Università degli Studi di Trento

DIPARTIMENTO DI MATEMATICA

Corso di Dottorato di Ricerca in Matematica

XXXII CICLO

A thesis submitted for the degree of Doctor of Philosophy

Some cryptographic properties of Boolean functions

Ph.D. Candidate:
Augustine Musukwa

Supervisor:
Prof. Massimiliano Sala

December 2019

Università degli Studi di Trento

DIPARTIMENTO DI MATEMATICA

Corso di Dottorato di Ricerca in Matematica

XXXII CICLO

Some cryptographic properties of Boolean functions

Ph.D. Candidate : ______________________________
Augustine Musukwa

Supervisor : ______________________________
Prof. Massimiliano Sala

Head of Ph.D. School : ______________________________
Prof. Stefano Bonaccorsi

December 2019

Abstract

We investigate some cryptographic properties of Boolean functions. Some of the properties we are going to consider include weight, balancedness, nonlinearity and resiliency. Mainly, we study how the properties of a Boolean function can be related to the properties of some other functions in a lower dimension. We utilise these relations to construct balanced and resilient functions. Another aspect which we consider is the set of linear structures of Boolean functions. Our interest is in construction of balanced functions which have a trivial set of linear structures.

It is well-known that block ciphers may suffer from two main attacks, namely, differential attacks and linear attacks. APN functions are known to provide the best resistance against differential attacks. We look at some properties of APN functions in even dimension. We study the linear structures of their components. We show that there must be at least a component whose set of linear structures is trivial. In particular, we determine the possible size of the set of linear structures for any component of an APN permutation. Based on the sizes of the sets of linear structures for the components, we establish a simple characterization of quadratic APN functions, and this knowledge is useful in proving some results on a general form for the number of bent components. We further consider counting bent components in any quadratic power functions.

Based on the behaviour of second order derivatives, we derive some quantities which are used for characterization of quadratic and cubic APN functions. We show that these quantities can also be used to characterize quadratic and cubic Bent functions. Furthermore, we show that these derived quantities can be linked to the size of the set of linear structures for any quadratic and cubic partially-bent functions.

Acknowledgements

First and foremost, I would like to thank Almighty God for good health during the whole time I was pursuing my studies and for the gift of life.

Second, I would like to express my profound gratitude to my supervisor Prof. Massimiliano Sala for the continuous support, guidance, encouragement and motivation given to me throughout my Ph.D. studies. His patience, insightful comments, scientific knowledge and professionalism made it possible for me to progress with my studies and be able to find some new results. I am so grateful that he was accessible when I needed his attention, gave me hope whenever I was down with my work, constructively and positively criticised my work, made the working environment favourable and gave me an opportunity for teaching experience. I am so proud and delighted to have done my thesis under his supervision.

I also extend my appreciation to Prof. Claude Carlet for suggesting to me some potential areas of research, in a private conversation, when we meet at BFA 2018 conference in Norway.

My deepest gratitude also goes to my beloved wife, Lelani, for her support, encouragement, understanding, patience and prayers during the whole time I was away from her pursuing my studies. Her love and constant communication made me emotionally and socially stable. She certainly felt, in one way or another, all the ups and downs I was going through during my studies. I am so grateful that she was there for me in all circumstances.

I am grateful to my brother Steve (Mwalawila) for his support, words of encouragement and inspiration all through the crucial stages of my education. During my

Ph.D. studies he always made sure I was okay. I, genuinely, appreciate for his wishes and efforts that I study to this far.

I owe my parents (Wedson and Veliness) a debt of gratitude for their endless support, prayers and unconditional love over the years. Without them, there is no way I could have gotten where I am today. At every stage of my education, they always supported, encouraged and wished me well. I am grateful for everything and proud to be their son.

Finally, I would like to thank the administration of Mzuzu University for granting me a study leave and providing me with "to and fro" air-ticket from Malawi (my home country) to Italy.

Contents

Introduction

We are going to consider the mappings from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, for positive integers n and m. These functions are called Boolean functions (or n-Boolean functions) if $m = 1$ and they are called vectorial Boolean functions if $m > 1$. They are widely studied and applied in coding theory, cryptography and other fields. In this thesis, we study them in relation to their cryptographic properties. The properties of (vectorial) Boolean functions play a critical role in cryptography, particularly in the design of symmetric key algorithms in block cipher, nonlinear filters and combiners in stream ciphers. Some authors refer vectorial Boolean functions to as substitution-boxes (S-boxes) or multi-output Boolean functions.

Differential and linear cryptanalysis are the most well-known and efficient attacks against block ciphers. The underlying vectorial Boolean functions need to satisfy some desirable properties, such as the differential uniformity and nonlinearity, in order for the cryptosystem to be resistible to such attacks. Functions with high nonlinearity have better resistance with respect to linear attack and those with low differential uniformity have better resistance with respect to differential attacks.

A vectorial Boolean function with differential uniformity two is optimal. Any function which attains this value is said to be Almost Perfect Nonlinear (APN). It is well-known that $2^{n-1} - 2^{\frac{n-1}{2}}$ is an upper bound on the nonlinearity of vectorial Boolean function from $\mathbb{F}_2^n$ to itself and the functions achieving this optimal nonlinearity are called Almost Bent (AB).

Balancedness is another aspect sought in cryptographic Boolean functions and many authors have studied balanced Boolean functions with respect to their desired cryptographic properties. Cryptographic Boolean functions should satisfy various criteria simultaneously, mainly balancedness, high nonlinearity and good autocorrelation properties, to resist linear cryptanalysis and differential cryptanalysis particularly. Generally, it is a difficult task to find a function with properties which are necessary for a cryptosystem to possess robust resistance against most of the known attacks. Thus, in some way, a compromise (trade off) is needed when picking a function of good cryptographic properties. For instance, bent functions [the functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ which achieve the upper bound $2^{n-1} - 2^{n/2-1}$ on the nonlinearity when n is even] have high nonlinearity but unfortunately they do not possess other desirable cryptographic properties. Among other properties, bent funtions are not balanced, not resilient and their algebraic degrees cannot exceed $n/2$.

Now we give an outline how this thesis is organised. Chapter 1 reports some known results which form the foundation for what is being studied (all preliminaries are included in this chapter). Our work is presented in Chapters 2, 3 and 4. In Chapter 2, we are mainly concerned with weight, balancedness, linear structures, resiliency and nonlinearity of Boolean functions. In Section 2.1, we show how the weight of any Boolean function can be related to the weights of some other functions in a lower dimension, we prove some results on weight of "splitting" functions and a special class of cubic Boolean functions, and we provide an algorithm which can be used to compute the weight of any cubic Boolean function. In Section 2.2, we construct balanced Boolean functions and determine those which have trivial linear space (the set of linear structures) and in Section 2.3, we construct resilient functions with respect to monotone sets. In Section 2.4, we give an inequality relation which relates the nonlinearity of any Boolean function to the nonlinearity of some functions in a lower dimension.

In Chapter 3, we derive some quantities based on the behaviour of second derivatives of Boolean functions and we show that these quantities can be used for characterization of quadratic and cubic APN functions. In Chapter 4, we focus our attention on components of APN and quadratic power functions in even dimension. In Section 4.1, we show that any APN function possess at least one component whose linear space is trivial. In Section 4.2, we establish a simple characterization of quadratic

APN functions based on the dimensions of linear spaces of their components and we utilize this knowledge to prove a general form for the number of bent components. Lastly, in Section 4.3, we determine the number of bent components in any quadratic power function.

NB: Any result in Chapters 2, 3 and 4 in this thesis which does not have a direct citation is my own.

Chapter 1

Preliminaries

In this chapter, we report the results which form the foundation for this thesis. The first section presents some definitions and results related to Boolean functions and in the second section we talk about some results in vectorial Boolean functions.

1.1 Boolean functions

In this section, we report some definitions and well-known results on Boolean functions and in case more details are sought, the reader is referred to [3, 4, 8, 11, 15, 16, 17, 24, 27, 37, 49].

1.1.1 Some definitions and notations

In this thesis, the field with two elements, 0 and 1, is denoted by $\mathbb{F}$ (other authors use $\mathbb{F}_2$ or $\mathbb{Z}_2$). We use n or m to represent a natural number. Let $\mathbb{F}^n$ be the n-dimensional vector space defined over the finite field $\mathbb{F}$. Any vector in $\mathbb{F}^n$ is denoted by v (instead of commonly used notations such as $\vec{v}$ or $\mathbf{v}$). The all-one vector is denoted by $\mathbf{1} = (1, 1, .., 1)$ and the all-zero vector is denoted by $\mathbf{0} = (0, 0, ..., 0)$. The vector with coordinate 1 at ith position and 0 elsewhere is denoted by e_i. We loosely use ordinary addition $+$ for XOR sum $\oplus$. For any two vectors $v = (v_1, ..., v_n)$ and $w = (w_1, ..., w_n)$ in $\mathbb{F}^n$, a dot product of v and w is given by $v \cdot w = \sum_{i=1}^{n} v_i w_i$.

For any two binary vectors $x = (x_1, ..., x_n)$ and $y = (y_1, ..., y_n)$ in $\mathbb{F}^n$, we define the sets $\mathrm{sup}(x) = \{i \mid x_i \neq 0\}$ (it is commonly called *support* of x) and $\delta(x, y) = \{i \mid x_i \neq y_i\}$. The size of a set A is denoted by $|A|$. We define the *Hamming weight* of the binary vector x as $\mathrm{w}(x) = |\,\mathrm{sup}(x)|$ and the *Hamming distance* between the two binary vectors x and y is defined as $\mathrm{d}(x, y) = |\delta(x, y)| = |\,\mathrm{sup}(x + y)|$.

A *Boolean function* is any function f from $\mathbb{F}^n$ to $\mathbb{F}$. The set of all Boolean functions is denoted by B_n. If $f \in B_n$ depends on m variables only, with $m < n$, then we denote its restriction to $\mathbb{F}^m$ by $f_{\restriction \mathbb{F}^m}$. Clearly, we have $f_{\restriction \mathbb{F}^m} \in B_m$. The support of $f \in B_n$ is defined as $\mathrm{sup}(f) = \{x \in \mathbb{F}^n \mid f(x) \neq 0\}$. The *weight* of f is defined as $\mathrm{w}(f) = |\,\mathrm{sup}(f)|$ and the *distance* between f and g is given by $\mathrm{d}(f, g) = \mathrm{w}(f + g)$. A Boolean function f is called *balanced* if $\mathrm{w}(f) = 2^{n-1}$. An image of a function f is denoted by $\mathrm{Im}(f)$, that is, $\mathrm{Im}(f) = \{f(x) \mid x \in \mathbb{F}^n\}$.

1.1.2 Representation of Boolean functions

We describe four representations of Boolean functions which are used in coding and cryptography.

The algebraic normal form

The most used representation of any Boolean function f is the algebraic normal form (ANF for short) which is the n-variable polynomial representation over $\mathbb{F}$ given by

$$f(x_1, ..., x_n) = \sum_{u \in \mathbb{F}^n} a_u \left(\prod_{i=1}^{n} x_i^{u_i} \right) = \sum_{u \in \mathbb{F}^n} a_u x^u,$$

where $a_u \in \mathbb{F}$ and $x^u = \prod_{i=1}^{n} x_i^{u_i}$ is the monomial in $\mathbb{F}[x_1, ..., x_n]/(x_1^2 + x_1, ..., x_n^2 + x_n)$. The *algebraic degree* (or simply *degree*) of f, denoted by $\deg(f)$, is the maximal value of the weight of u such that $a_u \neq 0$ in ANF, that is, $\deg(f) = \max_{a_u \neq 0} \mathrm{w}(u)$. In [19], it is shown that ANF exists and is unique.

A Boolean function f is called *linear* if $\deg(f) \leq 1$ and $f(0) = 0$. Alternatively, for any $a \in \mathbb{F}^n$, we define a linear function, denoted l_a, as $l_a(x) = a \cdot x$. A Boolean function is called *affine* if its degree is less than or equal to 1. In other words, affine functions are either linear functions or their complements, both denoted by $\varphi_a(x) = l_a(x) + c$, where $a \in \mathbb{F}^n$ and $c \in \mathbb{F}$. The set of all affine functions is denoted by A_n. Since $a \in \mathbb{F}^n$ and $c \in \mathbb{F}$ have no constraints in the definition of affine functions, so $|A_n| = 2 \cdot 2^n = 2^{n+1}$. A Boolean function is *quadratic* if its degree is 2 and *cubic* if its degree is 3.

The Truth-Table

Any Boolean function f can also be represented by the Truth Table, which gives the value of f at all of 2^n vectors in $\mathbb{F}^n$.

Let $\mathbb{F}^n = \{P_0, ..., P_{2^n-1}\}$, where P_i is a vector corresponding to binary expansion of i and let $f \in B_n$. Then the *Truth Table (TT)* of f is given by the value vector $\mathrm{TT}_f = (f(P_0), ..., f(P_{2^n-1}))$. It is clear that the length of TT_f is 2^n.

For instance, when $n = 3$, we can have a Boolean function f which corresponds to the following TT:

x_1	0	0	0	0	1	1	1	1
x_2	0	0	1	1	0	0	1	1
x_3	0	1	0	1	0	1	0	1
TT_f	0	1	0	1	0	1	1	0

Table 1: Truth Table

Since each coordinate of the vector TT_f arbitrarily takes any element of $\mathbb{F}$, then clearly there are 2^{2^n} Boolean functions.

The ANF can be computed directly from the TT with a complexity of $O(n2^n)$ operations by *Butterfly Algorithm* (sometimes known as *Fast Möbius Transform)* and vice versa.

The Fourier spectrum

The Fourier transform of a Boolean function f is defined by

$$\mathcal{F}_f(a) = \sum_{x \in \mathbb{F}^n} f(x)(-1)^{a \cdot x}.$$

The *Fourier spectrum* of a Boolean function f is the data/list of all the values of $\mathcal{F}_f(a)$, $a \in \mathbb{F}^n$, that is, the multi-set $\{\mathcal{F}_f(a), a \in \mathbb{F}^n\}$. The Fourier spectrum can also be considered as a representation of Boolean functions (see [18]). It can also be computed from the TT by a Butterfly algorithm.

The numerical normal form

For this representation of Boolean functions, we use [18, 19] as our standard reference.

Definition 1. *Let f be a real-valued function on $\mathbb{F}^n$. We call* Numerical Normal Form (NNF) *of f, the following expression of f as a polynomial with real coefficients:*

$$f(x_1, ..., x_n) = \sum_{I \in \mathcal{P}(N)} \lambda_I \left(\prod_{i \in I}^{n} x_i \right) = \sum_{I \in \mathcal{P}(N)} \lambda_I x^I, \tag{1.1}$$

where $\mathcal{P}(N)$ denotes the power set of $N = \{1, ..., n\}$.

The NNF is another representation of Boolean functions over the reals. We call the (global) degree of the NNF of a function its *numerical degree.* When NNF coefficients are taken modulo 2, they correspond to the ANF coefficients, that is:

$$a_I = \lambda_I \pmod 2.$$

Since the ANF is the modulo 2 version of the NNF, so the numerical degree is at least the algebraic degree.

The ANF of any Boolean function can be deduced from its NNF by reducing it modulo 2. Also NNF can be deduced from ANF. This is the case since we have

$$\begin{aligned} f(x) = \sum_{I \in \mathcal{P}(N)} a_I x^I &\iff (-1)^{f(x)} = \prod_{I \in \mathcal{P}(N)} (-1)^{a_I x^I} \\ &\iff 1 - 2f(x) = \prod_{I \in \mathcal{P}(N)} (1 - 2a_I x^I). \end{aligned} \tag{1.2}$$

Expanding the product in the last equality we obtain:

$$\prod_{I \in \mathcal{P}(N)} (1 - 2a_I x^I) = 1 + \sum_{k=1}^{2^n} (-2)^k \sum_{\substack{\{I_1, ..., I_k\} | \\ I_1 \cup \cdots \cup I_k = I}} a_{I_1} \cdots a_{I_k} x^I.$$

where "$\{I_1, ..., I_k\} | I_1 \cup \cdots \cup I_k = I$" means that the multi-indices $I_1, ..., I_k$ are all distinct, in indefinite order, and that their union equals I.

So, using Equation 1.2, we obtain the NNF as

$$f(x) = \sum_{k=1}^{2^n} (-2)^{k-1} \sum_{\substack{\{I_1, ..., I_k\} | \\ I_1 \cup \cdots \cup I_k = I}} a_{I_1} \cdots a_{I_k} x^I$$

from which we deduce that

$$\lambda_I = \sum_{k=1}^{2^n} (-2)^{k-1} \sum_{\substack{\{I_1, ..., I_k\} | \\ I_1 \cup \cdots \cup I_k = I}} a_{I_1} \cdots a_{I_k}. \tag{1.3}$$

Transformation from ANF to NNF can be accomplished by making use of the following conversion between binary and integer arithmetic:

$$a \oplus b = a + b - 2ab.$$

1.1.3 Reed-Muller codes

Reed-Muller codes are named after I.S. Reed and D.E. Muller who introduced them. These codes can be defined over $\mathbb{F}_q$ (a field of q elements) but we confine ourselves to the binary case, that is, when $q = 2$. In binary case, Read-Muller codes are easily defined in terms of Boolean functions and some authors, for this reason, consider Reed-Miller codes as another representation of Boolean functions.

Definition 2 (Reed-Muller codes)**.** *Let $n \in \mathbb{N}$ and r be an integer such that $0 \leq r \leq n$. The* r-th order binary Reed-Muller code *of length 2^n, denoted by $R(r, n)$, is the set of the value vectors of the all Boolean functions in B_n with degree at most r:*

$$R(r, n) = \{\mathrm{TT}_f \mid f \in B_n, \deg(f) \leq r\}.$$

In particular, $R(0, n)$ is composed of all-zero and the all-one 2^n-bit words, $R(1, n) = A_n$ and $R(n, n)$ contains all 2^n-bit words (i.e., $R(n, n) = \mathbb{F}^{2^n} = B_n$).

Next, we state some well-known properties satisfied by Reed-Muller codes.

Proposition 3. *Let $n \in \mathbb{N}$ and r be an integer such that $0 \leq r \leq n$.*

1. *$R(r, n)$ is a linear code,*

2. *The value vectors of all monomials of degree at most r form a basis of $R(r, n)$,*

3. $\dim R(r, n) = \sum_{i=0}^{r} \binom{n}{i}$,

4. *$R(r - 1, n) \subset R(r, n)$.*

1.1.4 Equivalence of Boolean functions

We earlier saw that $|B_n| = 2^{2^n}$, so it can be appreciated that the number of Boolean functions of n variables increases so fast with a minor increase in size of n. This makes it so difficult to find functions with good cryptographic properties such as balancedness, resiliency, high nonlinearity, etc. Equivalence relations, under which some cryptographic properties are invariant, are essential tools which help us to avoid examining all the Boolean functions.

Next, we give definitions of some equivalences which are commonly used in studying different properties in cryptography.

Definition 4. *Let $g, h \in B_n$ be related by $g(x) = h(Ax+a)+b\cdot x+c$, where $a, b \in \mathbb{F}^n$, $c \in \mathbb{F}$ and A is an $n \times n$ nonsingular matrix. We say that g and h are:*

1. affine equivalent *if $b = 0$ and $c = 0$ and we write $g \sim_A h$,*
2. affine equivalent modulo constant *if $b = 0$ and we write $g \sim_{A'} h$,*
3. extended-affine equivalent *for any b and c and we write $g \sim_{EA} h$,*
4. inequivalent *if no such transformation exists.*

We rewrite the first part of Definition 4 by using some notations which will often be used. Functions $g, h : \mathbb{F}^n \to \mathbb{F}$ are said to be affine equivalent if there exist an affinity $\varphi : \mathbb{F}^n \to \mathbb{F}^n$ such that $g = h \circ \varphi$. For $1 \leq i \leq n$ and $l \in A_{n-1}$, a *basic affinity* of $\mathbb{F}^n$ maps $x_i \mapsto x_i + l(x_1, ..., x_{i-1}, x_{i+1}, ..., x_n)$ and fixes all other coordinates.

Remark 5. The relations $\sim_A$, $\sim_{A'}$, and $\sim_{EA}$ are obviously equivalence relations, and if $f, g \in B_n$, then $f \sim_A g \Rightarrow f \sim_{A'} g \Rightarrow f \sim_{EA} g$.

We next present in the following proposition that weight and degree of a Boolean function are invariant under the equivalence defined.

Proposition 6. *Let $g, f \in B_n$. Then*

(i) $f \sim_A g \Rightarrow \mathrm{w}(f) = w(g)$,

(ii) $f \sim_A g \Rightarrow \deg(f) = \deg(g)$,

(iii) $f \sim_{A'} g \Rightarrow \deg(f) = \deg(g)$ *if* $f, g \neq 0, 1$,

(iv) $f \sim_{EA} g, \deg(f), \deg(g) \geq 2 \Rightarrow \deg(f) = \deg(g)$.

We present the theorem on classification of quadratic Boolean functions, via affine equivalence, whose proof can be found in [37] page 438.

Theorem 7 (Classification Theorem for Quadratics)**.** *Let $f \in B_n$ be a quadratic Boolean function. Then*

(i) $f \sim_A x_1x_2 + \cdots + x_{2i-1}x_{2i} + x_{2i+1}$, *with* $i \leq \lfloor \frac{n-1}{2} \rfloor$, *if f is balanced,*

(ii) $f \sim_A x_1x_2 + \cdots + x_{2i-1}x_{2i} + c$, *with* $i \leq \lfloor \frac{n}{2} \rfloor$ *and* $c \in \mathbb{F}$, *if f is unbalanced.*

1.1.5 Autocorrelation function

Definition 8. *The* correlation *(also called* bias or imbalance*) of a Boolean function f is*

$$\mathcal{F}(f) = \sum_{x \in \mathbb{F}^n} (-1)^{f(x)}.$$

Lemma 9. *For any $f \in B_n$, we have*

$$\mathcal{F}(f) = 2^n - 2\mathrm{w}(f).$$

Proof. We have

$$\mathcal{F}(f) = |\{x \in \mathbb{F}^n \mid f(x) = 0\}| - |\{x \in \mathbb{F}^n \mid f(x) = 1\}| = 2^n - 2|\{x \in \mathbb{F}^n \mid f(x) = 1\}|.$$

Since $\mathrm{w}(f) = |\{x \in \mathbb{F}^n \mid f(x) = 1\}|$, we have the result. □

Remark 10. *In other words, Lemma 9 says that*

$$\mathrm{Pr}_X[f(X) = 1] = \frac{\mathrm{w}(f)}{2^n} = \frac{1}{2}\left(1 - \frac{\mathcal{F}(f)}{2^n}\right).$$

Observe that $\mathcal{F}(f) = 0$ if and only if f is balanced.

