ON BENT AND HYPER-BENT FUNCTIONS

by

MEHMET SARIYÜCE

Submitted to the Graduate School of Engineering and Natural Sciences
in partial fulfillment of
the requirements for the degree of
Master of Science

Sabancı University

Fall 2011

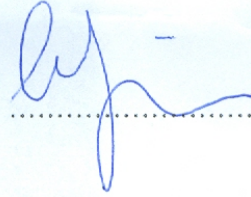ON BENT AND HYPER-BENT FUNCTIONS

APPROVED BY

Prof. Dr. Alev Topuzoğlu ....
(Thesis Supervisor)

Prof. Dr. Henning Stichtenoth ....

Assoc. Prof. Dr. Cem Güneri ....

Assoc. Prof. Dr. Erkay Savaş ....

Assist. Prof. Dr. Kağan Kurşungöz ....

DATE OF APPROVAL: February 3rd, 2012

ON BENT AND HYPER-BENT FUNCTIONS

Mehmet Sarıyüce

Mathematics, Master Thesis, 2011

Thesis Supervisor: Prof. Dr. Alev Topuzoğlu

Keywords: Bent functions, Hyper-bent functions, Kloosterman sums, Cubic sums, Dickson polynomials.

Abstract

Bent functions are Boolean functions which have maximum possible nonlinearity i.e. maximal distance to the set of affine functions. They were introduced by Rothaus in 1976. In the last two decades, they have been studied widely due to their interesting combinatorial properties and their applications in cryptography. However the complete classification of bent functions has not been achieved yet. In 2001 Youssef and Gong introduced a subclass of bent functions which they called hyper-bent functions. The construction of hyper-bent functions is generally more difficult than the construction of bent functions. In this thesis we give a survey of recent constructions of infinite classes of bent and hyper-bent functions where the classification is obtained through the use of Kloosterman and cubic sums and Dickson polynomials.

BENT ve HİPER-BENT FONKSİYONLARI ÜZERİNE

Mehmet Sarıyüce

Matematik, Yüksek Lisans Tezi, 2011

Tez Danışmanı: Prof. Dr. Alev Topuzoğlu

Özet

Bent fonksiyonları olası en az doğrusallığa sahip olan Boole fonksiyonlardır, yani afin fonksiyonlar kümesine olası en fazla uzaklığa sahip olan fonksiyonlardır. Bu kavram ilk olarak 1976 yılında Rothaus tarafından ortaya atılmıştır. Bent fonksiyonlar, kriptolojik uygulamalardaki kullanımından ve ilginç kombinatorik özelliklerinden dolayı son 20 yıl içerisinde geniş ilgi çekmiştir. Buna rağmen bent fonksiyonlarının tamamı henüz sınıflandırılamamıştır ve bu mümkün gözükmemektedir. 2001 yılında Youssef ve Gong, bent fonksiyonlarının, hiper-bent adını verdikleri bir alt kümesinin çalışılmasını önerdiler. Bu alt kümenin inşaası, genelde bent fonksiyonların inşaasından daha zordur. Bu tezde, Kloosterman ve kübik toplamlar ile Dickson polinomları yoluyla elde edilen sonsuz elemana sahip bent ve hiper-bent fonksiyon sınıfları hakkında son yıllarda yapılan bazı çalışmaları inceleyeceğiz.

Acknowledgments

First of all, I am very grateful to my supervisor, Prof. Dr. Alev Topuzoğlu, for her motivation, support and encouragement throughout this thesis and her insightful comments during the writing process of the thesis.

Moreover, I would like to express my deepest gratitude to my colleague at UEKAE, Dr. Orhun Kara, for his understanding, support and patience. Finally, I would like to thank to my colleague at UEKAE, Süleyman Kardaş, for his great encouragement and support.

Table of Contents

1

Introduction

Bent functions are Boolean functions which have maximal possible non-linearity. They
have been introduced first by Rothaus [27] in 1976. Lately there is a lot of interest
in them because they do not only have interesting properties, which are particularly
important for applications, but also there are still many open problems about them.
Bent functions play an important role especially in cryptographic applications since
non-linearity is one of the most important design criteria.

Despite extensive recent work on bent functions, full characterization of them has
not been achieved yet and it looks quite hopeless. Booelan functions which can be
expressed as the absolute trace of a single power function are called monomial Boolean
functions. There has been some progress in the last decades in the classification of
monomial bent functions. However, not much is known about the characterization of
bent functions which consist of multiple trace terms. For the case of binomial functions,
in 2009 Mesnager [23] has introduced an infinite class of Boolean bent functions on $\mathbb{F}_{2^n}$
defined as:

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

where $a \in \mathbb{F}_{2^n}$, $b \in \mathbb{F}_4$ and $\gcd(r, 2^m + 1) = 1$. In 2009 Mesnager [21] has also
shown that the functions in the form above with $r = 3$ are also bent. For the case
of multiple trace terms, in 2009 Charpin and Gong [5] have given a characterization
of bent functions in terms of Dickson polynomials. In 2010, with the help of result
of Charpin and Gong, Mesnager has given a characterization of bent functions with
multiple trace terms defined as

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

where E is the set of representatives of the cyclotomic cosets modulo $2^n - 1$ with each

coset having the full size n, $R \subseteq E$, $b \in \mathbb{F}_4$ and $a_r \in \mathbb{F}_{2^m}$ for all $r \in R$.

In 2001 Youssef and Gong [28] have introduced a subclass of bent functions, which they called hyper-bent functions. Hyper-bent functions have maximal possible distance to not only affine functions but also to bijective monomials, hence their characterization is generally harder than the characterization of bent functions. However it turns out that, the bent functions we mentioned above are also hyper-bent.

In this thesis we give a survey of recent constructions of classes of bent and hyper-bent functions. In Chapter 1, we give the necessary background, motivation about studying bent functions and some of the known classes of bent functions. In Chapter 2, we present characterization of Mesnager of binomial bent functions. In Chapter 3, we focus on hyper-bent functions. We show that the functions presented in Chapter 2 are also hyper-bent and then we give constructions of Mesnager, Charpin and Gong of hyper-bent functions obtained through Dickson polynomials.

1.1 Preliminaries

Definition 1.1. Let A be any set and k be any positive integer. A function $f : A^k \to \mathbb{F}_2$ is called a **Boolean function**.

In this thesis all functions we study are Booelan functions.

Definition 1.2. For any positive integers n, m such that m divides n, the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$, denoted by Tr_m^n is the mapping defined as:

$$Tr_m^n(x) := \sum_{i=0}^{\frac{n}{m}} x^{2^{im}}, \quad \forall x \in \mathbb{F}_{2^m}$$

Trace function is one of the most frequently used tools in the theory of finite fields. In this thesis we are going to use them also since the functions that we are going to study are expressed in terms of trace. Now we will see the following property of trace function.

Lemma 1.3. *Let $n = 2m$. We have*

$$\sum_{y \in \mathbb{F}_{2^m}} \chi((Tr_1^n(ay)) = \begin{cases} 0 & \text{if } a \notin \mathbb{F}_{2^m} \\ 2^m & \text{if } a \in \mathbb{F}_{2^m} \end{cases}$$

where $\chi(f(x)) = (-1)^{f(x)}$ for any Boolean function f.

Proof. First note that by the transitivity property of trace we have

$$\sum_{y \in \mathbb{F}_{2^m}} \chi\big((Tr_1^n(ay)\big) = \sum_{y \in \mathbb{F}_{2^m}} \chi\big((Tr_1^m(ay + (ay)^{2^m}))\big)$$

Since y is in $\mathbb{F}_{2^m}$, we have $y^{2^m} = y$. Then

$$\sum_{y \in \mathbb{F}_{2^m}} \chi\big((Tr_1^n(ay)\big) = \sum_{y \in \mathbb{F}_{2^m}} \chi\big(Tr_1^m((a + a^{2^m})y)\big)$$

Now assume $a \in \mathbb{F}_{2^m}$, then $a^{2^m} = a$. So we have $Tr_1^m((a + a^{2^m})y) = Tr_1^m(0)$. Then

$$\sum_{y \in \mathbb{F}_{2^m}} \chi\big((Tr_1^n(ay)\big) = \sum_{y \in \mathbb{F}_{2^m}} 1 = 2^m.$$

Now assume $a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$, then $(a + a^{2^m})^{2^m} = a^{2^m} + a$ which means $(a + a^{2^m}) \in \mathbb{F}_{2^m}$. Therefore $(a + a^{2^m})y$ runs through all elements of $\mathbb{F}_{2^m}$. Then we have

$$\sum_{y \in \mathbb{F}_{2^m}} \chi\big((Tr_1^n(ay)\big) = 0.$$

$\square$

Definition 1.4. The **Walsh-Hadamard transform** of a Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is defined as follows:

$$f^W(a) = \sum_{x \in \mathbb{F}_{2^n}} \chi\big(f(x) + Tr_1^n(ax)\big), \quad a \in \mathbb{F}_{2^n}. \tag{1.1}$$

Moreover, the values $f^W(a)$ are called the **Walsh-Hadamard coefficients of f**.

Definition 1.5. A Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is **bent** if $f^W(a) = \pm 2^{n/2}$, for all $a \in \mathbb{F}_{2^n}$.

Definition 1.6. An exponent d (always understood modulo $2^n - 1$) is called a **bent exponent**, if there exists an α such that the Boolean function $Tr_1^n(\alpha x^d)$ is bent.

The following property of a bent exponent will be used later.

Lemma 1.7. [17] *Let $f(x) = Tr_1^n(\alpha x^d)$ be a bent function defined on $\mathbb{F}_{2^n}$ and $n = 2m$. Then $gcd(d, 2^n - 1) \neq 1$. Furthermore either $gcd(d, 2^m - 1) = 1$ or $gcd(d, 2^m + 1) = 1$.*

Proof. Suppose $gcd(d, 2^n - 1) = 1$. Since $x \mapsto x^d$ is a permutation on $\mathbb{F}_{2^n}$, we have

$$f^W(0) = \sum_{x \in \mathbb{F}_{2^n}} \chi(f(x) + Tr_1^n(0.x^d)) = \sum_{x \in \mathbb{F}_{2^n}} \chi(Tr_1^n(\alpha x^d)) = 0.$$

which is a contradiction to the bent exponent property i.e. the bentness of f.
Now assume $gcd(d, 2^n - 1) = s \neq 1$. Let

$$D = \{y \in \mathbb{F}_{2^n} | y^d = 1\} = \{y \in \mathbb{F}_{2^n} | y^s = 1\}.$$

Obviously, for any $u \in \mathbb{F}_{2^n}^*$, f is constant on all cosets uD. If we represent $\mathbb{F}_{2^n}^*$ by cosets uD, let say there are N many cosets, then $\mathbb{F}_{2^n}^* = \bigcup_{i=1}^{N} u_i D$. It is clear that $Ns = 2^n - 1$ since $|D| = s$. Therefore we get

$$
\begin{aligned}
f^W(0) &= \sum_{x \in \mathbb{F}_{2^n}} \chi(Tr_1^n(\alpha x^d)) \\
&= 1 + \sum_{uy \in \mathbb{F}_{2^n}^*} \chi(Tr_1^n(\alpha u^d)) \\
&= 1 + s\left(\sum_{i=1}^{N} \chi(Tr_1^n(\alpha u_i^d)) \right) \\
&\equiv 1 \pmod{s}.
\end{aligned}
$$

4

Since d is a bent exponent, $f^W(0)$ is equal to either 2^m or -2^m. Assume $f^W(0) = 2^m$ then $2^m \equiv 1 \pmod{s}$ which means s divides $2^m - 1$. Now assume $f^W(0) = -2^m$ then $-2^m \equiv 1 \pmod{s}$ which means s divides $2^m + 1$. Since $gcd(2^m - 1, 2^m + 1) = 1$, we have either $gcd(d, 2^m - 1) = 1$ or $gcd(d, 2^m + 1) = 1$. $\qquad\square$

We have the following well-known theorem due to Dillon. For the proof we refer to [7].

Theorem 1.8. [7] *Let E_i, $i = 1, 2, \ldots, N$, be N subspaces of $\mathbb{F}_{2^n}$ of dimension m satisfying $E_i \cap E_j = \{0\}$ for all $i, j \in \{1, 2, \ldots, N\}$ with $i \neq j$. Let $n = 2m$ and f be a Boolean function over $\mathbb{F}_{2^n}$. Assume that the support of f, $supp(f) := \{x \in \mathbb{F}_{2^n} | f(x) = 1\}$, can be written as*

$$supp(f) = \bigcup_{i=1}^{N} E_i^*, \ \ where \ E_i^* := E_i \setminus \{0\}$$

Then f is bent if and only if $N = 2^{m-1}$. In this case f is said to be in $\mathcal{PS}^-$ class.

Kloosterman sums and *cubic sums* are the two key tools for most of the bentness characterizations that we consider in this thesis.

Definition 1.9. The binary **Kloosterman sums** on $\mathbb{F}_{2^m}$ are:

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

Remark 1.10. In this thesis, we consider the so called extended Kloosterman sums (extended from $\mathbb{F}_{2^m}^*$ to $\mathbb{F}_{2^m}$) by assuming that $\chi(Tr_1^m(1/x)) = 1$ for $x = 0$.

Theorem 1.11. [15] *Let m be a positive integer. The set $\{ K_m(a), a \in \mathbb{F}_{2^m} \}$, is the set of all the integers multiple of 4 in the range $[-2^{(m+2)/2} + 1, 2^{(m+2)/2} + 2]$.*

Proof. See the proof in [15]. $\qquad\square$

Definition 1.12. The **cubic sums** on $\mathbb{F}_{2^m}$ are:

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

1.2   Basic properties of bent functions

Boolean functions have wide applications, espacially in cryptography they play a crucial role. In cryptography, they have been mostly used for constructing stream ciphers, S-Boxes in block ciphers and hash functions. When one tries to construct these kind of cryptographic structures, one of the most important criteria is high non-linearity because high non-linearity makes cryptographic structures strong against most of the cryptanalytic attacks such as linear attack [19] and differential attack [3].

In 1976, Rothaus [27] introduced bent functions. They are Boolean functions that attain maximum possible non-linearity. However, bent functions are not balanced i.e. their images do not have equal number of zeros and ones. Since being balanced is another design criteria in cryptography, bent functions are combined with other structures in order to generate balanced functions and these functions still preserve the properties of bent functions, such as hash function HAVAL [29] and block cipher CAST [1].

As we have defined earlier (see Definition 1.5), a Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is bent if $f^W(a) = \pm 2^{n/2}$ for all $a \in \mathbb{F}_{2^n}$.

Remark 1.13. Note that Walsh-Hadamard coefficients are integers, therefore bent functions exist only for even n.

Bent functions can be defined in different ways, see the following Remarks 1.14, 1.18.

Remark 1.14. Bent functions can also be defined as follows: A function f in $\mathbb{F}_{2^n}$ is called bent if all Walsh-Hadamard coefficients of f have the same absolute value. One can see that the two definitions above are equivalent due to Parseval's Identity.

Lemma 1.15. *Parseval's Identity.* *Let f be a Boolean function defined on $\mathbb{F}_{2^n}$. We have*

$$\sum_{a \in \mathbb{F}_{2^n}} f^W(a)^2 = 2^{2n}$$

Definition 1.16. The **linearity** of a Boolean function f with respect to Walsh-Hadamard transform is defined by

$$Lin(f) = \max_{a \in \mathbb{F}_{2^n}} \left| f^W(a) \right|.$$

Definition 1.17. Nonlinearity of a a Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is defined by:

$$\mathcal{N}(f) = 2^{n-1} - \frac{1}{2}\Big(\max_{a\in\mathbb{F}_{2^n}} \big|f^W(a)\big|\Big)$$

Remark 1.18. We can give another definition of a Boolean bent function by linearity as follows: A Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is bent if $\mathrm{Lin}(f) = 2^{n/2}$. Note that this definition is equivalent with the others because $2^{n/2}$ is the minimal linearity that f can have due to Parseval's Identity.

Definition 1.19. Another measure of the linearity of a Boolean function f is the **autocorrelation** function. It is defined by

$$\mathrm{AC}_f(a) = \sum_{x\in\mathbb{F}_{2^n}} \chi\big(f(x) + f(x + a)\big).$$

Bent functions can also be defined by their autocorrelation functions. High autocorrelation values are considered as weakness in [25]. But bent functions have minimum autocorrelation values which is considered as another good property.

Proposition 1.20. [10] *A Boolean function f on $\mathbb{F}_{2^n}$ is bent if and only if $AC_f(a) = 0$ for all non-zero $a \in \mathbb{F}_{2^n}$.*

The following proposition gives another property of bent functions.

Proposition 1.21. [27] *If $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is a bent function, (then n is even) the algebraic degree of f is at most n/2, except in the case $n = 2$.*

Bent functions are also related to *difference sets*.

Definition 1.22. Given an abelian group G of order v, a subset $D \subseteq G$ of order k is called a (v, k, λ)-**difference set** in G, if for each non-identity element $g \in G$, the equation $g = xy^{-1}$ has exactly λ solutions (x, y) in D.

Definition 1.23. Let D be a (v, k, λ)-difference set in G. D is **Hadamard difference set** if $v = 4(k - \lambda)$.

The following characterization shows us how difference sets and bent functions are closely related.

Proposition 1.24. [7] *Let D be a Hadamard Difference set in $\mathbb{F}_{2^n}$. Let f be a Boolean function on $\mathbb{F}_{2^n}$ defined by $f(x) = 1$ if and only if $x \in D$. Then f is bent. Conversely, if $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is bent, then the support of f is a Hadamard difference set of $\mathbb{F}_{2^n}$.*

Proof. See the proof [7]. □

1.3 Known classes of bent functions

1.3.1 Monomial bent functions

The following characterizations of monomial bent functions have been well-established. Hence we present these results without proof.

