b = 0$, $f(x)$ *is hyper-bent if and only if* $K_m(a) + K_m(c) + K_m(d) = 0$;
(2) *If* $b = 1$, $f(x)$ *is hyper-bent if and only if* $-K_m(a) + K_m(c) + K_m(d) = 4$;
(3) *If* $b = w$, $f(x)$ *is hyper-bent if and only if* $K_m(a) + K_m(c) - K_m(d) = 4$;
(4) *If* $b = w^2$, $f(x)$ *is hyper-bent if and only if* $K_m(a) - K_m(c) + K_m(d) = 4$.

Parameters a, c, d considered in the above results are restricted in the subfield $\mathbb{F}_{2^m}$. Actually, this restriction is not necessary. For convenience, we shall provide some explanations for this fact by considering Theorem 7 as an example.

Some notations are given first. Let $A \in \mathbb{F}_{2^n}^*$ with unique polar decomposition $A = \widetilde{A}\xi^{I(A)}$, where $\widetilde{A} \in \mathbb{F}_{2^m}^*$, $0 \le I(A) \le 2^m$, and ξ is a primitive $2^m + 1$-th root of unity. Define $I(0) = 0$ and $\widetilde{0} = 0$. If $a \in \mathbb{F}_{2^m}$, $I(a) = 0$ and $\widetilde{a} = a$. Then we have a general result of Lemma 1.

Lemma 5 *Let* $A \in \mathbb{F}_{2^n}$ *and* $gcd(r, \frac{2^m+1}{3}) = 1$. *Then* $S_i((A)_{\{r\}}) = S_{ri+I(A)}(\widetilde{A}) = S_{(ri+I(A)) \mod 3}(\widetilde{A})$.

Proof We have

$$S_i((A)_{\{r\}}) = \sum_{v \in V} \chi(Tr_1^n(A(\xi^i v)^{r(2^m-1)})) = \sum_{v \in V} \chi(Tr_1^n(A(\xi^{ri} v^r)^{2^m-1})).$$

Since $gcd(r, \frac{2^m+1}{3}) = 1$, $v \mapsto v^r$ is a transform for V. Then

$$S_i((A)_{\{r\}}) = \sum_{v \in V} \chi(Tr_1^n(A(\xi^{ri} v)^{2^m-1})) = \sum_{v \in V} \chi(Tr_1^n(\widetilde{A}\xi^{i(A)}(\xi^{ri} v)^{2^m-1})).$$

Let l be an integer satisfying $(2^m - 1)l \equiv 1 \mod 2^m + 1$. Since $2^m - 1 \equiv 1 \mod 3$, $l \equiv 1 \mod 3$. Then

$$S_i((A)_{\{r\}}) = \sum_{v \in V} \chi(Tr_1^n(\widetilde{A}(\xi^{ri+lI(A)} v)^{2^m-1})) = \sum_{v \in V} \chi(Tr_1^n(\widetilde{A}(\xi^{ri+I(A)} v)^{2^m-1})) = S_{ri+I(A) \mod 3}(\widetilde{A}).$$

Hence, this lemma follows. □

From Lemma 5 and Theorem 1, this theorem can be obtained immediately.

Theorem 8 *[Theorem 2 in* [19]*] Let* $a, c, d \in \mathbb{F}_{2^n}$, $b \in \mathbb{F}_4$, $gcd(r, \frac{2^m+1}{3}) = 1$, *and* $f(x)$ *be defined in* (6). *Then*

(1) *If* $b = 0$, $f(x)$ *is hyper-bent if and only if* $S_{I(a)}(\widetilde{a}) + S_{r+I(c) \bmod 3}(\widetilde{c}) + S_{2r+I(d) \bmod 3}(\widetilde{d}) = 1$;
(2) *If* $b = 1$, $f(x)$ *is hyper-bent if and only if* $S_{I(a)}(\widetilde{a}) - S_{r+I(c) \bmod 3}(\widetilde{c}) - S_{2r+I(d) \bmod 3}(\widetilde{d}) = 1$;
(3) *If* $b = w$, $f(x)$ *is hyper-bent if and only if* $-S_{I(a)}(\widetilde{a}) - S_{r+I(c) \bmod 3}(\widetilde{c}) + S_{2r+I(d) \bmod 3}(\widetilde{d}) = 1$;
(4) *If* $b = w^2$, $f(x)$ *is hyper-bent if and only if* $-S_{I(a)}(\widetilde{a}) + S_{r+I(c) \bmod 3}(\widetilde{c}) - S_{2r+I(d) \bmod 3}(\widetilde{d}) = 1$.

