CONSTRUCTIONS OF BENT FUNCTIONS

FATİH SULAK

JANUARY 2006

CONSTRUCTIONS OF BENT FUNCTIONS

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF APPLIED MATHEMATICS
OF
THE MIDDLE EAST TECHNICAL UNIVERSITY

BY

FATİH SULAK

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF SCIENCE
IN
THE DEPARTMENT OF CRYPTOGRAPHY

JANUARY 2006

Approval of the Graduate School of Applied Mathematics

Prof. Dr. Ersan AKYILDIZ
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

Prof. Dr. Rüyal ERGÜL
Head of Department

Examining Committee Members

Prof. Dr. Semih KORAY

Prof. Dr. Ersan AKYILDIZ

Assoc. Prof. Dr. Ali DOĞANAKSOY

Assoc. Prof. Dr. Ferruh ÖZBUDAK

Dr. Muhiddin UĞUZ

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last name : Fatih SULAK
Signature :

Abstract

CONSTRUCTIONS OF BENT FUNCTIONS

SULAK, Fatih
M.Sc., Department of Cryptography
Supervisor: Assoc. Prof. Dr. Ali DOĞANAKSOY

January 2006, 50 pages

In cryptography especially in block design, Boolean functions are the basic elements. A cryptographic function should have high nonlinearity as it can be attacked by linear attack.

In this thesis the highest possible nonlinear boolean functions in the even dimension, that is bent functions, basic properties and construction methods of bent functions are studied. Also normal bent functions and generalized bent functions are presented.

Keywords: Cryptography, Boolean functions, Bent Functions, Nonlinearity, Walsh-Hadamard transformation, Normal Bent Functions, Generalized Bent Fuctions, Bent Function Constructions.

Öz

BÜKÜK FONKSİYONLARIN OLUŞTURULMASI

SULAK, Fatih
Yüksek Lisans, Kriptografi Bölümü
Tez Yöneticisi: Doç. Dr. Ali DOĞANAKSOY

Ocak 2006, 50 sayfa

Kriptografide ve özellikle de blok şifre tasarımında Boole fonksiyonları temel unsurlardır. Kriptololojik bir fonksiyonun doğrusal saldırılara karşı dayanıklı olması için nonlineeritesinin yüksek olması gerekmektedir.

Bu tezde de mümkün olan en yüksek nonlineeriteye sahip olan fonksiyonlar yani bükük fonksiyonlar, onların özellikleri ve oluşturulması incelenmiştir. Ayrıca normal bükük fonksiyonlara ve genelleştirilmiş bükük fonksiyonlara da değinilmiştir.

Anahtar Kelimeler: Kriptografi, Boole fonksiyonları, Bükük Fonksiyonlar, Nonlineerite, Walsh-Hadamard dönüşümü, Normal Bükük Fonksiyonlar, Genelleştirilmiş Bükük Fonksiyonlar, Bükük Fonksiyonların Oluşturulması.

ACKNOWLEDGMENTS

My first, and the most earnest, acknowledgment must go to my supervisor Ali Doğanaksoy for patiently guiding, motivating, and encouraging me throughout this study. In every sense, none of this work would have been possible without him.

I also would like to thank to all people in the Boolean Functions Working Group at IAM, especially to Baha Güçlü Dündar for his valuable comments. Muhiddin Uğuz, Zülfikar Saygı and Faruk Güloğlu helped me a lot in all stages of the thesis. Also Çağdaş Çalık's program BFW was very useful and saved my hours.

Finally I would like to thank to my family for their love and support during not only the thesis but also my whole educational life.

Table of Contents

Chapter 1

Introduction

A Boolean function maps a number of input bits into a single bit. In cryptography especially in block design, Boolean functions are the basic elements. A cryptographic function should have high nonlinearity in order to prevent attacks based on linear approximation. In this thesis the highest possible nonlinear Boolean functions, that is, bent functions are studied.

Bent functions are first studied by Dillon [6] in 1974 and Rothaus [16] in 1976. The word "bent" is first used by Rothaus. Further properties and constructions of bent functions can be found in [2], [8]. Kumar, Scholtz and Welch [11] defined and studied generalized bent functions.

The thesis is organized as follows:

In Chapter 2, we establish some notations which are used throughout the thesis and recall the properties of Boolean functions. Then, we state linear and affine functions. Later, we present nonlinearity and the Walsh-Hadamard transform of Boolean functions, its properties and relations with Sylvester-Hadamard matrices.

In Chapter 3 basic properties of bent functions are given.

In Chapter 4, we present the construction methods of Bent functions.

In Chapter 5, we present normal bent functions and their properties.

In Chapter 6, generalized bent functions and their properties are investigated. Some constructions of generalized bent functions in [11] are also given.

We summarize the thesis in chapter 7.

Chapter 2

Preliminaries

In this chapter we state the definitions and the notation we use in the following chapters. The reader may refer to [17] and [19] for further information.

2.1 Boolean Functions

Let $\mathcal{V}_n$ be the vector space composed of all n-tuples of elements from $GF(2)$. An element $\alpha_k = (a_1, a_2, \ldots, a_n)$ in $\mathcal{V}_n$, can be represented by the integer $k = \sum_{i=1}^{n} a_i 2^{n-i}$. With this representation, the natural ordering of integers induces an ordering on $\mathcal{V}_n$, so called the lexicographic ordering. We denote the element of $\mathcal{V}_n$ corresponding to the integer k by α_k so that $\mathcal{V}_n = \{\alpha_0, \alpha_1, \cdots, \alpha_{2^n-1}\}$ and $\alpha_0 < \alpha_1 < \cdots < \alpha_{2^n-1}$.

For $\alpha, \beta \in \mathcal{V}_n$, the sum $\alpha \oplus \beta \in \mathcal{V}_n$ is obtained by adding corresponding components of α and β modulo 2.

The standard basis of $\mathcal{V}_n$ is denoted by $\{e_1, e_2, \ldots, e_n\}$, where e_i represents the vector having all zero's except a 1 at the i-th position.

The Hamming weight of an element $\alpha \in \mathcal{V}_n$ is the number of components that are equal to 1 and is denoted by $w(\alpha)$. The Hamming distance between two elements $\alpha, \beta \in \mathcal{V}_n$ is the number of unequal components and is denoted by $d(\alpha, \beta)$. Obviously, $d(\alpha, \beta)$ is the Hamming weight of $\alpha \oplus \beta$. From now on "the

weight" and "the distance" will mean the Hamming weight and the Hamming distance, respectively.

Let $\alpha = (a_1, a_2, \ldots, a_n)$, $\beta = (b_1, b_2, \ldots, b_n) \in \mathcal{V}_n$. The standard inner product $\langle , \rangle$ on $\mathcal{V}_n$ is defined as

$$\langle \alpha, \beta \rangle = \sum_{i=1}^{n} a_i b_i.$$

A Boolean function is a $GF(2)$ valued map, with domain $\mathcal{V}_n$. The set of all Boolean functions is denoted by $\mathcal{F}_n$. From now on, unless otherwise stated, by "a function" we mean a Boolean function in $\mathcal{F}_n$

Any $f \in \mathcal{F}_n$ has a unique representation in each of the following forms:

- The ordered tuple,

$$T_f = (f(\alpha_0), f(\alpha_1), \ldots, f(\alpha_{2^n-1}))$$

  is called the truth table of f.

- Sometimes instead of T_f, it may be more convenient to use the real valued function of f, which is called the sign function $\hat{f}$. It is defined as $\hat{f}(\alpha) = (-1)^{f(\alpha)} = 1 - 2f(\alpha)$ for all $\alpha \in \mathcal{V}_n$. The truth table of the sign function $\hat{f}$ is called the sequence of f and is denoted by ζ_f. That is

$$\zeta_f = ((-1)^{f(\alpha_0)}, (-1)^{f(\alpha_1)}, \ldots, (-1)^{f(\alpha_{2^n-1})}).$$

- The polynomial representation

$$f(x) = a_0 \oplus a_1 x_1 \oplus \cdots \oplus a_n x_n \oplus a_{12} x_1 x_2 \oplus \cdots \oplus a_{12\ldots n} x_1 x_2 \cdots x_n$$

where $a_0, a_1, \cdots, a_{12\cdots n} \in GF(2)$, is called the algebraic normal form (ANF) of f. In this representation each product of variables appearing as a part of the sum is called a term. Number of variables in each term is called the degree of that term and the degree of a function is the degree of the term (not necessarily unique) with largest degree and is denoted by $deg(f)$.

The weight of a function is defined as the number of nonzero entries in T_f and is denoted by $w(f)$. If the weight of a function is 2^{n-1}, that is the numbers of 0's and 1's are equal, then the function is called balanced. We denote the set of all balanced functions by $\mathcal{B}_n$. Obviously, $|\mathcal{B}_n| = \binom{2^n}{2^{n-1}}$.

Let $f, g \in \mathcal{F}_n$. Then by the distance between f and g, we mean the distance between T_f and T_g on $\mathcal{V}_{2^n}$, which is donated by $d(f, g)$. Thus, $d(f, g) = w(f \oplus g)$.

The following lemma is immediate from the definition.

Lemma 2.1.1. *For any $f, g \in \mathcal{F}_n$, $d(f, g) = 2^{n-1} - \frac{1}{2}\langle \zeta_f, \zeta_g \rangle$.*

Two constant functions, whose weights are equal to 0 and 2^n will be denoted by 0_n and 1_n, respectively. For a function $f \in \mathcal{F}_n$, the complement function $\bar{f}$ is defined to be $\bar{f} = f \oplus 1_n$. Trivially, it follows that $w(\bar{f}) = 2^n - w(f)$.