Theorem 1.25. *The Gold Case* [17] *Let $\alpha \in \mathbb{F}_{2^n}$, $r \in \mathbb{N}$ and $d = 2^r + 1$. The function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ defined by $f(x) = Tr_1^n(\alpha x^d)$, is bent if and only if $\alpha \notin \{x^d \mid x \in \mathbb{F}_{2^n}\}$.*

Theorem 1.26. *The Dillon Case* [7] *Let $\alpha \in \mathbb{F}_{2^m}$, $n = 2m$ and $d = 2^m - 1$. The function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ defined by $f(x) = Tr_1^n(\alpha x^d)$, is bent if and only if $K_m(a) = 0$.*

Proof. We will see this case in the next chapter. See the proof of Theorem 2.7 $\qquad\square$

Theorem 1.27. *The Dillon-Dobbertin Case* [9] *Let n be an even integer coprime to 3. Let $\alpha \in \mathbb{F}_{2^n}$, $r \in \mathbb{N}$ and $d = 2^{2r} - 2^r + 1$ with $gcd(r, n) = 1$. The function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ defined by $f(x) = Tr_1^n(\alpha x^d)$, is bent if and only if $\alpha \notin \{x^d \mid x \in \mathbb{F}_{2^n}\}$.*

Theorem 1.28. *The Leander Case* [17] *Let $\alpha \in \mathbb{F}_{2^n}$. Let r be an odd integer with $n = 4r$ and $d = 2^{2r} - 2^{r+1} + 1$. Let β be a primitive element of $\mathbb{F}_{16}$ and $\alpha = \beta^5$. Then, the function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ defined by $f(x) = Tr_1^n(\alpha x^d)$, is bent.*

1.3.2 Bent functions with multiple trace terms

The following characterization is given by Charpin and Gong in [5]. We refer the reader to [5] for proof. But before we state the theorem, we need the following definition.

Definition 1.29. For any integer s, $0 \leq s < p^n - 1$, let r be the smallest integer with the property that $p^{r+1}s \equiv s \pmod{p^n - 1}$. **The cyclotomic coset** containing s modulo $p^n - 1$ consists of $\{s, ps, p^2 s, p^3 s, \ldots, p^r s\}$ where each $p^i s$ is reduced $\pmod{p^n - 1}$. The smallest entries of the cyclotomic cosets are called coset representatives.

Remark 1.30. The cyclotomic cosets partition the integers $\{0, \ldots, p^n - 1\}$. If s is relatively prime to $p^n - 1$, then $r = n - 1$. When $r = n - 1$, cyclotomic coset containing s has the full size n.

Theorem 1.31. [5] *Let $n = 2m$ and $\lambda \in \mathbb{F}_{2^n}^*$. Let R be a set of representatives of the cyclotomic cosets modulo $2^m + 1$ of full size n. Let f be a Boolean function defined on $\mathbb{F}_{2^n}$ as:*

$$f(x) = Tr_1^n\big(\lambda(x^{(2^r-1)(2^m-1)} + x^{(2^r+1)(2^m-1)})\big)$$

where $0 < r < m$ and $\{2^r - 1, 2^r + 1\} \subset R$. Assume that the function $x \mapsto Tr_1^m(\lambda x^{2^r+1})$ is balanced on $\mathbb{F}_{2^m}$, i.e. its image contains an equal number of zeros and ones. Then f is bent if and only if

$$\sum_{x \in \mathbb{F}_{2^m}} \chi\big(Tr_1^m(x^{-1} + \lambda x^{2^r+1})\big) = 0.$$

The following characterizations are given by Honggang Hu and Dengguo Feng in [14]. We refer the reader to [14] for the proofs. Let n be an even positive integer. Let e be a divisor of n such that n/e is also an even positive integer and $m = n/e$.

Theorem 1.32. [14] *For any $\beta \in \mathbb{F}_{2^e}^*$, the Boolean function defined on $\mathbb{F}_{2^n}$ as:*

$$f(x) = \sum_{i=1}^{m/2-1} Tr_1^n(\beta x^{1+2^{ei}}) + Tr_1^{n/2}(\beta x^{1+2^{n/2}})$$

is bent function. In particular, for any $\beta \in \mathbb{F}_{2^{n/2}}^*$, the function

$$f(x) = Tr_1^{n/2}(\beta x^{1+2^{n/2}})$$

is a bent function.

Theorem 1.33. [14] *Let $\beta \in \mathbb{F}_{2^e}^*$ and $c_i \in \mathbb{F}_2$, $i = 1, 2, \ldots, m/2$. The Boolean function f defined on $\mathbb{F}_{2^n}$ as:*

$$f(x) = \sum_{i=1}^{m/2-1} c_i Tr_1^n(\beta x^{1+2^{ei}}) + c_{m/2} Tr_1^{n/2}(\beta x^{1+2^{n/2}})$$

is bent if and only if $gcd(c(x), x^m + 1) = 1$, where

$$c(x) = \sum_{i=1}^{m/2-1} c_i(x^i + x^{m-i}) + c_{m/2} x^{m/2}.$$

In particular, $c_{m/2} = 1$ if $f(x)$ is bent.

The following characterizations are given by Dobbertin, Leander, Canteaut, Carlet, Felke and Gaborit in [11]. We refer the reader to [11] for proofs. But before we give their characterizations we need the following definition.

Definition 1.34. Let n, m be positive integers such that $n = 2m$. An exponent d is a *Niho exponent* and x^d is a *Niho power function* in $\mathbb{F}_{2^n}$ if $d \equiv 1 \pmod{2^m - 1}$.

Dobbertin, Leander, Canteaut, Carlet, Felke and Gaborit have obtained their characterizations through the use of Niho power functions. Let $n = 2m$ be a positive integer. They consider Boolean functions defined on $\mathbb{F}_{2^n}$ as in the form

$$f(x) = Tr_1^n(\alpha_1 x^{d_1} + \alpha_2 x^{d_2}) \tag{1.2}$$

for $\alpha_1, \alpha_2 \in \mathbb{F}_{2^n}$ such that $\alpha_1 + \alpha_1^{-1} = \alpha_2^{d_1}$, where $d_i = (2^m - 1)s_i + 1$, $i = 1, 2$ are Niho exponents. It is known that if f is bent, then necessarily w.l.o.g.

$$d_1 = (2^m - 1)\frac{1}{2} + 1.$$

.

Theorem 1.35. [11] *Define $d_2 = (2^m - 1)3 + 1$. If $m \equiv 2 \pmod 4$, assume that $\alpha_2 = \beta^5$ for some $\beta \in \mathbb{F}_{2^n}^*$. Otherwise, i.e. if $m \not\equiv 2 \pmod 4$, let $\alpha_2 \in \mathbb{F}_{2^n}^*$ be arbitrary. Then f defined as in 1.2 is a bent function of degree m.*

Theorem 1.36. [11] *Suppose that m is odd. Define $d_2 = (2^m - 1)(1/4) + 1$. Then f defined as in 1.2 is a bent function of degree 3.*

Theorem 1.37. [11] *Suppose that m is even. Define $d_2 = (2^m - 1)(1/6) + 1$. Then f defined as in 1.2 is a bent function of degree m.*

2

A New Infinite Class of Boolean Bent Functions

In this chapter we are going to study an infinite class of bent functions which is introduced recently by Mesnager in [23] and [21] . From now on, we assume $n = 2m$ be a positive integer. Let $a \in \mathbb{F}_{2^n}$, $b \in \mathbb{F}_4^*$ and r be an integer. Define the set of the Boolean functions $f_{a,b}^{(r)}$, denoted by $\Im_n$, on $\mathbb{F}_{2^n}$ as:

$$f_{a,b}(x) = Tr_1^n(ax^{r(2^m-1)}) + Tr_1^2(bx^{(\frac{2^n-1}{3})}), \quad \forall x \in \mathbb{F}_{2^n} \tag{2.1}$$

In [23], Mesnager has given the characterization of the bentness of the set of the functions $f_{a,b}^{(r)} \in \Im_n$ only for integers r such that $gcd(r, 2^m + 1) = 1$. Then, in [21] she has also given similar characterization for $r = 3$ which is not coprime to $2^m + 1$.

2.1 The characterization of the functions $f_{a,b}^{(r)} \in \Im_n$ where $\mathbf{gcd}(r, 2^m+1) = 1$

In this section, set r be a positive integer which is coprime to $2^m + 1$. Now we will see that it is enough to study the case where $a \in \mathbb{F}_{2^m}^*$ in order to give a characterization of the bentness of the set of the functions $f_{a,b}^{(r)} \in \Im_n$. But before that we need the following lemmas.

Lemma 2.1. *Let n be an even positive integer and m be an odd positive integer. Then*

1. *3 divides $2^n - 1$,*

2. *$gcd(2^m - 1, 3) = 1$ and $gcd(2^m + 1, 3) = 3$,*

3. *If $m \not\equiv 3 \pmod 6$, then $gcd(3, \frac{2^m+1}{3}) = 1$.*

Proof.   1. We know $n = 2k$ for some $k \in \mathbb{N}$. Note that $2^{2k} - 1 = (2^k - 1)(2^k + 1)$. Suppose $2^k = 3q + r$ where q, r in $\mathbb{N}$ and it is clear that we have either $r = 1$ or

$r = 2$. Assume $r = 1$, then 3 divides $2^k - 1$. Now, assume $r = 2$, then 3 divides $2^k + 1$. Hence $2^{2k} - 1$ is divisible by 3.

2. We know $m = 2k + 1$ for some $k \in \mathbb{N}$. By the previous case, we have $2^{2k} - 1 = 3l$ for some $l \in \mathbb{N}$. Therefore

$$2^{2k} = 3l + 1 \quad \Leftrightarrow \quad 2^{2k+1} = 6l + 2 \quad \Leftrightarrow \quad 2^{2k+1} - 1 = 6l + 1$$

Hence $2^m - 1$ is not divisible by 3. On the other hand $2^m + 1$ is divisible by 3.

3. Assume $gcd(3, \frac{2^m+1}{3}) \neq 1$ i.e. $gcd(3, \frac{2^m+1}{3}) = 3$. Then $2^m + 1 \equiv 0 \pmod 9$. Let $m \equiv j \pmod 6$. Then $2^m + 1 = 2^{6l+j} + 1$ for some $l \in \mathbb{N}$. Then $2^m + 1 = (64)^l 2^j + 1 \equiv 2^j + 1 \pmod 9$ which means $j = 3$ since we assumed $2^m + 1 \equiv 0 \pmod 9$.

$\square$

The following lemma is also known as *polar decomposition* of $\mathbb{F}_{2^n}^*$. It will be used frequently not only in this chapter but also in the next chapter.

Lemma 2.2. *Let m, n be positive integers such that $n = 2m$. Let $U = \{x \in \mathbb{F}_{2^n}^* \mid x^{2^m+1} = 1\}$. Then we can represent each $x \in \mathbb{F}_{2^n}^*$ uniquely as $x = yu$ where $y \in \mathbb{F}_{2^m}^*$ and $u \in U$.*

Proof. We will show that $\mathbb{F}_{2^n}^* = \mathbb{F}_{2^m}^* U = \{uy \mid y \in \mathbb{F}_{2^m}^*, \ u \in U\}$, then the result will follow.

1. $\mathbb{F}_{2^m}^* \cap U = \{1\}$. It holds since there can not be any other elements which has both order $2^m - 1$ and $2^m + 1$ at the same time.

2. If $x_1 = x_2$ such that $x_1 = u_1 y_1$ and $x_2 = u_2 y_2$ where $u_i \in U$ and $y_i \in \mathbb{F}_{2^m}^*$, then $u_1 = u_2$ and $y_1 = y_2$. It holds because

$$x_1 = x_2 \quad \Rightarrow \quad u_1 y_1 = u_2 y_2$$

$$(u_1 y_1)^{2^m+1} = (u_2 y_2)^{2^m+1} \quad \Rightarrow \quad y_1^2 = y_2^2.$$

The last equality holds since $u \in U$ has order $2^m + 1$. Now we have $y_1^2 = y_2^2$ means $y_1 = y_2$ and therefore $u_1 = u_2$.

Now note that $|\mathbb{F}_{2^m}^*| = 2^m - 1$ and $|U| = 2^m + 1$. By the above properties, it is clear that $|\mathbb{F}_{2^m}^* U| = (2^m - 1)(2^m + 1) = 2^n - 1 = |\mathbb{F}_{2^n}^*|$. Therefore $\mathbb{F}_{2^n}^* = \mathbb{F}_{2^m}^* U$ since $\mathbb{F}_{2^m}^* U \subseteq \mathbb{F}_{2^n}^*$. Uniqueness comes from the second property above. $\qquad \square$

Proposition 2.3. *Let $f_{a,b}^{(r)}$ be a Boolean function in the set $\Im_n$ defined as in (2.1). Then we have*

$$\{(a, b) \mid a \in \mathbb{F}_{2^n}^*, \ b \in \mathbb{F}_4, \ f_{a,b}^{(r)} \ is \ bent \ \} \tag{2.2}$$

$$= \{(a'\lambda^{r(2^m-1)}, b'\lambda^{\frac{2^n-1}{3}}) \mid a' \in \mathbb{F}_{2^m}^*, \ b' \in \mathbb{F}_4, \ \lambda \in \mathbb{F}_{2^n}^*, \ f_{a',b'}^{(r)} \ is \ bent \ \} \tag{2.3}$$

Proof. Let $a \in \mathbb{F}_{2^n}^*$, $b \in \mathbb{F}_4$ and $a' \in \mathbb{F}_{2^m}^*$. First note that if $a = a'\lambda^{r(2^m-1)}$ and $b = b'\lambda^{\frac{2^n-1}{3}}$ for some $\lambda \in \mathbb{F}_{2^n}^*$ and $b' \in \mathbb{F}_4$, then we have for all $x \in \mathbb{F}_{2^n}$

$$f_{a,b}^{(r)}(x) = Tr_1^n(a'\lambda^{r(2^m-1)}x^{r(2^m-1)}) + Tr_1^2(b'\lambda^{(\frac{2^n-1}{3})}x^{(\frac{2^n-1}{3})}) = f_{a',b'}^{(r)}(\lambda x)$$

Since the mapping $x \mapsto \lambda x$ is a permutation on $\mathbb{F}_{2^n}$ we have that $f_{a,b}^{(r)}$ is bent if and only if $f_{a',b'}^{(r)}$. Now it is clear that the set 2.2 already includes the set 2.3. Now we will show that the set 2.3 includes the set 2.2. Let $a \in \mathbb{F}_{2^n}^*$, $b \in \mathbb{F}_4$ and $U = \{x \in \mathbb{F}_{2^n}^* \mid x^{2^m+1} = 1\}$. Note that $\forall \lambda \in \mathbb{F}_{2^n}^*$, we have $\lambda^{r(2^m-1)} \in U$. Then by Lemma 2.2 and by the fact that $gcd(r, 2^m + 1) = 1$, $\exists \lambda \in \mathbb{F}_{2^n}^*$ such that $a = a'\lambda^{r(2^m-1)}$. Moreover since $\lambda^{\frac{2^n-1}{3}} \in \mathbb{F}_4^*$, we have that $\exists b' \in \mathbb{F}_4$ such that $b = b'\lambda^{\frac{2^n-1}{3}}$. Hence for any $f_{a,b}^{(r)}$, one can find the related $f_{a',b'}^{(r)}$. $\qquad \square$

The proposition above enables us to restrict our study to the case where $a \in \mathbb{F}_{2^m}^*$. In the following three sections we will study the following three cases,

1. $b = 0$,

2. $b \neq 0$ and m is odd,

3. $b \neq 0$ and m is even.

Before we begin to study these cases, we need to have the following lemmas.

Lemma 2.4. *Let $n = 2m$ and $U = \{x \in \mathbb{F}_{2^n}^* \mid x^{2^m+1} = 1\}$. For every element $u \in U$, the element $u + u^{-1}$ can be uniquely represented by c where $c \in \mathbb{F}_{2^m}$ and $Tr_1^m(1/c) = 1$, in other words we have $\{u + u^{-1} \mid u \in U\} = \{c \mid c \in \mathbb{F}_{2^m} \ and \ Tr_1^m(1/c) = 1\}$*

Proof. Let $c \in \mathbb{F}_{2^m}$. Note that $y^2 + yc + 1 = 0$ has a solution in $\mathbb{F}_{2^m} \Leftrightarrow (yc)^2 + yc^2 + 1 = 0$ has a solution in $\mathbb{F}_{2^m} \Leftrightarrow (y^2 + y)c^2 = 1$ has a solution in $\mathbb{F}_{2^m} \Leftrightarrow y^2 + y = (1/c^2)$ has a solution in $\mathbb{F}_{2^m} \Leftrightarrow Tr_1^m(y^2 + y) = Tr_1^m(1/c^2)$ i.e. $Tr_1^m(1/c^2) = 0$ since $Tr_1^m(y^2 + y) = 0$ i.e. $Tr_1^m(1/c) = 0$. Therefore $Tr_1^m(1/c) = 1$ if and only if $y^2 + yc + 1$ is irreducible over $\mathbb{F}_{2^m}$.

Define $g : U \to \mathbb{F}_{2^m}$ such that $g(u) = u + u^{2^m}$. Note that g is well-defined since $u + u^{2^m} \in \mathbb{F}_{2^m}$ for all $u \in U$. g is zero only for $u = 1$ and takes exactly twice each value in U since $g(u) = g(u^{-1})$. Let $c = g(y) = y + y^{-1}$, then $yc = y^2 + 1$ has no solution in $\mathbb{F}_{2^m}$ if and only if $Tr_1^m(1/c) = 1$. Since it is quadratic, the solution has to be in $\mathbb{F}_{2^n}$. Moreover, the solution is in U since $y + y^{-1} \in \mathbb{F}_{2^m}$ is possible only for $y \in U$. Also there are two solutions. Hence we have the result. $\qquad\square$

Here we have another well-known fact which will be used frequently.

