On Kasami Bent Functions

Deepmala Sharma and Sugata Gangopadhyay
Department of Mathematics
Indian Institute of Technology Roorkee 247 667 INDIA
E-mail: gsugata@gmail.com

Abstract

It is proved that no non-quadratic Kasami bent is affine equivalent to Maiorana-MacFarland type bent functions.

1 Introduction

The class of Kasami bent functions was characterized by Dillon and Dobbertin [7]. While searching for non-normal bent functions Canteaut, Daum, Dobbertin and Leander [2] pointed out that functions from this class are good candidates to be non-weakly normal bent functions. They found that there exists non-weakly normal bent functions on 14 variables within the class of Kasami bent functions. Dobbertin and Leander [9] provides a survey of recent developments on bent functions including these results. The existence of non-weakly normal bent functions imply that at least some of the Kasami type functions are not affine equivalent to Maiorana-MacFarland ($\mathcal{M}$) type bents, Partial-Spreads (PS) type bents nor to $\mathcal{N}$ type bents constructed in [8]. However we have not found any general proof dealing with this question. In this paper we prove that no non-quadratic Kasami bent function is affine equivalent to Maiorana-MacFarland type bent functions. Our proof depends on the techniques developed by Canteaut and Charpin in [1].

2 Preliminaries

Let $\mathbb{F}_2$ be the prime field of characteristic 2 and $\mathbb{F}_{2^n}$ be the extension field of degree n over $\mathbb{F}_2$. The finite field $\mathbb{F}_{2^n}$ can be considered as an n dimensional vector space over $\mathbb{F}_2$. The set containing all invertible elements of $\mathbb{F}_{2^n}$ is denoted by $\mathbb{F}_{2^n}^*$. Any function from $\mathbb{F}_{2^n}$ into $\mathbb{F}_2$ is called a Boolean function on n variables. The set of all Boolean functions on n variables is denoted by $\mathcal{B}_n$. For any set S the cardinality of S is denoted by $|S|$. For any two functions $f, g \in \mathcal{B}_n$, $|\{x : f(x) \neq g(x), x \in \mathbb{F}_{2^n}\}|$ is said to be the Hamming distance between f and g and denoted by $d(f, g)$. The trace function from $\mathbb{F}_{2^n}$ into $\mathbb{F}_2$ is defined by

$$Tr_1^n(x) = x + x^2 + x^{2^2} + \ldots + x^{2^{n-1}}$$

for all $x \in \mathbb{F}_{2^n}$. Given any $x, y \in \mathbb{F}_{2^n}$, $Tr_1^n(xy)$ is an inner product of x and y. If n is fixed then instead of Tr_1^n we often write Tr. Any affine function on n variables can be written as $Tr_1^n(\lambda x) + \epsilon$ for some $\lambda \in \mathbb{F}_{2^n}$ and $\epsilon \in \mathbb{F}_2$. The function is said to be a linear function if and only if $\epsilon = 0$.

Suppose $GL(n, \mathbb{F}_2)$ is the group of all invertible linear transformations on $\mathbb{F}_{2^n}$. Two Boolean functions f, $g \in \mathcal{B}_n$ are said to be affine equivalent if there exists a matrix $A \in GL(n, \mathbb{F}_2)$, $b, \lambda \in \mathbb{F}_2^n$ and $\epsilon \in \mathbb{F}_2$ such that $g(x) = f(Ax + b) + Tr_1^n(\lambda x) + \epsilon$.

Definition 1 *The Walsh transform $f \in \mathcal{B}_n$ at $\lambda \in \mathbb{F}_{2^n}$ is defined as follows:*

$$W_f(\lambda) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x) + Tr_1^n(\lambda x)}.$$

Next we define the nonlinearity of a Boolean function.

