Hyper-bent Boolean Functions with Multiple Trace Terms

Sihem Mesnager

LAGA (Laboratoire Analyse, Géometrie et Applications), UMR 7539, CNRS, Department of Mathematics, University of Paris XIII and University of Paris VIII, 2 rue de la liberté, 93526 Saint-Denis Cedex, France
mesnager@math.jussieu.fr

Abstract. Bent functions are maximally nonlinear Boolean functions with an even number of variables. These combinatorial objects, with fascinating properties, are rare. The class of bent functions contains a subclass of functions the so-called hyper-bent functions whose properties are still stronger and whose elements are still rarer. In fact, hyper-bent functions seem still more difficult to generate at random than bent functions and many problems related to the class of hyper-bent functions remain open. (Hyper)-bent functions are not classified. A complete classification of these functions is elusive and looks hopeless.

In this paper, we contribute to the knowledge of the class of hyper-bent functions on finite fields $\mathbb{F}_{2^n}$ (where n is even) by studying a subclass $\mathfrak{F}_n$ of the so-called Partial Spreads class PS^- (such functions are not yet classified, even in the monomial case). Functions of $\mathfrak{F}_n$ have a general form with multiple trace terms. We describe the hyper-bent functions of $\mathfrak{F}_n$ and we show that the bentness of those functions is related to the Dickson polynomials. In particular, the link between the Dillon monomial hyper-bent functions of $\mathfrak{F}_n$ and the zeros of some Kloosterman sums has been generalized to a link between hyper-bent functions of $\mathfrak{F}_n$ and some exponential sums where Dickson polynomials are involved. Moreover, we provide a possibly new infinite family of hyper-bent functions. Our study extends recent works of the author and is a complement of a recent work of Charpin and Gong on this topic.

Keywords: Boolean function, Bent functions, Hyper-bent functions, Maximum nonlinearity, Walsh-Hadamard transformation, Kloosterman sums, Cubic sums, Dickson polynomials.

1 Introduction

Bent functions are those Boolean functions whose Hamming distance to the set of all affine functions equals $2^{n-1} \pm 2^{\frac{n}{2}-1}$ (where the number n of variables is even). They were introduced by Rothaus [18] and have attracted a lot of research, specially in the last 15 years for their own sake as interesting combinatorial objects but also because of their applications in cryptography (design of stream ciphers) and their relations to coding theory. Despite their simple and natural definition,

M.A. Hasan and T. Helleseth (Eds.): WAIFI 2010, LNCS 6087, pp. 97–113, 2010.

bent functions have turned out to admit a very complicated structure in general. Currently, some algebraic properties of bent functions are well known but the general structure of bent functions on $\mathbb{F}_{2^n}$ is not yet clear. In particular a complete classification of bent functions is elusive and looks hopeless. On the other hand many special explicit constructions are known. Some infinite classes of bent functions have been obtained, thanks to the identification between the vectorspace $\mathbb{F}_2^n$ and the Galois field $\mathbb{F}_{2^n}$. A non exhaustive list of references devoted to the description of classes of bent functions, expressed by means of trace-functions is [1, 5, 7–11, 13–16, 20]. Current results on the known properties and general constructions of bent functions can be found in [2] (pages 77-109). The class of bent functions contains a subclass of functions introduced by Youssef and Gong in [19], the so-called *hyper-bent functions*, those Boolean functions over $\mathbb{F}_{2^n}$ (n even) whose Hamming distances to all functions $Tr_1^n(ax^i) \oplus \epsilon$ ($a \in \mathbb{F}_{2^n}$, $\epsilon \in \mathbb{F}_2$) where Tr_1^n is the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ and where i is co-prime with 2^n-1, equals $2^{n-1} \pm 2^{\frac{n}{2}-1}$. The classification of hyperbent functions and many related problems remain open. In particular, it seems difficult to define precisely an infinite class of hyperbent functions, as indicated by the number of open problems proposed by Charpin and Gong in [5].

In [5] the authors have studied the bentness of the class of Boolean functions f defined on $\mathbb{F}_{2^n}$ by $f(x) := \sum_{r \in R} Tr_1^n(\beta_r x^{r(2^m-1)}), \quad \beta_r \in \mathbb{F}_{2^n}$, where $n := 2m$ and R is a subset of a set of representatives of the cyclotomic cosets modulo $2^m + 1$ for which each coset has the full size $n = 2m$. When r is co-prime with $2^m + 1$, the functions f are the sums of several Dillon monomial functions. A new tool by means of Dickson polynomials to describe hyper-bent functions f has been introduced in [5]. In fact, Charpin and Gong have shown that the bentness of those functions is related to the Dickson polynomials under some restriction on the coefficients β_r. Thanks to this new approach, a characterization of a new class of binomial hyper-bent functions has been given: $Tr_1^n\left(a\left(x^{(2^r-1)(2^m-1)} + x^{(2^r+1)(2^m-1)}\right)\right)$, where $a \in \mathbb{F}_{2^m}^\star$ and r is an integer such that $0 < r < m, \{2^r - 1, 2^r + 1\} \subset R$. Continuing their interesting approach, Gologlu [12] has proved recently that the following functions defined on $\mathbb{F}_{2^n}$ ($n = 2m$), are hyper-bent:

- $f(x) := \sum_{i=1}^{2^{m-1}-1} Tr_1^n\left(\beta x^{i(2^m-1)}\right)$; $\beta \in \mathbb{F}_{2^m} \setminus \mathbb{F}_2$.
- $f(x) := \sum_{i=1}^{2^{m-2}-1} Tr_1^n\left(\beta x^{i(2^m-1)}\right)$; m odd and $\beta^{(2^m-4)^{-1}} \in \{x \in \mathbb{F}_{2^m}^* \mid Tr_1^m(x) = 0\}$.

Recently, two new infinite families of hyper-bent Boolean functions in polynomial forms defined on $\mathbb{F}_{2^n}$ ($n = 2m$) have been exhibited and studied in [15, 17]:

- $f_{a,b}(x) := Tr_1^n(ax^{r(2^m-1)}) + Tr_1^2(bx^{\frac{2^n-1}{3}})$; m odd, $\gcd(r, 2^m+1) = 1$, $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_4^*$([15]).
- $g_{a,b}(x) := Tr_1^n(ax^{3(2^m-1)}) + Tr_1^2(bx^{\frac{2^n-1}{3}})$; m odd, $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_4^*$ ([17]).

In particular, an explicit characterization of the hyper-bent functions of those families $f_{a,b}$ and $g_{a,b}$ by means of the Kloosterman sums, has been given.

In the line of the recent works [5, 15, 17], this paper is devoted to the study of a subclass $\mathfrak{F}_n$ of the so-called class PS^-. Functions of $\mathfrak{F}_n$ are of the form: $x \in \mathbb{F}_{2^n} \mapsto \sum_{r\in R} Tr_1^n(a_r x^{r(2^m-1)}) + Tr_1^2(bx^{\frac{2^n-1}{3}})$ where R is a set of representatives of the cyclotomic cosets modulo 2^n-1 of maximal size $n := 2m$, $\{a_r,\ r \in R\}$ is a collection of elements of $\mathbb{F}_{2^m}$ and b is an element of $\mathbb{F}_4$. The set of the functions $\mathfrak{F}_n$ includes the functions studied in [15] and in [17].

The paper is organized as follows. Section 2, we fix our main notation and recall the necessary background. Next, in Section 3, we show that hyper-bent functions of $\mathfrak{F}_n$ can be described by means of exponential sums involving Dickson polynomials (Theorem 13 and Theorem 15). In particular, when b is a primitive element of $\mathbb{F}_4$, we provide a way to transfer the characterization of hyper-bentness of an element of $\mathfrak{F}_n$ to the evaluation of the Hamming weight of some Boolean functions. To illustrate our results, we show in the Sub-section 3.2.3 that the results presented in [15] and in [17] can be deduced. Finally, in the end of section 3, we provide a possibly new infinite family of hyper-bent functions provided that some set is not empty (Conjecture 1).