Lemma 2.5. *Let $n = 2m$ and $a \in \mathbb{F}_{2^m}^*$. Let $U = \{x \in \mathbb{F}_{2^n}^* \mid x^{2^m+1} = 1\}$. Then the following equality holds*

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

Proof. By the transitivity property of trace we have

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

The last equality holds since $a^{2^m} = a$ and $u^{2^m} = u^{-1}$.

$$\sum_{u \in U} \chi(Tr_1^m(a(u + u^{-1}))) = 1 + \sum_{u \in U \setminus \{1\}} \chi\big(Tr_1^m(a(u + u^{-1}))\big)$$

$$= 1 + 2\bigg(\sum_{\substack{c \in \mathbb{F}_{2^m} \\ Tr_1^m(c)=1}} \chi(Tr_1^m(a/c)) \bigg)$$

The last equality comes from unique trace representation by Lemma 2.4 and the fact that $U \setminus \{1\} = 2\big|\{c \in \mathbb{F}_{2^m} \mid Tr_1^m(1/c) = 1\}\big|$.

$$= 1 + 2\bigg(\sum_{c \in \mathbb{F}_{2^m}} \chi(Tr_1^m(a/c)) \bigg) - 2\bigg(\sum_{\substack{c \in \mathbb{F}_{2^m} \\ Tr_1^m(c)=0}} \chi(Tr_1^m(a/c)) \bigg)$$

$$= 1 + 0 - 2\bigg(\sum_{\substack{c \in \mathbb{F}_{2^m} \\ Tr_1^m(c)=0}} \chi(Tr_1^m(a/c)) \bigg) \qquad (2.4)$$

$$= 1 + 0 - 2\bigg(\sum_{\substack{c \in \mathbb{F}_{2^m}^* \\ Tr_1^m(c)=0}} \chi(Tr_1^m(a/c)) \bigg) - 2$$

14

It is clear that if $Tr_1^m(c) = 0$, then $c = \beta^2 + \beta$ for some $\beta \in \mathbb{F}_{2^m}$. Also one can see that $2\big|\{c \in \mathbb{F}_{2^m}^* \mid Tr_1^m(c) = 0\}\big| = \big|\{\beta^2 + \beta \mid \beta \in \mathbb{F}_{2^m} \setminus \mathbb{F}_2\}\big|$. Now if we put $\beta^2 + \beta$ instead of c, we have

$$= -1 - \sum_{\beta \in \mathbb{F}_{2^m} \setminus \mathbb{F}_2} \chi(Tr_1^m(\frac{a}{\beta^2 + \beta}))$$

$$= -1 - \sum_{\beta \in \mathbb{F}_{2^m} \setminus \mathbb{F}_2} \chi(Tr_1^m(a(\frac{1}{\beta} + \frac{1}{1 + \beta})))$$

$$= -1 - \sum_{\frac{1}{\gamma} = \beta \in \mathbb{F}_{2^m} \setminus \mathbb{F}_2} \chi(Tr_1^m(a(\gamma + \frac{\gamma}{1 + \gamma})))$$

$$= -1 - \sum_{\delta + 1 = \gamma \in \mathbb{F}_{2^m} \setminus \mathbb{F}_2} \chi(Tr_1^m(a(\delta + 1 + \frac{\delta + 1}{\delta})))$$

$$= -1 - \sum_{\delta \in \mathbb{F}_{2^m} \setminus \mathbb{F}_2} \chi(Tr_1^m(a(\delta + \frac{1}{\delta})))$$

$$= -1 - \sum_{\gamma = a^{-1}\delta \in a^{-1}\mathbb{F}_{2^m} \setminus a^{-1}\mathbb{F}_2} \chi(Tr_1^m(a(a\gamma + \frac{1}{a\gamma})))$$

$$= -1 - \sum_{\gamma \in a^{-1}\mathbb{F}_{2^m} \setminus a^{-1}\mathbb{F}_2} \chi(Tr_1^m(a^2\gamma + \frac{1}{\gamma}))$$

$$= -1 - \sum_{\gamma \in a^{-1/2}\mathbb{F}_{2^m} \setminus a^{-1/2}\mathbb{F}_2} \chi(Tr_1^m(a\gamma + \frac{1}{\gamma}))$$

$$= -1 - \sum_{\gamma \in a^{-1/2}\mathbb{F}_{2^m}} \chi(Tr_1^m(a\gamma + \frac{1}{\gamma})) + 2$$

$$= 1 - K_m(a). \tag{2.5}$$

$\square$

2.1.1   The case where b=0

When $b = 0$, $f_{a,0}^{(1)}$ becomes a monomial function which has been already considered by Dillon [7] in 1974. The following theorem has been proved by Dillon in [7, 8] using the results from coding theory.

Theorem 2.6. [7] *Suppose that $a \in \mathbb{F}_{2^m}^*$. The function $f_{a,0}^{(1)}$ defined on $\mathbb{F}_{2^n}$ by $f_{a,0}^{(1)} = Tr_1^n(ax^{2^m-1})$, is bent if and only if $K_m(a) = 0$ where K_m is the Kloosterman sum on $\mathbb{F}_{2^m}$.*

Proof. see the proof of the next theorem or the proof in [7, 8] $\square$

In 2008, Leander [17] has given another proof which is different than proof of Dillon and gives more information. However there was a small error in his proof, but then Charpin and Gong [5] corrected that error. Moreover they have given characterization of bentness of $f_{a,0}^{(r)}$ for any r such that $gcd(r, 2^m + 1) = 1$.

Theorem 2.7. [5] *Let $a \in \mathbb{F}_{2^m}^*$ and r be an integer such that $gcd(r, 2^m + 1) = 1$. The function $f_{a,0}^{(r)}$ defined on $\mathbb{F}_{2^n}$ by $f_{a,0}^{(r)} = Tr_1^n(ax^{r(2^m-1)})$, is bent if and only if $K_m(a) = 0$ where K_m is the Kloosterman sum on $\mathbb{F}_{2^m}$.*

Proof. Let $U = \{x \in \mathbb{F}_{2^n}^* \mid x^{2^m+1} = 1\}$. By Lemma 2.2, we know $\forall x \in \mathbb{F}_{2^n}^*, \quad \exists u \in U$ and $\exists y \in \mathbb{F}_{2^m}^*$ such that $x = uy$.

$$f_{a,0}^{(r)W}(c) = \sum_{x \in \mathbb{F}_{2^n}} \chi(f_{a,0}^{(r)}(x) + Tr_1^n(cx)) = \sum_{x \in \mathbb{F}_{2^n}} \chi(Tr_1^n(ax^{r(2^m-1)}) + Tr_1^n(cx))$$

$$= 1 + \sum_{x \in \mathbb{F}_{2^n}^*} \chi(Tr_1^n(ax^{r(2^m-1)}) + Tr_1^n(cx))$$

$$= 1 + \sum_{u \in U} \sum_{y \in \mathbb{F}_{2^m}^*} \chi(Tr_1^n(au^{r(2^m-1)}) + Tr_1^n(cuy))$$

Since $u^{2m+1} = 1$, we have $u^{2^m-1} = u^{-2}$. Then

$$f_{a,0}^{(r)W}(c) = 1 + \sum_{u \in U} \sum_{y \in \mathbb{F}_{2^m}^*} \chi(Tr_1^n(au^{-2r}) + Tr_1^n(cuy))$$

$$= 1 + \sum_{u \in U} \chi(Tr_1^n(au^{-2r}) \sum_{y \in \mathbb{F}_{2^m}^*} \chi((Tr_1^n(cuy))$$

When $c = 0$, we have

$$f_{a,0}^{(r)W}(0) = 1 + \sum_{u \in U} \chi((Tr_1^n(au^{-2r})) \sum_{y \in \mathbb{F}_{2^m}^*} \chi(Tr_1^n(0))$$

$$= 1 + (2^m - 1) \sum_{u \in U} \chi((Tr_1^n(au^{-2r}))$$

Since $gcd(-2, 2^m + 1) = 1$ and $gcd(r, 2^m + 1) = 1$, the mapping $u \mapsto u^{-2r}$ is a permutation on U. Then we have

$$f_{a,0}^{(r)W}(0) = 1 + (2^m - 1) \sum_{u \in U} \chi((Tr_1^n(au))$$

By Lemma 2.5, we know $\sum_{u \in U} \chi(Tr_1^n(au)) = 1 - K_m(a)$. Then we have

$$f_{a,0}^{(r)W}(0) = 1 + (2^m - 1)(1 - K_m(a)) = 2^m(1 - K_m(a)) + K_m(a)$$

16

If $f_{a,0}^{(r)}$ is bent then $f_{a,0}^{(r)^W}(0) = \pm 2^m$. If it is 2^m, then $K_m(a) = 0$. If it is -2^m,
then $K_m(a) = \frac{2^{m+1}}{2^m-1}$ which is not an integer. Therefore, $f_{a,0}^{(r)}(0) = 2^m$ if and only if
$K_m(a) = 0$. Now we will study the case where $c \neq 0$ i.e. $c \in \mathbb{F}_{2^n}^*$

When $c \in \mathbb{F}_{2^n}^*$, we have

$$f_{a,0}^{(r)^W}(c) = 1 + \sum_{u \in U} \chi(Tr_1^n(au^{-2r})) \sum_{y \in \mathbb{F}_{2^m}^*} \chi((Tr_1^n(cuy))$$

$$= 1 + \sum_{u \in U} \chi(Tr_1^n(au^{-2r})) \left(\sum_{y \in \mathbb{F}_{2^m}} \chi((Tr_1^n(cuy)) - 1 \right)$$

From Lemma 1.3, we know

$$\sum_{y \in \mathbb{F}_{2^m}} \chi((Tr_1^n(sy)) = \begin{cases} 0 & \text{if } s \notin \mathbb{F}_{2^m} \\ 2^m & \text{if } s \in \mathbb{F}_{2^m} \end{cases}$$

In our case, we have

$$\sum_{y \in \mathbb{F}_{2^m}} \chi((Tr_1^n(cuy)) = \begin{cases} 0 & \text{if } cu \notin \mathbb{F}_{2^m} \Leftrightarrow (cu)^{2^m-1} \neq 1 \Leftrightarrow u^2 \neq c^{2^m-1} \\ 2^m & \text{if } cu \in \mathbb{F}_{2^m} \Leftrightarrow (cu)^{2^m-1} = 1 \Leftrightarrow u^2 = c^{2^m-1} \end{cases}$$

If we use this information, we have

$$f_{a,0}^{(r)^W}(c) = 1 + \sum_{u \in U} \chi(Tr_1^n(au^{-2r})) \left(\sum_{y \in \mathbb{F}_{2^m}} \chi((Tr_1^n(cuy)) - 1 \right)$$

$$= 1 + 2^m \sum_{\substack{u \in U \\ u^2 = c^{2^m-1}}} \chi(Tr_1^n(au^{-2r})) - \sum_{u \in U} \chi(Tr_1^n(au^{-2r})$$

Note that there is just one element in U such that $u^2 = c^{2^m-1}$. Then we have

$$f_{a,0}^{(r)^W}(c) = 1 + 2^m \chi(Tr_1^n(ac^{-r(2^m-1)})) - \sum_{u \in U} \chi(Tr_1^n(au^{-2r})$$

By the same arguement above we can replace u^{-2r} by u.

$$f_{a,0}^{(r)^W}(c) = 1 + 2^m \chi(Tr_1^n(ac^{-r(2^m-1)})) - \sum_{u \in U} \chi(Tr_1^n(au)$$

Again by Lemma 2.5, we have

$$f_{a,0}^{(r)^W}(c) = 2^m \chi(Tr_1^n(ac^{-r(2^m-1)})) + K_m(a)$$

if $f_{a,0}^{(r)}$ is bent, then we have

$$\pm 2^m = 2^m \chi(Tr_1^n(ac^{-r(2^m-1)})) + K_m(a)$$

This equality is satisfied if and only if $K_m(a) = 0$ since we have $|K_m(a)| < 2^m$ according
to Theorem 1.11. $\qquad \square$

2.1.2 The case where $b \neq 0$ and m is odd

In this subsection we will give the characterization of bentness of the set $\Im_n$ through the use of the support of $f_{a,b}^{(r)} \in \Im_n$. From now on, m is odd. First we will construct the support of $f_{a,b}^{(r)} \in \Im_n$.

Lemma 2.8. *Let m be an odd integer and $U = \{x \in \mathbb{F}_{2^n}^* \mid x^{2^m+1} = 1\}$. Let r be an integer such that $gcd(r, 2^m + 1) = 1$. Let $a \in \mathbb{F}_{2^m}^*$ and $b \in \mathbb{F}_4^*$. Let $f_{a,b}^{(r)}$ be a Boolean function in the set of $\Im_n$. We have the following support structure of $f_{a,b}^{(r)}$,*

$$supp(f_{a,b}^{(r)}) = \bigcup_{u \in S_{a,b}} u\mathbb{F}_{2^m}^*, \quad with \ S_{a,b} = \{ u \in U \mid f_{a,b}^{(r)}(u) = 1 \} \tag{2.6}$$

Proof. By Lemma 2.2, we know $\forall x \in \mathbb{F}_{2^n}^*$, $\exists u \in U$ and $\exists y \in \mathbb{F}_{2^m}^*$ such that $x = uy$. Also we know that by Lemma 2.1, $gcd(3, 2^m - 1) = 1$ and $gcd(3, 2^m + 1) \neq 1$. Then we have

$$\begin{aligned}
f_{a,b}^{(r)}(x) = f_{a,b}^{(r)}(uy) &= Tr_1^n(a(uy)^{r(2^m-1)}) + Tr_1^2(b(uy)^{(\frac{2^n-1}{3})}) \\
&= Tr_1^n(au^{r(2^m-1)}) + Tr_1^2(b(uy)^{(2^m-1)(\frac{2^m+1}{3})}) \\
&= Tr_1^n(au^{r(2^m-1)}) + Tr_1^2(bu^{(\frac{2^n-1}{3})}) \\
&= f_{a,b}^{(r)}(u)
\end{aligned}$$

Now we know that $f_{a,b}^{(r)}$ only depends on the set U. Moreover $f_{a,b}^{(r)}$ is constant on each coset of $\mathbb{F}_{2^m}^*$. For some $s \in U$, if $f_{a,b}^{(r)}(s) = 1$, then $f_{a,b}^{(r)}(z) = 1$ for all $z \in s\mathbb{F}_{2^m}^*$. Hence we have the result. $\qquad \square$

Now we can say that, according to Theorem 1.8, the set of functions $f_{a,b}^{(r)} \in \Im_n$ is in the $\mathcal{PS}^-$ class when m is odd. Moreover we can state the following proposition.

Proposition 2.9. *Let $n = 2m$, m be an odd integer and r be an integer such that $gcd(r, 2^m + 1) = 1$. Let $S_{a,b} = \{ u \in U \mid f_{a,b}^{(r)}(u) = 1 \}$. Then the Boolean function $f_{a,b}^{(r)} \in \Im_n$ is bent if and only if $wt(f_{a,b}^{(r)}|U) = 2^{m-1}$ where $wt(f)$ is the cardinality of its support i.e. $\left| S_{a,b} \right| = 2^{m-1}$.*

Proof. The result follows from Lemma 2.8 and Theorem 1.8. $\qquad \square$

Now we will restate the previous proposition after we introduce the following sum

$$\Lambda(a, b) := \sum_{u \in U} \chi(f_{a,b}^{(r)}(u)), \quad \forall(a, b) \in \mathbb{F}_{2^m}^* \times \mathbb{F}_4^*. \tag{2.7}$$

18

Corollary 2.10. *Let $n = 2m$, m be an odd integer. Then the Boolean function $f_{a,b}^{(r)} \in \mathfrak{I}_n$ is bent if and only if $\Lambda(a, b) = 1$.*

Proof. Let $A = \{u \in U \mid f_{a,b}^{(r)}(u) = 1\}$ and $B = \{u \in U \mid f_{a,b}^{(r)}(u) = 0\}$. Then we have

$$
\begin{aligned}
\Lambda(a, b) = \sum_{u \in U} \chi(f_{a,b}^{(r)}(u)) &= \sum_{u \in B} 1 - \sum_{u \in A} 1 \\
&= |B| - |A| = |U| - |A| - |A| \\
&= 2^m + 1 - 2|A| = 2^m + 1 - 2wt(f_{a,b}^{(r)}|U)
\end{aligned} \tag{2.8}
$$

By Proposition 2.9, $f_{a,b}^{(r)}$ is bent if and only if $wt(f_{a,b}^{(r)}|U) = 2^{m-1}$ i.e. $\Lambda(a, b) = 1$ $\qquad \square$

Now we are going to introduce new sums which will help us to calculate $\Lambda(a, b)$ in terms of Kloosterman sums and cubic sums. Let V be the set $\{u^3 \mid u \in U\}$ and ζ be a primitive element of the cyclic group $U = \{x \in \mathbb{F}_{2^n}^* \mid x^{2^m+1} = 1\}$. Define the sums

$$
S_i(a) = \sum_{v \in V} \chi(Tr_1^n(a\zeta^i v)), \quad i \in \{0, 1, 2\}, \quad \forall a \in \mathbb{F}_{2^m}^* \tag{2.9}
$$

Now we need the following two lemmas to show relations between $S_i(a)$ and Kloosterman and cubic sums.

Lemma 2.11. [6] *Let $n = 2m$, m be an odd integer and $a \in \mathbb{F}_{2^m}^*$. We have*

$$
2 \sum_{\substack{c \in \mathbb{F}_{2^m} \\ Tr_1^m(1/c) = 1}} \chi(Tr_1^m(ac^3 + ac)) = 2C_m(a, a) - K_m(a).
$$

To prove this lemma, first we need the following lemma.