The support of f is defined to be the set $\{\alpha \in V_n | f(\alpha) = 1\}$ and is denoted by $Supp(f)$. It is clear that $|Supp(f)| = w(f)$ and that $Supp(f) \cap Supp(\bar{f}) = \emptyset$.

2.2 Linear and Affine Functions

A function $f \in \mathcal{F}_n$ is called linear if $f(\alpha \oplus \beta) = f(\alpha) \oplus f(\beta)$ holds for all $\alpha, \beta \in \mathcal{V}_n$ and such a function is of the form $f(x) = a_1 x_1 \oplus a_2 x_2 \oplus \cdots \oplus a_n x_n$, $a_i \in GF(2)$. The set of all linear functions is denoted by $\mathcal{L}_n$.

A function $f \in \mathcal{F}_n$ is called affine if $f(\alpha \oplus \beta) = f(\alpha) \oplus f(\beta) \oplus a$ holds for all $\alpha, \beta \in \mathcal{V}_n$ and $a \in \{0,1\}$ and such a function is of the form $f(x) = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus \cdots \oplus a_n x_n,\ a_i \in GF(2)$. The set of all affine functions is denoted by $\mathcal{A}_n$. Obviously $\mathcal{L}_n \subset \mathcal{A}_n$ and $|\mathcal{A}_n| = 2\,|\mathcal{L}_n| = 2^{n+1}$

From the above definition, it is clear that any linear function f can be written in the form $f(x) = \alpha \cdot x$ for some $\alpha \in \mathcal{V}_n$ and this linear function is denoted by f_α.

Theorem 2.2.1. *Any non-constant affine function is balanced.*

Theorem 2.2.2. *For any $f_{\alpha_i}, f_{\alpha_j} \in \mathcal{L}_n$ we have the following:*

$$d(f_{\alpha_i}, f_{\alpha_j}) = \begin{cases} 0 & if \quad \alpha_i = \alpha_j, \\ 2^{n-1} & otherwise. \end{cases}$$

The set $\{\ell_0, \ell_1, \ldots, \ell_{2^n-1}\}$ of sequences of all linear functions, forms an orthogonal basis for $\mathbb{R}^{2^n}$ over the set of real numbers $\mathbb{R}$ with respect to the standard inner product on $\mathbb{R}^{2^n}$. It follows that the sign function of any function can be written uniquely as a linear combination of $\ell_0, \ell_1, \ldots, \ell_{2^n-1}$.

Let $\hat{f}(x) = \sum_{i=0}^{2^n-1} c_i \ell_i$, where $c_i \in \mathbb{R}$ are the coefficients. If we calculate the inner product of $\hat{f}(x)$ and ℓ_j for any j, we obtain:

$$\left\langle \hat{f}(x), \ell_j \right\rangle = \sum_{i=0}^{2^n-1} c_i \left\langle \ell_j, \ell_j \right\rangle$$

Using the theorem 2.2.2, the above sum simplifies into:

$$\left\langle \hat{f}(x), \ell_j \right\rangle = c_j 2^{n-1}$$

so,

$$c_j = 2^{-n+1} \left\langle \hat{f}(x), \ell_j \right\rangle .$$

2.3 Walsh Spectrum and Nonlinearity

One of the most important concepts of the Boolean functions is nonlinearity. Nonlinearity N_f of a function is the distance between the function and the set $\mathcal{A}_n$. In particular N_f is defined as:

$$N_f = \min_{g \in \mathcal{A}_n} d(f, g). \tag{2.3.1}$$

High nonlinearity is a very important design criteria, for it is a measure for linear cryptanalysis introduced by Matsui [12]. By definition, it is clear that $N_f = 0$ if and only if f is an affine function.

Nonlinearity simply divides functions into two parts: "affine(linear) functions" and "nonaffine(nonlinear) functions". Furthermore as nonlinearity measures the distance of a function to $\mathcal{A}_n$, it also measures how well a function is linearly approximated.

Definition 2.3.1. An $n \times n$ matrix H_n with all entries 1 or -1 is called a Hadamard matrix if $H_n \cdot H_n^t = nI_n$, where H_n^t is the transpose of H_n and I_n is the $n \times n$ identity matrix.

Definition 2.3.2. The Walsh transform of a real-valued function $f : \mathcal{V}_n \to \mathbb{R}$, is

again a real-valued function $W_f : \mathcal{V}_n \to \mathbb{R}$ defined by:

$$W_f(\omega) = \sum_{\alpha \in \mathcal{V}_n} f(\alpha)(-1)^{\langle \alpha, \omega \rangle}, \tag{2.3.2}$$

where $w \in \mathcal{V}_n$.

Also the inverse Walsh transform is defined by:

$$f(\alpha) = 2^{-n} \sum_{\omega \in \mathcal{V}_n} W_f(\omega)(-1)^{\langle \alpha, \omega \rangle}.$$

Observe that, the Walsh transform and its inverse are defined for real valued functions. Therefore, for a Boolean function f, while computing its Walsh transform, the sum and values of inner product are treated as integers. We denote the Walsh transform of f and $\hat{f}$ by W_f and $W_{\hat{f}}$, respectively. Similarly, we denote the inverse Walsh transform by W_f^{-1} and $W_{\hat{f}}^{-1}$.

Lemma 2.3.3. *If $\hat{f}$ is the sign function of f, then*

$$W_{\hat{f}}(\omega) = -2W_f(\omega) + 2^n \delta(\omega),$$

which is equivalent to

$$W_f(\omega) = 2^{n-1}\delta(\omega) - \frac{1}{2} W_{\hat{f}}(\omega),$$

where $\delta(\omega)$ is the Kronecker delta function.

The ordered tuple, $(W_{\hat{f}}(\alpha_0), W_{\hat{f}}(\alpha_1), \ldots, W_{\hat{f}}(\alpha_{2^n-1}))$, is called the Walsh spectrum of f and is denoted by $T_{W_{\hat{f}}}$.

The following theorem gives a necessary and sufficient condition for a Walsh

transform to belong to sign function of a Boolean function:

Theorem 2.3.4. *$g : \mathcal{V}_n \longrightarrow \mathbb{R}$ is the Walsh transform of sign function $\hat{f}$ of a function f if and only if the following holds for all λ in $\mathcal{V}_n$:*

$$\sum_{\omega \in \mathcal{V}_n} g(\omega)g(\omega+\lambda) = 2^n\delta(\lambda) = \begin{cases} 2^n & for\ \lambda = \alpha_0 \\ 0 & otherwise \end{cases}$$

If we re-compute the equation for $\lambda = \alpha_0$, we get the following identity which is known as Parseval identity.

Corollary 2.3.5.

$$\sum_{\omega \in \mathcal{V}_n} \left(W_{\hat{f}}(\omega)\right)^2 = 2^{2n}. \tag{2.3.3}$$

It is obvious that, for any $f \in \mathcal{F}_n$,

$$\begin{aligned} W_{\hat{f}}(\alpha_i) &= \sum_{\beta \in \mathcal{V}_n} (-1)^{f(\beta)}(-1)^{\langle \beta, \alpha_i \rangle} \\ &= \sum_{\beta \in \mathcal{V}_n} (-1)^{f(\beta)}(-1)^{f_{\alpha_i}(\beta)} \\ &= \langle \zeta_f, \ell_i \rangle . \end{aligned}$$

Thus, $W_{\hat{f}}(\alpha_i)$ is in fact, nothing but the difference between the number of 0's and the number of 1's in $T_{(f \oplus f_{\alpha_i})}$. Then, it is easy to see that:

$$d(f, f_{\alpha_i}) = \frac{1}{2}(2^n - W_{\hat{f}}(\alpha_i)) \tag{2.3.4}$$

From the equation above, it follows that:

$$T_{W_{\hat{f}}} = \zeta_f H_n,$$

Another criterion, a cryptographically good Boolean function should satisfy is correlation immunity. A Boolean function, whose output distribution probability is unchanged when any m of input bits are kept constant, is called m-th order correlation immune where $m \in \{1, 2, \ldots, n\}$. Furthermore, if a balanced Boolean function is m-th order correlation immune, f is then said to be m-resilient.

Correlation immunity and resiliency of a function f can be characterized through the Walsh transform of f as follows,

Theorem 2.3.6. *Any $f \in \mathcal{F}_n$ is m-th order correlation immune where $m \in \{1, 2, \ldots, n\}$ if and only if $W_{\hat{f}}$ satisfies*

$$W_{\hat{f}}(\omega) = 0, \text{ for all } \omega \in \mathcal{V}_n \text{ with } 1 \leq w(\omega) \leq m.$$

Theorem 2.3.7. *Let* $H_n = \begin{bmatrix} l_0 \\ l_1 \\ \vdots \\ l_{2^n-1} \end{bmatrix}$ *be the matrix of order 2^n ($n \geq 0$) where the i^{th} row is the sequence l_i of the linear function $f_{\alpha_i}(x) = \langle \alpha_i, x \rangle$ for $i = 0, 1, \cdots, 2^n - 1$ where $\alpha_i \in V_n$.*

The matrix H_n defined in the above theorem is called Slyvester-Hadamard matrix or order n. This theorem is very useful since it says that the n^{th} order Slyvester-Hadamard matrix is the complete table of the sequences of all linear functions in $\mathcal{F}_n$. Since H_n is a symmetric matrix, the above theorem is also valid for the columns of H_n.

One asks the natural question: What is the maximum possible value of the nonlinearity of a function?