Definition 2 *Nonlinearity of $f \in \mathcal{B}_n$ is defined as $nl(f) = \min_{l \in \mathcal{A}_n} \{d(f, l)\}$, where $\mathcal{A}_n$ is the set of all affine functions on n variables.*

The connection between Walsh spectrum and nonlinearity is given below

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{\lambda \in \mathbb{F}_{2^n}} |W_f(\lambda)|.$$

Using Parseval's identity

$$\sum_{\lambda \in \mathbb{F}_{2^n}} W_f(\lambda)^2 = 2^{2n}$$

it can be shown that $|W_f(\lambda)| \geq 2^{n/2}$ as a consequence $nl(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$.

Definition 3 *A Boolean function $f \in \mathcal{B}_n$, where n is even is said to be bent if and only if $|W_f(\lambda)| = 2^{n/2}$ for all $\lambda \in \mathbb{F}_{2^n}$.*

For results on bent functions we refer to [1, 2, 3, 5, 6, 10, 11, 14]. For each even positive integer n bent functions in $\mathcal{B}_n$ are the functions having the highest nonlinearity.

Dobbertin [8] introduced the notion of normality. We shall refer to t dimensional affine subspace as t dimensional flat.

Definition 4 *A bent function on $n = 2m$ variables is said to be normal if there exists an m dimensional flat over which it is constant.*

Definition 5 *A bent function on $n = 2m$ variables is said to be weakly normal if there exist an m dimensional flat over which it is affine.*

The class of Kasami bent functions discovered by Dillon and Dobbertin [7] is important since there exists bent functions within this class which are not weakly normal.

Definition 6 *Suppose $f(x) = Tr_1^n(\lambda x^k)$ for all $x \in \mathbb{F}_{2^n}$ such that*

1. *n is not divisible by* 3.

2. $k = 2^{2d} - 2^d + 1$ *with* $\gcd(n, d) = 1$, $0 < d < n$.

3. $\lambda \in \mathbb{F}_{2^n}^*$ *does not belong to* $\{x^3 : x \in \mathbb{F}_{2^n}\}$.

Then f is a bent function. Any bent function which can be written in this form is said to be a Kasami bent function. If only condition (2) above holds then f is called Kasami Boolean function.

A bent function f on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, where $m = n/2$, is said to be a Maiorana-MacFarland type bent function if and only if f can be written as $f(x, y) = Tr_1^m(x\phi(y)) + g(y)$, where ϕ is a permutation from $\mathbb{F}_{2^m}$ into $\mathbb{F}_{2^m}$ and g an arbitrary Boolean function on $\mathbb{F}_{2^m}$. We denote the class of all bent functions which are equivalent to Maiorana-MacFarland type bent functions under affine transformations by $\mathcal{M}^{\#}$, this class is also referred to as the complete class of Maiorana-MacFarland type bent functions. The following proposition stated in [2] clearly characterizes the class $\mathcal{M}^{\#}$.

Proposition 1 *A Boolean function f on $\mathbb{F}_2^n$ is affine equivalent to a Maiorana-MacFarland function if and only if there exists a subspace U of dimension m such that the function f is affine on every coset of U.*

We denote the set $\{0, 1, 2, \ldots, n-1\}$ by $\mathbb{Z}/(n)$. Any positive integer z can be written as $z = \sum_{i=0}^{l} z_i 2^i$, for some finite non-negative integer l. We shall refer to this as the binary expansion of z. The Hamming weight of the binary expansion of z is denoted by $wt(z) = \sum_{i=0}^{l} z_i$, where the sum is over integers. We define a partial order " $\preceq$ " on the set of positive integers as follows:

For any two integers z and z', $z \preceq z'$ if and only if $z_i \leq z'_i$, for all i. If $z_i < z'_i$, for all i then we write $z \prec z'$.