The above theorem is equivalent to Theorem 2 in [19] for the case $p = 2, e = 3$.

Corollary 6 *Let* $A, C \in \mathbb{F}_{2^m}$, $b \in \mathbb{F}_4$, $gcd(r, \frac{2^m+1}{3}) = 1$, $Tr_1^m((A + C)^{1/3}) = 0$, *and* $Tr_1^m((A^2 + AC + C^2)^{1/3}) = 0$. *Let* $f(x)$ *be defined by*

$$f(x) = Tr_1^n(Ax^{r(2^m-1)}) + Tr_1^n(Cx^{r(2^m-1)+\frac{2^n-1}{3}}) + Tr_1^2(bx^{\frac{2^n-1}{3}}). \tag{7}$$

Then

(1) *If* $b = 0$, $f(x)$ *is hyper-bent if and only if* $K_m(A + C) + 2K_m(A^2 + AC + C^2) = 0$;
(2) *If* $b = 1$, $f(x)$ *is hyper-bent if and only if* $-K_m(A + C) + 2K_m(A^2 + AC + C^2) = 4$;
(3) *If* b *is a primitive 3rd root of unity,* $f(x)$ *is hyper-bent if and only if* $K_m(A + C) = 4$.

Proof Take a, c, d as $A + C$, $A + Cw$, $A + Cw^2$ respectively. Note that

$$\widetilde{c}^2 = c^{2^m+1} = A^2 + AC + C^2, \quad \widetilde{d}^2 = d^{2^m+1} = A^2 + AC + C^2.$$

Then $S_{I(a)}(\widetilde{a}) = S_{I(a)}(A+C)$, $S_{r+I(c) \bmod 3}(\widetilde{c}) = S_{r+I(c) \bmod 3}(\widetilde{c}^2) = S_{r+i(c)}(A^2+AC+C^2)$, and $S_{2r+I(d) \bmod 3}(\widetilde{d}) = S_{2r+I(d) \bmod 3}(\widetilde{d}^2) = S_{2r+I(d) \bmod 3}(A^2 + AC + C^2)$. Note that $Tr_1^m((A + C)^{1/3}) = 0$, $Tr_1^m((A^2 + AC + C^2)^{1/3}) = 0$. From Corollary 1 and Lemma 2, we have

$$\begin{aligned} S_{I(a)}(A + C) &= \frac{-K_m(A + C) + 1}{3}, \\ S_{r+I(c) \bmod 3}(A^2 + AC + C^2) &= \frac{-K_m(A^2 + AC + C^2) + 1}{3}, \\ S_{2r+I(d) \bmod 3}(A^2 + AC + C^2) &= \frac{-K_m(A^2 + AC + C^2) + 1}{3}. \end{aligned}$$

Then

$$\begin{aligned} S_{I(a)}(\widetilde{a}) &= \frac{-K_m(A + C) + 1}{3}, \\ S_{r+I(c) \bmod 3}(\widetilde{c}) &= \frac{-K_m(A^2 + AC + C^2) + 1}{3}, \\ S_{2r+I(d) \bmod 3}(\widetilde{d}) &= \frac{-K_m(A^2 + AC + C^2) + 1}{3}, \end{aligned}$$

