A new class of hyper-bent functions and Kloosterman sums

Chunming Tang, Yanfeng Qi

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 $\sum_{r\in R} \mathrm{Tr}_1^n(a_r x^{r(2^m-1)})$ and Mesnager's $\sum_{r\in R} \mathrm{Tr}_1^n(a_r x^{r(2^m-1)}) + \mathrm{Tr}_1^2(bx^{\frac{2^n-1}{3}})$, where R is a set of representations of the cyclotomic cosets modulo 2^m+1 of full size n and $a_r \in \mathbb{F}_{2^m}$. In this paper, we generalize their results and consider 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 $a_{r,i}\in\mathbb{F}_{2^n}$. With the restriction of $a_{r,i}\in\mathbb{F}_{2^m}$, we present the characterization of hyper-bentness of these functions with character sums. Further, we reformulate this characterization in terms of the number of points on hyper-elliptic curves. For some special cases, with the help of Kloosterman sums and cubic sums, we determine the characterization for some hyper-bent functions including functions with four, six and ten traces terms. Evaluations of Kloosterman sums at three general points are used in the characterization. Actually, our results can generalized to the general case: $a_{r,i}\in\mathbb{F}_{2^n}$. And we explain this for characterizing binomial, trinomial and quadrinomial hyper-bent functions.

Index Terms

Bent function, hyper-bent functions, Walsh-Hadamard transform, Dickson polynomial, Kloosterman sums

I. 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 [31] as interesting combinatorial objects have been extensively studied for their applications not only in cryptography, but also in coding theory [3], [26] and combinatorial design. Some basic knowledge and recent results on bent functions can be found in [2], [9], [26]. A bent function can be considered as a Boolean function defined over $\mathbb{F}_2^n$, $\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$ $(n=2m)$ or $\mathbb{F}_{2^n}$. Thanks to the different structures of the vector space $\mathbb{F}_2^n$ and the Galois field $\mathbb{F}_{2^n}$, bent functions can be well studied. Although some algebraic properties of bent functions are well known, the general structure of bent functions on $\mathbb{F}_{2^n}$ is not clear yet. As a result, much research on bent functions on $\mathbb{F}_{2^n}$ can be found in [1], [5], [6], [7], [8], [10], [14], [18], [19], [24], [25], [26], [27], [28], [37]. Youssef and Gong [36] introduced a class of bent functions called hyper-bent functions, which achieve the maximal minimum distance to all the coordinate functions of all bijective monomials (i.e., functions of the form $\mathrm{Tr}_1^n(ax^i)+\epsilon$, $\gcd(i,2^n-1)=1$). However, the definition of hyper-bent functions was given by Gong and Golomb [15] by a property of the extend Hadamard transform of Boolean functions. Hyper-bent functions as special bent functions with strong properties are hard to characterize and many related problems are open. Much research give the precise characterization of hyper-bent functions in certain forms.

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 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 [20] 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 $O(r_{max}^a m^b)$, 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 function are monomial functions via Dillon-like exponent. Leander[18] 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 [26] generalized Charpin and Gong's hyper-bent functions and presented the characterization of hyper-bent functions of the form

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

C. Tang is with School of Mathematics and Information, China West Normal University, Sichuan Nanchong, 637002, China. e-mail: tangchunming-math@163.com

Y. Qi is with LMAM, School of Mathematical Sciences, Peking University, Beijing, 100871, and Aisino corporation Inc., Beijing, 100097, China

where $b \in \mathbb{F}_4$ and $a_r \in \mathbb{F}_{2^m}$. In the case $\#R = 1$, explicit characterization in [25] by Mesnager is presented. With the similar approach, Wang et al. [35] characterized the hyper-bentness of a class of Boolean functions of the form

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

where $b \in \mathbb{F}_{16}$ and $a_r \in \mathbb{F}_{2^m}$. In [33], [34], explicit characterization for the case $\#R = 1$ is given. 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 by Wang et al. Mesnager and Flori [29] 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. [22] considered 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 $e|p^l-1$. From Kloosterman sums, new binomial, trinomial, and quadrinomial bent functions of this type and bent functions with multiple trace terms are characterized.

The coefficients a_r in these above Boolean function are restricted to the subfield $\mathbb{F}_{2^m}$. Since r_{max} grows exponentially with m, the above techniques for characterizing hyper-bent functions are useless for big r_{max}. In this paper, we consider a class of Boolean functions with coefficients in $\mathbb{F}_{2^n}$. Meanwhile, our method applies to determining hyper-bent functions presented by Charpin and Gong, Mesnager for big r_{max}. In our paper, the class of Boolean functions is 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 $a_{r,i} \in \mathbb{F}_{2^n}$. With the help of character sums on $\mathbb{F}_{2^m}$, we first characterize the hyper-bentness of this class of Boolean functions. And we reformulate this characterization in terms of the number of points on hyperelliptic curves. Applying these results, we determine some hyper-bent functions via Dillon-like exponent (including quadrinomial function, functions with six trace terms and ten trace terms) with cubic sums and Kloosterman sums. Further, our techniques 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 backgroud. Section 3 considers a class of Boolean functions and presents the characterization of hyper-bentness of these functions with character sums on $\mathbb{F}_{2^m}$ and the number of rational points on hyper-elliptic curves. Section 4, Some special hyper-bent functions with multiple trace terms are determined from Kloosterman sums and cubic sums. Section 5 gives a conclusion.

II. Preliminaries

A. Boolean functions

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

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

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

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

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

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

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

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

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

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

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

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

When $I = \emptyset$, let $\prod\limits_{i\in I} = 1$. 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

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

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

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

called its polynomial form, where

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

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

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

B. Walsh-Hadamard transform

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

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

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

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

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

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

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

Definition 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.

C. Characterization of bent and hyper-bent functions

[3] and [36] 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 [7], [23].

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 [36] 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 $\{i | f(\xi^i) = 1, 0 \leq i \leq 2^m\}$ is 2^{m-1}.

In fact, Dillon [7] 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 $\mathcal{PS}^-$.

D. Dickson polynomials

Now we recall the knowledge of Dickson polynomials over $\mathbb{F}_2$ [30]. 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

$$\begin{aligned}
&D_1(x) = x,\\
&D_3(x) = x + x^3,\\
&D_5(x) = x + x^3 + x^5,\\
&D_7(x) = x + x^5 + x^7,\\
&D_9(x) = x + x^5 + x^7 + x^9,\\
&D_{11}(x) = x + x^3 + x^5 + x^9 + x^{11}.
\end{aligned}$$

E. Exponential sums and hyper-elliptic curves

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.

