A NEW CLASS OF BENT FUNCTIONS IN POLYNOMIAL FORMS

SIHEM MESNAGER

ABSTRACT. This paper is a contribution to the construction of bent functions having the form $f(x) = Tr_1^{o(s_1)}(ax^{s_1}) + Tr_1^{o(s_2)}(bx^{s_2})$ where $o(s_i)$ denotes the cardinality of the cyclotomic class of 2 modulo 2^n-1 which contains i and whose coefficients a and b are, respectively in $F_{2^{o(s_1)}}$ and $F_{2^{o(s_2)}}$. Many constructions of monomial bent functions are presented in the literature but very few are known even in the binomial case.

We prove that the exponents $s_1 = 2^{\frac{n}{2}} - 1$ and $s_2 = \frac{2^n-1}{3}$, where $a \in \mathbb{F}_{2^n}$ and $b \in \mathbb{F}_4$ provide the construction of new infinite class of bent functions over $\mathbb{F}_{2^n}$ with maximum algebraic degree. For m odd, we give an explicit characterization of the bentness of these functions, in terms of the Kloosterman sums of the corresponding coefficients. For m even, we give a necessary condition in terms of these Kloosterman sums.

Keywords. Boolean function, Bent functions, Maximum nonlinearity, Walsh-Hadamard transformation, Kloosterman sums.

1. INTRODUCTION

Bent functions, introduced by Rothaus [22], are maximally nonlinear Boolean functions (that is, achieve maximum distance to all affine functions) with even number $n = 2m$ of variables. Bent functions have been widely studied because of their interesting algebraic and combinatorial properties and also because of their applications in cryptography (design of stream ciphers), coding theory (Reed-Muller codes) and sequence design. The current results on the properties and constructions of bent functions can be found for instance in [3].

Some infinite classes of bent functions have been obtained, thanks to the identification between the vectorspace $\mathbb{F}_2^n$ and the field $\mathbb{F}_{2^n}$. There exist essentially two kinds of representations for a Boolean function f defined on a finite field $\mathbb{F}_{2^n}$ (see [3]). The first one called *absolute trace representation* of f, that is, an expression of f in terms of absolute trace function (that is, trace function on $\mathbb{F}_{2^n}$). The second one is called *univariate polynomial representation* of f, that is, an expression of f as a univariate polynomial over $\mathbb{F}_{2^n}$ with some conditions on its coefficients (in fact, such representation comes from the univariate polynomial representation

Date: December 5, 2008.

MAATICAH, Department of Mathematics, University of Paris VIII.
email : mesnager@math.jussieu.fr.

of a mapping from $\mathbb{F}_{2^n}$ to it self and, in this case, the representation is unique. The condition so that such a mapping is Boolean implies conditions on the coefficients of its associate univariate polynomial). While gathering the terms, we obtain Boolean functions of the form $\sum_j Tr_1^{o(j)}(a_j x^{s_j})$, so called *polynomial form* or *trace representation*, where $o(j)$ is the size of the cyclotomic class of 2 modulo 2^n-1 containing a positive integer j, and a_j an element of the Galois field $\mathbb{F}_{2^{o(j)}}$ of order $o(j)$.

Currently, the general structure of bent functions on $\mathbb{F}_{2^n}$ is not yet clear. In particular a complete classification of the bent functions is elusive and looks hopeless. A number of recent research works in the theory of bent functions was devoted to the description of new classes of bent functions, expressed by means of trace-functions. A non exhaustive list of references is [15, 11, 19, 12, 20, 14, 24, 9, 2, 6]. The most studied family is that whose expression is the absolute trace of a single power function, so called *monomial* Boolean functions. The complete classification of monomial bent functions is not yet achieved. The list of such functions known can be found in [1].

Very little is known on the characterization of bentness of functions whose expression is the absolute trace of linear combination of serval power functions.

In a recent paper [6], Charpin and Gong gave a characterization of the bentness of the Boolean functions defined on $\mathbb{F}_{2^n}$ of the form : $f(x)=\sum_{r\in E} Tr_1^n(\beta_r x^{r(2^m-1)})$, where E is a subset of the set of representatives of the cyclotomic cosets modulo 2^m+1 of size n, and the coefficients β_r are in $\mathbb{F}_{2^n}$. With some restriction, they showed that the bentness of those functions is related to the Dickson polynomials. The precise characterization of such functions which are bent, by giving explicitly the coefficients β_r, is still an open problem (see [6]).

Very little is known even in the particular case of *binomial* functions, that is, functions whose expression is the absolute trace of linear combination two particular power functions. The known example of such family is given by Dobbertin et.al in [14], in which, three families of binomial functions whose expression is the absolute trace of linear combinations of two Niho power functions, containing bent functions: $s_1=(2^{\frac{n}{2}}-1)\frac{1}{2}+1$ and $s_2=(2^{\frac{n}{2}}-1)3+1$, $s_2=(2^{\frac{n}{2}}-1)\frac{1}{4}+1$ ($\frac{n}{2}$ odd) or $s_2=(2^{\frac{n}{2}}-1)\frac{1}{6}+1$ ($\frac{n}{2}$ even).

A class of quadratic functions defined on $\mathbb{F}_{2^n}$ in polynomial forms whose expression has the form: $f(x)=\sum_{i=1}^{\frac{n}{2}-1} a_i Tr_1^n(x^{1+2^i})+a_{n/2}Tr_1^{\frac{n}{2}}(x^{2^{n/2}+1})$ with $a_i\in\mathbb{F}_2$, for $i\in\{1,\cdots,n/2\}$, was considered in several papers, in which, the authors investigate on the conditions of the choice of the coefficients a_i for explicit definition of new infinite class of quadratic bent functions. A non exhaustive list of references which deals with the characterization of the bentness of this class is [17, 23, 18, 21, 10, 24, 16].

Almost all the known bent trace-functions are restricted with the cyclotomic classes of maximum size. In the goal to find new expressions of bent Boolean

functions on finite fields, the representation of the form $\sum_j Tr_1^{o(j)}(a_j x^{s_j})$ seems to be the best adapted one because it does not exclude the trace (or absolute trace) of monomial and binomial functions of exponents of order n but included functions with traces of smaller natures (of order smaller than n) and then, allows us to seek bent functions more general than monomials and binomials bent functions. The simplest known example is the quadratic function $Tr_1^{n/2}(x^{2^{n/2}+1})$ which is bent ([17]). This brought us has to seek functions bent of the form $\sum_j Tr_1^{o(j)}(a_j x^{s_j})$ where $o(s_i)$ denotes the cardinality of cyclotomic class of 2 modulo 2^n-1 containing i and whose coefficients a_j are in the finite field $F_{2^{o(s_j)}}$. The characterization of the exponents s_i and the corresponding coefficients a_j defining a bent function on $\mathbb{F}_{2^n}$ is a difficult open problem. In this paper, we restrict ourselves to the class functions defined on $\mathbb{F}_{2^n}$ whose expression are written as the sum of two traces function, that is, which the expression is of the form : $f(x) = Tr_1^{o(s_1)}(a_1 x^{s_1}) + Tr_1^{o(s_2)}(a_2 x^{s_2})$, where the coefficients a_i are elements of $\mathbb{F}_{2^{o(s_i)}}$, $i = 1, 2$ ($o(s_i)$ are necessary dividers of n).