The result follows from Theorem 8. □

Example 3 Let $m = 23$ and $\mathbb{F}_{2^m} \cong \mathbb{F}_2[x]/(x^{23} + x^5 + 1)$. Take a positive integer r such that $gcd(r, \frac{2^m+1}{3}) = 1$. Take

$$\begin{aligned} A &= x^{23} + x^{20} + x^{17} + x^{16} + x^{15} + x^{14} + x^{12} + x^{11} + x^{10} + x^9 + x^6 + x^4 + x^2 + x + 1, \\ C &= x^{23} + x^{14} + x^{13} + x^7 + x^6 + x^5 + x^3 + x^2 + 1, \ b = 0; \end{aligned}$$

Then $A+C=x^{23}+x^{21}+x^{20}+x^{14}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x+1$, $A^2+AC+C^2=x^{23}+x^{22}+x^{20}+x^{19}+x^{18}+x^{16}+x^{15}+x^8+x^6+x^3+x^2+x+1$ and $Tr_1^m((A+C)^{1/3})=0$, $Tr_1^m((A^2+AC+C^2)^{1/3})=0$, $K_m(A+C)=-4280$, $K_m(A^2+AC+C^2)=2140$, $K_m(A+C)+2K_m(A^2+AC+C^2)=0$. From Result (1) in Corollary 6, $f(x)$ in (7) is a binomial hyper-bent function.

From an exhaustive search, when $m=5,7,9$, the number of hyper-bent functions in Result (1) in Corollary 6 are 40, 728 and 5346 respectively. And the number of hyper-bent functions in Result (2) in Corollary 6 are 100, 546 and 5112 respectively.

From Theorem 8 and Lemma 2, we can completely characterize all the quadrinomial hyper-bent functions in Theorem 8 by Kloosterman sums and cubic sums. The following lemma explains that exponents of x in the trace functions would be very big.

Lemma 6 *Let $r_{m,1}$ be the smallest integer in the cyclotomic coset of 2 modulo 2^m+1 containing $1+\frac{2^m+1}{3}$, and let $r_{m,2}$ be the smallest integer in the cyclotomic coset of 2 modulo 2^m+1 containing $1+2\frac{2^m+1}{3}$, i.e., $r_{m,1}=min_{0\le i\le 2m-1}(1+\frac{2^m+1}{3})\cdot 2^i \mod 2^m+1$, $r_{m,2}=min_{0\le i\le 2m-1}(1+2\frac{2^m+1}{3})\cdot 2^i \mod 2^m+1$. Then $r_{m,1}=\frac{2^{m-2}+1}{3}$ and $r_{m,2}=\frac{2^{m-1}-1}{3}$.*

Proof We first prove $r_{m,1}=\frac{2^{m-2}+1}{3}$.

(i) If $j=0,2,\cdots,m-1$, $3|(2^j-1)$. We have

$$(1+\frac{2^m+1}{3})\cdot 2^j=\frac{2^j-1}{3}(2^m+1)+\frac{2^m+1}{3}+2^j,$$

where $0<\frac{2^m+1}{3}+2^j<2^m+1$. Then

$$(1+\frac{2^m+1}{3})\cdot 2^j \mod (2^m+1)=\frac{2^m+1}{3}+2^j\ge\frac{2^m+1}{3}+1.$$

When $j=0$, the equality on $r_{m,1}$ holds.

(ii) If $j=1,3,\cdots,m-2$, $3|(2^j-2)$. We have

$$(1+\frac{2^m+1}{3})\cdot 2^j=\frac{2^j-2}{3}(2^m+1)+\frac{2(2^m+1)}{3}+2^j,$$

where $0<\frac{2(2^m+1)}{3}+2^j<2^m+1$. Then

$$(1+\frac{2^m+1}{3})\cdot 2^j \mod (2^m+1)=\frac{2(2^m+1)}{3}+2^j\ge\frac{2(2^m+1)}{3}+2$$

When $j=1$, the equality on $r_{m,1}$ holds.