2 Notation and Preliminaries

For any set E, $E^\star = E \setminus \{0\}$ and $|E|$ will denote the cardinality of E.

- *Boolean functions and polynomial forms*:

Let n be a positive integer. A Boolean function f on $\mathbb{F}_{2^n}$ is an $\mathbb{F}_2$-valued function on the Galois field $\mathbb{F}_{2^n}$ of order 2^n. The *weight* of f, denoted by $\mathrm{wt}(f)$, is the *Hamming weight* of the image vector of f i.e. the cardinality of its support $supp(f) := \{x \in \mathbb{F}_{2^n} \mid f(x) = 1\}$.

For any positive integer k, and r dividing k, the trace function from $\mathbb{F}_{2^k}$ to $\mathbb{F}_{2^r}$, denoted by Tr_r^k, is the mapping defined as: $Tr_r^k(x) := \sum_{i=0}^{\frac{k}{r}-1} x^{2^{ir}}$. In particular, we denote the *absolute trace* over $\mathbb{F}_2$ of an element $x \in \mathbb{F}_{2^n}$ by $Tr_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$. Recall that, the absolute trace satisfies $(Tr_1^n(x))^2 = Tr_1^n(x) = Tr_1^n(x^2)$ for every $x \in \mathbb{F}_{2^n}$ and that, for every integer r dividing k, the trace function Tr_r^k satisfies the transitivity property, that is, $Tr_1^k = Tr_1^r \circ Tr_r^k$.

Every non-zero Boolean function f defined on $\mathbb{F}_{2^n}$ has a (unique) trace expansion of the form:

$$\forall x \in \mathbb{F}_{2^n}, \quad f(x) = \sum_{j\in\Gamma_n} Tr_1^{o(j)}(a_j x^j) + \epsilon(1 + x^{2^n-1})$$

called its polynomial form, where Γ_n is the set of integers obtained by choosing one element in each cyclotomic class $\{j \times 2^i \pmod{2^n-1};\quad i \in \mathbb{N}\}$ of 2 modulo 2^n-1, $o(j)$ is the size of the cyclotomic coset of 2 modulo 2^n-1 containing j, $a_j \in \mathbb{F}_{2^{o(j)}}$ and, $\epsilon = \mathrm{wt}(f)$ modulo 2.

- *Walsh transform, bent and hyper-bent functions*:

Let f be a Boolean function on $\mathbb{F}_{2^n}$. Its *"sign" function* is the integer-valued function $\chi(f) := (-1)^f$. The Walsh Hadamard transform of f is the discrete Fourier transform of χ_f, whose value at $\omega \in \mathbb{F}_{2^n}$ is defined as follows:

$$\forall \omega \in \mathbb{F}_{2^n}, \quad \widehat{\chi_f}(\omega) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+Tr_1^n(\omega x)}.$$

Bent functions can be defined as follows:

Definition 1. A Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ (n even) is said to be bent if $\widehat{\chi_f}(\omega) = \pm 2^{\frac{n}{2}}$, for all $\omega \in \mathbb{F}_{2^n}$.

Hyper-bent functions have properties still stronger than bent functions. More precisely, they can be defined as follows:

Definition 2. A Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ (n even) is said to be hyper-bent if the function $x \mapsto f(x^i)$ is bent, for every integer i co-prime with $2^n - 1$.

Note that bent and hyper-bent functions defined on $\mathbb{F}_{2^n}$ exist only for even n. Moreover, it is well known that their Hamming weight is even. Therefore, their polynomial form is

$$\forall x \in \mathbb{F}_{2^n}, \quad f(x) = \sum_{j \in \Gamma_n} Tr_1^{o(j)}(a_j x^j) \tag{1}$$

where Γ_n, $o(j)$ are defined as above and $a_j \in \mathbb{F}_{2^{o(j)}}$.

- *Some results on bent and hyper-bent Boolean fucntions*:

Recall the following well-known result which includes the definition of the Partial Spreads class $\mathcal{PS}^-$ introduced by Dillon.

Theorem 1. *[8] Let E_i, $i = 1, 2, \cdots, N$, be N subspaces of $\mathbb{F}_{2^n}$ of dimension m satisfying $E_i \cap E_j = \{0\}$ for all $i, j \in \{1, 2, \cdots, N\}$ with $i \neq j$. Let f be a Boolean function over $\mathbb{F}_{2^n}$ ($n = 2m$). Assume that the support of f can be written as*
$supp(f) = \bigcup_{i=1}^{N} E_i^\star$, where $E_i^\star := E_i \setminus \{0\}$.
Then f is bent if and only if $N = 2^{m-1}$. In this case f is said to be in the $\mathcal{PS}^-$ class.

Youssef and Gong have shown that hyper-bent functions exist. They partially state this main result of [19] in terms of sequences. The following proposition is an easy translation of their result stated using only the terminology of Boolean functions (see [3])

Proposition 2. *[19] Let $n = 2m$ be an even integer. Let α be a primitive element of $\mathbb{F}_{2^n}$. Let f be a Boolean function defined on $\mathbb{F}_{2^n}$ such that $f(\alpha^{2^m+1}x) = f(x)$ for every $x \in \mathbb{F}_{2^n}$ and $f(0) = 0$. Then, f is a hyper-bent function if and only if the weight of the vector $(f(1), f(\alpha), f(\alpha^2), \cdots, f(\alpha^{2^m}))$ equals 2^{m-1}.*

Charpin and Gong [5] have derived a slightly different version of the preceding Proposition.

Proposition 3. *[5] Let $n = 2m$ be an even integer. Let α be a primitive element of $\mathbb{F}_{2^n}$. Let f be a Boolean function defined on $\mathbb{F}_{2^n}$ such that $f(\alpha^{2^m+1}x) = f(x)$ for every $x \in \mathbb{F}_{2^n}$ and $f(0) = 0$. Denote by G the cyclic subgroup of $\mathbb{F}_{2^n}^\star$ of order $2^m + 1$. Let ζ be a generator of G. Then, f is a hyper-bent function if and only if the cardinality of the set $\{i \mid f(\zeta^i) = 1, 0 \leq i \leq 2^m\}$ equals 2^{m-1}.*

Remark 1. It is important to point out that bent Boolean functions f defined on $\mathbb{F}_{2^n}$ such that $f(\alpha^{2^m+1}x) = f(x)$ for every $x \in \mathbb{F}_{2^n}$ (where α is a primitive element of $\mathbb{F}_{2^n}$) and $f(0) = 0$ are hyper-bent (see proof of Theorem 2 in [5] or observe that the support $supp(f)$ of such Boolean functions f can be decomposed as $supp(f) = \bigcup_{i \in S} \alpha^i \mathbb{F}_{2^m}^\star$, where $S = \{i \mid f(\alpha^i) = 1\}$, that is, thanks to Theorem 1, functions f are bent if and only if $|S| = 2^{m-1}$, proving that these bent functions are hyper-bent functions, according to Proposition 2).