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

$$T_i((a_r)_{r\in R})=\sum_{x\in\mathbb{F}_{2^m},Tr_1^m(x^{-1})=i}\chi(Tr_1^m(\sum_{r\in R}a_rD_r(x))). \tag{2}$$

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

$$\Xi((a_r)_{r\in R})=\sum_{x\in\mathbb{F}_{2^m}}\chi(Tr_1^m(\sum_{r\in R}a_rD_r(x))). \tag{4}$$

$$\overline{\Xi}((a_r)_{r\in R})=\sum_{x\in\mathbb{F}_{2^m}}\chi(Tr_1^m(\frac{1}{x}+\sum_{r\in R}a_rD_r(x))). \tag{5}$$

$$\Xi^3((a_r)_{r\in R})=\sum_{x\in\mathbb{F}_{2^m}}\chi(Tr_1^m(\sum_{r\in R}a_rD_r(D_3(x)))). \tag{6}$$

$$\overline{\Xi}^3((a_r)_{r\in R})=\sum_{x\in\mathbb{F}_{2^m}}\chi(Tr_1^m(\frac{1}{x}+\sum_{r\in R}a_rD_r(D_3(x)))). \tag{7}$$

Obviously, 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.

Proposition 2.5: (1)

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

(2)

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

The exponential sums $\Xi((a_r)_{r\in R}),\overline{\Xi}((a_r)_{r\in R}),\Xi^3((a_r)_{r\in R}),\overline{\Xi}^3((a_r)_{r\in R})$ are related to the number of rational points of hyper-elliptic curves.

Theorem 2.6: Let $a_r\in\mathbb{F}_{2^m}$. Define the following hyper-elliptic curves over $\mathbb{F}_{2^m}$:

$$G_{(a_r)_{r\in R}}: y^2+y=\sum_{r\in R}a_rD_r(x), \tag{8}$$

$$H_{(a_r)_{r\in R}}: y^2+xy=x+x^2\sum_{r\in R}a_rD_r(x), \tag{9}$$

$$G^3_{(a_r)_{r\in R}}: y^2+y=\sum_{r\in R}a_rD_r(D_3(x)), \tag{10}$$

$$H^3_{(a_r)_{r\in R}}: y^2+xy=x+x^2\sum_{r\in R}a_rD_r(D_3(x)). \tag{11}$$

Then

$$\begin{aligned}\Xi((a_r)_{r\in R}) &= \#G_{(a_r)_{r\in R}} - 2^m, \quad \Xi^3((a_r)_{r\in R}) = \#G^3_{(a_r)_{r\in R}} - 2^m,\\ \overline{\Xi}((a_r)_{r\in R}) &= \#H_{(a_r)_{r\in R}} - 2^m + 1, \quad \overline{\Xi}^3((a_r)_{r\in R}) = \#H^3_{(a_r)_{r\in R}} - 2^m + 1.\end{aligned}$$

Let $r_{max} = \max R$. Then the defined hyper-elliptic curves $G_{(a_r)_{r\in R}}$, $H_{(a_r)_{r\in R}}$, $G^3_{(a_r)_{r\in R}}$ and $H^3_{(a_r)_{r\in R}}$ are Artin-Schreier curves of genus $\frac{r_{max}-1}{2}$, $\frac{r_{max}+1}{2}$, $\frac{3r_{max}-1}{2}$ and $\frac{3r_{max}+1}{2}$ respectively. For small m and r_{max}, the number of rational points on these hyper-elliptic curves can be efficiently computed.

Theorem 2.7: Let C be an Artin-Schreier curve of genus g defined over $\mathbb{F}_{2^m}$. Then there exists an algorithm to compute $\#C$ in

$$O(g^3m^3(g^2 + \log^2 m \log\log m)\log gm \log\log gm)$$

bit operations and $O(g^3m^3)$ memory.

F. Kloosterman sums and subic sums

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

Definition The binary Kloosterman sums associated with a are

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

Properties of Kloosterman sums are given in the following propositions.

Proposition 2.8: 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.

Proposition 2.9: Let $m \geq 3$ be an odd integer and $a \in \mathbb{F}_{2^m}$. Then

$$K_m(a) \equiv 1 \mod 3, \Longleftrightarrow Tr_1^m(a^{1/3}) = 0.$$

The relationship between Kloosterman sums and the number of rational points on elliptic curves are given below [16], [17].

Theorem 2.10: Let $m \geq 3$ be a positive odd integer, $a \in \mathbb{F}^*_{2^m}$ and E_a be an elliptic curve over $\mathbb{F}_{2^m}$ of affine equation

$$y^2 + xy = x^3 + a.$$

Then

$$K_m(a) = \#E_a - 2^m.$$

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

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

Carlitz [4] computed the exact values of the cubic sums by means of the Jacobi symbol.

Proposition 2.11: 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 $c = \gamma^4+\gamma+1$,$\gamma \in \mathbb{F}_{2^m}$.

Corollary 2.12: 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)$Tr_1^m(a^{\frac{1}{3}}) = 0$.

Proof: From Proposition 2.9, Result (1) and Result (3) are equivalent. Note that

$$\begin{aligned}C_m(a,a) &= \sum_{x\in\mathbb{F}_{2^m}} (-1)^{Tr_1^m(ax^3+ax)}\\ &= \sum_{x\in\mathbb{F}_{2^m}} (-1)^{Tr_1^m((a^{\frac{1}{3}}x)^3 + a^{\frac{2}{3}}(a^{\frac{1}{3}}x))}\\ &= \sum_{x\in\mathbb{F}_{2^m}} (-1)^{Tr_1^m(x^3+a^{\frac{2}{3}}x)}\end{aligned}$$

and $Tr_1^m(a^{\frac{2}{3}}) = Tr_1^m(a^{\frac{1}{3}})$. From Proposition 2.11, Result (2) and Result (3) are equivalent. Hence, the corollary holds. ■

III. A CLASS OF HYPER-BENT FUNCTIONS WITH MULTIPLE TRACE TERMS

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

$$f_{a,b}(x)=\sum_{r\in R}\sum_{i=0}^{2}Tr_1^n(a_{r,i}x^{r(2^m-1)+\frac{2^n-1}{3}i})+Tr_1^2(bx^{\frac{2^n-1}{3}}), \tag{12}$$

where $n=2m$, m is odd, $a_{r,i}\in\mathbb{F}_{2^n}$ and $b\in\mathbb{F}_4$.

Theorem 3.1: Let $f_{a,b}$ be a Boolean function defined in (12). Let $a'_{r,i}$ be defined by

$$\begin{pmatrix} a'_{r,0}\\ a'_{r,1}\\ a'_{r,2}\end{pmatrix}=\begin{bmatrix}1&1&1\\1&w&w^2\\1&w^2&w\end{bmatrix}\begin{pmatrix}a_{r,0}\\ a_{r,1}\\ a_{r,2}\end{pmatrix}. \tag{13}$$

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

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

where $S_i((.)_{r\in R})$ is defined in (1). If $a'_{r,2}\in\mathbb{F}_{2^m}$, then

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

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

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

From Proposition 2.3, $f_{a,b}(x)$ is hyper-bent if and only if $\Lambda(f_{a,b})=1$. Since $U=V\cup\xi V\cup\xi^2V$,

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

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

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

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

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

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

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

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

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

Hence, this theorem 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 character sums on $\mathbb{F}_{2^m}$ or the number of rational points on hyper-elliptic curves. For the computation, some lemmas are given first.

Lemma 3.2: 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)$S_1((a_r)_{r\in R}) = \frac{1}{3}[-\Xi^3((a_r)_{r\in R}) + 2\Xi((a_r)_{r\in R}) - \overline{\Xi}((a_r)_{r\in R}) + 1]$.