Our main result in this paper is to present a new class of bent functions in polynomial forms. This class was initially found (for small values of n, because of the complexity of the problem) with the help of computer experiments.

The paper is organized as follows. In Section 2, we fix our main notation and recall the necessary background. Next, in Section 3, we focus on the class of Boolean functions of the form $f(x) = Tr_1^{o(s_1)}(a_1 x^{s_1}) + Tr_1^{o(s_2)}(a_2 x^{s_2})$. We study a particular subclass given with its explicit exponents s_i and we investigate the conditions on the choice of a_1 and a_2 for obtaining an new explicit family of bent functions.

2. Notation and Preliminaries

$|E|$ will denote the cardinality of a set E.
Let n be a positive integer. $\mathbb{F}_2^n$ denotes the vectorspace over the prime field $\mathbb{F}_2$ equal to the set of all binary n-tuples.

- Boolean functions and trace presentation (or polynomial form): A Boolean function f is an $\mathbb{F}_2$-valued function on the vectorspace $\mathbb{F}_2^n$ of n-tuples of elements from $\mathbb{F}_2$. We shall need a representation of Boolean functions by univariate polynomials over the Galois field $\mathbb{F}_{2^n}$ of order 2^n. For that, we identify the field $\mathbb{F}_{2^n}$ with $\mathbb{F}_2^n$ by choosing a basis of $\mathbb{F}_{2^n}$, viewed as vector space over $\mathbb{F}_2$. For any function f over $\mathbb{F}_{2^n}$, the *weight* of f, denoted by $wt(f)$, is the Hamming weight of the image vector of f, that is, the cardinality of its support $\{x \in \mathbb{F}_{2^n} \mid f(x) = 1\}$.

  We denote the *absolute trace* over $\mathbb{F}_2$ of an element $x \in \mathbb{F}_{2^n}$ by $Tr_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$. The function Tr_1^n from $\mathbb{F}_{2^n}$ to its prime field $\mathbb{F}_2$ is $\mathbb{F}_2$-linear and satisfies $(Tr_1^n(x))^2 = Tr_1^n(x) = Tr_1^n(x^2)$ for every $x \in \mathbb{F}_{2^n}$. The function $(x, y) \to Tr_1^n(xy)$ is an inner product in $\mathbb{F}_{2^n}$. For any positive integers 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:

$$\forall x \in \mathbb{F}_{2^k}, \quad Tr_r^k(x) := \sum_{i=0}^{\frac{k}{r}-1} x^{2^{ri}} = x + x^{2^r} + x^{2^{2r}} + \cdots + x^{2^{k-r}}$$

Recall that, for every integer r dividing k, the trace function Tr_r^k satisfies the transitivity property, that is, $Tr_1^k = Tr_1^r \circ Tr_r^k$.

Now, recall that the cyclotomic class of 2 modulo $2^n - 1$ containing a positive integer j, denoted by $\Gamma_n(j)$, is the set $\{j \times 2^i \text{ modulo}(2^n - 1), i \in \mathbb{N}\}$. We define then the set Γ_n, obtained by choosing one element in each cyclotomic class of 2 modulo 2^n-1, the most usual choice being the smallest element in each cyclotomic class, called the coset leader of the class. We denote $o(j)$ the cardinality of $\Gamma_n(j)$ ($o(j)$ is necessarily a divisor of n). Given a positive integer s, it is clear that x^s belong to $\mathbb{F}_{2^{o(s)}}$ for all x of $\mathbb{F}_{2^n}$, since $x^{2^{o(s)}s} = x^s$.

Given an integer e, $0 \leq e \leq 2^n - 1$, having the binary expansion: $e = \sum_{i=0}^{n-1} e_i 2^i$, $e_i \in \{0, 1\}$, the 2-weight of e, denoted by $w_2(e)$, is the Hamming weight of the binary vector $(e_0, e_1, \cdots, e_{n-1})$. Note that when the integers modulo $2^n - 1$ are partitioned into cyclotomic classes of 2 modulo $2^n - 1$, all the elements in a cyclotomic class have the same 2-weight.

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

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

called its trace representation, where $o(j)$ is the size of the cyclotomic coset $\Gamma_n(j) = \{j, j \cdot 2, \cdots, j \cdot 2^{o(j)-1}\}$ containing j.

The algebraic degree of f , denoted by $\deg(f)$, is equal to the maximum 2-weight of an exponent j for which $a_j \neq 0$.

- Walsh transform and bent functions:

The *"sign" function* of a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is the integer-valued function $\chi(f) := (-1)^f$. The *Walsh transform* of f is the discrete Fourier transform of χ_f, whose value at $\omega \in \mathbb{F}_2^n$ equals by definition:

$$\widehat{\chi_f}(\omega) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+<x,\omega>}$$

where $< \cdot, \cdot >$ is the canonical scalar product in $\mathbb{F}_2^n$ defined by $< x, y >= \sum_{i=1}^n x_i y_i$ for every $x = (x_1, \cdots, x_n) \in \mathbb{F}_2^n$ and $y = (y_1, \cdots, y_n) \in \mathbb{F}_2^n$. It satisfies Parseval's relation: $\sum_{\omega \in \mathbb{F}_2^n} \widehat{\chi_f}^2(\omega) = 2^{2n}$. As the notion of Walsh transform refers to a scalar product, it is convenient to choose the

isomorphism such that the canonical scalar product in $\mathbb{F}_2^n$ coincides with the scalar product in $\mathbb{F}_{2^n}$, which is the trace of the product: $< x, y >= Tr_1^n(xy)$ for all elements $x, y \in \mathbb{F}_{2^n}$. Then, the Walsh transform of $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is defined as follows:

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

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

Bent functions exist only for even n. From now on, throughout the whole paper, we assume that $n = 2m$ is even.