For any integer x we define an integer $[x]_N \in \{1, 2, 3, \ldots, N-1\}$ such that,

$$[x]_N \equiv x \bmod N.$$

In this paper, if nothing is mentioned $[x]$ implies $[x]_{2^n-1}$. For an integer k we denote the cyclotomic coset of k modulo $(2^n - 1)$ as $C(k)$ which is defined as

$$C(k) = \{k' \mid k' = [2^j k], 0 \leq j < n\}.$$

The derivative of a function $f \in \mathcal{B}_n$ with respect to $a \in \mathbb{F}_{2^n}$ is defined as $D_a f(x) = f(x + a) + f(x)$, for all $x \in \mathbb{F}_{2^n}$. The second derivative at $a, b \in \mathbb{F}_{2^n}$ is $D_a D_b f(x) = f(x + a + b) + f(x + b) + f(x + a) + f(x)$ for all $x \in \mathbb{F}_{2^n}$.

3 Main result

In this section we prove that non-quadratic Kasami bent functions are not affine equivalent to Maiorana-MacFarland type bent functions. First we prove few lemmas and theorems which lead to the main result.

Lemma 1 *For an integer d define the integer k_d such that $k_d = [2^{2d} - 2^d + 1]$. For any even positive integer n if $0 < d < \frac{n}{2}$ then $k_{n-d} = 2^r k_d$, for some integer r.*

Proof : It is given that $k_d = [2^{2d} - 2^d + 1]$. Since $2^{2d-1} + 2^{2d-2} + 2^{2d-3} + \ldots + 2^d$ is equal to $2^{2d} - 2^d$, the k_d can also be written as

$$k_d = [2^{2d-1} + 2^{2d-2} + 2^{2d-3} + \ldots + 2^d + 2^0].$$

Let us consider $0 < d < \frac{n}{2}$, i.e., $2d - 1 < n - 1$. This implies

$$k_d = 2^{2d-1} + 2^{2d-2} + 2^{2d-3} + \ldots + 2^d + 2^0.$$

Then

$$k_{n-d} = [2^{2(n-d)-1} + 2^{2(n-d)-2} + 2^{2(n-d)-3} + \ldots + 2^{n-d} + 2^0].$$

Since

$$\begin{aligned} 2^{2(n-d)-1} + 2^{2(n-d)-2} + \ldots + 2^{n-d} + 2^0 &= (2^n - 1)(2^{n-2d-1} + 2^{n-2d-2} + \ldots + 2^0) \\ &+ (2^{n-1} + 2^{n-2} + \ldots + 2^{n-d} + 2^{n-2d}), \end{aligned}$$

k_{n-d} is given by

$$\begin{aligned} k_{n-d} &= 2^{n-1} + 2^{n-2} + \ldots + 2^{n-d} + 2^{n-2d} \\ &= 2^{n-2d}(2^{2d-1} + 2^{2d-2} + \ldots + 2^d + 2^0) \\ &= 2^{n-2d} k_d. \end{aligned}$$

Hence Proved. ■

Lemma 2 *Consider $t, t' \in \mathbb{Z}/(2^n)$ such that*

$$t = 2^{2d-1} + 2^{2d-2} + 2^{2d-3} + \ldots + 2^d + 2^0,$$

$$t' = 2^{2d-3} + 2^{2d-4} + 2^{2d-5} + \ldots + 2^d + 2^0,$$

where n is even and d is such that $3 < d < \frac{n}{2}$. Let us define

$$S = \{x \in \mathbb{Z}/(2^n) \mid x \prec t\},$$

$$S' = \{y \in \mathbb{Z}/(2^n) \mid y = [2^j t'], 0 < j < n\},$$

then $S \cap S' = \phi$.

Proof : We consider the following three cases:

Case I: $0 < j < d$. We have:

$$[2^j t'] = [2^{2d-3+j} + 2^{2d-4+j} + 2^{2d-5+j} + \ldots + 2^{d+j} + 2^j].$$

If $(2d-3+j) \leq n-1$, then

$$[2^j t'] = 2^{2d-3+j} + 2^{2d-4+j} + 2^{2d-5+j} + \ldots + 2^{d+j} + 2^j.$$

If $(2d-3+j) > n-1$, then

$$\begin{aligned} 2^{2d-3+j} + 2^{2d-4+j} + \ldots + 2^{d+j} + 2^j &= (2^n-1)(2^{2d-n-3+j} + 2^{2d-n-4+j} + \ldots + 2^0) \\ &+ 2^{n-1} + 2^{n-2} + \ldots + 2^{d+j} + 2^j \\ &+ 2^{2d-n-3+j} + 2^{2d-n-4+j} + \ldots + 2^0. \end{aligned}$$