Proof: From Proposition 2.5, this lemma is obviously obtained. ■

Lemma 3.3: Let $a_r \in \mathbb{F}_{2^m}$, then (1)$S_0((a_r)_{r\in R}) = \frac{1}{3}[2\#G^3_{(a_r)_{r\in R}} - \#H_{(a_r)_{r\in R}} - \#G_{(a_r)_{r\in R}}]$; (2)$S_1((a_r)_{r\in R}) = \frac{1}{3}[-\#G^3_{(a_r)_{r\in R}} - \#H_{(a_r)_{r\in R}} + 2\#G_{(a_r)_{r\in R}}]$.

Proof: From Lemma 3.2 and Theorem 2.6, this lemma is obviously obtained. ■

From character sums on $\mathbb{F}_{2^m}$, the following proposition can compute $\Lambda(f_{a,b})$.

Proposition 3.4: Let $a'_{r,i} \in \mathbb{F}_{2^m}$, then

(1) If $b = 0$,

$$\begin{aligned}\Lambda(f_{a,b}) = & \frac{1}{3}[2\Xi^3((a'_{r,0})_{r\in R}) - \Xi((a'_{r,0})_{r\in R}) - \overline{\Xi}((a'_{r,0})_{r\in R})] \\ & + \frac{1}{3}[-\Xi^3((a'_{r,1})_{r\in R}) + 2\Xi((a'_{r,1})_{r\in R}) - \overline{\Xi}((a'_{r,1})_{r\in R})] \\ & + \frac{1}{3}[-\Xi^3((a'_{r,2})_{r\in R}) + 2\Xi((a'_{r,2})_{r\in R}) - \overline{\Xi}((a'_{r,2})_{r\in R})] + 1.\end{aligned}$$

(2) If $b = 1$,

$$\begin{aligned}\Lambda(f_{a,b}) = & \frac{1}{3}[2\Xi^3((a'_{r,0})_{r\in R}) - \Xi((a'_{r,0})_{r\in R}) - \overline{\Xi}((a'_{r,0})_{r\in R})] \\ & - \frac{1}{3}[-\Xi^3((a'_{r,1})_{r\in R}) + 2\Xi((a'_{r,1})_{r\in R}) - \overline{\Xi}((a'_{r,1})_{r\in R})] \\ & - \frac{1}{3}[-\Xi^3((a'_{r,2})_{r\in R}) + 2\Xi((a'_{r,2})_{r\in R}) - \overline{\Xi}((a'_{r,2})_{r\in R})] - \frac{1}{3}.\end{aligned}$$

(3) If $b = w$,

$$\begin{aligned}\Lambda(f_{a,b}) = & -\frac{1}{3}[2\Xi^3((a'_{r,0})_{r\in R}) - \Xi((a'_{r,0})_{r\in R}) - \overline{\Xi}((a'_{r,0})_{r\in R})] \\ & - \frac{1}{3}[-\Xi^3((a'_{r,1})_{r\in R}) + 2\Xi((a'_{r,1})_{r\in R}) - \overline{\Xi}((a'_{r,1})_{r\in R})] \\ & + \frac{1}{3}[-\Xi^3((a'_{r,2})_{r\in R}) + 2\Xi((a'_{r,2})_{r\in R}) - \overline{\Xi}((a'_{r,2})_{r\in R})] - \frac{1}{3}.\end{aligned}$$

(4) If $b = w^2$,

$$\begin{aligned}\Lambda(f_{a,b}) = & -\frac{1}{3}[2\Xi^3((a'_{r,0})_{r\in R}) - \Xi((a'_{r,0})_{r\in R}) - \overline{\Xi}((a'_{r,0})_{r\in R})] \\ & + \frac{1}{3}[-\Xi^3((a'_{r,1})_{r\in R}) + 2\Xi((a'_{r,1})_{r\in R}) - \overline{\Xi}((a'_{r,1})_{r\in R})] \\ & - \frac{1}{3}[-\Xi^3((a'_{r,2})_{r\in R}) + 2\Xi((a'_{r,2})_{r\in R}) - \overline{\Xi}((a'_{r,2})_{r\in R})] - \frac{1}{3}.\end{aligned}$$

Proof: Note $\chi(Tr_1^2(0)) = \chi(Tr_1^2(1)) = 1$ and $\chi(Tr_1^2(w)) = \chi(Tr_1^2(w^2)) = -1$. From Theorem 3.1 and Lemma 3.2, this proposition can be obviously obtained. ■

From the number of rational points on hyper-elliptic curves, the following theorem can determine the hyper-bentness for $f_{a,b}$.

Theorem 3.5: Let $a'_{r,i} \in \mathbb{F}_{2^m}$, Then

(1) If $b = 0$,

$$\begin{aligned}\Lambda(f_{a,b}) = & \frac{1}{3}[2\#G^3_{(a'_{r,0})_{r\in R}} - \#H_{(a'_{r,0})_{r\in R}} - \#G_{(a'_{r,0})_{r\in R}}] \\ & + \frac{1}{3}[-\#G^3_{(a'_{r,1})_{r\in R}} - \#H_{(a'_{r,1})_{r\in R}} + 2\#G_{(a'_{r,1})_{r\in R}}] \\ & + \frac{1}{3}[-\#G^3_{(a'_{r,2})_{r\in R}} - \#H_{(a'_{r,2})_{r\in R}} + 2\#G_{(a'_{r,2})_{r\in R}}].\end{aligned}$$

(2) If $b = 1$,

$$\begin{aligned}\Lambda(f_{a,b}) = \quad & \frac{1}{3}[2\#G^3_{(a'_{r,0})_{r\in R}} - \#H_{(a'_{r,0})_{r\in R}} - \#G_{(a'_{r,0})_{r\in R}}] \\ & - \frac{1}{3}[-\#G^3_{(a'_{r,1})_{r\in R}} - \#H_{(a'_{r,1})_{r\in R}} + 2\#G_{(a'_{r,1})_{r\in R}}] \\ & - \frac{1}{3}[-\#G^3_{(a'_{r,2})_{r\in R}} - \#H_{(a'_{r,2})_{r\in R}} + 2\#G_{(a'_{r,2})_{r\in R}}].\end{aligned}$$

(3) If $b = w$,

$$\begin{aligned}\Lambda(f_{a,b}) = & -\frac{1}{3}[2\#G^3_{(a'_{r,0})_{r\in R}} - \#H_{(a'_{r,0})_{r\in R}} - \#G_{(a'_{r,0})_{r\in R}}] \\ & - \frac{1}{3}[-\#G^3_{(a'_{r,1})_{r\in R}} - \#H_{(a'_{r,1})_{r\in R}} + 2\#G_{(a'_{r,1})_{r\in R}}] \\ & + \frac{1}{3}[-\#G^3_{(a'_{r,2})_{r\in R}} - \#H_{(a'_{r,2})_{r\in R}} + 2\#G_{(a'_{r,2})_{r\in R}}].\end{aligned}$$