- Some additional background:

  Let x be an element of $\mathbb{F}_{2^n}$. The conjugate of x over a subfield $\mathbb{F}_{2^m}$ of $\mathbb{F}_{2^n}$ will be denoted by of $\bar{x} = x^{2^m}$ and the relative norm with respect to the quadratic field extension $\mathbb{F}_{2^n}/\mathbb{F}_{2^m}$ by $norm(x) = x\bar{x}$. Also, we denote by U the set $\{u \in \mathbb{F}_{2^n} \mid norm(u) = 1\}$, which is the group of $(2^m + 1)$-st root of unity. Note that since the multiplicative group of the field $\mathbb{F}_{2^n}$ is cyclic and $2^m + 1$ divides $2^n - 1$ then, the order of U is $2^m + 1$. Finally, note that the unit 1 is the single element in $\mathbb{F}_{2^m}$ of norm one and each non-zero element x of $\mathbb{F}_{2^n}$ has a unique decomposition as: $x = \lambda u$ with $\lambda \in \mathbb{F}_{2^m}$ et $u \in U$.
  We also need to define two exponential sums on $\mathbb{F}_{2^n}$:

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

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

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

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

3. A new family $\mathfrak{F}_n$ of bent Boolean functions

Let $n = 2m$ be a even positive integer. We consider the subfamily of $\mathfrak{B}_n$ composed of the Boolean functions defined over $\mathbb{F}_{2^n}$ of the form

$$\forall x \in \mathbb{F}_{2^n}, \quad f_{a,b}(x) = Tr_1^n(ax^{2^m-1}) + Tr_1^2(bx^{\frac{2^n-1}{3}}). \tag{2}$$

where $a \in \mathbb{F}_{2^n}^\star$ and $b \in \mathbb{F}_4$

We denote by $\mathfrak{F}_n$ the set of functions $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ whose expression has the form given in (2).

Proposition 1. *The algebraic degree of any function $f_{a,b}$ belonging to $\mathfrak{F}_n$ is m (that is, the maximal algebraic degree of a bent function).*

Proof. The algebraic degree of $x \mapsto Tr_1^n(ax^{2^m-1})$ is equal to m since the 2-weight $w_2(2^m-1)$ is equal to m (since $2^m-1 = 1+2+2^2+\cdots+2^{m-1}$). Likewise, the algebraic degree of $x \mapsto Tr_1^2(bx^{\frac{2^n-1}{3}})$ is equal to m, since we have $\frac{2^n-1}{3} = 1+4+\cdots+4^{m-1}$. Since $Tr_1^n(ax^{2^m-1})$ and $Tr_1^2(bx^{\frac{2^n-1}{3}})$ are two separate parts in the trace representation of the function, the algebraic degree of $Tr_1^n(ax^{2^m-1}) + Tr_1^2(bx^{\frac{2^n-1}{3}})$ is the maximum of those of $Tr_1^n(ax^{2^m-1})$ and of $Tr_1^2(bx^{\frac{2^n-1}{3}})$, that is, equal to $\frac{n}{2} = m$. □

Remark 1. In the case where $b = 0$, it has been shown in [11, 13] that $f_{a,0}$, $a \in \mathbb{F}_{2^n}^\star$, is bent if and only if $K_n(a) = 0$, where K_n denotes the Kloosterman sum.

From now on, we assume that $b \neq 0$.

Lemma 1. *Let $a \in \mathbb{F}_{2^n}^\star$, $b \in \mathbb{F}_4^\star$ and $\lambda \in \mathbb{F}_{2^n}^\star$. Then $f_{a\lambda^{2^m-1},b}$ is bent if and only if $f_{a,b\lambda^{-\frac{2^n-1}{3}}}$ is bent*

Proof. Recall that $f_{a,b}(x)$ has the form $Tr_1^n(ax^{2^m-1}) + Tr_1^2(bx^{\frac{2^n-1}{3}})$.

One has, $f_{a\lambda^{2^m-1},b}(x) = Tr_1^n(a\lambda^{2^m-1}x^{2^m-1}) + Tr_1^2(bx^{\frac{2^n-1}{3}}) = Tr_1^n(a(\lambda x)^{2^m-1}) + Tr_1^2(b\lambda^{-\frac{2^n-1}{3}}(\lambda x)^{\frac{2^n-1}{3}}) = f_{a,b\lambda^{-\frac{2^n-1}{3}}}(\lambda x)$. Thus, $f_{a\lambda^{2^m-1},b}$ and $f_{a,b\lambda^{-\frac{2^n-1}{3}}}$ are linearly equivalent. □

Corollary 1. Let $a \in \mathbb{F}_{2^m}^\star$ and $u \in U$. Then, $f_{au,b}$ is bent if and only if $f_{a,b\lambda^{-\frac{2^n-1}{3}}}$ is bent where λ denotes the unique element of U such that $u = \lambda^{2^m-1}$.

Corollary 1 says that we can restrict ourselves to study only the case where $a \in \mathbb{F}_{2^m}^\star$. We denote by $\tilde{\mathfrak{F}}_n$ the class of functions belonging to $\mathfrak{F}_n$, with $a \in \mathbb{F}_{2^m}^\star$. We will search for a characterization of bentness for functions belonging to the family $\tilde{\mathfrak{F}}_n$.

Let us explain why we need to study separately the case where m is odd and the case where m is even.

Recall that functions in the class considered by Charpin et Gong in [6] are of the form :

$$\forall x \in \mathbb{F}_{2^n}, \quad f(x) = \sum_{r \in E} Tr_1^n(\beta_r x^{r(2^m-1)}) \tag{3}$$

where E is a subset of the set of representatives of the cyclotomic cosets modulo 2^m+1 of size n, and the coefficients β_r are in $\mathbb{F}_{2^n}$

When m is odd, Boolean functions (2) lie in the class (3). Indeed, let $\lambda \in \mathbb{F}_{2^n}$. Thanks to transitivity property of trace functions, we have $Tr_1^n(\lambda x^{\frac{2^n-1}{3}}) = Tr_1^2 \circ Tr_2^n(\lambda x^{\frac{2^n-1}{3}}) = Tr_1^2(x^{\frac{2^n-1}{3}} Tr_2^n(\lambda))$ (since $x^{\frac{2^n-1}{3}} \in \mathbb{F}_4$). Thus, if we put $b = Tr_2^n(\lambda) \in \mathbb{F}_4$ then $Tr_1^n(\lambda x^{\frac{2^n-1}{3}}) = Tr_1^2(bx^{\frac{2^n-1}{3}})$, and then, $\{Tr_1^n(ax^{2^m-1} + \lambda x^{\frac{2^n-1}{3}})$, $a \in \mathbb{F}_{2^n}^\star$, $\lambda \in \mathbb{F}_{2^n}\} \subset \mathfrak{F}_n$. Conversely, if $f \in \mathfrak{F}_n$ then $f(x)$ can be written