(iii) If $j=m+1,m+3,\cdots,2m-2$, $3|(2^j-1)$. We have

$$(1+\frac{2^m+1}{3})\cdot 2^j=(\frac{2^j-1}{3}+2^{j-m})(2^m+1)+\frac{2^m+1}{3}-2^{j-m},$$

where $0<\frac{2^m+1}{3}-2^{j-m}<2^m+1$. Then

$$(1+\frac{2^m+1}{3})\cdot 2^j \mod (2^m+1)=\frac{2^m+1}{3}-2^{j-m}\ge\frac{2^m+1}{3}-2^{m-2}=\frac{2^{m-2}+1}{3}.$$

When $j = 2m-2$, the equality on $r_{m,1}$ holds.

(iv) If $j = m, m+2, \cdots, 2m-1$, $3|(2^j-2)$. We have

$$(1+\frac{2^m+1}{3})\cdot 2^j = (\frac{2^j-2}{3}+2^{j-m})(2^m+1)+\frac{2(2^m+1)}{3}-2^{j-m},$$

where $0 < \frac{2(2^m+1)}{3} - 2^{j-m} < 2^m+1$. Then

$$(1+\frac{2^m+1}{3})\cdot 2^j \mod (2^m+1) = \frac{2(2^m+1)}{3}-2^{j-m} \geq \frac{2(2^m+1)}{3}-2^{m-1} = \frac{2^{m-1}+2}{3}.$$

When $j = 2m-1$, the equality on $r_{m,1}$ holds.

Hence, $r_{m,1} = \frac{2^{m-2}+2}{3}$. From the similar discussion, $r_{m,2} = \frac{2^{m-1}-1}{3}$. □

Further, we analyze a subclass of functions in Theorem 8 of the form

$$f(x) = Tr_1^n(a_0x^{2^m-1}) + Tr_1^n(a_1x^{(2^m-1)+\frac{2^n-1}{3}}) + Tr_1^n(a_2x^{(2^m-1)+2\frac{2^n-1}{3}}) + Tr_1^2(bx^{\frac{2^n-1}{3}}),$$

where $a_i \in \mathbb{F}_{2^m}$ $(i = 0, 1, 2)$ and $b \in \mathbb{F}_4$. From Lemma 6, $f(x)$ can be transformed into another function

$$f'(x) = Tr_1^n(a_0x^{2^m-1}) + Tr_1^n(a_1'x^{r_{m,1}(2^m-1)}) + Tr_1^n(a_2'x^{r_{m,2}(2^m-1)}) + Tr_1^2(bx^{\frac{2^n-1}{3}}), \quad (8)$$

where $r_{m,1} = \frac{2^{m-2}+1}{3}$ and $r_{m,2} = \frac{2^{m-1}-1}{3}$. If $b = 0$, $f(x)$ in (8) belongs to cases studied by Charpin and Gong [5]. If $b \neq 0$, $f(x)$ is studied by Mesnager [25]. From results in [5] and [25], some exponential sums on $\mathbb{F}_{2^m}$ should be computed to determine the hyper-bent functions in (8). From Lisoněk [20] and Flori, Mesnager [11, 12], to determine the hyper-bentness of $f(x)$ in (8) is equivalent to counting the number of rational points on hyper-elliptic curves of genus $g \in \{\frac{3r_{m,2}+1}{2}, \frac{3r_{m,2}-1}{2}, \frac{r_{m,2}+1}{2}, \frac{r_{m,2}-1}{2}\}$ over $\mathbb{F}_{2^m}$, where $r_{m,2} = \frac{2^{m-1}-1}{3}$. The genus grows exponentially with m, hence algorithms for counting rational points cannot be applied to determine hyper-bentness of $f(x)$ for big m. From Theorem 8, to determine hyper-bentness of $f(x)$, we just need to compute $S_{I(a)}(a)$, $S_{1+I(c) \mod 3}(\widetilde{c})$ and $S_{1+I(d) \mod 3}(\widetilde{d})$, where $a = a_0+a_1+a_2$, $c = a_0+a_1w+a_2w^2$, $d = a_0+a_1w^2+a_2w$. Values of $C_m(a,a)$, $C_m(\widetilde{c},\widetilde{c})$ and $C_m(\widetilde{d},\widetilde{d})$ can be computed by Proposition 6. From Lemma 2, we have just to compute Kloosterman sums $K_m(a)$, $K_m(\widetilde{c})$ and $K_m(\widetilde{d})$ on $\mathbb{F}_{2^m}$. They can be computed by counting algorithms on elliptic curves or hyper-elliptic curves [21], such as Schoof algorithm [30]. Hence, it explains that our techniques can efficiently characterize the hyper-bentness property of some special functions studied by Charpin, Gong [5] and Mesnager [25].

