DIVISIBILITY RESULTS ON BOOLEAN FUNCTIONS USING THE NUMERICAL NORMAL FORM

FARUK GÖLOĞLU

SEPTEMBER 2004

DIVISIBILITY RESULTS ON BOOLEAN FUNCTIONS USING THE NUMERICAL NORMAL FORM

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

BY

FARUK GÖLOĞLU

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

SEPTEMBER 2004

Approval of the Graduate School of Applied Mathematics

_____

Prof. Dr. Aydın AYTUNA
Director

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

_____

Prof. Dr. Ersan AKYILDIZ
Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

_____

Assoc. Prof. Dr. Melek D. YÜCEL
Supervisor

Examining Committee Members

Prof. Dr. Ersan AKYILDIZ _____

Assoc. Prof. Dr. Ali DOĞANAKSOY _____

Prof. Dr. Kemal LEBLEBİCİOĞLU _____

Assoc. Prof. Dr. Ferruh ÖZBUDAK _____

Assoc. Prof. Dr. Melek D. YÜCEL _____

ABSTRACT

DIVISIBILITY RESULTS ON BOOLEAN FUNCTIONS USING THE NUMERICAL NORMAL FORM

GÖLOĞLU, Faruk
M.Sc., Department of Cryptography
Supervisor: Assoc. Prof. Dr. Melek D. YÜCEL

September 2004, 53 pages

A Boolean function can be represented in several different forms. These different representation have advantages and disadvantages of their own. The Algebraic Normal Form, truth table, and Walsh spectrum representations are widely studied in literature. In 1999, Claude Carlet and Phillippe Guillot introduced the Numerical Normal Form. Numerical Normal Form (NNF) of a Boolean function is similar to Algebraic Normal Form, with integer coefficients instead of coefficients from the two element field. Using NNF representation, just like the Walsh spectrum, characterization of several cryptographically important functions, such as resilient and bent functions, is possible. In 2002, Carlet had shown several divisibility results concerning resilient and correlation-immune functions using NNF. With these divisibility results, Carlet is able to give bounds concerning nonlinearity of resilient and correlation immune functions.

In this thesis, following Carlet and Guillot, we introduce the Numerical Normal Form and derive the pairwise relations between the mentioned representations. Characterization of Boolean, resilient and bent functions using NNF is also given. We then review the divisibility results of Carlet, which will be linked to some results on the nonlinearity of resilient and correlation immune functions.

We show the Möbius inversion properties of NNF of a Boolean function, using Gian-Carlo Rota's work as a guide. Finally, using a lot of the mentioned results, we

prove a necessary condition on the Walsh spectrum of Boolean functions with given degree.

Keywords: Cryptography, Boolean functions, Numerical Normal Form, Walsh spectrum, Balance, Resilience, Correlation-Immunity, Nonlinearity, Bent functions, Möbius inversion.

Öz

SAYISAL NORMAL BİÇİM KULLANILARAK BULUNAN BOOLE FONKSİYONLARINA İLİŞKİN BÖLÜNEBİLİRLİK SONUÇLARI

GÖLOĞLU, Faruk
Yüksek Lisans, Kriptografi Bölümü
Tez Yöneticisi: Doç. Dr. Melek D. YÜCEL

Eylül 2004, 53 sayfa

Boole fonksiyonları çeşitli biçimlerde gösterilebilir. Bu değişik gösterimlerin birbirlerine göre olumlu ve olumsuz yanları vardır. Cebirsel Normal Biçim, doğruluk tablosu ve Walsh tayfı gösterimleri, üzerinde geniş çalışılmış ve hayli bilinen gösterimlerdir. 1999 yılında, Claude Carlet ve Philippe Guillot tarafından Sayısal Normal Biçim geliştirildi. Sayısal Normal Biçim, Cebirsel Normal Biçime benzemekle birlikte, iki elemanlı Galois cisiminden katsayılar yerine tamsayı katsayılar kullanılarak oluşturulmuştur. Walsh tayfında olduğu gibi, Sayısal Normal Biçim gösterimi kullanılarak, bükük ve dayanıklı fonksiyonlar gibi kriptolojik açıdan önemli fonksiyonlar karakterize edilebilir. 2002 yılında, Carlet tarafından dayanıklı ve ilintiye-bağışık fonksiyonlara ilişkin bölünebilirlik sonuçları ispatlandı. Ayrıca yine Carlet tarafından, bu sonuçlara dayanan, dayanıklı ve ilintiye-bağışık fonksiyonlar için eğrisellik sınırları bulundu.

Bu tezde, Carlet ve Guillot'nun yolundan gidilerek Sayısal Normal Biçim tanıtılıp, bahsi geçen gösterimler arasındaki dönüşümler gösterilmiş; Boole fonksiyonlarının, dayanıklı ve bükük fonsiyonların karakterizasyonu verilmiştir. Carlet'nin bulduğu bölünebilirlik sonuçları tekrarlanıp, bu sonuçlar dayanıklı ve ilintiye-bağışık fonksiyonların eğriselliklerıyle ilişkilendirilmiştir.

Gian-Carlo Rota'nın çalışması esas alınarak Boole fonksiyonlarının Möbius tersdönüşüm özellikleri gösterilmiştir. Son olarak bahsi geçen birçok sonuç kullanılarak

cebirsel derecesi bilinen Boole fonksiyonlarının Walsh tayfıyla ilgili bir gerekli koşul ispatlanmıştır.

Anahtar Kelimeler: Kriptografi, Boole fonksiyonları, Sayısal Normal Biçim, Walsh tayfı, Denge, Dayanıklılık, İlintiye-bağışıklılık, Doğrusallık, Bükük fonksiyonlar, Möbius ters-dönüşüm.

ACKNOWLEDGMENTS

I wish to express deep and warm gratitude to my supervisor Assoc. Prof. Dr. Melek D. Yücel. Without her guidance, motivation and encouragements; this work would not have been possible.

I would like to acknowledge the debt I owe to Assoc. Prof. Dr. Ali Doğanaksoy and Assoc. Prof. Dr. Ferruh Özbudak. Through my years at the Institute of Applied Mathematics, I have learned a lot from them.

I would like to thank to all of the people at the institute for their kindness and support.

I also would like to thank to my colleagues at Bilkent University for their friendship.

Last but not least, I would like to thank to my family. I cannot express enough gratitude to them; for their limitless support, love and belief.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

The Numerical Normal Form (NNF) has been introduced by Claude Carlet and Philippe Guillot [3] in 1999. Divisibility properties of NNF coefficients lead to some important consequences concerning the nonlinearity of resilient functions. The aim of this thesis is to review the works of Carlet and Guillot ([3],[4],[2]). NNF can be seen as Möbius inversion in the partially ordered set $\mathbb{F}_2^n$. We investigate this property using the work of Gian-Carlo Rota [10]. We also make some original contributions in Section 4.3.

In Chapter 2, we introduce the notation and conventions that are used throughout the work. Furthermore, we will recall several basic facts on Boolean functions and cryptography. Chapter 2 does not intend to give all the background necessary for this work, instead it gives the material in a logical order for self completeness. The concepts we will deal with in Chapter 2 includes several cryptographically important criteria such as resiliency, correlation immunity, bentness, nonlinearity and balance of Boolean functions; several important tools that are necessary for any kind of treatment, such as Walsh transform, Hamming weight and distance, sign function, *etc.* Chapter 2 also includes a section devoted to the ordering relations in $\mathbb{F}_2^n$, which is required throughout the text.

Chapter 3 is devoted to the Numerical Normal Form of Boolean functions introduced by Carlet and Guillot [3]. The chapter begins with an introduction to several

representations of Boolean functions that are widely used, namely the truth table, the Algebraic Normal Form and the Walsh spectrum. Their advantages and drawbacks are given. Section 3.3 introduces the Numerical Normal Form as it is given in [3]. Conversion formulae between several representations are presented [3]. Then characterization of several cryptographically important functions, such as resilient and bent functions, are given ([2], [4]). The relation between the Numerical Normal Form and truth table is an example of Möbius inversion in a Partially Ordered Set. Finally, in Section 3.4 we prove the Möbius inversion properties of NNF, with the help from the work of Gian-Carlo Rota [10].

Divisibility results are valuable intermediate results which can directly be linked to important consequences concerning, for instance, Walsh spectrum of Boolean functions. In Chapter 4, the divisibility results on resilient and correlation immune functions using NNF coefficients are summarized [2]. In Section 4.2, nonlinearity bounds for resilient functions are given [2] using the divisibility results given in Section 4.1. Section 4.3 is devoted to some consequences. In Section 4.3, we prove a necessary condition for Walsh spectrum coefficients of a Boolean function.

Throughout the work we will cite every lemma, proposition, theorem and proof, whenever we have little or no contribution.

CHAPTER 2

NOTATION AND CONVENTIONS

2.1 Introduction

In this chapter we introduce the notation and the conventions used throughout the work. In the first section, we review the definitions of some important terms widely used in cryptography; such as balance, resiliency, bentness, *etc.* We show some basic properties of $\mathbb{F}_2^n$, the basic vector space where all our functions are defined.

2.2 Definitions

The Hamming weight of a vector and Hamming distance between two vectors are defined as follows.

Definition 2.2.1. Let $a = (a_1, a_2, \ldots, a_n) \in \mathbb{F}_2^n$. Then *Hamming weight* of a is given as:

$$\mathrm{wt}(a) = |\{1 \leq i \leq n \mid a_i = 1\}|$$

We should make the distinction between addition in $\mathbb{F}_2$ and addition in $\mathbb{Z}$. We will use ordinary addition sign, $+$, for addition in $\mathbb{Z}$, and the so-called XOR sign, $\oplus$,

for addition in $\mathbb{F}_2$. There is no ambiguity for vector addition in $\mathbb{F}_2^n$, however we will use the + sign for component-wise addition of two $\mathbb{F}_2^n$ vectors.

Definition 2.2.2. Let $a = (a_1, a_2, \ldots, a_n),\ b = (b_1, b_2, \ldots, b_n) \in \mathbb{F}_2^n$. The *Hamming distance* between a and b is given as:

$$d_H(a,b) = \mathrm{wt}(a+b) = |\{1 \le i \le n \mid a_i \oplus b_i = 1\}|$$

The inner product of two vectors $u = (u_1, \ldots, u_n), v = (v_1, \ldots, v_n) \in \mathbb{F}_2^n$ will be shown

$$u \cdot v = u_1 v_1 \oplus \cdots \oplus u_n v_n$$

Definition 2.2.3. A *Boolean function* is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$.

Weight of a Boolean function f, $\mathrm{wt}(f)$, is the number of elements $a \in \mathbb{F}_2^n$ for which $f(a) = 1$:

$$\mathrm{wt}(f) = \sum_{a \in \mathbb{F}_2^n} f(a)$$

A function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is *balanced* if $\mathrm{wt}(f) = 2^{n-1}$. Balancedness is a highly important criterion since, to be cryptographically useful, the output of the function should not give any information. An important class of Boolean functions is the class of *affine functions*.

Definition 2.2.4. An *affine function* is a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ of the form

$$f(x) = a \cdot x \oplus \epsilon$$

where $a \in \mathbb{F}_2^n$ and $\epsilon \in \mathbb{F}_2$.

A *linear function* is an affine function with $\epsilon = 0$.

We sometimes need to consider the same function f, with the range $\{-1,+1\}$. This can be done by the following *sign*[1] function.

$$\hat{f}(x) = (-1)^{f(x)} = 1 - 2f(x)$$

Walsh transform defined below is an important tool for studying Boolean functions.

Definition 2.2.5. Walsh transform of f, $W_f : \mathbb{F}_2^n \to \mathbb{Z}$ is defined as:

$$W_f(a) = \sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{a \cdot x} \tag{2.2.1}$$

Remark 2.2.6. Walsh transform of $\hat{f}$ is widely used:

$$W_{\hat{f}}(a) = \sum_{x \in \mathbb{F}_2^n} \hat{f}(x)(-1)^{a \cdot x} = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus a \cdot x} \tag{2.2.2}$$

Walsh transform is directly related to the distance of a Boolean function to affine functions.

Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$, and $l(x) = a \cdot x \oplus \epsilon$, where $a \in \mathbb{F}_2^n$ and $\epsilon \in \mathbb{F}_2$ be an affine function. Then

$$d_H(f, l) = 2^{n-1} - \frac{(-1)^{\epsilon}}{2} W_{\hat{f}}(a) \tag{2.2.3}$$

We may call $(-1)^{\epsilon} W_{\hat{f}}(a)$, the *Walsh distance* of f to l.