in the form $Tr_1^n(ax^{2^m-1}+\lambda x^{\frac{2^n-1}{3}})$, with $a\in\mathbb{F}_{2^n}^\star$,and $\lambda\in\mathbb{F}_{2^n}$ (since, the (linear) mapping Tr_2^n form $\mathbb{F}_{4^m}$ to $\mathbb{F}_4$ is surjective). Therefore $\mathfrak{F}_{\mathfrak{n}}$ is a subclass of that of the form (3). In this case, their support can be written as

$$supp(f_{a,b})=\bigcup_{u\in V_{a,b}} u\mathbb{F}_{2^m}^\star$$

where $U=\{u\in\mathbb{F}_{2^n}\mid norm(u)=1\}$ and $V_{a,b}=\{u\in U\mid f_{a,b}(u)=1\}$ since

$$\begin{aligned}\forall(u,y)\in U\times\mathbb{F}_{2^m}^\star,\quad f_{a,b}(uy)&=Tr_1^n\big(au^{2^m-1}y^{2^m-1}\big)+Tr_1^2\big(bu^{\frac{2^n-1}{3}}y^{\frac{2^n-1}{3}}\big)\\&=Tr_1^n\big(au^{2^m-1}\big)+Tr_1^2\big(bu^{\frac{2^n-1}{3}}\big)\\&=f_{a,b}(u).\end{aligned}$$

The bentness of Boolean functions of type (2) can then be characterized by the Hamming weight of their restrictions to U as follows.

Proposition 2. *Let $a\in\mathbb{F}_{2^m}^\star$ (m odd) and $b\in\mathbb{F}_4^\star$. The Boolean function $f_{a,b}$ is bent if and only if $wt(f_{a,b}|_U)=2^{m-1}$.*

Now, if m is even (in this case 3 divides 2^m+1) then, a Boolean function of $\mathfrak{F}_{\mathfrak{n}}$ is not of the form (3) since, $x^{\frac{(2^m-1)}{3}}$ is not of the form $x^{(2^m+1)r}$ (with r integer). Moreover, one has in this case , for every $u\in U$ and $y\in\mathbb{F}_{2^m}^\star$,

$$\begin{aligned}f_{a,b}(uy)&=Tr_1^n\big(au^{2^m-1}y^{2^m-1}\big)+Tr_1^2\big(bu^{\frac{2^n-1}{3}}y^{\frac{2^n-1}{3}}\big)\\&=Tr_1^n\big(au^{2^m-1}\big)+Tr_1^2\big(by^{\frac{2^n-1}{3}}\big).\end{aligned}\tag{4}$$

The support of $f_{a,b}$ can not thus be written as in the odd case in the form $\bigcup_{i=1}^N E_i^\star$ where the E_i's are m-dimensional vector spaces of $\mathbb{F}_{2^n}$ such that $E_i\cap E_j=\{0\}$ for every pair (i,j). We can not thus use the characterization of bentness of Proposition 2 when m is even.

Remark 2. C. Carlet and P. Gaborit proved in [4] that any bent function (more precisely any hyper-bent, see definition for instance in [4]) of the form of (3), belongs to the class of belongs to the class PS_{ap} which is a subclass of partial spread's class PS^- (for definitions see for instance in [4])

3.1. **The odd case.** We assume in this subsection that m is odd and $a\in\mathbb{F}_{2^m}^\star$ (in this case 3 divides 2^m+1).

Let $g_{a,b}$ be the Boolean function defined on U by $g_{a,b}(u)=Tr_1^n(au)+Tr_1^2(bu^{\frac{2^m+1}{3}})$ for every u in U where $a\in\mathbb{F}_{2^m}^\star$ and $b\in\mathbb{F}_4^\star$.

One has $f_{a,b}(u)=g_{a,b}(u^{2^m-1})$ for every $u\in\mathbb{F}_{2^n}$. Then, one can reword the characterization of bentness of Proposition 2 as follows.

Proposition 3. *Let $a\in\mathbb{F}_{2^m}^\star$ and $b\in\mathbb{F}_4^\star$. Then*

1. *The Boolean function $f_{a,b}$ is bent if and only if $\Lambda(a,b):=\sum_{u\in U}\chi(g_{a,b}(u))=1$.*

(2) *Moreover, one has* $\Lambda(a,b)=\Lambda(a,b^2)$ *and thus that* $f_{a,b}$ *is bent if and only if* f_{a,b^2} *is bent.*

Proof.

(1) According to Proposition 2, the Boolean function $f_{a,b}$ is bent if and only if $wt(f_{a,b}|_U)=2^{m-1}$ which is equivalent to say that

$$\sum_{u\in U}\chi(f_{a,b}(u))=2^m+1-2wt(f_{a,b}|_U)=1.$$

On the other hand, $\sum_{u\in U}\chi(f_{a,b}(u))=\sum_{u\in U}\chi(g_{a,b}(u^{2^m-1}))=\sum_{u\in U}\chi(g_{a,b}(u))$ since the map $u\in U\mapsto u^{2^m-1}\in U$ is a permutation.

(2) For all $x\in\mathbb{F}_{2^k}$ $(k=2r)$, we have $Tr_1^k(x^{2^r})=Tr_1^k(x)$ (this comes by applying r times the equality $Tr_1^k(x^2)=Tr_1^k(x)$, for all $x\in\mathbb{F}_{2^k}$). Then, $\Lambda(a,b)=\sum_{u\in U}\chi(Tr_1^n(au)+Tr_1^2(bu^{\frac{2^m+1}{3}})=\sum_{u\in U}\chi(Tr_1^n(\bar{a}\bar{u})+Tr_1^2(\bar{b}\bar{u}^{\frac{2^m+1}{3}}))=\sum_{u\in U}\chi(Tr_1^n(a\bar{u})+Tr_1^2(b^2\bar{u}^{\frac{2^m+1}{3}}))$ (since $\bar{b}=b^2$ and $\bar{a}=a$). Hence, $\Lambda(a,b)=\sum_{u\in U}\chi(Tr_1^n(au)+Tr_1^2(b^2u^{\frac{2^m+1}{3}}))=\Lambda(a,b^2)$ (since the map $u\mapsto\bar{u}$ is a permutation on U).

□

Proposition 3 says that, given $a\in\mathbb{F}_{2^m}^\star$ and β a primitive element of $\mathbb{F}_4^\star$, only four situations may occur: the three Boolean functions $f_{a,1}$, $f_{a,\beta}$ and f_{a,β^2} are all bent, only the two Boolean functions $f_{a,\beta}$ and f_{a,β^2} are bent and $f_{a,1}$ is not bent, only the Boolean functions $f_{a,1}$ is bent and none of the two Boolean functions $f_{a,\beta}$ and f_{a,β^2} is not, none of the three Boolean functions $f_{a,1}$, $f_{a,\beta}$, f_{a,β^2} is bent.