Lemma 2.12. *The cubic equation $x^3 + x = a$ where $a \in \mathbb{F}_{2^m}$, $a \neq 0$ has a unique solution $x \in \mathbb{F}_{2^m}$ if and only if $Tr_1^m(1/a) \neq Tr_1^m(1)$.*

Proof. Set $x = 1/y$. Then the equation becomes $ay^3 + y^2 + 1 = 0$. If we set $y = z + 1$, then the equation becomes $az^3 + (a+1)z^2 + az + z = 0$ or $z^3 + bz^2 + z + 1 = 0$ where $b = (a+1)/a$. So equation $(*)$ $x^3 + x + a = 0$ has a unique solution if and only if equation $(**)$ $z^3 + bz^2 + z + 1 = 0$ has. If u is a solution of $(**)$, then $v = 1/(u+1)$ or $u = (v+1)/v$ is a solution of $(*)$. Suppose u is a solution of $(**)$, then $u^3 + bu^2 + u + 1 = 0$ i.e. $u^4 + bu^3 + u^2 + u = 0$. Then

$$
Tr_1^m(u^4 + bu^3 + u^2 + u) = Tr_1^m(0) = 0 = Tr_1^m(u^4) + Tr_1^m(bu^3) + Tr_1^m(u^2) + Tr_1^m(u)
$$

19

Since $Tr_1^m(u^4) = Tr_1^m(u^2)$, we have $Tr_1^m(bu^3) = Tr_1^m(u)$. Also $bu^3 + b^2u^2 + bu + b = 0$ implies $Tr_1^m(bu^3) = Tr_1^m(b)$. Therefore we have $Tr_1^m(u) = Tr_1^m(b)$. Since u is a root of $(**)$,

$$u^3 + bu^2 + u + 1 = 0 \quad \Longrightarrow \quad b = \frac{u+1}{u^2} + u$$

Then

$$z^3 + bz^2 + z + 1 = 0 \quad \Longrightarrow \quad z^3 + \frac{u+1}{u^2}z^2 + uz^2 + 1 + \frac{u+1}{u}z + \frac{z}{u} = 0$$

$$\Longrightarrow \quad z\Big(z^2 + \frac{u+1}{u^2}z + \frac{1}{u}\Big) + u\Big(z^2 + \frac{u+1}{u^2}z + \frac{1}{u}\Big) = (z+u)\Big(z^2 + \frac{u+1}{u^2}z + \frac{1}{u}\Big) = 0$$

If $\quad z^2 + \frac{u+1}{u^2}z + \frac{1}{u} = 0 \quad$ has no solution, then u is unique solution of $(**)$ i.e. the following equation has no solution by setting $z = w(\frac{u+1}{u^2})$ and then $w = z$

$$\Big(\frac{u+1}{u^2}z\Big)^2 + \Big(\frac{u+1}{u^2}\Big)^2 z = \frac{1}{u} \quad \Longrightarrow \quad z^2 + z = \frac{u^4}{u(u+1)^2}.$$

By using the similar arguement as in the proof of Lemma 2.4, we say that there is no solution if and only if

$$Tr_1^m(z^2 + z) \neq Tr_1^m\Big(\frac{u^4}{u(u+1)^2}\Big) \quad \text{i.e.} \quad Tr_1^m\Big(\frac{u^3}{(u+1)^2}\Big) = 1$$

Note that

$$\frac{u^3}{(u+1)^2} = \frac{u^3}{1+u^2} = u + \frac{u}{u+1} + \frac{u^2}{(u+1)^2}$$

Then

$$Tr_1^m\Big(\frac{u^3}{1+u^2}\Big) = Tr_1^m(u) + Tr_1^m\Big(\frac{u}{u+1}\Big) + Tr_1^m\Big(\frac{u^2}{(u+1)^2}\Big)$$

$$Tr_1^m\Big(\frac{u^3}{1+u^2}\Big) = Tr_1^m(u) = Tr_1^m(b).$$

Hence if $(**)$ has a unique solution, then $Tr_1^m(b) = 1 = Tr_1^m(a/(a+1)) = Tr_1^m(1) + Tr_1^m(1/a)$ i.e. $Tr_1^m(1/a) \neq Tr_1^m(1)$. If $(*)$ has three distinct roots, then $Tr_1^m(1/a) = Tr_1^m(1)$. Now we must show that if $Tr_1^m(1/a) \neq Tr_1^m(1)$, then $(*)$ has a unique solution.

Let A_i, $(i = 0, 1, 3)$ be the set of $a \in \mathbb{F}_{2^m}^*$ such that the equation $x^3 + x = a$ has i solutions in $\mathbb{F}_{2^m}$. Let X_i, $(i = 1, 3)$ be the corresponding solution sets. It is obvious that $|X_3| = 3|A_3|$ and $|X_1| = |A_1|$. Since 0 and 1 are the only solutions of $x^3 + x = 0$, all elements $x \in \mathbb{F}_{2^m} \setminus \mathbb{F}_2$ must correspond to some nonezero a and $X_1 \cup X_3 = \mathbb{F}_{2^m} \setminus \mathbb{F}_2$. Let T_i, $(i = 0, 1)$ be the set of $x \in \mathbb{F}_{2^m} \setminus \mathbb{F}_2$ such that $Tr_1^m((x+1)/x) = i$, i.e.

$Tr_1^m(1/x) + Tr_1^m(1) = i$. We already know that $X_1 \subseteq T_1$, $X_3 \subseteq T_0$, $A_1 \subseteq T_1$ and $A_3 \subseteq T_0 \cup \{1\}$. Note that we have $X_1 \cup X_3 = T_1 \cup T_0$ due to the construction of those sets. Therefore we have $X_1 = T_1$ and $X_3 = T_0$. Since $|A_1| = |X_1| = |T_1|$, we have $A_1 = X_1 = T_1$. Hence if $Tr_1^m(1/a) \neq Tr_1^m(1)$, then $x^3 + x = a$ has a unique solution in $\mathbb{F}_{2^m}$. $\square$

Now we can prove Lemma 2.11.

Proof of Lemma 2.11 . Since m is odd, $Tr_1^m(1) = 1$. By Lemma 2.12, we know that $x^3 + x = y$, $y \neq 0$ has a unique solution in $\mathbb{F}_{2^m}$ if and only if $Tr_1^m(1/y) = 0$. Note that

$$Tr_1^m\left(\frac{1}{x^3 + x}\right) = Tr_1^m\left(\frac{1}{x^2 + 1} + \frac{1}{x + 1} + \frac{1}{x}\right) = Tr_1^m(1/x)$$

Therefore we have

$$\{x^3 + x \mid x \in \mathbb{F}_{2^m}^*, \; Tr_1^m(1/x) = 0\} = \{y \in \mathbb{F}_{2^m}^* \mid Tr_1^m(1/y) = 0\}$$

Then for any $a \in \mathbb{F}_{2^m}^*$ we have

$$\sum_{\substack{x \in \mathbb{F}_{2^m} \\ Tr_1^m(1/x)=0}} \chi\left(Tr_1^m(a(x^3 + x))\right) = \sum_{\substack{y \in \mathbb{F}_{2^m} \\ Tr_1^m(1/y)=0}} \chi\left(Tr_1^m(ay)\right) \tag{2.10}$$

By using equations 2.4 and 2.5, we have

$$\sum_{\substack{y \in \mathbb{F}_{2^m} \\ Tr_1^m(1/y)=0}} \chi\left(Tr_1^m(ay)\right) = \frac{K_m(a)}{2} \tag{2.11}$$

If we combine 2.10 and 2.11, we have

$$\sum_{\substack{x \in \mathbb{F}_{2^m} \\ Tr_1^m(1/x)=0}} \chi\left(Tr_1^m(a(x^3 + x))\right) = \frac{K_m(a)}{2}$$

Then

$$C_m(a,a) = \sum_{x \in \mathbb{F}_{2^m}} \chi\left(Tr_1^m(a(x^3 + x))\right) = \frac{K_m(a)}{2} + \sum_{\substack{x \in \mathbb{F}_{2^m} \\ Tr_1^m(1/x)=1}} \chi\left(Tr_1^m(a(x^3 + x))\right)$$

Hence

$$2C_m(a,a) - K_m(a) = 2 \sum_{\substack{x \in \mathbb{F}_{2^m} \\ Tr_1^m(1/x)=1}} \chi\left(Tr_1^m(a(x^3 + x))\right)$$

$\square$

Lemma 2.13. *Let $a \in \mathbb{F}_{2^m}^*$ and m be odd. Set $U = \{x \in \mathbb{F}_{2^n}^* \mid x^{2^m+1} = 1\}$. Then we have*

$$\sum_{u \in U} \chi(Tr_1^n(au^3)) = 1 - K_m(a) + 2C_m(a, a).$$

Proof. Using the equality $Tr_m^n(au^3) = au^3 + (au^3)^{2^m}$ and the transitivity rule of trace function, we have

$$Tr_1^n(au^3) = Tr_1^m(Tr_m^n(au^3)) = Tr_1^m\left(au^3 + (au^3)^{2^m}\right).$$

Since $u^{2^m} = u^{-1}$ and $a^{2^m} = a$, we have

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

Now by lemma 2.4 we can represent every $u + u^{-1}$ by c^{-1} such that $c \in \mathbb{F}_{2^m}^*$ and $Tr(c) = 1$. Now note that $(c^{-1})^3$ represents $(u + u^{-1})^3 = u^3 + u^{-3} + u + u^{-1} = u^3 + u^{-3} + c^{-1}$ which means $c^{-3} + c^{-1} = u^3 + u^{-3}$. Then we have

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

In the last equality, we use each c^{-1} twice because when we take sum on each $u \in U \setminus \{1\}$, we get same $(u^3 + u^{-3})$ two times. Now if we use the fact that the map $c \mapsto c^{-1}$ is a permutation on $\mathbb{F}_{2^m}$, we have

$$\sum_{u \in U} \chi(Tr_1^n(au^3)) = 1 + 2 \sum_{\substack{c \in \mathbb{F}_{2^m} \\ Tr_1^m(1/c)=1}} \chi(Tr_1^m(ac^3 + ac))$$

Now by lemma 2.11, we have

$$2 \sum_{\substack{c \in \mathbb{F}_{2^m} \\ Tr_1^m(1/c)=1}} \chi(Tr_1^m(ac^3 + ac)) = 2C_m(a, a) - K_m(a).$$

Hence we have

$$\sum_{u \in U} \chi(Tr_1^n(au^3)) = 1 - K_m(a) + 2C_m(a, a).$$

$\square$

In the following lemma we are going to express $S_i(a)$ in terms of Kloosterman sums and cubic sums.

Lemma 2.14. *Let $a \in \mathbb{F}_{2^m}^*$ and m be an odd integer. We have*

$$S_0(a) = \frac{1 - K_m(a) + 2C_m(a,a)}{3}, \quad S_1(a) = S_2(a) = \frac{1 - K_m(a) - C_m(a,a)}{3}$$

Proof. Since there are 3 elements $u \in U$ for each $v \in V$ such that $u^3 = v$ (i.e. the map $u \mapsto u^3$ is 3 to 1 map on U), we have

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

Then by Lemma 2.13, we have

$$S_0(a) = \frac{1 - K_m(a) + 2C_m(a,a)}{3} \tag{2.12}$$

Now since $\{\zeta u^3 \mid u \in U\} = \{\zeta^{-1}u^{-3} \mid u \in U\} = \{\zeta^{2^m}v^{2^m} \mid v = u^3 , u \in U\}$, we have

$$S_1(a) = \sum_{v \in V} \chi(Tr_1^n(a\zeta v)) = \sum_{v \in V} \chi(Tr_1^n(a\zeta^{2^m}v^{2^m}))$$

Now note that $\zeta^{2^m-2} \in V$ since 3 divides $2^m - 2$ by Lemma 2.1, then $v \mapsto \zeta^{2^m-2}v^{2^m} = \zeta^{2^m-2}v^{-1}$ is a permutation on V which gives us

$$S_1(a) = \sum_{v \in V} \chi(Tr_1^n(a\zeta^{2^m}v^{2^m})) = \sum_{v \in V} \chi\left(Tr_1^n\left(a\zeta^2(\zeta^{2^m-2}v^{2^m})\right)\right) = S_2(a) \tag{2.13}$$

We can write

$$U = \{\zeta^{3i+j} \mid 0 \le 3i + j \le 2^m, \ 0 \le i \le \frac{2^m - 2}{3}, \ 0 \le j \le 2\} \tag{2.14}$$

which means $U = V \cup \zeta V \cup \zeta^2 V$, then we have

$$\sum_{u \in U} \chi(Tr_1^n(au)) = \sum_{j=0}^{2} \sum_{v \in V} \chi(Tr_1^n(a\zeta^i v)) = S_0(a) + S_1(a) + S_2(a)$$

Now by Lemma 2.5, we have

$$S_0(a) + S_1(a) + S_2(a) = \sum_{u \in U} \chi(Tr_1^n(au)) = 1 - K_m(a)$$

Hence by equation 2.12 and 2.13 above, we have

$$S_1(a) = S_2(a) = \frac{1 - K_m(a) - C_m(a,a)}{3}$$

$\square$

Proposition 2.15. *Let $a \in \mathbb{F}_{2^m}^*$ and m be an odd integer. Let β be a primitive element of $\mathbb{F}_4$. Then We have*

$$\Lambda(a,1) = \frac{K_m(a) + 4C_m(a,a) - 1}{3}, \qquad \Lambda(a,\beta) = \Lambda(a,\beta^2) = \frac{K_m(a) - 2C_m(a,a) - 1}{3}$$

Proof. First we will find the relation between $\Lambda(a,b)$ and $S_i(a)$, then by Lemma 2.14, the result will follow.

$$
\begin{aligned}
\Lambda(a,b) = \sum_{u \in U} \chi(f_{a,b}^{(r)}(u)) &= \sum_{u \in U} \chi\big(Tr_1^n(au^{r(2^m-1)}) + Tr_1^2(bu^{\frac{2^n-1}{3}})\big) \\
&= \sum_{u \in U} \chi\big(Tr_1^n(au^{r(2^m-1)}) + Tr_1^2(bu^{(2^m-1)\frac{2^m+1}{3}})\big) \\
&= \sum_{u \in U} \chi\big(Tr_1^n(au^r) + Tr_1^2(bu^{\frac{2^m+1}{3}})\big)
\end{aligned}
$$

Above we haved used two facts. First, $gcd(3, 2^m - 1) = 1$ which follows from Lemma 2.1. Second, since $gcd(2^m - 1, 2^m + 1) = 1$, the mapping $u \mapsto u^{2^m-1}$ is a permutation on U. Now if we use the decomposition (2.14), $\forall a \in \mathbb{F}_{2^m}^*$, $\forall b \in \mathbb{F}_4^*$ we have

$$
\begin{aligned}
\Lambda(a,b) &= \sum_{j=0}^{2} \sum_{v \in V} \chi\big(Tr_1^n(a(\zeta^j v)^r) + Tr_1^2(b(\zeta^j v)^{\frac{2^m+1}{3}})\big) \\
&= \sum_{j=0}^{2} \chi\big(Tr_1^2(b\zeta^{j\frac{2^m+1}{3}})\big) \sum_{v \in V} \chi(Tr_1^n(a\zeta^{jr} v^r)) \qquad (2.15) \\
&= \sum_{j=0}^{2} \chi\big(Tr_1^2(b\zeta^{\frac{j}{r} \cdot \frac{2^m+1}{3}})\big) \sum_{v \in V} \chi(Tr_1^n(a\zeta^j v)) \qquad (2.16) \\
&= \sum_{j=0}^{2} \chi\big(Tr_1^2(b\zeta^{\frac{j}{r} \cdot \frac{2^m+1}{3}})\big) S_j(a) \qquad \\
&= \sum_{j=0}^{2} \chi\big(Tr_1^2(b\zeta^{j\frac{2^m+1}{3}})\big) S_j(a) \qquad (2.17)
\end{aligned}
$$

In 2.15 we used the fact that v has order $(2^m + 1)/3$. In 2.16 and 2.17 we used the fact that $gcd(r, 2^m + 1) = 1$. Now we will find the value $Tr_1^2(b\zeta^{j\frac{2^m+1}{3}})$ for each j. Since ζ is a primitive element of U, $\zeta^{\frac{2^m+1}{3}}$ has order 3 in $\mathbb{F}_{2^n}$ which means $\zeta^{\frac{2^m+1}{3}}$ is a primitive element of $\mathbb{F}_4$. Note that $Tr_1^2(1) = Tr_1^2(0) = 0$, which means other two elements in $\mathbb{F}_4$ has trace value 1 i.e. for any $b \in \mathbb{F}_4 \setminus \mathbb{F}_2$, $Tr_1^2(b) = 1$. Moreover for any $b \in \mathbb{F}_4 \setminus \mathbb{F}_2$, we have $Tr_1^2(b\zeta^{\frac{2^m+1}{3}}) + Tr_1^2(b\zeta^{2\frac{2^m+1}{3}}) = 1$ since we have either $b\zeta^{\frac{2^m+1}{3}} \in \mathbb{F}_2$ or $b\zeta^{2\frac{2^m+1}{3}} \in \mathbb{F}_2$, in other words one of them is equal to 1. Also recall that by Lemma 2.14, we know

$S_1(a) = S_2(a)$. Hence we have

$$\Lambda(a, 1) = \chi\big(Tr_1^2(1)\big)S_0(a) + \chi\big(Tr_1^2(\zeta^{\frac{2^{m+1}}{3}})\big)S_1(a) + \chi\big(Tr_1^2(\zeta^{2\frac{2^{m+1}}{3}})\big)S_2(a)$$

$$= S_0(a) - 2S_1(a)$$

$$\Lambda(a, \beta) = \chi\big(Tr_1^2(\beta)\big)S_0(a) + \chi\big(Tr_1^2(\beta\zeta^{\frac{2^{m+1}}{3}})\big)S_1(a) + \chi\big(Tr_1^2(\beta\zeta^{2\frac{2^{m+1}}{3}})\big)S_2(a)$$

$$= S_0(a)$$

$$\Lambda(a, \beta^2) = \chi\big(Tr_1^2(\beta^2)\big)S_0(a) + \chi\big(Tr_1^2(\beta^2\zeta^{\frac{2^{m+1}}{3}})\big)S_1(a) + \chi\big(Tr_1^2(\beta^2\zeta^{2\frac{2^{m+1}}{3}})\big)S_2(a)$$

$$= S_0(a)$$

$\square$

The following property of cubic sums is useful.

Lemma 2.16. *Let m be odd and $a \in \mathbb{F}_{2^m}^*$. Then $C_m(a, a) = C_m(1, a^{2/3})$.*

Proof. By Lemma 2.1, the mapping $x \mapsto x^3$ is a permutation on $\mathbb{F}_{2^m}$ which means every element $a \in \mathbb{F}_{2^m}$ can be written as $a = c^3$ s.t. $c \in \mathbb{F}_{2^m}$. Then we have

$$C_m(a, a) := \sum_{x \in \mathbb{F}_{2^m}} \chi\big(Tr_1^m(ax^3 + ax)\big) = \sum_{x \in \mathbb{F}_{2^m}} \chi\big(Tr_1^m((cx)^3 + ax)\big)$$

$$C_m(a, a) = \sum_{x \in \mathbb{F}_{2^m}} \chi\big(Tr_1^m((cx)^3 + a^{2/3}(cx))\big) = \sum_{x \in \mathbb{F}_{2^m}} \chi\big(Tr_1^m(x^3 + a^{2/3}x)\big)$$

$$C_m(a, a) = C_m(1, a^{2/3})$$

$\square$

The following two results are very useful and we will use them in order to prove the characterization of bentness. We do not include the proofs here since they are very long and technical.