Therefore

$$[2^j t'] = 2^{n-1} + 2^{n-2} + 2^{n-3} + \ldots + 2^{d+j} + 2^j + 2^{2d-n-3+j} + 2^{2d-n-4+j} + \ldots + 2^0.$$

Since $2d-n-3 < 0$, we obtain $(2d-n-3+j) < j$.

Thus in the binary expansion of $[2^j t']$ there exists at least one term 2^i with $0 < i < d$ having non-zero coefficient. This implies $[2^j t'] \not\prec t$. Therefore for $0 < j < d$ there exists no $y \in S'$ which belongs to the set S.

Case II: $d \leq j \leq n-d-1$. We have

$$[2^j t'] = [2^{2d-3+j} + 2^{2d-4+j} + 2^{2d-5+j} + \ldots + 2^{d+j} + 2^j].$$

Since $d \leq j \leq n-d-1$, we obtain $2d \leq d+j \leq n-1$. Thus in the above expression the term 2^{d+j} corresponds to the exponent which is in the range [2d,n-1]. In this case the elements of S' are greater than t therefore none of them belong to the set S.

Case III: $n-d \leq j < n$. Let us first consider $j = n-d$. We have

$$\begin{aligned} 2^{n+d-3} + 2^{n+d-4} + 2^{n+d-5} + \ldots + 2^n + 2^{n-d} &= (2^n-1)(2^{d-3} + 2^{d-4} + \ldots + 2^0) \\ &+ 2^{n-d} + 2^{d-3} + 2^{d-4} + \ldots + 2^0. \end{aligned}$$

Therefore

$$\begin{aligned} [2^{n-d} t'] &= [2^{n+d-3} + 2^{n+d-4} + 2^{n+d-5} + \ldots + 2^n + 2^{n-d}] \\ &= 2^{n-d} + 2^{d-3} + 2^{d-4} + \ldots + 2^0. \end{aligned}$$

Since $3 < d$, we get $0 < d-3 < d$ which implies $[2^{n-d} t'] \not\prec t$. If $n-d < j < n$, suppose that $j = n-d+j'$, where $0 < j' < d$, then

$$\begin{aligned} [2^j t'] &= [(2^{n-d} t') 2^{j'}] \\ &= [2^{n-d+j'} + 2^{d-3+j'} + 2^{d-4+j'} + \ldots + 2^{j'}], \end{aligned}$$

Proceeding in the same manner as case 1, it can be inferred that that the binary expansion of $[2^j t']$ contains at least one term 2^i for $0 < i < d$. Thus $[2^j t']$ can not belong to the set S. ■

Lemma 3 *Consider the element $t' \in \mathbb{Z}/(2^n)$ such that*

$$t' = 2^{2d-3} + 2^{2d-4} + 2^{2d-5} + \ldots + 2^d + 2^0,$$

where n is even and d is such that $3 < d < \frac{n}{2}$. Then the cyclotomic coset containing t' has cardinality n.

Proof : Suppose if possible $|C(t')| < n$, then there exists at least one $0 < j < n$ such that $[2^j t'] = t'$ i.e. $t' \in S'$. Moreover $t' \prec t$, in that case $S \cap S' \neq \phi$ which is a contradiction by Lemma 2. Therefore cardinality of $C(t')$ is exactly n. ■

The above three lemmas are used to prove the following:

Theorem 1 *Let us consider the function in $\mathcal{B}_n$ of the form*

$$f(x) = Tr(\lambda x^k),$$

where n is even and $\lambda \in \mathbb{F}_{2^n}^*$. For $k = 2^{2d} - 2^d + 1$, where $3 < d < \frac{n}{2}$, the function f is such that there exists no non zero elements a, b, $a \neq b$ in $\mathbb{F}_{2^n}$ such that $D_a D_b f$ is constant and equal to zero.