(4) If $b = w^2$,

$$\begin{aligned}\Lambda(f_{a,b}) = & -\frac{1}{3}[2\#G^3_{(a'_{r,0})_{r\in R}} - \#H_{(a'_{r,0})_{r\in R}} - \#G_{(a'_{r,0})_{r\in R}}] \\ & + \frac{1}{3}[-\#G^3_{(a'_{r,1})_{r\in R}} - \#H_{(a'_{r,1})_{r\in R}} + 2\#G_{(a'_{r,1})_{r\in R}}] \\ & - \frac{1}{3}[-\#G^3_{(a'_{r,2})_{r\in R}} - \#H_{(a'_{r,2})_{r\in R}} + 2\#G_{(a'_{r,2})_{r\in R}}].\end{aligned}$$

Proof: From Theorem 3.1 and Lemma 3.3, this theorem can be obviously obtained. ■

From the above theorem, to determine the hyper-bentness for $f_{a,b}$, we just compute the number of rational points for 9 hyper-elliptic curves, which include three hyper-elliptic curves of genus $\frac{3r_{max}-1}{2}$, three hyper-elliptic curves of genus $\frac{r_{max}+1}{2}$ and three hyper-elliptic curves of genus $\frac{r_{max}-1}{2}$ ($r_{max} = \max R$). From Theorem 7, for not big r_{max}, many techniques for counting the number of rational points on hyper-elliptic curves can be used in the computation. From some special cases of $f_{a,b}$ with coefficients satisfying some relations, we have the following corollary for hyper-bentness characterization.

Corollary 3.6: Let $a_{r,0} \in \mathbb{F}_{2^m}$, $a_{r,1} = a_{r,2} \in \mathbb{F}_{2^m}$ and $b \in \mathbb{F}_4 \backslash \mathbb{F}_2$, then $f_{a,b}$ is hyper-bent if and only if $S_0((a_{r,0})_{r\in R}) = -1$, i.e.,

$$2\#G^3_{(a_{r,0})_{r\in R}} - \#H_{(a_{r,0})_{r\in R}} - \#G_{(a_{r,0})_{r\in R}} = -3.$$

Proof: From $a_{r,1} = a_{r,2}$, we have

$$\begin{aligned}a'_{r,0} =& a_{r,0} + a_{r,1} + a_{r,2} = a_{r,0} \in \mathbb{F}_{2^m}, \\ a'_{r,1} =& a_{r,0} + a_{r,1}w + a_{r,2}w^2 = a_{r,0} + a_{r,1} \in \mathbb{F}_{2^m}, \\ a'_{r,2} =& a_{r,0} + a_{r,1}w^2 + a_{r,2}w = a_{r,0} + a_{r,1} \in \mathbb{F}_{2^m},\end{aligned}$$

For any $r \in R$, we have $a'_{r,} = a'_{r,2}$. Obviously, $S_1((a'_{r,})_{r\in R}) = S_1((a'_{r,2})_{r\in R})$. From Theorem 3.1, we have $\Lambda(f_{a,b}) = -S_0((a_{r,0})_{r\in R})$. Then $f_{a,b}$ is hyper-bent if and only if $S_0((a_{r,0})_{r\in R}) = -1$. From Lemma 3.3, we have

$$2\#G^3_{(a_{r,0})_{r\in R}} - \#H_{(a_{r,0})_{r\in R}} - \#G_{(a_{r,0})_{r\in R}} = -3.$$

Hence, this corollary follows. ■

IV. Hyper-bent functions and Kloosterman sums

In this section, we present the hyper-bentness of some special functions with Kloosterman sums or linear combination of Kloosterman sums. When $\#R = 1$, we write $(a)_R$ for $(a)_{r\in R}$ and a for $(a)_{\{1\}}$.

Lemma 4.1: 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 $3 \mid r$, $S_1((a)_{\{r\}}) = S_0(a)$.

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

$$\begin{aligned}S_0((a)_{\{r\}}) =& \sum_{v\in V} \chi(Tr_1^n(av^{r(2^m-1)})) \\ =& \sum_{v\in V} \chi(Tr_1^n(av^{2^m-1})) \\ =& S_0(a)\end{aligned}$$

(2) Since $gcd(r, \frac{2^m+1}{3}) = 1$,

$$\begin{aligned} S_1((a)_{\{r\}}) &= \sum_{v\in V} \chi(Tr_1^n(a(\xi v)^{r(2^m-1)})) \\ &= \sum_{v\in V} \chi(Tr_1^n(a(\xi^r v^r)^{2^m-1})) \\ &= \sum_{v\in V} \chi(Tr_1^n(a(\xi^r v)^{2^m-1})) \end{aligned}$$

If $3 \nmid r$, $r \equiv 1 \text{ or } 2 \mod 3$. Then

$$S_1((a)_{\{r\}}) = S_1(a) \text{ or } S_2(a).$$

From Result (1) in Proposition 2.5, $S_1(a) = S_2(a)$. Then we have

$$S_1((a)_{\{r\}}) = S_1(a).$$

If $3 \mid r$, $\xi^r \in V$. Then

$$S_1((a)_{\{r\}}) = S_0(a).$$

■

Actually, $S_0(a)$ and $S_1(a)$ can be expressed by cubic sums and Kloosterman sums [25].

Lemma 4.2: 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 $S_i(a) = S_i(a^2)$.

A. Hyper-bent functions with nine or ten trace terms

Theorem 4.3: 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

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

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 $b = 1$, $f(x)$ 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 $R = \{r_0, r_1, r_2\}$. From the definition of $a'_{r,i}$ in (13),

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

From Lemma 4.1, we have

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

From $Tr_1^2(w) = Tr_1^2(w^2) = 1, Tr_1^2(1) = 0$ and Theorem 3.1, this theorem can be obviously obtained. ■

Corollary 4.4: Let $gcd(r_i, \frac{2^m+1}{3}) = 1 (i = 1, 2)$, $a, c, d \in \mathbb{F}_{2^m}$, $Tr_1^m(a^{\frac{1}{3}}) = Tr_1^m(c^{\frac{1}{3}}) = Tr_1^m(d^{\frac{1}{3}}) = 0$, and w be a primitive 3rd root of unity. Let $f(x)$ be defined by

$$\begin{aligned} f(x) = \quad & Tr_1^n(a(x^{r_0(2^m-1)} + x^{r_0(2^m-1)+\frac{2^n-1}{3}} + x^{r_0(2^m-1)+2\frac{2^n-1}{3}})) \\ & + Tr_1^n(c(x^{r_1(2^m-1)} + w^2 x^{r_1(2^m-1)+\frac{2^n-1}{3}} + w x^{r_1(2^m-1)+2\frac{2^n-1}{3}})) \\ & + Tr_1^n(d(x^{r_2(2^m-1)} + w x^{r_2(2^m-1)+\frac{2^n-1}{3}} + w^2 x^{r_2(2^m-1)+2\frac{2^n-1}{3}})) \\ & + Tr_1^2(bx^{\frac{2^n-1}{3}}). \end{aligned} \tag{14}$$

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: If $Tr_1^m(a^{\frac{1}{3}})=Tr_1^m(c^{\frac{1}{3}})=Tr_1^m(d^{\frac{1}{3}})=0$, from Corollary 2.12 we have

$$C_m(a,a)=C_m(c,c)=C_m(d,d)=0,$$

From Lemma 4.2,

$$\begin{aligned} S_0(a)=S_1(a)&=\frac{1}{3}(-K_m(a)+1),\\ S_0(c)=S_1(c)&=\frac{1}{3}(-K_m(c)+1),\\ S_0(d)=S_1(d)&=\frac{1}{3}(-K_m(d)+1). \end{aligned}$$

From Lemma 4.1 and Theorem 4.3, this corollary can be obviously obtained. ■

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

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

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 (14) is a hyper-bent functions with 9 trace terms.