Proposition 11. *Every non-constant affine function is balanced.*

Proof. Recall that $l_a(x) = a \cdot x$ is a linear function and $\varphi_a(x) = l_a(x) + c$, with $c \in \mathbb{F}$, is an affine function. Note that φ_a is a non-constant affine function if a is nonzero. Suppose that $c = 0$, that is, $\varphi_a = l_a = a \cdot x$. Then

$$\begin{aligned} |\{x \in \mathbb{F}^n \mid \varphi_a(x) = 0\}| &= |\{x \in \mathbb{F}^n \mid a \cdot x = 0\}| \\ &= |< a >^{\perp}| \\ &= 2^{n-1} \end{aligned}$$

which implies that $\mathrm{w}(\varphi_a) = \mathrm{w}(l_a) = |\mathbb{F}^n| - |< a >^{\perp}| = 2^{n-1}$.

If $c = 1$ then we have $\mathrm{w}(\varphi_a) = \mathrm{w}(l_a + 1) = 2^n - \mathrm{w}(l_a) = 2^{n-1}$. □

Lemma 12. *Let l_a, with $a \in \mathbb{F}^n$, be a linear function. Then*

$$\mathcal{F}(l_a) = \sum_{x \in \mathbb{F}^n} (-1)^{l_a(x)} = \begin{cases} 2^n & \textit{if } a = 0 \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. Suppose $a = 0$. So

$$\sum_{x \in \mathbb{F}^n} (-1)^{l_a(x)} = \sum_{x \in \mathbb{F}^n} (-1)^{a \cdot x} = \sum_{x \in \mathbb{F}^n} (-1)^0 = \sum_{x \in \mathbb{F}^n} 1 = 2^n.$$

If $a \neq 0$ then $l_a(x) = a \cdot x$ is non-constant and so, by Proposition 11, it is balanced, that is, $\mathcal{F}(l_a) = 0$. □

Lemma 13. *Let $f \in B_n$. Then $\mathcal{F}(f + 1) = -\mathcal{F}(f)$.*

Proof. It is clear that $\mathrm{w}(f + 1) = 2^n - \mathrm{w}(f)$. So we have

$$\mathcal{F}(f + 1) = 2^n - 2\mathrm{w}(f + 1) = 2^n - 2(2^n - \mathrm{w}(f)) = -2^n + 2\mathrm{w}(f) = -\mathcal{F}(f). \quad \square$$

Definition 14. *Let $f \in B_n$. If $f(x_1, ..., x_n) \sim_A g(x_1, ...x_s) + h(x_{s+1}, ..., x_s)$, with $g \in B_s$, $h \in B_{n-s}$, we say that f is a* splitting function.

Remark 15. *It follows from Definition 14 and Theorem 7 that all the quadratic Boolean functions are splitting functions.*

Lemma 16. *Let $f \in B_n$ be such that $f \sim_A g(x_1, ..., x_s) + h(x_{s+1}, ..., x_n)$, with $s < n$ Then*

$$\mathcal{F}(f) = \mathcal{F}(g_{\restriction \mathbb{F}^s})\mathcal{F}(h_{\restriction \mathbb{F}^{n-s}}) = 2^{-n}\mathcal{F}(g)\mathcal{F}(h).$$

Proof. Let $X = (y, x)$ with $y \in \mathbb{F}^s$ and $x \in \mathbb{F}^{n-s}$. So

$$\begin{aligned}
\mathcal{F}(f) &= \sum_{X \in \mathbb{F}^n} (-1)^{f(X)} = \sum_{y \in \mathbb{F}^s; x \in \mathbb{F}^{n-s}} (-1)^{g(y)+h(x)} \\
&= \sum_{y \in \mathbb{F}^s} (-1)^{g(y)} \sum_{x \in \mathbb{F}^{n-s}} (-1)^{h(x)} = \mathcal{F}(g_{\restriction \mathbb{F}^s})\mathcal{F}(h_{\restriction \mathbb{F}^{n-s}}) \\
&= 2^{-n}\left(2^{n-s}\mathcal{F}(g_{\restriction \mathbb{F}^s})\right)\left(2^s\mathcal{F}(h_{\restriction \mathbb{F}^{n-s}})\right) \\
&= 2^{-n}\mathcal{F}(g)\mathcal{F}(h).
\end{aligned}$$

□

It is immediate from Lemma 16 that the following corollary holds.

Corollary 17. *Let f be a function on $\mathbb{F}^n$ defined by $f(X) = \sum_{i=1}^k g_i(X_i)$, where $X_i \subset X = \{x_1, ...x_n\}$ are disjoint, $g_i \in B_{n_i}$, with $n_i = |X_i|$ and let $t = \sum_{i=1}^k n_i \leq n$. Then*

$$\mathcal{F}(f) = 2^{n-t} \prod_{i=1}^{k} \mathcal{F}(g_{i \restriction \mathbb{F}^{n_i}}).$$

Remark 18. *If $g = h(Mx + a)$, with M invertible in $GL_n(\mathbb{F})$ and $a \in \mathbb{F}^n$, then we have $\mathcal{F}(g) = \sum_{x \in \mathbb{F}^n} (-1)^{h(Mx+a)} = \sum_{y \in \mathbb{F}^n} (-1)^{h(y)} = \mathcal{F}(h)$, where $y = Mx + a$ [i.e., if $g \sim_A h$ implies $\mathcal{F}(f) = \mathcal{F}(g)$]. Hence correlation is invariant under affine equivalence. Since $\mathrm{w}(g)$ is invariant under affine equivalence (see Proposition 6) and $\mathcal{F}(g) = 2^n - 2\mathrm{w}(g)$, we can also deduce from this that $\mathcal{F}(g)$ is invariant under equivalence.*

Theorem 19. *Let f be a quadratic Boolean function on n variables, that is, $f \sim_A x_1x_2 + \cdots + x_{2k-1}x_{2k} + x_{2k+1}$, with $k \leq \lfloor \frac{n-1}{2} \rfloor$ if f is balanced; $f \sim_A x_1x_2 + \cdots +$*

$x_{2k-1}x_{2k}+c$, with $k \le \lfloor \frac{n}{2} \rfloor$ and $c \in \mathbb{F}$, if f is unbalanced. Then

$$\mathcal{F}(f) = \begin{cases} 0 & \textit{if } f \textit{ is balanced} \\ \pm 2^{n-k} & \textit{if } f \textit{ is unbalanced.} \end{cases}$$

Proof. Since f is balanced when $f \sim_A x_1x_2 + \cdots + x_{2k-1}x_{2k} + x_{2k+1}$, so in this case $\mathcal{F}(f) = 0$. Observe that when $x_{2k-1}x_{2k}$ is restricted to $\mathbb{F}^2$, we have $\mathcal{F}(x_{2k-1}x_{2k}) = 2$. Applying Lemma 13, Corollary 17 and Remark 18, if $f \sim_A x_1x_2 + \cdots + x_{2k-1}x_{2k}$, we have $\mathcal{F}(f) = 2^{n-2k}2^k = 2^{n-k}$ and if $f = x_1x_2 + \cdots + x_{2k-1}x_{2k} + 1$, we have $\mathcal{F}(f) = -2^{n-k}$. □

The *(first-order) derivative* of f at a is defined by $D_af(x) = f(x+a) + f(x)$ and the *(second-order) derivative* at a and b is $D_bD_af(x) = f(x) + f(x+b) + f(x+a) + f(x+a+b)$. It is important to note that $\deg(D_af) < \deg(f)$.

Definition 20. *Let $f \in B_n$. The* autocorrelation function *of f, denoted by $\hat{r}_f$, is defined as*

$$\hat{r}_f : a \mapsto \sum_{x \in \mathbb{F}^n} (-1)^{D_af(x)}. \tag{1.4}$$

So $\hat{r}_f(a) = \mathcal{F}(D_af)$ and it is clear that $\hat{r}_f(0) = 2^n$.

1.1.6 Weight of Boolean functions

In Proposition 11, we showed that any non-constant affine function is balanced, so the weight of any affine function is 0, 2^{n-1} or 2^n.

It can be easily observed from the definition of Boolean functions on n variables that half of them have degree n. The following property characterize the weights of these functions.

Proposition 21. *Any Boolean function on n variables, with $n > 1$, has an odd weight if and only if it has degree n.*

Obviously, odd weight implies that the output distribution of these functions (with maximal degree) is biased, so they are not suitable to be used in most cryptographic applications.

We next consider the weight of some splitting functions.

Proposition 22. *If $f(x,y) \sim_A g(x) + h(y)$, with $g \in B_m$ and $h \in B_n$, then*

$$\mathrm{w}(f) = 2^m \mathrm{w}(h_{\restriction \mathbb{F}^n}) + 2^n \mathrm{w}(g_{\restriction \mathbb{F}^m}) - 2\mathrm{w}(g_{\restriction \mathbb{F}^m})\mathrm{w}(h_{\restriction \mathbb{F}^n}).$$

Proof. Since bias of Boolean function is invariant under affine equivalence (see Remark 18), we have

$$\begin{aligned}
\mathcal{F}(f) &= \sum_{(x,y)\in \mathbb{F}^m \times \mathbb{F}^n} (-1)^{f(x,y)} \\
&= \sum_{(x,y)\in \mathbb{F}^m \times \mathbb{F}^n} (-1)^{g(x)+h(y)} \\
&= \sum_{x\in \mathbb{F}^m} (-1)^{g(x)} \sum_{y\in \mathbb{F}^n} (-1)^{h(y)} \\
&= \mathcal{F}(g_{\restriction \mathbb{F}^m})\mathcal{F}(h_{\restriction \mathbb{F}^n}). \qquad (1.5)
\end{aligned}$$

So

$$\begin{aligned}
\mathrm{w}(f) &= 2^{n+m-1} - \frac{1}{2}\mathcal{F}(f) \\
&= 2^{n+m-1} - \frac{1}{2}\mathcal{F}(g_{\restriction \mathbb{F}^m})\mathcal{F}(h_{\restriction \mathbb{F}^n}) \\
&= 2^{n+m-1} - \frac{1}{2}\left(2^m - 2\mathrm{w}(g_{\restriction \mathbb{F}^m})\right)\left(2^n - 2\mathrm{w}(h_{\restriction \mathbb{F}^n})\right) \\
&= 2^m \mathrm{w}(h_{\restriction \mathbb{F}^n}) + 2^n \mathrm{w}(g_{\restriction \mathbb{F}^m}) - 2\mathrm{w}(g_{\restriction \mathbb{F}^m})\mathrm{w}(h_{\restriction \mathbb{F}^n}).
\end{aligned}$$

□

Proposition 23. *A function $f(x,y) \sim_A g(x) + h(y)$, with $g \in B_m$, $h \in B_n$, $x \in \mathbb{F}^m$ and $y \in \mathbb{F}^n$, is balanced if and only if either g or h is balanced.*

Proof. Recall, from Equation (1.5), that $\mathcal{F}(f) = \mathcal{F}(g_{\restriction \mathbb{F}^m})\mathcal{F}(h_{\restriction \mathbb{F}^n})$. We know that f is balanced if and only if $\mathcal{F}(f) = 0$ if and only if either $\mathcal{F}(g_{\restriction \mathbb{F}^m}) = 0$ or $\mathcal{F}(h_{\restriction \mathbb{F}^m}) = 0$

if and only if either g or h is balanced. □

We next report a well-known result which can be found in [37] on page 372.

Proposition 24. *A Boolean function $g(x_1, ..., x_{n-1}) + x_n$ on n variables is balanced.*

Proof. It is clear that $g(x_1, ..., x_{n-1}) + x_n$ is a splitting function. Since x_n is a linear function, so it is balanced (see Proposition 11). The proof is concluded by Proposition 23. □

Corollary 25. *Let $f \in B_n$ be such that $f \sim_A x_1x_2 + \cdots + x_{2k-1}x_{2k} + x_{2k+1}$, with $k \leq \lfloor (n-1)/2 \rfloor$, if f is balanced; $f \sim_A x_1x_2 + \cdots + x_{2k-1}x_{2k} + c$, with $k \leq \lfloor n/2 \rfloor$ and $c \in \mathbb{F}$, if f is unbalanced. Then*

$$\mathrm{w}(f) = \begin{cases} 2^{n-1} & \textit{if } f \textit{ is balanced,} \\ 2^{n-1} \pm 2^{n-k-1} & \textit{if } f \textit{ is unbalanced.} \end{cases}$$

Proof. The result follows from Theorem 19 and the fact that $\mathrm{w}(f) = 2^{n-1} - \frac{1}{2}\mathcal{F}(f)$ (see Lemma 9). □

Proposition 26. *A monomial in B_n of degree r has the weight 2^{n-r}.*

Proof. From Proposition 22, we can assume that $g \in B_r$ and $h \in B_{n-r}$ such that $g(x) = \prod_{i=1}^{r} x_i$ and $h = 0$. It is clear that $\mathrm{w}(g_{\restriction \mathbb{F}^r}) = 1$ and $\mathrm{w}(h_{\restriction \mathbb{F}^{n-r}}) = 0$. So by applying the formula $\mathrm{w}(f) = 2^{n-r}\mathrm{w}(g_{\restriction \mathbb{F}^r}) + 2^r\mathrm{w}(h_{\restriction \mathbb{F}^{n-r}}) - 2\mathrm{w}(g_{\restriction \mathbb{F}^r})\mathrm{w}(h_{\restriction \mathbb{F}^{n-r}})$, we have $\mathrm{w}(f) = 2^{n-r}\mathrm{w}(g_{\restriction \mathbb{F}^r}) = 2^{n-r}$.

Alternatively, since it is clear that, for $(c_1, ..., c_n) \in \mathbb{F}^n$, $g(c_1, ..., c_n) = 1$ if and only if $c_1 = \cdots = c_r = 1$, so we have

$$\begin{aligned} \mathrm{w}(g) &= |\{x \in \mathbb{F}^n \mid g(x) = 1\}| \\ &= |\{(c_1, ..., c_n) \in \mathbb{F}^n \mid c_1 = c_2 = \cdots = c_r = 1\}| \\ &= 2^{n-r}. \end{aligned}$$ □

Remark 27. *If $g(x_1, ..., x_t)$, with a positive integer $t < n$, is in B_n then we have* $\mathrm{w}(g) = 2^{n-t}\mathrm{w}(g_{\upharpoonright \mathbb{F}^t})$ *and $\mathcal{F}(g) = 2^{n-t}\mathcal{F}(g_{\upharpoonright \mathbb{F}^t})$. Furthermore, g is balanced if and only if $g_{\upharpoonright \mathbb{F}^t}$ is balanced and also $\mathcal{F}(g) = 0$ if and only if $\mathcal{F}(g_{\upharpoonright \mathbb{F}^t}) = 0$.*

1.1.7 Walsh transform of Boolean functions

In this subsection, we define and give some properties of the Walsh transform, a tool which is crucial in proving different significant results in Boolean functions.

Definition 28. *Let f be a Boolean function on n variables. For all $a \in \mathbb{F}^n$, the* Walsh transform *$\mathcal{W}_f$ of a Boolean function f is the function from $\mathbb{F}^n$ to $\mathbb{Z}$ defined by*

$$\mathcal{W}_f : a \mapsto \mathcal{F}(f + l_a) = \sum_{x \in \mathbb{F}^n} (-1)^{f(x)+a \cdot x}$$

The value $\mathcal{W}_f(a)$ is called the *Walsh coefficient* of f at a point a and we call the list (or multiset) of the 2^n Walsh coefficients of f (i.e., $\{\mathcal{W}_f(a) \mid a \in \mathbb{F}^n\}$) the *Walsh spectrum* of f. The list of the 2^n absolute values of Walsh coefficients of f (i.e., $|\mathcal{W}_f(a)|$, for all $a \in \mathbb{F}^n$) is called the *extended-Walsh spectrum.*

We now consider some properties of Walsh transform.

Proposition 29. *Let $f \in B_n$. Then, for all $b \in \mathbb{F}^n$, we have*

$$\sum_{a \in \mathbb{F}^n} (-1)^{a \cdot b} \mathcal{W}_f(a) = 2^n (-1)^{f(b)}.$$

Proof. We have

$$\begin{aligned}
\sum_{a \in \mathbb{F}^n} (-1)^{a \cdot b} \mathcal{W}_f(a) &= \sum_{a \in \mathbb{F}^n} \sum_{x \in \mathbb{F}^n} (-1)^{a \cdot b} (-1)^{f(x)+a \cdot x} \\
&= \sum_{x \in \mathbb{F}^n} (-1)^{f(x)} \sum_{a \in \mathbb{F}^n} (-1)^{a \cdot (x+b)} \\
&= \sum_{x \in \mathbb{F}^n} (-1)^{f(x)} \mathcal{F}(l_{x+b}) = 2^n (-1)^{f(b)}
\end{aligned}$$

where the last equality follows from Lemma 12 which states that $\mathcal{F}(l_{x+b}) = 2^n$ if $x = b$ and 0 otherwise. □

Proposition 30 (Parseval's relation)**.** *Let $f \in B_n$. Then we have*

$$\sum_{a\in\mathbb{F}^n} \mathcal{W}_f^2(a) = 2^{2n}.$$

Proof. We have

$$\begin{aligned}
\sum_{a\in\mathbb{F}^n} \mathcal{W}_f^2(a) &= \sum_{a\in\mathbb{F}^n}\sum_{x\in\mathbb{F}^n}(-1)^{f(x)+a\cdot x}\sum_{y\in\mathbb{F}^n}(-1)^{f(y)+a\cdot y} \\
&= \sum_{x\in\mathbb{F}^n}\sum_{y\in\mathbb{F}^n}(-1)^{f(x)+f(y)}\sum_{a\in\mathbb{F}^n}(-1)^{a\cdot(x+y)} \\
&= 2^n\sum_{x\in\mathbb{F}^n}(-1)^{f(x)+f(x)} \qquad (1.6) \\
&= 2^n\sum_{x\in\mathbb{F}^n}(-1)^0 = 2^{2n},
\end{aligned}$$

where Equation (1.6) follows from Lemma 12, that is, $\sum_{a\in\mathbb{F}^n}(-1)^{a\cdot(x+y)} = 2^n$ if $x = y$ and 0 otherwise. □

Next, we show how the Fourier transform is related to Walsh transform.

Lemma 31. *Let f be a Boolean function on n variables. Then*

$$\mathcal{W}_f(a) = 2^n\delta(a) - 2\mathcal{F}_f(a),$$

where $\delta(a) = 1$ if $a = 0$ and $\delta(a) = 0$ otherwise.

Proof. First note that $(-1)^{f(x)} = 1 - 2f(x)$. We have

$$\begin{aligned}
\mathcal{W}_f(a) &= \sum_{x\in\mathbb{F}^n}(-1)^{f(x)+a\cdot x} \\
&= \sum_{x\in\mathbb{F}^n}(-1)^{f(x)}(-1)^{a\cdot x}
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{x\in\mathbb{F}^n} (1-2f(x))(-1)^{a\cdot x} \\
&= \sum_{x\in\mathbb{F}^n} (-1)^{a\cdot x} - 2\sum_{x\in\mathbb{F}^n} f(x)(-1)^{a\cdot x} \\
&= \mathcal{F}(l_a) - 2\sum_{x\in\mathbb{F}^n} f(x)(-1)^{a\cdot x} \\
&= 2^n\delta(a) - 2\mathcal{F}_f(a),
\end{aligned}
$$

where the last step follows from the fact that $\mathcal{F}(l_a) = 2^n\delta(a)$(see Lemma 12). □

We now consider the Fourier transform of f on an arbitrary subspace of $\mathbb{F}^n$.

Theorem 32. *Let f be a Boolean function on n variables. Let S be an arbitrary subspace of $\mathbb{F}^n$ and $S^\perp$ be the dual of S. Then*

$$\sum_{y\in S} \mathcal{F}_f(y) = 2^{\dim S} \sum_{y\in S^\perp} f(y).$$

Proof. We have

$$
\begin{aligned}
\sum_{y\in S} \mathcal{F}_f(y) &= \sum_{y\in S}\sum_{x\in\mathbb{F}^n} f(x)(-1)^{y\cdot x} \\
&= \sum_{x\in\mathbb{F}^n} f(x)\sum_{y\in S}(-1)^{y\cdot x} \\
&= 2^{\dim S}\sum_{x\in S^\perp} f(x).
\end{aligned}
$$

□

The following corollary can be proved in a similar way as Theorem 32.

Corollary 33. *Let f be a Boolean function on n variables. Let S be an arbitrary subspace of $\mathbb{F}^n$ and $S^\perp$ be the dual of S. Then*

$$\sum_{y\in S} \mathcal{W}_f(y) = 2^{\dim S} \sum_{y\in S^\perp} (-1)^{f(y)}.$$

Taking S to be the set of all vectors y "included" in a, that is, $y \leq a$ meaning that

$y_i \leq a_i$, for all $1 \leq i \leq n$ and $\bar{a} = 1 - a$, then Corollary 33 transformed into the following.

Corollary 34. *For any $f \in B_n$,*

$$\sum_{y \leq a} \mathcal{W}_f(y) = 2^{\mathrm{w}(a)} \sum_{y \leq \bar{a}} (-1)^{f(y)}.$$

We next present a result which shows some relations between autocorrelation and Walsh transform of a Boolean function.

Proposition 35. *Let $f \in B_n$ and $u \in \mathbb{F}^n$. Then we have*

$$\sum_{x \in \mathbb{F}^n} \hat{r}_f(x)(-1)^{u \cdot x} = \mathcal{W}_f^2(u).$$

Proof. We have

$$\begin{aligned}
\sum_{x \in \mathbb{F}^n} \hat{r}_f(x)(-1)^{u \cdot x} &= \sum_{x \in \mathbb{F}^n} \sum_{y \in \mathbb{F}^n} (-1)^{D_x f(y) + u \cdot x} \\
&= \sum_{x \in \mathbb{F}^n} \sum_{y \in \mathbb{F}^n} (-1)^{f(y+x) + f(y) + u \cdot x + u \cdot y + u \cdot y} \\
&= \sum_{y \in \mathbb{F}^n} (-1)^{f(y) + u \cdot y} \sum_{x \in \mathbb{F}^n} (-1)^{f(x+y) + u \cdot (x+y)} \\
&= \mathcal{W}_f^2(u).
\end{aligned}$$

□

In the next result we show that the extended-Walsh spectrum is invariant under extended-affine equivalence.