Theorem 2.3.8. *For any function f, N_f satisfies the following inequality:*

$$N_f \leq 2^{n-1} - 2^{\frac{n}{2}-1}.$$

Proof: Combining equation 2.3.1 and 2.3.4, we conclude that

$$N_f = 2^{n-1} - \frac{1}{2} \max_{f_{\alpha_i} \in \mathcal{A}_n} \left| W_{\hat{f}}(\alpha_i) \right|. \tag{2.3.5}$$

From Parseval identity we know that

$$\sum_{\omega \in \mathcal{V}_n} \left(W_{\hat{f}}(\omega) \right)^2 = 2^{2n}.$$

In this summation there are 2^n terms. So the maximum term is not less than $\frac{2^{2n}}{2^n} = 2^n$. Then

$$\max_{f_{\alpha_i} \in \mathcal{A}_n} \left| W_{\hat{f}}(\alpha_i) \right| \geq 2^{n/2}$$

Then 2.3.5 yields

$$N_f \leq 2^{n-1} - 2^{\frac{n}{2}-1}.$$

□

Chapter 3

Properties of Bent Functions

One of the most important class of Boolean functions is bent functions. They play an important role in cryptography. Bent functions are first studied by Dillon [6] and Rothaus [16] in seventies. Rothaus used the word "bent" for the first time and gave constructions of bent functions of degree 3 on $\mathcal{F}_6$.

In a private communication to Dillon, Maiorana generalized a class of Rothaus' bent functions. The general theory of bent functions are studied by Kumar, Scholtz and Welch [11].

3.1 Basic Properties of Bent Functions

Definition 3.1.1. A function f is called bent if the components of the Walsh spectrum of f all have the same magnitude, up to the absolute value.

Example 3.1.2. Let $f \in \mathcal{F}_2$ be defined as $f(x) = x_1x_2+x_2$. Since $T_f = (0, 1, 0, 0)$ and Walsh spectrum = [2,2,-2,2], f is a bent function.

Example 3.1.3. Let $f \in \mathcal{F}_4$ be defined as $f(x) = x_1 + x_1x_2 + x_3x_4 + x_4$. Since

$$T_f = (0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 1, 0, 0)$$

and

$$W_f = [4, 4, -4, 4, -4, -4, 4, -4, 4, 4, -4, 4, 4, 4, -4, 4]$$

f is a bent function.

Using the Parseval identity one easily obtains:

Theorem 3.1.4. *$f \in \mathcal{F}_n$ is a bent function if and only if $\left|W_{\hat{f}}(\alpha)\right| = 2^{n/2}$ for all $\alpha \in \mathcal{V}_n$.*

Rothaus gave the basic properties of bent functions in his article [16]. Following theorems are due to him and Dillon [5], [6].

Theorem 3.1.5. *([16]) Let f be a bent function. g, defined by setting $(-1)^{g(x)} = \frac{W_{\hat{f}(\alpha)}}{2^{n/2}}$ for all $\alpha \in \mathcal{V}_n$, is also a bent function.*

Proof: Since f is bent, by theorem 3.1.4 g is in $\mathcal{F}_n$.

$$\hat{f}(x) = \frac{1}{2^n} \sum_{\alpha \in \mathcal{V}_n} W_{\hat{f}}(\alpha)(-1)^{\langle \alpha, x \rangle} = \frac{1}{2^{n/2}} \sum_{\alpha \in \mathcal{V}_n} (-1)^{g(\alpha) + \langle \alpha, x \rangle} = \frac{1}{2^{n/2}} W_{\hat{g}}(x).$$

Thus, g is bent. □

The function g in the previous theorem is called the dual of f. The dual of a bent function will be used to construct new bent functions, in the next chapter. Also it is easy to observe that if g is the dual of a function f then the dual of g is f.

Lemma 3.1.6. *([16]) A function f is bent if and only if the matrix $A = (a_{ij})$ of order 2^n where $a_{ij} = \frac{1}{2^{n/2}} W_{\hat{f}}(\alpha_i + \alpha_j)$ for $0 \leq i, j \leq 2^n - 1$ is a Hadamard matrix.*

Proof: Let $AA^t = (x_{ij})$ where $x_{ij} = \frac{1}{2^n}\sum_{t=0}^{2^n-1} W_{\hat{f}}(\alpha_i + \alpha_t)W_{\hat{f}}(\alpha_j + \alpha_t)$. But since

$$\sum_{\alpha \in \mathcal{V}_n} W_{\hat{f}}(\alpha)W_{\hat{f}}(\alpha+\beta) = \begin{cases} 2^{2n} & if \quad \beta = 0, \\ 0 & otherwise. \end{cases}$$

we get:

$$x_{ij} = \begin{cases} 2^n & if \quad i = j, \\ 0 & otherwise. \end{cases}$$

We conclude that A is a Hadamard matrix. The converse is trivial. □

Given $f \in \mathcal{F}_n$, the function $f_\alpha \in \mathcal{F}_n$ defined by $g_\alpha(x) = f(x) + f(x+\alpha)$ is called the directional derivative of f in the direction $\alpha \in \mathcal{V}_n$.

Theorem 3.1.7. *([5]) All directional derivatives of a bent function are balanced.*

Theorem 3.1.8. *([16]) A function f is bent if and only if the matrix defined by*

$$M_f = (m_{ij});\ where\ m_{ij} = (-1)^{f(\alpha_i+\alpha_j)},\ 0 \le i,j \le 2^n - 1$$

is a Hadamard matrix.

Proof: Let $MM_f^t = (x_{ij})$ where

$$x_{ij} = \sum_{\alpha_t \in \mathcal{V}_n} (-1)^{f(\alpha_i+\alpha_t)+f(\alpha_j+\alpha_t)}$$

If we change the variable we get:

$$x_{ij} = \sum_{\theta \in \mathcal{V}_n} (-1)^{f(\theta)+f(\alpha_i+\alpha_j+\theta)}$$

But the function inside the summation is nothing but a directional derivative of

f. By using theorem 3.1.7 we get:

$$x_{ij} = \begin{cases} 2^n & if \quad i = j, \\ 0 & otherwise. \end{cases}$$

We conclude that M_f is a Hadamard matrix. The converse is trivial. □

Theorem 3.1.9. *([16]) If $f \in \mathcal{F}_n$ is a bent function, then n is even, $n = 2k$; the degree of f is at most k, except for the case $k = 1$.*

Proof: That n is even follows from the observation that $\left|W_{\hat{f}}(\alpha)\right| = 2^{n/2}$ is an integer. For the second statement, let $n > r > k > 1$. We define the functions f and g:

$$f(x_1, x_2, \cdots, x_r, 0, 0, \cdots, 0) = g(x_1, x_2, \cdots, x_r)$$

and put

$$(-1)^{g(x)} = \frac{1}{2^r} \sum_{\alpha_1, \alpha_2, \cdots, \alpha_r = 0,1} W_{\hat{g}}(\alpha_1, \alpha_2, \cdots, \alpha_r)(-1)^{\alpha_1 \cdot x_1 + \alpha_2 \cdot x_2 + \cdots + \alpha_r \cdot x_r}.$$

We have

$$(-1)^{f(x)} = \frac{1}{2^n} \sum_{\alpha_1, \alpha_2, \cdots, \alpha_n = 0,1} W_{\hat{f}}(\alpha_1, \alpha_2, \cdots, \alpha_n)(-1)^{\alpha_1 \cdot x_1 + \alpha_2 \cdot x_2 + \cdots + \alpha_n \cdot x_n}.$$

Comparing these equations and using the uniqueness of the Walsh transform,

we conclude

$$W_{\hat{g}}(\alpha_1, \alpha_2, \cdots, \alpha_r) = \frac{1}{2^{n-r}} \sum_{\alpha_{r+1}, \alpha_{r+2}, \cdots, \alpha_n = 0,1} W_{\hat{f}}(\alpha_1, \alpha_2, \cdots, \alpha_n). \tag{3.1.1}$$

At this point letting $\omega = 0$ in 2.3.2, we get:

$$W_{\hat{g}}(0) = \sum_{\alpha \in \mathcal{V}_n} (-1)^{g(\alpha)} = \ number\ of\ 0's - \ number\ of\ 1's. \tag{3.1.2}$$

But also

$$number\ of\ 0's + \ number\ of\ 1's = 2^n. \tag{3.1.3}$$

Then we find that

$$number\ of\ 0's = 2^{n-1} + \frac{1}{2} W_{\hat{g}}(0).$$

If we combine this result with equation 3.1.1, the number of 0's of g is equal to

$$2^{r-1} + \frac{1}{2^{n-r+1}} \sum_{\alpha_{r+1}, \alpha_{r+2}, \cdots, \alpha_n = 0,1} W_{\hat{f}}(0, 0, \cdots, \alpha_{r+1}, \alpha_{r+2}, \cdots, \alpha_n).$$

Since f is bent, $\left| W_{\hat{f}}(0, 0, \cdots, \alpha_{r+1}, \alpha_{r+2}, \cdots, \alpha_n) \right| = 2^{n/2}$ for all 2^{n-r} summands. So the number of 0's of g and the weight of g is even for $n > 2$. However $w(g) \equiv a_{12\ldots r} (mod\ 2)$ where $a_{12\ldots r}$ is the coefficient of $x_1 x_2 \ldots x_r$ [17]. Thus, $a_{12\ldots r} = 0$ and the degree of g is less than r for any arbitrary $r > k$. We conclude that $deg(f) \leq k$.

□

Since bent functions are defined only for even values of n, from now on unless otherwise stated explicitly we assume that n is even and $n > 2$. Also we find that

this theorem gives us an obvious upper bound for the number of bent functions, that is the number of bent functions is at most $2^{\binom{n}{0}+\binom{n}{1}+\cdots+\binom{n}{n/2}}$.