Theorem 2.17. [4] *Let m be an odd integer. For the cubic sums on $\mathbb{F}_{2^m}$, we have*

1. *$C_m(1, 1) = \big(\frac{2}{m}\big)2^{(m+1)/2}$ where $\big(\frac{2}{m}\big)$ 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 $C_m(1, c) = \chi(Tr_1^m(\gamma^3 + \gamma))\big(\frac{2}{m}\big)2^{(m+1)/2}$ where $c = \gamma^4 + \gamma + 1$ for some $\gamma \in \mathbb{F}_{2^m}$.*

25

Here we have an interesting fact due to Charpin, Helleseth and Zinoviev.

Lemma 2.18. [6] *Let $m \geq 3$ be an odd integer and $a \in \mathbb{F}_{2^m}^*$. Then*

$$K_m(a) - 1 \equiv 0 \pmod{3} \quad \Longleftrightarrow \quad Tr_1^m(a^{1/3}) = 0$$

Now we can give the characterization of bentness of the set of the functions $f_{a,b}^{(r)} \in \mathfrak{F}_n$ for the case where $b \neq 0$ and m is odd.

Theorem 2.19. *Let $n = 2m$, m be odd and $m > 3$. Let $a \in \mathbb{F}_{2^m}^*$ and β be a primitive element of $\mathbb{F}_4$. Let r be an integer such that $gcd(r, 2^m + 1) = 1$. Let $f_{a,1}^{(r)}$, $f_{a,\beta}^{(r)}$ and $f_{a,\beta^2}^{(r)}$ be the Boolean functions in the set $\mathfrak{F}_n$. Then $f_{a,1}^{(r)}$, $f_{a,\beta}^{(r)}$ and $f_{a,\beta^2}^{(r)}$ are bent if and only if $K_m(a) = 4$.*

Proof. By Lemma 2.16, we know $C_m(a, a) = C_m(1, a^{2/3})$ for any $a \in \mathbb{F}_{2^m}^*$ where m is odd.

($\Leftarrow$) Suppose $K_m(a) = 4$. Then by Lemma 2.18, we have $Tr_1^m(a^{1/3}) = 0$. Also $Tr_1^m(a^{1/3}) = 0$ means $Tr_1^m(a^{2/3}) = 0$. Recall Theorem 2.17, it says if $Tr_1^m(a^{2/3}) = 0$ then $C_m(1, a^{2/3}) = 0$. Also by the arguement at the beginning of the proof we have $C_m(a, a) = 0$. Now by Corollary 2.10 and Proposition 2.15, we can say that $f_{a,1}^{(r)}$, $f_{a,\beta}^{(r)}$ and $f_{a,\beta^2}^{(r)}$ are bent if and only if $(K_m(a) - 1)/3 = 1$ i.e. $K_m(a) = 4$.

($\Rightarrow$) We will show it by contrapositive. Suppose $K_m(a) \neq 4$. Then By Lemma 2.18, we have $Tr_1^m(a^{1/3}) = 1$. Also $Tr_1^m(a^{1/3}) = 1$ means $Tr_1^m(a^{2/3}) = 1$. Again recall Theorem 2.17, it says if $Tr_1^m(a^{2/3}) = 1$ then $C_m(1, a^{2/3}) = \pm 2^{(m+1)/2}$. Also by the arguement at the beginning of the proof we have $C_m(a, a) = \pm 2^{(m+1)/2}$. Now by Corollary 2.10 and Proposition 2.15, we can say that $f_{a,\beta}^{(r)}$ and $f_{a,\beta^2}^{(r)}$ are bent if and only if

$$\Lambda(a, \beta) = \Lambda(a, \beta^2) = \frac{K_m(a) - 1 \mp 2^{(m+3)/2}}{3} = 1$$

$$\text{i.e.} \quad K_m(a) = 4 \pm 2^{(m+3)/2}.$$

Also we have the similar arguement for $f_{a,1}^{(r)}$. That is, $f_{a,1}^{(r)}$ is bent if and only if $K_m(a) = 4 \mp 2^{(m+5)/2}$. Note that by Theorem 1.11, we know Kloosterman sum K_m takes integer values in the range $[-2^{(m+2)/2} + 1, 2^{(m+2)/2} + 1]$. But the values that makes $f_{a,\beta}^{(r)}$, $f_{a,\beta^2}^{(r)}$ and $f_{a,1}^{(r)}$ bent are not in the range for any $m > 3$. Hence $f_{a,\beta}^{(r)}$, $f_{a,\beta^2}^{(r)}$ and $f_{a,1}^{(r)}$ are not bent if $K_m(a) \neq 4$. $\qquad \square$

2.1.3 The case where $b \neq 0$ and m is even

In the case where m is even, $f_{a,b}^{(r)}$ is not constant on $\mathbb{F}_{2^m}^*$ therefore we can not express the support of $f_{a,b}^{(r)}$ by cosets of $\mathbb{F}_{2^m}^*$ because in the proof of Lemma 2.8, we have used the fact that $gcd(3, 2^m - 1) = 1$ when m is odd. But we can give the following necessary condition.

Theorem 2.20. *Let $n = 2m$, m be odd and $m > 2$. Let $a \in \mathbb{F}_{2^m}^*$ and $b \in \mathbb{F}_4^*$. Let r be an integer such that $gcd(r, 2^m + 1) = 1$. Let $f_{a,b}^{(r)}$ be the Boolean function in the set $\Im_n$. If $f_{a,b}^{(r)}$ is bent, then $K_m(a) = 4$.*

Proof. Suppose $f_{a,b}^{(r)}$ is bent, then we must have $f_{a,b}^{(r)^W}(0) = \pm 2^m$. Now we are going to calculate $f_{a,b}^{(r)^W}(0)$. By Lemma 2.2, for any $x \in \mathbb{F}_{2^n}^*$ we can uniquely write $x = uy$ where $u \in U$ and $y \in \mathbb{F}_{2^m}^*$. Then we have

$$f_{a,b}^{(r)^W}(0) = \sum_{x \in \mathbb{F}_{2^n}} \chi\big(f_{a,b}^{(r)}(x)\big) = 1 + \sum_{x \in \mathbb{F}_{2^n}^*} \chi\big(f_{a,b}^{(r)}(x)\big)$$

$$= 1 + \sum_{u \in U} \sum_{y \in \mathbb{F}_{2^m}^*} \chi\big(f_{a,b}^{(r)}(uy)\big)$$

$$= 1 + \sum_{u \in U} \sum_{y \in \mathbb{F}_{2^m}^*} \chi\Big(Tr_1^n(a(uy)^{r(2^m-1)}) + Tr_1^2(b(uy)^{\frac{2^n-1}{3}})\Big)$$

$$= 1 + \sum_{u \in U} \chi\big(Tr_1^n(au^{r(2^m-1)})\big) \sum_{y \in \mathbb{F}_{2^m}^*} \chi\big(Tr_1^2(by^{\frac{2^n-1}{3}})\big)$$

The last equality holds because of the facts that $y^{2^m-1} = 1$ and that $u^{\frac{2^n-1}{3}} = 1$ since $gcd(3, 2^m + 1) = 1$. Now let $C = \{y^3 \mid y \in \mathbb{F}_{2^m}^*\}$ and $\beta \in \mathbb{F}_{2^m} \setminus C$. Then we can partition $\mathbb{F}_{2^m}^*$ as $\mathbb{F}_{2^m}^* = C \cup \beta C \cup \beta^2 C$. Now if we write $f_{a,b}^{(r)^W}(0)$ again, we have

$$f_{a,b}^{(r)^W}(0) = 1 + \sum_{u \in U} \chi\big(Tr_1^n(au^{r(2^m-1)})\big) \sum_{j=0}^{2} \sum_{c \in C} \chi\big(Tr_1^2(b(c\beta^j)^{\frac{2^n-1}{3}})\big)$$

Now note that $\beta^{\frac{2^n-1}{3}}$ has order 3 which means it is in $\mathbb{F}_4^*$. Also we know c is a cube of an element of $\mathbb{F}_{2^m}^*$. If we use these facts, we have

$$\sum_{j=0}^{2} \sum_{c \in C} \chi\big(Tr_1^2(b(c\beta^j)^{\frac{2^n-1}{3}})\big) = \sum_{c \in C} \sum_{j=0}^{2} \chi\big(Tr_1^2(b\beta^{j\frac{2^n-1}{3}})\big) = \sum_{c \in C} \sum_{\tau \in \mathbb{F}_4^*} \chi\big(Tr_1^2(\tau)\big)$$

$$= \sum_{c \in C} \left(\sum_{\tau \in \mathbb{F}_4} \chi\big(Tr_1^2(\tau)\big) - 1 \right)$$

$$= \sum_{c \in C} (-1) = -\frac{2^m - 1}{3}.$$

27

Now we have
$$f_{a,b}^{(r)W}(0) = 1 - \frac{2^m - 1}{3} \sum_{u \in U} \chi\left(Tr_1^n(au^{r(2^m-1)})\right)$$

We know $gcd(r, 2^m + 1) = 1$ and $gcd(2^m - 1, 2^m + 1) = 1$, therefore the mappings $u \mapsto u^r$ and $u \mapsto u^{2^m-1}$ are permutations on U. Then we have
$$f_{a,b}^{(r)W}(0) = 1 - \frac{2^m - 1}{3} \sum_{u \in U} \chi\left(Tr_1^n(au)\right)$$

By Lemma 2.5, we can write it as follows
$$f_{a,b}^{(r)W}(0) = 1 + \frac{2^m - 1}{3}\left(K_m(a) - 1\right)$$

If $f_{a,b}^{(r)W}(0) = 2^m$, then $K_m(a) = 4$. If $f_{a,b}^{(r)W}(0) = -2^m$, then $K_m(a)$ is not an integer which is impossible. Hence we have the result. □

Now we are going to prove that the bentness of $f_{a,b}^{(r)}$ is equivalent to the bentness of $f_{a,1}^{(r)}$.

Proposition 2.21. [24] *Let $n = 2m$, m be odd and $m > 2$. Let $a \in \mathbb{F}_{2^m}^*$ and $b \in \mathbb{F}_4^*$. Let r be an integer such that $gcd(r, 2^m + 1) = 1$. Let $f_{a,b}^{(r)}$ and $f_{a,1}^{(r)}$ be the Boolean functions in the set $\mathfrak{I}_n$. Then $f_{a,b}^{(r)}$ is bent if and only if $f_{a,1}^{(r)}$ is bent.*

Proof. By Lemma 2.1, $gcd(3, 2^m - 1) = 3$, then $\mathbb{F}_4^* \subset \mathbb{F}_{2^m}^*$. Therfore for any $b \in \mathbb{F}_4^*$ one can find $\alpha \in \mathbb{F}_{2^m}^*$ such that $\alpha^{\frac{2^m-1}{3}} = b$. If we use this fact, we have

$$\begin{aligned}
f_{a,b}^{(r)}(x) &= Tr_1^n\left(ax^{r(2^m-1)}\right) + Tr_1^2\left(bx^{\frac{2^n-1}{3}}\right) \\
&= Tr_1^n\left(a\alpha^{r(2^m-1)}x^{r(2^m-1)}\right) + Tr_1^2\left(\alpha^{\frac{2^m-1}{3}}x^{\frac{2^n-1}{3}}\right) \\
&= f_{a,1}^{(r)}(\alpha x)
\end{aligned}$$

Now by this equality, for any $c \in \mathbb{F}_{2^n}^*$, we have

$$\begin{aligned}
f_{a,b}^{(r)W}(c) &= \sum_{x \in \mathbb{F}_{2^n}} \chi\left(f_{a,b}^{(r)}(x) + Tr_1^n(cx)\right) \\
&= \sum_{x \in \mathbb{F}_{2^n}} \chi\left(f_{a,1}^{(r)}(\alpha x) + Tr_1^n(cx)\right) \\
&= \sum_{x \in \mathbb{F}_{2^n}} \chi\left(f_{a,1}^{(r)}(x) + Tr_1^n(c\alpha^{-1}x)\right) \\
&= f_{a,b}^{(r)W}(c\alpha^{-1})
\end{aligned}$$

Above we have used the fact that the mapping $x \mapsto \alpha x$ is a permutation on $\mathbb{F}_{2^n}$. □

2.2 The characterization of the functions $f_{a,b}^{(r)} \in \Im_n$ where $r = 3$

In this section we are going to give the characterization of the bentness of the set of functions $f_{a,b}^{(3)} \in \Im_n$. First, recall the set of the functions $\Im_n$:

Let $n = 2m$ be a positive integer. Let $a \in \mathbb{F}_{2^n}$ and $b \in \mathbb{F}_4^*$. Define the set of the Boolean functions $f_{a,b}^{(3)}$, denoted by $\Im_n$, on $\mathbb{F}_{2^n}$ as:

$$\forall x \in \mathbb{F}_{2^n}, \quad f_{a,b}^{(3)}(x) = Tr_1^n(ax^{3(2^m-1)}) + Tr_1^2(bx^{(\frac{2^n-1}{3})}). \tag{2.18}$$

Remark 2.22. First note that by Lemma 2.1, 3 divides $2^m + 1$ when m is odd. Now recall Definition 1.6 and Lemma 1.7. Unlike the other bent functions $f_{a,0}^{(r)}$ where $gcd(r, 2^m + 1)$, $f_{a,0}^{(3)}$ which becomes monomial function is not a bent function since neither $gcd(3(2^m - 1), 2^m - 1)$ nor $gcd(3(2^m - 1), 2^m + 1)$ is equal to 1.

Now we can state a proposition which is similar to Proposition 2.3 as in the previous section. Then we can restrict our study to a smaller set instead of $\mathbb{F}_{2^n}$. However, we can not restrict our study to $\mathbb{F}_{2^m}$ since $r = 3$ is not coprime to $2^m + 1$. For that restriction, first recall that in 2.14, we partitioned the set $U = \{x \in \mathbb{F}_{2^n}^* \mid x^{2^m+1} = 1\}$ as $U = V \cup \zeta V \cup \zeta^2 V$ where $V = \{u^3 \mid u \in U\}$ and ζ is a generator of the cyclic group U. Then by Lemma 2.2, we can represent any $a \in \mathbb{F}_{2^n}^*$ uniquely as $a = a'\zeta^i v$ where $v \in V$ and $a' \in \mathbb{F}_{2^m}^*$.

Proposition 2.23. *Let $f_{a,b}^{(3)}$ be a Boolean function in the set $\Im_n$ defined as in (2.18). Let ζ be a generator of the cyclic group $U = \{x \in \mathbb{F}_{2^n}^* \mid x^{2^m+1} = 1\}$. Then we have*

$$\{(a,b) \mid a \in \mathbb{F}_{2^n}^*, \ b \in \mathbb{F}_4^*, \ f_{a,b}^{(3)} \ is \ bent \ \} = \tag{2.19}$$

$$\{(a'\zeta^i\lambda^{3(2^m-1)}, b'\lambda^{\frac{2^n-1}{3}}) \mid a' \in \mathbb{F}_{2^m}^*, \ b' \in \mathbb{F}_4^*, \ \lambda \in \mathbb{F}_{2^n}^*, \ 0 \le i \le 2, \ f_{a'\zeta^i,b'}^{(3)} \ is \ bent\} \tag{2.20}$$

Proof. Let $a \in \mathbb{F}_{2^n}^*$, $b \in \mathbb{F}_4^*$ and $a' \in \mathbb{F}_{2^m}^*$. First note that if $a = a'\zeta^i\lambda^{3(2^m-1)}$ and $b = b'\lambda^{\frac{2^n-1}{3}}$ for some $\lambda \in \mathbb{F}_{2^n}^*$ and $b' \in \mathbb{F}_4^*$, then we have for all $x \in \mathbb{F}_{2^n}$

$$f_{a,b}^{(3)}(x) = Tr_1^n(a'\zeta^i\lambda^{3(2^m-1)}x^{3(2^m-1)}) + Tr_1^2(b'\lambda^{(\frac{2^n-1}{3})}x^{(\frac{2^n-1}{3})}) = f_{a'\zeta^i,b'}^{(3)}(\lambda x)$$

Since the mapping $x \mapsto \lambda x$ is a permutation on $\mathbb{F}_{2^n}$ we have that $f_{a,b}^{(3)}$ is bent if and only if $f_{a'\zeta^i,b'}^{(3)}$. Now it is clear that the set 2.19 already includes the set 2.20. Now we will show that the set 2.20 includes the set 2.19. Let $a \in \mathbb{F}_{2^n}^*$, $b \in \mathbb{F}_4^*$. By Lemma 2.2,

29

we can say that $\exists a' \in \mathbb{F}_{2^m}^*$ and $\exists u \in U$ such that $a = a'u$, moreover $a = a'\zeta^i v$ for some $0 \leq i \leq 2$ and $v \in V$. Suppose ξ is a generator of $\mathbb{F}_{2^n}^*$, then ξ^{2^m-1} is a generator of U. Also we know $v = u^3$ for some $u \in U$. Suppose $u = (\xi^{2^m-1})^k$ for some integer k. Then $v = u^3 = (\xi^k)^{3(2^m-1)}$ which gives us $a = a'\zeta^i(\xi^k)^{3(2^m-1)}$. One can call ξ^k as λ. Now note that $\lambda^{\frac{2^n-1}{3}} \in \mathbb{F}_4^*$ since it has order 3. Hence we have found related $a'\zeta^i$ and b' for any $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_4^*$. $\qquad\square$

Due to result above, from now on we will restrict our study to the bentness of $f_{a\zeta^i,b}^{(3)}$ with $a \in \mathbb{F}_{2^m}^*$.

Lemma 2.24. *Let $a \in \mathbb{F}_{2^n}^*$, $b \in \mathbb{F}_4^*$ and m be odd. Define $\Gamma(a,b) := \sum_{u \in U} \chi(f_{a,b}^{(3)}(u))$. Then $f_{a,b}^{(3)} \in \Im_n$ is bent if and only if $\Gamma(a,b) = 1$.*

Proof. See the proof of Corollary 2.10 since the proof is similar. $\qquad\square$

Now we are going to use the sums defined in (2.9) which will help us to calculate $\Gamma(a,b)$ in terms of Kloosterman sums and cubic sums. Let V be the set $\{u^3 \mid u \in U\}$ and ζ be a primitive element of the cyclic group $U = \{x \in \mathbb{F}_{2^n}^* \mid x^{2^m+1} = 1\}$. Define the sums

$$S_i(a) = \sum_{v \in V} \chi(Tr_1^n(a\zeta^i v)), \quad i \in \{0,1,2\}, \quad \forall a \in \mathbb{F}_{2^m}^* \qquad (2.21)$$

In Lemma 2.14, $S_i(a)$ are already expressed in terms of Kloosterman sums and cubic sums. In the following lemma we will express the relations between $S_i(a)$ and $\Gamma(a,b)$.