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

$$\begin{aligned} a=a_0^3&=x^{23}+x^{20}+x^{18}+x^{15}+x^{14}+x^{12}+x^{10}+x^4+1,\\ c=c_0^3&=x^{23}+x^{20}+x^{19}+x^{17}+x^{15}+x^{14}+x^{11}+x^{10}+x^9+x^6+x^3+x^2+1,\\ d=d_0^3&=x^{23}+x^{22}+x^{21}+x^{18}+x^{17}+x^{16}+x^{14}+x^{13}+x^{12}+x^{11}+x^9+x^8+x^7+x^5+x^4+x^3+1,\\ b&=1; \end{aligned}$$

where $a_0=x^{23}+x^{21}+x^{19}+x^{15}+x^{14}+x^{12}+x^{11}+x^{10}+x^8+x^7+1$, $c_0=x^{23}+x^{15}+x^{14}+x^{13}+x^{11}+x^9+x^6+x^5+x^3+x+1$, $d_0=x^{23}+x^{20}+x^{19}+x^{18}+x^{16}+x^{12}+x^{11}+x^9+x^8+x^4+1$. Then $Tr_1^m(a_0)=0$, $Tr_1^m(c_0)=0$, $Tr_1^m(d_0)=0$, and $K_m(a)=64$, $K_m(c)=1264$, $K_m(d)=-1196$, $-K_m(a)+K_m(c)+K_m(d)=4$. Hence, $f(x)$ in (14) is a hyper-bent functions with 10 trace terms.

Many hyper-bent functions of the form (14) exists. From exhaustive search by computer, when $m=5,7$, numbers of the hyper-bent functions in Result (1) in Corollary 4.4 are 1500 and 58653 respectively, and numbers of the hyper-bent functions in Result (2) in Corollary 4.4 are 1500 and 57624 respectively.

Lemma 4.5: 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) $S_0(a)-2S_1(a)=1$.

Proof: From Lemma 4.2, we have

$$-S_0(a)=\frac{1}{3}(K_m(a)-2C_m(a,a)-1) \tag{15}$$

If Condition (1) holds, from Corollary 2.12 we have $C_m(a,a)=0$ and $-S_0(a)=1$. If Condition (2) holds, we have $K_m(a)=2C_m(a,a)+4$. From Proposition 2.11, $C_m(a)\in\{0,\pm 2^{\frac{m+1}{2}}\}$, $K_m(a)\in\{4,4\pm 2\cdot 2^{\frac{m+1}{2}}\}$. Note that when $m\geq 5$,

$$4+2\cdot 2^{\frac{m+1}{2}}>2^{\frac{m+2}{2}}+1, 4-2\cdot 2^{\frac{m+1}{2}}<-2^{\frac{m+2}{2}}+1.$$

From Proposition 2.8, we have $K_m(a)=4$. Hence, Condition (1) and Condition (2) are equivalent.

Note that

$$-2S_0(a)+S_1(a)=\frac{1}{3}(K_m(a)-5C_m(a,a)-1),$$
$$S_0(a)-2S_1(a)=\frac{1}{3}(K_m(a)+4C_m(a,a)-1).$$

Similarly, Condition (1) and Condition (3) are equivalent, and Condition (1) and Condition (4) are equivalent. Hence, this lemma follows. ■

Theorem 4.6: 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

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

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) $b=w$, $3\nmid r_1$, $3\mid r_2$;

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 $K_m(a)=4$.

Proof: (1) From Result (2) in Lemma 4.1, we have

$$S_0(a)+S_1((c)_{\{r_1\}})+S_1((d)_{\{r_2\}})=3S_0(a).$$

Obviously, $3S_0(a)\neq 1$. Hence, from Result (1) in Theorem 4.3, $f(x)$ is not hyper-bent.

(2) From Result (2) in Lemma 4.1(2), we have

$$S_0(a)+S_1((c)_{\{r_1\}})+S_1((d)_{\{r_2\}})=S_0(a)-2S_1(a).$$

From Lemma 4.5, $S_0(a)-2S_1(a)=1$ if and only if $K_m(a)=4$. From Result (1) in Theorem 4.3, $f(x)$ is hyper-bent if and only if $K_m(a)=4$.

(3) From Result (2) in Lemma 4.1, we have

$$\begin{aligned}S_0(a)+S_1((c)_{\{r_1\}})+S_1((d)_{\{r_2\}}) =&2S_0(a)+S_1(a),\\ =&-K_m(a)+C_m(a,a)+1(from\ Lemma 4.2).\end{aligned}$$

Hence, from Result (1) in Theorem 4.3, $f(x)$ is hyper-bent if and only if $K_m(a)=C_m(a,a)$.

(4) From Theorem 3.1 and Theorem 4.3, for all the three cases, we have

$$\Lambda(f)=-S_1(a)=\frac{1}{3}(K_m(a)+C_m(a,a)-1)(from\ Lemma 4.2).$$

Hence, from Theorem 3.1, $f(x)$ is hyper-bent if and only if $K_m(a)=-C_m(a,a)+4$.

(5) The rest cases except cases in (1), (2), (3) and (4) are 8 cases. For cases:
1) $b=1,3|r_i,i=1,2$ 2) $b=w,3|r_i,i=1,2$
3) $b=w,\#\{r_i:r_i\equiv 0 \mod 3,i=1,2\}=1$ 4) $b=w^2,3|r_i,i=1,2$
5) $b=w^2,\#\{r_i:r_i\equiv 0 \mod 3,i=1,2\}=1$. From Theorem 4.3 and Lemma 4.1, we have

$$\Lambda(f)=-S_0(a).$$

From Theorem 3.1 and Lemma 4.5, Result (5) holds.

For cases: 6) $b=w$,$3\mid r_1$,$3\nmid r_2$ 7) $b=w^2$,$3\nmid r_1$,$3\mid r_2$
we have

$$\Lambda(f)=-2S_0(a)+S_1(a).$$

From Theorem 3.1 and Lemma 4.5, Result (5) holds.

For the last case: $8)b = 1, 3 \nmid r_i$ $(i = 1, 2)$, we have

$$\Lambda(f) = S_0(a) - 2S_1(a).$$

From Theorem 3.1 and Lemma 4.5, Result (5) holds.

Hence, this theorem follows. ■

Remark 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], [7], [18] or binomial hyper-bent function by Mesnager [25], [28]. 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 2.12, 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.

B. Hyper-bent functions with 5 or 6 trace terms

Theorem 4.7: 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

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

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 $S_0(a) = -1$.