5 Conclusion

This paper generalizes classes of hyper-bent functions proposed by Charpin, Gong [5] and Mesnager [25], and presents a characterization of a more general class of hyper-bent functions. These hyper-bent functions with coefficients in $\mathbb{F}_{2^m}$ are characterized by exponential sums. For many special cases, we give an explicit characterization of the obtained hyper-bent functions by means of Kloosterman sums and cubic sums. For some special cases, we present some attempts to generalize our characterization in the case where the coefficients belong to the whole ambient space $\mathbb{F}_{2^n}$.

Acknowledgments We would like to thank the anonymous reviewers and Prof. Claude Carlet for their helpful comments and suggestions.

This work was supported by the National Natural Science Foundation of China (Grant No. 11401480, No. 11531002, No. 11501154). C. Tang also acknowledges support from 14E013 and CXTD2014-4 of China West Normal University.

Y. Qi aslo acknowledges support from Zhejiang provincial Natural Science Foundation of China (Grant No. LQ17A010008).

References

1. Canteaut, A., Charpin, P., Kyureghyan, G.: A new class of monomial bent functions. Finite Fields Appl **14**(1), 221–241 (2008)
2. Carlet, C.: Boolean Functions for Cryptography and Error Correcting Codes. In: Crama, Y., Hammer, P. (eds.) Chapter of the monography Boolean Models and Methods in Mathematics, Computer Science, and Engineering, pp. 257–397. Cambridge University Press, Cambridge (2010)
3. Carlet, C., Gaborit, P.: Hyper-bent functions and cyclic codes. J. Comb. Theory Ser. A **113**(3), 466–482 (2006)
4. Carlitz, L.: Explicit evaluation of certain exponential sums. Math. Scand. **44**, 5–16 (1979)
5. Charpin, P., Gong, G.: Hyperbent functions, Kloosterman sums and Dickson polynomials. IEEE Trans. Inf. Theory **54**(9), 4230–4238 (2008)
6. Charpin, P., Helleseth, T., Zinoviev, V.: The divisibility modulo 24 of Kloosterman sums of GF(2^m), m odd. J. Comb. Theory, Series A **114**, 322–338 (2007)
7. Charpin, P., Kyureghyan, G.: Cubic monomial bent functions: a subclass of M. SIAM J. Discret. Math. **22**(2), 650–665 (2008)
8. Dillon, J.F.: Elementary Hadamard difference sets. PhD Dissertation, University of Maryland College Park (1974)
9. Dillon, J.F., Dobbertin, H.: New cyclic difference sets with Singer parameters. Finite Fields Appl. **10**(3), 342–389 (2004)
10. Dobbertin, H., Leander, G., Canteaut, A., Carlet, C., Felke, P., Gaborit, P.: Construction of bent functions via Niho power functions. J. Comb. Theory Ser. A **113**, 779–798 (2006)
11. Flori, J.P., Mesnager, S.: An efficient characterization of a family of hyper-bent functions with multiple trace terms. J. Math. Cryptol. **7**(1), 43–68 (2013)
12. Flori, J.P., Mesnager, S.: Dickson polynomials, hyperelliptic curves and hyper-bent functions. In: Proceedings of the 7th International Conference Sequences and Their Applications, SETA 2012, Waterloo. Lecture Notes in Computer Science, vol. 7780, pp. 40–52. Springer, Berlin (2012)
13. Flori, J.P., Mesnager, S., Cohen, G.: The Value 4 of Binary Kloosterman Sums. In: Proceedings of the Thirteenth International Conference on Cryptography and Coding, Oxford, United Kingdom, IMACC 2011. Lecture Notes in Computer Science, vol. 7089, pp. 61–78. Springer, Berlin (2011)
14. Gold, R.: Maximal recursive sequences with 3-valued recursive crosscorrelation functions. IEEE Trans. Inf. Theory **14**(1), 154–156 (1968)
15. Gong, G., Golomb, S.: Transform domain analysis of DES. IEEE Trans. Inf. Theory **45**(6), 2065–2073 (1999)
16. Lachaud, G., Wolfmann, J.: The weights of the orthogonals of the extended quadratic binary Goppa codes. IEEE Trans. Inf. Theory **36**(3), 686–692 (1990)
17. Leander, G.: Monomial bent functions. Proceedings of WCC 2006, pp. 462–470, (2005). And IEEE Trans. Inf. Theory, 52(2), 738–743 (2006)
18. Leander, G., Kholosha, A.: Bent functions with 2^r Niho exponents. IEEE Trans. Inf. Theory **52**, 5529–5532 (2006)
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. Lisoněk, P.: An efficient characterization of a family of hyperbent functions. IEEE Trans. Inf. Theory **57**(9), 6010–6014 (2011)
21. Lisoněk, P.: On the connection between Kloosterman sums and elliptic curves. In: Golomb et al. (ed.) Proceedings of the 5th International Conference on Sequences and Their Applications (SETA 2008), Lecture Notes in Computer Science, vol. 5203, pp. 182–187. Springer (2008)
22. Mesnager, S.: A new class of bent and Hyper-Bent Boolean functions in polynomial forms. Des. Codes Cryptogr. **59**(1-3), 265–279 (2011). see also proceedings of WCC 2009