Dillon exhibits a subclass of $\mathcal{PS}^-$, denoted by $\mathcal{PS}_{ap}$, whose elements are defined in an explicit form ($\mathbb{F}_{2^{2m}}$ is a $\mathbb{F}_{2^m}$-vectorspace of dimension 2; every element $z \in \mathbb{F}_{2^{2m}}$ can be decomposed as $z = x + wy$ with $(x, y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ where $\{1, w\}$ stands for a basis of the $\mathbb{F}_{2^m}$-vectorspace $\mathbb{F}_{2^{2m}}$):

Definition 3. Let $n = 2m$. The Partial Spreads class $\mathcal{PS}_{ap}$ consists of all functions f defined as follows: let g be a balanced Boolean function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$ such that $g(0) = 0$. Define a Boolean function f from $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ to $\mathbb{F}_2$ as $f(x, y) = g(xy^{2^m-2})$ for every $(x, y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$.

It is well-known (see *e.g* [3]) that, all the functions of the class $\mathcal{PS}_{ap}$ are hyper-bent. Carlet and Gaborit have proved in [3] the following more precise statement of Proposition 2.

Proposition 4. *[3] Boolean functions of Proposition 2 such that $f(1) = 0$ are elements of the class $\mathcal{PS}_{ap}$. Those such that $f(1) = 1$ are the functions of the form $f(x) = g(\delta x)$ for some $g \in \mathcal{PS}_{ap}$ and $\delta \in \mathbb{F}_{2^n} \setminus \{1\}$ such that $g(\delta) = 1$.*

- *Some classical binary exponential sums*:

Recall two classical binary exponential sums on $\mathbb{F}_{2^n}$ (where n is a positive integer):

Definition 4. The binary Kloosterman sums on $\mathbb{F}_{2^n}$ are:

$$K_n(a) := \sum_{x \in \mathbb{F}_{2^n}} \chi\big(Tr_1^n(ax + \frac{1}{x})\big), \quad a \in \mathbb{F}_{2^n}$$

Recall the following result

Proposition 5. *[13] The Kloosterman sums K_n on $\mathbb{F}_{2^n}$ takes integer values in the range $[-2^{(n+2)/2} + 1, 2^{(n+2)/2} + 1]$.*

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

$$C_n(a, b) := \sum_{x \in \mathbb{F}_{2^n}} \chi\big(Tr_1^n(ax^3 + bx)\big), \quad a \in \mathbb{F}_{2^n}^\star, b \in \mathbb{F}_{2^n}$$

The exact values of the cubic sums $C_m(a,a)$ on $\mathbb{F}_{2^m}$ can be computed thanks to Carlitz's result [4] by means of the Jacobi symbol. Recall that the Jacobi symbol $\left(\frac{2}{m}\right)$ is a generalization of the Legendre symbol (which is defined when m is an odd prime). For m odd, $\left(\frac{2}{m}\right)=(-1)^{\frac{(m^2-1)}{8}}$.

Proposition 6. *[4] Let m be an odd integer. Let $a \in \mathbb{F}_{2^m}^{\star}$ and $c \in \mathbb{F}_{2^m}$, Then*

1. *$C_m(1,1)=\left(\frac{2}{m}\right)2^{\frac{m+1}{2}}$ where $\left(\frac{2}{m}\right)$ is the Jacobi symbol.*
2. *If $Tr_1^m(c)=0$, then $C_m(1,c)=0$.*
3. *If $Tr_1^m(c)=1$ (with $c\neq 1$), then $C_m(1,c)=\chi(Tr_1^m(\gamma^3+\gamma))\left(\frac{2}{m}\right)2^{\frac{m+1}{2}}$ where $c=\gamma^4+\gamma+1$ for some $\gamma\in\mathbb{F}_{2^m}$.*

• *Dickson Polynomials:*

Recall that the family of Dickson polynomials $D_r(X)\in\mathbb{F}_2[X]$ is defined by

$$D_r(X)=\sum_{i=0}^{\frac{r}{2}}\frac{r}{r-i}\binom{r-i}{i}X^{r-2i},\quad r=2,3,\cdots$$

Moreover, the family of Dickson polynomials $D_r(X)\in\mathbb{F}_2[X]$ can also be defined by the following recurrence relation:

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

with initial values

$$D_0(X)=0,\quad D_1(X)=X.$$

Now, recall the following properties which we use in the sequel. For any non-zero positive integers r and p, Dickson polynomials satisfy:

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

3 Hyper-bent Functions Whose Expression is the Sum of Multiple Trace Terms

In the sequel, n is an even positive integer, $m=\frac{n}{2}$ is an odd integer and E is a set of representatives of the cyclotomic classes modulo 2^n-1 for which each class has the full size n. We denote by $\mathfrak{F}_n$ the set of Boolean functions f_b, $(b\in\mathbb{F}_4)$ defined on $\mathbb{F}_{2^n}$ whose polynomial forms are:

$$f_b(x):=\sum_{r\in R}Tr_1^n(a_rx^{r(2^m-1)})+Tr_1^2(bx^{\frac{2^n-1}{3}}). \tag{2}$$

where $R\subseteq E$ and all the coefficients a_r are in $\mathbb{F}_{2^m}$.

Note that the size of the cyclotomic coset of 2 modulo 2^n-1 containing $\frac{2^n-1}{3}$ is equal to 2 (i.e. $o(\frac{2^n-1}{3})=2$) and that, the function f_b does not belong to the class considered by Charpin and Gong in [5].

For m odd, 2^m+1 is a multiple of 3 and thus all exponents for x in (2) are multiples of 2^m-1. Therefore, every Boolean function f_b in $\mathfrak{F}_n$ satisfies

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

where α denotes any primitive element of $\mathbb{F}_{2^n}$. Furthermore, since every Boolean f_b of $\mathfrak{F}_n$ vanishes at 0, one can then apply Proposition 3 to get the following characterization of hyper-bentness for an element of $\mathfrak{F}_n$.

Proposition 7. *Let $f_b \in \mathfrak{F}_n$. Set $\Lambda(f_b) := \sum_{u\in U} \chi(f_b(u))$ where U is the group of (2^m+1)-st roots of unity, that is, $U = \{x \in \mathbb{F}_{2^n} \mid x^{2^m+1} = 1\}$. Then, f_b is hyper-bent if and only if $\Lambda(f_b) = 1$. Moreover, a hyper-bent function f_b is in the Partial Spreads class PS_{ap} if and only if $b \in \mathbb{F}_2$.*

Proof. The Boolean function f_b satisfies the assumptions of Proposition 3. Therefore f_b is hyper-bent if and only if its restriction to U has Hamming weight 2^{m-1} according to Proposition 3. Now, one has $\Lambda(f_b) = 2^m+1-2|\{u \in U \mid f_b(u) = 1\}|$. Therefore, the Hamming weight of the restriction of f_b to U equals 2^{m-1} if and only if $\Lambda(f_b) = 1$. The second part of the proposition is a direct application of Proposition 4. Indeed, note that $f_b(1) = \sum_{r\in R} Tr_1^n(a_r) + Tr_1^2(b) = Tr_1^2(b)$ (since $Tr_1^n(a_r) = 0$ for every $r \in R$ because $a_r \in \mathbb{F}_{2^m}$) and it is clear that the elements b of $\mathbb{F}_4$ whose trace over $\mathbb{F}_4$ equals 0, are the elements of $\mathbb{F}_2$.

3.1 The Case $b = 0$

Charpin and Gong [5] have studied the functions of $\mathfrak{F}_n$ in the case where $b = 0$ and provide the following characterization of the hyper-bentness in terms of Dickson polynomials.