Theorem 36. *Let g and h be Boolean functions on n variables such that $g \sim_{EA} h$. Then $\{|\mathcal{W}_g(a)|, a \in \mathbb{F}^n\} = \{|\mathcal{W}_h(a)|, a \in \mathbb{F}^n\}$.*

Proof. Suppose that g and h are extended-affine equivalent, that is, $g = h(Ax + a) + b \cdot x + c$, for some $a, b \in \mathbb{F}^n$, $c \in \mathbb{F}$ and A is an $n \times n$ nonsingular matrix in

$GL_n(\mathbb{F})$. So we have

$$\begin{aligned}\mathcal{W}_g(u) &= \sum_{x\in\mathbb{F}^n}(-1)^{g(x)+u\cdot x}\\ &= \sum_{x\in\mathbb{F}^n}(-1)^{h(Ax+a)+(b+u)\cdot x+c}\\ &= (-1)^{(b+u)\cdot(A^{-1}a)+c}\sum_{y\in\mathbb{F}^n}(-1)^{h(y)+(b+u)\cdot(A^{-1}y)}\end{aligned}$$

For any $y \in \mathbb{F}^n$, we have

$$\begin{aligned}(b+u)\cdot(A^{-1}y) &= \sum_{i=1}^{n}(b_i+u_i)(A^{-1}y)_i\\ &= \sum_{i=1}^{n}\sum_{j=1}^{n}(b_i+u_i)A^{-1}_{ij}y_j\\ &= \sum_{j=1}^{n}y_j\sum_{i=1}^{n}(b_i+u_i)A^{-1}_{ij}\\ &= y\cdot((A^{-1})^T(b+u))\end{aligned}$$

Let $\mu = (b+u)\cdot(A^{-1}a)+c$ and $w = (A^{-1})^T(b+u)$. We thus obtain

$$\mathcal{W}_g(u) = (-1)^{\mu}\sum_{y\in\mathbb{F}^n}(-1)^{h(y)+y\cdot w} = (-1)^{\mu}\mathcal{W}_h(w) \tag{1.7}$$

from which the result follows. □

Now we consider the Walsh transform of some splitting functions.

Proposition 37. *For $g \in B_m$ and $h \in B_n$, define $f(x,y) = g(x)+h(y)$ on $\mathbb{F}^{m+n}$. Then, for $z = (a,b) \in \mathbb{F}^m \times \mathbb{F}^n$,*

$$\mathcal{W}_f(z) = \mathcal{W}_{g_{\restriction\mathbb{F}^n}}(a)\mathcal{W}_{h_{\restriction\mathbb{F}^n}}(b).$$

Proof. For $z = (a, b) \in \mathbb{F}^m \times \mathbb{F}^n$, we have

$$\begin{aligned}
\mathcal{W}_f(z) &= \sum_{(x,y)\in\mathbb{F}^m\times\mathbb{F}^n} (-1)^{f(x,y)+a\cdot x+b\cdot y} = \sum_{(x,y)\in\mathbb{F}^m\times\mathbb{F}^n} (-1)^{g(x)+h(y)+a\cdot x+b\cdot y} \\
&= \sum_{x\in\mathbb{F}^m} (-1)^{g(x)+a\cdot x} \sum_{y\in\mathbb{F}^n} (-1)^{h(y)+b\cdot y} \\
&= \mathcal{W}_{g_{\restriction\mathbb{F}^n}}(a)\mathcal{W}_{h_{\restriction\mathbb{F}^n}}(b).
\end{aligned}$$ □

Next, we determine the Walsh transform of quadratic Boolean functions.

Theorem 38. *Let $f \in B_n$ be such that $f \sim_A q = x_1x_2 + \cdots + x_{2k-1}x_{2k} + x_{2k+1}$, with $k \leq \lfloor \frac{n-1}{2} \rfloor$, if f is balanced and $f \sim_A \bar{q} = x_1x_2 + \cdots + x_{2k-1}x_{2k} + c$, with $k \leq \lfloor \frac{n}{2} \rfloor$ and $c \in \mathbb{F}$, if f is unbalanced. Then, for any $a \in \mathbb{F}^n$, $\mathcal{W}_f(a) \in \{0, \pm 2^{n-k}\}$*

Proof. We have

$$\mathcal{W}_q(a) = \sum_{x\in\mathbb{F}^n} (-1)^{q(x)+a\cdot x} = \mathcal{F}(q(x) + a \cdot x)$$

If $q(x) + a \cdot x$ is balanced then $\mathcal{W}_q(a) = \mathcal{F}(q(x) + a \cdot x) = 0$. If $q(x) + a \cdot x$ is unbalanced then $q(x) + a \cdot x \sim_A x_1x_2 + \cdots + x_{2k-1}x_{2k} + c$, with $c \in \mathbb{F}$, and so $\mathcal{F}(q(x) + a \cdot x) = \pm 2^{n-k}$, by Theorem 19. Thus, $\mathcal{W}_q(a) \in \{0, \pm 2^{n-k}\}$. In a similar manner, we can show that $\mathcal{W}_{\bar{q}}(a) \in \{0, \pm 2^{n-k}\}$. We deduce from Equation (1.7) that $\mathcal{W}_f(a) \in \{0, \pm 2^{n-k}\}$. □

Definition 39. *An element $a \in \mathbb{F}^n$ is a* linear structure *of a Boolean function f on $\mathbb{F}^n$ if D_af is a constant. Define $V(f) = \{a \in \mathbb{F}^n | D_af \text{ is a constant}\}$. The set $V(f)$ is said to be the* linear space *of a Boolean function f.*

In [16], the Walsh transform of a quadratic Boolean function is presented in a different form.

Theorem 40. *Let $f \in B_n$ be a quadratic function. Then, for $a \in \mathbb{F}^n$, we have $W_f(a) \in \left\{0, \pm 2^{(n+\ell)/2}\right\}$, where $\ell = \dim V(f)$.*

1.1.8 Nonlinearity of Boolean functions

Nonlinearity of a Boolean function is an important property in cryptography and it is desirable for the Boolean functions used in designing cryptographic schemes to have high nonlinearity, since such schemes are believed to have high resistance to linear attacks. In this subsection, we define and give some results on nonlinearity of Boolean functions.

Definition 41. *Let $f \in B_n$. Then the* nonlinearity *of f is defined as*

$$\mathcal{N}(f) = \min_{a \in \mathbb{F}^n} d(f, \varphi_a),$$

where $\varphi_a = a \cdot x + c$ is in A_n.

The distance between a Boolean function f and an affine function φ_a is related to the Walsh transform $\mathcal{W}_f(a)$ as follows:

Lemma 42. *Let f be a Boolean function on n variables. Then, for $a \in \mathbb{F}^n$,*

$$d(f, \varphi_a) = 2^{n-1} \pm \frac{1}{2}\mathcal{W}_f(a).$$

Proof. We have $\varphi_a = a \cdot x + c$, with $c \in \mathbb{F}$. So

$$\begin{aligned} d(f, \varphi_a) &= \mathrm{w}(f + \varphi_a) = 2^{n-1} - \frac{1}{2}\mathcal{F}(f + \varphi_a) \\ &= 2^{n-1} - \frac{1}{2}\mathcal{F}(f + a \cdot x + c) \\ &= \begin{cases} 2^{n-1} - \frac{1}{2}\mathcal{F}(f + a \cdot x) & \text{if } c = 0 \\ 2^{n-1} + \frac{1}{2}\mathcal{F}(f + a \cdot x) & \text{if } c = 1 \qquad \text{(see Lemma 13)} \end{cases} \\ &= 2^{n-1} \pm \frac{1}{2}\mathcal{W}_f(a). \end{aligned}$$

□

We next apply Lemma 42 to relate the nonlinearity to Walsh transform of a Boolean function.

Theorem 43. *Let $f \in B_n$. Then $\mathcal{N}(f) = 2^{n-1} - \frac{1}{2}\max_{a \in \mathbb{F}^n} |\mathcal{W}_f(a)|$.*

Proof. By applying Lemma 42, we have

$$\begin{aligned}\mathcal{N}(f) &= \min_{a\in\mathbb{F}^n} d(f,\varphi_a)\\ &= \min_{a\in\mathbb{F}^n}\left(2^{n-1}\pm\frac{1}{2}\mathcal{W}_f(a)\right)\\ &= 2^{n-1}-\frac{1}{2}\max_{a\in\mathbb{F}^n}|\mathcal{W}_f(a)|.\end{aligned}$$ □

In the following result we show that two extended-affine equivalent Boolean functions have the same nonlinearity.

Corollary 44. *Let $g, h \in B_n$ be such that $g \sim_{EA} h$. Then $\mathcal{N}(g) = \mathcal{N}(h)$.*

Proof. The proof follows from Theorem 43 and the fact, in Theorem 36, that the extended-Walsh spectrum is invariant under extended-affine equivalence. □

Corollary 45. *If $f \in B_n$ then $\max_{a\in\mathbb{F}^n}|\mathcal{W}_f(a)| \geq 2^{\frac{n}{2}}$.*

Proof. Applying Parseval's relation, we have

$$\max_{a\in\mathbb{F}^n}\mathcal{W}_f^2(a) \geq \frac{2^{2n}}{2^n} = 2^n \iff \max_{a\in\mathbb{F}^n}|\mathcal{W}_f(a)| \geq 2^{\frac{n}{2}}.$$ □

By Theorem 43 and Corollary 45, the following result holds.

Corollary 46. *Let $f \in B_n$. Then $\mathcal{N}(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$.*

Since, for any quadratic function f, $\mathcal{W}_f(a) \in \{0, \pm 2^{n-k}\}$ (see Theorem 38), so the following result which can be found in [26] on page 134 is deduced.

Corollary 47. *Let $f \in B_n$ be such that $f \sim_A q = x_1x_2 + \cdots + x_{2k-1}x_{2k} + x_{2k+1}$, with $k \leq \lfloor\frac{n-1}{2}\rfloor$ if f is balanced and $f \sim_A \bar{q} = x_1x_2 + \cdots + x_{2k-1}x_{2k} + c$, with $k \leq \lfloor\frac{n}{2}\rfloor$ and $c \in \mathbb{F}$, if f is unbalanced. Then $\mathcal{N}(f) = 2^{n-1} - 2^{n-k-1}$.*

In a different form, when we apply the result in Theorem 40, the nonlinearity of quadratic functions is given as in the following.

Corollary 48 ([16])**.** *Let $f \in B_n$ be a quadratic function. Then*

$$\mathcal{N}(f) = 2^{n-1} - 2^{\frac{n+\ell}{2}-1},$$

where $\ell = \dim V(f)$.

The following lemma can be found in [27] on page 134.

Lemma 49. *Any two quadratic Boolean functions g and h on n variables are affine equivalent if and only if $\mathrm{w}(g) = \mathrm{w}(h)$ and $\mathcal{N}(g) = \mathcal{N}(h)$.*

The following result of a spitting function can be found in [49] on page 80.

Corollary 50. *Let $f = g(x) + h(y)$, with $x \in \mathbb{F}^n$ and $y \in \mathbb{F}^m$. Then we have*

$$\mathcal{N}(f) = 2^m \mathcal{N}(g_{\upharpoonright \mathbb{F}^n}) + 2^n \mathcal{N}(h_{\upharpoonright \mathbb{F}^m}) - 2\mathcal{N}(g_{\upharpoonright \mathbb{F}^n})\mathcal{N}(h_{\upharpoonright \mathbb{F}^m}).$$

Proof. We know from Proposition 37 that, for $z = (a, b) \in \mathbb{F}^n \times \mathbb{F}^m$, we have

$$\mathcal{W}_f(z) = \mathcal{W}_{g_{\upharpoonright \mathbb{F}^n}}(a)\mathcal{W}_{h_{\upharpoonright \mathbb{F}^m}}(b).$$

Clearly, from the definition of nonlinearity, we have

$$\max_{a\in\mathbb{F}^m} |\mathcal{W}_{g_{\upharpoonright \mathbb{F}^n}}(a)| = 2^n - 2\mathcal{N}(g_{\upharpoonright \mathbb{F}^n}) \quad \text{and} \quad \max_{b\in\mathbb{F}^m} |\mathcal{W}_{h_{\upharpoonright \mathbb{F}^m}}(b)| = 2^m - 2\mathcal{N}(h_{\upharpoonright \mathbb{F}^m}).$$

So we have

$$\begin{aligned}
\mathcal{N}(f) &= 2^{n-1} - \frac{1}{2} \max_{z\in\mathbb{F}^n\times\mathbb{F}^m} |\mathcal{W}_f(z)| \\
&= 2^{n-1} - \frac{1}{2} \max_{(a,b)\in\mathbb{F}^n\times\mathbb{F}^m} |\mathcal{W}_{g_{\upharpoonright \mathbb{F}^n}}(a)\mathcal{W}_{h_{\upharpoonright \mathbb{F}^m}}(b)| \\
&= 2^{n-1} - \frac{1}{2} \left(\max_{a\in\mathbb{F}^s} |\mathcal{W}_{g_{\upharpoonright \mathbb{F}^n}}(a)|\right) \left(\max_{b\in\mathbb{F}^m} |\mathcal{W}_{h_{\upharpoonright \mathbb{F}^m}}(b)|\right) \\
&= 2^{n-1} - \frac{1}{2} (2^s - 2\mathcal{N}(g_{\upharpoonright \mathbb{F}^n}))(2^m - 2\mathcal{N}(h_{\upharpoonright \mathbb{F}^m})) \\
&= 2^m \mathcal{N}(g_{\upharpoonright \mathbb{F}^n}) + 2^n \mathcal{N}(h_{\upharpoonright \mathbb{F}^m}) - 2\mathcal{N}(g_{\upharpoonright \mathbb{F}^n})\mathcal{N}(h_{\upharpoonright \mathbb{F}^m}).
\end{aligned}$$

□

1.1.9 Plateaued functions

Definition 51. *A function f in B_n is said to be* plateaued *if its Walsh coefficients take at most three values: 0 and $\pm\vartheta$. The value ϑ is called the* amplitude *of the plateaued function f.*

Proposition 52. *A Boolean function f on n variables is plateaued if and only if there exists σ such that, for every $x \in \mathbb{F}^n$, $\sum_{a,b\in\mathbb{F}^n}(-1)^{D_aD_bf(x)} = \sigma$. The amplitude ϑ of f is related to σ by $\sigma = \vartheta^2$.*

It is immediate that all linear functions are plateaued and the same is true for quadratic functions (this can also be verified by Theorem 38).

1.1.10 Bent functions

In this subsection, we define and give some properties of bent functions.

Definition 53. *Let $f \in B_n$, with n even. A function f is* bent *if and only if $\mathcal{N}(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$. Equivalently, a Boolean function f is bent if and only if $\mathcal{W}_f(a) = \pm 2^{\frac{n}{2}}$, for all $a \in \mathbb{F}^n$.*

Next, we state a result which relate bent functions to its first-order derivatives.

Theorem 54. *A Boolean function f on n variables is bent if and only if D_af is balanced for any nonzero $a \in \mathbb{F}^n$.*

For a given Boolean function f, we define a real valued function by

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

Definition 55. *Let $f \in B_n$ be a bent function. Then a Boolean function $\tilde{f}$ is the* dual *of f if, for $a \in \mathbb{F}^n$,*

$$\frac{\mathcal{W}_f(a)}{2^{\frac{n}{2}}} = (-1)^{\tilde{f}(a)} = 1 - 2\tilde{f}(a). \tag{1.8}$$

Proposition 56. *Let $f \in B_n$ be bent. Then its dual $\tilde{f}$ is bent.*

Proof. Since f is bent then, by definition, we have $\mathcal{W}_f(a) = \pm 2^{n/2}$, for all $a \in \mathbb{F}^n$. Now we need to show that $\mathcal{W}_{\tilde{f}}(a) = \pm 2^{n/2}$, for all $a \in \mathbb{F}^n$. Thus, we have

$$\begin{aligned}
\mathcal{W}_{\tilde{f}}(a) &= \sum_{x\in\mathbb{F}^n} (-1)^{\tilde{f}(x)+a\cdot x} \\
&= \sum_{x\in\mathbb{F}^n} \frac{\mathcal{W}_f(x)}{2^{n/2}}(-1)^{a\cdot x} && \text{(by definition of dual)} \\
&= \frac{1}{2^{n/2}} \sum_{x\in\mathbb{F}^n}\sum_{y\in\mathbb{F}^n} (-1)^{f(y)+x\cdot y+a\cdot x} \\
&= \frac{1}{2^{n/2}} \sum_{y\in\mathbb{F}^n} (-1)^{f(y)} \sum_{x\in\mathbb{F}^n} (-1)^{x\cdot(y+a)} \\
&= \frac{1}{2^{n/2}} \left((-1)^{f(a)}\right)(2^n) && \text{(apply Lemma 12)} \\
&= 2^{n/2}(-1)^{f(a)} = \pm 2^{n/2}.
\end{aligned}$$

Hence it implies that $\tilde{f}$ is also bent. □

Theorem 57 (Rothaus's bound)**.** *Let $f \in B_n$ be a bent function. Then, for $n > 2$,* $\deg(f) \leq n/2$.

Proof. Let $f \in B_n$ be bent and $n > 2$. By Corollary 34, we have

$$\sum_{y\leq a} \mathcal{W}_f(y) = 2^{\mathrm{w}(a)} \sum_{y\leq \bar{a}} (-1)^{f(y)}.$$

Equivalently, we can write

$$\sum_{y\leq a} \mathcal{W}_f(y) = 2^{\mathrm{w}(a)} \sum_{y\leq \bar{a}} (1-2f(y)). \tag{1.9}$$

Since f is bent, by Equation (1.8) that defines the dual $\tilde{f}$, we obtain

$$\mathcal{W}_f(y) = 2^{\frac{n}{2}} - 2^{\frac{n}{2}+1}\tilde{f}(y)). \tag{1.10}$$

Substituting (1.10) in Equation (1.9) we have

$$\begin{aligned}
&\sum_{y\leq\bar{a}}\left(2^{\frac{n}{2}}-2^{\frac{n}{2}+1}\tilde{f}(y)\right)=2^{\mathrm{w}(\bar{a})}\sum_{y\leq a}(1-2f(y))\\
\iff\ & 2^{-\mathrm{w}(\bar{a})}\sum_{y\leq\bar{a}}\left(2^{\frac{n}{2}}-2^{\frac{n}{2}+1}\tilde{f}(y)\right)=\sum_{y\leq a}(1-2f(y))\\
\iff\ & 2^{-\mathrm{w}(\bar{a})}\left(2^{\frac{n}{2}+\mathrm{w}(\bar{a})}\right)-2^{\frac{n}{2}-\mathrm{w}(\bar{a})+1}\sum_{y\leq\bar{a}}\tilde{f}(y)=2^{\mathrm{w}(a)}-2\sum_{y\leq a}f(y)\\
\iff\ & 2^{\mathrm{w}(a)-1}-2^{\frac{n}{2}-1}+2^{\frac{n}{2}-\mathrm{w}(\bar{a})}\sum_{y\leq\bar{a}}\tilde{f}(y)=\sum_{y\leq a}f(y)\\
\iff\ & \sum_{y\leq a}f(y)=2^{\mathrm{w}(a)-1}-2^{\frac{n}{2}-1}+2^{\mathrm{w}(a)-\frac{n}{2}}\sum_{y\leq\bar{a}}\tilde{f}(y), \qquad (1.11)
\end{aligned}$$

where Equation (1.11) follows from the fact that $\mathrm{w}(\bar{a})=n-\mathrm{w}(a)$.

Note that f can be written as

$$f(x)=\sum_{a\in\mathbb{F}^n}g(a)x^a \qquad (1.12)$$

where the coefficients are given by

$$g(a)=\sum_{y\leq a}f(y)$$

(see [37], Theorem 1, p. 372). So the monomial x^a is present in $f(x)$ if and only if $g(a)$ is odd. Since if $\mathrm{w}(a)>n/2$, with $n>2$, implies that $\mathrm{w}(a)-n/2\geq 1$, then $g(a)=\sum_{y\leq a}f(y)$ in (1.11) is even [i.e., $g(a)\equiv 0 \pmod 2$]. Thus, f does not contain any monomial of degree $>n/2$. Hence f must have at most degree $n/2$. □

Given two bent functions, one with m variables and another one with n variables, we can construct another bent function on $m+n$ variables as in the following.

Theorem 58. *For $g\in B_m$ and $h\in B_n$, define $f(x,y)=g(x)+h(y)$ on $\mathbb{F}^{m+n}$, $x\in\mathbb{F}^m$ and $y\in\mathbb{F}^n$. Then f is bent if and only if g and h are bent.*

Proof. By Proposition 37, $\mathcal{W}_f(z)=\mathcal{W}_g(a)\mathcal{W}_h(b)$, for $z=(a,b)\in\mathbb{F}^m\times\mathbb{F}^n$. If g

and h are both bent, then $\mathcal{W}_g(a) = \pm 2^{m/2}$ and $\mathcal{W}_h(b) = \pm 2^{n/2}$. Thus we have $\mathcal{W}_g(a) = \pm 2^{(m+n)/2}$, and so f is bent.

Conversely, assume that f is bent. We prove that g and h are both bent. Suppose, by contradiction, that g is not bent. Then it follows that $\max_{u \in \mathbb{F}^n} |\mathcal{W}_g(u)| > 2^{m/2}$. Thus, we must have $\max_{v \in \mathbb{F}^m} |\mathcal{W}_h(v)| < 2^{n/2}$, since

$$\begin{aligned} 2^{(m+n)/2} &= \max_{w=(u,v) \in \mathbb{F}^n \times \mathbb{F}^m} |\mathcal{W}_f(w)| \\ &= \max_{(u,v) \in \mathbb{F}^n \times \mathbb{F}^m} (|\mathcal{W}_g(u)||\mathcal{W}_h(v)|) \\ &= \left(\max_{u \in \mathbb{F}^n} |\mathcal{W}_g(u)| \right) \left(\max_{v \in \mathbb{F}^n} |\mathcal{W}_h(v)| \right). \end{aligned}$$

This contradicts Corollary 45, that is, $\max_{v \in \mathbb{F}^n} |\mathcal{W}_h(v)| \geq 2^{n/2}$. □

Observe that the Walsh transform of $g = x_1 x_2$, for any $a \in \mathbb{F}^2$, is $\mathcal{W}_f(a) = \pm 2$, so g is bent. Thus, the following corollary holds by Theorem 58.

Corollary 59. *The function $f(x_1, ..., x_{2k}) = x_1 x_2 + \cdots + x_{2k-1} x_{2k}$, $k \geq 1$ on $2k$ variables, is bent.*

By definition of bent functions and Corollary 44, we have the following result.

Corollary 60. *Let $g, h \in B_n$ be such that $g \sim_{EA} h$. Then g is bent if and only if h is bent.*

Theorem 61. *Let $f \in B_n$ be a bent functions. Then $\mathrm{w}(f) = 2^{n-1} \pm 2^{\frac{n}{2}-1}$.*

Proof. By definition f is bent $\iff$ $\mathcal{W}_f(a) = \pm 2^{\frac{n}{2}}$, for any $a \in \mathbb{F}^n$. So it implies that $\mathcal{F}(f) = \mathcal{W}_f(0) = \pm 2^{\frac{n}{2}}$. Hence, by Lemma 9, $\mathrm{w}(f) = 2^{n-1} - \frac{1}{2}\mathcal{F}(f) = 2^{n-1} \pm 2^{\frac{n}{2}-1}$ □

1.1.11 Partially-bent functions

We now define partially-bent functions as in [7].