23. Mesnager, S.: A new family of hyper-bent Boolean functions in polynomial form. In: Mesnager, S. (ed.) Proceedings of Twelfth International Conference on Cryptography and Coding. Cirencester, IMACC 2009, LNCS 5921, pp. 402–417. Springer, Heidelberg (2009)
24. Mesnager, S.: Hyper-bent Boolean functions with multiple trace terms. In: Proceedings of International Workshop on the Arithmetic of Finite Fields (WAIFI 2010). Lecture Notes in Computer Science, vol. 6087, pp. 97–113 (2010)
25. Mesnager, S.: Bent and hyper-bent functions in polynomial form and their link with some exponential sums and Dickson polynomials. IEEE Trans. Inf. Theory **57**(9), 5996–6009 (2011)
26. Mesnager, S.: A new family of hyper-bent Boolean functions in polynomial form. In: Proceedings of Twelfth International Conference on Cryptography and Coding (IMACC 2009). Lecture Notes in Computer Science, vol. 5921, pp. 402–417. Springer, Heidelberg (2009)
27. Mesnager, S., Flori, J.P.: Hyper-bent functions via Dillon-like exponents. IEEE Trans. Inf. Theory **59**(5), 3215–3232 (2013)
28. Lidl, R., Mullen, G.L., Turnwald, G.: Dickson Polynomials (1993)
29. Rothaus, O.S.: On bent functions. J. Comb. Theory Ser. A **20**, 300–305 (1976)
30. Schoof, R.: Counting Points on Elliptic Curves over Finite Fields. J. Theor. Nombres Bordeaux **7**, 219–254 (1995)
31. Tang, C., Li, N., Qi, Y., Zhou, Z., Helleseth, T.: Linear codes with two or three weights from weakly regular bent functions. IEEE Trans. Inf. Theory **62**(3), 1166-1176 (2016)
32. 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/
33. 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)
34. Wang, B., Tang, C., Qi, Y., Yang, Y., Xu, M.: A new class of hyper-bent Boolean functions in binomial forms. CoRR, arXiv:1112.0062
35. Youssef, A.M., Gong, G.: Hyper-bent functions. In: Proceedings of EUROCRYPT 2001. Lecture Notes in Computer Science, vol. 2045, pp. 406–419. Springer, Berlin (2001)
36. Yu, N.Y., Gong, G.: Construction of quadratic bent functions in polynomial forms. IEEE Trans. Inf. Theory **7**(52), 3291–3299 (2006)