Proof: Let $R = \{r_0, r_1\}$. From the definition of $a'_{r,i}$, we have

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

From Lemma 4.1, we have

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

Note that $Tr_1^2(w) = Tr_1^2(w^2) = 1, Tr_1^2(1) = 0$. From Theorem 3.1, this theorem can be obviously obtained. ■

Corollary 4.8: Let $a, c \in \mathbb{F}_{2^m}$, $Tr_1^m(a^{\frac{1}{3}}) = Tr_1^m(c^{\frac{1}{3}}) = 0$, $b \in \mathbb{F}_4$, and $gcd(r_i, \frac{2^m+1}{3}) = 1$. Let $f(x)$ be defined by

$$\begin{aligned} f(x) = \quad & Tr_1^n(a(x^{r_0(2^m-1)} + x^{r_0(2^m-1)+\frac{2^n-1}{3}} + x^{r_0(2^m-1)+2\frac{2^n-1}{3}})) \\ & + Tr_1^n(c(x^{r_1(2^m-1)+\frac{2^n-1}{3}} + x^{r_1(2^m-1)+2\frac{2^n-1}{3}})) + Tr_1^2(bx^{\frac{2^n-1}{3}}), \end{aligned} \tag{16}$$

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 $K_m(a) = 4$.

Proof: When $Tr_1^m(a^{\frac{1}{3}}) = Tr_1^m(c^{\frac{1}{3}}) = 0$, from Corollary 2.12, we have

$$C_m(a, a) = C_m(c, c) = 0.$$

From Lemma 4.2, we have

$$\begin{aligned} S_0(a) = S_1(a) = \frac{1}{3}(-K_m(a) + 1), \\ S_0(c) = S_1(c) = \frac{1}{3}(-K_m(c) + 1). \end{aligned}$$

From Lemma 4.1 and Theorem 4.7, this corollary can be obviously obtained. ■

Example 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 (16) is a hyper-bent function with 5 trace terms.

Example 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

$$\begin{aligned}
&a = a_0^3 = x^{23}+x^{22}+x^{21}+x^{20}+x^{15}+x^{14}+x^9+x^8+x^7+x^5+x^3+x^2+1,\\
&c = c_0^3 = x^{23}+x^{22}+x^{21}+x^{19}+x^{17}+x^{14}+x^{13}+x^{12}+x^9+x^8+x^6+x^4+x^3+x^2+1,\\
&b = 1;
\end{aligned}$$

where $a_0 = x^{23}+x^{21}+x^{20}+x^{19}+x^{18}+x^{16}+x^{12}+x^{11}+x^{10}+x^9+x^6+x^5+x^2+x+1$, $c_0 = x^{23}+x^{20}+x^{19}+x^{15}+x^{14}+x^{12}+x^{11}+x^8+x^2+x+1$. Then $Tr_1^m(a_0)=0$, $Tr_1^m(c_0)=0$, and $K_m(a)=-764$, $K_m(c)=-380$, $-K_m(a)+2K_m(c)=4$. Hence, $f(x)$ in (16) is a hyper-bent function in 6 trace terms.

With exhaustive search by the computer, when $m=5,7,9$, numbers of hyper-bent functions in Result (1) in Corollary 4.8 are 50, 735 and 5346 respectively, and numbers of hyper-bent functions in Result (2) in Corollary 4.8 are 100, 588 and 5103 respectively.

Theorem 4.9: 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

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

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 $b=w$, $f(x)$ 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 $-S_0(a)+S_1((a)_{\{r_0\}})-S_1((c)_{\{r_1\}})=1$.

Proof: Let $R=\{r_0,r_1\}$. From the definition of $a'_{r,i}$, we have

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

From Lemma 4.1,

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

Note that $Tr_1^2(w)=Tr_1^2(w^2)=1, Tr_1^2(1)=0$. From Theorem 3.1, this theorem can be obviously obtained. ■

Corollary 4.10: Let $a, c \in \mathbb{F}_{2^m}$, $Tr_1^m(a^{\frac{1}{3}}) = Tr_1^m(c^{\frac{1}{3}}) = 0$, $b\in\mathbb{F}_4$, and $gcd(r_i, \frac{2^m+1}{3}) = 1$. Let $f(x)$ be defined by

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

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 $2K_m(a)-K_m(c)=4$.

Proof: When $Tr_1^m(a^{\frac{1}{3}}) = Tr_1^m(c^{\frac{1}{3}}) = 0$, from Corollary 2.12, we have

$$C_m(a,a) = C_m(c,c) = 0.$$

From Lemma 4.2,

$$\begin{aligned}
&S_0(a) = S_1(a) = \frac{1}{3}(-K_m(a)+1),\\
&S_0(c) = S_1(c) = \frac{1}{3}(-K_m(c)+1),
\end{aligned}$$

From Lemma 4.1 and Theorem 4.9, this corollary can be obviously obtained. ■

C. Hyper-bent functions with multiple trace terms

Theorem 4.11: 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

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

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

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

From Lemma 4.1,

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

Note that $Tr_1^2(w) = Tr_1^2(w^2) = 1, Tr_1^2(1) = 0$. From Theorem 3.1, this theorem can be obviously obtained. ■

D. Binomial, trinomial and quadrinomial hyper-bent functions

Some results on binomial, trinomial and quadrinomial hyper-bent functions for ($p = 2, e = 3$) are given by Li et al. [22]. From our techniques, we will present some results, which includes results in [22].

Theorem 4.12: [Theorem 2 in [22]] 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

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

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 $-S_0(a) + S_1((c)_{\{r\}}) - S_1((d)_{\{r\}}) = 1$.

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

$$a'_{r,0} = a, \quad a'_{r,1} = c, \quad a'_{r,2} = d, \quad a'_{r',2} = 0 \ (r' \neq r),$$

From Lemma 4.1,

$$\begin{aligned} S_0((a'_{r,0})_{r\in R}) &= S_0((a)_{\{r\}}) = S_0(a), \\ S_1((a'_{r,1})_{r\in R}) &= S_1((c)_{\{r\}}), \\ S_2((a'_{r,2})_{r\in R}) &= S_2((d)_{\{r\}}). \end{aligned}$$

Note that $Tr_1^2(w) = Tr_1^2(w^2) = 1, Tr_1^2(1) = 0$. From Theorem 3.1, this theorem can be obviously obtained. ■
The above theorem is a special case of Theorem in [22].

Corollary 4.13: Let $a, c, d \in \mathbb{F}_{2^m}$, $Tr_1^m(a^{\frac{1}{3}}) = Tr_1^m(c^{\frac{1}{3}}) = Tr_1^m(d^{\frac{1}{3}}) = 0$, $b \in \mathbb{F}_4$, and $gcd(r, \frac{2^m+1}{3}) = 1$. Let $f(x)$ be defined by

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

Then

(1) If $b = 0$, $f(x)$ 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: When $Tr_1^m(a^{\frac{1}{3}}) = Tr_1^m(c^{\frac{1}{3}}) = Tr_1^m(d^{\frac{1}{3}}) = 0$, from Corollary 2.12, we have

$$C_m(a, a) = C_m(c, c) = C_m(d, d) = 0.$$

From Lemma 4.2,

$$\begin{aligned}S_0(a) = S_1(a) = \frac{1}{3}(-K_m(a)+1),\\ S_0(c) = S_1(c) = \frac{1}{3}(-K_m(c)+1),\\ S_0(d) = S_1(d) = \frac{1}{3}(-K_m(d)+1).\end{aligned}$$

From Lemma 4.1 and Theorem 4.12, this corollary can be obviously obtained. ■

Parameters a, c, d considered in the above results are restricted in the subfield $\mathbb{F}_{2^m}$. Actually, this restriction is not necessary and it is just out of convenience. In the following, we will give the explanation and take Theorem 4.12 for example. Some notations are given first. Let $A \in \mathbb{F}_{2^n}^*$ with unique polar decomposition $A = \widetilde{A}\xi^{i(A)}$, where $\widetilde{A} \in \mathbb{F}_{2^m}^*$ and $0 \leq i(A) \leq 2^m$. 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 4.1.