Definition 62. *A Boolean function f is* partially-bent *if there exists a linear subspace W of $\mathbb{F}^n$ such that the restriction of f to W is affine and the restriction of f to any complementary subspace U of W, $W \oplus U = \mathbb{F}^n$, is bent.*

That is, for all $x \in U$ and $y \in W$,

$$f(x+y) = \underbrace{f(x)}_{\text{bent part}} + \underbrace{f(y)}_{\text{affine part}} . \tag{1.13}$$

Equivalently, as in [21], a Boolean function f is called partially-bent if, for any $a \in \mathbb{F}^n$, $D_a f$ is either balanced or constant.

Remark 63. *The linear subspace W of $\mathbb{F}^n$, in Definition 62, is formed by the set of all linear structures of f, that is, $W = V(f)$. Observe that since bent functions exist only in even dimensions then $\dim U = n - \dim V(f)$ is even, implying that $\dim V(f)$ is even if n is even and it is odd if n is odd. The dimension of $V(f)$ is 0 if and only if f is bent.*

Let $x = y + z$, where $y \in U$ and $z \in V(f)$. Then, for any $a \in V(f) \setminus \{0\}$,

$$\begin{aligned} D_a f(x) &= f(x+a) + f(x) = f(y+z+a) + f(y+z) \\ &= f(y) + f(z) + f(a) + f(y) + f(z) = f(a). \end{aligned} \tag{1.14}$$

The result in the following corollary is immediately deduced from Theorem 7 and Definition 62.

Corollary 64. *Every quadratic function is partially-bent.*

1.1.12 Semi-bent functions

We have seen that bent functions exist only in even dimension and they are the only Boolean functions which attain maximal nonlinearity. We next define, as in [40], a family of functions which attain relatively high nonlinearity in odd dimension. This family of functions was first introduced by Chee et al. in [24].

Definition 65. *Let f be a Boolean function of n variables, with n odd. Then f is called* semi-bent *if $\mathcal{N}(f) = 2^{n-1} - 2^{\frac{n-1}{2}}$. Equivalently, for n odd,* semi-bent *functions are those Boolean functions whose Walsh transform takes the values: 0 or $\pm 2^{\frac{n+1}{2}}$.*

For n even, $f \in B_n$ is called semi-bent *if $\mathcal{N}(f) = 2^{n-1} - 2^{\frac{n}{2}}$. Equivalently, for n even,* semi-bent *functions are those Boolean functions whose Walsh transform takes the values 0 or $\pm 2^{\frac{n+2}{2}}$.*

Remark 66. *For odd $n \leq 7$, the maximal nonlinearity of a Boolean functions in B_n attainable is $2^{n-1} - 2^{\frac{n-1}{2}}$ and for odd $n > 7$, the maximal nonlinearity can exceed this bound (see [38]).*

By Corollary 44, the following holds.

Corollary 67. *Let $g, h \in B_n$ be such that $g \sim_{EA} h$. Then g is semi-bent if and only if h is semi-bent.*

Proposition 68. *If $f \in B_n$, with n odd, is a semi-bent function then*

$$\mathrm{w}(f) \in \left\{ 2^{n-1}, 2^{n-1} \pm 2^{\frac{n-1}{2}} \right\}.$$

Proof. By definition of semi-bent function f, we have $\mathcal{F}(f) \in \left\{ 0, \pm 2^{\frac{n+1}{2}} \right\}$ from which the result follows. □

The following corollary can be easily proved.

Corollary 69. *Let $f \in B_n$ be a quadratic Boolean function and $c \in \mathbb{F}$. Then*

1. *for even n, f is bent if and only if*

$$f \sim_A x_1x_2 + \cdots + x_{n-1}x_n + c.$$

2. *for even n, f is semi-bent if and only if*

$$f \sim_A x_1x_2 + \cdots + x_{n-3}x_{n-2} + x_{n-1} \text{ or } f \sim_A x_1x_2 + \cdots + x_{n-3}x_{n-2} + c.$$

3. *for odd n, f is semi-bent if and only if*

$$f \sim_A x_1x_2 + \cdots + x_{n-2}x_{n-1} + x_n \text{ or } f \sim_A x_1x_2 + \cdots + x_{n-2}x_{n-1} + c.$$

1.1.13 Resilient Boolean functions

We begin with a classical approach to correlation-immune and resilient functions and later the generalised approach by Braeken et al. in [4] is considered.

Definition 70 ([3]). *A Boolean function f on n variables is* correlation-immune (CI) *of order t (or simply write t-CI function) if and only if $\mathcal{W}_f(u) = 0$, for all $u \in \mathbb{F}^n$ such that $1 \leq w(u) \leq t$.*

The output of a correlation-immune function of order t is statistically independent of the combination of any t of its inputs. In other words, a Boolean function $f(x)$ in n variables is correlation immune of order t if, for any fixed subset of t variables, the probability that, given the value of $f(x)$, the t variables have any fixed set of values is always 2^{-t}, no matter what the choice of the fixed set of t values is.

Definition 71 ([3]). *A balanced function which is of correlation-immune of order t is said to be* resilient *or it is said to satisfy the property of* resiliency *(simply write t-resilient function). Equivalently, a Boolean function f on n variables is said be t-resilient if and only if $\mathcal{W}_f(u) = 0$, for all $u \in \mathbb{F}^n$, such that $0 \leq \mathrm{w}(u) \leq t$.*

Next, we give a result which relates the order of a resilient function to its degree.

Theorem 72. *For any t-resilient Boolean function f, $\deg(f) \leq n - t - 1$.*

We say that a t-resilient function f is optimal algebraic degree if we have $\deg(f) = n - t - 1$. The next result shows that the order of a resilient function, its degree and nonlinearity are related.

Theorem 73. *Let $f \in B_n$ be t-resilient, with $t \leq n - 2$. If*

(i) $\deg(f) = n - t - 1$ *then* $\mathcal{N}(f) = 2^{n-1} - 2^{t+1}$,

(ii) $\deg(f) < n - t - 1$ *then* $\mathcal{N}(f) \leq 2^{n-1} - 2^{t+1}$.

Observe, from Theorems 72 and 73, that there are some trade-offs between the order of a resilient function and some other properties such as algebraic degree and nonlinearity.

We now consider the generalized presentation of correlation-immune and resilient functions with respect to some collections of subspaces as introduced by Braeken et al. in [4]. Canteaut et al. in [11] were the first to extend the properties of resiliency with respect to subspaces. Braeken et al. indicated that one advantage of this approach is that it relaxes some trade-offs between important properties of Boolean functions.

We now present some definitions and notations which are used to generalize the definition of resilient and correlation immune functions.

Let $\mathcal{P} = \{1, ..., n\}$ and denote the power set of $\mathcal{P}$ by $P(\mathcal{P})$. We call the set $\Delta \subseteq P(\mathcal{P})$ *monotone decreasing* if, for each set A in Δ, each subset of A is also in Δ and the set $\Gamma \subseteq P(\mathcal{P})$ is *monotone increasing* if, for each set B in Γ, each set containing B is also in Γ. We can efficiently describe a monotone increasing set Γ by the set Γ^- which consists of the minimal elements (sets) in Γ, that is, the elements in Γ for which no proper subset is also in Γ. Similarly, a monotone decreasing set Δ can be described by the set Δ^+ which consists of the maximal elements (sets) in Δ, that is, the elements in Δ for which no proper superset is also in Δ.

Let $\Delta^c = P(\mathcal{P}) \setminus \Delta$ and set $\Gamma = \Delta^c$. From this, it can be easily noted that Γ is monotone increasing if and only if Δ is monotone decreasing.

For any two monotone decreasing sets Δ_1 and Δ_2, define

$$\Delta_1 \uplus \Delta_2 = \{A = A_1 \cup A_2 : A_1 \in \Delta_1, A_2 \in \Delta_2\}.$$

Notice that $\Delta_1 \uplus \Delta_2$ is also a monotone decreasing set.

Observe that $\sup(x)$ and $\delta(x, y) = \sup(x-y)$ are subsets of $\mathcal{P}$ and that $\mathcal{P}$ is partially ordered, that is, $x \preceq y$ if and only if $\sup(x) \subseteq \sup(y)$. As noted in [32, 41], $\delta(x, y)$ has similar properties to a metric while $\sup(x)$ has similar properties to a norm.

Next, we define correlation-immune and resilient functions with respect to a monotone decreasing set Δ. In this case, we are assuming that the set Δ is the maximal possible monotone decreasing set for which the function satisfies the corresponding property. Consequently, as indicated earlier, the monotone increasing set Γ corresponding with Δ is defined by $\Gamma = \Delta^c$.

Definition 74 ([4])**.** *Let $f \in B_n$ and Δ be a monotone decreasing set. Then f is called* Δ-resilient *(or it is said to satisfy the property of* Δ-resiliency*) if and only if $f(x) + w \cdot x$ is a balanced function for all $w \in \mathbb{F}^n$ such that* $\sup(w) \in \Delta$*. Furthermore, f is called a* Δ-correlation immune function (or Δ-CI function) *if and only if $f(x) + w \cdot x$ is a balanced function for all w such that* $\sup(w) \in \Delta \setminus \{\emptyset\}$*.*

Remark 75. *For some positive integer t, if $\Delta = \{A \in P(\mathcal{P}) : |A| \leq t\}$ then the definitions of Δ-resilient function and t-resilient function coincide (this is true also for Δ-CI function and t-CI function) and in Definition 74, we can replace the property of balancedness of $f(x) + w \cdot x$ with $\mathcal{W}_f(w) = 0$*

If we denote the set of vectors which have zero Walsh coefficients by ZW_f, then $\Delta \subseteq \{\sup(u) : u \in ZW_f\}$. It can be noted that $ZW_f \cap \Gamma$ is not necessarily empty. Notice that Δ is a collection of subspaces, that is, it is not necessarily a subspace itself.

We can also establish some relations with the classical definition of resiliency by using Δ^+ and Γ^-. For the monotone sets Γ and Δ, define the parameters:

$$t_1 = \min\{|A| : A \in \Gamma^-\} \text{ and } t_2 = \max\{|A| : A \in \Delta^+\}.$$

Observe that from the definition of t_1 and the fact that Γ is a monotone increasing set, each subset of size $t_1 - 1$ belongs to Δ, implying that a Δ-resilient function is also $(t_1 - 1)$-resilient. Similarly, a Δ-CI function is $(t_1 - 1)$-CI. Also worth noting is that the parameter t_2 defines the maximum dimension of a subspace in which a function is Δ-resilient.

Finally, we report the construction of Siegenthaler and Camion et al. which was later extended with respect to monotone sets by Braeken et al. in [4].

Theorem 76. *Let $g(x_1, ..., x_n)$ and $h(x_1, ..., x_n)$ be two Δ-resilient functions on $\mathbb{F}^n$. The function f on $n+1$ variables defined by*

$$f(x_1, ..., x_{n+1}) = x_{n+1}g(x_1, ..., x_n) + (1 + x_{n+1})h(x_1, ..., x_n)$$

is $\widetilde{\Delta}$-resilient, where $\widetilde{\Delta} = \Delta \uplus P(\{n+1\})$. Furthermore, if $w \in \Gamma$ and for any $u \preceq w$ it holds that $\mathcal{W}_{h_{\restriction \mathbb{F}^n}}(u) + \mathcal{W}_{g_{\restriction \mathbb{F}^n}}(u) = 0$, then f is $\widehat{\Delta}$-resilient, where $\widehat{\Delta} = \widetilde{\Delta} \cup P(\sup(w))$.

Proof. Let $a = (a_1, ..., a_n) \in \mathbb{F}^n$ and $\tilde{a} = (a, a_{n+1}) \in \mathbb{F}^n \times \mathbb{F}$. From Equation (2.9), we have

$$\mathcal{W}_f(\tilde{a}) = \mathcal{W}_{h_{\restriction \mathbb{F}^n}}(a) + (-1)^{a_{n+1}}\mathcal{W}_{g_{\restriction \mathbb{F}^n}}(a).$$

If $\tilde{a}$ satisfies $\sup(\tilde{a}) \in \widetilde{\Delta}$, then $\sup(a) \in \Delta$. Since h and g are Δ-resilient functions (i.e., $\mathcal{W}_{h_{\restriction \mathbb{F}^n}}(a) = \mathcal{W}_{g_{\restriction \mathbb{F}^n}}(a) = 0$), so we conclude that $\mathcal{W}_f(\tilde{a}) = 0$, implying that f is $\widetilde{\Delta}$-resilient.

Suppose that $\tilde{a}$ satisfies $\sup(\tilde{a}) \in \widehat{\Delta}$. Then we have to deal with two cases:

(i) $\sup(\tilde{a}) \in \Delta \uplus P(\{n+1\})$, which has already been shown that $\mathcal{W}_f(\tilde{a}) = 0$,

(ii) $\sup(\tilde{a}) \in P(\sup(w))$, for some $w \in \Gamma$. We have now that $a_{n+1} = 0$ and thus $\mathcal{W}_f(\tilde{a}) = \mathcal{W}_{h_{\restriction \mathbb{F}^n}}(a) + \mathcal{W}_{g_{\restriction \mathbb{F}^n}}(a) = 0$ since $\tilde{a} \preceq w$. □

Remark 77. *Theorem 76 extends the Siegenthaler's result in [47] which states that "if h and g are t-resilient then f is t-resilient" and also it generalises the result of Camion et al. in [8] which states that "if, for all v such that $w(v) = t+1$, it holds that $\mathcal{W}_h(v) + \mathcal{W}_g(v) = 0$, then f is $t+1$-resilient."*

1.2 Vectorial Boolean functions

In this section, we are going to report some results on vectorial Boolean functions and the reader is referred to [1, 2, 7, 9, 13, 40, 43, 44, 45] in case more details are sought.

1.2.1 Definitions and notations

A *vectorial Boolean function* F is any function from $\mathbb{F}^n$ to $\mathbb{F}^m$, where $n, m \geq 1$. Observe that the case $m = 1$ is what we considered in the previous section, so we assume that $n, m > 1$. Any vectorial Boolean function can be written as $F = (f_1, ..., f_m)$, where f_i's are Boolean functions from $\mathbb{F}^n$ to $\mathbb{F}$ called *coordinate functions* of F. For any $\lambda \neq 0 \in \mathbb{F}^m$, the function $\lambda \cdot F$ is called a *component* of F and we denote it by F_λ.

Notice that we can extend the definition of derivatives to vectorial Boolean functions. The *first-order derivative* of a function F from $\mathbb{F}^n$ to $\mathbb{F}^m$ at $a \in \mathbb{F}^n$ is given by $D_aF(x) = F(x+a) + F(x)$ and the *second-order derivative* of a function F from $\mathbb{F}^n$ to $\mathbb{F}^m$ at $a, b \in \mathbb{F}^n$ is given by $D_aD_bF(x) = F(x) + F(x+a) + F(x+b) + F(x+a+b)$.

1.2.2 Representation of vectorial Boolean functions

We give two well-known representations which are commonly used in cryptography and our standard reference is [13, 14].

The algebraic normal form

The notion of algebraic normal form of Boolean functions, we considered in the previous section, can easily be extended to vectorial Boolean functions. We have seen in the previous subsection that each coordinate function of vectorial Boolean function F is uniquely represented as a polynomial on n variables, where every variable appears in each monomial with degree 0 or 1 and its coefficients are in $\mathbb{F}$, that is, it is an element of $\mathbb{F}[x_1, ..., x_n]/ < x_1^2 + x_1, ..., x_n^2 + x_n >$. So F must also be uniquely represented as a polynomial of the same form but with coefficients in $\mathbb{F}^m$, that is, it is an element of $\mathbb{F}^m[x_1, ..., x_n]/ < x_1^2 + x_1, ..., x_n^2 + x_n >$. Thus, we have:

$$F(x) = \sum_{u \in \mathbb{F}^n} a_u \left(\prod_{i=1}^{n} x_i^{u_i} \right) = \sum_{u \in \mathbb{F}^n} a_u x^u, \tag{1.15}$$

where $a_u \in \mathbb{F}^m$. We call this polynomial the algebraic normal form of vectorial Boolean function F. The algebraic degree of vectorial Boolean function F is $\deg(F) = \max_{u \in \mathbb{F}^n}\{\mathrm{w}(u) | a_u \neq 0\}$. Equivalently, $\deg(F) = \max_{\lambda \in \mathbb{F}^n} \deg(F_\lambda) = \max_{1 \leq i \leq m}\{\deg(f_i)\}$, where f_i's are coordinate functions of F. A function F is said to be balanced if it takes every value of $\mathbb{F}^m$ the same number 2^{n-m} of times. A function F from $\mathbb{F}^n$ to itself is balanced if and only if all components are balanced (see [13]). We call a balanced function from $\mathbb{F}^n$ to itself a *permutation* of $\mathbb{F}^n$.

Univariate polynomial representation over $\mathbb{F}_{2^n}$

We now focus on a special representation when $n = m$, that is, a vectorial Boolean function from $\mathbb{F}^n$ to itself. Consider the finite field $\mathbb{F}_{2^n}$ consisting of 2^n elements. It is well-known that the set $\mathbb{F}_{2^n}^* = \mathbb{F}_{2^n} \setminus \{0\}$ is a cyclic group which has $2^n - 1$ elements. An element in $\mathbb{F}_{2^n}$ which is a generator of the multiplicative group $\mathbb{F}_{2^n}^*$ is called a *primitive element*. It is well explained in [13] that the vector space $\mathbb{F}^n$ can be endowed with the structure of the finite field $\mathbb{F}_{2^n}$. So any vectorial Boolean function F from $\mathbb{F}_{2^n}$ into $\mathbb{F}_{2^n}$ admits a unique *univariate polynomial representation* over $\mathbb{F}_{2^n}$, given as:

$$F(x) = \sum_{i=0}^{2^n-1} \delta_i x^i, \tag{1.16}$$

where $\delta_i \in \mathbb{F}_{2^n}$ and the degree of F is at most $2^n - 1$.

Next, we see how the ANF can be obtained from a given univariate polynomial. For every vector $x \in \mathbb{F}^n$, we can also denote by x the element $\sum_{j=1}^{n} x_j \alpha_j$ of $\mathbb{F}_{2^n}$, where $(\alpha_1, ..., \alpha_n)$ is a basis of the $\mathbb{F}$-vectorspace $\mathbb{F}_{2^n}$. If we write the *binary expansion* of every integer $i \in \{0, 1, ..., 2^n - 1\}$ as $i = \sum_{s=0}^{n-1} i_s 2^s$, $i_s \in \{0, 1\}$, then we have

$$\begin{aligned} F(x) = \sum_{i=0}^{2^n-1} \delta_i x^i &= \sum_{i=0}^{2^n-1} \delta_i \left(\sum_{j=1}^{n} x_j \alpha_j \right)^i \\ &= \sum_{i=0}^{2^n-1} \delta_i \left(\sum_{j=1}^{n} x_j \alpha_j \right)^{\sum_{s=0}^{n-1} i_s 2^s} \end{aligned}$$

$$= \sum_{i=0}^{2^n-1} \delta_i \prod_{s=0}^{n-1} \left(\sum_{j=1}^{n} x_j \alpha_j^{2^s} \right)^{i_s}$$

since the mapping $x \mapsto x^2$ is $\mathbb{F}$-linear over $\mathbb{F}_{2^n}$ and $x_j \in \mathbb{F}$. The ANF of F is obtained by expanding these last products, simplifying and decomposing them again over the basis $(\alpha_1, ..., \alpha_n)$. Another way to do this is by the Lagrage interpolation theorem.

With this established relationship between the ANF and univariate polynomial, it is certainly possible to read the algebraic degree of F directly on the univariate polynomial representation. Given the binary expansion $i = \sum_{s=0}^{n-1} i_s 2^s$, define $\mathrm{w}_2(i) = \sum_{s=0}^{n-1} i_s$. The value $\mathrm{w}_2(i)$ is called the *2-weight* of i. Then the algebraic degree of F is

$$\deg(F) = \max_{\substack{0 \le i \le 2^n - 1 \\ \delta_i \neq 0}} \mathrm{w}_2(i).$$

Any function of the form $F(x) = x^d$, for some non negative integer d, is called a *power function* and if $d = 2^i + 2^j$, for some non negative integers i and j, $i \neq j$, we say that F is a quadratic power function since it algebraic degree is clearly 2.

Remark 78. *The* (absolute) trace function Tr, *defined on* $\mathbb{F}_{2^n}$ *by*

$$Tr(z) = z + z^2 + z^{2^2} + \cdots + z^{2^{n-1}},$$

is $\mathbb{F}$*-linear and satisfies* $(Tr(z))^2 = Tr(z^2) = Tr(z)$*; thus it is valued in its prime field* $\mathbb{F}$*. Every Boolean function can be written in the form:*

$$f(x) = Tr(F(x)) = Tr\left(\sum_{i=0}^{2^n-1} \delta_i x^i \right).$$

However, it is important to note that this representation is not unique.

1.2.3 Properties of Walsh transform for functions from $\mathbb{F}^n$ to $\mathbb{F}^m$

Let $b \neq 0 \in \mathbb{F}^m$ and $a \in \mathbb{F}^n$. The Walsh transform of a component F_b of vectorial Boolean function F is given by

$$\mathcal{W}_F(a,b) = W_{F_b}(a) = \sum_{x \in \mathbb{F}^n} (-1)^{F_b(x)+a \cdot x}.$$

The set defined by

$$\Lambda_F = \{\mathcal{W}_F(a,b) \mid a \in \mathbb{F}^n, b \neq 0 \in \mathbb{F}^m\}$$

is called the *Walsh spectrum* of F.

Next, we give the Parseval relation for a function from $\mathbb{F}^n$ to $\mathbb{F}^m$ whose proof naturally follows from the proof of Proposition 30.

Corollary 79 (Parseval relation). *Let F be a function from $\mathbb{F}^n$ to $\mathbb{F}^m$. Then*

$$\sum_{b \neq 0 \in \mathbb{F}^m} \sum_{a \in \mathbb{F}^n} \mathcal{W}_F^2(a,b) = 2^{2n}(2^m - 1) \tag{1.17}$$

We call $\mathcal{W}_F^4(a,b)$, with $a, b \in \mathbb{F}^n$, a *4th power moment* of the Walsh transform of F_b. We next report a result which gives a lower bound on the sum of all 4th power moments of the Walsh transform.