Fact 3.1.10. *A function f is bent if and only if the complement $\bar{f}$ of f, is bent.*

Example 3.1.11. Let $f \in \mathcal{F}_4$ be defined as $f(x) = x_1x_2 + x_3x_4$. Since

$$T_f = (0,0,0,1,0,0,0,1,0,0,0,1,1,1,1,0)$$

and

$$W_f = [4,4,4,-4,4,4,4,-4,4,4,4,-4,-4,-4,-4,4],$$

f is a bent function.

Let $g \in \mathcal{F}_4$ be defined as $g(x) = 1 + x_1x_2 + x_3x_4$. Since

$$T_g = (1,1,1,0,1,1,1,0,1,1,1,0,0,0,0,1)$$

and

$$W_g = [-4,-4,-4,4,-4,-4,-4,4,-4,-4,-4,4,4,4,4,-4],$$

g is also a bent function.

Fact 3.1.12. *A bent function cannot be correlation immune.*

The following theorem is very important because it enables us to obtain many new bent functions once we have one. Moreover, in the next chapter completeness of a class of bent functions will be obtained on the basis of this theorem.

Theorem 3.1.13. *[16] A bent function is invariant*

- *under a linear or an affine transformation in coordinates, that is f is bent if and only if the function $h = f \circ \theta$ is bent where $\theta(x) = xA + \alpha$, A is a nonsingular matrix of order n and α is any vector in $\mathcal{V}_n$.*

- *by adding an affine function, that is f is bent if and only if $f + \phi$ is bent for any affine function ϕ.*

Example 3.1.14. Let $f \in \mathcal{F}_4$ be defined as $f(x) = x_1x_2 + x_1x_3 + x_2x_4$. f is a bent function. Let $g \in \mathcal{F}_4$ be defined as $g(x) = x_1x_2 + x_1x_3 + x_2x_4 + x_1$. Since

$$T_g = (0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0)$$

and

$$W_g = [4, 4, -4, 4, 4, -4, -4, -4, 4, 4, 4, -4, 4, -4, 4, 4],$$

g is also a bent function.

The following theorem says that bent functions are the furthest functions to the set of all affine functions.

Theorem 3.1.15. *Let f be a function. Then f is bent if and only if $d(f, A_n) = N_{max}$ where $N_{max} = 2^{n-1} - 2^{\frac{n}{2}-1}$ is the largest value of nonlinearity.*

The following theorem says that bent functions are not balanced.

Theorem 3.1.16. *Let f be a bent function. Then $w(f) = 2^{n-1} \pm 2^{\frac{n}{2}-1}$.*

Proof: If we combine equation 3.1.2 and 3.1.3 we find that

$$w(f) = \text{ number of } 1's = 2^{n-1} - \frac{1}{2}W_{\hat{f}}(0)$$

But since $W_{\hat{f}}(0) = \pm 2^{n/2}$ we conclude

$$w(f) = 2^{n-1} \pm 2^{\frac{n}{2}-1}$$

□

A main obstacle in the study of bent functions is the lack of recurrence laws. There are few constructions deriving bent functions from smaller ones. But it seems that most of them appear without any roots to bent functions in lower dimensions. In the next chapter, construction methods will be given.

Theorem 3.1.17. *([16]) Let the function h be defined as $h(z) = f(x) + g(y)$ for $z = (x, y) \in \mathcal{V}_m \oplus \mathcal{V}_n$. Then h is bent if and only if f and g are bent.*

Definition 3.1.18. A function f is said to be decomposable if there is a linear transformation on the input coordinates such that h can be written as a sum of functions on disjoint variables as in Theorem 3.1.17.

In other words $h \in \mathcal{F}_n$ is decomposable if there exists a binary matrix of order n such that $h(zA) = f(x)+g(y)$ where $z = (x, y) \in V_n$ for $x \in V_k$, $y \in V_t$ satisfying $k + t = n$. If there exists no such matrix, then h is said to be indecomposable.

If h is a decomposable bent function for $n = 2k$, then by Theorem 3.1.17 $deg(f) < k$ and $deg(g) < k$ if $k \neq 2$. So we obtain:

Theorem 3.1.19. *([16]) If f is a bent function in $\mathcal{F}_n$ where $n = 2k$ for $k \geq 3$, then f is indecomposable.*

Chapter 4

Constructions of Bent Functions

4.1 Rothaus' Bent Function Classes

In 1975, Rothaus [16] presented the first two classes of bent functions. He made an exhaustive search on all polynomials in $\mathcal{V}_6$. It was feasible due to the observation that the degree three part of any bent function in $\mathcal{V}_6$ could be brought into one of the following four forms by a linear transformation in coordinates:

1. $x_1x_2x_3$
2. $x_1x_2x_3 + x_4x_5x_6$
3. $x_1x_2x_3 + x_2x_4x_5$
4. $x_1x_2x_3 + x_2x_4x_5 + x_3x_4x_6$

Then all of the 2^{15} possible quadratic parts were tried. Answers were found in classes 1,3 and 4 of which typical ones are listed below:

1. $x_1x_2x_3 + x_1x_4 + x_2x_5 + x_3x_6$
2. $x_1x_2x_3 + x_2x_4x_5 + x_1x_2 + x_1x_4 + x_2x_6 + x_3x_5 + x_4x_5$

3. $x_1x_2x_3 + x_2x_4x_5 + x_3x_4x_6 + x_1x_4 + x_2x_6 + x_3x_4 + x_3x_5 + x_2x_6 + x_4x_5 + x_4x_6$

It is observed that all the members in a class are related to each other by an affine transformation of coordinates followed by the addition of linear terms. Also, since all quadratic bent functions are known [14], all bent functions in $\mathcal{V}_n$ for $n \leq 6$ are known. For case $n = 8$ Hou [10] classified bent functions of degree lees than or equal to 3. It is still an open problem to classify all bent functions in $\mathcal{V}_8$.

Finally, two general classes of bent functions are presented in [16].

Theorem 4.1.1 (Rothaus Class I)**.** *([16]) Let $n = 2k$ and $x, y \in \mathcal{V}_k$ and f be any function in $\mathcal{F}_k$. Then the function $Q(x, y) \in \mathcal{F}_{2k}$ given by $Q(x, y) = x_1y_1 + x_2y_2 + \cdots + x_ky_k + f$ is bent.*

Example 4.1.2. Let's take $k = 2$. Then $f = x_1x_2 + x_3x_4$, whose truth table is given by

$$T_f = [0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0]$$

and whose Walsh spectrum is given by

$$W_f = [4, 4, 4, -4, 4, 4, 4, -4, 4, 4, 4, -4, -4, -4, -4, 4]$$

is a bent function.

Theorem 4.1.3 (Rothaus Class II)**.** *([16]) Let $A(x), B(x), C(x)$ be bent functions on F_{2k} such that $A(x)+B(x)+C(x)$ is also bent. Let $y, z \in \mathcal{V}_1$. Then the function*

$$\begin{aligned} Q(x, y, z) &= A(x)B(x) + B(x)C(x) + C(x)A(x) \\ &\quad + [A(x) + B(x)]y + [A(x) + C(x)]z + yz \end{aligned}$$

is a bent function in F_{2k+2}.

Example 4.1.4. Let's take $k = 2$, $A(x) = B(x) = x_1x_2 + x_3x_4$ and $C(x) = x_1x_2 + x_3x_4 + x_1x_3$. Then $A(x) + B(x) + C(x) = C(x)$ is a bent function. Let $x_5, x_6 \in \mathcal{V}_1$. Then $Q(x) = x_1x_2 + x_3x_4 + x_5x_6 + x_1x_3x_6$ is a bent function in F_6

4.2 Maiorana McFarland's Class

Maiorana McFarland's class of bent functions is a generalization of Rothaus' class I. This class is not complete (recall theorem 3.1.13) and denoted by $\mathcal{M}$; its completed version is denoted by $\mathcal{M}^{\#}$.

Theorem 4.2.1 (Maiorana McFarland Class)**.** *([13]) Let k be an arbitrary positive integer and $n = 2k$. Then the function $f \in \mathcal{F}_n$ given by*

$$f(x) = x_2 \cdot \pi(x_1) + g(x_1)$$

where $x_1, x_2 \in \mathcal{V}_k$ are defined by

$$x = [x_1, x_2]$$

π is an arbitrary permutation of $\mathcal{V}_k$ and g is an arbitrary function from $\mathcal{V}_k$ into $\mathcal{V}_1$ is bent.

The number of functions in $\mathcal{F}_{n/2}$ is $2^{2^{n/2}}$ and the number of permutations in $\mathcal{V}_{n/2}$ is $2^{(n/2)}!$. So the number of functions satisfying the condition in the above theorem is $2^{2^{n/2}}2^{(n/2)}!$.

Example 4.2.2. Lets consider the vector space $\mathcal{V}_4$. First we divide y_i's into two:

$$x_1 = [y_1, y_2] \; and \; x_2 = [y_3, y_4]$$

Let $\pi(x_1) = [y_2, y_1]$ and $g(x_1) = y_1 + y_1y_2$. Then

$$f(y) = x_2 \cdot \pi(x_1) + g(x_1) = [y_3, y_4] \cdot [y_2, y_1] + y_1 + y_1y_2 = y_2y_3 + y_1y_4 + y_1 + y_1y_2,$$

whose truth table is given by

$$T_f = [0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 1, 0]$$

and whose Walsh spectrum is given by

$$W_f = [4, -4, 4, 4, 4, -4, -4, -4, 4, 4, 4, -4, 4, 4, -4, 4],$$

is a bent function.