When n is even, there exists some functions called *bent* functions, which are

[1] The sign function differs from the signum function, which is defined as:

$$\text{signum}(x) = \begin{cases} -1 & when\ x < 0 \\ 0 & when\ x = 0 \\ 1 & when\ x > 0 \end{cases}$$

at highest distance to affine functions. Bent functions ([9],[5],[11]) are at the same Hamming distance to all affine functions. They can be characterized with the help of the Walsh transform as follows.

Definition 2.2.7. A Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is called *bent* if:

$$W_{\hat{f}}(a) = \pm 2^{\frac{n}{2}}$$

for all $a \in \mathbb{F}_2^n$.

Some main open problems in cryptography and coding theory are related with bent functions. In the literature, another name of bent functions is "perfect nonlinear functions", as the following definition of nonlinearity implies.

Definition 2.2.8. Nonlinearity of f, $nl(f)$, is the minimum distance of f to affine functions, which is:

$$nl(f) = 2^{n-1} - \max_{a \in \mathbb{F}_2^n} \{|W_{\hat{f}}(a)|\}$$

$nl(f)$ reaches its maximum value if and only if f is bent. Nonlinearity of affine functions is 0.

Nonlinearity of the function is important for use in both stream and block ciphers. Carlet [2] signifies the importance of nonlinearity in stream ciphers: "...existence of a "good" approximation of f by an affine function makes fast correlation attacks possible".

In addition to balancedness and nonlinearity, there exist other important cryptographic criteria. In this thesis we are interested in *correlation immune* and *resilient* functions.

To be cryptographically useful, the output of the function should be changed

with equal probability, when we fix some of the input variables [3]. This is the idea behind *correlation immunity* [12]. A function f is called *m-th order correlation immune* if f satisfies this property when m of the input variables are fixed. We call a balanced m-th order correlation immune function an *m-resilient function*. Following characterization is given in [13].

Definition 2.2.9. Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$. Let $1 \leq m < n$. f is m-th order correlation immune if

$$W_f(a) = 0$$

for all a such that $1 \leq \mathrm{wt}(a) \leq m$.

Remark 2.2.10. Observe that $W_f(a) = 0 \iff W_{\hat{f}}(a) = 0$, if $\mathrm{wt}(a) \neq 0$.

Definition 2.2.11. f is m-resilient if

- f is m-th order correlation immune, and
- f is balanced.

2.3 Vectors and Ordering

Let $v \in \mathbb{F}_2^n$ be represented as $(v_1, \ldots, v_n)$. The support I_v of v is the set of indices of v which are nonzero (*i.e.* 1):

$$I_v = \{i \mid v_i \neq 0,\ 1 \leq i \leq n\}$$

We say $u \preceq v$ if $I_u \subseteq I_v$. Complement $\bar{u}$ of u has support $I_{\bar{u}} = I_{\mathbf{1}} - I_u$, where $\mathbf{1}$ denotes the all-one vector in $\mathbb{F}_2^n$. Furthermore $u \preceq v \iff \bar{v} \preceq \bar{u}$.

The following proposition is given in [3] without proof.

Proposition 2.3.1. *[3] Let $a, u \in \mathbb{F}_2^n$,*

$$\sum_{x \in \mathbb{F}_2^n \mid x \preceq u} (-1)^{a \cdot x} = \begin{cases} 2^{\mathrm{wt}(u)} & a \preceq \bar{u} \\ 0 & \textit{otherwise} \end{cases}$$

Proof:

$$\sum_{x \in \mathbb{F}_2^n \mid x \preceq u} (-1)^{a \cdot x} = \sum_{x \in \mathbb{F}_2^n \mid x \preceq u} (1 - 2a \cdot x) = \sum_{x \in \mathbb{F}_2^n \mid x \preceq u} 1 - 2 \sum_{x \in \mathbb{F}_2^n \mid x \preceq u} a \cdot x$$

First let $a \preceq \bar{u}$. Since $a \preceq \bar{u}$ and $x \preceq u$, $I_a \cap I_x = \emptyset$, hence $a \cdot x = 0$.

$$\sum_{x \in \mathbb{F}_2^n \mid x \preceq u} (-1)^{a \cdot x} = 2^{\mathrm{wt}(u)} - 2 \sum_{x \in \mathbb{F}_2^n \mid x \preceq u} a \cdot x = 2^{\mathrm{wt}(u)}$$

Now let $a \not\preceq \bar{u}$. Since $I_a \cap I_x \neq \emptyset$, and $|\{I_x \in \mathscr{P}(I_u) \mid |I_x \cap I_a| \textit{ is odd}\}| = 2^{\mathrm{wt}(u)-1}$,

$$\sum_{x \in \mathbb{F}_2^n \mid x \preceq u} a \cdot x = 2^{\mathrm{wt}(u)-1}$$

where $\mathscr{P}(A)$ is the power-set of A. And,

$$2^{\mathrm{wt}(u)} - 2 \sum_{x \in \mathbb{F}_2^n \mid x \preceq u} a \cdot x = 0$$

This completes the proof. □

CHAPTER 3

THE NUMERICAL NORMAL FORM OF BOOLEAN FUNCTIONS

3.1 Introduction

In this chapter, a survey on several representations of Boolean functions is given. The well known representations are truth table, Algebraic Normal Form and Walsh spectrum representations of Boolean functions. Claude Carlet and Philippe Guillot introduced (in [3]) the Numerical Normal Form (NNF) of Boolean functions. In this chapter, we define NNF and give its relations with other representations. Characterization of several cryptographically important functions are possible using NNF. In Section 3.3 characterization of Boolean, affine, resilient and bent functions are given. When $\mathbb{F}_2^n$ is viewed as a partially ordered set (POSET), the conversion between these representations have similarities with Möbius inversion functions. In the last section, we give some results given by Gian-Carlo Rota [10], and we show the Möbius inversion relations between the representations used for Boolean functions, which are mentioned by Carlet [4], but not detailed as in Section 3.4.

3.2 Representations of Boolean Functions

3.2.1 Truth Table

A Boolean function f is a function from $\mathbb{F}_2^n$ into $\mathbb{F}_2$. A usual way of representing f, is using a truth table[1]. The *truth table* of f,

$$T_f = (f(w_0), f(w_1), \ldots, f(w_{2^n-1})),$$

is a vector of $\mathbb{F}_2$ elements, listed in some predefined order $w_0 < w_1 < \cdots < w_{2^n-1}$, defined on $\mathbb{F}_2^n$ elements. A mainly used ordering is called *lexicographical ordering*, order of which is the traditional encyclopaedic ordering, where 0 precedes 1. Equivalently, in the lexicographical ordering w_i corresponds to the binary representation of i, for $0 \le i \le 2^n - 1$.

This representation is well known. In [3] several advantages and disadvantages are given. To name a few advantages:

- This *simple* representation requires only 2^n *bits*, when an ordering convention is agreed upon.
- Given a list $\xi = (\xi_1, \ldots, \xi_{2^n})$, of 2^n elements, ξ is truth table of a Boolean function if $\xi_i \in \mathbb{F}_2$, for all ξ_i.
- Weight of f is easily computed by $\mathrm{wt}(f) = \sum_{w \in \mathbb{F}_2^n} f(w)$.

[1] Another type of truth table [1] is an array whose rows are the elements of the support I_f of f:

$$\mathbf{T_f} = \begin{bmatrix} t_1 \\ t_2 \\ \vdots \\ t_k \end{bmatrix}$$

where $t_i \in I_f$.

On the other side, truth table representation gives us little information on the nonlinearity, degree and other cryptographically important properties.

3.2.2 Algebraic Normal Form

Algebraic Normal Form (ANF) is another well known representation. We will use the notation of [3]. Any $f : \mathbb{F}_2^n \to \mathbb{F}_2$ can be represented in the following form:

$$f(x_1, \ldots, x_n) = \bigoplus_{u \in \mathbb{F}_2^n} a_u \left(\prod_{i=1}^{n} x_i^{u_i} \right), \; a_u \in \mathbb{F}_2$$

with unique a_u's found by:

$$a_u = \bigoplus_{x \in \mathbb{F}_2^n \mid x \preceq u} f(x)$$

The *algebraic degree* of f is the degree of (3.2.0). Reed-Muller codes can be defined ([9], Chapter 13) using the above representation.

Definition 3.2.1. [9] The r^{th} order Reed-Muller code $\mathscr{R}(r, n)$ of length $l = 2^n$, for $0 \leq r \leq n$, is the set of all truth table vectors T_f, where $f(v_1, \ldots, v_n)$ is a Boolean function which is a polynomial of degree at most r.

Details of ANF can be found in ([5],[9]).

The intimate relation between Reed-Muller codes and Boolean functions is apparent. $\mathscr{R}(n, n)$ consists of every Boolean function with n variables. $\mathscr{R}(d, n)$ consist of every Boolean function with n variables with degree at most d. To show the degree d functions we may use the notation $\mathscr{R}(d, n) \setminus \mathscr{R}(d-1, n)$.

For example truth tables of affine functions are recognized as the codewords of the first order Reed-Muller code of length 2^n, $\mathscr{R}(1, n)$.

Example 3.2.2. [9] Affine functions of 3 variables, or equally, $\mathscr{R}(1,3)$:

0	0 0 0 0 0 0 0 0
$\mathbf{x_3}$	0 0 0 0 1 1 1 1
$\mathbf{x_2}$	0 0 1 1 0 0 1 1
$\mathbf{x_1}$	0 1 0 1 0 1 0 1
$\mathbf{x_2}+\mathbf{x_3}$	0 0 1 1 1 1 0 0
$\mathbf{x_1}+\mathbf{x_3}$	0 1 0 1 1 0 1 0
$\mathbf{x_1}+\mathbf{x_2}$	0 1 1 0 0 1 1 0
$\mathbf{x_1}+\mathbf{x_2}+\mathbf{x_3}$	0 1 1 0 1 0 0 1
$\mathbf{1}$	1 1 1 1 1 1 1 1
$\mathbf{1}+\mathbf{x_3}$	1 1 1 1 0 0 0 0
$\mathbf{1}+\mathbf{x_2}$	1 1 0 0 1 1 0 0
$\mathbf{1}+\mathbf{x_1}$	1 0 1 0 1 0 1 0
$\mathbf{1}+\mathbf{x_2}+\mathbf{x_3}$	1 1 0 0 0 0 1 1
$\mathbf{1}+\mathbf{x_1}+\mathbf{x_3}$	1 0 1 0 0 1 0 1
$\mathbf{1}+\mathbf{x_1}+\mathbf{x_2}$	1 0 0 1 1 0 0 1
$\mathbf{1}+\mathbf{x_1}+\mathbf{x_2}+\mathbf{x_3}$	1 0 0 1 0 1 1 0

Another way of handling the conversion between ANF and the truth table is by matrix multiplication. We mention the following result without a proof.

Theorem 3.2.3. *[5] Let*

$$T_f = (f(0), f(1), \ldots, f(2^n - 1)),$$

$$A_f = (a_0, a_1, \ldots, a_{2^n-1})$$

be the truth table and ANF representations of a Boolean function f respectively, and integers $0,1,\ldots,2^n-1$ are used as their binary representations. Then $T_f = U_n A_f$ and $A_f = U_n T_f$, where $U_n = \bigotimes^n \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$.

As for the case of truth table representation, 2^n bits are sufficient to store ANF representation of a Boolean function.

A drawback of ANF representation is the hardness of computing weight and the Walsh spectrum directly. On the other hand, the algebraic degree, is apparent with ANF.

3.2.3 Walsh Spectrum

Let us recall the formula (2.2.1):

$$W_f(a) = \sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{a \cdot x}$$

The above transform is called the *Walsh transform of f*. The ordered list of values

$$\mathcal{W}_f = (W_f(0), W_f(1), \ldots, W_f(2^n-1)),$$

is called the Walsh spectrum of f, where $0,1,\ldots,2^n-1$ are used to denote the elements of $\mathbb{F}_2^n$, which correspond to their binary representations.

Recall that the Walsh transform of the sign function $\hat{f}$

$$W_{\hat{f}}(a) = \sum_{x \in \mathbb{F}_2^n} \hat{f}(x)(-1)^{a \cdot x} = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus a \cdot x}$$

is defined by (2.2.2). Similar to the Walsh spectrum of f,

$$\mathcal{W}_{\hat{f}} = (W_{\hat{f}}(0), W_{\hat{f}}(1), \ldots, W_{\hat{f}}(2^n - 1)),$$

will be called the Walsh spectrum of $\hat{f}$ in this study.