Theorem 8. *[5] Let $n = 2m$. Let E' be a set of representatives of the cyclotomic cosets modulo 2^m+1 for which each coset has the full size n. Let f be the function defined on $\mathbb{F}_{2^n}$ by $f(x) = \sum_{r\in R} Tr_1^n(a_r x^{r(2^m-1)}), \quad a_r \in \mathbb{F}_{2^m}$ where $R \subseteq E'$. Let g be the Boolean function defined on $\mathbb{F}_{2^m}$ by $g(x) = \sum_{r\in R} Tr_1^m(a_r D_r(x))$. Then f is hyper-bent if and only if*

$$\sum_{x\in\mathbb{F}_{2^m}} \chi(Tr_1^m(x^{-1}) + g(x)) = 2^m - 2\,\mathrm{wt}(g).$$

Remark 2. The bentness of monomial functions of $\mathfrak{F}_n$ has been studied. More precisely, the exponent 2^m-1 has been considered by Dillon in [8] as an example of bent functions belonging to $\mathcal{PS}^-$ (Theorem 1). Using results from coding theory, Dillon has proved in [8] that the function $x \in \mathbb{F}_{2^n} \mapsto Tr_1^n(ax^{2^m-1})$ is (hyper)-bent if and only if the Kloosterman sum K_m on $\mathbb{F}_{2^m}$ satisfies $K_m(a) = 0$. Further, the exponent $r(2^m-1)$ where r is co-prime with 2^m+1, has been considered firstly by Leander [14] and next by Charpin and Gong [5] (in fact Leander has found another proof of Dillon's result which gives more insight; a small error in his proof has been corrected in [5]). It has been proved that the function $x \in \mathbb{F}_{2^n} \mapsto Tr_1^n(a_r x^{r(2^m-1)})$ where $\gcd(r, 2^m+1) = 1$, is hyper-bent if and only if a is a zero of the Kloosterman sum K_m on $\mathbb{F}_{2^m}$.

3.2 The Case Where $b \in \mathbb{F}_4^\star$

We are interested in characterizing the hyper-bentness of the Boolean function of the form (2) where $b \neq 0$. To this end, we begin by introducing some additional notation while underlining some facts.

Let β be a primitive element of $\mathbb{F}_4$. Suppose that $\beta = \alpha^{\frac{2^n-1}{3}}$ for some primitive element α of $\mathbb{F}_{2^n}$. Set $\xi := \alpha^{2^m-1}$ so that ξ is a generator of the cyclic group $U := \{u \in \mathbb{F}_{2^n} \mid u^{2^m+1} = 1\}$. Note that U can be decomposed as : $U = \bigcup_{i=0}^{2} \xi^i V$ where $V := \{u^3,\ u \in U\}$. Next, let introduce the sums

$$S_i := \sum_{v \in V} \chi(f_0(\xi^i v)), \quad \forall i \in \{0,1,2\} \tag{3}$$

First of all, note that

$$S_0 + S_1 + S_2 = \sum_{u \in U} \chi(f_0(u)). \tag{4}$$

Next, one has

Lemma 9. *$S_1 = S_2$.*

Proof. Since the trace map is invariant under the Frobenius automorphism $x \mapsto x^2$, we get applying m times the Frobenius automorphism : $\forall x \in \mathbb{F}_{2^n}$,

$$f_0(x) = \sum_{r \in R} Tr_1^n\left(a_r^{2^m} x^{2^m r(2^m-1)}\right) = \sum_{r \in R} Tr_1^n\left(a_r x^{2^m r(2^m-1)}\right) = f_0(x^{2^m})$$

because all the coefficients a_r are in $\mathbb{F}_{2^m}$. Hence, $S_1 = \sum_{v \in V} \chi(f_0(\xi^{2^m} v^{2^m})) = \sum_{v \in V} \chi(f_0(\xi^2(\xi^{2^m-2} v^{2^m})))$. Now, since m is odd, 3 divides $2^m + 1$ and then divides $2^m - 2$. Hence, ξ^{2^m-2} is a cube of U and the mapping $v \mapsto \xi^{(2^m-2)} v^{2^m}$ is a permutation of V. Consequently, $S_1 = \sum_{v \in V} \chi(f_0(\xi^2 v)) = S_2$.

Now, for $b \in \mathbb{F}_4^\star$, we establish expressions for $\Lambda(f_b) := \sum_{u \in U} \chi(f_b(u))$ (where U is the group of (2^m+1)-st roots of unity) involving the sums S_i.

Proposition 10. *$\Lambda(f_\beta) = \Lambda(f_{\beta^2}) = -S_0$ and $\Lambda(f_1) = S_0 - 2S_1$.*

Proof. Introduce for every element c of $\mathbb{F}_4$ $T(c) := \sum_{b \in \mathbb{F}_4} \Lambda(f_b)\chi(Tr_1^2(bc))$. Recall that one has

$$\Lambda(f_b) = \frac{1}{4} \sum_{c \in \mathbb{F}_4} T(c)\chi(Tr_1^2(bc)). \tag{5}$$

Indeed

$$\begin{aligned}
&\sum_{c \in \mathbb{F}_4} T(c)\chi(Tr_1^2(bc)) \\
&= \sum_{c \in \mathbb{F}_4} \sum_{d \in \mathbb{F}_4} \Lambda(f_d)\chi(Tr_1^2(dc))\chi(Tr_1^2(bc)) \\
&= \sum_{d \in \mathbb{F}_4} \Lambda(f_d) \sum_{c \in \mathbb{F}_4} \chi(Tr_1^2(c(d+b)))
\end{aligned}$$

But $\sum_{c\in\mathbb{F}_4}\chi(Tr_1^2(c(d+b)))=4$ if $d=b$ (i.e $b+d=0$) and 0 otherwise. Then, one gets $\sum_{c\in\mathbb{F}_4}T(c)\chi(Tr_1^2(bc))=4\Lambda(f_b)$.

Now, note that $T(c)=\sum_{u\in U}\chi(f_0(u))\sum_{b\in\mathbb{F}_4}\chi\Big(Tr_1^2\Big(b\big(c+u^{\frac{2^n-1}{3}}\big)\Big)\Big)$. Furthermore, one has

$$\sum_{b\in\mathbb{F}_4}\chi\Big(Tr_1^2\Big(b\big(c+u^{\frac{2^n-1}{3}}\big)\Big)\Big)=0 \text{ if } u^{\frac{2^n-1}{3}}\neq c \text{ and } 4 \text{ otherwise.}$$

Since, $u^{\frac{2^n-1}{3}}\neq 0$ for every $u\in U$, $T(0)=0$. Since β is a primitive element of $\mathbb{F}_4$, let suppose from now that $c=\beta^i$, $i\in\{0,1,2\}$. Recall that $\beta=\alpha^{\frac{2^n-1}{3}}$ and $\xi=\alpha^{2^m-1}$ for some primitive element α of $\mathbb{F}_{2^n}$. Then $\beta^i=\xi^{i\frac{2^m+1}{3}}$. Hence, $T(\beta^i)=4\sum_{u\in U,\, u^{\frac{2^n-1}{3}}=\beta^i=\xi^{i\frac{2^m+1}{3}}}\chi(f_0(u))$. Now,

$$u^{\frac{2^n-1}{3}}=\xi^{i\frac{2^m+1}{3}} \iff \left(u^{-2}\xi^{-i}\right)^{\frac{2^m+1}{3}}=1 \iff u^{-2}\in\xi^iV.$$

That follows from the fact that the only elements x of U such that $x^{\frac{2^m+1}{3}}=1$ are the elements of V. Next, noting that the map $x\mapsto x^{2^{m-1}}$ is one-to-one from ξ^iV to ξ^iV (because $\xi^{i(2^{m-1}-1)}$ is a cube since $2^{m-1}-1\equiv 0 \pmod 3$ for m odd), one gets that $u^{\frac{2^n-1}{3}}=\xi^{i\frac{2^m+1}{3}} \iff u\in\xi^iV$. Therefore

$$T(\beta^i)=4\sum_{v\in V}\chi(f_0(\xi^iv))=4S_i.$$

Finally, by the inversion formula (5), one gets $\Lambda(f_b)=\frac{1}{4}\sum_{c\in\mathbb{F}_4}T(c)\chi(Tr_1^2(bc))$ that is,

$$\begin{aligned}
\Lambda(f_1)&=S_0\chi(Tr_1^2(1))+S_1\chi(Tr_1^2(\beta))+S_2\chi(Tr_1^2(\beta^2)),\\
\Lambda(f_\beta)&=S_0\chi(Tr_1^2(\beta))+S_1\chi(Tr_1^2(\beta^2))+S_2\chi(Tr_1^2(1)),\\
\Lambda(f_{\beta^2})&=S_0\chi(Tr_1^2(\beta^2))+S_1\chi(Tr_1^2(1))+S_2\chi(Tr_1^2(\beta)).
\end{aligned}$$

The result follows then from Lemma 9 and from the fact that $Tr_1^2(1)=0$ and $Tr_1^2(\beta)=Tr_1^2(\beta^2)=1$.