Then question then arises from knowing, given an element b of $\mathbb{F}_4^\star$, for which values of $a\in\mathbb{F}_{2^m}^\star$, the Boolean function $f_{a,b}$ is bent. To this end, we begin with showing that, for every $a\in\mathbb{F}_{2^m}^\star$ and $b\in\mathbb{F}_4^\star$, $\Lambda(a,b)$ can be expressed by means of Kloosterman sums and the cubic sums (Definition 2) on $\mathbb{F}_{2^m}$.

Proposition 4. *Let* $a\in\mathbb{F}_{2^m}^\star$ *and* β *be a primitive element of* $\mathbb{F}_4$*. Then*

$$\begin{aligned}\Lambda(a,\beta)=\Lambda(a,\beta^2) &= \frac{K_m(a)-1-2C_m(a,a)}{3},\\ \Lambda(a,1) &= \frac{4C_m(a,a)+K_m(a)-1}{3}.\end{aligned}$$

Proof. Take $a\in\mathbb{F}_{2^m}^\star$. Let ζ be a primitive element of U. Set $V_0=\{u^3\mid u\in U\}$. Set, for every $a\in\mathbb{F}_{2^m}^\star$,

$$S_i(a) = \sum_{v\in V_0}\chi(Tr_1^n(a\zeta^i v)),\quad i\in\{0,1,2\},$$

Remark that $S_1(a)=\sum_{v\in V}\chi(Tr_1^n(a\zeta v))=\sum_{v\in V}\chi(Tr_1^n(a\bar{\zeta}\bar{v}))$ (since $Tr_1^n(x)=Tr_1^n(x^2)$, for all $x\in\mathbb{F}_{2^n}$ and , $\bar{x}=x^{2^m}$). Then, $S_1(a)=\sum_{v\in V}\chi(Tr_1^n(a\zeta^2(\zeta^{2^m-2}\bar{v})))=$

$S_2(a)$ since ζ^{2^m-2} is an element of V (because 3 divides 2^m+1) and $v \mapsto \zeta^{2^m-2}\bar{v}$ is a permutation on V.

The first step of the proof is to express the sums $\Lambda(a,1)$, $\Lambda(a,\beta)$ and $\Lambda(a,\beta^2)$ by means of $S_0(a)$, $S_1(a)$ and $S_2(a)$. To this end, we begin with splitting U as follows : $U = V_0 \cup \zeta V_0 \cup \zeta^2 V_0$ (union disjoint) since $U = \{\zeta^{3i+j},\ 0 \leq 3i+j \leq 2^m, 0 \leq i \leq \frac{2^m-2}{3}, 0 \leq j \leq 2\} = \cup_{j=0}^{2} \zeta^j \{\zeta^{3i},\ 0 \leq 3i \leq 2^m, 0 \leq i \leq \frac{2^m-2}{3}\}$. Therefore, for every $b \in \mathbb{F}_4^\star$, we have

$$\begin{aligned}\Lambda(a,b) := \sum_{u\in U} \chi(g_{a,b}(u)) &= \sum_{i=0}^{2}\sum_{v\in V_0} \chi(Tr_1^n(a\zeta^i v) + Tr_1^2(b\zeta^{i\frac{2^m+1}{3}})).\\ &= \sum_{i=0}^{2} \chi(Tr_1^2(b\zeta^{i\frac{2^m+1}{3}}))S_i(a).\end{aligned}$$

(since $v^{\frac{2^m+1}{3}} = 1$ for $v \in V_0$)

Now, one has $\beta = \zeta^{j\frac{2^m+1}{3}}$ with $j \in \{1,2\}$ and thus that

$$\begin{aligned}\Lambda(a,\beta) &= \chi(Tr_1^2(\zeta^{j\frac{2^m+1}{3}}))S_0(a)\\ &\quad + \big(\chi(Tr_1^2(\zeta^{(j+1)\frac{2^m+1}{3}})) + \chi(Tr_1^2(\zeta^{(j+2)\frac{2^m+1}{3}}))\big)S_1(a)\end{aligned}$$

from which we deduce that

$$\Lambda(a,\beta) = -S_0(a) \tag{5}$$

because $Tr_1^2(1) = 0$ and $Tr_1^2(\zeta^{\frac{2^m+1}{3}}) = 1$. From Proposition 3, we have also

$$\Lambda(a,\beta^2) = \Lambda(a,\beta) = -S_0(a). \tag{6}$$

On the other hand, one has

$$\Lambda(a,1) = \chi(Tr_1^2(1))S_0(a) + \big(\chi(Tr_1^2(\zeta^{\frac{2^m+1}{3}})) + \chi(Tr_1^2(\zeta^{2\frac{2^m+1}{3}}))\big)S_1(a)$$

form which we get

$$\Lambda(a,1) = S_0(a) - 2S_1(a). \tag{7}$$

The next step is to show that

$$S_0(a) + 2S_1(a) = 1 - K_m(a) \tag{8}$$

For that, we compute the sum $\sum_{b\in\mathbb{F}_4^\star} \Lambda(a,b)$ in two ways. Firstly, we have $\sum_{b\in\mathbb{F}_4^\star} \Lambda(a,b) = \sum_{u\in U} \chi(Tr_1^n(au)) \sum_{b\in\mathbb{F}_4^\star} \chi(Tr_1^2(bu^{\frac{2^m+1}{3}}))$. But $\sum_{b\in\mathbb{F}_4} \chi(Tr_1^2(\lambda b) = 0$ for every $\lambda \neq 0$ and thus that $\sum_{b\in\mathbb{F}_4^\star} \chi(Tr_1^2(\lambda b) = -1$. Then $\sum_{b\in\mathbb{F}_4^\star} \Lambda(a,b) = -\sum_{u\in U} \chi(Tr_1^n(au))$. Now, recall the well-known result, that is: $\sum_{u\in G} \chi(Tr_1^n(au)) = 1 - K_m(a)$, where G is a cyclic group of order 2^m+1 (different proofs can be found in [7], [12], [19], [20]). Take $G = U$ then, we obtain $\sum_{b\in\mathbb{F}_4^\star} \Lambda(a,b) = K_m(a) - 1$.
On the other hand, we have :

$\sum_{b\in\mathbb{F}_4^\star}\Lambda(a,b)=\sum_{i=0}^{2}\sum_{v\in V_0}\chi(Tr_1^n(a\zeta^i v))\sum_{b\in\mathbb{F}_4^\star}\chi(Tr_1^2(b\zeta^{i\frac{2^m+1}{3}}))=-\sum_{i=0}^{2}S_i(a)$ (because $\sum_{b\in\mathbb{F}_4}\chi(Tr_1^2(b\zeta^{i\frac{2^m+1}{3}}))=0$). Hence, $\sum_{b\in\mathbb{F}_4^\star}\Lambda(a,b)=-S_0(a)-2S_1(a)$.