The relation between W_f and $W_{\hat{f}}$ is given by:

Theorem 3.2.4. $W_{\hat{f}}(a) = 2^n \delta_0(a) - 2W_f(a)$

Proof:

$$\begin{aligned} W_{\hat{f}}(a) &= \sum_{x \in \mathbb{F}_2^n} \hat{f}(x)(-1)^{a \cdot x} \\ &= \sum_{x \in \mathbb{F}_2^n} \left[1 - 2f(x)\right](-1)^{a \cdot x} \\ &= \sum_{x \in \mathbb{F}_2^n} (-1)^{a \cdot x} - 2 \sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{a \cdot x} \\ &= 2^n \delta(a) - 2W_f(a) \end{aligned}$$

In the last line of the proof, the first term is obtained using Proposition 2.3.1, with $u = 2^n - 1$. □

The Walsh spectrum of f and $\hat{f}$ can be thought as a representation since it uniquely identifies the Boolean function. The following theorem proves this argument (proof is omitted, can be found in [5]).

Theorem 3.2.5. *[5] Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function. Let $W_f : \mathbb{F}_2^n \to \mathbb{R}$ be the Walsh transform of f. Then:*

$$f(x) = 2^{-n} \sum_{a \in \mathbb{F}_2^n} W_f(a)(-1)^{x \cdot a}$$

Let T_f and $\mathcal{W}_f$ be the truth table and Walsh spectrum of f respectively. Then we have:

$T_f = 2^{-n} H_n W_f$ *and* $W_f = H_n T_f$, *where* $H_n = \bigotimes^n \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$.

Walsh spectrum of f as a representation has many advantages [3]:

- Bent functions are easily characterized. f is bent if and only if $W_{\hat{f}}(a) = \pm 2^{\frac{n}{2}}$, for all $a \in \mathbb{F}_2^n$.
- Affine functions are easily charecterized. f is affine if and only if $W_{\hat{f}}(a) = \pm 2^n$, for some fixed a, and $W_{\hat{f}}(u) = 0$, for all $u \neq a$.
- Weight of f is easily calculated by $\mathrm{wt}(f) = W_f(0) = 2^{n-1} - \frac{W_{\hat{f}}(0)}{2}$.

Given a list $\xi = (\xi_0, \ldots, \xi_{2^n-1})$ of 2^n integers, the only known way to deduce that the list corresponds to Walsh spectrum of a Boolean function is to use the Inverse Walsh Transform, which is quite inefficient (requires $\mathcal{O}(n2^n)$ operations [7]). However, the following theorems list some of the necessary conditions for the Walsh spectrum of Boolean functions.

Theorem 3.2.6. *Let* $f : \mathbb{F}_2^n \to \mathbb{F}_2$ *be a Boolean function and* $\hat{f} : \mathbb{F}_2^n \to \{+1, -1\}$ *be its sign function. Let* $\mathcal{W}_{\hat{f}} = (W_{\hat{f}}(0), \ldots, W_{\hat{f}}(2^n - 1))$ *be the Walsh spectrum of* $\hat{f}$. *Then:*

- $W_{\hat{f}}(i) \equiv 0 \pmod 4$, $\forall\, i$ *with* $0 \leq i \leq 2^n - 1$, *if* $\mathrm{wt}(f)$ *is even or,*
- $W_{\hat{f}}(i) \equiv 2 \pmod 4$, $\forall\, i$ *with* $0 \leq i \leq 2^n - 1$. *if* $\mathrm{wt}(f)$ *is odd.*

Proof:

$$\begin{aligned} W_{\hat{f}}(a) &= \sum_{x\in\mathbb{F}_2^n} \hat{f}(x)(-1)^{a\cdot x} \\ &= \sum_{x\in\mathbb{F}_2^n} \left[1-2f(x)\right][1-2(a\cdot x)] \\ &= \sum_{x\in\mathbb{F}_2^n} 1-2f(x)-2(a\cdot x)+4f(x)(a\cdot x) \\ &= \sum_{x\in\mathbb{F}_2^n} 1-2\sum_{x\in\mathbb{F}_2^n} f(x)-2\sum_{x\in\mathbb{F}_2^n}(a\cdot x)+4\sum_{x\in\mathbb{F}_2^n} f(x)(a\cdot x) \\ &= 2^n-2\sum_{x\in\mathbb{F}_2^n} f(x)-2\sum_{x\in\mathbb{F}_2^n}(a\cdot x)+4\sum_{x\in\mathbb{F}_2^n} f(x)(a\cdot x) \end{aligned}$$

Now $2^n \equiv 0 \pmod 4$ since $n \geq 2$. $2\sum_{x\in\mathbb{F}_2^n}(a\cdot x) \equiv 0 \pmod 4$ from Proposition 2.3.1. And $2\sum_{x\in\mathbb{F}_2^n} f(x) \equiv 2 \pmod 4$ if $\mathrm{wt}(f)$ is odd, and $2\sum_{x\in\mathbb{F}_2^n} f(x) \equiv 0 \pmod 4$ if $\mathrm{wt}(f)$ is even. Hence the result follows. □

Next theorem is a classical result (cf. [9]):

Theorem 3.2.7 (Parseval's equality).

$$\sum_{x\in\mathbb{F}_2^n} W_{\hat{f}(x)} = 2^{2n}$$

The following theorem will be generalized and be proved later in Section 4.3.

Theorem 3.2.8. *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function with algebraic degree d, and $\hat{f} : \mathbb{F}_2^n \to \{+1,-1\}$ be its sign function. Let $\mathcal{W}_{\hat{f}} = (W_{\hat{f}}(0),\ldots,W_{\hat{f}}(2^n-1))$ be the Walsh spectrum of $\hat{f}$. If $d = n-1$, half of $u \in \mathcal{W}_{\hat{f}}$ satisfies $u \equiv 0 \pmod 8$, and half of $v \in \mathcal{W}_{\hat{f}}$ satisfies $v \equiv 4 \pmod 8$.*

3.3 The Numerical Normal Form

Numerical Normal Form is introduced in [3]. Most of the results of this section are from this paper.

3.3.1 Definitions and Basic Properties

We first give the existence and uniqueness of an integer valued polynomial representation of a Boolean function.

Proposition 3.3.1. *[3] Every Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ can be represented by a polynomial $\tilde{f}$ in $\mathbb{Z}[x_1,\ldots,x_n]$. Furthermore, representation is unique if we consider only the polynomials in which any variable appears with power at most* 1.

Proof: [3] Let $\delta_a : \mathbb{F}_2^n \to \mathbb{F}_2$ be the Boolean function satisfying:

$$\delta_a(u) = \begin{cases} 1 & if\ u = a, \\ 0 & if\ u \neq a. \end{cases}$$

We can represent δ_a as a polynomial in $\mathbb{Z}[x_1,\ldots,x_n]$:

$$\tilde{\delta}_a = \left(\prod_{i \notin I_a} (1 - x_i)\right)\left(\prod_{i \in I_a} x_i\right) \tag{3.3.1}$$

where I_a is the support of a and $x = (x_1,\ldots,x_n)$. In the above polynomial power of any variable x_i is at most 1, since any x_i appears only once.

f can be represented by a polynomial $\tilde{f}$ in $\mathbb{Z}[x_1,\ldots,x_n]$ by using:

$$\tilde{f} = \sum_{a \in \mathbb{F}_2^n} f(a) \cdot \tilde{\delta}_a \tag{3.3.2}$$

Similarly, in $\tilde{f}$ power of any variable x_i is at most 1. This proves the existence.

Equivalently we can write $\tilde{f}$ as:

$$\tilde{f} = \sum_{u \in \mathbb{F}_2^n} \lambda_u \left(\prod_{i=1}^{n} x_i^{u_i}\right),\ \lambda_u \in \mathbb{Z} \tag{3.3.3}$$

where $\prod_{i=1}^{n} x_i^{u_i} = x^u$.

Let $a = (a_1, \ldots, a_n) \in \mathbb{F}_2^n$. It is clear that $\prod_{i=1}^{n} a_i^{u_i} = 1$ if $u_1 \leq a_1, \cdots, u_n \leq a_n$ (or equivalently $u \preceq a$) since $0^0 = 1$ whereas $0^1 = 0$ and $\prod_{i=1}^{n} a_i^{u_i} = 0$ otherwise. Therefore:

$$f(a) = \sum_{u \preceq a} \lambda_u, \ \forall a \in \mathbb{F}_2^n \tag{3.3.4}$$

For uniqueness, assume $\tilde{f_1}$ and $\tilde{f_2}$ be two polynomial representations of f with integer coefficients and in which any variable has power at most 1. Hence $\tilde{f_1} = \sum_{u \in \mathbb{F}_2^n} \mu_u x^u$ and $\tilde{f_2} = \sum_{u \in \mathbb{F}_2^n} \nu_u x^u$, where $\mu_u, \nu_u \in \mathbb{Z}$.

We claim for any $u \in \mathbb{F}_2^n$, $\mu_u = \nu_u$. We shall prove by mathematical induction on $\mathrm{wt}(u)$.

For $u = (0, \ldots, 0)$ clearly $f(0, \ldots, 0) = \mu_{(0,\ldots,0)} = \nu_{(0,\ldots,0)}$.

Assume $\mu_u = \nu_u$ for all u with $\mathrm{wt}(u) < m$. Let $v \in \mathbb{F}_2^n$ with $\mathrm{wt}(v) = m + 1$.

$$\begin{aligned} f(v) &= \sum_{a \preceq v} \mu_a = \sum_{a \preceq v} \nu_a \\ &= \sum_{a \prec v} \mu_a + \mu_v = \sum_{a \prec v} \nu_a + \nu_v \end{aligned}$$

But by our inductive hypothesis, $\sum_{a \prec v} \mu_a = \sum_{a \prec v} \nu_a$, implying $\mu_v = \nu_v$.

Therefore we proved any two representation of f should be same. This proves the uniqueness. □

For the sequel, we will not make distinction between functions and their polynomial representations.

Definition 3.3.2. [3] Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function. *Numerical Normal Form*

(NNF) of f is the integer valued polynomial (3.3.3).

$$f(x_1,\ldots,x_n) = \sum_{u\in\mathbb{F}_2^n} \lambda_u \left(\prod_{i=1}^{n} x_i^{u_i}\right),\ \lambda_u \in \mathbb{Z} \tag{3.3.5}$$

Example 3.3.3. Let $f:\mathbb{F}_2^3 \to \mathbb{F}_2$ have the following truth table:

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

Then

$$\begin{aligned}
f(x_3,x_2,x_1) &= 0\cdot\delta_{000} + 0\cdot\delta_{001} + 1\cdot\delta_{010} + 0\cdot\delta_{011} \\
&\quad + 1\cdot\delta_{100} + 1\cdot\delta_{101} + 1\cdot\delta_{110} + 0\cdot\delta_{111} \\
&= 0\cdot(1-x_3)(1-x_2)(1-x_1) \\
&\quad + 0\cdot(1-x_3)(1-x_2)(x_1) \\
&\quad + 1\cdot(1-x_3)(x_2)(1-x_1) \\
&\quad + 0\cdot(1-x_3)(x_2)(x_1) \\
&\quad + 1\cdot(x_3)(1-x_2)(1-x_1) \\
&\quad + 1\cdot(x_3)(1-x_2)(x_1) \\
&\quad + 1\cdot(x_3)(x_2)(1-x_1) \\
&\quad + 0\cdot(x_3)(x_2)(x_1) \\
&= x_2 - x_1x_2 - x_2x_3 + x_1x_2x_3 \\
&\quad + x_3 - x_1x_3 - x_2x_3 + x_1x_2x_3 \\
&\quad + x_1x_3 - x_1x_2x_3 \\
&\quad + x_2x_3 - x_1x_2x_3 \\
&= x_2 + x_3 - x_1x_2 - x_2x_3
\end{aligned}$$

Proposition 3.3.4. *[3] Truth table of f can be calculated by the formula (3.3.4):*

$$f(a) = \sum_{u \preceq a} \lambda_u, \ \forall a \in \mathbb{F}_2^n \tag{3.3.6}$$

Proof: [3] Given in the proof of Proposition 3.3.1. □

We know how to find NNF of a function whose truth table is known by (3.3.2). However, it is rather inefficient as Example 3.3.3 demonstrates. Following is a more efficient formula, which will be proved once more using a different technique in Section 3.4.