From Proposition 7, Proposition 10, Lemma 9 and (4), one straight-forwardly deduces the following statement.

Lemma 11. *Let $n=2m$ be an even integer with m odd. For $b\in\mathbb{F}_4$, let f_b be a function defined by (2). Let β be a primitive element of $\mathbb{F}_4$. Let U be the cyclic group of (2^m+1)-st roots of unity and V be the set of the cube of U. Then,*

1. *f_β is hyper-bent if and only if $\sum_{v\in V}\chi(f_0(v))=-1$.*
2. *f_β is hyper-bent if and only if f_{β^2} is hyper-bent.*
3. *f_1 is hyperbent if and only if $2\sum_{v\in V}\chi(f_0(v))-\sum_{u\in U}\chi(f_0(u))=1$.*

The case where b is a primitive element of $\mathbb{F}_4$. According to assertion (2) of Lemma 11, we can suppose that $b = \beta$ without loss of generality. As in the case where $b = 0$ (Theorem 8), one can establish a characterization of the hyper-bentness of f_β involving the Dickson polynomials. To this end, we begin with proving the following result.

Lemma 12. *Let f_0 be the function defined on $\mathbb{F}_{2^n}$ by (2) with $b = 0$. Let g be the related function defined on $\mathbb{F}_{2^m}$ by $g(x) = \sum_{r\in R} Tr_1^m(a_r D_r(x))$, where $D_r(x)$ is the Dickson polynomial of degree r. Let U be the cyclic group of (2^m+1)-st roots of unity. Then, for any positive integer p, we have*

$$\sum_{u\in U} \chi\Big(f_0(u^p)\Big) = 1 + 2 \sum_{c\in\mathbb{F}_{2^m}^\star, Tr_1^m(c^{-1})=1} \chi\Big(g(D_p(c))\Big).$$

Proof. Using the transitivity rule $Tr_1^n = Tr_1^m \circ Tr_m^n$, the fact that the coefficients a_r are in the subfield $\mathbb{F}_{2^m}$ of $\mathbb{F}_{2^n}$ and the fact that the mapping $u \mapsto u^{2^m-1}$ is a permutation of U, one has

$$\begin{aligned}\sum_{u\in U} \chi\Big(f_0(u^p)\Big) &= \sum_{u\in U} \chi\Big(\sum_{r\in R} Tr_1^m\big(a_r(u^{(2^m-1)rp} + u^{2^m(2^m-1)rp})\big)\Big)\\ &= \sum_{u\in U} \chi\Big(\sum_{r\in R} Tr_1^m\big(a_r(u^{rp} + u^{-rp})\big)\Big) = \sum_{u\in U} \chi\Big(\sum_{r\in R} Tr_1^m\big(a_r D_{rp}(u+u^{-1})\big)\Big)\end{aligned}$$

since $u^p + u^{-p} = D_p(u+u^{-1})$. Recall now that every element $1/c$ where $c \in \mathbb{F}_{2^m}^\star$ with $Tr_1^m(c) = 1$ can be uniquely represented as $u + u^{2^m} = u + u^{-1}$ with $u \in U$. Thus

$$\begin{aligned}\sum_{u\in U} \chi\Big(f_0(u^p)\Big) &= 1 + \sum_{u\in U\setminus\{1\}} \chi\Big(\sum_{r\in R} Tr_1^m\big(a_r D_{rp}(u+u^{-1})\big)\Big)\\ &= 1 + 2 \sum_{c\in\mathbb{F}_{2^m}^\star, Tr_1^m(c)=1} \chi\Big(\sum_{r\in R} Tr_1^m\big(a_r D_{rp}(1/c)\big)\Big)\\ &= 1 + 2 \sum_{c\in\mathbb{F}_{2^m}^\star, Tr_1^m(c^{-1})=1} \chi\Big(\sum_{r\in R} Tr_1^m\big(a_r D_{rp}(c)\big)\Big).\end{aligned}$$

In the last equality, we use the fact that the map $c \mapsto 1/c$ is a permutation on $\mathbb{F}_{2^m}$. Now, since $D_{rp} = D_r \circ D_p$, one gets

$$\sum_{u\in U} \chi\Big(f_0(u^p)\Big) = 1 + 2 \sum_{c\in\mathbb{F}_{2^m}^\star, Tr_1^m(c^{-1})=1} \chi\Big(g(D_p(c))\Big).$$

From Lemma 11 and Lemma 12, one deduce the following statement.

Theorem 13. *Let $n = 2m$ be an even integer with m odd. Let β be a primitive element of $\mathbb{F}_4$. Let f_β be the function defined on $\mathbb{F}_{2^n}$ by (2). Let g be the related function defined on $\mathbb{F}_{2^m}$ by $g(x) = \sum_{r\in R} Tr_1^m(a_r D_r(x))$, where $D_r(x)$ is the Dickson polynomial of degree r. Then, the three assertions are equivalent*

1. f_β *is hyper-bent.*
2. $\displaystyle\sum_{x\in\mathbb{F}_{2^m}^\star, Tr_1^m(x^{-1})=1} \chi\Big(g(D_3(x))\Big) = -2.$
3. $\displaystyle\sum_{x\in\mathbb{F}_{2^m}^\star} \chi\Big(Tr_1^m(x^{-1}) + g(D_3(x))\Big) = 2^m - 2\,\mathrm{wt}(g\circ D_3) + 4.$

Proof. According to Lemma 12, we have

$$S_0 = \sum_{v\in V} \chi\Big(f_0(v)\Big) = \frac{1}{3}\sum_{u\in U} \chi\Big(f_0(u^3)\Big) = \frac{1}{3}\left(1 + 2\sum_{x\in\mathbb{F}_{2^m}^\star, Tr_1^m(x^{-1})=1} \chi\Big(g(D_3(x))\Big)\right).$$

The equivalence between assertions (1) and (2) follows then from assertion (1) of Lemma 11.