Proof : Let $a \neq 0$ and $b \neq 0$ in $\mathbb{F}_{2^n}$ be such that $a \neq b$. Then

$$\begin{aligned} D_a D_b f(x) &= Tr[\lambda(x^k + (x+a)^k + (x+b)^k + (x+a+b)^k)] \\ &= \sum_{i \prec k} Tr[\lambda(a^{k-i} + b^{k-i} + (a+b)^{k-i})x^i]. \end{aligned}$$

When $i = k - 2^r$, for some r, we have

$$a^{k-i} + b^{k-i} + (a+b)^{k-i} = 0.$$

Then

$$D_a D_b f(x) = \sum_{i \in I} Tr[\lambda(a^{k-i} + b^{k-i} + (a+b)^{k-i})x^i],$$

where $I = \{i \mid i \prec k, wt(k-i) \neq 1\}$. Let us denote

$$Q(x) = \sum_{i \in I} Tr[\lambda(a^{k-i} + b^{k-i} + (a+b)^{k-i})x^i].$$

Since Trace is a linear function, $Q(x)$ can be expressed as

$$Q(x) = Tr(\sum_{i \in I} q_i x^i), \tag{1}$$

where $q_i = \lambda(a^{k-i} + b^{k-i} + (a+b)^{k-i})$. Let us take the partition of I such that each block contain the elements of same cyclotomic coset. Then the expression of $Q(x)$ can be written as

$$Q(x) = Tr(\sum_{j \in J} \sum_{i \in C'(j)} q_i x^i), \tag{2}$$

where J is the subset of I consists of the smallest elements of the cyclotomic cosets modulo 2^n-1 of all i which appear as exponent of x in the function $Q(x)$ in (1) and $C'(j) = I \cap C(j)$, $C(j)$ is the cyclotomic coset of j modulo (2^n-1) . Since $Tr(x) = Tr(x^{2^r})$ for any r, we can expressed the polynomial $Q(x)$ as:

$$Q(x) = Tr(\sum_{j\in J} q'_j x^j) = \sum_{j\in J} Tr(q'_j x^j), \tag{3}$$

where q'_j only depends on λ, a, b and $C'(j)$. Since j varies over the set containing the smallest elements of cyclotomic cosets, $Q(x) = 0$ for all x, if and only if $Tr(q'_j x^j) = 0$ for all $j \in J$. It is to be noted that for any non zero $j \in J$ such that the size of $C(j)$ is equal to n, the function $Tr(q'_j x^j)$ cannot be constant when $q'_j \neq 0$. In order to prove required result we have to show that there exists at least one q'_j for $j > 0$ and $|C(j)| = n$, which can not be equal to zero. It is given that $k = 2^{2d} - 2^d + 1$, which can also be written as,

$$k = 2^{2d-1} + 2^{2d-2} + 2^{2d-3} + \ldots + 2^d + 2^0.$$

If we choose $l = 2^{2d-3} + 2^{2d-4} + 2^{2d-5} + \ldots + 2^d + 2^0$, we have clearly $wt(l) = wt(k) - 2$ $(wt(k) > 3)$ and $l \prec k$ i.e. $l \in J$. Moreover from Lemma 2 and Lemma 3 it is obvious that $C'(l)$ contains only single element l and the cardinality of $C(l)$ is n, this implies

$$\begin{aligned} q'_l &= \lambda(a^{k-l} + b^{k-l} + (a+b)^{k-l}) \\ &= \lambda(a^{2^{2d-1}+2^{2d-2}} + b^{2^{2d-1}+2^{2d-2}} + (a+b)^{2^{2d-1}+2^{2d-2}}) \\ &= \lambda(a^{2^{2d-1}} b^{2^{2d-2}} + a^{2^{2d-2}} b^{2^{2d-1}}) \\ &= \lambda a^{2^{2d-2}} b^{2^{2d-2}} (a^{2^{2d-2}} + b^{2^{2d-2}}) \\ &= \lambda a^{2^{2d-2}} b^{2^{2d-2}} (a+b)^{2^{2d-2}}. \end{aligned}$$