Proposition 3.3.5. *[3] Let f be a Boolean function, and λ_u be the NNF coefficients of f for all $u \in \mathbb{F}_2^n$ as in Definition 3.3.2. Then*

$$\lambda_u = (-1)^{\mathrm{wt}(u)} \sum_{a \in \mathbb{F}_2^n \mid a \preceq u} (-1)^{\mathrm{wt}(a)} f(a) \tag{3.3.7}$$

Proof: [3] Recall the formula (3.3.2): $f = \sum_{a \in \mathbb{F}_2^n} f(a) \cdot \delta_a$. Proposition states that coefficient of x^u in δ_a is:

$$\begin{cases} 0 & \text{if } a \not\preceq u, \\ (-1)^{\mathrm{wt}(u)-\mathrm{wt}(a)} & \text{if } a \preceq u. \end{cases}$$

Recall the formula (3.3.1):

$$\delta_a = \left(\prod_{i \notin I_a} (1 - x_i) \right) \left(\prod_{i \in I_a} x_i \right)$$

Let $u = (u_1, \ldots u_n)$ and $a = (a_1, \ldots, a_n)$. If $a \not\preceq u$, then $a_j = 1$ but $u_j = 0$ for some $j \in \mathbb{F}_2^n$. Then every term of (3.3.2) includes x_j by (3.3.1). Not divisible by x_j, coefficient of x^u is 0. Now consider the case $a \preceq u$. Let $I_a = \{i_1, \ldots, i_m\}$ be the support

of a. δ_a consists of every term which includes $x_{i_1} \cdots x_{i_m}$. Since the support of u satisfies, $I_u \supseteq I_a$, the coefficient of x^u is ± 1. Finally, the sign of the terms of (3.3.1) with degree $\mathrm{wt}(u)$ is determined by observing $(\mathrm{wt}(u) - \mathrm{wt}(a))$ x_j's are coming from the left product. And the sign of the $\mathrm{wt}(u) - \mathrm{wt}(a)$ degree term of the left product is $(-1)^{\mathrm{wt}(u)-\mathrm{wt}(a)}$. □

Remark 3.3.6. Proposition 3.3.5 implies, Boolean functions with even weight, in particular balanced functions with more than one variable, have algebraic degree less than n, the number of variables. To see this, observe that $\lambda_{1\cdots 1}$ is even and $a_{1\cdots 1} \equiv \lambda_{1\cdots 1} \pmod 2$.

As in Algebraic Normal Form and Walsh spectrum representations, conversion to and from the truth table can be realized by matrix multiplications.

Theorem 3.3.7. *Let*

$$T_f = (f(0), f(1), \ldots, f(2^n - 1)),$$

$$\Lambda_f = (\lambda_0, \lambda_1, \ldots, \lambda_{2^n-1})$$

be the truth table and NNF representations of a Boolean function f respectively, and integers $0, 1, \ldots, 2^n - 1$ are used as their binary representations. Then $T_f = U_n \Lambda_f$ and $\Lambda_f = V_n T_f$, where $U_n = \bigotimes^n \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$, and $V_n = \bigotimes^n \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}$.

3.3.2 Conversion Formulae Between NNF and Other Representations

We will now give conversion formulae between several representations.

NNF and ANF

We prove the following lemma, given in [3] without proof, relating the summation in $\mathbb{F}_2$, $\oplus$, and the summation in $\mathbb{Z}$, $+$:

Lemma 3.3.8 (Poincaré Formula). *[3] Let $a_1, \ldots, a_n \in \mathbb{F}_2$. The following formula holds:*

$$\bigoplus_{i=1}^{n} a_i = \sum_{k=1}^{n} (-2)^{k-1} \sum_{1 \le i_1 < \ldots < i_k \le n} a_{i_1} \cdots a_{i_k}$$

Proof: We will prove by induction on n.

Let

$$S_n = \bigoplus_{i=1}^{n} a_i$$

For the base case $n = 2$, clearly $S_2 = a_1 \oplus a_2 = a_1 + a_2 - 2a_1a_2$.

Now assume

$$S_m = \sum_{k=1}^{m} (-2)^{k-1} \sum_{1 \le i_1 < \ldots < i_k \le m} a_{i_1} \cdots a_{i_k}$$

for all $m < n$.

S_n consists of two mutually exclusive parts: terms not including a_n, and terms including a_n,

$$\begin{aligned}
S_n &= \left[\sum_{k=1}^{n-1} (-2)^{k-1} \sum_{1 \le i_1 < \ldots < i_k \le n-1} a_{i_1} \cdots a_{i_k} \right] + \\
&\quad \left[a_n + \left(\sum_{k=1}^{n-1} (-2)^{k} \sum_{1 \le i_1 < \ldots < i_k \le n-1} a_{i_1} \cdots a_{i_k} a_n \right) \right] \\
&= S_{n-1} + \left[a_n - 2a_n \left(\sum_{k=1}^{n-1} (-2)^{k-1} \sum_{1 \le i_1 < \ldots < i_k \le n-1} a_{i_1} \cdots a_{i_k} \right) \right] \\
&= S_{n-1} + a_n - 2a_n S_{n-1} \\
&= S_{n-1} \oplus a_n
\end{aligned}$$

proving the induction. In the last three lines of the proof we used our inductive hypothesis. □

Consider now the 2^n terms in the Algebraic Normal Form of f:

$$f(x) = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus \cdots \oplus a_n x_n \oplus a_{12} x_1 x_2 \oplus a_{13} x_1 x_3 \oplus \cdots \oplus a_{12\cdots n} x_1 x_2 \cdots x_n \quad (3.3.8)$$

Applying Poincaré formula to (3.3.8), we get the unique polynomial representation of f.

$$f(x) = \sum_{k=1}^{2^n} (-2)^{k-1} \sum_{\{u^1,\ldots,u^k\}} a_{u^1} \cdots a_{u^k} x^{u^1 \vee \cdots \vee u^k}$$

where $\{u^1,\ldots,u^k\}$ means $u^i \in \mathbb{F}_2^n,\ i = 1,\ldots,k$ are distinct and $u^1 \vee \cdots \vee u^k$ is the word, whose support is the union of supports of u^i's.

Then the coefficient λ_u corresponding to $x_u,\ u \in \mathbb{F}_2^n$ can be found by using:

Proposition 3.3.9. *[3] Let $f(x) = \sum_{u\in\mathbb{F}_2^n} \lambda_u x^u$ be the NNF representation of f, and $f(x) = \bigoplus_{u\in\mathbb{F}_2^n} a_u x^u$ be the ANF representation of f. Then:*

$$\lambda_u = \sum_{k=1}^{2^n} (-2)^{k-1} \sum_{\{u^1,\ldots,u^k\} \mid u^1 \vee \cdots \vee u^k = u} a_{u^1} \cdots a_{u^k} \quad (3.3.9)$$

Where $\{u^1,\ldots,u^k\}$ means $u^i \in \mathbb{F}_2^n,\ i = 1,\ldots,k$ are distinct and $u^1 \vee \cdots \vee u^k = u$ means u is the word whose support is the union of supports of u^i's.

Proof: Proof as given in [3] is given before the statement of the proposition. □

NNF and Walsh Spectrum

We begin by a result relating NNF and Walsh spectrum of a given Boolean function.

Proposition 3.3.10. *[3] Let f be a Boolean function, and for all $u \in \mathbb{F}_2^n$, λ_u's be the NNF coefficients of f. Then the Walsh transform of f at $a \in \mathbb{F}_2^n$ is given as:*

$$W_f(a) = (-1)^{\mathrm{wt}(a)} \sum_{u \in \mathbb{F}_2^n | a \preceq u} 2^{n-\mathrm{wt}(u)} \lambda_u \tag{3.3.10}$$

Proof: [3]

$$\begin{aligned}
W_f(a) &= \sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{a \cdot x} \\
&= \sum_{x \in \mathbb{F}_2^n} \left(\sum_{u \in \mathbb{F}_2^n} \lambda_u x^u \right) (-1)^{a \cdot x}, \quad \textit{by (3.3.5)} \\
&= \sum_{u \in \mathbb{F}_2^n} \lambda_u \sum_{x \in \mathbb{F}_2^n | u \preceq x} (-1)^{a \cdot x}, \quad x^u \textit{ is 1 if } u \preceq x, \textit{ and 0 otherwise} \\
&\quad (\textit{we make the change of variable } x \textit{ to } \bar{x} = x + \mathbf{1}) \\
&= \sum_{u \in \mathbb{F}_2^n} \lambda_u \sum_{x \in \mathbb{F}_2^n | x \preceq \bar{u}} (-1)^{a \cdot \bar{x}} \\
&= \sum_{u \in \mathbb{F}_2^n} \lambda_u \sum_{x \in \mathbb{F}_2^n | x \preceq \bar{u}} (-1)^{a \cdot x + \mathrm{wt}(a)} \\
&= (-1)^{\mathrm{wt}(a)} \sum_{u \in \mathbb{F}_2^n \mid a \preceq u} 2^{n-\mathrm{wt}(u)} \lambda_u
\end{aligned}$$

In the last step we used Proposition 2.3.1. □

Remark 3.3.11. [3] Recall that weight of f is given by $\mathrm{wt}(f) = W_f(0)$. Hence

$$\mathrm{wt}(f) = \sum_{u \in \mathbb{F}_2^n} 2^{n-\mathrm{wt}(u)} \lambda_u \tag{3.3.11}$$

Remark 3.3.12. [3] We immediately have the following relation between NNF and

the Walsh transform of $\hat{f}$, by using Theorem 3.2.4:

$$W_{\hat{f}}(a) = 2^n\delta_0(a) - 2W_f(a) = 2^n\delta_0(a) + (-1)^{\mathrm{wt}(a)+1} \sum_{u\in\mathbb{F}_2^n \mid a\preceq u} 2^{n-\mathrm{wt}(u)+1}\lambda_u$$

Similarly, conversion from Walsh spectrum to NNF is possible using the following formula.

Proposition 3.3.13. *[3] Let f be a Boolean function, and for all $x \in \mathbb{F}_2^n$, $W_f(x)$'s be the Walsh spectrum coefficients of f. Then NNF coefficients of f at $u \in \mathbb{F}_2^n$ are given as:*

$$\lambda_u = 2^{-n}(-2)^{\mathrm{wt}(u)} \sum_{x\in\mathbb{F}_2^n \mid u\preceq x} W_f(x) \tag{3.3.12}$$

Proof: The proof of this proposition can be found in [3]. □

Definition 3.3.14. [3] Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function. Let d_{ANF} be the algebraic degree of f.

$$d_{ANF} = \max_{u\in\mathbb{F}_2^n}\{\mathrm{wt}(u) \mid a_u \neq 0\}$$

Numerical degree, d_{NNF}, and Walsh degree d_W of f is defined as:

$$\begin{aligned} d_{NNF} &= \max_{u\in\mathbb{F}_2^n}\{\mathrm{wt}(u) \mid \lambda_u \neq 0\} \\ d_W &= \max_{u\in\mathbb{F}_2^n}\{\mathrm{wt}(u) \mid W_f(u) \neq 0\} \end{aligned}$$

Proposition 3.3.15. *[3] Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function. Then*

$$d_W = d_{NNF} \geq d_{ANF}$$

Proof: $d_{NNF} \geq d_{ANF}$ since $a_u \equiv \lambda_u \pmod 2$. $d_W = d_{NNF}$ follows from (3.3.10) and (3.3.12). □

3.3.3 Characterization of Several Types of Functions

Given an integer valued polynomial, the problem of characterizing polynomials of several functions arises naturally.

Characterization of Boolean Functions

To characterize Boolean functions, an immediate idea is to use the formula between NNF coefficients and the truth table (3.3.6). Observe that the complexity of such a calculation is $\mathcal{O}(3^n)$.

Proposition 3.3.16. *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$. Complexity of calculating $f(a)$'s using:*

$$f(a) = \sum_{u \preceq a} \lambda_u, \ \forall a \in \mathbb{F}_2^n$$

is $\mathcal{O}(3^n)$.

Proof: Let $w_i = |\{u \mid \mathrm{wt}(u) = i\}|$, $0 \leq i \leq n$. $w_i = \binom{n}{i}$. To compute $f(a)$ by using (3.3.6), one needs $2^{\mathrm{wt}(a)}$ NNF coefficients. One easily gets:

$$\sum_{i=0}^{n} \binom{n}{i} 2^i = (1+2)^n = 3^n$$

□

Remark 3.3.17. Indeed computing (3.3.6) can be done in $\mathcal{O}(n2^n)$ steps using a Fast Walsh Transform-like algorithm, resulting an asymptotically better bound given in [7].