Now, note that the indicator of the set $\{x \in \mathbb{F}_{2^m}^\star \mid Tr_1^m(x^{-1}) = 1\}$ can be written as $\frac{1}{2}\left(1 - \chi(Tr_1^m(x^{-1}))\right)$. Therefore,

$$\begin{aligned}
&\sum_{x\in\mathbb{F}_{2^m}^\star, Tr_1^m(x^{-1})=1} \chi\Big(g(D_3(x))\Big) \\
&\quad= \frac{1}{2}\left(\sum_{x\in\mathbb{F}_{2^m}^\star} \chi\Big(g(D_3(x))\Big) - \sum_{x\in\mathbb{F}_{2^m}^\star} \chi\Big(Tr_1^m(x^{-1} + g(D_3(x)))\Big)\right) \\
&\quad= \frac{1}{2}\left(\sum_{x\in\mathbb{F}_{2^m}} \chi\Big(g(D_3(x))\Big) - \sum_{x\in\mathbb{F}_{2^m}} \chi\Big(Tr_1^m(x^{-1} + g(D_3(x)))\Big)\right).
\end{aligned}$$

Now, f_β is hyper-bent if and only if $\sum_{x\in\mathbb{F}_{2^m}^\star, Tr_1^m(x^{-1})=1} \chi\Big(g(D_3(x))\Big) = -2$. Therefore, using the fact that, for a Boolean function h defined on $\mathbb{F}_{2^n}$, $\sum_{x\in\mathbb{F}_{2^n}} \chi(h(x)) = 2^n - 2\,\mathrm{wt}(h)$, we get that f_β is hyper-bent if and only if

$$\sum_{x\in\mathbb{F}_{2^m}} \chi\Big(Tr_1^m(x^{-1}) + g(D_3(x))\Big) = 4 + 2^m - 2\,\mathrm{wt}(g\circ D_3).$$

One also has

Proposition 14. *Let $n = 2m$ be an even integer with m odd. Let d be a positive integer. Suppose that d and $\frac{2^m+1}{3}$ are co-prime. Let β be a primitive element of $\mathbb{F}_4$. Let f_β be the function defined by (2) and h_β be the function whose expression is*

$$\sum_{r\in R} Tr_1^n(a_r x^{dr(2^m-1)}) + Tr_1^2(\beta x^{\frac{2^n-1}{3}})$$

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

Proof. According to assertion (1) of Lemma 11, h_β is hyper-bent if and only if $\sum_{v\in V} \chi(h_0(v)) = -1$. Now, $\sum_{v\in V} \chi(h_0(v)) = \sum_{v\in V} \chi(f_0(v^d)) = \sum_{v\in V} \chi(f_0(v))$ since the mapping $v \mapsto v^d$ is then a permutation of V if $\frac{2^m+1}{3}$ and d are co-prime. The result follows again from assertion (1) of Lemma 11.

The case where $b = 1$. In this subsection, we are interested in characterizing the hyper-bentness of the Boolean function f_1 whose polynomial form is $f_1(x) = \sum_{r\in R} Tr_1^n(a_r x^{r(2^m-1)}) + Tr_1^2(x^{\frac{2^n-1}{3}})$. In this case one can give a characterization of the bentness, analogous to the assertion (2) of Theorem 13.

Theorem 15. *Let $n = 2m$ be an even integer with m odd. Let f_1 be the Boolean function defined on $\mathbb{F}_{2^n}$ by*

$$f_1(x) = \sum_{r\in R} Tr_1^n(a_r x^{r(2^m-1)}) + Tr_1^2(x^{\frac{2^n-1}{3}}).$$

Let g be the related function defined on $\mathbb{F}_{2^m}$ by $g(x) = \sum_{r\in R} Tr_1^m(a_r D_r(x))$, where $D_r(x)$ is the Dickson polynomial of degree r.
Then, f_1 is hyper-bent if and only if,

$$2\sum_{x\in\mathbb{F}_{2^m}^\star, Tr_1^m(x^{-1})=1} \chi\Big(g(D_3(x))\Big) - 3\sum_{x\in\mathbb{F}_{2^m}^\star, Tr_1^m(x^{-1})=1} \chi\Big(g(x)\Big) = 2.$$

Proof. Note that

$$\begin{aligned} 2\sum_{v\in V}\chi(f_0(v)) - \sum_{u\in U}\chi(f_0(u)) &= \frac{2}{3}\sum_{u\in U}\chi(f_0(u^3)) - \sum_{u\in U}\chi(f_0(u)) \\ &= -\frac{1}{3} + \frac{4}{3}\sum_{x\in\mathbb{F}_{2^m}^\star, Tr_1^m(x^{-1})=1} \chi\Big(g(D_3(x))\Big) - 2\sum_{x\in\mathbb{F}_{2^m}^\star, Tr_1^m(x^{-1})=1} \chi\Big(g(x)\Big) \end{aligned}$$

according to Lemma 12. One then concludes using Lemma 11 that states that f_1 is hyper-bent if and only if

$$2\sum_{v\in V}\chi(f_0(v)) - \sum_{u\in U}\chi(f_0(u)) = 1.$$

On can also prove the similar result to Proposition 14.

Proposition 16. *Let $n = 2m$ be an even integer with m odd. Suppose that $m \not\equiv 3 \pmod 6$. Let d be a positive integer such that $\gcd(d, 2^m + 1) = 3$. Let β be a primitive element of $\mathbb{F}_4$. Let f_β be the function defined by (2) and h_1 be the function whose expression is*

$$\sum_{r\in R} Tr_1^n(a_r x^{dr(2^m-1)}) + Tr_1^2(x^{\frac{2^n-1}{3}})$$

If f_β is hyper-bent then, h_1 is hyper-bent.

Proof. Set $h_0(x) := \sum_{r\in R} Tr_1^n(a_r x^{dr(2^m-1)})$. One has (since $\gcd(d, 2^m+1) = 3$)

$$\sum_{v\in V}\chi(h_0(v)) = \sum_{v\in V}\chi(f_0(v^d)) = \sum_{v\in V}\chi(f_0(v^3)) = \sum_{v\in V}\chi(f_0(v))$$

since the mapping $v \mapsto v^3$ is a permutation when $m \not\equiv 3 \pmod 6$. On the other hand, note that (since $\gcd(d, 2^m + 1) = 3$)

$$\sum_{u \in U} \chi(h_0(u)) = \sum_{u \in U} \chi(f_0(u^d)) = \sum_{u \in U} \chi(f_0(u^3)) = 3 \sum_{v \in V} \chi(f_0(v)).$$

Now, $\sum_{v \in V} \chi(f_0(v)) = -1$ according to Lemma 11, since f_β is hyper-bent. Hence, $2\sum_{v \in V} \chi(h_0(v)) - \sum_{u \in U} \chi(h_0(u)) = -2 - (-3) = 1$, proving that h_1 is hyper-bent (according to Lemma 11).

Examples

Example 1. To illustrate our results, we describe the set of hyper-bent functions of a particular family of Boolean functions belonging to the class (2), that is, the Boolean functions $f_{\beta^i}, i \in \{0, 1, 2\}$ (studied in [15, 16]) defined on $\mathbb{F}_{2^n}$ ($n = 2m$, m odd) as:

$$f_{\beta^i}(x) = Tr_1^n(ax^{2^m-1}) + Tr_1^2(\beta^i x^{\frac{2^n-1}{3}}), \quad \forall x \in \mathbb{F}_{2^n}$$

where $a \in \mathbb{F}_{2^m}^\star$ and β is a primitive element of $\mathbb{F}_4$.
In this case, $f_0(x) = Tr_1^n(ax^{2^m-1})$ is the Dillon function and the related function g is defined by $g(x) = Tr_1^m(ax)$.
According to Lemma 11, f_β is hyper-bent if and only if f_{β^2} is hyper-bent and, according to Theorem 13,
f_β is hyper-bent if and only if $\sum_{x \in \mathbb{F}_{2^m}^\star, Tr_1^m(1/x)=1} \chi(g(D_3(x))) = -2$. But

$$\begin{aligned}
&\sum_{x \in \mathbb{F}_{2^m}^\star, Tr_1^m(1/x)=1} \chi(g(D_3(x))) \\
&= \sum_{x \in \mathbb{F}_{2^m}^\star} \chi(Tr_1^m(a(x^3+x))) - \sum_{x \in \mathbb{F}_{2^m}^\star, Tr_1^m(1/x)=0} \chi(Tr_1^m(a(x^3+x))) \\
&= C_m(a,a) - 1 - \sum_{x \in \mathbb{F}_{2^m}^\star, Tr_1^m(1/x)=0} \chi(Tr_1^m(a(x^3+x))) \\
&= C_m(a,a) - 1 - \sum_{x \in \mathbb{F}_{2^m}^\star, Tr_1^m(1/x)=0} \chi(Tr_1^m(ax)).
\end{aligned}$$