For non zero value of λ, a and b, the right hand side of the above expression is zero if and only if $a = b$. By hypothesis $a \neq b$, we conclude that q'_l can not be zero. Hence proved. ■

For $d = 3$, $k = 2^{2d} - 2^d + 1 = 57$, then we get the following result.

Theorem 2 *Let us consider the function in $\mathcal{B}_n$ of the form*

$$f(x) = Tr(\lambda x^k),$$

where $\lambda \in \mathbb{F}^*_{2^n}$. For $n \geq 10$, n even and $k = 57$ there exists no non zero elements a, b, $a \neq b$ in $\mathbb{F}_{2^n}$ such that $D_a D_b f$ is equal to zero.

Proof : For $n > 10$ the theorem is direct consequence of [1, Lemma 3]. So we will consider only the case $n = 10$. Let $a \neq 0$ and $b \neq 0$ in $\mathbb{F}_{2^n}$ be such that $a \neq b$. Then Proceeding in the same manner as in theorem 1 we get

$$Q(x) = Tr(\sum_{j\in J} \sum_{i\in C'(j)} q_i x^i),$$

For $n = 10$ and $k = 57$ the set I is given by

$$I = \{1, 8, 9, 16, 17, 24, 32, 33, 40, 48\}.$$

Since $Tr(x) = Tr(x^{2^r})$ for any r, we can expressed the polynomial $Q(x)$ in this case as: $Q(x) = Tr[(q_1 + q_8^{2^7} + q_{16}^{2^6} + q_{32}^{2^5})x] + Tr[q_9x^9] + Tr[(q_{24}^{2^7} + q_{48}^{2^6})x^3] + Tr[q_{17}x^{17}] + Tr[q_{33}x^{33}] + Tr[q_{40}^{2^7}x^5]$.
Let there exists non zero elements a, b, $a \neq b$ in $\mathbb{F}_{2^n}$ such that $Q(x) = 0$. This implies

$$\begin{aligned} q_1 + q_8^{2^7} + q_{16}^{2^6} + q_{32}^{2^5} &= 0 & (4)\\ q_9 &= 0 & (5)\\ q_{24}^{2^7} + q_{48}^{2^6} &= 0 & (6)\\ q_{17} &= 0 & (7)\\ q_{40} &= 0. & (8)\end{aligned}$$

q_{33} may or may not be equal to zero because the cardinality of $C(33)$ is not equal to $n = 10$. In order to prove the required result we have to show that there exists at least one coefficient which can not be equal to zero. Let us consider equation (12), we get

$$a^{48} + b^{48} + (a + b)^{48} = 0,$$

which is possible if and only if $a = b$ i.e. for non zero a, b, $a \neq b$, q_9 can not be zero. Therefore $Q(x)$ can not be equal to zero. Hence Proved. ■

Theorem 3 *For n even and $n \geq 10$ no non-quadratic Kasami Boolean function has second derivative equal to zero.*

Proof : From the definition given in [2], the function of the form

$$f(x) = Tr(\lambda x^k),$$

where $k = 2^{2d} - 2^d + 1$ with $\gcd(n, d) = 1$, $0 < d < n$ and $\lambda \in \mathbb{F}_{2^n}^*$, is a Kasami Boolean function. If $d = 1$, the function f is quadratic, so we do not consider the case $d = 1$. For $d = 3$ the result is direct consequence of Theorem 2 and when $3 < d < \frac{n}{2}$, the proof is obvious by theorem 1. Therefore consider the case $\frac{n}{2} < d < n$. It is given $\gcd(n, d) = 1$, this implies $\gcd(n, n - d) = 1$ i.e. for each $\frac{n}{2} < d < n$ and $\gcd(n, d) = 1$ there exists $n - d = d'$ such that $0 < d' < \frac{n}{2}$. Also from lemma 1

$$\begin{aligned} k &= 2^{2d} - 2^d + 1\\ &= 2^r(2^{2d'} - 2^{d'} + 1)\\ &= 2^r k' \ \ (say)\end{aligned}$$