4.3 Partial Spreads (PS)

Dillon [6] defines Partial Spreads as union of two disjoint classes $\mathcal{PS}^-$ and $\mathcal{PS}^+$:

- the elements of $\mathcal{PS}^-$ are those functions whose supports are the unions of 2^{k-1} disjoint k-dimensional subspaces of $\mathcal{V}_n$, less the point 0 ($k = n/2$). In this definition disjoint means that any two of these spaces have only 0 as common element and therefore their sum is direct and equal to $\mathcal{V}_n$, that is

they are the sums of 2^{k-1} characteristic functions of disjoint k-dimensional subspaces.

- the elements of $\mathcal{PS}^+$ are those functions whose supports are the unions of $2^{k-1}+1$ disjoint k-dimensional subspaces of $\mathcal{V}_n$. They are the sums of $2^{k-1}+1$ characteristic functions of disjoint k-dimensional subspaces.

The Walsh transform of any function of $\mathcal{PS}$ is deduced from the function itself by replacing the spaces by their duals, $\mathcal{PS}$ is not complete but the completed version, which is denoted by $\mathcal{PS}^{\#}$, can be obtained by changing the subspaces into flats, two of them having a single (fixed) point in common, and by adding affine functions. $\mathcal{PS}^{\#}$ does not include $\mathcal{M}^{\#}$ and $\mathcal{M}^{\#}$ does not include $\mathcal{PS}^{\#}$.

Example 4.3.1. Let's try to construct a bent function in $\mathcal{PS}^-$ for $k=3$, that is $f \in \mathcal{F}_6$. We start by choosing 4 disjoint 3-dimensional subspaces. Let the subspaces of $\mathcal{F}_6$ are defined as

$$\begin{aligned} G_1 &= \{(0,0,0,0,0,0),(0,0,1,0,0,0),(0,1,0,0,0,0),(1,0,0,0,0,0),\\ &\quad (0,1,1,0,0,0),(1,0,1,0,0,0),(1,1,0,0,0,0),(1,1,1,0,0,0)\} \end{aligned}$$

$$\begin{aligned} G_2 &= \{(0,0,0,0,0,0),(0,0,0,0,0,1),(0,0,0,0,1,0),(0,0,0,1,0,0),\\ &\quad (0,0,0,0,1,1),(0,0,0,1,0,1),(0,0,0,1,1,0),(0,0,0,1,1,1)\} \end{aligned}$$

$$G_3 = \{(0,0,0,0,0,0),(0,0,1,0,0,1),(0,1,0,0,1,0),(1,0,0,1,0,0),$$
$$(0,1,1,0,1,1),(1,0,1,1,0,1),(1,1,0,1,1,0),(1,1,1,1,1,1)\}$$

$$G_4 = \{(0,0,0,0,0,0),(0,0,1,1,0,0),(0,1,0,0,0,1),(1,0,0,1,1,0),$$
$$(0,1,1,1,0,1),(1,0,1,0,1,0),(1,1,0,1,1,1),(1,1,1,0,1,1)\}$$

Then the truth table of the function f is given by

$$T_f = (1,1,1,1,1,1,1,1,1,0,0,1,0,0,0,1,1,1,0,0,0,0,0,1,0,0,1,0,1,0,0,1,$$
$$0,0,0,1,0,1,0,1,0,1,0,0,1,0,0,1,0,0,0,0,0,1,1,1,0,0,1,0,0,0,1,0)$$

is a bent function.

$\mathcal{PS}$ is a very important class of bent functions but it is not defined expilicitly. But Dillon defines an explicit subclass of $\mathcal{PS}^-$ denoted by $\mathcal{PS}_{ap}$.

Definition 4.3.2. $\mathcal{PS}_{ap}$ is the set of all the functions of the form $g(\frac{x}{y})$, (with $\frac{x}{y} = 0$ if $x = 0$ or $y = 0$) where g is a balanced function on $\mathcal{V}_{n/2}$ which vanishes at 0 ($g(0) = 0$).

4.4 Carlet's Bent Functions

Carlet [2] used known bent functions and altered them to obtain new bent functions. Dillon [6] presented a result in this sense, which may be stated as follows: "Let f be a bent function on $\mathcal{F}_n$; suppose its support contains a k-dimensional linear subspace E of $\mathcal{F}_n$. Then, denoting by ϕ_E the function of support E, the function $f + \phi_E$ is bent". Carlet used this result to obtain new classes.

Theorem 4.4.1. *([2]) Let E be a $(n/2)$-dimensional linear subspace of $\mathcal{F}_n$ and π be a permutation on $\mathcal{F}_{n/2}$ such that, for any (x, y) in E, the number: $x \cdot \pi(y)$ equals 0. Then the function defined on $\mathcal{F}_n$ as:*

$$f(x, y) = x \cdot \pi(y) + \phi_E(x, y)$$

is bent, where ϕ_E denotes the function of support E.

This class does not lead to an effective construction method since there is no simple description of all the subspaces and permutations satisfying the condition of theorem 4.4.1. But there is a simple subcase of the theorem.

Definition 4.4.2. Class $\mathcal{D}$ consists of all functions $f \in \mathcal{F}_n$ of the form:

$$f(x, y) = \phi_E(x, y) + x \cdot \pi(y)$$

where E is a subspace of $\mathcal{F}_n$ equal to $E_1 \times E_2$, E_1 and E_2 being subspaces of $\mathcal{F}_{n/2}$ with $dim\ E_1 + dim\ E_2 = n/2$ and π is any permutation on $\mathcal{F}_{n/2}$ such that $\pi(E_2) = E_1^{\perp}$.

Class $\mathcal{D}_0$ consists of all the functions $f \in \mathcal{F}_n$ of the form:

$$f(x,y) = \prod_{i=1}^{n/2}(x_i + 1) + x \cdot \pi(y)$$

$\mathcal{D}_0$ corresponds to the case: $E = 0 \times \mathcal{F}_{n/2}$.

By theorem 4.4.1 $\mathcal{D}$ and $\mathcal{D}_0$ are bent function classes. Carlet [2] showed that $\mathcal{D}$ and $\mathcal{D}_0$ are neither included in $\mathcal{M}^{\#}$, nor included in $\mathcal{PS}^{\#}$. Also he showed that the bent functions of degree 3 on $\mathcal{F}_6$ all belong to class $\mathcal{D}_0^{\#}$.

The sizes of $\mathcal{D}$ and $\mathcal{M}$ have approximately same order since the number $2^{2^{n/2}}$ of functions in $\mathcal{F}_{n/2}$ is small, compared with the number of permutations on the same space: $(2^{n/2})!$.

Theorem 4.4.3. *([2]) Let L be any linear subspace of $\mathcal{F}_{n/2}$ and π be a permutation on $\mathcal{F}_{n/2}$ such that, for any element λ of $\mathcal{F}_{n/2}$, the set $\pi^{-1}(\lambda + L)$ is a flat. Then the function defined on $\mathcal{F}_n$ as:*

$$f(x,y) = x \cdot \pi(y) + \phi_L^{\perp}(x,y)$$

is bent.

Definition 4.4.4. Class $\mathcal{C}$ consists of all functions $f \in \mathcal{F}_n$ of the form:

$$f(x,y) = x \cdot \pi(y) + \phi_L^{\perp}(x,y)$$

where L and π satisfy the conditions of theorem 4.4.3.

Class $\mathcal{C}$ contains $\mathcal{D}_0$ (which corresponds to the case $L = \mathcal{F}_{n/2}$), so it is not included in classes $\mathcal{M}^{\#}$ and $\mathcal{PS}^{\#}$. As well, $\mathcal{C}$ is not included in class $\mathcal{D}^{\#}$ since it

contains functions of degrees less than $n/2$.

The following theorem Carlet [3] proved that from a set $\{f_{x'}, x' \in \mathcal{V}_r\}$ of bent functions on $\mathcal{V}_n$ (n, r even) and under a certain condition, we can deduce the bentness of the function $(x, x') \to f_{x'}(x)$ on $\mathcal{V}_{n+r}$.

Theorem 4.4.5. *([3]) Let n and r be two positive even integers and f be a function on $\mathcal{V}_{n+r} = \mathcal{V}_n \times \mathcal{V}_r$ such that, for any element x' of $\mathcal{V}_r$, the function on $\mathcal{V}_n$ defined as $f_{x'} : x \to f(x, x')$ is bent. Then f is bent if and only if for any element s of $\mathcal{V}_n$, the function*

$$\varphi_s : x' \longrightarrow \tilde{f_{x'}}(s)$$

is bent on $\mathcal{V}_r$.

Example 4.4.6. Let us choose $n = 2$ and replace x with (x_1, x_2), x' with x and r with n. Take:

$$f(x_1, x_2, x) = g(x)h(x)+g(x)k(x)+h(x)k(x)+[g(x)+h(x)]x_1+[g(x)+k(x)]x_2+x_1x_2$$

We know that any function of the form $x_1x_2+a_1x_1+a_2x_2+a_3$ is bent on $\mathcal{V}_2$. So f is bent for any x. It is trivial to check that the dual of the function $x_1x_2+a_1x_1+a_2x_2+a_3$ is $x_1x_2+a_2x_1+a_1x_2+a_1a_2+a_3$. Here $a_1 = g(x)+h(x)$, $a_2 = g(x)+k(x)$ and $a_3 = g(x)h(x) + g(x)k(x) + h(x)k(x)$.