In the last equality, we use that the mapping $x \mapsto D_3(x) := x^3 + x$ is a permutation on the set of $\mathbb{F}_{2^m}^\star$ such that $Tr_1^m(1/x) = 0$ (see for instance [6, Lemma 7]). Now, according to Charpin, Helleseth and Zinoviev [6],

$$\sum_{x \in \mathbb{F}_{2^m}^\star, Tr_1^m(1/x)=0} \chi(Tr_1^m(ax)) = \frac{K_m(a)}{2} - 1.$$

Hence, we get that
$\sum_{x \in \mathbb{F}_{2^m}^\star, Tr_1^m(1/x)=1} \chi(g(D_3(x))) = C_m(a,a) - \frac{K_m(a)}{2}$. Therefore, f_β (resp. f_{β^2})

is hyper-bent if and only if $K_m(a) - 2C_m(a,a) = 4$. The mapping $x \mapsto x^3$ being a permutation on $\mathbb{F}_{2^m}$ for m odd, then every element $a \in \mathbb{F}_{2^m}$ can be (uniquely) written as $a = a'^3$ with $a' \in \mathbb{F}_{2^m}$. One has $C_m(a,a) = \sum_{x\in\mathbb{F}_{2^m}} \chi(Tr_1^m((a'x)^3 + ax) = C_m(1, a^{2/3})$.

Hence, according to Proposition 6 (note that $Tr_1^m(a^{2/3}) = Tr_1^m(a^{1/3})$), the function f_β (resp. f_{β^2}) is hyper-bent if and only if,

$$K_m(a) = \begin{cases} 4 \text{ if } Tr_1^m(a^{1/3}) = 0 \\ 4 \pm \left(\frac{2}{m}\right) 2^{(m+3)/2} \text{ if } Tr_1^m(a^{1/3}) = 1 \end{cases}$$

However, using Proposition 5, the value $4 \pm \left(\frac{2}{m}\right) 2^{(m+3)/2}$ does not belong to $[-2^{(m+2)/2}+1, 2^{(m+2)/2}+1]$ for every $m > 3$. This proves that if $Tr_1^m(a^{1/3}) = 0$ then, the Boolean function f_β (resp. f_{β^2}) is hyper-bent whenever $K_m(a) = 4$ while, when $K_m(a) \neq 4$, f_β (resp. f_{β^2}) is not hyper-bent. Otherwise, if $Tr_1^m(a^{1/3}) = 1$ (which implies that $K_m(a) \neq 4$) then, the function f_β (resp. f_{β^2}) cannot be hyper-bent when $m > 3$.

In the other hand, according to Theorem 15, f_1 is hyper-bent if and only if, $2\sum_{x\in\mathbb{F}_{2^m}^\star, Tr_1^m(x^{-1})=1} \chi\Big(g(D_3(x))\Big) - 3\sum_{x\in\mathbb{F}_{2^m}^\star, Tr_1^m(x^{-1})=1} \chi\Big(g(x)\Big) = 2$.
We have seen that $\sum_{x\in\mathbb{F}_{2^m}^\star, Tr_1^m(1/x)=1} \chi(g(D_3(x))) = C_m(a,a) - \frac{K_m(a)}{2}$.
Furthermore, according to Charpin, Helleseth and Zinoviev [6],
$\sum_{x\in\mathbb{F}_{2^m}^\star, Tr_1^m(x^{-1})=1} \chi\Big(g(x)\Big) = \sum_{x\in\mathbb{F}_{2^m}^\star, Tr_1^m(1/x)=1} \chi(Tr_1^m(ax)) = -\frac{K_m(a)}{2}$.
Therefore, f_1 is hyper-bent if and only if $K_m(a) + 4C_m(a,a) = 4$.

Now, one has $C_m(a,a) = C_m(1, a^{2/3})$. Hence, according to Proposition 6, f_1 is hyper-bent if and only if,

$$K_m(a) = \begin{cases} 4 \text{ if } Tr_1^m(a^{1/3}) = 0 \\ 4 \pm \left(\frac{2}{m}\right) 2^{(m+5)/2} \text{ if } Tr_1^m(a^{1/3}) = 1 \end{cases}$$

However, using Proposition 5, the value $4 \pm \left(\frac{2}{m}\right) 2^{(m+5)/2}$ does not belong to $[-2^{(m+2)/2}+1, 2^{(m+2)/2}+1]$ for every $m > 3$. This proves that if $Tr_1^m(a^{1/3}) = 0$ then, the Boolean function f_1 is hyper-bent whenever $K_m(a) = 4$ while, when $K_m(a) \neq 4$, f_1 is not hyper-bent. Otherwise, if $Tr_1^m(a^{1/3}) = 1$ (which implies that $K_m(a) \neq 4$) then, the function f_1 cannot be hyper-bent when $m > 3$. One recovers then the results given in [15] (Theorem 12).

Example 2. To illustrate again our results, let consider the set of functions of a particular family of Boolean functions belonging to the subclass (2), that is, the Boolean functions h_β (studied in [17]) defined on $\mathbb{F}_{2^n}$ ($n = 2m$, m odd) as:

$$h_\beta(x) = Tr_1^n(ax^{3(2^m-1)}) + Tr_1^2(\beta x^{\frac{2^n-1}{3}}), \quad \forall x \in \mathbb{F}_{2^n}$$

where $a \in \mathbb{F}_{2^m}^\star$ and β is a primitive element of $\mathbb{F}_4$. Suppose $m \not\equiv 3 \pmod 6$. According to Proposition 14 and the results of Example 1, one can deduce that if $Tr_1^m(a^{1/3}) = 0$ then, the Boolean function h_β is hyper-bent whenever $K_m(a) = 4$ and if $Tr_1^m(a^{1/3}) = 1$ then, the Boolean function h_β is not hyper-bent. Thus, one recovers the results given in [17] (Theorem 17).

Table 1. Exponents i and j such that (α^i, α^j) satisfy Conjecture 1 for $n = 10$

i=1	j= 0, 1, 2, 3, 5, 7, 8, 9, 11, 12, 13, 14, 17, 20, 22, 24, 26, 27, 29
i=2	j= 0, 2, 3, 4, 6, 9, 10, 13, 14, 16, 17, 18, 21, 22, 23, 24, 26, 27, 28
i=4	j= 0, 1, 3, 4, 5, 6, 8, 11, 12, 13, 15, 17, 18, 20, 21, 23, 25, 26, 28
i=7	j= 0, 3, 4, 5, 7, 8, 10, 11, 12, 14, 16, 18, 19, 23, 26, 27, 28, 29, 30
i=8	j= 0, 2, 3, 5, 6, 8, 9, 10, 11, 12, 15 16, 19, 21, 22, 24, 25, 26, 30,
i=14	j= 0, 1, 5, 6, 7, 8, 10, 14, 15, 16, 20, 21, 22, 23, 24, 25, 27, 28, 29
i=16	j= 0, 1, 4, 6, 7, 10, 11 12, 13, 16, 17, 18, 19, 20, 21, 22, 24, 29, 30
i=19	j= 0, 4, 5, 6, 7, 8, 9, 13, 14, 15, 17, 18, 19, 21, 25, 27, 29, 2, 30
i=25	j= 0, 1, 2, 3, 4, 7, 9, 15, 18, 19, 20, 22, 23, 24, 25, 26, 28, 29, 30
i=28	j= 0, 1, 2, 9, 10, 11, 12, 13, 14, 15 16, 17, 19, 20, 23, 25, 27, 28, 30

Table 2. Number of pairs (a, a') such that $K_m(a) = 4$ and $\mathcal{S}(a, a') = -1$

n	14	18	22
Number of pairs	882	3978	13948

We now make a conjecture. We need for that to introduce some notations. Let $I := \{x \in \mathbb{F}_{2^m}^\star \mid x = c^3 + c, Tr_1^m(c^{-1}) = 1\}$ and set, for a, $a' \in \mathbb{F}_{2^m}$,

$$\mathcal{S}(a, a') := \sum_{x \in I} \chi(Tr_1^m(a(x + x^3) + a'x^5).$$

Conjecture 1. For every $a \in \mathbb{F}_{2^m}^\star$ such that $K_m(a) = 4$, the set $\mathfrak{S}_a = \{a' \in \mathbb{F}_{2^m}^\star \mid \mathcal{S}(a, a') = -1\}$ is non empty.