Lemma 2.25. *Let m be odd, $a \in \mathbb{F}_{2^m}^*$, β be a primitive element of $\mathbb{F}_4$ and ζ be a generator of the cyclic group $U = \{x \in \mathbb{F}_{2^n}^* \mid x^{2^m+1} = 1\}$. Assume that $m \not\equiv 3 \pmod 6$, then for $(i,j) \in \{0,1,2\}^2$ we have $\Gamma(a\zeta^i, \beta^j) = -S_i(a)$ where $\Gamma(a,b) := \sum_{u \in U} \chi(f_{a,b}^{(3)}(u))$.*

Proof. Since the map $u \mapsto u^{2^m-1}$ is a permutation of U and $(2^n-1) = (2^m+1)(2^m-1)$, we have

$$\Gamma(a\zeta^i, \beta^j) := \sum_{u \in U} \chi\left(f_{a\zeta^i,\beta^j}^{(3)}(u)\right) = \sum_{u \in U} \chi\left(Tr_1^n(a\zeta^i u^{3(2^m-1)}) + Tr_1^2(\beta^j u^{(\frac{2^n-1}{3})})\right)$$

$$= \sum_{u \in U} \chi\left(Tr_1^n(a\zeta^i u^3) + Tr_1^2(\beta^j u^{(\frac{2^m+1}{3})})\right)$$

By the set equality (2.14) we can partition U as follows

$$\Gamma(a\zeta^i, \beta^j) = \sum_{k=0}^{2} \sum_{v \in V} \chi\left(Tr_1^n(a\zeta^i(\zeta^k v)^3) + Tr_1^2(\beta^j(\zeta^k v)^{(\frac{2^m+1}{3})}) \right)$$

Since the set V has order $\frac{2^m+1}{3}$

$$\Gamma(a\zeta^i, \beta^j) = \sum_{k=0}^{2} \sum_{v \in V} \chi\left(Tr_1^n(a\zeta^{3k+i} v^3) + Tr_1^2(\beta^j \zeta^{k(\frac{2^m+1}{3})}) \right)$$

By hypothesis $m \not\equiv 3 \pmod 6$ and Lemma 2.1, we have $gcd(3, \frac{2^m+1}{3}) = 1$ which means $v \mapsto v^3$ is a permutation on V. Then

$$\Gamma(a\zeta^i, \beta^j) = \sum_{k=0}^{2} \sum_{v \in V} \chi\left(Tr_1^n(a\zeta^{3k+i} v) + Tr_1^2(\beta^j \zeta^{k(\frac{2^m+1}{3})}) \right)$$

Since $\zeta^{3k} \in V$, $v \mapsto \zeta^{3k} v$ is a permutation on V. Then we have

$$\Gamma(a\zeta^i, \beta^j) = \sum_{k=0}^{2} \sum_{v \in V} \chi\left(Tr_1^n(a\zeta^i v) + Tr_1^2(\beta^j \zeta^{k(\frac{2^m+1}{3})}) \right)$$

Note that $\zeta^{(\frac{2^m+1}{3})} \in \mathbb{F}_4^*$ and $\zeta^{(\frac{2^m+1}{3})} \neq 1$. Then $\mathbb{F}_4^* = \{\beta^j, \beta^j\zeta^{(\frac{2^m+1}{3})}, \beta^j\zeta^{2(\frac{2^m+1}{3})}\}$. $\mathbb{F}_4$ has two elements of absolute trace of value 1 and two elements of absolute trace of value 0. Since $Tr_1^2(0) = 0$, in the set $\{\beta^j, \beta^j\zeta^{(\frac{2^m+1}{3})}, \beta^j\zeta^{2(\frac{2^m+1}{3})}\}$, there are 2 elements of absolute trace of value 1 and one element of absolute trace of value 0. Therefore we have

$$\begin{aligned}
\Gamma(a\zeta^i, \beta^j) &= 2\sum_{v \in V} \chi\left(Tr_1^n(a\zeta^i v) + 1 \right) + \sum_{v \in V} \chi\left(Tr_1^n(a\zeta^i v) + 0 \right) \\
&= -2\sum_{v \in V} \chi\left(Tr_1^n(a\zeta^i v) \right) + \sum_{v \in V} \chi\left(Tr_1^n(a\zeta^i v) \right) \\
&= -\sum_{v \in V} \chi\left(Tr_1^n(a\zeta^i v) \right) \\
&= -S_i(a)
\end{aligned}$$

$\square$

Now we can state and prove the following theorem which describes the bent functions in the family $\Im_n$.

Theorem 2.26. *Let m be odd, $a \in \mathbb{F}_{2^m}^*$, β be a primitive element of $\mathbb{F}_4$ and ζ be a generator of the cyclic group $U = \{x \in \mathbb{F}_{2^n}^* \mid x^{2^m+1} = 1\}$. Let $f_{a\zeta^i,\beta^j}^{(3)}$ be a function in the family $\Im_n$ defined as in (2.18) for $(i, j) \in \{0, 1, 2\}^2$.*

1. *Assume* $m \not\equiv 3 \pmod{6}$. *Then we have:*

   - *If* $Tr_1^m(a^{1/3}) = 0$, *then, for every* $(i, j) \in \{0, 1, 2\}^2$, *the function* $f^{(3)}_{a\zeta^i, \beta^j}$ *is bent if and only if* $K_m(a) = 4$.

   - *If* $Tr_1^m(a^{1/3}) = 1$, *then:*

     (a) $f^{(3)}_{a, \beta^j}$ *is not bent for any* $j \in \{0, 1, 2\}$.

     (b) *For every* $i \in \{1, 2\}$, $f^{(3)}_{a\zeta^i, \beta^j}$ *is bent if and only if* $K_m(a) + C_m(a, a) = 4$.

2. *Assume* $m \equiv 3 \pmod{6}$. *Then* $f^{(3)}_{a\zeta^i, b}$ *is not bent for any* $i \in \{0, 1, 2\}$, $a \in \mathbb{F}_{2^m}^*$ *and* $b \in \mathbb{F}_4^*$.

Proof.

1. Assume $m \not\equiv 3 \pmod{6}$.

   - If $Tr_1^m(a^{1/3}) = 0$, then we have $Tr_1^m(a^{2/3}) = 0$ since $Tr_1^m(a^{2/3}) = Tr_1^m(a^{1/3})$. If we use $Tr_1^m(a^{2/3}) = 0$, by lemmas 2.17 and 2.16, we have $C_m(a, a) = 0$. Now recall the Lemma 2.14 and use the equality $C_m(a, a) = 0$, then we have

     $$-S_i(a) = \frac{K_m(a) - 1}{3}$$

     Therefore, due to Lemma 2.25,

     $$\Gamma(a\zeta^i, \beta^j) = -\frac{K_m(a) - 1}{3}$$

     Hence by Lemma 2.24, $f^{(3)}_{a\zeta^i, \beta^j}$ is bent if and only if $\frac{K_m(a) - 1}{3} = 1$.

   - If $Tr_1^m(a^{1/3}) = 1$, then by Lemma 2.16 and Lemma 2.17, we have $C_m(a, a) = \pm(\frac{2}{m})2^{(m+1)/2}$.

     (a) Let $j \in \{0, 1, 2\}$. By Lemma 2.25, we have $\Gamma(a, \beta^j) = -S_0(a)$, also by Lemma 2.14 we have

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

     therefore we obtain that

     $$\Gamma(a, \beta^j) = \frac{K_m(a) - 1 \pm (\frac{2}{m})2^{(m+3)/2}}{3}.$$

     Now by Lemma 2.24, $f^{(3)}_{a, \beta^j}$ is bent if and only if

     $$1 = \Gamma(a, \beta^j) = \frac{K_m(a) - 1 \pm (\frac{2}{m})2^{(m+3)/2}}{3}$$

i.e. $K_m(a) = 4 \pm (\frac{2}{m})2^{(m+3)/2}$. From Theorem 1.11, we know that the Kloosterman sums take values in the range $[-2^{(m+2)/2} + 1, 2^{(m+2)/2} + 1]$ which tells us that $K_m(a) = 4 \pm (\frac{2}{m})2^{(m+3)/2}$ is not possible for $m > 3$.

(b) As in the previous case we have

$$\Gamma(a\zeta^i, \beta^j) = \frac{K_m(a) - 1 + C_m(a,a)}{3}$$

for every $i \in \{1,2\}$ and $j \in \{0,1,2\}$. Hence by Lemma 2.24, we have that $f^{(3)}_{a\zeta^i, \beta^j}$ is bent if and only if $K_m(a) + C_m(a,a) = 4$.

2. Assume $m \equiv 3 \pmod 6$. From Lemma 2.24, we know that $f^{(3)}_{a\zeta^i, b}$ is bent if and only if $\Gamma(a\zeta^i, b) = 1$ in other words $\sum_{u \in U} \chi(f^{(3)}_{a\zeta^i, b}(u)) = 1$. Now we will try to calculate the sum $\sum_{u \in U} \chi(f^{(3)}_{a\zeta^i, b}(u))$. Note that we already know 9 divides $2^m + 1$ by our hypothesis and proof of Lemma 2.1. Then

$$\sum_{u \in U} \chi(f^{(3)}_{a\zeta^i, b}(u)) = \sum_{u \in U} \chi(Tr_1^n(a\zeta^i u^{3(2^m - 1)}) + Tr_1^2(bu^{3(2^m - 1) \cdot \frac{2^m + 1}{9}}))$$

Since $gcd(2^m - 1, 2^m + 1) = 1$, the mapping $x \mapsto x^{2^m - 1}$ is a permutation on U and the mapping $x \mapsto x^3$ is 3-to-1 on U, then we have that the mapping $x \mapsto x^{3(2^m - 1)}$ is a 3-to-1 from U to V. Using that fact, we obtain

$$\sum_{u \in U} \chi(f^{(3)}_{a\zeta^i, b}(u)) = 3 \sum_{v \in V} \chi(Tr_1^n(a\zeta^i v) + Tr_1^2(bv^{\frac{2^m + 1}{9}}))$$

This sum is not equal to 1 since it is divisible by 3, hence $f^{(3)}_{a\zeta^i, b}$ is not bent.

$\square$

3

Hyper-bent Boolean Functions

As we have noted earlier, bent functions have the maximal distance to all the coordinate functions of affine monomials in the form $Tr_1^n(ax) + \epsilon$ where $\epsilon \in \mathbb{F}_2$. The idea behind this property of bent functions comes from S-Boxes, since S-Boxes are designed so that they can not be approximated by affine monomials. In 1999, Gong and Golomb have introduced a new criteria for S-Boxes in [12] . They said that S-Boxes should not be approximated also by bijective monomials. For that reason they have introduced a new tool called *extended Walsh-Hadamard transform*. Then, in [28] Youssef and Gong have shown that those kind of functions which have maximal distance to all coordinate functions of bijective monomials in the form $Tr_1^n(ax^j) + \epsilon$ where $\epsilon \in \mathbb{F}_2$ $\gcd(j, 2^n - 1) = 1$ exist and they called those functions as *hyper-bent*.

Definition 3.1. A Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is said to be **hyper-bent** if and only if the *Extended Walsh-Hadamard* transform of f

$$f^W(a, i) = \sum_{x \in \mathbb{F}_{2^n}} \chi\big(Tr_1^n(ax^i) + f(x)\big) = \pm 2^{n/2}$$

for all $a \in \mathbb{F}_{2^n}$ and for all i such that $\gcd(i, 2^n - 1) = 1$.

We can give another useful and more simple characterization of hyper-bent functions by using relation between Walsh-Hadamard transform and extended Walsh Hadamard-transform.

Proposition 3.2. *A Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is hyper-bent if and only if the function $f(x^i)$ is bent for all i such that $gcd(i, 2^{n/2} - 1) = 1$.*

Proof. Extended Walsh-Hadamard transform of f is

$$
\begin{aligned}
f^W(a, j) &= \sum_{x \in \mathbb{F}_{2^n}} \chi\big(Tr_1^n(ax^j) + f(x)\big) \\
&= \sum_{y = x^i \in \mathbb{F}_{2^n}} \chi\big(Tr_1^n(ax^{ij}) + f(x^i)\big) \quad \text{where} \ \ ij \equiv 1 \pmod{2^n - 1} \qquad (3.1) \\
&= \sum_{x^i \in \mathbb{F}_{2^n}} \chi\big(Tr_1^n(ax) + f(x^i)\big) \\
&= \text{Walsh-Hadamard transform of } f(x^i) \ \text{ where } \ ij \equiv 1 \pmod{2^n - 1} \quad (3.2)
\end{aligned}
$$

Equality 3.1 holds since $x \mapsto x^j$ is a permutation on $\mathbb{F}_{2^n}$. Now f is hyper-bent if and only if $f^W(a, j) = \pm 2^{n/2}$ for all j, $\gcd(j, 2^n - 1) = 1$ i.e. $f(x^i)$ is bent for all i, $\gcd(i, 2^n - 1) = 1$. $\qquad\square$

Remark 3.3. Note that if a function $f(x)$ in the form 2.1 is bent then $f(x^i)$ is also bent for i coprime to $2^n - 1$. Therefore, we can say that bent functions we have studied in Chapter 2 are also hyper-bent by the previous proposition. One can also say directly that bent functions studied in Chapter 2 are hyper-bent by Proposition 3.5.

In the previous chapter we have studied the Boolean bent functions whose expression is the sum of at most two trace terms. In this chapter we are going to study hyper-bent Boolean functions with multiple trace terms which have been introduced by Mesnager in [22]. Let $n = 2m$ and m be an odd integer. Define, denoted by $\mathfrak{I}_n$, the set of Boolean functions f_b over $\mathbb{F}_{2^n}$ which have the polynomial forms as follows:

$$
f_b(x) := \sum_{r \in R} Tr_1^n(a_r x^{r(2^m - 1)}) + Tr_1^2(bx^{\frac{2^n - 1}{3}}) \qquad (3.3)
$$

where E is the set of representatives of the cyclotomic cosets modulo $2^n - 1$ with each coset having the full size n, $R \subseteq E$, $b \in \mathbb{F}_4$ and $a_r \in \mathbb{F}_{2^m}$ for all $r \in R$.

Proposition 3.4. *(Youssef and Gong [28]) Let $n = 2m$ be an even integer and α be a primitive element of $\mathbb{F}_{2^n}$. Let f be a boolean function on $\mathbb{F}_{2^n}$ such that $f(0) = 0$ and $f(\alpha^{2^m + 1} x) = f(x)$ for every $x \in \mathbb{F}_{2^n}$. Then f is hyper-bent if and only if Hamming weight of the vector $\Big(f(1), f(\alpha), f(\alpha^2), \ldots, f(\alpha^{2^m})\Big)$ equals 2^{m-1}*

Proof. See [28, Theorem 1] $\qquad\square$

Now we will modify and restate Propositon 3.4.

Proposition 3.5. *Let $n = 2m$ be an even integer and α be a primitive element of $\mathbb{F}_{2^n}$. Let f be a boolean function on $\mathbb{F}_{2^n}$ such that $f(0) = 0$ and $f(\alpha^{2^m+1}x) = f(x)$ for every $x \in \mathbb{F}_{2^n}$. Let ζ be a generator of the cyclic group $U = \{x \in \mathbb{F}_{2^n}^* \mid x^{2^m+1} = 1\}$. Then f is a hyper-bent function if and only if $|\{ i \mid f(\zeta^i) = 1,\ 0 \le i \le 2^m\}| = 2^{m-1}$.*

Proof. Recall the Proposition 3.4, f is hyper-bent if and only if

$$\left|\{ i \mid f(\alpha^i) = 1,\ 0 \le i \le 2^m\}\right| = 2^{m-1}.$$

Note that α^{2^m+1} is a generator of $\mathbb{F}_{2^m}^*$. Due to hypothesis, for any $r \in \mathbb{N}$, we have $f((\alpha^{2^m+1})^r x) = f((\alpha^{2^m+1})^{r-1}x) \quad \forall x \in \mathbb{F}_{2^n}$. Therefore f is constant on $\mathbb{F}_{2^m}^*$ (we can also say it is constant on cosets of $\mathbb{F}_{2^m}^*$). By Lemma 2.2, we know that each element $x \in \mathbb{F}_{2^n}$ can be written uniquely as $x = uy$ where $u \in U$ and $y \in \mathbb{F}_{2^m}$, then $\alpha = uy$ for some $u \in U$ and $y \in \mathbb{F}_{2^m}$. We see that $f(\alpha^i) = f((uy)^i) = f(u^i)$. Now it is enough to show that u is a generator of U. Suppose $u^s = 1$ for some $s \in \mathbb{N}$, then we have $\alpha^{s(2^m-1)} = (uy)^{s(2^m-1)} = u^s = 1$ which means $s = 2^m + 1$ since α is a generator of $\mathbb{F}_{2^n}^*$. Hence we have

$$\left|\{ i \mid f(\alpha^i) = 1,\ 0 \le i \le 2^m\}\right| = \left|\{ i \mid f(u^i) = 1,\ 0 \le i \le 2^m\}\right|.$$

One can put any other generator instead of u, then result follows. $\square$

Proposition 3.6. *Let $f_b \in \Im_n$ and $U = \{x \in \mathbb{F}_{2^n}^* \mid x^{2^m+1} = 1\}$. Then f_b is hyper-bent if and only if $\Lambda(f_b) = 1$ where $\Lambda(f_b) := \sum_{u \in U} \chi(f_b(u))$.*

Proof. We will make use of Proposition 3.5. Let us show f_b satisfies the assumptions. It is obvious that $f_b(0) = 0$. We see that 3 divides $2^m + 1$ since we have m is odd and Lemma 2.1. Then all exponents of x in (3.3) are multiple of $2^m - 1$ which means $f_b(\alpha^{2^m+1}x) = f_b(x), \forall x \in \mathbb{F}_{2^n}$. Now by Propositon 3.5, f_b is hyper-bent if and only if the cardinality of the support of f_b restricted to U is $2^m - 1$. Now note that

$$\Lambda(f_b) = \sum_{u \in U} \chi(f_b(u)) = \sum_{t \in T}(1) - \sum_{s \in S}(-1) = |T| - |S| = (|U| - |S|) - |S|$$

$$\Lambda(f_b) = |U| - 2|S| = 2^m + 1 - 2|S|$$

where $T = \{u \in U \mid f_b(u) = 0\}$ and $S = \{u \in U \mid f_b(u) = 1\}$. By the arguement above we see that f_b is hyper-bent if and only if $\Lambda(f_b) = 1$. $\square$

3.1 The case where b=0

In this section we will study the characterization of the hyper-bent functions of $\Im_n$ in the case where $b = 0$ and m is any integer. This characterization was presented by Charpin and Gong in [5] in terms of Dickson polynomials. But before we study the characterization, we need the following definition and proposition.