According to theorem 4.4.5, f is bent if and only if the following functions are bent:

- for $s_1 = s_2 = 0$: $a_1a_2 + a_3 = g(x)$
- for $s_1 = 0$, $s_2 = 1$: $a_1 + a_1a_2 + a_3 = h(x)$

- for $s_1 = 1$, $s_2 = 0$: $a_2 + a_1a_2 + a_3 = k(x)$
- for $s_1 = s_2 = 1$: $1 + a_2 + a_1 + a_1a_2 + a_3 = 1 + g(x) + h(x) + k(x)$. And $1 + g(x) + h(x) + k(x)$ is bent if and only if $g(x) + h(x) + k(x)$ is bent.

So it leads to the Rothaus Class II.

Carlet [3] used this theorem to construct new classes. He used $\mathcal{M}$, $\mathcal{PS}_{ap}$ and $\mathcal{D}_0$ as known classes. The first proposition uses classes $\mathcal{M}$ and $\mathcal{D}_0$.

Proposition 4.4.7. *([3]) Let n be a positive even integer and m, r two positive integers whose sum is equal to n. The elements of $\mathcal{V}_n$ are written in the form (x, y, x', y'), where x, y are elements of $\mathcal{V}_{m/2}$ and x', y' are elements of $\mathcal{V}_{r/2}$. Let π and π' be permutations on $\mathcal{V}_{m/2}$ and $\mathcal{V}_{r/2}$ respectively and h be a function in $\mathcal{F}_{r/2}$. Then the following function $f \in \mathcal{F}_n$ is bent:*

$$f(x, y, x', y') = x \cdot \pi(y) + x' \cdot \pi'(y') + \delta_0(x)h(y')$$

where δ_0 denotes the Dirac symbol at 0, that is $\delta_0 = 1$ if $x = 0$, $\delta_0 = 0$ otherwise.

The definition of f in the proposition 4.4.7 is very similar to that of Maiorana McFarland class but it is not included in $\mathcal{M}^{\#}$.

Second proposition uses the single class $\mathcal{PS}_{ap}$.

Proposition 4.4.8. *([3]) Let n be any positive even integer and m, r two positive integers whose sum is equal to n. Let k be a function in $\mathcal{F}_{m/2} \times \mathcal{F}_{r/2}$ such that for any element x of $\mathcal{V}_{m/2}$, the function $x' \to k(x, x')$ is balanced on $\mathcal{V}_{r/2}$ and for any element x' of $\mathcal{V}_{r/2}$, the function $x \to k(x, x')$ is balanced on $\mathcal{V}_{m/2}$. Then the*

following function $f \in \mathcal{F}_n$ is bent:

$$f(x, y, x', y') = k(\frac{x}{y}, \frac{x'}{y'})$$

Third proposition uses classes $\mathcal{M}$, $\mathcal{PS}_{ap}$ and $\mathcal{D}_0$.

Proposition 4.4.9. *([3]) Assume $n = 4q$. Let π and π' be two permutations on $\mathcal{V}_q$ and $g \in \mathcal{F}_q$ be a balanced function. Then the following function $f \in \mathcal{F}_n = (\mathcal{F}_q)^4$ is bent:*

$$f(x, y, x', y') = x' \cdot \pi' \left[y' + \pi \left(\frac{x}{y} \right) \right] + \delta_0(x') g \left(\frac{x}{y} \right)$$

4.5 Dobbertin's Bent Functions

Definition 4.5.1. ([7]) Let σ, ϕ and γ be chosen such that:

$$\sigma : \mathcal{V}_n \longrightarrow \mathcal{V}_1 \ balanced,$$
$$\phi : \mathcal{V}_n \longrightarrow \mathcal{V}_n \ bijective,$$
$$\gamma : \mathcal{V}_n \longrightarrow \mathcal{V}_n \ arbitrary.$$

The function $f_{\sigma,\phi,\gamma}$ on $\mathcal{V}_{2n}$ associated to the triple (σ, ϕ, γ) is defined as follows:

$$f(x, \phi(y)) = \begin{cases} \sigma \left(\frac{x+\gamma(y)}{y} \right) & if \quad y \neq 0, \\ 0 & otherwise. \end{cases}$$

This construction is called triple construction. If $f_{\sigma,\phi,\gamma}$ is a bent function then (σ, ϕ, γ) is called a bent triple associated to $f_{\sigma,\phi,\gamma}$.

Lemma 4.5.2. *([7]) Let U be a subspace of $\mathcal{V}_n$ and $y_0 \in \mathcal{V}_n$. Then there is an*

onto linear mapping $\rho : \mathcal{V}_n \to U$ *such that a one to one correspondence between all functions* $\sigma \in \mathcal{F}_n$ *with*

$$Supp(W_\sigma) \subseteq y_0 + U$$

and all functions τ *on* U *is given by setting*

$$\sigma(x) = \tau\rho(x) + \langle x, y_0 \rangle .$$

Moreover, all σ *are ablanced if and only if* $y_0 \notin U$.

Theorem 4.5.3. *([7]) Let* (σ, ϕ, γ) *be given as described in the triple construction. Suppose* $\phi(x) = x^d$, $\gamma(x) = x^{d'}$ *(or* $\gamma = 0$*) for* $d, d' < 2^n - 1$ *and let a non-trivial subspace* U *of* $\mathcal{V}_n$ *and* $y_0 \in \mathcal{V}_n - U$ *be given such that the following conditions are satisfied:*

1. ϕ *is bijective, that is* d *is relatively prime to* $2^n - 1$.
2. ϕ *and* γ *are not affine, that is* d *and* d' *are not powers of* 2.
3. ϕ *and* γ *are affine on* $y_0 + U$.

Define $\sigma : \mathcal{V}_n \longrightarrow \mathcal{V}_1$ *as a nonaffine balanced function such that the support of* W_σ *is a subset of* $y_0 + U$. *This means that* σ *is of the form*

$$\sigma(x) = \tau\rho(x) + Tr(xy_0),$$

where $\rho : \mathcal{V}_n \to U$ *is an onto linear mapping chosen according to the previous lemma and* τ *is an arbitrary nonaffine function on* U. *Then* (σ, ϕ, γ) *is a bent*

triple. The explicit definition of the corresponding bent function is:

$$f(x, y^d) = \begin{cases} \tau\rho\left(\frac{x}{y} + y^{d'-1}\right) + Tr\left((\frac{x}{y} + y^{d'-1})y_0\right) & if \quad y \neq 0, \\ 0 & otherwise. \end{cases}$$

This class is a generalization of $\mathcal{PS}_{ap}$. Dobbertin denotes this class by $\mathcal{N}$. He proved that class $\mathcal{N}$ is not contained in $\mathcal{M}^{\#}$ [7].

4.6 Constructions of Bent Functions from Two Known Bent Functions

If we are given two bent functions, we can construct another bent function of higher dimension. The results of this sections can be found in [18].

Definition 4.6.1. We call the sequence of a function a bent sequence if the function is bent. A sequence is called an affine sequence (a linear sequence) if it is the sequence of an affine function (a linear function).

Definition 4.6.2. We call a $(1, -1)$ matrix of order $2^m \times 2^n$ a bent type matrix if each row is a bent sequence of length 2^n and each column is a bent sequence of length 2^m.

Definition 4.6.3. We call a $(1, -1)$ matrix of order $2^m \times 2^n$ an affine type matrix if each row is an affine sequence of length 2^n and each column is an affine sequence of length 2^m.

Definition 4.6.4. Let A_1 and A_2 be affine type matrices of order $2^m \times 2^n$. If $A_2 = QA_1P$ where Q and P are diagonal matrices of order 2^m and 2^n whose diagonals consist of ± 1, we say A_1 and A_2 are equivalent.

Lemma 4.6.5. *([18]) Let $b_0, b_1, \cdots, b_{2^n-1}$ be a bent sequence and $c_0, c_1, \cdots, c_{2^n-1}$ be an affine sequence. Then $b_0c_0, b_1c_1, \cdots, b_{2^n-1}c_{2^n-1}$ is a bent sequence.*

Theorem 4.6.6. *([18])*

Let $B = (b_{ij})$ be a bent type matrix of order $2^m \times 2^n$. Write

$$\beta_j = (b_{1j}, \cdots, b_{2^m j}),\ j = 1, 2, \cdots, 2^n \text{ and}$$

$$\alpha_i = (b_{i1}, \cdots, b_{i2^n}),\ i = 1, 2, \cdots, 2^m$$

Then both

$$(2^{-\frac{1}{2}m}\beta_1 H_m, \cdots, 2^{-\frac{1}{2}m}\beta_{2^n} H_m) \text{ and}$$

$$(2^{-\frac{1}{2}n}\alpha_1 H_n, \cdots, 2^{-\frac{1}{2}n}\alpha_{2^m} H_n)$$

are bent sequences of length $2^m \times 2^n$

Theorem 4.6.7. *([18]) Let A be an affine type matrix of order $2^m \times 2^n$, P be a diagonal matrix of order 2^n whose diagonal is a bent sequence of length 2^n, say $a_0, a_1, \cdots, a_{2^n-1}$ and Q be a diagonal matrix of order 2^m whose diagonal is a bent sequence of length 2^m, say $b_0, b_1, \cdots, b_{2^m-1}$. Then QAP is a bent type matrix of order $2^m \times 2^n$.*

Theorem 4.6.8. *([18]) Let $a_1, a_2, \cdots, a_{2^{2k-1}}$ be the $\beta_0^{th}, \beta_1^{th}, \cdots, \beta_{2^{2k-2}-1}^{th}$ entries of η_1 respectively and let $b_1, b_2, \cdots, b_{2^{2k-1}}$ be the $\beta_{2^{2k-2}+1}^{th}, \beta_{2^{2k-2}+2}^{th}, \cdots, \beta_{2^{2k-1}-1}^{th}$ entries of η_1 respectively.*