Lemma 80. *Let F be a function from $\mathbb{F}^n$ to $\mathbb{F}^m$. Then*

$$\sum_{b \in \mathbb{F}^m} \sum_{a \in \mathbb{F}^n} \mathcal{W}_F^4(a,b) \geq 2^{n+m}(3 \cdot 2^{2n} - 2 \cdot 2^n). \tag{1.18}$$

Proof. We have

$$
\begin{aligned}
&\sum_{b\in\mathbb{F}^m}\sum_{a\in\mathbb{F}^n}\mathcal{W}_F^4(a,b) = \sum_{b\in\mathbb{F}^m}\sum_{a\in\mathbb{F}^n}\left(\sum_{x\in\mathbb{F}^n}(-1)^{b\cdot F+a\cdot x}\right)^4\\
&= \sum_{x,y,z,t\in\mathbb{F}^n}\left(\sum_{b\in\mathbb{F}^m}(-1)^{b\cdot(F(x)+F(y)+F(z)+F(t))}\right)\left(\sum_{a\in\mathbb{F}^n}(-1)^{a\cdot(x+y+z+t)}\right)\\
&= 2^{n+m}\left|\left\{(x,y,z,t)\in\mathbb{F}^{4n}\;\middle|\;\begin{cases}x+y+z+t=0\\ F(x)+F(y)+F(z)+F(t)=0\end{cases}\right\}\right|\\
&= 2^{n+m}|\{(x,y,z)\in\mathbb{F}^{3n}\mid F(x)+F(y)+F(z)+F(x+y+z)=0\}| \qquad (1.19)\\
&\geq 2^{n+m}|\{(x,y,z)\in\mathbb{F}^{3n}\mid x=y \text{ or } x=z \text{ or } y=z\}| \qquad (1.20)\\
&= 2^{n+m}\left(3|\{(x,x,y)\mid x,y\in\mathbb{F}^n\}|-2|\{(x,x,x)\mid x\in\mathbb{F}^n\}|\right)\\
&= 2^{n+m}(3\cdot 2^{2n}-2\cdot 2^n). \qquad \square
\end{aligned}
$$

1.2.4 Nonlinearity of vectorial Boolean functions

We talk about nonlinearity of vectorial Boolean functions and the reader is referred to [13] if more information is sought.

Definition 81. *Let F be a function from $\mathbb{F}^n$ to $\mathbb{F}^m$. The nonlinearity of F is given by*

$$\mathcal{N}(F) = 2^{n-1} - \frac{1}{2}\max_{b\neq 0\in\mathbb{F}^m;a\in\mathbb{F}^n}|\mathcal{W}_F(a,b)|.$$

Equivalently, the nonlinearity of F is equal to the minimum of all the nonlinearities of components of F, that is, $\mathcal{N}(F) = \min_{b\neq 0\in\mathbb{F}^m}\mathcal{N}(F_b)$.

It can be deduced, from Corollary 46 and Definition 81, that if n is even then $2^{n-1}-2^{n/2-1}$ is an upper bound for the nonlinearity of a vectorial Boolean function from $\mathbb{F}^n$ to $\mathbb{F}^m$. We are going to see later that this bound is not tight for some values of m. Next, we report the best upper bound known for $m\geq n-1$.

Theorem 82 (Sidelnikov-Chabaud-Vaudenay bound)**.** *Let $n, m \in \mathbb{N}$ be such that $m \geq n-1$ and let F be any function from $\mathbb{F}^n$ to $\mathbb{F}^m$. Then*

$$\mathcal{N}(F) \leq 2^{n-1} - \frac{1}{2}\sqrt{3 \cdot 2^n - 2 - \frac{2(2^n-1)(2^{n-1}-1)}{2^m-1}}.$$

Proof. First note that, we have

$$\max_{b \neq 0 \in \mathbb{F}^m; a \in \mathbb{F}^n} \mathcal{W}_F^2(a,b) \geq \frac{\sum\limits_{b \neq 0 \in \mathbb{F}^m} \sum\limits_{a \in \mathbb{F}^n} \mathcal{W}_F^4(a,b)}{\sum\limits_{b \neq 0 \in \mathbb{F}^m} \sum\limits_{a \in \mathbb{F}^n} \mathcal{W}_F^2(a,b)}. \tag{1.21}$$

By relation (1.18), we can deduce that

$$\sum_{b \neq 0 \in \mathbb{F}^m} \sum_{a \in \mathbb{F}^n} \mathcal{W}_F^4(a,b) \geq 2^{n+m}(3 \cdot 2^{2n} - 2 \cdot 2^n) - 2^{4n}. \tag{1.22}$$

Hence, by Equation (1.17), the relations (1.21) and (1.22), we have:

$$\begin{aligned}
\max_{b \neq 0 \in \mathbb{F}^m; a \in \mathbb{F}^n} \mathcal{W}_F^2(a,b) &\geq \frac{2^{n+m}(3 \cdot 2^{2n} - 2 \cdot 2^n) - 2^{4n}}{2^{2n}(2^m-1)} \\
&= \frac{3 \cdot 2^{3n+m} - 2 \cdot 2^{2n+m} - 2^{4n}}{2^{2n}(2^m-1)} \\
&= \frac{3 \cdot 2^{n+m} - 2 \cdot 2^m - 2^{2n}}{2^m-1} \\
&= \frac{(3 \cdot 2^n - 2)(2^m-1) - (2^{2n} - 3 \cdot 2^n + 2)}{2^m-1} \\
&= 3 \cdot 2^n - 2 - \frac{2(2^n-1)(2^{n-1}-1)}{2^m-1}.
\end{aligned}$$

This implies

$$\max_{b \neq 0 \in \mathbb{F}^m; a \in \mathbb{F}^n} |\mathcal{W}_F(a,b)| \geq \sqrt{3 \cdot 2^n - 2 - \frac{2(2^n-1)(2^{n-1}-1)}{2^m-1}}.$$

Since $\mathcal{N}(F) = 2^{n-1} - \frac{1}{2} \max\limits_{b \neq 0 \in \mathbb{F}^m; a \in \mathbb{F}^n} |\mathcal{W}_F(a,b)|$, then the desired bound is obtained. □

The condition $m \geq n-1$ is assumed in Theorem 82 to make sure that the expression located under the square root is non-negative.

1.2.5 Bent vectorial Boolean functions

In this subsection, the definition of bent function, seen in previous section, is extended to vectorial Boolean functions and some results are reported.

Definition 83. *A function F from $\mathbb{F}^n$ to $\mathbb{F}^m$, with n even, is said to be* bent *if and only if $\mathcal{N}(F) = 2^{n-1} - 2^{\frac{n}{2}-1}$. Equivalently, a function F from $\mathbb{F}^n$ to $\mathbb{F}^m$ is called bent if any component F_b is bent for all $b \neq 0 \in \mathbb{F}^n$, that is, the Walsh transform for any component F_b is equal to $\pm 2^{\frac{n}{2}}$.*

It is immediate from the definition and Theorem 57 that if function F from $\mathbb{F}^n$ to $\mathbb{F}^m$ is bent then every component has degree at most $n/2$, implying that $\deg(F) \leq n/2$.

Proposition 84. *A function F from $\mathbb{F}^n$ to $\mathbb{F}^m$ is bent if and only if all its derivatives $D_aF(x)$, for all $a \neq 0 \in \mathbb{F}^n$, are balanced (i.e., $D_aF(x)$ are all permutations).*

Since bent Boolean functions exist only if n is even, so bent vectorial Boolean functions from $\mathbb{F}^n$ to $\mathbb{F}^m$ exist only under this same hypothesis that n is even. However, this condition is not sufficient for the existence of bent vectorial Boolean functions from $\mathbb{F}^n$ to $\mathbb{F}^m$ as shown by Nyberg in [44]. The following result provide conditions for existence.

Proposition 85. *Bent functions from $\mathbb{F}^n$ to $\mathbb{F}^m$ exist only if n is even and $m \leq n/2$.*

Open problem: In Proposition 82, we saw that, for $m \geq n-1$, the Sidelnikov-Chabaud-Vaudenay bound is better especially if m is large enough. However, to determine a better bound when n is odd and $m < n-1$ is an open problem [13]. We know from [44] that, for n even, the upper bound $2^{n-1} - 2^{\frac{n}{2}-1}$ is the best and tight for nonlinearity of functions from $\mathbb{F}^n$ to $\mathbb{F}^m$, with $m \leq n/2$. But it is a long standing problem to determine a better upper bound on the nonlinearity of (n, m)-functions when n is even and $n/2 < m < n-1$.

Remark 86. *Proposition 85 implies that no vectorial Boolean functions from $\mathbb{F}^n$ to itself can be bent. However, we can discuss about the number of bent components which functions from $\mathbb{F}^n$ to itself can contain. In [45], it is shown that such functions can have at most $2^n - 2^{n/2}$ bent components and some functions which achieve this bound can be easily constructed.*

1.2.6 Almost Perfect Nonlinear functions

In this subsection, we define and give some results on almost perfect nonlinear functions and our standard reference is [1, 2, 13, 34].

Definition 87. *For $a, b \in \mathbb{F}^n$ and a vectorial Boolean function F from $\mathbb{F}^n$ to $\mathbb{F}^m$, let*

$$\delta_F(a, b) = |\{x \in \mathbb{F}^n \mid D_aF(x) = b\}|.$$

The differential uniformity *of F is given by*

$$\delta = \max_{a \neq 0, b \in \mathbb{F}^n} \delta_F(a, b)$$

and it always satisfies the relation $\delta \geq 2$. We say that a function F is differentially δ-uniform *in $\mathbb{F}^n$. A function with $\delta = 2$ is called* Almost Perfect Nonlinear (APN)*.*

The statements which we state in the following theorem are obvious from the definition of APN function.

Theorem 88. *A function from $\mathbb{F}^n$ to itself is APN if and only if one of the following conditions holds:*

(i) $\delta = 2$;

(ii) *for any $a \neq 0 \in \mathbb{F}^n$,*

$$H_a = \{F(x + a) + F(x) \mid x \in \mathbb{F}^n\}$$

contains 2^{n-1} elements, that is, $|H_a| = 2^{n-1}$;

(iii) for every $(a, b) \neq 0$*, the system*

$$\begin{cases} x + y & = a \\ F(x) + F(y) & = b \end{cases}$$

admits 0 *or* 2 *solutions;*

(iv) for any $a \neq 0 \in \mathbb{F}^n$*, the derivative* D_aF *is a two-to-one mapping;*

(v) F *is not affine on any* 2*-dimensional affine subspace of* $\mathbb{F}^n$*.*

The result that follows associate APN functions to second-order derivatives and can be found in [9].

Proposition 89. *An function* F *from* $\mathbb{F}^n$ *to itself is APN if and only if, for any nonzero elements* a *and* b *in* $\mathbb{F}^n$*, with* $a \neq b$*, we have* $D_aD_bF(x) \neq 0$*, for all* $x \in \mathbb{F}^n$*.*

In other words, Proposition 89 can be presented as: *a function* F *from* $\mathbb{F}^n$ *to itself is APN if and only if it holds that "for all* $x \in \mathbb{F}^n$*,* $D_aD_bF(x) = 0 \iff a = 0$ *or* $b = 0$ *or* $a = b$*."*

The statement: "for all $x \in \mathbb{F}^n$, $D_aD_bF(x) = 0 \iff a = 0$ or $b = 0$ or $a = b$" can also be presented in different way. First, we recall that $D_aD_bF(x) = F(x) + F(x+b) + F(x+a) + F(x+b+a)$. Let $y = x + a$ and $z = x + b$. Thus, it implies that $x + y + z = x + a + b$. So we can deduce that the statements: "for all $x \in \mathbb{F}^n$, $D_aD_bF(x) = 0 \iff a = 0$ or $b = 0$ or $a = b$" and "$F(x) + F(y) + F(z) + F(x+y+z) = 0 \iff x = y$ or $x = z$ or $y = z$" are equivalent. It implies that Proposition 89 can also stated as in the following.

Corollary 90. *A function* F *from* $\mathbb{F}^n$ *to itself is APN if and only if it holds that "*$F(x) + F(y) + F(z) + F(x+y+z) = 0 \iff x = y$ *or* $x = z$ *or* $y = z$*."*

Next, we use Lemma 80 and Corollary 90 to prove a result which relate APN functions to the 4th power moment of Walsh transform.

Theorem 91. *A function F from $\mathbb{F}^n$ to itself is APN if and only if*

$$\sum_{b\neq 0,a\in\mathbb{F}^n} \mathcal{W}_F^4(a,b) = 2^{3n+1}(2^n-1). \tag{1.23}$$

Proof. Observe that we have equality in the relation (1.20) if and only if the statement: "$F(x)+F(y)+F(z)+F(x+y+z)=0 \iff x=y$ or $x=z$ or $y=z$" holds. By Corollary 90, the statement: "$F(x)+F(y)+F(z)+F(x+y+z)=0 \iff x=y$ or $x=z$ or $y=z$" holds if and only if F is APN. Thus, it implies that

$$\sum_{a,b\in\mathbb{F}^n} \mathcal{W}_F^4(a,b) = 3\cdot 2^{4n} - 2\cdot 2^{3n} \tag{1.24}$$

if and only if F is APN. Observe that Equation (1.24) can be modified to

$$\sum_{b\neq 0,a\in\mathbb{F}^n} \mathcal{W}_F^4(a,b) = \sum_{a,b\in\mathbb{F}^n} \mathcal{W}_F^4(a,b) - 2^{4n} = 2^{3n+1}(2^n-1) \tag{1.25}$$

from which the assertion is deduced. □

Lemma 92. *For any (n,n)-function, we have*

$$\sum_{\lambda\neq 0,a\in\mathbb{F}^n} \mathcal{W}_F^4(a,\lambda) = 2^n \sum_{\lambda\neq 0,a\in\mathbb{F}^n} \mathcal{F}^2(D_aF_\lambda) \tag{1.26}$$

Proof. We have

$$\begin{aligned}
\sum_{\lambda\neq 0,a\in\mathbb{F}^n} \mathcal{W}_F^4(a,\lambda) &= \sum_{\lambda\neq 0,a\in\mathbb{F}^n}\ \sum_{x,y,z,w\in\mathbb{F}^n} (-1)^{F_\lambda(x)+F_\lambda(y)+F_\lambda(z)+F_\lambda(w)+a\cdot(x+y+z+w)}\\
&= \sum_{\lambda\neq 0,a\in\mathbb{F}^n}\ \sum_{x,y,z,w\in\mathbb{F}^n} (-1)^{F_\lambda(x)+F_\lambda(y)+F_\lambda(z)+F_\lambda(w)}(-1)^{a\cdot(x+y+z+w)}\\
&= \sum_{x,y,z,w\in\mathbb{F}^n}\ \sum_{\lambda\neq 0\in\mathbb{F}^n} (-1)^{F_\lambda(x)+F_\lambda(y)+F_\lambda(z)+F_\lambda(w)} \sum_{a\in\mathbb{F}^n}(-1)^{a\cdot(x+y+z+w)}\\
&= \sum_{x,y,z,w\in\mathbb{F}^n|x+y+z+w=0} 2^n \sum_{\lambda\neq 0\in\mathbb{F}^n} (-1)^{F_\lambda(x)+F_\lambda(y)+F_\lambda(z)+F_\lambda(w)}\\
&= 2^n \sum_{x,y,z,w\in\mathbb{F}^n|w=x+y+z}\ \sum_{\lambda\neq 0\in\mathbb{F}^n} (-1)^{F_\lambda(x)+F_\lambda(y)+F_\lambda(z)+F_\lambda(w)}
\end{aligned}$$

$$= 2^n \sum_{x,y,z\in\mathbb{F}^n} \sum_{\lambda\neq 0\in\mathbb{F}^n} (-1)^{F_\lambda(x)+F_\lambda(y)+F_\lambda(z)+F_\lambda(x+y+z)}$$

[substituting $y = x + a$ and $z = x + b$ we have]

$$= 2^n \sum_{\lambda\neq 0\in\mathbb{F}^n} \sum_{x,a,b\in\mathbb{F}^n} (-1)^{F_\lambda(x)+F_\lambda(x+a)+F_\lambda(x+b)+F_\lambda(x+a+b)}$$

$$= 2^n \sum_{\lambda\neq 0\in\mathbb{F}^n} \sum_{x,a,b\in\mathbb{F}^n} (-1)^{D_aF_\lambda(x)+D_aF_\lambda(x+b)}$$

$$= 2^n \sum_{\lambda\neq 0,a\in\mathbb{F}^n} \sum_{x,b\in\mathbb{F}^n} (-1)^{D_aF_\lambda(x)+D_aF_\lambda(x+b)}$$

$$= 2^n \sum_{\lambda\neq 0,a\in\mathbb{F}^n} \mathcal{F}^2(D_aF_\lambda).$$ □

By applying Theorem 91 and Lemmas 80 and 92, the following result which can be found in [1] is deduced.

Theorem 93. *Let F be a function from $\mathbb{F}^n$ into $\mathbb{F}^n$. Then*

$$\sum_{\lambda\neq 0,a\in\mathbb{F}^n} \mathcal{F}^2(D_aF_\lambda) \geq 2^{2n+1}(2^n-1). \tag{1.27}$$

Moreover, F is APN if and only if equality holds.

There are a lot of APN functions which are known today (for instance see [5, 34, 50]). We list all the powers for all known power APN functions in Table ??.

We denote the greatest common divisor integers d and d' by (d, d'). We begin with the following well-known result which can be found in [31].

Lemma 94. *For any positive integer k, we have*

(a) $(2^n - 1, 2^k - 1) = 2^{(n,k)} - 1,$

(b) $(2^n - 1, 2^k + 1) = \begin{cases} 1 & \text{if } n/(n,k) \text{ is odd,} \\ 2^{(n,k)} + 1 & \text{if } n/(n,k) \text{ is even.} \end{cases}$

Family	Power	Condition	Proven in
Gold	$2^i + 1$	$(i, n) = 1$	[33]
Kasami	$2^{2i} - 2^i + 1$	$(i, n) = 1$	[35]
Welch	$2^i + 3$	$n = 2i + 1$	[28]
Niho	$2^i + 2^{\frac{i}{2}} - 1, i$ even $2^i + 2^{\frac{3i+1}{2}} - 1, i$ odd	$n = 2i + 1$	[29]
Inverse	$2^{2i} - 1$	$n = 2i + 1$	[43]
Dobbertine	$2^{4i} + 2^{3i} + 2^{2i} + 2^i - 1$	$n = 5i$	[30]

Table 2: APN power functions

We give the proof for quadratic APN power function (Gold APN function).

Theorem 95. *Let k be a positive integer. A quadratic power function $F(x) = x^{2^k+1}$ is APN if $(k, n) = 1$.*

Proof. Note that since F is a quadratic function, so

$$F(x + a) + F(x) + F(a),$$

with $a \in \mathbb{F}_{2^n}$, is a linear function in x whose kernel has the same size as any of its translates such as the solution set of

$$F(x) + F(x + a) = b$$

in $\mathbb{F}_{2^n}$, for any $b \in \mathbb{F}_{2^n}$. Thus, we show that, for any $a \neq 0, b \in \mathbb{F}_{2^n}$,

$$F(x) + (x + a) = b$$

has at most two solutions by simply finding the size of the solution set of

$$F(x + a) + F(x) + F(a) = 0.$$

We have

$$\begin{aligned} F(x+a)+F(x)+F(a) &= (x+a)^{2^k+1}+x^{2^k+1}+a^{2^k+1} \\ &= ax^{2^k}+a^{2^k}x \end{aligned}$$

So it follows that

$$\begin{aligned} \gamma(a) &= |\{x \in \mathbb{F}_{2^n} \mid F(x+a)+F(x)+F(a)=0\}| \\ &= |\{x \in \mathbb{F}_{2^n} \mid ax^{2^k}=a^{2^k}x\}| \\ &= |\{0\} \cup \{x \in \mathbb{F}_{2^n} \mid (x/a)^{2^k-1}=1\}| \end{aligned}$$

Thus, $\gamma(a)=2$ if $(2^n-1, 2^k-1)=1$ and by Lemma 94, this happens when $(n,k)=1$. Hence F is APN if $(n,k)=1$. □

Next, we present the proof of inverse power APN function as done by Nybeg. The inversion mapping $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ of Nybeg is also presented as:

$$F(x) = \begin{cases} x^{-1} & \text{if } x \neq 0 \\ 0 & \text{if } x = 0. \end{cases}$$

This inversion mapping is sometimes called *patched inversion.*

Theorem 96 ([43])**.** *The patched inversion is an APN function for n odd and a differentially 4-uniform for n even.*

Proof. Let $\alpha \neq 0, \beta \in \mathbb{F}_{2^n}$. Consider the equation

$$(x+\alpha)^{-1}+x^{-1}=\beta. \tag{1.28}$$

Assume that $x \neq 0$ and $x \neq \alpha$. Then (1.28) is equivalent to

$$\beta x^2+\alpha\beta x+\alpha=0, \tag{1.29}$$

which has at most two solutions in $\mathbb{F}_{2^n}$. If either $x = 0$ or $x = \alpha$ is solution to (1.28), then both of them are solutions and $\beta = \alpha^{-1}$. In that case (1.29) is equivalent to

$$x^2 + \alpha x + \alpha^2 = 0, \tag{1.30}$$

which may give two more solutions to (1.28). By squaring (1.30) and substituting $x^2 = \alpha x + \alpha^2$ we obtain

$$x(x^3 + \alpha^3) = 0, \tag{1.31}$$

which has no other solutions than $x = 0$ or α if $\gcd(3, 2^n - 1) = 1$ (i.e., if n is odd). If n is even then 3 divides $2^n - 1$. Let $d = \frac{1}{3}(2^n - 1)$. Then there are two more solutions, $x = \alpha^{1+d}$ and $x = \alpha^{1+2d}$. □

Proposition 97 ([7]). *Let a function F from $\mathbb{F}^n$ to itself, with n even, be an APN permutation. If there are elements $a, \lambda \neq 0 \in \mathbb{F}^n$ such that D_aF_λ is constant, then $D_aF_\lambda = 1$.*

Proof. Let $F = (f_1, ..., f_n)$, where $f_i : \mathbb{F}^n \to \mathbb{F}$. Suppose there exist nonzero elements $a, \lambda \neq 0 \in \mathbb{F}^n$ such that $D_aF_\lambda = 0$. Without loss of generality, we can suppose that $F_\lambda = f_i$. Thus, we have

$$\mathrm{Im}(D_aF) = \{(0, y_2, ..., y_n) \mid y_i \in \mathbb{F}\}.$$

Since F is APN, so we have $|\mathrm{Im}(D_aF)| = 2^{n-1}$ which implies that 0 lies in $\mathrm{Im}(D_aF)$, contradicting the fact that F is a permutation. □

We next show that we cannot have a partially-bent component in any APN permutation in even dimension.

Theorem 98 ([7]). *Let a function F from $\mathbb{F}^n$ to itself, with n even, be an APN permutation. Then, for any $\lambda \neq 0 \in \mathbb{F}^n$, no component F_λ is partially-bent.*

Proof. Suppose that F_λ is partially-bent, for some $\lambda \neq 0 \in \mathbb{F}^n$. Then F being a permutation in even dimension and by Remark 63, the linear space of F_λ has at least dimension 2. Let a_1 and a_2 be two distinct nonzero elements in $V(F_\lambda)$. By Proposition 97 and Equation (1.14), we have

$$D_{a_1}F_\lambda(x) = F_\lambda(a_1) = 1 \text{ and } D_{a_2}F_\lambda(x) = F_\lambda(a_2) = 1.$$

Clearly, $a_1 + a_2$ is a nonzero element in $V(F_\lambda)$. But we have

$$D_{a_1+a_2}F_\lambda(x) = F_\lambda(a_1 + a_2) = F_\lambda(a_1) + F_\lambda(a_2) = 0,$$

which contradicts Proposition 97. □

1.2.7 Almost-bent functions

We briefly define and give some results on almost bent functions and the reader is referred to [13, 20, 22] if more details are required.