Fact 1. By a computer program, we have checked that the conjecture holds for all $n = 2m$ up to $n = 26$.

Proposition 17. *Let $n = 2m$ with m odd. Suppose that conjecture 1 holds. Let $a \in \mathbb{F}_{2^m}^\star$ such that $K_m(a) = 4$, $a' \in \mathfrak{S}_a$ ($\neq \emptyset$) and β is a primitive element of $\mathbb{F}_4$. Then, the Boolean function f defined on $\mathbb{F}_{2^n}$ whose polynomial form equals*

$$Tr_1^n((a + a')x^{3(2^m-1)}) + Tr_1^n(a'x^{5(2^m-1)}) + Tr_1^2(\beta x^{\frac{2^n-1}{3}})$$

is hyper-bent.

Proof. Let g be the Boolean function defined on $\mathbb{F}_{2^m}$ as

$$g(x) = Tr_1^m((a + a')D_3(x)) + Tr_1^m(a'D_5(x)).$$

According to Theorem 13,

$$f \text{ is hyper-bent if and only if } \sum_{x \in \mathbb{F}_{2^m}^\star, Tr_1^m(x^{-1})=1} \chi(g(D_3(x))) = -2.$$

Now, according to Charpin *et al. [6] (Lemma 6), the map* $x \mapsto D_3(x)$ *is* 3*-to-*1 *from* $\{x \in \mathbb{F}_{2^m} \setminus \mathbb{F}_2 \mid Tr_1^m(x^{-1}) = 1\}$ *to* $I := \{x \in \mathbb{F}_{2^m}^\star \mid x = c^3 + c, Tr_1^m(c^{-1}) = 1\}$. *Thus, the former condition can be reworded as* $1 + 3\sum_{x \in I} \chi(g(x)) = -2$ *that is,* $\sum_{x \in I} \chi(g(x)) = -1$. *Recall now that* $D_3(x) = x + x^3$ *and,* $D_5(x) = x + x^3 + x^5$. *So* $g(x) = Tr_1^m\big(a(x + x^3) + a'x^5\big)$.

Remark 3. We have made an exhaustive search by a computer program for $n \in \{10, 14, 18, 22\}$ of all sets $\mathfrak{S}_a$ for each value a such that $K_m(a) = 4$. Let ζ be a primitive element of $\mathbb{F}_{2^{10}}$ (whose minimal polynomial is $x^{10} + x^7 + 1$) and set $\alpha = \zeta^{33}$ (so that α is a primitive element of $\mathbb{F}_{2^5}$).

We list in Table 1 all the pairs of indices (i, j) such that $K_5(\alpha^i) = 4$ and $\alpha^j \in \mathfrak{S}_{\alpha^i}$. We have also found all pairs (i, j) for $n \in \{14, 18, 22\}$. Due to their number, we do not list them like for $n = 10$ but we only give in Table 2 the numbers of pairs that we found (including the case where $K_m(a) = 4$ and $S(a, 0) = -1$).

4 Conclusion

In this paper, we generalize the results of [15–17] to multiple trace terms functions. We provide several characterizations of hyper-bentness by means of exponential sums involving Dickson polynomials. The characterizations introduced in this paper provide new methods for exploring theoritically or by computer search for possible hyper-bent functions of the form (2). In this paper, we have restrict ourselves to the case where the coefficients a_r in (2) are in $\mathbb{F}_{2^m}$. A natural expansion of those characterizations should be to investigate their generalizations to the case where some of the coefficients are in $\mathbb{F}_{2^n}$, but not in $\mathbb{F}_{2^m}$.

References

1. Canteaut, A., Charpin, P., Kyureghyan, G.: A New Class of Monomial Bent Functions. Finite Fields and Their Applications 14(1), 221–241 (2008)
2. Carlet, C.: Boolean Functions for Cryptography and Error Correcting Codes. In: Crama, Y., Hammer, P.L. (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.: Hyperbent functions and cyclic codes. Journal of Combinatorial Theory, Series A 113(3), 466–482 (2006)
4. Carlitz, L.: Explicit evualation of certain exponential sums. Math. Scand. 44, 5–16 (1979)
5. Charpin, P., Gong, G.: Hyperbent functions, Kloosterman sums and Dickson polynomials. IEEE Trans. Inform.Theory 9(54), 4230–4238 (2008)
6. Charpin, P., Helleseth, T., Zinoviev, V.: Divisibility properties of Kloosterman sums over finite fields of characteristic two. In: ISIT 2008, Toronto, Canada, July 6–11, 2008, pp. 2608–2612 (2008)
7. Charpin, P., Kyureghyan, G.: Cubic monomial bent functions: A subclass of $\mathcal{M}$. SIAM, J. Discr. Math. 22(2), 650–665 (2008)
8. Dillon, J.: Elementary Hadamard difference sets. PhD dissertation, University of Maryland (1974)

9. Dillon, J.F., Dobbertin, H.: New cyclic difference sets with Singer parameters. Finite Fields and Their Applications 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. Journal of Combinatorial therory, Serie A 113, 779–798 (2006)
11. Gold, R.: Maximal recursive sequences with 3-valued recursive crosscorrelation functions. IEEE Trans. Inform. Theory 14(1), 154–156 (1968)
12. Gologlu, F.: Almost Bent and Almost Perfect Nonlinear Functions, Exponential Sums, Geometries ans Sequences. PhD dissertation, University of Magdeburg (2009)
13. Lachaud, G., Wolfmann, J.: The weights of the orthogonals of the extended quadratic binary Goppa codes. IEEE Trans. Inform. Theory 36(3), 686–692 (1990)
14. Leander, G.: Monomial Bent Functions. IEEE Trans. Inform. Theory 2(52), 738–743 (2006)
15. Mesnager, S.: A new class of bent and hyper-bent boolean functions in polynomial forms. Journal Design, Codes and Cryptography (in press)
16. Mesnager, S.: A new class of bent boolean functions in polynomial forms. In: Proceedings of international Workshop on Coding and Cryptography, WCC 2009, pp. 5–18 (2009)
17. Mesnager, S.: A new family of hyper-bent boolean functions in polynomial form. In: Parker, M.G. (ed.) IMACC 2009. LNCS, vol. 5921, pp. 402–417. Springer, Heidelberg (2009)
18. Rothaus, O.: On "bent" functions. J. Combin. Theory Ser. A 20, 300–305 (1976)
19. Youssef, A.M., Gong, G.: Hyper-bent functions. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 406–419. Springer, Heidelberg (2001)
20. Yu, N.Y., Gong, G.: Construction of quadratic Bent functions in polynomial forms. IEEE Trans. Inform. Theory 7(52), 3291–3299 (2006)