Next let the $\beta_0^{th}, \beta_1^{th}, \cdots, \beta_{2^{2k-2}-1}^{th}$ *entries of* η_1 *be* $a_1, a_2, \cdots, a_{2^{2k-1}}$ *respectively and let the* $\beta_{2^{2k-2}+1}^{th}, \beta_{2^{2k-2}+2}^{th}, \cdots, \beta_{2^{2k-1}-1}^{th}$ *entries of* η_1 *be* $-b_1, -b_2, \cdots, -b_{2^{2k-1}}$ *respectively.*

Set $\eta = (\eta_1, \eta_2)$*. Then* η *is a bent sequence of length* 2^{2k}*.*

Theorem 4.6.9. *([18]) Let* $a_1, a_2, \cdots, a_{2^{2k-1}}$ *be the* $\beta_0^{th}, \beta_1^{th}, \cdots, \beta_{2^{2k-2}-1}^{th}$ *entries of* η_1 *respectively and let* $b_1, b_2, \cdots, b_{2^{2k-1}}$ *be the* $\beta_{2^{2k-2}+1}^{th}, \beta_{2^{2k-2}+2}^{th}, \cdots, \beta_{2^{2k-1}-1}^{th}$ *entries of* η_1 *respectively.*

Next let the $\beta_0^{th}, \beta_1^{th}, \cdots, \beta_{2^{2k-2}-1}^{th}$ *entries of* η_1 *be* $-a_1, -a_2, \cdots, -a_{2^{2k-1}}$ *respectively and let the* $\beta_{2^{2k-2}+1}^{th}, \beta_{2^{2k-2}+2}^{th}, \cdots, \beta_{2^{2k-1}-1}^{th}$ *entries of* η_1 *be* $b_1, b_2, \cdots, b_{2^{2k-1}}$ *respectively.*

Set $\eta = (\eta_1, \eta_2)$*. Then* η *is a bent sequence of length* 2^{2k}*.*

Chapter 5

Normal Bent Functions

Normality is first introduced by Dobbertin [8]. Bent functions, we have studied until here are all normal functions and Dobbertin proposed the conjecture that any normal bent function is normal. But then some examples of non-normal bent functions are given using a specific algorithm. It is still an open problem to find an infinite class of non-normal bent functions.

5.1 Introduction of Normality

Definition 5.1.1. ([4]) A function $f \in \mathcal{F}_n$ is said to be normal when it is constant on an affine subspace U of $\mathcal{F}_n$ of dimension $\lceil n/2 \rceil$ where $\lceil n/2 \rceil$ is equal to $n/2$ for even n and to $(n+1)/2$ for odd n. In this case f is said to be normal with respect to U. The function f is said weakly normal when it is affine, and not constant, on a flat U of dimension $\lceil n/2 \rceil$.

The normality is connected with the problem of the determination of the highest dimension of the affine space where f is constant.

Definition 5.1.2. ([4]) A function $f \in \mathcal{F}_n$ is said to be k-normal, $k \leq m$ if there exists a k-dimensional flat on which f is constant. The function f is said weakly k-normal if it is affine, and not constant, on some k-dimensional flat.

Theorem 5.1.3. *([4]) Let $f \in \mathcal{F}_n$. Then f is k-normal with respect to U if and only if there is $v \in \mathcal{F}_n$ such that $f + \varphi_v$ is affine on U where φ_v denotes a linear function in $\mathcal{F}_n$, that is $\varphi_v : x \in \mathcal{F}_n \longmapsto v \cdot x$. When $v \notin V^{\perp}$, where V denotes the subspace which has U as a coset, then $f + \varphi_v$ is affine and not constant on U.*

Example 5.1.4. Let $f \in \mathcal{F}_8$ given by

$$f(x) = x_1x_2x_3x_4 + x_2x_4x_8 + x_1x_3 + x_5x_6 + x_6x_7 + x_7x_8.$$

Let U be a subspace of dimension 4, defined by $x_1 = x_4 = x_5 = x_7 = 0$. Since each term of f contains at least one $x_i, i \in 1, 4, 5, 7$, $f(0, x_2, x_3, 0, 0, x_6, 0, x_8) = 0$ for all x. Then f is normal with respect to U.

We see an obvious property here. If

$$f(x_1, \ldots, x_m) = x_1A_1 + \cdots + x_tA_t$$

where $t = n/2$ for even n and $t = (n-1)/2$ for odd n and each A_i denotes the function of $n-1$ variables $\{x_j | 1 \leq j \leq n, j \neq i\}$. Then f is normal with respect to U, the subspace defined by $x_1 = \cdots = x_t = 0$.

We obtain a general result easily.

Theorem 5.1.5. *([4]) Let k be an integer and $1 \leq k \leq n$ and let $f \in \mathcal{F}_n$ given by,*

$$f(x_1, \cdots, x_n) = \sum_{u \in \mathcal{F}_n, w(u) > k} \lambda_u \left(\prod_{i=1}^{n} x_i^{u_i} \right), \ \lambda_u \in \{0, 1\}$$

Then f is k-normal, equal to zero, with respect to any subspace U defined by

$$x_{i_1} = \cdots = x_{i_{n-k}} = 0;\ 1 \leq i_j \leq n.$$

Proof: Each term of f is of degree strictly greater than k. So each term is zero. □

It is known that for $n \geq 4$ any function is 2-normal and for $n \geq 6$ any function is 3-normal [4]. This result is based on Dubuc's [9] theorem.

Theorem 5.1.6. *([9]) For $n \leq 7$, any function of n variables is $\lfloor n/2 \rfloor$ -normal.*

5.2 Normal Bent Functions

Theorem 5.2.1. *([4]) Let $n = 2t$ and assume that $f \in \mathcal{F}_n$ is bent. We denote by V any subspace of dimension t. Then we have:*

1. *f is normal with respect to V if and only if its dual function $\tilde{f}$ is normal with respect to $V^\perp$;*

2. *f is normal with respect to $a + V$, $a \notin V$ if and only if $\tilde{f} + \varphi_a$ is normal with respect to $V^\perp$;*

3. *f is normal with respect to $a + V$, $a \notin V$ if and only if $\tilde{f}$ is weakly normal with respect to $V^\perp$.*

The previous theorem is important because it leads to an improvement when we want to check if any bent function is normal.

Corollary 5.2.2. *([4]) Let $f \in \mathcal{F}_n$, $n = 2t$, be a bent function and let $\tilde{f}$ be its dual. Let V be a subspace of dimension t. Then f is not normal with respect to*

any coset of V if and only if $\tilde{f}$ is neither normal nor weakly normal with respect to $V^{\perp}$.

Theorem 5.2.3. *([4]) Any cubic function of 8 variables is normal.*

If there exists non-normal bent functions of 8 variables the degree should be greater than 3. But since maximum degree of bent functions of 8 variables is 4, the degree should be equal to 4. It is still an open problem whether there exists non-normal bent bunctions of 8 variables and degree 4 or not. It is known that there exists non-normal bent functions of 10 variables [1]. Canteut [1] presented a class of weakly non-normal class of bent functions of 14 variables.

Chapter 6

Generalized Bent Functions

6.1 Introduction

All definitions in this thesis considers binary bent functions but sometimes it may be useful to study generalized bent functions. The general theory of the bent functions from Z_q^n to Z_q is developed by Kumar, Scholtz and Welch [11]. Then, generalized bent functions are studied by Nyberg [15].

6.2 Basic Definitions

Let q be a positive integer and Z_q denote the set of integers modulo q. Let

$$u = e^{i\frac{2\pi}{q}}$$

be the q^{th} root of unity in $\mathbb{C}$, where $i = \sqrt{-1}$ and $\mathbb{C}$ denotes the set of complex numbers. Let f be a function from the set Z_q^n of n-tuples of integers modulo q to Z_q.

Definition 6.2.1. The Walsh Transform of u^f is defined as follows:

$$F(w) = \frac{1}{\sqrt{q^n}} \sum u^{f(x)-w\cdot x}, w \in Z_q^n.$$

Definition 6.2.2. A function $f : Z_q^n \to Z^q$ is bent if $|F(w)| = 1$ for all $w \in Z_q^n$.

Definition 6.2.3. Let f be a function mapping from Z_q^n into Z_q. For each pair of elements Z in Z_q^n and C in Z_q, the function $f_{Z,C}$ given by

$$f_{Z,C}(X) = f(X) + Z \cdot X + C, \ for\ all\ X \in Z_q^n$$

with the arithmetic being in modulo q, is called an affine ($C \neq 0$) or linear ($C = 0, Z \neq 0$) translate of f.

Definition 6.2.4. A $n \times n$ matrix H whose entries are integral powers of a complex primitive n^{th} root of unity and which satisfies

$$HH^* = nI$$

is called a generalized Hadamard matrix.

Definition 6.2.5. f is called a regular bent function if the Walsh transform F of u^f can be expressed in the form

$$F(\lambda) = w^{g(\lambda)}, \ for\ all\ \lambda \in Z_q^n,$$

for some function mapping Z_q^n into Z_q.

6.3 Properties

All of the properties given in this section can be found in [11].

1. Every affine or linear translate of a bent function is also bent.

2. A bent function remains bent under a linear or affine transformation in coordinates.

3. If f and g are bent functions over Z_q^m and Z_q^n respectively, the function $f+g$ over Z_q^{m+n} defined by $(f+g)(x_1, x_2, \cdots, x_{m+n}) = f(x_1, x_2, \cdots, x_m) + g(x_{m+1}, x_{m+2}, \cdots, x_{m+n})$, for all $(x_1, x_2, \cdots, x_{m+n}) \in Z_q^{m+n}$ is a bent function.