Collecting together the two above equalities yield relation (8).

The last step is to show that

$$S_0(a)=\frac{2C_m(a,a)+1-K_m(a)}{3}. \tag{9}$$

First, recall that the map $x\mapsto x^3$ is 3-to-1 from $\mathbb{F}_{2^n}$ to itself since n is even. Moreover, since 3 divides 2^m+1, the group $\mathbb{F}_4^\star$ is contained in U. Therefore, the map $x\mapsto x^3$ is also 3-to-1 from U to itself. That implies in particular that

$$S_0(a):=\sum_{v\in V}\chi(Tr_1^n(av))=\frac{1}{3}\sum_{u\in U}\chi(Tr_1^n(au^3)).$$

Now, using the transitivity rule of trace function, we have $Tr_1^n(au^3)=Tr_1^m(Tr_m^n(au^3))=Tr_1^m(au^3+(au^3)^{2^m})$. Then

$$S_0(a)=\frac{1}{3}\sum_{u\in U}\chi(Tr_1^m(a(u^3+u^{-3}))).$$

Moreover, every element $1/c$ ($c\in\mathbb{F}_{2^m}$) with $Tr_1^m(c)=1$ can be uniquely represented as $u+\bar{u}$ with $u\in U$. Note now that $1/c^3+1/c=u^3+u^{-3}$. Therefore, we have

$$\begin{aligned}
3S_0(a) &= 1+\sum_{u\in U\setminus\{1\}}\chi(Tr_1^m(a(u^3+u^{-3})))\\
&= 1+2\sum_{c\in\mathbb{F}_{2^m},Tr_1^m(c)=1}\chi(Tr_1^m(a/c^3+a/c))\\
&= 1+2\sum_{c\in\mathbb{F}_{2^m},Tr_1^m(1/c)=1}\chi(Tr_1^m(ac^3+ac))
\end{aligned}$$

In the last equality , we use the fact that the map $c\mapsto 1/c$ is a permutation on $\mathbb{F}_{2^m}$. Now, Charpin and *al* [8, Theorem 3] have shown that $2\sum_{c\in\mathbb{F}_{2^m},Tr_1^m(1/c)=1}\chi(Tr_1^m(ac^3+ac))=2C_m(a,a)-K_m(a)$ from which we deduce (9).

From (5), (6) and (9), we get that

$$\Lambda(a,\beta)=\Lambda(a,\beta^2)=\frac{K_m(a)-1-2C_m(a,a)}{3}.$$

From (8), we deduce that $-2S_1(a)=S_0(a)+K_m(a)-1$ and thus, according to (7) and (9), that

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

□

The exact values of the cubic sums $C(a,a)$ on $\mathbb{F}_{2^m}$ can be computed thanks to a Carlitz's result [5] 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. The Jacobi symbol $\left(\frac{2}{m}\right)$ can be computed thanks to the explicit formula : $\left(\frac{2}{m}\right) = (-1)^{\frac{(m^2-1)}{8}}$.

Proposition 5. *([5]) Let m be odd. Recall that the cubic sums on $\mathbb{F}_{2^m}$ denoted by $C_m(a,b) := \sum_{x\in\mathbb{F}_{2^m}} \chi\big(Tr_1^m(ax^3+bx)\big)$ were $a \in \mathbb{F}_{2^m}^\star$ and $b \in \mathbb{F}_{2^m}$. Then we have:*

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

A precise version of the last point (3) is given in a recent paper ([7]). More precisely :
If $Tr_1^m(b) = 1$ and $a \neq 1$, then $C_m(1,a) = \chi(Tr_1^m(\gamma^3)) \left(\frac{2}{m}\right) 2^{(m+1)/2}$ where γ is the unique element of $\mathbb{F}_{2^m}$ satisfying $b = \gamma^4+\gamma+1$ and $Tr_1^m(\gamma) = 0$.

Lemma 2. *Let $a \in \mathbb{F}_{2^m}^\star$. Then we have:*

1. *If $Tr_1^m(a^{1/3}) = 0$ then $C_m(a,a) = 0$.*
2. *If $Tr_1^m(a^{1/3}) = 1$, then $C_m(a,a) = \epsilon_a \left(\frac{2}{m}\right) 2^{(m+1)/2}$ where $\left(\frac{2}{m}\right)$ is the Jacobi symbol and ϵ_a is defined as : $\epsilon_1 = 1$ and, for $a \neq 1$, $\epsilon_a = \chi(Tr_1^m(\gamma^3))$ where γ is the unique element of $\mathbb{F}_{2^m}$ satisfying $a^{1/3} = \gamma^4+\gamma+1$ and $Tr_1^m(\gamma) = 0$.*

Proof. The mapping $x \mapsto x^3$ is a permutation on $\mathbb{F}_{2^m}$ (since m is odd). Then every element a of $\mathbb{F}_{2^m}^\star$ can be (uniquely) written as $a = c^3$ with $c \in \mathbb{F}_{2^m}$. Therefore, $C_m(a,a) := \sum_{x\in\mathbb{F}_{2^m}} \chi\big(Tr_1^m(ax^3+ax)\big) = \sum_{x\in\mathbb{F}_{2^m}} \chi\big(Tr_1^m((cx)^3+a^{2/3}(cx))\big) = C_m(1,a^{2/3})$. We conclude thanks to the above results. □

Thanks to proposition 4 and lemma 2, we are able to identify the values of a for which the Boolean functions $f_{a,1}$, $f_{a,\beta}$ or f_{a,β^2} is bent.

Theorem 1. Let $a \in \mathbb{F}_{2^m}^\star$. Let β the primitive element of $\mathbb{F}_4$. With the notations of Lemma 2 we have:

1. Suppose $Tr_1^m(a^{1/3}) = 0$. if $K_m(a) = 4$ then $f_{a,1}$, $f_{a,\beta}$ and f_{a,β^2} are bent and, if $K_m(a) \neq 4$, $f_{a,1}$, $f_{a,\beta}$ and f_{a,β^2} are not bent
2. Suppose $Tr_1^m(a^{1/3}) = 1$. Then, $f_{a,\beta}$ and f_{a,β^2} are bent if and only if $K_m(a) = 4 + \epsilon_a \left(\frac{2}{m}\right) 2^{(m+3)/2}$ while, $f_{a,1}$ is bent if and only if $K_m(a) = 4 - \epsilon_a \left(\frac{2}{m}\right) 2^{(m+5)/2}$.