Definition 99. *A function F from $\mathbb{F}^n$ to itself, with n odd, is said to be* almost-bent (AB) *if $\mathcal{N}(F) = 2^{n-1} - 2^{\frac{n-1}{2}}$. Equivalently, F is almost-bent if any F_λ is semi-bent, for all $\lambda \neq 0 \in \mathbb{F}^n$, that is, the Walsh transform for any F_λ is in $\{0, \pm 2^{\frac{n+1}{2}}\}$.*

Note that, for $m = n$ and n odd, the Sidelnikov-Chabaud-Vaudenay bound coincides with the upper bound $2^{n-1} - 2^{\frac{n-1}{2}}$, the nonlinearity of AB functions.

Next, we state some well-known results which associate AB functions to APN functions.

Proposition 100 ([22])**.** *Let F be an AB function from $\mathbb{F}^n$ to itself, then F is an APN function.*

Theorem 101. *An APN function $F : \mathbb{F}^n \to \mathbb{F}^n$ is AB if and only if one of the following conditions holds:*

(i) all the values in Λ_F are divisible by $2^{\frac{n+1}{2}}$;

(ii) for any $\lambda \in \mathbb{F}^n$, the function F_λ is plateaued.

Proposition 102 ([20])**.** *Let F be a quadratic APN function from $\mathbb{F}^n$ to itself, with n odd, then F is an AB function.*

1.2.8 Equivalences of vectorial Boolean functions

In this subsection, we give some definitions of equivalences for vectorial Boolean functions as in [10].

Definition 103. *Let F and G be functions from $\mathbb{F}^n$ to $\mathbb{F}^m$. Then F and G are*

1. affine equivalent *if there exist two affine permutations:*

$$A : \mathbb{F}^n \to \mathbb{F}^n \text{ and } B : \mathbb{F}^m \to \mathbb{F}^m$$

such that $G(x) = (B \circ F \circ A)(x)$.

2. extended affine equivalent *(or* EA-equivalent *for short) if there exist two affine permutations:*

$$A : \mathbb{F}^n \to \mathbb{F}^n \text{ and } B : \mathbb{F}^m \to \mathbb{F}^m$$

and an affine function $\Lambda : \mathbb{F}^n \to \mathbb{F}^m$ such that

$$G(x) = (B \circ F \circ A)(x) + \Lambda(x).$$

3. CCZ-equivalent *if there exists an affine permutation $\mathcal{A}$ of $\mathbb{F}^n \times \mathbb{F}^m$ such that*

$$\{(x, F(x)), x \in \mathbb{F}^n\} = \mathcal{A}(\{(x, G(x)), x \in \mathbb{F}^n\}).$$

CCZ-equivalence is named after Carlet, Charpin and Zinoviev who introduced the notion.

Affine equivalence is a particular case of EA-equivalence. It can also be shown that EA-equivalence and CCZ-equivalence are both equivalence relations, and EA-equivalence is a particular case of CCZ-equivalence. So it is possible to partition the space of all functions from $\mathbb{F}^n$ to $\mathbb{F}^m$ into CCZ-equivalence classes and then further partition each CCZ-equivalence class into EA-equivalence classes.

The degree, nonlinearity and differential uniformity of functions from $\mathbb{F}^n$ to $\mathbb{F}^m$ are invariant under affine and extended affine equivalences. Under CCZ-equivalence, the nonlinearity and differential uniformity are invariant, but not the degree. Since all three equivalence relations preserve the nonlinearity and differential uniformity, then bent functions are mapped to bent functions and similarly for APN and AB functions. So when searching for or constructing new bent functions or AB functions or APN functions, it is usually important to check that they are inequivalent to the already known ones. However, it should be noted that it is not obvious to check if two functions are equivalent.

Chapter 2

Weight, balancedness, resiliency and nonlinearity of Boolean functions

In this chapter, we are mainly going to look at the weight of cubic functions and other functions, construct and determine balanced Boolean functions whose linear space is trivial, construct resilient functions whose properties are studied with respect to monotone sets, and finally we study the nonlinearity of functions in some special forms.

2.1 On the weight of Boolean functions

In this section, we determine the weight for a special class of cubic functions and other functions. We also establish how the weight of a function can be related to weights of some other functions in a lower dimension.

We start by determining the weight of a given splitting function.

Proposition 104. *Let f be a Boolean function on n variables of degree m defined* *by*

$$f \sim_A \sum_{i=0}^{k-1} \prod_{j=1}^{m} x_{mi+j} + c,$$

with $c \in \mathbb{F}$. *Then* $\mathcal{F}(f) = \pm 2^{n-mk}(2^m - 2)^k$ *and* $\mathrm{w}(f) = 2^{n-1} \pm 2^{n-mk-1}(2^m - 2)^k$.

Proof. Let $c = 0$ and $f_i = \prod_{j=1}^{m} x_{mi+j}$ so that we have $f \sim_A \sum_{i=0}^{k-1} f_i$. Since $\mathcal{F}(f)$ is invariant under affine equivalence (see Remark 18) then, by Corollary 17, we have

$$\mathcal{F}(f) = 2^{n-mk} \prod_{i=0}^{k-1} \mathcal{F}(f_{i\restriction\mathbb{F}^m}).$$

Observe that we have $f_{i\restriction\mathbb{F}^m}(x) = 0$, for all $x \in \mathbb{F}^m \setminus \{\mathbf{1}\}$, and $f_{i\restriction\mathbb{F}^m}(\mathbf{1}) = 1$, so it implies that $\mathcal{F}(f_{i\restriction\mathbb{F}^m}) = 2^m - 2$. Thus, it follows that

$$\mathcal{F}(f) = 2^{n-mk}(2^m - 2)^k.$$

Recall that $\mathrm{w}(f) = 2^{n-1} - \frac{1}{2}\mathcal{F}(f)$, so we have

$$\mathrm{w}(f) = 2^{n-1} - \frac{1}{2}[2^{n-mk}(2^m - 2)^k] = 2^{n-1} - 2^{n-mk-1}(2^m - 2)^k.$$

If $c = 1$ then, by Lemma 13, we have $\mathcal{F}(f) = -2^{n-mk}(2^m - 2)^k$ and by using the fact that $\mathrm{w}(f + 1) = 2^n - \mathrm{w}(f)$, we have $\mathrm{w}(f) = 2^{n-1} + 2^{n-mk-1}(2^m - 2)^k$. □

Remark 105. *The function f in Proposition 104 is balanced if and only if $m = 1$, that is, f is balanced if and only if it is a linear function. If f is quadratic (i.e., $m = 2$) then, by Theorem 7, f is unbalanced and we have $\mathcal{F}(f) = \pm 2^{n-k}$ and $\mathrm{w}(f) = 2^{n-1} \pm 2^{n-k-1}$ just as seen in Corollary 25.*

Now we study the weight and balancedness of Boolean functions given in a special form. We show how the weight of a Boolean function on n variables can be related to the weights of some other functions in a lower dimension.

Any Boolean function can be expressed in the form

$$f \sim_A x_1 g(x_2, ..., x_n) + h(x_2, ..., x_n). \tag{2.1}$$

Observe that $f \sim_A x_1 g(x_2, ..., x_n) + h(x_2, ..., x_n) = x_1(g+h) + (1+x_1)h$. So any Boolean function f on $n+1$ variables can be written in the form

$$f \sim_A x_{n+1} g(x_1, ..., x_n) + (1 + x_{n+1}) h(x_1, ..., x_n). \tag{2.2}$$

We say that f is the *convolutional product* of g and h.

Remark 106. *Since the convolutional product of g and h can be reduced to $f = x_{n+1}(g+h)+h$, so either $\deg(f) = \deg(h)$ [this happens when $\deg(g+h) < \deg(h)$] or $\deg(f) = \max\{\deg(g), \deg(h)\} + 1$.*

Observe that the convolutional product is a special case of the form defined by

$$f \sim_A \left(\prod_{j=1}^{m} x_j\right) g(x_{m+1}, ..., x_{m+n}) + \left(1 + \prod_{j=1}^{m} x_j\right) h(x_{m+1}, ..., x_{m+n}), \tag{2.3}$$

for some positive integer m and Boolean functions g and h on n variables. In fact, for any Boolean function f, there exists a positive integer m such that f can be expressed in the form (2.3).

The next result shows that if the weights of g and h are known, then the weight of f is obtained.

Theorem 107. *Let f be a Boolean function on $n+m$ variables expressed in the form (2.3). Then*

(a) $\mathrm{w}(f) = (2^m - 1)\mathrm{w}(h_{\restriction \mathbb{F}^n}) + \mathrm{w}(g_{\restriction \mathbb{F}^n})$,

(b) f is balanced if and only if $\mathcal{F}(h_{\restriction \mathbb{F}^n}) = -\mathcal{F}(g_{\restriction \mathbb{F}^n})/(2^m - 1)$,

(b) f is balanced if both g and h are balanced,

(d) f is unbalanced if one in $\{g, h\}$ is balanced and the other is not.

Proof. We have

$$f \sim_A \left(\prod_{j=1}^{m} x_j\right) g(x_{m+1}, ..., x_{m+n}) + \left(1 + \prod_{j=1}^{m} x_j\right) h(x_{m+1}, ..., x_{m+n}).$$

(a) Let $X = (x, y) \in \mathbb{F}^m \times \mathbb{F}^n$. Recall that $\mathcal{F}(f)$ is invariant under affine equivalence (see Remark 18), so we have

$$\begin{aligned} \mathcal{F}(f) = \sum_{X \in \mathbb{F}^m \times \mathbb{F}^n} (-1)^{f(X)} &= \sum_{(x,y) \in (\mathbb{F}^m \setminus \{\mathbf{1}\}) \times \mathbb{F}^n} (-1)^{h(y)} + \sum_{(x,y) \in \{\mathbf{1}\} \times \mathbb{F}^n} (-1)^{g(y)} \\ &= (2^m - 1) \sum_{y \in \mathbb{F}^n} (-1)^{h(y)} + \sum_{y \in \mathbb{F}^n} (-1)^{g(y)} \\ &= (2^m - 1)\mathcal{F}(h_{\restriction \mathbb{F}^n}) + \mathcal{F}(g_{\restriction \mathbb{F}^n}) \qquad (2.4) \end{aligned}$$

From Lemma 9, $\mathrm{w}(f) = 2^{m+n-1} - \frac{1}{2}\mathcal{F}(f)$, so we have

$$\begin{aligned} w(f) = 2^{n+m-1} - \frac{1}{2}\mathcal{F}(f) &= 2^{n+m-1} - \frac{1}{2}\left[(2^m - 1)\mathcal{F}(h_{\restriction \mathbb{F}^n}) + \mathcal{F}(g_{\restriction \mathbb{F}^n})\right] \\ &= 2^{n+m-1} - \frac{1}{2}\left[(2^m - 1)(2^n - 2w(h_{\restriction \mathbb{F}^n})) + (2^n - 2w(g_{\restriction \mathbb{F}^n}))\right] \\ &= 2^{n+m-1} - \frac{1}{2}\left[2^{n+m} - 2^{m+1}w(h_{\restriction \mathbb{F}^n}) + 2w(h_{\restriction \mathbb{F}^n}) - 2w(g_{\restriction \mathbb{F}^n})\right] \\ &= (2^m - 1)w(h_{\restriction \mathbb{F}^n}) + w(g_{\restriction \mathbb{F}^n}). \end{aligned}$$

(b) Recall that f is balanced if and only if we have $\mathcal{F}(f) = 0$ if and only if $(2^m - 1)\mathcal{F}(h_{\restriction \mathbb{F}^n}) + \mathcal{F}(g_{\restriction \mathbb{F}^n}) = 0$ if and only if $\mathcal{F}(h_{\restriction \mathbb{F}^n}) = -\mathcal{F}(g_{\restriction \mathbb{F}^n})/(2^m - 1)$.

(c) Suppose that g and h are both balanced. Then $\mathcal{F}(g_{\restriction \mathbb{F}^n}) = \mathcal{F}(h_{\restriction \mathbb{F}^n}) = 0$. By Equation (2.4), it implies that $\mathcal{F}(f) = 0$, and so f is balanced.

(d) Without loss of generality, suppose that g is balanced while h is not. Then $\mathcal{F}(g_{\restriction \mathbb{F}^n}) = 0$ and $\mathcal{F}(h_{\restriction \mathbb{F}^n}) \neq 0$ which, by Equation (2.4), implies that $\mathcal{F}(f) \neq 0$, and so f is unbalanced. □

Remark 108. *If we have $m = 1$ in Theorem 107, then the form (2.3) becomes $f \sim_A x_{n+1}g(x_1, ..., x_n) + (1 + x_{n+1})h(x_1, ..., x_n)$ and $\mathrm{w}(f) = \mathrm{w}(h_{\restriction \mathbb{F}^n}) + \mathrm{w}(g_{\restriction \mathbb{F}^n})$.*

We now consider the weight for a special class of cubic Boolean functions. As alluded to in [16], it is generally difficult to determine the weight of Boolean functions of degree greater than 2. We completely determine the weight for the special class of cubic Boolean functions and give a classification for those which are balanced. This result allows us to construct an algorithm that computes the weight of any cubic function.

Our result for the weight of the special class of cubic functions uses the knowledge of weights of affine and quadratic functions (see Lemma 11 and Corollary 25).

Theorem 109. *Let $f = x_{n+1}g(x_1, ..., x_n)+(1+x_{n+1})h(x_1, ..., x_n)$ be a cubic Boolean function such that $\deg(g), \deg(h) \leq 2$. Then $h \sim_A q = x_1x_2 + \cdots + x_{2k-1}x_{2k}$ or $h \sim_A \bar{q} = q + 1$; $g \sim_A r = x_1x_2 + \cdots + x_{2\ell-1}x_{2\ell}$ or $g \sim_A \bar{r} = r + 1$, with $k, \ell \leq \lfloor \frac{n}{2} \rfloor$, if g and h are unbalanced quadratic. Moreover,*

$$\mathrm{w}(f) = \begin{cases} 2^n & \textit{if both } h \textit{ and } g \textit{ are balanced} \\ 2^{n-1} & \textit{if } h \textit{ (resp. } g\textit{) is bal. quad. and } g \textit{ (resp. } h\textit{)} = 0 \\ 2^n + 2^{n-1} & \textit{if } h \textit{ (resp. } g\textit{) is bal. quad. and } g \textit{ (resp. } h\textit{)} = 1 \\ 2^{n-1} \pm 2^{n-k-1} & \textit{if } h \textit{ is unbal. quad. and } g = 0 \\ 2^n + 2^{n-1} \pm 2^{n-k-1} & \textit{if } h \textit{ is unbal. quad. and } g = 1 \\ 2^{n-1} \pm 2^{n-\ell-1} & \textit{if } h = 0 \textit{ and } g \textit{ is unbal. quad.} \\ 2^n + 2^{n-1} \pm 2^{n-\ell-1} & \textit{if } h = 1 \textit{ and } g \textit{ is unbal. quad.} \\ 2^n \pm 2^{n-k-1} & \textit{if } h \textit{ is unbal. quad. and } g \textit{ is bal.} \\ 2^n \pm 2^{n-\ell-1} & \textit{if } h \textit{ is bal. and } g \textit{ is unbal. quad.} \\ 2^n - 2^{n-k-1} - 2^{n-\ell-1} & \textit{if } h \sim_A q \textit{ and } g \sim_A r \\ 2^n + 2^{n-k-1} + 2^{n-\ell-1} & \textit{if } h \sim_A \bar{q} \textit{ and } g \sim_A \bar{r} \\ 2^n + 2^{n-k-1} - 2^{n-\ell-1} & \textit{if } h \sim_A \bar{q} \textit{ and } g \sim_A r \\ 2^n - 2^{n-k-1} + 2^{n-\ell-1} & \textit{if } h \sim_A q \textit{ and } g \sim_A \bar{r}. \end{cases}$$

Proof. The first part of our assertion follows directly from Theorem 7. To prove the second part of our assertion, we use a direct case-by-case computation. For the weight of quadratic functions, we recall Corollary 25. By Remark 108, we know that $\mathrm{w}(f) = \mathrm{w}(h_{\restriction \mathbb{F}^n}) + \mathrm{w}(g_{\restriction \mathbb{F}^n})$.

If both g and h are balanced, then $\mathrm{w}(f) = \mathrm{w}(h_{\restriction \mathbb{F}^n}) + \mathrm{w}(g_{\restriction \mathbb{F}^n}) = 2^{n-1} + 2^{n-1} = 2^n$. If h (resp. g) is a balanced quadratic and $g = 0$ (resp. $h = 0$), then $\mathrm{w}(f) = 2^{n-1}$. If h (resp. g) is a balanced quadratic function and $g = 1$ (resp. $h = 1$), then $\mathrm{w}(f) = 2^n + 2^{n-1}$. If h is an unbalanced quadratic and $g = 0$, then $\mathrm{w}(f) = 2^{n-1} \pm 2^{n-k-1}$ and if g is an unbalanced quadratic and $h = 0$, then $\mathrm{w}(f) = 2^{n-1} \pm 2^{n-\ell-1}$. If h is unbalanced quadratic and $g = 1$, then $\mathrm{w}(f) = 2^n + 2^{n-1} \pm 2^{n-k-1}$ and if g is an unbalanced quadratic and $h = 1$, then $\mathrm{w}(f) = 2^n + 2^{n-1} \pm 2^{n-\ell-1}$. If h is unbalanced quadratic and g is balanced, then $\mathrm{w}(f) = 2^{n-1} + 2^{n-1} \pm 2^{n-k-1} = 2^n \pm 2^{n-k-1}$ and if g is unbalanced quadratic and h balanced, then we have $\mathrm{w}(f) = 2^{n-1} + 2^{n-1} \pm 2^{n-\ell-1} = 2^n \pm 2^{n-\ell-1}$.

If $h \sim_A q$ and $g \sim_A r$, then we have $\mathrm{w}(h_{\restriction \mathbb{F}^n}) = 2^{n-1} - 2^{n-k-1}$ and $\mathrm{w}(g_{\restriction \mathbb{F}^n}) = 2^{n-1} - 2^{n-\ell-1}$. So it implies that $\mathrm{w}(f) = 2^n - 2^{n-k-1} - 2^{n-\ell-1}$. If $h \sim_A \bar{q}$ and $g \sim_A \bar{r}$, then $\mathrm{w}(h_{\restriction \mathbb{F}^n}) = 2^{n-1} + 2^{n-k-1}$ and $\mathrm{w}(g_{\restriction \mathbb{F}^n}) = 2^{n-1} + 2^{n-\ell-1}$. So it implies that $\mathrm{w}(f) = 2^n + 2^{n-k-1} + 2^{n-\ell-1}$. If $h \sim_A \bar{q}$ and $g \sim_A r$, then we have $\mathrm{w}(h_{\restriction \mathbb{F}^n}) = 2^{n-1} + 2^{n-k-1}$ and $\mathrm{w}(g_{\restriction \mathbb{F}^n}) = 2^{n-1} - 2^{n-\ell-1}$ from which we deduce that $\mathrm{w}(f) = 2^n + 2^{n-k-1} - 2^{n-\ell-1}$. If $h \sim_A q$ and $g \sim_A \bar{r}$, then $\mathrm{w}(h_{\restriction \mathbb{F}^n}) = 2^{n-1} - 2^{n-k-1}$ and $\mathrm{w}(g_{\restriction \mathbb{F}^n}) = 2^{n-1} + 2^{n-\ell-1}$ which implies that $\mathrm{w}(f) = 2^n - 2^{n-k-1} + 2^{n-\ell-1}$. □

Thanks to Theorem 109, we can now state our classification theorem for all balanced functions in our special class of cubic functions:

$$f = x_{n+1} g(x_1, ..., x_n) + (1 + x_{n+1}) h(x_1, ..., x_n),$$

with $\deg(g), \deg(h) \leq 2$.

Corollary 110. *With the same notation from Theorem 109, a cubic Boolean function f is balanced if and only if one of the following holds:*

(a) both h and g are balanced,

(b) $h \sim_A q$ and $g \sim_A \bar{q}$,

(c) $h \sim_A \overline{q}$ *and* $g \sim_A q$.

Proof. In Theorem 109, we notice that there are only three cases for f to be balanced. That is, when both h and g are balanced or $h \sim_A q = x_1x_2 + \cdots + x_{2k-1}x_{2k}$ and $g \sim_A \overline{r} = x_1x_2 + \cdots + x_{2\ell-1}x_{2\ell} + 1$, with $k = \ell$ or $h \sim_A \overline{q} = x_1x_2 + \cdots + x_{2k-1}x_{2k} + 1$ and $g \sim_A r = x_1x_2 + \cdots + x_{2\ell-1}x_{2\ell}$, with $k = \ell$. Hence this completes the proof. □

By applying Lemma 49 and Theorem 109, we can equivalently rewrite Corollary 110 as follows:

Corollary 111. *Let* $f = x_{n+1}g(x_1, ..., x_n) + (1 + x_{n+1})h(x_1, ..., x_n)$ *be a cubic Boolean function on* $n + 1$ *variables, with* $\deg(g), \deg(h) \leq 2$. *Then* f *is balanced if and only if either both* g *and* h *are balanced or* $g = h \circ \varphi + 1$, *for some affinity* φ.

Proof. Recall from Lemma 9 that $\mathcal{F}(g) = 2^n - 2\mathrm{w}(g)$ and by Equation (2.4), we have $\mathcal{F}(f) = \mathcal{F}(g_{\restriction \mathbb{F}^n}) + \mathcal{F}(h_{\restriction \mathbb{F}^n})$. So f is balanced $\iff$ $\mathcal{F}(f) = 0$ $\iff$ $\mathcal{F}(g_{\restriction \mathbb{F}^n}) = -\mathcal{F}(h_{\restriction \mathbb{F}^n})$ $\iff$ $2^n - 2\mathrm{w}(g_{\restriction \mathbb{F}^n}) = -2^n + 2\mathrm{w}(h_{\restriction \mathbb{F}^n})$ $\iff$ $\mathrm{w}(g_{\restriction \mathbb{F}^n}) + \mathrm{w}(h_{\restriction \mathbb{F}^n}) = 2^n$ $\iff$ $\mathrm{w}(g_{\restriction \mathbb{F}^n}) = 2^n - \mathrm{w}(h_{\restriction \mathbb{F}^n})$ $\iff$ $\mathrm{w}(g_{\restriction \mathbb{F}^n}) = \mathrm{w}(h_{\restriction \mathbb{F}^n} + 1)$ $\iff$ either both g and h are balanced or both g and h are unbalanced quadratics related by $g = h \circ \varphi + 1$, for some affinity φ (see Lemma 49). □

Next, we consider a way in which the weight of cubic Boolean functions that cannot be expressed in the form described in Theorem 109 can be determined.