Lemma 4.14: 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

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

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

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

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

$$\begin{aligned}S_i((A)_{\{r\}}) =& \sum_{v\in V} \chi(Tr_1^n(\widetilde{A}(\xi^{ri+li(A)} v)^{2^m-1}))\\ =& \sum_{v\in V} \chi(Tr_1^n(\widetilde{A}(\xi^{ri+i(A)} v)^{2^m-1}))\\ =& S_{ri+i(A)}(\widetilde{A})\end{aligned}$$

Hence, this lemma follows. ■

Theorem 4.15: [Theorem 2 in [22]] Let $a, c, d \in \mathbb{F}_{2^n}$, $b \in \mathbb{F}_4$, and $gcd(r, \frac{2^m+1}{3}) = 1$. Let $f(x)$ be defined by

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

Then

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

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

$$a'_{r,0} = a,\quad a'_{r,1} = c,\quad a'_{r,2} = d,\quad a'_{r',2} = 0\ (r' \neq r).$$

From Lemma 4.14,

$$\begin{aligned}S_0((a'_{r,0})_{r\in R}) = S_0((a)_{\{r\}}) = S_{i(a)}(\widetilde{a}),\\ S_1((a'_{r,1})_{r\in R}) = S_1((c)_{\{r\}}) = S_{r+i(c)}(\widetilde{c}),\\ S_2((a'_{r,2})_{r\in R}) = S_2((d)_{\{r\}}) = S_{2r+i(d)}(\widetilde{d}).\end{aligned}$$

Note that $Tr_1^2(w) = Tr_1^2(w^2) = 1, Tr_1^2(1) = 0$. From Theorem 3.1, this theorem can be obviously obtained. ■

The above theorem is equivalent to Theorem 2 in [22] for the case $p = 2, e = 3$.

Corollary 4.16: 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

$$f(x) = Tr_1^n(Ax^{r(2^m-1)}) + Tr_1^n(Cx^{r(2^m-1)+\frac{2^n-1}{3}}) + Tr_1^2(bx^{\frac{2^n-1}{3}}). \tag{17}$$

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

$$\begin{aligned}\widetilde{c}^2 &= c^{2^m+1} = A^2+AC+C^2,\\ \widetilde{d}^2 &= d^{2^m+1} = A^2+AC+C^2.\end{aligned}$$

Then

$$\begin{aligned}S_{i(a)}(\widetilde{a}) &= S_{i(a)}(A+C),\\ S_{r+i(c)}(\widetilde{c}) &= S_{r+i(c)}(\widetilde{c}^2) = S_{r+i(c)}(A^2+AC+C^2),\\ S_{2r+i(d)}(\widetilde{d}) &= S_{2r+i(d)}(\widetilde{d}^2) = S_{2r+i(d)}(A^2+AC+C^2).\end{aligned}$$

Note that $Tr_1^m((A+C)^{1/3}) = 0$,$Tr_1^m((A^2+AC+C^2)^{1/3}) = 0$. From Corollary 2.12 and Lemma 4.2, we have

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

Then

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

Hence, from Theorem 4.15, this corollary can be obviously obtained. ■

Example 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 4.16, $f(x)$ in (17) is a binomial hyper-bent function.

Example 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

$$\begin{aligned}A &= x^{23}+x^{22}+x^{21}+x^{20}+x^{19}+x^{18}+x^{16}+x^{14}+x^{12}+x^{11}+x^{10}+x^9+x^8+x^5+x^4+x^3+1,\\ C &= x^{23}+x^{20}+x^{17}+x^{16}+x^{15}+x^{12}+x^9+x^8+1,\\ b &= 1;\end{aligned}$$

Then $A+C = x^{23}+x^{22}+x^{20}+x^{18}+x^{17}+x^{12}+x^{11}+x^8+x^4+x^2+1$, $A^2+AC+C^2 = x^{23}+x^{21}+x^{17}+x^{16}+x^{14}+x^{13}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^6+x^5+x^4+x^2+x+1$ and $Tr_1^m((A+C)^{1/3}) = 0$, $Tr_1^m((A^2+AC+C^2)^{1/3}) = 0$, $K_m(A+C) = 1420$, $K_m(A^2+AC+C^2) = 712$, $-K_m(A+C)+2K_m(A^2+AC+C^2) = 4$. From Result (1) in Corollary 4.16, $f(x)$ is a trinomial hyper-bent function.

From exhaustive search by the computer, when $m = 5, 7, 9$, numbers of hyper-bent functions in Result (1) in Corollary 4.16 are 40, 728 and 5346 respectively. And numbers of hyper-bent functions in Result (2) in Corollary 4.16 are 100, 546 and 5112 respectively.

From Theorem 4.15 and Lemma 4.2, we can completely characterize all the quadrinomial hyper-bent functions in Theorem 4.15 by Kloosterman sums and cubic sums. The following lemma explains that exponents of x in the trace functions would be very big.

Lemma 4.17: 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., $r_{m,1} = min_{0\leq i\leq 2m-1}\ (1+\frac{2^m+1}{3})\cdot 2^i \mod 2^m+1$, $r_{m,2} = min_{0\leq i\leq 2m-1}\ (1+2\frac{2^m+1}{3})\cdot 2^i \mod 2^m+1$. Then $r_{m,1} = \frac{2^{m-2}+1}{3}$ and $r_{m,2} = \frac{2^{m-1}-1}{3}$.

Proof: (1) 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

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

When $j = 0$, ”=” 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

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

When $j = 1$, ”=” 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

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

When $j = 2m-2$, ”=” 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 $j = 2m-1$, ”=” holds.

Hence, $r_{m,1} = \frac{2^{m-2}+2}{3}$.

(2) We will prove $r_{m,2} = \frac{2^{m-1}-1}{3}$.

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

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

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

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

When $j = 0$, ”=” holds.

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

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

Then

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

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

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

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

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

When $j=1$, "=" holds.

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

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

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

$$(1+2\frac{2^m+1}{3})\cdot 2^j \mod (2^m+1)=\frac{2(2^m+1)}{3}-2^{j-m}\geq\frac{2(2^m+1)}{3}-2^{m-2}=\frac{5\cdot 2^{m-2}+2}{3}.$$

When $j=2m-2$, "=" holds.

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

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

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

$$(1+2\frac{2^m+1}{3})\cdot 2^j \mod (2^m+1)=\frac{2^m+1}{3}-2^{j-m}\geq\frac{2^m+1}{3}-2^{m-3}=\frac{5\cdot 2^{m-3}+1}{3}.$$

When $j=2m-3$, "=" holds.