Another characterization ([3]) uses the basic fact that $y^2 = y \iff y \in \{0,1\}$. Applying this to (3.3.6) one gets:

$$\left(\sum_{u \preceq a} \lambda_u\right)^2 = \sum_{u \preceq a} \lambda_u$$

Multiplication of two terms $\lambda_u x^u$, and $\lambda_v x^v$ adds to $\lambda_w x^w$ if and only if $I_u \cup I_v = I_w$. This proves:

Proposition 3.3.18. *[3] The integer valued polynomial $\sum_{w \in \mathbb{F}_2^n} \lambda_w x^w$ is NNF of a Boolean function if and only if:*

$$\lambda_w = \sum_{u,v \in \mathbb{F}_2^n \mid I_u \cup I_v = I_w} \lambda_u \lambda_v \tag{3.3.13}$$

This characterization is worse considering efficiency.

Proposition 3.3.19. *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$. Complexity of calculating $f(a)$'s using:*

$$\lambda_w = \sum_{u,v \in \mathbb{F}_2^n \mid I_u \cup I_v = I_w} \lambda_u \lambda_v$$

is $\mathcal{O}(2^{2n})$.

Proof: Let $w_i = |\{u \mid \mathrm{wt}(u) = i\}|$, $0 \le i \le n$. $w_i = \binom{n}{i}$. Consider a vector $a \in \mathbb{F}_2^n$ with $\mathrm{wt}(a) = m$. To compute $f(a)$ by using (3.3.13), one needs to perform several multiplications and additions. To count the number of operations we need to find out $\left|\{u, v \in \mathbb{F}_2^n \mid I_u \cup I_v = I_a\}\right|$.

- If $\mathrm{wt}(u) = 0$, then there exists only one v satisfying $I_u \cup I_v = a$. Namely v is the vector with support I_a.

- If $\mathrm{wt}(u) = 1$, then there are $2^1 = 2$ v's, namely the vector with support I_a and the vector with support $I_a \setminus I_u$.
- Generally if $\mathrm{wt}(u) = j$, then there are 2^j v's, whose supports are given as $\{I_a \setminus U \mid U \in \mathscr{P}(I_u)\}$.

Then, since there are $\binom{m}{i}$ subsets of a with i elements:

$$\left|\{u, v \in \mathbb{F}_2^n \mid I_u \cup I_v = I_a\}\right| = \sum_{i=0}^{m} \binom{m}{i} 2^i = (1+2)^m = 3^m$$

And consequently

$$\sum_{i=0}^{n} \binom{n}{i} 3^i = (1+3)^n = 4^n$$

□

Carlet and Guillot argue that there is a better characterization using the following argument:

Proposition 3.3.20. *[3] An integer valued function f is Boolean if and only if*

$$\sum_{x \in \mathbb{F}_2^n} f^2(x) = \sum_{x \in \mathbb{F}_2^n} f(x)$$

Proof: If f is Boolean, then $\sum_{x \in \mathbb{F}_2^n} f^2(x) = \sum_{x \in \mathbb{F}_2^n} f(x)$.

For the converse, observation of $m^2 > m$, whenever $m \geq 2$ or $m < 0$, $m \in \mathbb{Z}$ is enough. □

Proposition 3.3.21. *[3] The integer valued polynomial $\sum_{w \in \mathbb{F}_2^n} \lambda_w x^w$ is NNF of a Boolean function if and only if:*

$$\sum_{w \in \mathbb{F}_2^n} 2^{n-\mathrm{wt}(u)} \sum_{u,v \in \mathbb{F}_2^n \mid I_u \cup I_v = I_w} \lambda_u \lambda_v = \sum_{w \in \mathbb{F}_2^n} 2^{n-\mathrm{wt}(u)} \lambda_w \tag{3.3.14}$$

Proof: [3] Follows from Proposition 3.3.20 and (3.3.11). □

Proposition 3.3.22. *Characterization using (3.3.14) requires* $\mathcal{O}(2^{2n})$ *operations.*

Proof: Computing $\left(\sum_{u\in\mathbb{F}_2^n}\lambda_u x^u\right)^2$ requires $2^n\cdot 2^n$ operations in the worst case, since the polynomial in question has at most 2^n terms. □

Characterization of Affine Functions

Proposition 3.3.23. *[3] Let* $f(x)=l\cdot x\oplus\epsilon$ *be an affine function, where* $l\in\mathbb{F}_2^n$*, and* $\epsilon\in\mathbb{F}_2$*. Then*

$$\lambda_u=\begin{cases}(-1)^{\epsilon}(-2)^{\mathrm{wt}(u)-1} & \text{if } u\preceq l \text{ and } u\neq(0,\ldots,0)\\ \epsilon & \text{if } u=(0,\ldots,0)\\ 0 & \text{otherwise.}\end{cases}$$

Proof: For the case $u=(0,\ldots,0)$, $\lambda_{(0,\ldots,0)}=f(0)=\epsilon$ by (3.3.6) . Consider the case $u\not\preceq l$. (3.3.9) implies there must be some $a_{u^i}=0$, for any term $a_{u^1}\cdots a_{u^k}$ in the computation of λ_u; since $I_u\setminus I_l\neq\emptyset$. Hence $\lambda_u=0$.

Now consider $u\preceq l$. Then there are two sums in the calculation of λ_u if $\epsilon=1$, one sum if $\epsilon=0$.

- $\lambda_u=(-2)^{\mathrm{wt}(u)}\epsilon\cdot\prod_{i\in I_a}a_i+(-2)^{\mathrm{wt}(u)-1}\cdot\prod_{i\in I_a}a_i=(-1)\cdot(-2)^{\mathrm{wt}(u)-1}$, if $\epsilon=1$;
- $\lambda_u=(-2)^{\mathrm{wt}(u)-1}\cdot\prod_{i\in I_a}a_i=(-2)^{\mathrm{wt}(u)-1}$, if $\epsilon=0$.

□

Characterization of Bent Functions

Recall that a Boolean function f is perfectly nonlinear or *bent* if $W_{\hat{f}}(a)=\pm 2^{\frac{n}{2}}$, for all $a\in\mathbb{F}_2^n$.

Definition 3.3.24. [9] Dual of a bent function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is defined as follows:

$$\tilde{f}(a) = \frac{1}{2} - \frac{W_{\hat{f}}(a)}{2^{\frac{n}{2}+1}}$$

We have the following characterization of bent functions using NNF.

Proposition 3.3.25. *[4] Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ and let $f(x) = \sum_{u \in \mathbb{F}_2^n} \lambda_u x^u$ be the NNF of f. f is bent if and only if f satisfies the following conditions:*

1. *For every u such that $\frac{n}{2} < \mathrm{wt}(u) < n$, $2^{\mathrm{wt}(u)-\frac{n}{2}} \mid \lambda_u$,*
2. *$\lambda_{1,\cdots,1} \equiv 2^{\frac{n}{2}-1} mod\, 2^{\frac{n}{2}}$.*

Proof: Proof of this can be found in [4] and in [2]. □

Characterization of Resilient Functions

Characterization of resilient functions is possible by using NNF: We need the following lemma for the characterization:

Lemma 3.3.26. *[4] Let $g : \mathbb{F}_2^n \to \mathbb{F}_2$ be defined as:*

$$g(x) = f(x) \oplus x_1 \oplus x_2 \oplus \cdots \oplus x_n$$

Then $W_{\hat{g}}(a) = W_{\hat{f}}(\bar{a})$ where $\bar{a} = \mathbf{1} + a$.

Proof:

$$\begin{aligned} W_{\hat{g}}(a) &= \sum_{x \in \mathbb{F}_2^n} (-1)^{g(x) \oplus a \cdot x} = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus x \oplus a \cdot x} \\ &= \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus (a \oplus 1) \cdot x} = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus \bar{a} \cdot x} \\ &= W_{\hat{f}}(\bar{a}) \end{aligned}$$

□

Proposition 3.3.27. *[4] Let m and n be integers with $0 \leq m < n$. Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$. f is m-resilient if and only if $d_{NNF}(g) \leq n - m - 1$, where $g(x) = f(x) \oplus x_1 \oplus x_2 \oplus \cdots \oplus x_n$.*

Proof: [4] By the previous lemma $W_{\hat{g}}(a) = W_{\hat{f}}(\bar{a})$. Since f is m-resilient, $W_{\hat{f}}(a) = 0$, for a having weight less than or equal to m. Hence f is m-resilient if and only if $W_{\hat{g}}(a) = 0$ for a such that $\mathrm{wt}(a) \geq n - m$, (since $\mathrm{wt}(a) \leq m \iff \mathrm{wt}(\bar{a}) \geq n - m$, $for\ all\ a \in \mathbb{F}_2^n$). Hence Walsh degree $d_W(g) \leq n - m - 1$. But we know $d_{NNF}(g) = d_W(g)$ from Proposition 3.3.15, we deduce $d_{NNF} \leq n - m - 1$ if and only if f is m-resilient. □

Above result is a generalization of Siegenthaler's inequality.

3.4 Partially Ordered Sets and Their Möbius Functions

We investigate the connection between the truth table, NNF and Walsh Transform of Boolean functions. Möbius inversion is one of the tools that can be used in the analysis. In this section we will be dealing with the Möbius inversion. Our main references in this section are Gian-Carlo Rota [10] and Marshall Hall Jr. [6].

3.4.1 Basic Results

A *partially ordered set* P is a set of elements with an order relation $\geq$ and an equality $=$, such that the following axioms hold:

1. $x \geq x$ for all $x \in P$ (reflexive).

2. if $x \geq y$ and $y \geq z$ then $x \geq z$ for all $x, y, z \in P$ (transitive).

3. if $x \succeq y$ and $y \succeq x$ then $x = y$ for all $x, y \in P$ (antisymmetric).

The order relation intuitively has $u \succeq v \iff v \preceq u$. Since our main concern is the vector space $\mathbb{F}_2^n$, let us examine $\mathbb{F}_2^n$ with $\preceq$ order relation defined before. First let us recall the definition.

Let $v \in \mathbb{F}_2^n$ be represented as $(v_1, \ldots, v_n)$. The support of v, I_v, is the places (indices) of v which are nonzero (*i.e.* 1):

$$I_v = \{i \mid v_i \neq 0,\ 1 \leq i \leq n\}$$

We say $u \preceq v$ if $I_u \subseteq I_v$.

Remark 3.4.1. [10] $\mathbb{F}_2^n$ with order $\succeq$ and equality $=$, can be viewed as a partially ordered set.

Proof: Since:

1. $v \preceq v$, since $I_v = I_v$, for all $v \in \mathbb{F}_2^n$.

2. $u \preceq v$ and $v \preceq w$ implies , since $I_u \subseteq I_v$ and $I_v \subseteq I_w$ implies $I_u \subseteq I_w$ for all $u, v, w \in \mathbb{F}_2^n$.

3. $u \preceq v$ and $v \preceq u$ implies $u = v$ since $I_u \subseteq I_v$ and $I_v \subseteq I_u$ implies $I_u = I_v$, for all $u, v \in \mathbb{F}_2^n$.

□

$\mathbb{F}_2^n$ has a *least upper bound* $\mathbf{1}$ (since $\mathbf{1} \succeq x$, for all $x \in \mathbb{F}_2^n$) and a *greatest lower bound* $\mathbf{0}$ (since $\mathbf{0} \preceq x$, for all $x \in \mathbb{F}_2^n$).

An *interval* $[x, y]$ where $x \preceq y$ is the set of all w with $x \preceq w \preceq y$. A partially ordered set P is called *locally finite* if every interval of P is finite.

Since we are interested only in $\mathbb{F}_2^n$ we will be dealing with locally finite partially ordered sets with a greatest lower bound. From now on we will assume P is a locally finite partially ordered set with a greatest lower bound.

Let us consider a class of real-valued functions $f : P \times P \to \mathbb{R}$, with the restriction $f(x, y) = 0$, if $x \not\preceq y$. The product of two such functions $h = f \cdot g$ is defined as:

$$h(x, y) = \sum_{x \preceq z \preceq y} f(x, z) \cdot g(z, y) \tag{3.4.15}$$

Sum of these functions are defined as usual. *i.e.*:

$$(f + g)(x, y) = f(x, y) + g(x, y) \ for\ all\ x, y \in P \tag{3.4.16}$$

The *incidence algebra* $\mathscr{A}(P)$ of P is defined under the operations of sum (3.4.16), scalar product and the product (3.4.15) operations.