Since any Boolean function expressed in the form (2.1) can be written in the convolutional form as: $f = x_1g(x_2, ..., x_n) + h(x_2, ..., x_n) = x_1(g + h) + (1 + x_1)h$, then we can apply Theorem 107 to deduce the following.

Corollary 112. *Let* g *and* h *be Boolean functions on* n *variables and define a function on* $n + 1$ *variables by* $f = x_{n+1}g(x_1, ..., x_n) + h(x_1, ..., x_n)$. *Then*

(a) $\mathrm{w}(f) = \mathrm{w}([g + h]_{\restriction \mathbb{F}^n}) + \mathrm{w}(h_{\restriction \mathbb{F}^n})$,

(b) f *is balanced if both* $g + h$ *and* h *are balanced,*

(c) f *is unbalanced if one in* $\{g + h, h\}$ *is balanced and the other is not.*

Since our interest is in finding the weight of any cubic Boolean function given in the form: $f = x_1 g(x_2, ..., x_n) + h(x_2, ..., x_n)$, so we assume that g is quadratic while h can be affine, quadratic or cubic. If h is affine or quadratic, then the weight of f is determined by Theorem 109 since in this case the degrees of $g+h$ and h are at most 2, implying that their weights are known. It becomes difficult to find the weight of f if h is cubic since in this case it implies that $g+h$ is also cubic and finding $\mathrm{w}(h_{\restriction \mathbb{F}^{n-1}})$ and $\mathrm{w}([g+h]_{\restriction \mathbb{F}^{n-1}})$ is not easy. However, we can recursively repeat the process of decomposing the function f so that its weight is the sum of weights of some affine or quadratic functions on vector spaces of dimension lower than n over $\mathbb{F}$. For instance, further expressing $g+h$ and h in the form $g+h = x_2 g_1(x_3, ..., x_n) + h_1(x_3, ..., x_n)$ and $h = x_2 g_1'(x_3, ..., x_n) + h_1'(x_3, ..., x_n)$, the weight of f clearly becomes $\mathrm{w}(f) = \mathrm{w}([g_1 + h_1]_{\restriction \mathbb{F}^{n-2}}) + \mathrm{w}(h_{1\restriction \mathbb{F}^{n-2}}) + \mathrm{w}([g_1' + h_1']_{\restriction \mathbb{F}^{n-2}}) + \mathrm{w}(h'_{1\restriction \mathbb{F}^{n-2}})$. We use this idea to build an algorithm which computes the weight of cubic Boolean functions and its efficiency and simplicity relies on the well-known results of the weights of affine and quadratic functions.

Algorithm 1

The following algorithm computes the weight of any cubic function f on $\mathbb{F}^n$:

```
Input:    cubic function $f$,
Output:   $\mathrm{w}(f)$,
Step 1:   express $f$ in the form $f = x_1 g(x_2, ..., x_n) + h(x_2, ..., x_n)$ such that
          $g$ is quadratic,
Step 2:   if $\deg(h) \leq 2$, compute $\mathrm{w}(f)$ by using Theorem 109 and return $\mathrm{w}(f)$,
Step 3:   otherwise, recursively compute the weights of $g + h$ and $h$ by
          applying Step 1 and Step 2,
Step 4:   sum up all the weights computed to obtain $\mathrm{w}(f)$.
```

2.2 Construction of balanced functions

In this section, we are going to construct balanced Boolean functions based on some known functions. In one construction, we have the classification of quadratic functions via affine equivalence in Theorem 7 as a special case.

2.2.1 Balanced Boolean functions

The first two constructions use the well-known result in Proposition 24 and Corollary 112.

Proposition 113. *Let $g = \tilde{g}(x_1, ..., x_{n-1}) + x_n$ and $h = \tilde{h}(x_1, ..., x_{n-2}) + x_{n-1}$ such that $f \sim_A x_{n+1}g(x_1, ..., x_n) + h(x_1, ..., x_{n-1})$. Then f is balanced.*

Proof. It follows from Proposition 24 that both $g + h$ and h are balanced and we deduce by Corollary 112 that f is balanced. □

Lemma 114. *If $f = x_{n+1}g(x_1, ..., x_n) + h(x_1, ..., x_n)$, with $f \in B_{n+1}$ and $g, h \in B_n$, then we have*

$$\mathcal{F}(f) = \mathcal{F}([g + h]_{\restriction \mathbb{F}^n}) + \mathcal{F}(h_{\restriction \mathbb{F}^n}).$$

Proof. Let $X = (x, x_{n+1}) \in \mathbb{F}^n \times \mathbb{F}$. We have

$$\begin{aligned}\mathcal{F}(f) &= \sum_{X \in \mathbb{F}^{n+1}} (-1)^{f(X)} \\ &= \sum_{(x, x_{n+1}) \in \mathbb{F}^n \times \mathbb{F}} (-1)^{x_{n+1}g(x)+h(x)} \\ &= \sum_{x \in \mathbb{F}^n} (-1)^{g(x)+h(x)} + \sum_{x \in \mathbb{F}^n} (-1)^{h(x)} \\ &= \mathcal{F}([g + h]_{\restriction \mathbb{F}^n}) + \mathcal{F}(h_{\restriction \mathbb{F}^n}).\end{aligned}$$ □

Notice that the result which we present in the following proposition is partly an extension of Proposition 113.

Proposition 115. *Let $g_i = \tilde{g}_i(x_{i+1}, ..., x_{n-i}) + x_{n-i+1}$ be a Boolean function on $n - 2i + 1$ variables, with $1 \leq i \leq \lfloor \frac{n}{2} \rfloor$ and $n \geq 3$, and define the two functions on n*

variables as:

$$f_\ell \sim_A \sum_{i=1}^{\ell-1} x_i g_i + g_\ell \tag{2.5}$$

and

$$\bar{f}_\ell \sim_A \sum_{i=1}^{\ell} x_i g_i + c, \tag{2.6}$$

with $\ell \leq \lfloor \frac{n}{2} \rfloor$ and $c \in \mathbb{F}$. Then f_ℓ is balanced and $\bar{f}_\ell$ is unbalanced.

Proof. For a positive integer $t \leq \ell - 1$, define

$$h_t = \sum_{i=t}^{\ell-1} x_i g_i + g_\ell \qquad \text{and} \qquad \bar{h}_t = \sum_{i=t}^{\ell} x_i g_i + c,$$

with $c \in \mathbb{F}$. Since $\mathcal{F}(f_\ell)$ is invariant under affine equivalence (see Remark 18) then, by Lemma 114, we obtain

$$\mathcal{F}(f_\ell) = \sum_{i=1}^{\ell-2} \mathcal{F}(g_i + h_{i+1}) + \mathcal{F}(g_{\ell-1} + g_\ell) + \mathcal{F}(g_\ell) \tag{2.7}$$

and

$$\mathcal{F}(\bar{f}_\ell) = \sum_{i=1}^{\ell-1} \mathcal{F}(g_i + \bar{h}_{i+1}) + \mathcal{F}(g_\ell + c) + \mathcal{F}(c). \tag{2.8}$$

Observe that the functions: $g_i + h_{i+1}$, $g_i + \bar{h}_{i+1}$, $g_{\ell-1} + g_\ell$ and $g_\ell + c$ have the same form as the functions defined in Proposition 24, so they are balanced. This implies that

$$\mathcal{F}(g_\ell + c) = \mathcal{F}(g_{\ell-1} + g_\ell) = \mathcal{F}(g_i + h_{i+1}) = \mathcal{F}(g_i + \bar{h}_{i+1}) = 0.$$

It follows that Equation (2.7) becomes $\mathcal{F}(f_\ell) = 0$, implying that f_ℓ is balanced and

Equation (2.8) becomes $\mathcal{F}(\bar{f}_\ell) = \mathcal{F}(c) \neq 0$ which implies that $\bar{f}_\ell$ is unbalanced. □

Remark 116. *All the quadratic Boolean functions are a special case of the functions constructed in Proposition 115 since if we let $\tilde{g}_i = 0$, for all $1 \leq i \leq \ell$, we obtain their classification via affine equivalence as given in Theorem 7.*

Proposition 117. *Let $f = x_{n+1}g(x_1, ..., x_n) + (1 + x_{n+1})h(x_1, ..., x_n)$, where g and h are Boolean functions on n variables related by $g = h \circ \varphi + 1$, for some affinity φ. Then f is a balanced.*

Proof. Since $g = h \circ \varphi + 1$, for some affinity φ, then clearly $\mathrm{w}(g_{\restriction \mathbb{F}^m}) = 2^n - \mathrm{w}(h_{\restriction \mathbb{F}^m})$. It follows that $\mathrm{w}(f) = \mathrm{w}(g_{\restriction \mathbb{F}^m}) + \mathrm{w}(h_{\restriction \mathbb{F}^m}) = 2^n$, implying that f is balanced. □

In the next result we construct balanced functions on $n + 1$ variables by using any two bent functions on n variables of unequal weight.

Proposition 118. *Let g and h be any bent functions on n variables and define $f = x_{n+1}g(x_1, ..., x_n) + (1 + x_{n+1})h(x_1, ..., x_n)$. Then f is balanced if and only if $\mathrm{w}(g) \neq \mathrm{w}(h)$.*

Proof. Suppose that g and h are any bent functions on n variables. Since $\mathcal{F}(g) = \mathcal{W}_g(0) = \pm 2^{\frac{n}{2}}$, so the weight of g is $\mathrm{w}(g) = 2^{n-1} - \frac{1}{2}\mathcal{F}(g) = 2^{n-1} \pm 2^{\frac{n}{2}-1}$. Similarly, we have $\mathrm{w}(h) = 2^{n-1} \pm 2^{\frac{n}{2}-1}$. Since $\mathrm{w}(f) = \mathrm{w}(g_{\restriction \mathbb{F}^n}) + \mathrm{w}(h_{\restriction \mathbb{F}^n})$, so $\mathrm{w}(f) = 2^n \pm 2^{\frac{n}{2}}$ if $\mathrm{w}(g_{\restriction \mathbb{F}^n}) = \mathrm{w}(h_{\restriction \mathbb{F}^n})$ and $\mathrm{w}(f) = 2^n$ if $\mathrm{w}(g_{\restriction \mathbb{F}^n}) \neq \mathrm{w}(h_{\restriction \mathbb{F}^n})$. Hence f is balanced if and only if $\mathrm{w}(g) \neq \mathrm{w}(h)$. □

We can deduce that the balanced functions in Proposition 118 [also for the unbalanced, that is, if $\mathrm{w}(g) = \mathrm{w}(h)$] are in fact plateaued.

Proposition 119. *Let g and h be any bent functions on n variables and define $f = x_{n+1}g(x_1, ..., x_n) + (1 + x_{n+1})h(x_1, ..., x_n)$. Then f is a plateaued function.*

Proof. Let $\alpha = (a, a_{n+1}) \in \mathbb{F}^n \times \mathbb{F}$ and $X = (x, x_{n+1}) \in \mathbb{F}^n \times \mathbb{F}$. Then we have

$$\begin{aligned}
\mathcal{W}_f(\alpha) &= \sum_{X \in \mathbb{F}^{n+1}} (-1)^{f(X)+\alpha\cdot X} \\
&= \sum_{(x_{n+1},x)\in\mathbb{F}\times\mathbb{F}^n} (-1)^{x_{n+1}g(x)+(1+x_{n+1})h(x)+a\cdot x+a_{n+1}\cdot x_{n+1}} \\
&= \sum_{x\in\mathbb{F}^n} (-1)^{h(x)+a\cdot x} + \sum_{x\in\mathbb{F}^n} (-1)^{g(x)+a\cdot x+a_{n+1}} \\
&= \mathcal{W}_{h_{\restriction\mathbb{F}^n}}(a) + (-1)^{a_{n+1}} W_{g_{\restriction\mathbb{F}^n}}(a). \qquad (2.9)
\end{aligned}$$

Since g and h are bent then, for any $a \in \mathbb{F}^n$, we have $\mathcal{W}_{h_{\restriction\mathbb{F}^n}}(a) = \pm 2^{\frac{n}{2}}$ and $\mathcal{W}_{g_{\restriction\mathbb{F}^n}}(a) = \pm 2^{\frac{n}{2}}$. So, for any $\alpha = (a, a_{n+1}) \in \mathbb{F}^n \times \mathbb{F}$, we deduce from Equation (2.9) that $\mathcal{W}_f(\alpha)$ takes one of the values 0 or $\pm 2^{\frac{n}{2}+1}$. Hence f is plateaued. □

2.2.2 Balanced functions with trivial linear space

In this section, we present some conditions which help to determine whether a derivative of a Boolean function is constant and we utilise them to check some balanced Boolean functions, among the constructed functions in Subsection 2.2.1, whose linear space is trivial. (I acknowledge that this topic was proposed to me by Prof. C. Carlet in a private conversation at "2018 Boolean Functions and their Applications (BFA) conference" in Norway.)

Proposition 120. *Let $f = x_{n+1}g(x_1, ..., x_n) + h(x_1, ..., x_n)$, where g and h are Boolean functions on n variables. Let $\lambda = (a, a_{n+1}) \in \mathbb{F}^n \times \mathbb{F}$. Then*

$$D_\lambda f \sim_A x_{n+1}D_a g + a_{n+1}g + D_a h. \qquad (2.10)$$

Proof. Let $(X, x_{n+1}) \in \mathbb{F}^n \times \mathbb{F}$ and $\lambda = (a, a_{n+1}) \in \mathbb{F}^n \times \mathbb{F}$. We are given that $f = x_{n+1}g(X) + h(X)$. So

$$\begin{aligned}
D_\lambda f &= (x_{n+1} + a_{n+1})g(X + a) + h(X + a) + x_{n+1}g(X) + h(X) \\
&= x_{n+1}\left[g(X + a) + g(X)\right] + a_{n+1}g(X + a) + h(X + a) + h(X)
\end{aligned}$$

$$= x_{n+1}D_ag(X) + a_{n+1}[D_ag(X) + g(X)] + D_ah(X)$$
$$\sim_A x_{n+1}D_ag(X) + a_{n+1}g(X) + D_ah(X) \quad \text{(apply } x_{n+1} \mapsto x_{n+1} + a_{n+1}\text{).} \quad \square$$

For $f \in B_n$, we define the set which contains all $a \in \mathbb{F}^n$ such that D_af is balanced by $\Gamma(f)$, that is, $\Gamma(f) = \{a \mid D_af \text{ is balanced}\}$. This definition was introduced in [7]. We show in the following lemma that the sizes of $\Gamma(f)$ and the linear space of a function are invariant under affine equivalence.

Lemma 121. *Let g_1 and g_2 be Boolean functions on n variables such that $g_1 \sim_A g_2$. Then $|V(g_1)| = |V(g_2)|$ and $|\Gamma(g_1)| = |\Gamma(g_2)|$.*

Proof. Let φ be the affinity of $\mathbb{F}^n$ associated with invertible $M \in GL_n(\mathbb{F})$ (here $GL_n(\mathbb{F})$ is the general linear group of degree n over $\mathbb{F}$) and $w \in \mathbb{F}^n$, that is, $\varphi(y) = M \cdot y + w$, for all $y \in \mathbb{F}^n$. For $a \in \mathbb{F}^n$, we have

$$\begin{aligned} D_ag_1(x) &= D_a(g_2 \circ \varphi)(x) \\ &= g_2(\varphi(x + a)) + g_2(\varphi(x)) \\ &= g_2(M \cdot (x + a) + w) + g_2(\varphi(x)) \\ &= g_2(M \cdot x + M \cdot a + w) + g_2(\varphi(x)) \\ &= g_2(M \cdot a + \varphi(x)) + g_2(\varphi(x)) \\ &= D_{M\cdot a}g_2(\varphi(x)) = (D_{M\cdot a}g_2 \circ \varphi)(x). \end{aligned} \tag{2.11}$$

So it implies that $D_ag_1 = (D_{M\cdot a}g_2) \circ \varphi \sim_A D_{M\cdot a}g_2$. It follows by Proposition 6 that $\mathrm{w}(D_ag_1) = \mathrm{w}(D_{M\cdot a}g_2)$, so we conclude that D_ag_1 is balanced if and only if $D_{M\cdot a}g_2$ is balanced, $D_ag_1 = 0$ if and only if $D_{M\cdot a}g_2 \sim_A 0$, and $D_ag_1 = 1$ if and only if $D_{M\cdot a}g_2 \sim_A 1$. Hence we must have $|V(g_1)| = |V(g_2)|$ and $|\Gamma(g_1)| = |\Gamma(g_2)|$. □

The result that follows gives sufficient condition for a derivative of a function to be constant.

Proposition 122. *Let $f = x_{n+1}g(x_1, ..., x_n) + h(x_1, ..., x_n)$, where g and h are Boolean functions on n variables. Let $\lambda = (a, a_{n+1}) \in \mathbb{F}^n \times \mathbb{F}$. Then $D_\lambda f = c$, with $c \in \mathbb{F}$ (i.e., $D_\lambda f$ is constant) if and only if $D_ag = 0$ and $D_ah = a_{n+1}g + c$.*

Proof. Observe that $D_\lambda f = c$, with $c \in \mathbb{F}$ (i.e., $D_\lambda f$ is constant) if and only if

$$x_{n+1} D_a g + a_{n+1} g + D_a h = c$$

(see the relation 2.10) if and only if $D_a g = 0$ and $D_a h = a_{n+1} g + c$. □

The following result is directly deduced from Proposition 122.

Corollary 123. *Let $f = x_{n+1} g(x_1, ..., x_n) + h(x_1, ..., x_n)$, where g and h are non-constant functions on n variables. Let $\lambda = (a, a_{n+1}) \in \mathbb{F}^n \times \mathbb{F}$. Then $D_\lambda f$ is non-constant if and only if one of the following happens:*

(i) $D_a g \neq 0$,

(ii) $D_a g = 0$ *and* $D_a h \neq a_{n+1} g + c$, *for some* $c \in \mathbb{F}$.

We now determine some functions whose linear space is trivial by using Corollary 123.

Proposition 124. *If $f = x_{n+1} g(x_1, ..., x_n) + h(x_1, ..., x_n)$, with n even and g bent, then f has a trivial linear space.*

Proof. Suppose that g is a bent function and let $\lambda = (a, a_{n+1}) \in \mathbb{F}^n \times \mathbb{F}$. By Proposition 120, we have $D_\lambda f \sim_A x_{n+1} D_a g + a_{n+1} g + D_a h$. Observe that when $\lambda = (0, 1)$ we have $D_\lambda f \sim_A g$ which is a non-constant function since g is bent. If we show that $D_\lambda f$ is non-constant, for all $\lambda = (a, a_{n+1}) \in (\mathbb{F}^n \times \{0\}) \times \mathbb{F}$, then we are done. Since g is bent then $D_a g$ is balanced (i.e. nonzero), for any $a \in \mathbb{F}^n \setminus \{0\}$, and so we conclude by Corollary 123(i) that $D_\lambda f$ is non-constant, for all $\lambda = (a, a_{n+1}) \in (\mathbb{F}^n \times \{0\}) \times \mathbb{F}$. □

In the next Proposition, we apply Proposition 122 to show that some balanced functions constructed in Proposition 113 have trivial linear space.

Proposition 125. *Let a Boolean function f on $n+1$ variables be as constructed in Proposition 113, with $n \geq 3$ odd. If $\tilde{g}$, with restriction to $\mathbb{F}^{n-1}$, is bent then the linear space of f is trivial.*

Proof. Suppose that $\tilde{g}$, with restriction to $\mathbb{F}^{n-1}$, is bent and let $\lambda = (a, a_{n+1}) \in \mathbb{F}^n \times \mathbb{F}$. We know, by Proposition 120, that $D_\lambda f \sim_A x_{n+1}D_a g + a_{n+1}g + D_a h$. Observe that when $\lambda = (0, 1)$ we have $D_\lambda f \sim_A g$ which is clearly non-constant as $\tilde{g}$ is bent. Now we remain to show that $D_\lambda f$ is non-constant, for all $\lambda = (a, a_{n+1}) \in (\mathbb{F}^n \setminus \{0\}) \times \mathbb{F}$. We know from Corollary 123 that if $D_a g$ is nonzero then $D_\lambda f$ is non-constant. So we can simply show that $D_a g$ is nonzero, for all $a \in \mathbb{F}^n \setminus \{0\}$.

Let $a = (\tilde{a}, a_n) \in \mathbb{F}^{n-1} \times \mathbb{F}$, where $\tilde{a} = (a_1, ..., a_{n-1})$. If $\tilde{a} = (0, ..., 0)$ and $a_n = 1$, then we have $D_a g = 1$ which is nonzero. If $a = (\tilde{a}, 1)$, with $\tilde{a} \in \mathbb{F}^{n-1} \setminus \{0\}$, we have $D_a g = D_{\tilde{a}}\tilde{g} + 1$ which must be nonzero as $D_{\tilde{a}}\tilde{g}$ is balanced because $\tilde{g}$ is bent. If $a = (\tilde{a}, 0)$, with $\tilde{a} \in \mathbb{F}^{n-1} \setminus \{0\}$, we have $D_a g = D_{\tilde{a}}\tilde{g}$ which is balanced as $\tilde{g}$ is bent. Thus, $D_a g$ is nonzero, for all $a \in \mathbb{F}^n \setminus \{0\}$. Hence the linear space of f is trivial. □

Notice that we can apply similar arguments as in the proof of Theorem 125 to show that the linear space for any function, with $\tilde{g}_1$ bent, in Proposition 115 is trivial.

Example 126. *For any odd positive integer $n > 1$, a function of the form:*

$$f = x_{n+1}(x_1x_2 + \cdots + x_{n-2}x_{n-1} + x_n) + h(x_1, ..., x_{n-2}) + x_{n-1}$$

is balanced and its linear space is trivial.

Next, we determine whether the linear space of any balanced cubic function of the form: $f = x_{n+1}g(x_1, ..., x_n) + (1 + x_{n+1})h(x_1, ..., x_n)$, with $\deg(g), \deg(h) \leq 2$, is trivial. From Theorem 111, we know that such functions are balanced if and only if either both g and h are balanced or $g = h \circ \varphi + 1$, for some unbalanced quadratics g and h, and an affinity φ.