(vi) If $j=2m-1$, $3|(2^{j+1}-1)$. We have

$$\begin{aligned}(1+2\frac{2^m+1}{3})\cdot 2^j=&(\frac{2^{j+1}-1}{3}+2^{j-m}-1)(2^m+1)+\frac{4(2^m+1)}{3}-2^{m-1}\\=&(\frac{2^{j+1}-1}{3}+2^{j-m}-1)(2^m+1)+\frac{5\cdot 2^{m-1}+4}{3}.\end{aligned}$$

Then

$$(1+2\frac{2^m+1}{3})\cdot 2^j \mod (2^m+1)=\frac{5\cdot 2^{m-1}+4}{3}$$

Hence, $r_{m,2}=\frac{2^{m-1}-1}{3}$. ■

Further, we analyze a subclass of functions in Theorem 4.15 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 4.17, $f(x)$ can be transformed into another function

$$f'(x)=Tr_1^n(a_0x^{2^m-1})+Tr_1^n(a_1'x^{r_{m,1}(2^m-1)})+Tr_1^n(a_2'x^{r_{m,2}(2^m-1)})+Tr_1^2(bx^{\frac{2^n-1}{3}}),\tag{18}$$

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 (18) belongs to cases studied by Charpin and Gong [5]. If $b\neq 0$, $f(x)$ is studied by Mesnager [26]. From results in [5] and [26], some character sums on $\mathbb{F}_{2^m}$ should be computed to determine the hyper-bent functions in (18). From Lisonek [20] and Flori, Mesnager [11], [12], to determine the hyper-bentness of $f(x)$ in (18) is equivalent to count the number of rational points of 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 $f(x)$. From Theorem 4.15, to determine hyper-bentness of $f(x)$, we just need to compute $S_{i(a)}(a)$, $S_{1+i(c)}(\widetilde{c})$ and $S_{1+i(\underset{\sim}{d})}(\widetilde{d})$, 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 2.11. From Lemma 4.2, we just need 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 [32]. Hence, it explains that our techniques can efficiently determine hyper-bentness of some special functions by Charpin, Gong [5] and Mesnager[26].

V. Conclusion

This paper generalizes classes of hyper-bent functions proposed by Charpin, Gong[5] and Mesnager[26] and consider a class of Boolean functions 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 $a_{r,i} \in \mathbb{F}_{2^n}$. From character sums on $\mathbb{F}_{2^m}$, we present the characterization of such hyper-bent functions and reformulate the characterization in terms of the number of rational points on hyper-elliptic curves. Hence, this paper extends the work of Lisonek [20] and Flori, Mesnager [11], [12]. Generally, character sums with few properties involved in hyper-bent functions via Dillon-like exponent are complicated and are difficult to construct new hyper-bent functions and characterize hyper-bent functions. So far, Kloosterman sums solves the construction and characterization of monomial functions via Dillon-like exponent [18] and some special binomial hyper-bent functions via Dillon-like exponent [25], [33], [34]. In this paper, with the help of Kloosterman sums or linear combination of Kloosterman sums, we determine the hyper-bent functions with multiple trace terms via Dillon-like exponent (including quadrinomial functions, functions with six, ten trace terms). Evaluations of Kloosterman sums at some specified points (mainly 0 and 4) [13] are often used to characterize hyper-bent functions. Our results generalize to evaluations of Kloosterman sums at three general points for determining hyper-bent functions. Hence, from known monomial hyper-bent functions via Dillon-like exponent and some special binomial hyper-bent functions via Dillon-like exponent, we can get new hyper-bent functions. Linear combinations of Kloostermans sums are helpful in characterizing hyper-bent function. Our further work will focus on linear combinations of Kloosterman sums with two or three terms and their relation with hyper-bent functions.

Acknowledgment

This work was supported by the Natural Science Foundation of China (Grant No.10990011 & No. 61272499). Yanfeng Qi also acknowledges support from Aisino Corporation Inc.

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] L. Carlitz, Explicit evaluation of certain exponential sums, Math. Scand., vol. 44, pp. 5–16, 1979.

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

[6] 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.

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

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

[9] 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.

[10] 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.

[11] J. Flori and S. Mesnager. An efficient characterization of a family of hyperbent functions with multiple trace terms. Cryptology ePrint Archive, Report 2011/373, 2011. http://eprint.iacr.org/.

[12] J. Flori and S. Mesnager. Dickson polynomials, hyperelliptic curves and hyper-bent functions. To be published in the proceedings of SETA 2012, 2012.

[13] J. Flori, S. Mesnager, and G. Cohen,"The value 4 of binary kloosterman sums," Cryptology ePrint Archive, Report 2011/364, 2011. http://eprint.iacr.org/.

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

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

[16] N. Katz and Ron Livne, Sommes de Kloosterman et courbes elliptiques universelles en caracteristiques 2 et 3. C. R. Acad. Sci. Paris Ser. I Math., 309(11):723–726, 1989.

[17] G. Lachaud and J. Wolfmann. Sommes de Kloosterman, courbes elliptiques et codes cycliques en caracteristique2. C. R. Acad. Sci. Paris Ser. I Math., 305(20):881–883, 1987.

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

[19] G. Leander andA.Kholosha, Bent functionswith Niho exponents, IEEE Trans. Inf. Theory, vol. 57, no. 9, pp. 6010–6014, 2011.

[20] P. Lisonek, "An Efficient Characterization of a Family of Hyperbent Functions," IEEE Trans. Inf. Theory, vol. 52, no. 12, pp. 5529–5532, 2006.

[21] P. Lisonek, "On the connection between Kloosterman sums and elliptic curves," in SETA, S. W. Golomb, M. G. Parker, A. Pott, and A. Winterhof, eds., vol. 5203 of Lecture Notes in Computer Science, Springer, 2008, pp. 182–187.

[22] Li, N., Helleseth, T., Tang, X., Kholosha, A. (2013). Several new classes of bent functions from Dillon exponents.

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

[24] 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.

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

[26] 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

[27] 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.

[28] 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.

[29] S. Mesnager,J. Flori,"A note on hyper-bent functions via Dillon-like exponents," ,IACR Cryptology ePrint Archive (2012)

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

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

[32] R. Schoof: Counting Points on Elliptic Curves over Finite Fields. J. Theor. Nombres Bordeaux 7:219–254, 1995.

[33] Baocheng Wang, Chunming Tang, Yanfeng Qi, and Yixian Yang. A generalization of the class of hyper-bent Boolean functions in binomial forms. Cryptology ePrint Archive, Report 2011/698, 2011. http://eprint.iacr.org/.

[34] Baocheng Wang, Chunming Tang, Yanfeng Qi, Yixian Yang, and Maozhi Xu. A new class of hyper-bent Boolean functions in binomial forms.CoRR, abs/1112.0062, 2011.

[35] Baocheng Wang, Chunming Tang, Yanfeng Qi, Yixian Yang, and Maozhi Xu. A new class of hyper-bent Boolean functions with multiple trace terms. Cryptology ePrint Archive, Report 2011/600, 2011. http://eprint.iacr.org/

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

[37] 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.