Definition 3.7. A **Dickson polynomial** (of the first kind) is defined by

$$D_r(x) = \sum_{i=0}^{r/2} \frac{r}{r-i} \binom{r-i}{i} x^{r-2i}, \quad r = 2, 3, \ldots \tag{3.4}$$

Remark 3.8. Dickson polynomials $D_r \in \mathbb{F}_2[x]$ can also be recursively defined by

$$D_{i+2}(x) = xD_{i+1}(x) + D_i(x) \quad \text{where} \quad D_0(x) = 0 \text{ and } D_1(x) = x. \tag{3.5}$$

Proposition 3.9. [18] *The Dickson polynomials defined by (3.4) satisfy*

1. *$deg(D_i) = i$,*

2. *$D_{ij}(x) = D_i(D_j(x))$,*

3. *$D_i(x + x^{-1}) = x^i + x^{-i}$,*

for any positive integers i, j.

A comprehensive reference about Dickson polynomials is the book [18] by Lidl, Mullen and Turnwald.

Theorem 3.10. [5] *Let $n = 2m$ and E' be a set of representatives of the cyclotomic cosets modulo $2^m + 1$ that each class has the full size n. Let f and g be the functions defined, respectively, on $\mathbb{F}_{2^n}$ and $\mathbb{F}_{2^m}$ by*

$$f(x) = \sum_{r \in R} Tr_1^n(a_r x^{r(2^m-1)}) \quad \text{and} \quad g(x) = \sum_{r \in R} Tr_1^m(a_r D_r(x))$$

where $a_r \in \mathbb{F}_{2^m}$, $R \subseteq E'$. Then f is hyper-bent if and only if

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

Proof. Let ζ be a generator of the cyclic group $U = \{x \in \mathbb{F}_{2^n}^* \mid x^{2^m+1} = 1\}$. Recall Proposition 3.5, it is clear that f satisfies the assumptions that $f(0) = 0$ and $f(\alpha^{2^m+1}x) = f(x)$ for every $x \in \mathbb{F}_{2^n}$ and for some primitive element α of $\mathbb{F}_{2^n}$. Then f is hyper-bent if and only if

$$N = \left|\{ i \mid f(\zeta^i) = 1,\ 0 \le i \le 2^m\}\right| = 2^{m-1}.$$

By transitivity property of trace function we have

$$f(\zeta^i) = \sum_{r \in E'} Tr_1^n(a_r\zeta^{ir(2^m-1)}) = \sum_{r \in E'} Tr_1^m\left(Tr_m^n(a_r\zeta^{-2ir})\right)$$

$$= \sum_{r \in E'} Tr_1^m\left(a_r\zeta^{-2ir} + (a_r\zeta^{-2ir})^{2^m}\right)$$

Since $a_r^{2^m-1} = 1$ and $\zeta^{2^m+1} = 1$, we have

$$f(\zeta^i) = \sum_{r \in E'} Tr_1^m\left(a_r(\zeta^{-2ir} + \zeta^{2ir})\right).$$

That means f is hyper-bent if and only if

$$N = \left|\{ i \mid \sum_{r \in E'} Tr_1^m\left(a_r(\zeta^{-ir} + \zeta^{ir})\right) = 1,\ 0 \le i \le 2^m\}\right| = 2^{m-1}.$$

Above we replaced ζ^2 by ζ since the mapping $\zeta \mapsto \zeta^2$ is a permutation on U. Now note that if we use Proposition 3.9, we have

$$\zeta^{ir} + \zeta^{-ir} = D_{ir}(\zeta + \zeta^{-1}) = D_r(\zeta^i + \zeta^{-i})$$

also by Lemma 2.4, we can uniquely represent $u + u^{-1}$ for $\forall u \in U$ by $c \in \mathbb{F}_{2^m}$ such that $Tr_1^m(1/c) = 1$. Since ζ is a generator of U, we can say

$$\{ \zeta^i + \zeta^{-i} \mid 0 \le i \le 2^m\} = \{c \in \mathbb{F}_{2^m} \mid Tr_1^m(1/c) = 1\}$$

Now remember $g(x)$ and that there are two $\zeta^i + \zeta^{-i}$ when we go through all i's. Then we have

$$N = \left|\{ i \mid \sum_{r \in E'} Tr_1^m\left(a_r D_r(\zeta^i + \zeta^{-i})\right) = 1,\ 0 \le i \le 2^m\}\right|$$

$$N = 2\left|\{ c \in \mathbb{F}_{2^m} \mid g(c) = 1 \text{ and } Tr_1^m(1/c) = 1\}\right|.$$

Now let $wt(g)$ be the weight of g and denote the function $c \mapsto Tr_1^m(1/c)$ by h. The following is a clear fact that we have

$$\sum_{x \in \mathbb{F}_{2^m}} \chi(f(x)) = \left(|\mathbb{F}_{2^m}| - wt(f)\right) - wt(f) = 2^m - 2wt(f). \tag{3.6}$$

Then using that fact, we also have

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

Then

$$wt(h + g) = wt(h) + wt(g) - 2wt(hg) = 2^{m-1} + wt(g) - 2wt(hg)$$

Last equality holds because the inverse function is a permutation, $h(x) = Tr_1^m(1/x)$ and so half of the elements takes value 1 i.e. $wt(h) = 2^{m-1}$. Now see that $h(x)g(x) = 1$ if and only if $h(x) = g(x) = 1$ which gives us

$$wt(hg) = \left| \{ \ c \in \mathbb{F}_{2^m} \mid g(c) = 1 \ \text{and} \ Tr_1^m(1/c) = 1 \} \right| = N/2.$$

If we put everything together, we have

$$\sum_{x \in \mathbb{F}_{2^m}} \chi(h(x) + g(x)) = 2^m - 2wt(h + g) = 2^m - 2\left(2^{m-1} + wt(g) - N\right)$$

$$\sum_{x \in \mathbb{F}_{2^m}} \chi(h(x) + g(x)) = 2N - 2wt(g)$$

We said above that f is hyper-bent if and only if $N = 2^{m-1}$, therefore we have the result that f is hyper-bent if and only if

$$\sum_{x \in \mathbb{F}_{2^m}} \chi(h(x) + g(x)) = 2^m - 2wt(g)$$

$\square$

3.2 The case where $b \in \mathbb{F}_4^*$

From now on we will study the characterization of hyper-bentness of the set of the functions $\Im_n$ when $b \neq 0$. We will construct characterization of hyper-bentness of f_b separately for each element of $\mathbb{F}_4^*$

Let β be a primitive element of $\mathbb{F}_4$ and α be a primitive element of $\mathbb{F}_{2^n}$ such that $\beta = \alpha^{\frac{2^n-1}{3}}$. It is clear that α^{2^m-1} has order $2^m + 1$ which means $\zeta := \alpha^{2^m-1}$ is a generator of the cyclic group $U = \{x \in \mathbb{F}_{2^n}^* \mid x^{2^m+1} = 1\}$. Now recall equation (2.14) which gives us $U = V \cup \zeta V \cup \zeta^2 V$ where $V = \{u^3 \mid u \in U\}$. Then we define the sums

$$S_i := \sum_{v \in V} \chi(f_0(\zeta^i v)), \quad \forall i \in 0, 1, 2 \tag{3.7}$$

By using the decomposition of $U = V \cup \zeta V \cup \zeta^2 V$, we have

$$\sum_{i=0}^{2} S_i = \sum_{u \in U} \chi(f_0(u)). \tag{3.8}$$

Proposition 3.11. *Set $\Lambda(f_b) := \sum_{u \in U} \chi(f_b(u))$. We have the followings:*

1. $S_1 = S_2$,

2. $\Lambda(f_\beta) = \Lambda(f_{\beta^2}) = -S_0$,

3. $\Lambda(f_1) = S_0 - 2S_1$,

Proof. 1. Since $Tr_1^n(x) = Tr_1^n(x^2)$, we have $Tr_1^n(x) = Tr_1^n(x^{2^m})$ by applying m times. Then we have

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

$$f_0(x) = f_0(x^{2^m})$$

since $a_r \in \mathbb{F}_{2^m}, \ \forall r \in R$. If we use the equality $f_0(x) = f_0(x^{2^m})$, we have

$$S_1 = \sum_{v \in V} \chi(f_0(\zeta^{2^m} v^{2^m})) = \sum_{v \in V} \chi(f_0(\zeta^2(\zeta^{2^m-2} v^{2^m})))$$

By Lemma 2.1, 3 divides $2^m + 1$ i.e. 3 divides $2^m - 2$ that means ζ^{2^m-2} is a cube of U. So the mapping $v \mapsto \zeta^{2^m-2} v^{2^m}$ is a permutation of V. Hence we have

$$S_1 = \sum_{v \in V} \chi(f_0(\zeta^2(\zeta^{2^m-2} v^{2^m}))) = \sum_{v \in V} \chi(f_0(\zeta^2 v)) = S_2$$

Now we are going to prove (2) & (3) together.

For all $c \in \mathbb{F}_4$, define the sum

$$T(c) := \sum_{b \in \mathbb{F}_4} \Lambda(f_b) \chi(Tr_1^2(bc)).$$

Now we will show an equality that will help us.

$$\sum_{c \in \mathbb{F}_4} T(c) \chi(Tr_1^2(bc)) = \sum_{c \in \mathbb{F}_4} \sum_{d \in \mathbb{F}_4} \Lambda(f_d) \chi(Tr_1^2(dc)) \chi(Tr_1^2(bc))$$

$$= \sum_{d \in \mathbb{F}_4} \Lambda(f_d) \sum_{c \in \mathbb{F}_4} \chi(Tr_1^2(c(b+d)))$$

$$= \sum_{\substack{d \in \mathbb{F}_4 \\ d \neq b}} \Lambda(f_d) \sum_{c \in \mathbb{F}_4} \chi(Tr_1^2(c(b+d))) + \sum_{\substack{d \in \mathbb{F}_4 \\ d = b}} \Lambda(f_d) \sum_{c \in \mathbb{F}_4} \chi(Tr_1^2(0))$$

$$= 0 + \sum_{\substack{d \in \mathbb{F}_4 \\ d = b}} \Lambda(f_d) . 4 = 4\Lambda(f_b)$$

40

Hence we have the equality

$$\Lambda(f_b) = \frac{1}{4}\sum_{c\in\mathbb{F}_4}T(c)\chi(Tr_1^2(bc)) \tag{3.9}$$

Now we will show another equality,

$$
\begin{aligned}
T(c) &= \sum_{b\in\mathbb{F}_4}\Lambda(f_b)\chi(Tr_1^2(bc)) = \sum_{b\in\mathbb{F}_4}\sum_{u\in U}\chi(f_b(u))\chi(Tr_1^2(bc)) \\
&= \sum_{b\in\mathbb{F}_4}\sum_{u\in U}\chi\left(\sum_{r\in R}Tr_1^n(a_r u^{r(2^m-1)}) + Tr_1^2(bu^{\frac{2^n-1}{3}})\right)\chi(Tr_1^2(bc)) \\
&= \sum_{b\in\mathbb{F}_4}\sum_{u\in U}\chi\left(\sum_{r\in R}Tr_1^n(a_r u^{r(2^m-1)})\right)\chi\left(Tr_1^2(b(c+u^{\frac{2^n-1}{3}}))\right) \\
&= \sum_{b\in\mathbb{F}_4}\sum_{u\in U}\chi(f_0(u))\chi\left(Tr_1^2(b(c+u^{\frac{2^n-1}{3}}))\right) \\
&= \sum_{u\in U}\chi(f_0(u))\sum_{b\in\mathbb{F}_4}\chi\left(Tr_1^2(b(c+u^{\frac{2^n-1}{3}}))\right)
\end{aligned}
$$

Now note that

$$\sum_{b\in\mathbb{F}_4}\chi\left(Tr_1^2(b(c+u^{\frac{2^n-1}{3}}))\right) = 0 \text{ if } u^{\frac{2^n-1}{3}} \neq c \text{ and } 4 \text{ otherwise.} \tag{3.10}$$

Then $T(0) = 0$ since $u^{\frac{2^n-1}{3}} \neq 0 \ \ \forall u \in U$. Now we will check $T(c)$ when $c \neq 0$.
Since $\beta \in \mathbb{F}_4$ is primitive element, assume $c = \beta^i$, $i \in \{0,1,2\}$. At the beginning
of this section we defined that $\beta = \alpha^{\frac{2^n-1}{3}}$ and $\zeta = \alpha^{2^m-1}$ for some primitive
element α of $\mathbb{F}_{2^n}$. So $\beta^i = \zeta^{i\frac{2^m-1}{3}}$. Recall Equation 3.10, therefore it is enough to
calculate $T(c) = T(\beta^i)$ only for $u^{\frac{2^n-1}{3}} = \beta^i = \zeta^{i\frac{2^m-1}{3}}$. Then we have

$$T(\beta^i) = 4\sum_{\substack{u\in U \\ u^{\frac{2^n-1}{3}}=\zeta^{i\frac{2^m-1}{3}}}}\chi(f_0(u)).$$

Now note that

$$u^{\frac{2^n-1}{3}} = \zeta^{i\frac{2^m-1}{3}} \Leftrightarrow \left(u^{2^m-1}\zeta^{-i}\right)^{\frac{2^m+1}{3}} = 1 \Leftrightarrow \left(u^{-2}\zeta^{-i}\right) \in V \Leftrightarrow u^{-2} \in \zeta^i V$$

Because $u^{2^m+1} = 1$ and only V has elements whose orders are $\frac{2^m+1}{3}$, the last
equivalence holds. Next, we are going to show

$$u^{-2} \in \zeta^i V \Leftrightarrow u \in \zeta^i V$$

Now the fact we need is that the mapping $x \mapsto x^{2^{m-1}}$ is permutation on $\zeta^i V$.
It holds for two reasons. First one is that 2^{m-1} is coprime to $\frac{2^m+1}{3}$ which is

the order of $\zeta^i V$ and second one is that for any $\zeta^i v \in \zeta^i V$, $(\zeta^i v)^{2^{m-1}} = \zeta^i(\zeta^{i(2^{m-1}-1)}v^{2^{m-1}}) \in \zeta^i V$ since from Lemma 2.1, $2^{m-1} - 1 \equiv 0 \pmod 3$ for m odd. Hence we have the relation

$$u^{\frac{2^n-1}{3}} = \zeta^{i\frac{2^m-1}{3}} \Leftrightarrow u \in \zeta^i V$$

Now we can write

$$T(\beta^i) = 4 \sum_{\substack{u \in U \\ u^{\frac{2^n-1}{3}} = \zeta^{i\frac{2^m-1}{3}}}} \chi(f_0(u)) = 4 \sum_{v \in V} \chi(f_0(\zeta^i v)) = 4S_i.$$

If we put the results of $T(c)$, $c \in \mathbb{F}_4$, into Equality 3.9, we have

$$\Lambda(f_b) = \sum_{i=0}^{2} S_i \chi(Tr_1^2(b\beta^i))$$

In detail, we have

$$\Lambda(f_1) = S_0\chi(Tr_1^2(1)) + S_1\chi(Tr_1^2(\beta)) + S_2\chi(Tr_1^2(\beta^2)),$$

$$\Lambda(f_\beta) = S_0\chi(Tr_1^2(\beta)) + S_1\chi(Tr_1^2(\beta^2)) + S_2\chi(Tr_1^2(1)),$$

$$\Lambda(f_{\beta^2}) = S_0\chi(Tr_1^2(\beta^2)) + S_1\chi(Tr_1^2(1)) + S_2\chi(Tr_1^2(\beta)),$$

Now by the fact that $Tr_1^2(1) = 0$ and $Tr_1^2(\beta) = Tr_1^2(\beta^2) = 1$ and by part (1), we have the results.

$\square$

Now we can state the following Proposition.

Proposition 3.12. *Let* $n = 2m$*,* m *be an odd integer and* $b \in \mathbb{F}_4$*. Let* β *be a primitive element of* $\mathbb{F}_4$ *and set* $U = \{x \in \mathbb{F}_{2^n}^* \mid x^{2^m+1} = 1\}$ *and* $V = \{v \in U \mid v^3 = 1\}$*. Let* $f_b \in \Im_n$ *be a function as (3.3). 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 hyper-bent if and only if* $2\sum_{v \in V} \chi(f_0(v)) - \sum_{u \in U} \chi(f_0(u)) = 1$*.*

Proof. 1. By Proposition 3.6, f_β is hyper-bent if and only if $\Lambda(f_\beta) = 1$ and also we know $\Lambda(f_\beta) = -S_0$ by Proposition 3.11(1). Therefore f_β is hyper-bent if and only if $S_0 = -1$

2. It follows by Proposition 3.11(2).

3. By Equation 3.8 and Proposition 3.11(3), we have

$$2S_1 = \sum_{u \in U} \chi(f_0(u)) - S_0$$

$$\Lambda(f_1) = S_0 - 2S_1 = 2S_0 - \sum_{u \in U} \chi(f_0(u)) = 2\sum_{v \in V} \chi(f_0(v)) - \sum_{u \in U} \chi(f_0(u)).$$

$\square$

3.2.1 The case where b is a primitive element of $\mathbb{F}_4^*$

Now we will characterize hyper-bent function f_β in terms of Dickson polynomials when β is a primitive element of $\mathbb{F}_4^*$. Note that β^2 is the other primitive element of $\mathbb{F}_4^*$. For more information about Dickson polynomials, see Definition 3.7 and Proposition 3.9.