Proposition 3.4.2. *([10],[6]) Multiplication defined for* $\mathscr{A}(P)$ *is associative, distributive and has an identity, the Kronecker delta*

$$\delta(x, y) = \begin{cases} 1 & x = y, \\ 0 & x \neq y \end{cases}$$

Proof: Let $a = f \cdot g$ and $b = g \cdot h$,

$$\begin{aligned} a \cdot h &= \sum_{x \preceq t \preceq y} a(x,t) \cdot h(t,y) \\ &= \sum_{x \preceq t \preceq y} \left(\sum_{x \preceq z \preceq t} f(x,z) \cdot g(z,t) \right) h(t,y) \\ &= \sum_{x \preceq z \preceq t} f(x,z) \left(\sum_{x \preceq t \preceq y} g(z,t) \cdot h(t,y) \right) \\ &= \sum_{x \preceq z \preceq t} f(x,z) \left(\sum_{z \preceq t \preceq y} g(z,t) \cdot h(t,y) \right) \\ &= f \cdot b \end{aligned}$$

proves associativity. For distributivity observe that

$$\begin{aligned} f \cdot (g+h) &= \sum_{x \preceq z \preceq y} f(x,z) \cdot (g+h)(z,y) \\ &= \sum_{x \preceq z \preceq y} f(x,z) \cdot \big[g(z,y) + h(z,y) \big] \\ &= \sum_{x \preceq z \preceq y} f(x,z) \cdot g(z,y) + \sum_{x \preceq z \preceq y} f(x,z) \cdot h(z,y) \\ &= f \cdot g + f \cdot h \end{aligned}$$

Identity is rather clear, for all $x, y \in P$:

$$\begin{aligned} f \cdot \delta &= \sum_{x \preceq z \preceq y} f(x,z) \cdot \delta(z,y) \\ &= f(x,y) \end{aligned}$$

and

$$\begin{aligned} \delta \cdot f &= \sum_{x \preceq z \preceq y} \delta(x,z) \cdot f(z,y) \\ &= f(x,y) \end{aligned}$$

□

Proposition 3.4.3. *([10],[6]) A function $f(x,y) \in \mathscr{A}(P)$ has left and right inverses if and only if $f(x,x) \neq 0$ for all $x \in P$. Moreover left and right inverses are the same.*

Proof: ([10],[6]) We wish to find $g = f^{-1}$ such that $\delta = f \cdot g$. Since $1 = \delta(x,x) = f(x,x) \cdot g(x,x)$, $f(x,x)$ is necessarily nonzero for all $x \in P$. Now assume $f(x,x) \neq 0$, for all $x \in P$. Then from $1 = \delta(x,x) = f(x,x) \cdot g(x,x)$, $g(x,x) = (f(x,x))^{-1}$. Now, assume we know all $g(z,y)$ with $x \prec z \preceq y$. Then we may find $g(x,y)$ by

$$0 = \delta(x,y) = \sum_{x \preceq z \preceq y} f(x,z) \cdot g(z,y) = f(x,x) \cdot g(x,y) + \sum_{x \prec z \preceq y} f(x,z) \cdot g(z,y)$$

which implies

$$g(x,y) = -\frac{\sum_{x \prec z \preceq y} f(x,z) \cdot g(z,y)}{f(x,x)}$$

Hence, existence of the right inverse is obtained from our assumption that $f(x,x)$ is nonzero. Existence of the left inverse is obtained in a similar manner.

For the equality, let g_l be the left inverse and g_r be the right inverse, thus $f \cdot g_r = 1 = g_l \cdot f$; hence, $g_l = g_l \cdot 1 = g_l \cdot (f \cdot g_r) = (g_l \cdot f) \cdot g_r = g_r$. □

Definition 3.4.4. ([10],[6]) The zeta function $\zeta(x,y) \in \mathscr{A}(P)$ is defined as follows:

$$\zeta(x,y) = \begin{cases} 1 & \text{if } x \preceq y \\ 0 & \text{otherwise} \end{cases}$$

The Möbius function $\mu(x,y) \in \mathscr{A}(P)$ is the inverse of the zeta function.

$\mu(x,y)$ can be defined inductively on $[x,y]$ as follows: First, define $\mu(x,x) = 1$ for all $x \in P$. Now suppose $\mu(x,z)$ is defined for all $z \in [x,y)$. Now set

$$\mu(x,y) = -\sum_{x \leq z < y} \mu(x,z)$$

Clearly μ is inverse of ζ, (expressed as left inverse).

Theorem 3.4.5 (Möbius inversion). *[10] Let f be defined for all elements in P, and g be determined from*

$$g(x) = \sum_{y \leq x} f(y) \tag{3.4.17}$$

Then, if $\mu(x,y)$ is the Möbius function of P:

$$f(x) = \sum_{y \leq x} g(y) \cdot \mu(y,x) \tag{3.4.18}$$

Proof: [10] We assumed P to be a locally finite POSET, and hence the sums given in (3.4.17) and (3.4.18) are well-defined.

$$\begin{aligned}
\sum_{y \leq x} g(y) \cdot \mu(y,x) &= \sum_{y \leq x} \left(\sum_{z \leq y} f(z) \right) \cdot \mu(y,x) \\
&= \sum_{y \leq x} \left(\sum_{z} f(z) \cdot \zeta(z,y) \right) \cdot \mu(y,x) \\
&= \sum_{z} f(z) \sum_{y \leq x} \zeta(z,y) \cdot \mu(y,x) \\
&= \sum_{z} f(z) \cdot \delta(z,x) \\
&= f(x)
\end{aligned}$$

□

Proposition 3.4.6. *[6] Consider the locally finite partially ordered set $\mathbb{F}_2^n$ with $\mathbf{0}$, we*

have the Möbius function:

$$\mu(x,y) = (-1)^{\mathrm{wt}(y)-\mathrm{wt}(x)}$$

Proof: [6] For base case $\mathrm{wt}(y)-\mathrm{wt}(x)=0$, $\mu(x,x)=(-1)^0=1$.

For $\mathrm{wt}(y)-\mathrm{wt}(x)=1$, $\mu(x,y)=-\sum_{x\preceq z\prec y}\mu(x,z)=(-1)^1=-1$.

Assume it is true for $\mathrm{wt}(y)-\mathrm{wt}(x)<r$. Now let $\mathrm{wt}(y)-\mathrm{wt}(x)=r$

$$\mu(x,y) = -\left[1-\binom{r}{1}+\binom{r}{2}-\cdots+\binom{r}{r-1}(-1)^{r-1}\right]$$

since there are $\binom{r}{i}$ elements $z\in\mathbb{F}_2^n$ with $x\preceq z\prec y$ and $\mathrm{wt}(z)=i$. Consider

$$0=(1-1)^r=1-\binom{r}{1}+\binom{r}{2}-\cdots+\binom{r}{r-1}(-1)^{r-1}+(-1)^r$$

Therefore

$$\mu(x,y)=(-1)^r=(-1)^{\mathrm{wt}(y)-\mathrm{wt}(x)}$$

□

3.4.2 Möbius Inversion Properties of NNF Coefficients

As pointed out in [2], NNF can be seen as the Möbius inverse of the truth table. Now let us apply the results of Rota's work [10] to $\mathbb{F}_2^n$ and the NNF; and find out the relations between NNF and truth table representations of a Boolean function once more.

We have seen the following equation relating NNF and truth table before (3.3.6):

$$f(a)=\sum_{u\preceq a}\lambda_u$$

According to Theorem 3.4.5:

$$\begin{aligned}\lambda_u &= \sum_{u \preceq a} f(u) \cdot \mu(u,a) \\ &= \sum_{u \preceq a} f(u)(-1)^{(\mathrm{wt}(a)-\mathrm{wt}(u))} \\ &= (-1)^{\mathrm{wt}(a)} \sum_{u \preceq a} (-1)^{\mathrm{wt}(u)} f(u)\end{aligned}$$

We recognize the last formula (3.3.7). Hence, truth table and NNF representations are Möbius inverse pairs.

Another Möbius inversion is between NNF and Walsh coefficients of the same function.

We have the following equality (3.3.12):

$$\begin{aligned}\lambda_u &= 2^{-n}(-2)^{\mathrm{wt}(u)} \sum_{u \preceq x} W_f(x) \\ (-1)^{\mathrm{wt}(u)} 2^{n-\mathrm{wt}(u)} \lambda_u &= \sum_{u \preceq x} W_f(x) \\ W_f(u) &= \sum_{u \preceq x} (-1)^{\mathrm{wt}(x)} 2^{n-\mathrm{wt}(x)} \lambda_x \cdot \mu(u,x) \\ W_f(u) &= \sum_{u \preceq x} (-1)^{\mathrm{wt}(x)} 2^{n-\mathrm{wt}(x)} \lambda_x (-1)^{\mathrm{wt}(x)-\mathrm{wt}(u)}\end{aligned}$$

Which gives us the inverse relation (3.3.10):

$$W_f(u) = (-1)^{\mathrm{wt}(u)} \sum_{u \preceq x} 2^{n-\mathrm{wt}(x)} \lambda_x.$$

CHAPTER 4

DIVISIBILITY PROPERTIES OF NNF COEFFICIENTS

4.1 Introduction

In this chapter, we are going to show that the coefficients of NNF have some divisibility properties depending on the algebraic degree and the number of terms having maximal degree, originally given in [2]. Using this result we will prove McEliece theorem following [2]. This divisibility property has some consequences concerning the nonlinearity of resilient (and balanced) functions. We will also give these results of Carlet in Section 4.2. In Section 4.3, we will prove a necessary condition for the Walsh spectrum coefficients of Boolean functions. This result follows from several results concerning subset sums of integer multi-sets, which we will also prove.

4.2 Divisibility Results

Depending on the algebraic degree of f and the number of terms having maximal degree, in (3.3.9) some terms are 0. This is given in the next proposition.

Proposition 4.2.1. *[3] Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ with algebraic degree d. Let r be the number of monomials of degree d in the ANF of f. Then for all $u \in \mathbb{F}_2^n$:*

$$\lambda_u = \sum_{k=\max\left(\left\lceil \frac{\mathrm{wt}(u)}{d} \right\rceil, \left\lceil \frac{\mathrm{wt}(u)-r}{d-1} \right\rceil\right)}^{2^n} (-2)^{k-1} \sum_{\{u^1,\ldots,u^k\} \mid u^1 \vee \cdots u^k = u} a_{u^1} \cdots \vee a_{u^k}$$

Proof: [3]

As before, $\{u^1,\ldots,u^k\}$ refers to k distinct vectors in $\mathbb{F}_2^n$. If $\mathrm{wt}(u^1 \vee \cdots \vee u^k) > kd$, then for at least one of u^i, $\mathrm{wt}(u^i) > d$. This means for $k < \frac{\mathrm{wt}(u)}{d}$ (*i.e.*: $k \leq \left\lceil \frac{\mathrm{wt}(u)}{d} \right\rceil - 1$, or $k \leq \left\lfloor \frac{\mathrm{wt}(u)-1}{d} \right\rfloor$), a_{u^i} is 0, since $\mathrm{wt}(u^i) > d$, the algebraic degree of f. This makes the right sum of (3.3.9) 0.

Now, if $\mathrm{wt}(u^1 \vee \cdots \vee u^k) > rd + (k-r)(d-1) = k(d-1) + r$, then for at least one of u^i, $\mathrm{wt}(u^i) > d$. This means for $k < \frac{\mathrm{wt}(u)-r}{d-1}$ (*i.e.*: $k \leq \left\lceil \frac{\mathrm{wt}(u)-r}{d-1} \right\rceil - 1$, or $k \leq \left\lfloor \frac{\mathrm{wt}(u)-r-1}{d-1} \right\rfloor$), a_{u^i} is 0, making the right sum of (3.3.9) 0. □

Corollary 4.2.2. *[3] Coefficients λ_u in the NNF of f are divisible by $2^{\left\lceil \frac{\mathrm{wt}(u)}{d} \right\rceil - 1}$ (or $2^{\left\lfloor \frac{\mathrm{wt}(u)-1}{d} \right\rfloor}$) and $2^{\left\lceil \frac{\mathrm{wt}(u)-r}{d-1} \right\rceil - 1}$ (or $2^{\left\lfloor \frac{\mathrm{wt}(u)-r-1}{d-1} \right\rfloor}$).*

This corollary is helpful for proving divisibility results. Now we are ready to prove the following important result.