Then

$$\begin{array}{rcl} Tr(\lambda x^k) & = & Tr(\lambda x^{2^r k'}) \\ & = & Tr(\lambda'^{2^r} x^{2^r k'}), \quad where \lambda = \lambda'^{2^r} \in \mathbb{F}_{2^n}^* \\ & = & Tr((\lambda' x^{k'})^{2^r}) \\ & = & Tr(\lambda' x^{k'}), \end{array}$$

which is again the case of $0 < d < \frac{n}{2}$. Therefore in this case also f does not have any second derivative equal to zero. Hence proved. ■

Corollary 1 *There exists no non-quadratic Kasami bent function on n variables which is affine equivalent to Maiorana-MacFarland type bent functions.*

Proof : For $n \geq 10$ it is obvious from Theorem 3 that for any non-quadratic Kasami bent function f there exists no non zero elements a, b, $a \neq b$ in $\mathbb{F}_{2^n}$ such that $D_a D_b f$ is equal to zero. For $n = 8$ the result can be obtained by direct computation. Then there does not exist any 2-dimensional subspace hence $\frac{n}{2}$-dimensional subspace U such that the function f is affine on every coset of U. Therefore from Proposition 1 f does not belong to the Maiorana-MacFarland class. ■

References

[1] A. Canteaut and P. Charpin. Decomposing Bent Functions. *IEEE Transactions on Information Theory*, Vol. 49, no. 8, (2003) 2004 - 2019.

[2] A. Canteaut, M. Daum, H. Dobbertin and G. Leander, Finding non-normal bent functions, *Discrete Appl. Math.* 154 (2006), 202-218.

[3] C. Carlet. Two new classes of bent functions. In *Advances in cryptology - EUROCRYPT'93.* Lecture Notes in Computer Science, number 765, pages 77-101, 1994.

[4] Pascale Charpin. Normal Boolean functions. Journal of Complexity , "Complexity Issue in Cryptography and Coding Theory", dedicated to Prof. Harald Niederreiter on the occasion of his 60th birthday.

[5] J. F. Dillon. Elementary Hadamard Difference sets. PhD Thesis, University of Maryland, 1974.

[6] J. F. Dillon. Elementary Hadamard difference sets. In *Proceedings of 6th S. E. Conference of Combinatorics, Graph Theory, and Computing.* Utility Mathematics, Winnipeg, Pages 237–249, 1975.

[7] J. F. Dillon and H. Dobbertin. New Cyclic Difference Sets with Singer Parameters, Finite Fields And Applications, 2004, Pages 342–389.

[8] H. Dobbertin. Construction of bent functions and highly nonlinear balanced Boolean functions. *FSE 1994* Lecture Notes in Computer Science, number 1008, pages 61-74, 1995.

[9] H. Dobbertin and G. Leander. A survey of some recent results on bent functions. *SETA 2004* Lecture Notes in Computer Science, number 3486, pages 1-29, 2004.

[10] X. D. Hou. $GL(m,2)$ acting on $R(r,m)/R(r-1,m)$, *Discrete Math.* 149 (1996), 99-122.

[11] X. D. Hou. Cubic bent functions, *Discrete Math.* 189 (1998), 149-161.

[12] R. Lidl and H. Niederreiter. Introduction to finite fields and their applications. Cambridge University Press, 1994.

[13] R. L. McFarland. A family difference sets in non-cyclic groups. In *J. Combinatorial Theory, Ser. A, 15*, Pages 1–10, 1973.

[14] O. S. Rothaus. On bent functions. *Journal of Combinatorial Theory, Series A*, 20:300–305, 1976.