Lemma 3.13. *Let* $n = 2m$, $U = \{ x \in \mathbb{F}_{2^n} \mid x^{2^m+1} = 1\}$ *and* $D_r(x)$ *be the Dickson polynomial of degree* r. *Let* $f_0 \in \mathfrak{S}_n$ *defined on* $\mathbb{F}_{2^n}$ *and* g *be the related function defined on* $\mathbb{F}_{2^m}$ *as*

$$f_0 = \sum_{r \in R} Tr_1^n(a_r x^{r(2^m-1)}) \text{ and } g(x) = \sum_{r \in R} Tr_1^m(a_r D_r(x)).$$

Then for any positive integer p, *we have*

$$\sum_{u \in U} \chi(f_0(u^p)) = 1 + 2 \sum_{\substack{c \in \mathbb{F}_{2^m}^* \\ Tr_1^m(1/c)=1}} \chi(g(D_p(c))).$$

Proof. By the transitivity property of trace function we have $Tr_1^n(x) = Tr_1^m(Tr_m^n(x)) = Tr_1^m(x + x^{2^m})$. We know also $a_r^{2^m} = a_r$ since $a_r \in \mathbb{F}_{2^m}$. By these facts, we have

$$\sum_{u \in U} \chi(f_0(u^p)) = \sum_{u \in U} \chi\left(\sum_{r \in R} Tr_1^m(a_r(u^{rp(2^m-1)} + u^{rp(2^m-1)2^m}))\right)$$

Since $gcd(2^m+1, 2^m-1) = 1$, the mapping $x \mapsto x^{2^m-1}$ is a permutation of U. We know also $u^{2^m} = u^{-1}$ since $u \in U$. Now if we use these facts, we have

$$\sum_{u \in U} \chi(f_0(u^p)) = \sum_{u \in U} \chi\left(\sum_{r \in R} Tr_1^m(a_r(u^{rp} + u^{-rp}))\right)$$

Now recall Proposition 3.9 which is about Dickson polynomials, then we have

$$\sum_{u \in U} \chi(f_0(u^p)) = \sum_{u \in U} \chi\left(\sum_{r \in R} Tr_1^m(a_r D_{rp}(u + u^{-1}))\right)$$

$$= 1 + \sum_{u \in U \setminus \{1\}} \chi\left(\sum_{r \in R} Tr_1^m(a_r D_{rp}(u + u^{-1}))\right)$$

43

By Lemma 2.4, we can replace each $u + u^{-1}$ by $1/c \in \mathbb{F}_{2^m}$ such that $Tr_1^m(c) = 1$. Then we have

$$\sum_{u \in U} \chi\big(f_0(u^p)\big) = 1 + 2 \sum_{\substack{1/c \in \mathbb{F}_{2^m}^* \\ Tr_1^m(c) = 1}} \chi\bigg(\sum_{r \in R} Tr_1^m\big(a_r D_{rp}(1/c)\big)\bigg)$$

By the fact that the inverse function is a permutation on $\mathbb{F}_{2^m}^*$, we can replace $1/c$ by c. Also by Proposition 3.9, $D_{rp}(x) = D_r(D_p(x))$. Therefore we have

$$\sum_{u \in U} \chi\big(f_0(u^p)\big) = 1 + 2 \sum_{\substack{c \in \mathbb{F}_{2^m}^* \\ Tr_1^m(1/c) = 1}} \chi\bigg(\sum_{r \in R} Tr_1^m\big(a_r D_{rp}(c)\big)\bigg)$$

$$= 1 + 2 \sum_{\substack{c \in \mathbb{F}_{2^m}^* \\ Tr_1^m(1/c) = 1}} \chi\bigg(\sum_{r \in R} Tr_1^m\big(a_r D_r(D_p(c))\big)\bigg)$$

$$\sum_{u \in U} \chi\big(f_0(u^p)\big) = 1 + 2 \sum_{\substack{c \in \mathbb{F}_{2^m}^* \\ Tr_1^m(1/c) = 1}} \chi\big(g(D_p(c))\big)$$

$\square$

Now we can give the characterization of f_b when b is a primitive element of $\mathbb{F}_4$.

Theorem 3.14. *Let $n = 2m$, m be odd integer, β be a primitive element of $\mathbb{F}_4$ and $D_r(x)$ be the Dickson polynomial of degree r. Let $f_\beta \in \Im_n$ defined on $\mathbb{F}_{2^n}$ and g be the related function defined on $\mathbb{F}_{2^m}$ as*

$$f_\beta = \sum_{r \in R} Tr_1^n(a_r x^{r(2^m - 1)}) + Tr_1^2(\beta x^{\frac{2^n - 1}{3}}) \quad and \quad g(x) = \sum_{r \in R} Tr_1^m(a_r D_r(x)).$$

Then the followings are equivalent

1. *f_β is hyper-bent*

2. *$\sum_{\substack{x \in \mathbb{F}_{2^m}^* \\ Tr_1^m(1/x) = 1}} \chi\big(g(D_3(x))\big) = -2$*

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

Proof. First we will show that $(1) \Leftrightarrow (2)$

$$S_0 = \sum_{v \in V} \chi\big(f_0(v)\big) = \frac{1}{3} \sum_{u \in U} \chi\big(f_0(u^3)\big) = \frac{1}{3}\bigg(1 + 2 \sum_{\substack{x \in \mathbb{F}_{2^m}^* \\ Tr_1^m(1/x) = 1}} \chi\big(g(D_3(x))\big)\bigg)$$

44

The last equality holds by Lemma 3.13. Now recall Proposition 3.12, we know f_β is hyper-bent if and only if $\sum_{v\in V}\chi(f_0(v))=-1$ i.e. f_β is hyper-bent if and only if

$$-1 = \frac{1}{3}\left(1+2\sum_{\substack{x\in\mathbb{F}_{2^m}^* \\ Tr_1^m(1/x)=1}}\chi\big(g(D_3(x))\big)\right)$$

$$-2 = \sum_{\substack{x\in\mathbb{F}_{2^m}^* \\ Tr_1^m(1/x)=1}}\chi\big(g(D_3(x))\big)$$

Now it is enough to show that $(2)\Leftrightarrow(3)$

$$\sum_{\substack{x\in\mathbb{F}_{2^m}^* \\ Tr_1^m(1/x)=1}}\chi\Big(g(D_3(x))\Big) = \frac{1}{2}\left(\sum_{x\in\mathbb{F}_{2^m}}\chi\big(g(D_3(x))\big)-\sum_{x\in\mathbb{F}_{2^m}}\chi\big(Tr_1^m(x^{-1})+g(D_3(x))\big)\right)$$

This equality holds because when $Tr(x^{-1})=0$ for any $x\in\mathbb{F}_{2^m}^*$, the right hand side becomes zero for that particular x, but when $Tr(x^{-1})=1$, the right hand side becomes $\chi\big(g(D_3(x))\big)$ for that particular x. Now we have the equality

$$-2 = \frac{1}{2}\left(\sum_{x\in\mathbb{F}_{2^m}}\chi\big(g(D_3(x))\big)-\sum_{x\in\mathbb{F}_{2^m}}\chi\big(Tr_1^m(x^{-1})+g(D_3(x))\big)\right)$$

$$\sum_{x\in\mathbb{F}_{2^m}}\chi\big(g(D_3(x))\big)+4 = \sum_{x\in\mathbb{F}_{2^m}}\chi\big(Tr_1^m(x^{-1})+g(D_3(x))\big)$$

Using Equality (3.6), we have the result

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

$\square$

Corollary 3.15. *Let $n=2m$ and m be odd integer. Let β be a primitive element of $\mathbb{F}_4$ and d be a positive integer. Assume that $gcd(d,\frac{2^m+1}{3})=1$. Let $f_\beta\in\Im_n$ and h_β be the functions defined on $\mathbb{F}_{2^n}$ as*

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

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

Then f_β is hyper-bent if and only if h_β is hyper-bent.

Proof. By Proposition 3.12, we know that h_β is hyper-bent if and only if

$$\sum_{v \in V} \chi(h_0(v)) = -1.$$

By hypothesis, we know that the mapping $v \mapsto v^d$ is a permutation on V. Then we have

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

Due to this equality, we have that h_β is hyper-bent if and only if f_β is hyper-bent. $\quad\square$

3.2.2 The case where $b = 1$

Now we will characterize hyper-bent functions f_b when $b = 1$ which is the last remaining case. In this characterization, Dickson polynomials and similar related function are used as in the previous case.

Theorem 3.16. *Let $n = 2m$, m be odd integer and $D_r(x)$ be the Dickson polynomial of degree r. Let $f_1 \in \Im_n$ defined on $\mathbb{F}_{2^n}$ and g be the related function defined on $\mathbb{F}_{2^m}$ as*

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

Then f_1 is hyper-bent if and only if

$$2 \sum_{\substack{x \in \mathbb{F}_{2^m}^* \\ Tr_1^m(1/x)=1}} \chi\big(g(D_3(x))\big) - 3 \sum_{\substack{x \in \mathbb{F}_{2^m}^* \\ Tr_1^m(1/x)=1}} \chi\big(g(x)\big) = 2.$$

Proof. It is clear that $\sum_{v \in V} \chi(f_0(v)) = \frac{1}{3} \sum_{u \in U} \chi(f_0(u^3))$. Then we have

$$2 \sum_{v \in V} \chi(f_0(v)) - \sum_{u \in U} \chi(f_0(u)) = \frac{2}{3} \sum_{u \in U} \chi(f_0(u^3)) - \sum_{u \in U} \chi(f_0(u))$$

Now if we use Lemma 3.13, we have

$$\frac{2}{3} \sum_{u \in U} \chi(f_0(u^3)) - \sum_{u \in U} \chi(f_0(u))$$

$$= \frac{2}{3}\left(1 + 2 \sum_{\substack{x \in \mathbb{F}_{2^m}^* \\ Tr_1^m(1/x)=1}} \chi(g(D_3(x)))\right) - \left(1 + 2 \sum_{\substack{x \in \mathbb{F}_{2^m}^* \\ Tr_1^m(1/x)=1}} \chi(g(x))\right)$$

$$= -\frac{1}{3} + \frac{4}{3} \sum_{\substack{x \in \mathbb{F}_{2^m}^* \\ Tr_1^m(1/x)=1}} \chi(g(D_3(x))) - 2 \sum_{\substack{x \in \mathbb{F}_{2^m}^* \\ Tr_1^m(1/x)=1}} \chi(g(x))$$

Now recall Proposition 3.12, it says that f_1 is hyper-bent if and only if

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

Therefore, we have that f_1 is hyper-bent if and only if

$$1 = -\frac{1}{3} + \frac{4}{3}\sum_{\substack{x\in\mathbb{F}_{2^m}^* \\ Tr_1^m(1/x)=1}}\chi(g(D_3(x))) - 2\sum_{\substack{x\in\mathbb{F}_{2^m}^* \\ Tr_1^m(1/x)=1}}\chi(g(x))$$

$\square$

Corollary 3.17. *Let $n = 2m$ and m be odd integer. Let β be a primitive element of $\mathbb{F}_4$ and d be a positive integer. Assume that $gcd(d, 2^m + 1) = 3$ and $m \not\equiv 3 \pmod 6$. Let $f_\beta \in \Im_n$ and h_1 be the functions defined on $\mathbb{F}_{2^n}$ as*

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

$$h_1(x) = \sum_{r\in R} Tr_1^n(a_r x^{dr(2^m-1)}) + Tr_1^2(x^{\frac{2^n-1}{3}}).$$

Then f_β is hyper-bent if and only if h_1 is hyper-bent.

Proof. Set $h_0(x) := \sum_{r\in R} Tr_1^n(a_r x^{dr(2^m-1)})$. Since $gcd(d, 2^m + 1) = 3$, we have $gcd(d/3, \frac{2^m+1}{3}) = 1$. Then the mapping $v^{d/3} \mapsto v$ is a permutation on V i.e. the mapping $v^d \mapsto v^3$ is a permutation on V. Then we have

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

Since $m \not\equiv 3 \pmod 6$, we have $gcd(3, \frac{2^m+1}{3}) = 1$ by Lemma 2.1. Then we have

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

Now we will show that $\{u^d \mid u^{2^m+1} = 1\} = \{u^3 \mid u^{2^m+1} = 1\}$. Assume that the order of u^d is s in $\mathbb{F}_{2^n}$ i.e. s is the least positive integer satisfying $u^{ds} = 1$. That means $lcm(d, 2^m+1) = ds$. Since $gcd(d, 2^m+1) = 3$, we have $lcm(d, 2^m+1) = (d(2^m+1))/3$ i.e. $ds = (d(2^m+1))/3$. Hence we have $s = (2^m+1)/3$ which is the order of the elements in V. Therefore we have

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

47

Now we will use these two equalities together,

$$2\sum_{v\in V}\chi(h_0(v)) - \sum_{u\in U}\chi(h_0(u)) = 2\sum_{v\in V}\chi(f_0(v)) - 3\sum_{v\in V}\chi(f_0(v))$$

$$2\sum_{v\in V}\chi(h_0(v)) - \sum_{u\in U}\chi(h_0(u)) = -\sum_{v\in V}\chi(f_0(v))$$

By Proposition 3.12, we know that h_1 is hyper-bent if and only if left hand side is equal to 1 i.e. $\sum_{v\in V}\chi(f_0(v)) = -1$ i.e. f_β is hyper-bent by Proposition 3.12. $\qquad\square$

Bibliography

[1] Carlisle M. Adams. Constructing symmetric ciphers using the cast design procedure. *Des. Codes Cryptography*, 12:283–316, November 1997.

[2] Elwyn R. Berlekamp, H. Rumsey, and G. Solomon. On the solution of algebraic equations over finite fields. *Information and Control*, 10(6):553–564, 1967.

[3] Eli Biham and Adi Shamir. Differential cryptanalysis of des-like cryptosystems. In Menezes and Vanstone [20], pages 2–21.

[4] L. Carlitz. *Explicit evaluation of certain exponential sums.* Math. Scand. 44, 5-16, 1979.

[5] Pascale Charpin and Guang Gong. Hyperbent functions, kloosterman sums, and dickson polynomials. *IEEE Transactions on Information Theory*, 54(9):4230–4238, 2008.

[6] Pascale Charpin, Tor Helleseth, and Victor Zinoviev. Divisibility properties of classical binary kloosterman sums. *Discrete Mathematics*, 309(12):3975–3984, 2009.

[7] J. F. Dillon. *Elementary Hadamard difference sets.* Ph.D. dissertation, University of Maryland, 1974.

[8] J. F. Dillon. *Elementary Hadamard difference sets.* In: Proceedings of the Sixth S-E Conf. Comb. Graph Theory and Comp., Winnipeg Utilitas Math, pp. 237-249, 1975.

[9] J. F. Dillon and Hans Dobbertin. New cyclic difference sets with singer parameters. *Finite Fields and Their Applications*, 10(3):342–389, 2004.

[10] C. Ding, G. Xiao, and W. Shan. *The stability theory of stream ciphers / C. Ding, G. Xiao, W. Shan.* Springer-Verlag, Berlin ; New York :, 1991.

[11] Hans Dobbertin, Gregor Leander, Anne Canteaut, Claude Carlet, Patrick Felke, and Philippe Gaborit. Construction of bent functions via niho power functions. *J. Comb. Theory, Ser. A*, 113(5):779–798, 2006.

[12] Guang Gong and Solomon W. Golomb. Transform domain analysis of des. *IEEE Transactions on Information Theory*, 45(6):2065–2073, 1999.

[13] Tor Helleseth, editor. *Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings*, volume 765 of *Lecture Notes in Computer Science*. Springer, 1994.

[14] Honggang Hu and Dengguo Feng. On quadratic bent functions in polynomial forms. *IEEE Transactions on Information Theory*, 53(7):2610–2615, 2007.

[15] Gilles Lachaud and Jacques Wolfmann. The weights of the orthogonals of the extended quadratic binary goppa codes. *IEEE Transactions on Information Theory*, 36(3):686–692, 1990.

[16] N.G. Leander. *Normality of bent functions monomial and binomial bent functions.* 2004.

[17] N.G. Leander. Monomial bent functions. *IEEE Transactions on Information Theory*, 52(2):738–743, 2006.

[18] Rudolf Lidl, Gary L Mullen, and G Turnwald. *Dickson polynomials / R. Lidl, G.L. Mullen, G. Turnwald.* Harlow, Essex, England : Longman Scientific & Technical; New York : Copublished in the United States with John Wiley & Sons, 1993. Includes bibliographical references (p. 186-199) and indexes.

[19] Mitsuru Matsui. Linear cryptoanalysis method for des cipher. In Helleseth [13], pages 386–397.

[20] Alfred Menezes and Scott A. Vanstone, editors. *Advances in Cryptology - CRYPTO '90, 10th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1990, Proceedings*, volume 537 of *Lecture Notes in Computer Science*. Springer, 1991.

[21] Sihem Mesnager. A new family of hyper-bent boolean functions in polynomial form. In Parker [26], pages 402–417.

[22] Sihem Mesnager. Hyper-bent boolean functions with multiple trace terms. In *Proceedings of the Third international conference on Arithmetic of finite fields*, WAIFI'10, pages 97–113, Berlin, Heidelberg, 2010. Springer-Verlag.

[23] Sihem Mesnager. A new class of bent and hyper-bent boolean functions in polynomial forms. *Des. Codes Cryptography*, 59:265–279, April 2011.

[24] Sihem Mesnager. Semibent functions from dillon and niho exponents, kloosterman sums, and dickson polynomials. *IEEE Transactions on Information Theory*, 57(11):7443–7458, 2011.

[25] William Millan, Joanne Fuller, and Ed Dawson. New concepts in evolutionary search for boolean functions in cryptology. *Computational Intelligence*, 20(3):463–474, 2004.

[26] Matthew G. Parker, editor. *Cryptography and Coding, 12th IMA International Conference, Cryptography and Coding 2009, Cirencester, UK, December 15-17, 2009. Proceedings*, volume 5921 of *Lecture Notes in Computer Science*. Springer, 2009.

[27] O. S. Rothaus. On "bent" functions. *J. Comb. Theory, Ser. A*, 20(3):300–305, 1976.

[28] Amr M. Youssef and Guang Gong. Hyper-bent functions. In *Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques: Advances in Cryptology*, EUROCRYPT '01, pages 406–419, London, UK, 2001. Springer-Verlag.

[29] Yuliang Zheng, Josef Pieprzyk, and Jennifer Seberry. Haval - a one-way hashing algorithm with variable length of output. In *Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques: Advances in Cryptology*, ASIACRYPT '92, pages 83–104, London, UK, 1993. Springer-Verlag.