Proposition 4.2.3. *[3] Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function with algebraic degree d, then $\mathrm{wt}(f)$ is divisible by $2^{\lceil \frac{n}{d} \rceil - 1}$.*

Proof: [3] By (3.3.11)

$$\mathrm{wt}(f) = \sum_{u \in \mathbb{F}_2^n} 2^{n-\mathrm{wt}(u)} \lambda_u = \sum_{u \in \mathbb{F}_2^n} k \cdot 2^{n-\mathrm{wt}(u)+\left\lceil \frac{\mathrm{wt}(u)}{d} \right\rceil - 1}$$

Since $\mathrm{wt}(u) - \left\lceil \frac{\mathrm{wt}(u)}{d} \right\rceil$ does not decrease as $\mathrm{wt}(u)$ increase, $n - \mathrm{wt}(u) + \left\lceil \frac{\mathrm{wt}(u)}{d} \right\rceil - 1$ is

minimum when $\mathrm{wt}(u) = n$. Hence $2^{n-n+\lceil \frac{n}{d} \rceil - 1} = 2^{\lceil \frac{n}{d} \rceil - 1} \mid \mathrm{wt}(f)$. □

Proposition 4.2.3 explains the relation between the algebraic degree and the weight of a Boolean function. Following theorem gives a divisibility bound on the Hamming distance to affine functions for resilient functions.

Theorem 4.2.4. *[2] Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be an m-resilient function with $0 \le m \le n-2$. Let d be the algebraic degree of f. Then for every affine function $l(x) : \mathbb{F}_2^n \to \mathbb{F}_2$, the Hamming distance between f and l, $d_H(f,l)$ is divisible by $2^{m+1+\lfloor \frac{n-m-2}{d} \rfloor}$.*

Proof: [2]

Let $l(x) = a \cdot x \oplus \epsilon$

f is balanced, since any m-resilient function is balanced (if f is 0-resilient; then f is not correlation immune, but balanced). Then $d \ge 1$.

Assume $d = 1$, $d_H(f,l)$ is either:

$$d_H(f,l) = \begin{cases} 0 & if\ f = l \\ 2^n & if\ f = l \oplus \epsilon \\ 2^{n-1} & otherwise \end{cases}$$

Hence $d_H(f,l)$ is divisible by $2^{m+1+n-m-2} = 2^{n-1}$.

Now assume $d > 1$. Let $g : \mathbb{F}_2^n \to \mathbb{F}_2$ be defined as:

$$g(x) = f(x) \oplus x_1 \oplus x_2 \oplus \cdots \oplus x_n$$

$W_{\hat{f}}(a) = W_{\hat{g}}(\bar{a})$, for all $a \in \mathbb{F}_2^n$. Using (2.2.3) and (3.2.4), or changing Hamming distance to Walsh distance and Walsh transform of $\hat{f}$ to f:

$$d_H(f,l) = 2^{n-1} - \frac{(-1)^\epsilon}{2} W_{\hat{f}}(a) = 2^{n-1} - (-1)^\epsilon 2^{n-1} \delta_0 \bar{a} + (-1)^\epsilon W_g(\bar{a}) \qquad (4.2.1)$$

Now consider (3.3.10):

$$W_g(a) = (-1)^{\mathrm{wt}(a)} \sum_{u \in \mathbb{F}_2^n | a \preceq u} 2^{n-\mathrm{wt}(u)} \lambda_u$$

by using Corollary 4.2.2,

$$W_g(a) = (-1)^{\mathrm{wt}(a)} \sum_{u \in \mathbb{F}_2^n | a \preceq u} k \cdot 2^{n-\mathrm{wt}(u)+\left\lfloor \frac{\mathrm{wt}(u)-1}{d} \right\rfloor}$$

Since f is m-resilient, $\lambda_u = 0$ if $\mathrm{wt}(u) > n-m-1$, according to Proposition 3.3.27. Therefore for any nonzero λ_u, $\mathrm{wt}(u) \leq n-m-1$. since $2^{n-\mathrm{wt}(u)+\left\lfloor \frac{\mathrm{wt}(u)-1}{d} \right\rfloor}$ reaches minimum when $\mathrm{wt}(u)$ is maximum, we deduce that $W_g(a)$ is divisible by $2^{m+1+\lfloor \frac{n-m-2}{d} \rfloor}$.

Now (4.2.1) implies $d_H(f,l)$ is divisible by $2^{m+1+\lfloor \frac{n-m-2}{d} \rfloor}$. □

We give the following two theorems without proofs. Proofs can be found in [2]. First one proves the tightness of the bound:

Theorem 4.2.5. *[2] For every $n \geq 2$, every $0 \leq m \leq n-2$ and every $1 \leq d \leq n-m-1$, there exists an m-resilient Boolean function on $\mathbb{F}_2^n$ with algebraic degree d and an affine function l such that $d_H(f,l) \nmid 2^{m+2+\lfloor \frac{n-m-2}{d} \rfloor}$.*

If the number of terms with highest algebraic degree in the ANF is small enough, a better bound can be given:

Theorem 4.2.6. *[2] Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be an m-resilient function with $0 \leq m \leq n-2$. Let $d > 1$ be the algebraic degree of f, and r be the number of terms in the ANF of f with highest degree. Then for every affine function $l(x) : \mathbb{F}_2^n \to \mathbb{F}_2$, the Hamming distance between f and l, $d_H(f,l)$ is divisible by $2^{m+1+\lfloor \frac{n-m-r-2}{d-1} \rfloor}$.*

4.2.1 Consequences on Nonlinearity

The discussion in the last section has consequences concerning the nonlinearity of resilient functions. The following result gives an upper bound on the nonlinearity of resilient functions.

Theorem 4.2.7. *[2] Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be an m-resilient Boolean function with $0 \le m \le n-2$ and algebraic degree $d > 1$. The nonlinearity, $nl(f)$, is divisible by $2^{m+1+\lfloor \frac{n-m-2}{d} \rfloor}$, and, $nl(f)$ satisfies:*

$$nl(f) \le \begin{cases} 2^{n-1} - 2^{m+1+\lfloor \frac{n-m-2}{d} \rfloor} \\ \qquad if\ \frac{n}{2} - 1 < m+1+\lfloor \frac{n-m-2}{d} \rfloor, \\ 2^{n-1} - 2^{\frac{n}{2}-1} - 2^{m+1+\lfloor \frac{n-m-2}{d} \rfloor} \\ \qquad if\ n\ is\ even\ and\ \frac{n}{2} - 1 \ge m+1+\lfloor \frac{n-m-2}{d} \rfloor, \\ 2^{n-1} - 2^{m+1+\lfloor \frac{n-m-2}{d} \rfloor} \left\lceil 2^{\frac{n}{2}-m-2-\lfloor \frac{n-m-2}{d} \rfloor} \right\rceil \\ \qquad if\ n\ is\ odd\ and\ \frac{n}{2} - 1 \ge m+1+\lfloor \frac{n-m-2}{d} \rfloor. \end{cases}$$

Furthermore let r be the number of terms with degree d in the ANF of f. The nonlinearity, $nl(f)$, is divisible by $2^{m+1+\lfloor \frac{n-m-r-2}{d-1} \rfloor}$. And $nl(f)$ satisfies:

$$nl(f) \le \begin{cases} 2^{n-1} - 2^{m+1+\lfloor \frac{n-m-r-2}{d} \rfloor} \\ \qquad if\ \frac{n}{2} - 1 < m+1+\lfloor \frac{n-m-r-2}{d} \rfloor, \\ 2^{n-1} - 2^{\frac{n}{2}-1} - 2^{m+1+\lfloor \frac{n-m-r-2}{d} \rfloor} \\ \qquad if\ n\ is\ even\ and\ \frac{n}{2} - 1 \ge m+1+\lfloor \frac{n-m-r-2}{d} \rfloor, \\ 2^{n-1} - 2^{m+1+\lfloor \frac{n-m-r-2}{d} \rfloor} \left\lceil 2^{\frac{n}{2}-m-2-\lfloor \frac{n-m-2}{d} \rfloor} \right\rceil \\ \qquad if\ n\ is\ odd\ and\ \frac{n}{2} - 1 \ge m+1+\lfloor \frac{n-m-r-2}{d} \rfloor. \end{cases}$$

Proof: [2] Divisibility results follow from Theorems 4.2.4 and 4.2.6. For the nonlinearity bound, observation of the fact $nl(f) < 2^{n-1} - 2^{\frac{n}{2}-1}$, for balanced f, is enough for the proof. Given nonlinearity bounds are the largest possible nonlinearity values that are less than $2^{n-1} - 2^{\frac{n}{2}-1}$, which are divisible by $2^{m+1+\lfloor \frac{n-m-2}{d-1} \rfloor}$ (or $2^{m+1+\lfloor \frac{n-m-r-2}{d-1} \rfloor}$ for the second part). □

4.3 Further Results

In this section we will prove some results concerning Boolean functions. We will prove a necessary condition on the Walsh spectrum of a Boolean function. In order to prove this result, we have to prove several propositions and lemmas. The following proposition will be necessary.

Proposition 4.3.1. *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a balanced Boolean function with even $n \geq 6$. If $nl(f) = 2^{n-1} - 2^{\frac{n}{2}-1} - 2$ then degree d of f is $n-1$.*

Proof: Let f be a balanced Boolean function of n variables with $nl(f) = 2^{n-1} - 2^{\frac{n}{2}-1} - 2$, with degree d. $d < n$ since f is balanced by Remark 3.3.6. If $d \leq n-2$ then $4 \mid nl(f)$ by Theorem 4.2.7. Since $4 \nmid 2^{n-1} - 2^{\frac{n}{2}-1} - 2$ for $n \geq 6$, we deduce $d > n-2$. This completes the proof. □

Remark 4.3.2. Above proposition is not true for $n = 4$. Consider the function $f : \mathbb{F}_2^4 \to \mathbb{F}_2$:

$$f = x_2x_3 \oplus x_2x_4 \oplus x_3x_4 \oplus 1$$

Not depending on x_1, f is balanced. Observe that the algebraic degree of f is $d = 2$; while one can check that $nl(f) = 2^3 - 2^1 - 2 = 4$.

We will need the following simple lemma concerning sum of subsets of an integer multi-set.

Lemma 4.3.3. *Let $A = \{*z_1, \ldots, z_n*\}$, $z_i \in \mathbb{Z}$ be a multi-set. Let the subset sum S_X be defined on the subsets $X \subseteq A$ as:*

$$S_X = \begin{cases} 0 & if\ X = \emptyset, \\ \sum_{x \in X} x & otherwise. \end{cases}$$

Then

$$|\{X \subseteq A \mid S_X\ is\ even\}| = \begin{cases} 2^{n-1} & if\ \exists z_i \in A\ s.t.\ z_i\ is\ odd, \\ 2^n & otherwise. \end{cases}$$

Proof: If all $z_i \in A$ are even, then, being sum of even numbers or 0, all S_X are even. Otherwise let A_E and A_O be the even and odd parts of A respectively, satisfying $A_E \cup A_O = A$ and $A_E \cap A_O = \emptyset$, with $|A_O| = m > 0$. All $X \subseteq A$ are from the set:

$$\mathscr{P}(A_E) \times \mathscr{P}(A_O)$$

Writing any X as $X = X_E \cup X_O$, with $X_E \in A_E$ and $X_O \in A_O$, the subset sum of X is $S_X = \sum_{x \in X_E} x + \sum_{x \in X_O} x$. Observe that all subsets X_E of A_E have even subset sums. Then, the claim is true if and only if half of the subsets of A_O have odd subset sums and half of the subsets of A_O have even subset sums. But we know that only the sum of an odd number of odd numbers is odd. That is, exactly $\sum_{j=1 \mid j\ is\ odd}^{m} \binom{m}{j} = 2^{m-1}$ subsets of A_O have odd subset sums. The number is half of 2^m, the number of all subsets of A_O, and the result follows. □