Proof. Take $a \in \mathbb{F}_{2^m}^\star$.
we have

(1) Suppose $Tr_1^m(a^{1/3}) = 0$. In this case, we have $C(a,a) = 0$ according to Lemma 2. We then deduce from Proposition 4 that

$$\Lambda(a,1) = \Lambda(a,\beta) = \Lambda(a,\beta^2) = \frac{K_m(a)-1}{3}.$$

Thus, the three Boolean functions $f_{a,1}$, $f_{a,\beta}$ and f_{a,β^2} are all bent whenever $K_m(a) = 4$ while, when $K_m(a) \neq 4$, none of them is bent.

(2) Suppose $Tr_1^m(a^{1/3}) = 1$. In this case, $C(a,a) = \epsilon_a \left(\frac{2}{m}\right) 2^{(m+1)/2}$. Thus, according to Proposition 4, we have

$$\begin{aligned}\Lambda(a,\beta) = \Lambda(a,\beta^2) &= \frac{K_m(a) - 1 - \epsilon_a \left(\frac{2}{m}\right) 2^{(m+3)/2}}{3},\\ \Lambda(a,1) &= \frac{K_m(a) - 1 + \epsilon_a \left(\frac{2}{m}\right) 2^{(m+5)/2}}{3}.\end{aligned}$$

□

Remark 3. When m is odd, the Walsh transform of bent Boolean functions of the form (2) can be computed. Firstly, we have $\widehat{\chi_{f_{a,b}}}(0) = 2^m$. Now, let w be an element of $\mathbb{F}_{2^n}^\star$. We have $\widehat{\chi_{f_{a,b}}}(w) = \sum_{x\in\mathbb{F}_{2^n}} \chi(f_{a,b}(x) + Tr_1^n(wx)) = 1 + \sum_{u\in U}\sum_{y\in\mathbb{F}_{2^m}^\star} \chi(f_{a,b}(yu)+Tr_1^n(wyu))$ (since every element x of $\mathbb{F}_{2^n}^\star$ has a unique decomposition as : $x = yu$, with $y \in \mathbb{F}_{2^m}^\star$ and $u \in U$). But $\sum_{u\in U}\sum_{y\in\mathbb{F}_{2^n}^\star} \chi(f_{a,b}(yu)) = \sum_{u\in U}\chi(f_{a,b}(u))$ (because 3 divides 2^m+1 (m odd) and $y^{2^m-1} = 1 = y^{\frac{2^n-1}{3}}$). Therefore, $\widehat{\chi_{f_{a,b}}}(w) = 1-\sum_{u\in U}\chi(f_{a,b}(u))+\sum_{u\in U}\chi(f_{a,b}(u))\sum_{y\in\mathbb{F}_{2^m}}\chi(Tr_1^n(wyu)))$
$= 1 - \sum_{u\in U}\chi(f_{a,b}(u)) + \sum_{u\in U}\chi(f_{a,b}(u))\sum_{y\in\mathbb{F}_{2^m}}\chi(Tr_1^m(yTr_m^n(wu)))$
$= 1 - \sum_{u\in U}\chi(f_{a,b}(u)) + 2^m\sum_{\substack{u\in U\\ Tr_m^n(wu)=0}}\chi(f_{a,b}(u))$. Note now that $Tr_m^n(wu) = 0$ if and only if $uw+u^{2^m}w^{2^m} = 0$, that is, $u^{2^m-1} = w^{1-2^m}$. Then, $\sum_{\substack{u\in U\\ Tr_m^n(wu)=0}}\chi(f_{a,b}(u)) = \chi(f_{a,b}(w^{-1}))|\{u \in U \mid u^{2^m-1} = \omega^{1-2^m}\}| = \chi(f_{a,b}(w^{-1}))$, since the mapping $x \mapsto x^{2^m-1}$ is a permutation of U. But f is being bent then, $\sum_{u\in U}\chi(f_{a,b}(u)) = 1$. We finally get $\widehat{\chi_{f_{a,b}}}(w) = 2^m\chi(f_{a,b}(w^{-1}))$.

3.2. **The even case.** Assume that m is even (in this case, 3 divides 2^m-1). Recall that we can restrict our self to $a \in \mathbb{F}_{2^m}^\star$. The situation is different from the preceding subsection since in this case, one has, for every $u \in U$ and $y \in \mathbb{F}_{2^m}^\star$,

$$\begin{aligned} f_{a,b}(uy) &= Tr_1^n\big(au^{2^m-1}y^{2^m-1}\big) + Tr_1^2\big(bu^{\frac{2^n-1}{3}}y^{\frac{2^n-1}{3}}\big)\\ &= Tr_1^n\big(au^{2^m-1}\big) + Tr_1^2\big(by^{\frac{2^n-1}{3}}\big)\end{aligned} \tag{10}$$

since $y^{2^m-1} = 1$, $u^{2^m+1} = 1$ and $\frac{2^n-1}{3} = (2^m+1)\cdot\frac{2^m-1}{3}$ (3 does not divides 2^m+1 as in the odd case). Therefore, unfortunately, the bentness of $f_{a,b}$ cannot be treated as in the odd case

The following result give a necessary condition on the corresponding coefficient a defining a bent functions belonging to the class $\mathfrak{F}_n$.

Theorem 2. Let $a \in \mathbb{F}_{2^m}^\star$ $(m > 2)$ and $b \in \mathbb{F}_4^\star$. Then we have:

$$(f_{a,b} \text{ is bent}) \Longrightarrow K_m(a) = 4.$$

where $K_m(a)$ denotes the Kloosterman sums on $\mathbb{F}_{2^m}$

Proof. Set $A_\epsilon = |\{u \in U \mid Tr_1^n(au^{2^m-1}) = \epsilon\}|$ and $B_\epsilon = |\{y \in \mathbb{F}_{2^m}^\star \mid Tr_1^2(by^{\frac{2^n-1}{3}}) = \epsilon\}|$ for every $\epsilon \in \mathbb{F}_2$. One then has, according to (4),

$$wt(f_{a,b}) = A_0B_1 + A_1B_0. \tag{11}$$

Let g be the map from $\mathbb{F}_{2^m}^\star$ to $\mathbb{F}_4^\star$ defined as : $\forall y \in \mathbb{F}_{2^m}^\star$, $g(y) = by^{\frac{2^n-1}{3}}$. Clearly, g is invariant under the map $c \mapsto c^3$, that is, $g(c^3y) = g(y)$ for every y and c in $\mathbb{F}_{2^m}^\star$. Thus $|g^{-1}(\alpha)|$ is a multiple of $\frac{2^m-1}{3}$ for every $\alpha \in \mathbb{F}_4^\star$. Now, since g is onto, one has necessarily $|g^{-1}(\alpha)| = \frac{2^m-1}{3}$ for every $\alpha \in \mathbb{F}_4^\star$. Thus, $B_1 = 2 \cdot \frac{2^m-1}{3}$ and $B_0 = \frac{2^m-1}{3}$. Replacing B_0 and B_1 by these values in (11), we get