4. A function f with values in Z^q is bent if and only if the matrix H whose $(x, y)^{th}$ entry is $w^{f(x-y)}$ is a generalized Hadamard matrix.

5. If f is a bent function defined on Z_q^n, the Walsh coefficients of γ^f have unit magnitude for every choice of complex primitive q^{th} root γ of unity.

6. Let n be odd $q \equiv 2(mod 4)$. In addition, let q satisfy either of the following two conditions:

   - q=2
   - $q \neq 2$ but such that there exists and integer b satisfying

   $$2^b = -1(mod \frac{q}{2})$$

   Then bent functions over Z_q^n do not exist.

7. Let f be a bent function over Z_q^n and let q and n satisfies any one of the following conditions:

   - $q = p^k$, p prime, $q \neq 2$,

- $q = \prod_{i=1}^{r} p_i^{k_i}$, $r > 1$, p_i prime all $i, (i = 1, 2, \cdots, r)$ with the primes p_i being such that for each integer $i, (i = 1, 2, \cdots, r)$ there exists an integer f_i for which

$$p_i^{f_i} = -1(mod \frac{q}{p_i^{k_i}})$$

Then each Walsh coefficient $F(\lambda), \lambda \in Z_q^n$ of w^f is a root of unity.

8. Let $w = e^{i\frac{2\pi}{q}}, \gamma = e^{i\frac{2\pi}{2q}}$ and $\delta = e^{i\frac{2\pi}{4q}}$. Let $\lambda \in Z_q^n$ be fixed and let f be a bent function over Z_q^n whose Walsh coefficient $F(\lambda)$ is a root of unity. Then $F(\lambda)$ is of the form

   - $F(\lambda) = \omega^k$, if both m and q are even,
   - $= \gamma^k$, if m is even but q is odd,
   - $= \omega^k$, if m is odd and $q = 0 \pmod 4$,
   - $= \gamma^k$, if m is odd and $q = 1 \pmod 4$,
   - $= \delta^{2k+1}$, if m is odd and $q = 2 \pmod 4$,
   - $= \delta^{2k+1}$, if m is odd and $q = 3 \pmod 4$,

   for some integer k.

9. Let f be a regular bent function defined on Z_q^n having Walsh transform F. Let g be the function given by

$$F(\lambda) = w^{g(\lambda)}, forall \lambda \in Z_q^n,$$

Then g is also a regular bent function over Z_q^n

6.4 Constructions

In this section constructions for bent functions over Z_q^n for every possible value of q and n excepting the case when n is odd and $q = 2(mod4)$ are given.

Theorem 6.4.1. *([11]) Let q and k be arbitrary positive integers. Set $n = 2k$. Then the function f over Z_q^n given by*

$$f(x) = x_2 \cdot \pi(x_1) + g(x_1) \tag{6.4.1}$$

where $x_1, x_2 \in Z_q^n$ are defined by

$$x = [x_1, x_2]$$

and π is an arbitrary permutation of the elements of Z_q^k and g is an arbitrary function mapping from Z_q^k into Z_q, is bent.

Proof: ([11]) The Walsh Transform F of w^f is given by

$$F(\lambda) = \frac{1}{q^k} \sum_{x \in Z_q^n} w^{f(x) - \lambda \cdot x} \tag{6.4.2}$$

Let $\lambda \in Z_q^n$ be fixed and $\lambda_1, \lambda_1 \in Z_q^k$ be defined by

$$\lambda = [\lambda_1, \lambda_2]. \tag{6.4.3}$$

Replacing the sum over x in equation 6.4.2 with the sums over components x_1, x_2 of x and substituting the expressions for $f(\cdot)$ and λ contained in equation 6.4.2

and equation 6.4.3, one obtains

$$F(\lambda) = \frac{1}{q^k} \sum_{x_1 \in Z_q^k} \omega^{g(x_1) - \lambda_1 \cdot x_1} \sum_{x_2 \in Z_q^k} \omega^{x_2 \cdot (\pi(x_1) - \lambda_2)}$$

The inner sum vanishes unless $\pi(x_1) = \lambda(2)$ or equivalently unless

$$x_1 = \pi^{-1}(\lambda_2),$$

and therefore

$$F(\lambda) = w^{g(\pi^{-1}(\lambda_2)) - \lambda_1 \cdot \pi^{-1}(\lambda_2)}$$

so that

$$|F(\lambda)| = 1.$$

Since λ is chosen arbitrarily, f is bent. □

Theorem 6.4.2. *([11]) Let q be odd. Then the function f over Z_q defined by*

$$f(k) = k^2 + ck$$

is bent for all c in Z_q.

Definition 6.4.3. $Z_q^{1,t} = \{k \in Z^q \,|0 \leq k \leq t-1\}$.

Theorem 6.4.4. *([11]) Let q be a perfect square and r be defined by $q = r^2$.*

Then the function f over Z_q given by

$$f(k) = r \cdot k_1\pi(k_2) + g(k_2)$$

where $k_1, k_2 \in Z_q^{1,r}$ are defined by

$$k = rk_1 + k_2,$$

and π is an arbitrary permutation of the elements of $Z_q^{1,r}$ and g is an arbitrary integer-valued function defined on $Z_q^{1,r}$, is bent.

Theorem 6.4.5. *([11]) Let $q = 2^{2k+1}, k > 0$. Let the function h mapping the integers 0,1 into $Z_q^{1,8}$, be given by*

$$h(z) = c4z + 2z, z \in 0, 1$$

where c is either 0 or 1. Let the function f over Z_q be defined by

$$f(x) = g(y_1) + y_1x + \frac{q}{8}h(x_k)$$

where $x_j, j = 0, 1, 2, \cdots 2k$ are digits in the binary representation of x, that is

$$x = \sum_{j=0}^{2k} x_j 2^j;$$

y_1, y_2 and y_3 are the partial sums,

$$y_1 = \sum_{j=0}^{k-1} x_j 2^j,\ y_2 = x_k 2^k \text{ and } y_3 = \sum_{j=k+1}^{2k} x_j 2^j$$

and g is an arbitrary integer-valued function defined on Z_q. Then f is bent.

Chapter 7

Conclusion

In this thesis we investigated bent functions from the cryptographic view. We presented the most important properties of bent functions. We include the proofs of important properties and theorems. We also gave examples.

We presented the most important construction methods of bent functions. Although there exists some other construction methods, we have not considered them since they mostly do not lead to new classes.

We cover normal bent functions since Dobbertin [8] uses such functions to achieve highly nonlinear balanced functions. These functions are very important in cryptography.

In cryptography we focus on binary functions. But there is a general theory of bent functions introduced by Kumar, Scholtz and Welch [11]. We include this study in the thesis, for completeness.

References

[1] Canteut A., Daum M., Leander G., Dobbertin H., *Normal and nonnormal bent functions*, In Proceedings of the 2003 International Workshop on Coding and Cryptography (WCC 2003), 91100 (2003).

[2] Carlet C., *Two new classes of bent functions*, EUROCRYPT'94, Lecture Notes in Computer Science 765.(1994).

[3] Carlet C., *A construction of bent functions*, Conference on Finite Fields and Applications (1996).

[4] Charpin P., *Normal boolean functions*, Journal of Complexity 20: 245-265 (2004).

[5] Dillon J.F., *A survey of bent functions*, The NSA Technical Journal, unclassified, 191-215 (1972).

[6] Dillon J.F., *Elementary hadamard difference sets*, Ph. D. Thesis, University of Maryland (1974).

[7] Dobbertin H., *Construction of bent functions and balanced Boolean functions with high nonlinearity*, Fast Software Encryption (Workshop on Cryptographic Algorithms, Leuven 1994), Lecture Notes in Computer Science, vol. 1008: 61-740, Springer-Verlag, (1995).

[8] Dobbertin H., Leander G., *Crypographer's toolkit for construction of 8-bit bent functions*, (2005).

[9] Dubuc S., *Etude des proprietes de degenerescence et de normalite des fonctions booleennes et construction de fonctions q-aries parfaitement non-linearies*, PH.D. Thesis, Universite de Caen (2001).

[10] Hou X.D., *Cubic Bent Functions*, Discrete Mathematics, 189: 149-161 (1998).

[11] Kumar P.V., Scholtz R.A., Welch L.R., *Generalized bent functions and their properties*, Journal of Combinatorial Theory, Ser. A, 40: 90-107 (1985).

[12] Matsui M., *Linear cryptanalysis method for des cipher*, EUROCRYPT'93, Lecture Notes in Computer Science 765, 386397 (1994).

[13] McFarland R. *A family of noncyclic difference sets*, Journal of Combinatorial Theory, Ser. A, 15: 541542 (1965).

[14] Mac Williams F.J., Sloane N.J.A., *The theory of error correcting codes*, North Holland (1977).

[15] Nyberg K., *Construction of bent functions and difference sets*, EUROCRYPT'90, Lecture Notes in Computer Science 473, 151-160 (1991).

[16] Rothaus O.S., *On "bent" functions*, Journal of Combinatorial Theory, Ser. A, 20: 300-305 (1976).

[17] Sağdıçoğlu S., *Cryptological viewpoint of boolean functions*, M. Sc. Thesis, The Department of Mathematics, Middle East Technical University, Ankara, Turkey, (2003).

[18] Seberry J., Zhang X., *Construction of bent functions from two known bent functions*, Australasian Journal of Combinatorics, 9: 21-35, (1994).

[19] Sertkaya İ., *Nonlinearity preserving post-transformations*, Insttute of Applied Mathematics, Middle East Technical University, Ankara, Turkey, (2004).