Lemma 4.3.4. *Let $A = \{*z_1, \ldots, z_n*\}$, $z_i \in \mathbb{Z}$ be a multi-set, and o_A denote the number*

of odd entries in A, that is:

$$o_A = |\{z_i \in A \mid z_i \ is\ odd\}|$$

If $o_A = 0$, *then*

$$\begin{aligned}
|\{X \subseteq A \mid |X| \ is\ odd\ and\ S_X\ is\ odd\}| &= 0,\\
|\{X \subseteq A \mid |X| \ is\ odd\ and\ S_X\ is\ even\}| &= 2^{n-1},\\
|\{X \subseteq A \mid |X| \ is\ even\ and\ S_X\ is\ odd\}| &= 0,\\
|\{X \subseteq A \mid |X| \ is\ even\ and\ S_X\ is\ even\}| &= 2^{n-1};
\end{aligned}$$

if $o_A = n$, *then*

$$\begin{aligned}
|\{X \subseteq A \mid |X| \ is\ odd\ and\ S_X\ is\ odd\}| &= 2^{n-1},\\
|\{X \subseteq A \mid |X| \ is\ odd\ and\ S_X\ is\ even\}| &= 0,\\
|\{X \subseteq A \mid |X| \ is\ even\ and\ S_X\ is\ odd\}| &= 0,\\
|\{X \subseteq A \mid |X| \ is\ even\ and\ S_X\ is\ even\}| &= 2^{n-1};
\end{aligned}$$

if $0 < o_A < n$, *then*

$$\begin{aligned}
|\{X \subseteq A \mid |X| \ is\ odd\ and\ S_X\ is\ odd\}| &= 2^{n-2},\\
|\{X \subseteq A \mid |X| \ is\ odd\ and\ S_X\ is\ even\}| &= 2^{n-2},\\
|\{X \subseteq A \mid |X| \ is\ even\ and\ S_X\ is\ odd\}| &= 2^{n-2},\\
|\{X \subseteq A \mid |X| \ is\ even\ and\ S_X\ is\ even\}| &= 2^{n-2}.
\end{aligned}$$

Proof: If $o_A = 0$, then all subset sums are even. For half of $X \subseteq A$, $|X|$ is odd. If $o_A = n$, then S_X is odd if and only if $|X|$ is odd. Recall that only the sum of an odd number of odd numbers is odd. If $0 < o_A < n$, then let, as in the previous lemma,

$A = A_E \cup A_O$ and $A_E \cap A_O = \emptyset$, with $|A_O| = m > 0$ and $|A_E| = n - m > 0$. Let $\mathscr{P}_O(A)$ be the subsets of A with odd cardinality, and $\mathscr{P}_E(A)$ be the subsets of A with even cardinality. $\mathscr{P}_O(A) = \mathscr{P}_O(A_E) \times \mathscr{P}_E(A_O) \cup \mathscr{P}_E(A_E) \times \mathscr{P}_O(A_O)$, and S_X is odd for the former and S_X is even for the latter. $|\mathscr{P}_O(A_E) \times \mathscr{P}_E(A_O)| = |\mathscr{P}_E(A_E) \times \mathscr{P}_O(A_O)| = 2^{n-2}$. $\mathscr{P}_E(A) = \mathscr{P}_O(A_E) \times \mathscr{P}_O(A_O) \cup \mathscr{P}_E(A_E) \times \mathscr{P}_E(A_O)$, and S_X is odd for the former and S_X is even for the latter. $|\mathscr{P}_O(A_E) \times \mathscr{P}_O(A_O)| = |\mathscr{P}_E(A_E) \times \mathscr{P}_E(A_O)| = 2^{n-2}$. □

Theorem 4.3.5. *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function. Consider the multi-set $\mathscr{W} = \{* W_{\hat{f}}(u) \mid u \in \mathbb{F}_2^n *\}$. Then*

- *If $d = n - 1$, exactly half of the elements of $\mathscr{W}$ is divisible by 8, and half of the elements w_i of $\mathscr{W}$ satisfy $w_i \equiv 4 \bmod 8$.*
- *If $d < n - 1$, all of the elements of $w_i \in \mathscr{W}$ satisfy $w_i \equiv k \pmod 8$. With $k = 4$ or $k = 0$, depending on $\lambda_{11\cdots1}$.*
- *If $d = n$, let r be the terms in ANF with degree $d - 1$.*
  - *if $r = 0$, exactly half of the elements w_i of $\mathscr{W}$ satisfy $w_i \equiv 2 \bmod 8$, and half of the elements w_i of $\mathscr{W}$ satisfies $w_i \equiv 6 \bmod 8$,*
  - *if $r = n$, all of the elements of $w_i \in \mathscr{W}$ satisfy $w_i \equiv k \pmod 8$. With $k = 6$ or $k = 2$, depending on $\lambda_{11\cdots1}$,*
  - *otherwise exactly half of the elements w_i of $\mathscr{W}$ satisfy $w_i \equiv 2 \bmod 8$, and half of the elements w_i of $\mathscr{W}$ satisfy $w_i \equiv 6 \bmod 8$.*

Proof: Let $\Lambda_w = \{* \lambda_i \mid \mathrm{wt}(i) = w *\}$ be the multi-set of NNF coefficients with weight w of f. In the following formula, let $X_w \subseteq \Lambda_w$ for $0 \leq w < n$, and S_{X_w} be

the subset sum of the given subset. The Walsh transform of f at a can be written as:

$$W_f(a) = (-1)^{\mathrm{wt}(a)} \left[\lambda_{1\cdots 1} + 2S_{X_{n-1}} + 2^2 S_{X_{n-2}} + \cdots + 2^n S_{X_0}\right]$$

where $X_w \subseteq \Lambda_w$ for $0 \leq w < n$ is completely determined by:

$$X_w = \{\lambda_i \mid \mathrm{wt}(i) = w \; and \; i \succeq a\}$$

Hence, for each $a \in \mathbb{F}_2^n$ there corresponds a unique $X_w \in \mathscr{P}(\Lambda_w)$. Observe $\lambda_{1\cdots 1}$ is even since $d = n-1$. Then Lemma 4.3.3 and the fact $-k \equiv k \pmod 4$ if and only if $k = 0$ or $k = 2$ assures us $W_f(a) \equiv 0 \pmod 4$ for half of $a \in \mathbb{F}_2^n$ and $W_f(a) \equiv 2 \pmod 4$ for (the other) half of $a \in \mathbb{F}_2^n$. Recall that $W_{\hat{f}}(a) = 2^n \delta_0(a) - 2W_f(a)$ by Theorem 3.2.4. Observe that $W_{\hat{f}}(a) \equiv 4 \pmod 8 \iff W_f(a) \equiv 2 \pmod 4$ and $W_{\hat{f}}(a) \equiv 0 \pmod 8 \iff W_f(a) \equiv 0 \pmod 4$ whenever $n \geq 3$.

Moreover, if $d < n-1$, Lemma 4.3.3 implies for all $a \in \mathbb{F}_2^n$, $W_f(a) \equiv 0 \pmod 8$ or $W_f(a) \equiv 4 \pmod 8$, depending on $\lambda_{1\cdots 1}$.

Now let $d = n$. Assume n is even:

(1) $W_f(a) \equiv k \pmod 4$, if $\mathrm{wt}(a)$ is odd and $S_{X_{n-1}}$ is odd,

(2) $W_f(a) \equiv -k \pmod 4$, if $\mathrm{wt}(a)$ is odd and $S_{X_{n-1}}$ is even,

(3) $W_f(a) \equiv -k \pmod 4$, if $\mathrm{wt}(a)$ is even and $S_{X_{n-1}}$ is odd,

(4) $W_f(a) \equiv k \pmod 4$, if $\mathrm{wt}(a)$ is even and $S_{X_{n-1}}$ is even.

If $r = 0$, by Lemma 4.3.4 $W_f(a) = -k$ for 2^{n-1} a's (2) and $W_f(a) = k$ for 2^{n-1} a's (4).

If $r = n$, by Lemma 4.3.4 $W_f(a) = k$ for 2^n a's (1),(4).

If $0 < r < n$, by Lemma 4.3.4 $W_f(a) = -k$ for 2^{n-1} a's (2),(3) and $W_f(a) = k$ for 2^{n-1} a's (1),(4). Assume n is odd:

(1) $W_f(a) \equiv -k \pmod 4$, if $\mathrm{wt}(a)$ is odd and $S_{X_{n-1}}$ is odd,

(2) $W_f(a) \equiv k \pmod 4$, if $\mathrm{wt}(a)$ is odd and $S_{X_{n-1}}$ is even,

(3) $W_f(a) \equiv k \pmod 4$, if $\mathrm{wt}(a)$ is even and $S_{X_{n-1}}$ is odd,

(4) $W_f(a) \equiv -k \pmod 4$, if $\mathrm{wt}(a)$ is even and $S_{X_{n-1}}$ is even.

If $r = 0$, by Lemma 4.3.4 $W_f(a) = k$ for 2^{n-1} a's (2) and $W_f(a) = -k$ for 2^{n-1} a's (4).

If $r = n$, by Lemma 4.3.4 $W_f(a) = -k$ for 2^n a's (1),(4).

If $0 < r < n$, by Lemma 4.3.4 $W_f(a) = k$ for 2^{n-1} a's (2),(3) and $W_f(a) = -k$ for 2^{n-1} a's (1),(4). □

Following is a naïve try to show the inexistence of balanced Boolean functions with nonlinearity equal to $2^{n-1} - 2^{\frac{n}{2}-1} - 2$. Recall that maximum possible nonlinearity for balanced functions can be reached only if $d = n-1$. And if $d = n-1$, then Walsh spectrum coefficients have some restrictions.

Proposition 4.3.6. *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function with even n. Then $nl(f) = 2^{n-1} - 2^{\frac{n}{2}-1} - 2$ only if*

$$\sum_{i=1}^{2^{n-1}} (8a_i + 4)^2 + (8b_i)^2 = 2^{2n}$$

with $0 \le a_i, b_i \le 2^{\frac{n}{2}-3}$. Or equally:

$$\sum_{i=1}^{2^{n-1}} a_i^2 + a_i + b_i^2 = 2^{2n-6} - 2^{n-3}$$

Proof: For f to reach nonlinearity $2^{n-1} - 2^{\frac{n}{2}-1} - 2$, maximum Walsh spectrum absolute value can be $2^{\frac{n}{2}} + 4$. Result follows from Theorem 4.3.5. □

CHAPTER 5

CONCLUSION

In the thesis, we study the Numerical Normal Form of Boolean functions, first presented by Carlet and Guillot in 1999. We study the properties of NNF, its pairwise relations with other representations, characterization of several functions. We also study its Möbius inversion relations on the partially ordered set where the functions are defined using Gian-Carlo Rota's work. We review the results of Carlet and Guillot with detailed proofs.

NNF can be seen as a generalization of the Algebraic Normal Form from the field with two elements, to the set of integers. With NNF, we see that generalization of several properties, for instance Siegenthaler's inequality, are possible. Moreover, several results concerning the Walsh spectrum of resilient functions are studied in this work, again recovering material written by Carlet in 2002.

NNF proved to be a good analytical tool for studying Boolean functions. We exemplify this by proving a simple result, Theorem 4.3.5, on the Walsh spectrum coefficients of Boolean functions.

REFERENCES

[1] CAMION, P., CARLET, C., CHARPIN, P., AND SENDRIER, N. On correlation-immune functions. In *CRYPTO '91* (Santa Barbara, USA, 1992), no. 576 in Lecture Notes in Computer Science, pp. 86–100.

[2] CARLET, C. On the coset weight divisibility and nonlinearity of resilient and correlation-immune functions. In *Proceedings of the 2nd international conference (SETA'01) Discrete Mathematics and Theoretical Computer Science* (1999), pp. 131–144.

[3] CARLET, C., AND GUILLOT, P. A new representation of boolean functions. In *Proceedings of AAECC'13* (1999), no. 1719 in Lecture Notes in Computer Science.

[4] CARLET, C., AND GUILLOT, P. Bent, resilient functions and the numerical normal form. *DIMACS Series in Discrete Mathematics and Theoretical Computer Science 56* (2001), 87–96.

[5] DILLON, J. F. *Elementary Hadamard Difference Sets.* PhD thesis, University of Maryland, 1974.

[6] HALL JR., M. *Combinatorial Theory,* 2nd ed. Wiley, New York, 1986.

[7] JANSEN, C. J. A. *Investigations on Nonlinear Streamcipher Systems: Construction and Evaluation Methods.* Philips, 1989.

[8] KUNG, J. P. S. *A Source Book in Matroïd Theory.* Birkhäuser, 1986.

[9] MACWILLIAMS, F. J., AND SLOANE, N. *The theory of error correcting codes*. North Holland, Amsterdam, 1977.

[10] ROTA, G.-C. *On the foundations of Combinatorial Theory*. Springer Verlag, 1964. reprint in [8].

[11] ROTHAUS, O. S. On "bent" functions. *Journal of Combinatorial Theory 20A* (1976), 300–305.

[12] SIEGENTHALER, T. Correlation-immunity of nonlinear combining functions for cryptographic applications. *IEEE Transactions on Information Theory IT 30*, 5 (1984), 776–780.

[13] XIAO, G.-Z., AND MASSEY, J. L. A spectral characterization of correlation immune combining functions. *IEEE Transactions on Information Theory IT 34*, 3 (1988), 569–571.