$$wt(f_{a,b}) = \frac{2^m-1}{3}(A_1 + 2A_0) = \frac{2^m-1}{3}(2^m + 1 + A_0).$$

On the other hand, since $z \mapsto z^{2^m-1}$ is a permutation on U to itself, one has $A_1 = |\{u \in U \mid Tr_1^n(au) = 1\}|$. Then, $\sum_{u\in U} \chi(Tr_1^n(au)) = A_0 - A_1$. Recall now the well-known result used previously

$$\sum_{u\in U} \chi(Tr_1^n(au)) = 1 - K_m(a)$$

where K_m is the Kloosterman sums on $\mathbb{F}_{2^m}$. Since $A_0 + A_1 = 2^m + 1$, one thus has

$$A_0 = 2^{m-1} + 1 - \frac{K_m(a)}{2} \qquad (\text{and } A_1 = 2^{m-1} + \frac{K_m(a)}{2})$$

This leads to

$$wt(f_{a,b}) = \frac{2^m-1}{3}(3 \cdot 2^{m-1} + 2 - \frac{K_m(a)}{2}) = 2^{n-1} - 2^{m-1} + \frac{4 - K_m(a)}{6} \cdot (2^m - 1).$$

Therefore, $f_{a,b}$ can be bent only if $\frac{4-K_m(a)}{6} \cdot (2^m - 1) \in \{0, 2^m\}$. Assume that $\frac{4-K_m(a)}{6} \cdot (2^m - 1) = 2^m$. That implies that $2^m - 1$ divides $6 \cdot 2^m$. Now, since 2^m and $2^m - 1$ are co-prime, one has $2^m - 1|6$ which requires that $m = 2$. Hence, if $m \geq 4$, one has finally: if $K_m(a) \neq 4$ then $f_{a,b}$ is not bent.

□

References

[1] A. Canteaut. Analysis and disign of symetric ciphers. In *Habilitation for directing Theses, Unversity of Paris 6*, 2006.

[2] A. Canteaut, P. Charpin, and G. Kyureghyan. A new class of monomial bent functions. In *Finite Fields and Their Applications, Vol 14, no. 1*, pages 221–241, 2008.

[3] C. Carlet. Boolean functions for cryptography and error correcting codes. In *in: Y. Crama, P. Hammer (Eds.), Boolean methods and model, Cambridge Univ. Press, in press.*

[4] C. Carlet and P. Gaborit. Hyperbent functions and cyclic codes. In *Journal of Combinatorial Theory, Series A, Vol 113, no. 3*, pages 466–482, 2006.

[5] L. Carlitz. Explicit evualation of certain exponential sums. *Math. Scand.*, 44:5–16, 1979.

[6] P. Charpin and G. Gong. Hyperbent functions, kloosterman sums and dickson polynomials. In *IEEE Trans. Inform. Theory (54) 9*, pages pp. 4230–4238, 2008.

[7] P. Charpin, T. Helleseth, and V. Zinoviev. The divisibility modulo 24 of Kloosterman sums of $GF(2^m)$, m odd. *Journal of Combinatorial Theory, Series A*, 114:322–338, 2007.

[8] P. Charpin, T. Helleseth, and V. Zinoviev. Divisibility properties of Kloosterman sums over finite fields of characteristic two. In *ISIT 2008, Toronto, Canada, July 6 – 11*, pages 2608–2612, 2008.

[9] P. Charpin and G. Kyureghyan. Cubic monomial bent functions: A subclass of $\mathcal{M}$. In *SIAM, J. Discr. Math., Vol.22, no.2*, pages 650–665, 2008.

[10] P. Charpin, E. Pasalic, and C. Tavernier. On bent and semi-bent quadratic boolean functions. In *IEEE Trans. Inform. Theory, vol. 51, no. 12*, pages 4286–4298, 2005.

[11] J. Dillon. Elementary hadamard difference sets. In *PhD dissertation, University of Maryland*, 1974.

[12] J. Dillon and H. Dobbertin. New cyclic difference sets with singer parameters. In *Finite Fields Appl. 10*, pages 342–389, 2004.

[13] J. F. Dillon. Elementary hadamard difference sets, 1975.

[14] H. Dobbertin, G. Leander, A. Canteaut, C. Carlet, P. Felke, and P. Gaborit. Construction of bent functions via niho power functions. In *Journal of Combinatorial therory, Serie A 113*, pages 779–798, 2006.

[15] R. Gold. Maximal recursive sequences with 3-valued recursive crosscorrelation functions. In *IEEE Trans. Inform. Theory 14 (1)*, pages 154–156, 1968.

[16] H.Hu and D. Feng. On quadratic bent functions in polynomial forms. In *IEEE Trans. Inform. Theory 53 (7), pp. 2610-2615*, pages 2610–2615, 2007.

[17] T. Kassami. Weight enumerators for sevral classes of subcodes of the 2nd-order reed-muller codes. In *Information control, Vol 18*, pages 369–394, 1971.

[18] S. H. Kim and J. S. No. New families of binary sequences with low correlation. In *IEEE Trans. Inform. Theory, vol. 49, no. 11*, pages 3059–3065, 2003.

[19] G. Lachaud and J. Wolfmann. The weights of the orthogonals of the extended quadratic binary goppa codes. In *IEEE Trans. Inform. Theory 36 (3)*, pages 686–692, 1990.

[20] G. Leander. Monomial bent functions. In *IEEE Trans. Inform. Theory (52) 2*, pages pp. 738–743, 2006.

[21] W. Ma, M. Lee, and F. Zhang. A new class of bent functions. In *IEICE Trans. Fundamentals, Vol E88-A , Issue 7*, pages 2039–2040, 2005.

[22] O.S. Rothaus. On "bent" functions. In *J. Combin.Theory Ser A 20*, pages pp. 300–305, 1976.

[23] P. Udaya. Polyphase and frequency hopping sequences obtained from finite rings. In *Ph. D. dissertation, Dept. Elec. Eng., Indian Inst. Technol., Kanpur*, 1992.

[24] N. Y. Yu and G. Gong. Construction of quadratic bent functions in polynomial forms. In *IEEE Trans. Inform. Theory (52) 7*, pages pp. 3291–3299, 2006.