Proposition 127. *Let $f = x_{n+1}g(x_1, ..., x_n) + (1+x_{n+1})h(x_1, ..., x_n)$ on $\mathbb{F}^{n+1}$, with n even, be cubic such that g and h, with restriction to $\mathbb{F}^n$, are quadratic bent functions related by $g = h \circ \varphi + 1$, for some affinity φ. Then the linear space of f is trivial.*

Proof. Suppose that both g and h, with restrictions to $\mathbb{F}^n$, are bent. Let $\lambda = (a, a_{n+1}) \in \mathbb{F}^n \times \mathbb{F}$. Observe that $f = x_{n+1}(g + h) + h$, and so f is cubic if and only if $g + h$ is a quadratic function. So we assume that $g + h$ is quadratic. By

Proposition 120, we have $D_\lambda f \sim_A x_{n+1} D_a(g+h) + a_{n+1}(g+h) + D_a h$. Observe that when $\lambda = (1,0)$ we have $D_\lambda f \sim_A g+h$ which is non-constant as we assumed that $g+h$ is quadratic.

Next, we prove that $D_\lambda f$ is non-constant, for all $\lambda = (a, a_{n+1}) \in (\mathbb{F}^n \setminus \{0\}) \times \mathbb{F}$. By Corollary 123(i), we know that if $D_a(g+h) \neq 0$, then $D_\lambda f$ is non-constant. Now we show that $D_\lambda f$ is still non-constant if $D_a(g+h) = 0$, for some $a \in \mathbb{F}^n \setminus \{0\}$. Assume that $D_a(g+h) = 0$, for some $a \in \mathbb{F}^n \setminus \{0\}$. Then we have $D_\lambda f \sim_A a_{n+1}(g+h) + D_a h$. If $a_{n+1} = 0$, then $D_\lambda f \sim_A D_a h$, and so it is non-constant since $D_a h$ has to be balanced as h is bent. If $a_{n+1} = 1$, then $D_\lambda f \sim_A g+h+D_a h$ which is also non-constant since $g+h$ is a quadratic and $D_a h$ has degree 1 as it is balanced. □

Finally, we determine some balanced functions constructed in Proposition 118 [i.e., $f = x_{n+1} g(x_1, ..., x_n) + (1 + x_{n+1}) h(x_1, ..., x_n)$, where g and h are both bent and $\mathrm{w}(g) \neq \mathrm{w}(h)$] which have trivial linear space.

Proposition 128. *Let $f = x_{n+1} g(x_1, ..., x_n) + (1 + x_{n+1}) h(x_1, ..., x_n)$, with n even, be a Boolean function on $n+1$ variables such that g and h are both bent. Then the linear space of f is trivial if* $\deg(f) = \max\{\deg(g), \deg(h)\} + 1$.

Proof. Recall that $D_\lambda f \sim_A x_{n+1} D_a(g+h) + a_{n+1}(g+h) + D_a h$, for $\lambda = (a, a_{n+1}) \in \mathbb{F}^n \times \mathbb{F}$ (see Proposition 127). Observe that $f = x_{n+1}(g+h) + h$. We are given that $\deg(f) = \max\{\deg(g), \deg(h)\} + 1$. So it follows that $\deg(g+h) = \max\{\deg(g), \deg(h)\}$, implying that $g+h$ is non-constant since g and h are bent. When $\lambda = (0,1)$, we have $D_\lambda f \sim_A g+h$ which is non-constant.

Now we prove that $D_\lambda f$, for all $\lambda = (a, a_{n+1}) \in (\mathbb{F}^n \setminus \{0\}) \times \mathbb{F}$, is non-constant. If $D_a(g+h) \neq 0$, then $D_\lambda f$ is non-constant, by Corollary 123(i). Suppose that $D_b(g+h) = 0$, for some $b \in \mathbb{F}^n \setminus \{0\}$. We need to show that $D_\lambda f$ is still non-constant, for $\lambda = (b, a_{n+1}) \in (\mathbb{F}^n \setminus \{0\}) \times \mathbb{F}$. In this case, we have $D_\lambda f \sim_A a_{n+1}(g+h) + D_b h$. If $a_{n+1} = 0$ then we have $D_\lambda f \sim_A D_b h$ which is non-constant since $D_b h$ has to be balanced as h is bent. If $a_{n+1} = 1$ then we have $D_\lambda f \sim_A g+h+D_b h$. Since $\deg(g+h) = \max\{\deg(g), \deg(h)\}$, so we have $\deg(g+h) = \max\{\deg(g), \deg(h)\} > \deg(D_b h)$, implying that $\deg(D_\lambda f) = \deg(g+h) > \deg(D_b h)$. So $D_\lambda f$ must be non-constant. Hence the linear space of f is trivial. □

Example 129. *Let $g = x_1x_2 + x_3x_4 + 1$ and $h = x_1x_4 + x_2x_3$. Note that both g and h are bent when restricted to $\mathbb{F}^4$ and are related by $g = h \circ \varphi + 1$, where $\varphi = A(x_1, x_2, x_3, x_4)^T$ and*

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

So we conclude by Corollary 111 and Proposition 127, that the cubic function $f = x_5g + (1 + x_5)h$ is balanced and its linear space is trivial.

2.3 Construction of resilient Boolean functions

In this section, we construct resilient Boolean functions whose properties are extended with respect to monotone sets. As noted in the previous chapter, Braeken et al. introduced the definition of resilient Boolean functions with respect to monotone sets because in this way some trade-offs (seen in the classical approach) between important cryptographic properties are relaxed. In our construction we basically consider the functions expressed in the form (2.3) and also other forms. It should be acknowledged that our ideas for the constructions of these functions were motivated by the (classical) construction of Siegenthaler and Camion et al. which was later modified with respect to monotone sets (in Theorem 76) by Braeken and others.

First, we present a result which shows how the Walsh coefficients for a function expressed in the form (2.3) can be computed in terms of the Walsh coefficients of g and h with restriction to $\mathbb{F}^n$.

Lemma 130. *Let f be a Boolean function of the form (2.3). Let $\alpha = (a, b) \in \mathbb{F}^m \times \mathbb{F}^n$, with $a = (a_1, ..., a_m)$ and $b = (b_1, ..., b_n)$. Then*

$$\mathcal{W}_f(\alpha) = \begin{cases} (2^m - 1)\,\mathcal{W}_{h_{\restriction \mathbb{F}^n}}(b) + \mathcal{W}_{g_{\restriction \mathbb{F}^n}}(b) & \text{if } a = 0 \\ (-1)^{\lambda}\left[\mathcal{W}_{g_{\restriction \mathbb{F}^n}}(b) - \mathcal{W}_{h_{\restriction \mathbb{F}^n}}(b)\right] & \text{otherwise,} \end{cases} \tag{2.12}$$

with $\lambda = a_1 + \cdots + a_m$.

Proof. Let $X = (y, x) \in \mathbb{F}^m \times \mathbb{F}^n$. Then we have

$$\begin{aligned}
\mathcal{W}_f(\alpha) &= \sum_{X \in \mathbb{F}^{m+n}} (-1)^{f(X)+\alpha\cdot X} \\
&= \sum_{(y,x)\in\mathbb{F}^m\setminus\{\mathbf{1}\}\times\mathbb{F}^n} (-1)^{h(x)+a\cdot y+b\cdot x} + \sum_{(y,x)\in\{\mathbf{1}\}\times\mathbb{F}^n} (-1)^{g(x)+a\cdot y+b\cdot x} \\
&= \sum_{(y,x)\in\mathbb{F}^m\times\mathbb{F}^n} (-1)^{h(x)+a\cdot y+b\cdot x} - \sum_{(y,x)\in\{\mathbf{1}\}\times\mathbb{F}^n} (-1)^{h(x)+a\cdot y+b\cdot x} \\
&+ \sum_{(y,x)\in\{\mathbf{1}\}\times\mathbb{F}^n} (-1)^{g(x)+a\cdot y+b\cdot x} \\
&= \sum_{y\in\mathbb{F}^m} (-1)^{a\cdot y} \sum_{x\in\mathbb{F}^n} (-1)^{h(x)+b\cdot x} - (-1)^\lambda \sum_{x\in\mathbb{F}^n} (-1)^{h(x)+b\cdot x} \\
&+ (-1)^\lambda \sum_{x\in\mathbb{F}^n} (-1)^{g(x)+b\cdot x} \\
&= \left(\sum_{y\in\mathbb{F}^m} (-1)^{a\cdot y} - (-1)^\lambda \right) \sum_{x\in\mathbb{F}^n} (-1)^{h(x)+b\cdot x} + (-1)^\lambda \sum_{x\in\mathbb{F}^n} (-1)^{g(x)+b\cdot x} \\
&= \left(\sum_{y\in\mathbb{F}^m} (-1)^{a\cdot y} - (-1)^\lambda \right) \mathcal{W}_{h_{\restriction\mathbb{F}^n}}(b) + (-1)^\lambda \mathcal{W}_{g_{\restriction\mathbb{F}^n}}(b) \\
&= \begin{cases} (2^m - 1)\mathcal{W}_{h_{\restriction\mathbb{F}^n}}(b) + \mathcal{W}_{g_{\restriction\mathbb{F}^n}}(b) & \text{if } a = 0 \\ (-1)^\lambda \left[\mathcal{W}_{g_{\restriction\mathbb{F}^n}}(b) - \mathcal{W}_{h_{\restriction\mathbb{F}^n}}(b)\right] & \text{otherwise.} \end{cases}
\end{aligned}$$

In the final step we used the fact that

$$\sum_{y\in\mathbb{F}^m} (-1)^{a\cdot y} = \begin{cases} 2^m & \text{if } a = 0 \\ 0 & \text{otherwise} \end{cases}$$

and also that $\lambda = 0$ if $a = 0$. □

We next present some results whose proofs use the idea by Braeken et al. in the construction of $\widetilde{\Delta}$-resilient functions as given in Theorem 76.

Theorem 131. *Let $g(x_{m+1}, ..., x_{m+n})$ and $h(x_{m+1}, ..., x_{m+n})$ be two Δ-resilient functions on $\mathbb{F}^n$, with $\Delta \subseteq P(\{m+1, ..., m+n\})$. Then the function, in the form (2.3), given by*

$$f \sim_A \left(\prod_{j=1}^{m} x_j\right) g(x_{m+1}, ..., x_{m+n}) + \left(1 + \prod_{j=1}^{m} x_j\right) h(x_{m+1}, ..., x_{m+n}).$$

is $\widetilde{\Delta}$-resilient, where $\widetilde{\Delta} = \Delta \uplus P(\{1, ..., m\})$.

Proof. Let $\alpha = (a, b) \in \mathbb{F}^m \times \mathbb{F}^n$, with $a = (a_1, ..., a_m)$ and $b = (b_1, ..., b_n)$. By Lemma 130, we have

$$\mathcal{W}_f(\alpha) = \begin{cases} (2^m - 1)\, \mathcal{W}_{h\restriction\mathbb{F}^n}(b) + \mathcal{W}_{g\restriction\mathbb{F}^n}(b) & \text{if } a = 0 \\ (-1)^{\lambda} \left[\mathcal{W}_{g\restriction\mathbb{F}^n}(b) - \mathcal{W}_{h\restriction\mathbb{F}^n}(b)\right] & \text{otherwise,} \end{cases}$$

with $\lambda = a_1 + \cdots + a_m$.

Observe that if α satisfies $\sup(\alpha) \in \widetilde{\Delta}$, then it implies that $\sup(b) \in \Delta$. Since we are given that g and h are Δ-resilient functions (i.e., $\mathcal{W}_{g_{\restriction\mathbb{F}^n}}(b) = \mathcal{W}_{h_{\restriction\mathbb{F}^n}}(b) = 0$), so it follows that $\mathcal{W}_f(\alpha) = 0$ which implies that f is $\widetilde{\Delta}$-resilient. □

We next construct a function on $n + 2$ variables which takes four functions on n variables as input and it is balanced if all the four functions are balanced.

Proposition 132. *Let $\alpha = (\alpha_1, \alpha_2) \in \mathbb{F}^2$ and $g_\alpha(x)$ be functions on n variables. For all $X = (x, x') \in \mathbb{F}^n \times \mathbb{F}^2$, with $x = (x_1, ..., x_n)$ and $x' = (x_{n+1}, x_{n+2})$, define*

$$f(X) = \sum_{\alpha \in \mathbb{F}^2} (x_{n+1}x_{n+2} + \alpha_1 x_{n+1} + \alpha_2 x_{n+2} + \alpha_1 \cdot \alpha_2) g_\alpha(x). \tag{2.13}$$

Let $\tilde{\beta} = (\beta, \beta') \in \mathbb{F}^n \times \mathbb{F}^2$, with $\beta = (\beta_1, ..., \beta_n)$ and $\beta' = (\beta_{n+1}, \beta_{n+2})$. Then

(a) $\mathcal{W}_f(\tilde{\beta}) = \mathcal{W}_{g_{\mathbf{1}\restriction\mathbb{F}^n}}(\beta) + (-1)^{\beta_{n+1}+\beta_{n+2}} \mathcal{W}_{g_{\mathbf{0}\restriction\mathbb{F}^n}}(\beta) + \sum_{\alpha \in \mathbb{F}^2 \setminus \{\mathbf{0}, \mathbf{1}\}} (-1)^{\beta' \cdot \alpha} \mathcal{W}_{g_{\alpha\restriction\mathbb{F}^n}}(\beta)$,

(b) $\mathrm{w}(f) = \sum_{\alpha\in\mathbb{F}^2} \mathrm{w}(g_{\alpha\upharpoonright\mathbb{F}^n})$*,*

(c) f *is balanced if all* g_α*'s are balanced,*

(d) f *is unbalanced if three of* g_α*'s are balanced while one is not.*

Proof. (a) We have

$$
\begin{aligned}
\mathcal{W}_f(\tilde{\beta}) &= \sum_{X\in\mathbb{F}^{n+2}} (-1)^{f(X)+\tilde{\beta}\cdot X} = \sum_{(x,x')\in\mathbb{F}^n\times\mathbb{F}^2} (-1)^{f(x,x')+\beta\cdot x+\beta'\cdot x'} \\
&= \sum_{(x,x')\in\mathbb{F}^n\times\{(0,0)\}} (-1)^{g_{(1,1)}+\beta\cdot x} + \sum_{(x,x')\in\mathbb{F}^n\times\{(1,0)\}} (-1)^{g_{(1,0)}+\beta\cdot x+\beta_{n+1}} \\
&+ \sum_{(x,x')\in\mathbb{F}^n\times\{(0,1)\}} (-1)^{g_{(0,1)}+\beta\cdot x+\beta_{n+2}} + \sum_{(x,x')\in\mathbb{F}^n\times\{(1,1)\}} (-1)^{g_{(0,0)}+\beta\cdot x+\beta_{n+1}+\beta_{n+2}} \\
&= \sum_{x\in\mathbb{F}^n} (-1)^{g_{(1,1)}+\beta\cdot x} + \sum_{x\in\mathbb{F}^n} (-1)^{g_{(1,0)}+\beta\cdot x+\beta_{n+1}} + \sum_{x\in\mathbb{F}^n} (-1)^{g_{(0,1)}+\beta\cdot x+\beta_{n+2}} \\
&+ \sum_{x\in\mathbb{F}^n} (-1)^{g_{(0,0)}+\beta\cdot x+\beta_{n+1}+\beta_{n+2}} \\
&= \mathcal{W}_{{g_{(1,1)}}_{\upharpoonright\mathbb{F}^n}}(\beta) + (-1)^{\beta_{n+1}} \mathcal{W}_{{g_{(1,0)}}_{\upharpoonright\mathbb{F}^n}}(\beta) + (-1)^{\beta_{n+2}} \mathcal{W}_{{g_{(0,1)}}_{\upharpoonright\mathbb{F}^n}}(\beta) \\
&+ (-1)^{\beta_{n+1}+\beta_{n+2}} \mathcal{W}_{{g_{(0,0)}}_{\upharpoonright\mathbb{F}^n}}(\beta) \\
&= \mathcal{W}_{{g_{(1,1)}}_{\upharpoonright\mathbb{F}^n}}(\beta) + (-1)^{\beta_{n+1}+\beta_{n+2}} \mathcal{W}_{{g_{(0,0)}}_{\upharpoonright\mathbb{F}^n}}(\beta) + \sum_{\alpha\in\mathbb{F}^2\setminus\{\mathbf{0},\mathbf{1}\}} (-1)^{\beta'\cdot\alpha} \mathcal{W}_{g_{\alpha\upharpoonright\mathbb{F}^n}}(\beta).
\end{aligned}
\tag{2.14}
$$

(b) We deduce from Equation (2.14) that

$$
\mathcal{F}(f) = \mathcal{W}_f(0) = \sum_{\alpha\in\mathbb{F}^2} \mathcal{W}_{g_{\alpha\upharpoonright\mathbb{F}^n}}(0) = \sum_{\alpha\in\mathbb{F}^2} \mathcal{F}(g_{\alpha\upharpoonright\mathbb{F}^n}). \tag{2.15}
$$

Thus, we have

$$
\mathrm{w}(f) = 2^{n+1} - \frac{1}{2}\mathcal{F}(f) = 2^{n+1} - \frac{1}{2}\left(\sum_{\alpha\in\mathbb{F}^2} \mathcal{F}(g_{\alpha\upharpoonright\mathbb{F}^n})\right)
$$

$$
\begin{aligned}
&= 2^{n+1} - \frac{1}{2}\left(\sum_{\alpha\in\mathbb{F}^2}[2^n - 2\mathrm{w}(g_{\alpha\restriction\mathbb{F}^n})]\right)\\
&= 2^{n+1} - \frac{1}{2}\left(2^{n+2} - 2\sum_{\alpha\in\mathbb{F}^2}\mathrm{w}(g_{\alpha\restriction\mathbb{F}^n})\right)\\
&= \sum_{\alpha\in\mathbb{F}^2}\mathrm{w}(g_{\alpha\restriction\mathbb{F}^n}). \qquad (2.16)
\end{aligned}
$$

(c) Suppose that, for all $\alpha \in \mathbb{F}^2$, g_α is balanced. Then $\mathcal{F}(g_{\alpha\restriction\mathbb{F}^n}) = 0$, for all $\alpha \in \mathbb{F}^2$, from which we deduce, by Equation (2.15), that $\mathcal{F}(f) = 0$. So f is balanced.

(d) If three of g_α's are balanced and one not, then $\mathcal{F}(f) \neq 0$, implying that f is unbalanced. □

Remark 133. *Any Boolean function with algebraic degree at least two can be expressed in form* (2.13).

We utilise our construction in Proposition 132 to show that given any four Δ-resilient functions on n variables we can always construct some functions on $n+2$ variables which are $\widetilde{\Delta}$-resilient.

Theorem 134. *Let $\alpha = (\alpha_1, \alpha_2) \in \mathbb{F}^2$ and $g_\alpha(x)$ be Δ-resilient functions on n variables. Let a function f on $n+2$ variables be as constructed in Proposition 132. Then f is $\widetilde{\Delta}$-resilient, where $\widetilde{\Delta} = \Delta \uplus P(\{n+1, n+2\})$. Furthermore, if $w \in \Gamma$ and for any $u \preceq w$ it holds that $\sum_{\alpha\in\mathbb{F}^2}\mathcal{W}_{g_{\alpha\restriction\mathbb{F}^n}}(u) = 0$, then f is $\widehat{\Delta}$-resilient, where $\widehat{\Delta} = \widetilde{\Delta} \cup P(\sup(w))$.*

Proof. Let $X = (x, x') \in \mathbb{F}^n \times \mathbb{F}^2$, with $x = (x_1, ..., x_n)$ and $x' = (x_{n+1}, x_{n+2})$. We have $f(X) = \sum_{\alpha\in\mathbb{F}^2}(x_{n+1}x_{n+2} + \alpha_1 x_{n+1} + \alpha_2 x_{n+2} + \alpha_1\cdot\alpha_2)g_\alpha(x)$. Let $\tilde{\beta} = (\beta, \beta') \in \mathbb{F}^n \times \mathbb{F}^2$, with $\beta = (\beta_1, ..., \beta_n)$ and $\beta' = (\beta_{n+1}, \beta_{n+2})$.

Observe that if $\tilde{\beta}$ satisfies $\sup(\tilde{\beta}) \in \widetilde{\Delta}$, then $\sup(\beta) \in \Delta$. Since we are given that all g_α's are Δ-resilient functions, so it follows that, for all $\alpha \in \mathbb{F}^2$, $\mathcal{W}_{g_{\alpha\restriction\mathbb{F}^n}}(\beta) = 0$ and by Equation (2.14), we deduce that $\mathcal{W}_f(\tilde{\beta}) = 0$, implying that f is $\widetilde{\Delta}$-resilient.

If $\tilde{\beta}$ satisfies $\sup(\tilde{\beta}) \in \widehat{\Delta}$ then, as in the proof of Theorem 76, we have to deal with two cases:

(i) $\sup(\tilde{\beta}) \in \Delta \uplus P(\{n+1, n+2\})$, which we have already proven that $\mathcal{W}_f(\tilde{\beta}) = 0$,

(ii) $\sup(\tilde{\beta}) \in P(\sup(w))$ for some $w \in \Gamma$. We must have $\beta_{n+1} = \beta_{n+2} = 0$ and thus $\sum_{\alpha\in\mathbb{F}^2} \mathcal{W}_{g_{\alpha\restriction\mathbb{F}^n}}(u) = 0$ since $\tilde{\beta} \preceq w$. □

Remark 135. *Note that if, in Theorem 131, we have two distinct Δ-resilient functions on $\mathbb{F}^n$ then we can construct two (i.e, $2!$) different $\widetilde{\Delta}$-resilient functions on $\mathbb{F}^{n+1}$, and more interesting if, in Theorem 134, we have four distinct Δ-resilient functions on $\mathbb{F}^n$ then we can construct at least 24 (i.e., $4!$) different $\widetilde{\Delta}$-resilient functions on $n+2$ variables. That is, Theorem 134 shows that we can use the knowledge of functions which are Δ-resilient on n variables to construct even more functions which are $\widetilde{\Delta}$-resilient on $n+2$ variables.*

Next, we give a result which shows that Theorem 134 can be extended in such way that the inputs are more than four functions. By applying the same arguments used in the proofs of Proposition 132 and Theorem 134, the following result is deduced.

Corollary 136. *Let $\alpha = (\alpha_1, ..., \alpha_m) \in \mathbb{F}^m$ and $g_\alpha(x)$ be functions on n variables. For all $X = (x, x') \in \mathbb{F}^n \times \mathbb{F}^m$, with $x = (x_1, ..., x_n)$ and $x' = (x_{n+1}, ..., x_{n+m})$, define*

$$f(X) = \sum_{\alpha\in\mathbb{F}^m} \left(\prod_{i=n+1}^{n+m} x_i + \alpha \cdot x' + \prod_{i=1}^{m} \alpha_i \right) g_\alpha(x). \tag{2.17}$$

Let $\tilde{\beta} = (\beta, \beta') \in \mathbb{F}^n \times \mathbb{F}^m$, with $\beta = (\beta_1, ..., \beta_n)$ and $\beta' = (\beta_{n+1}, ..., \beta_{n+m})$. Then

(a) $\mathcal{W}_f(\tilde{\beta}) = \mathcal{W}_{g_{\mathbf{1}\restriction\mathbb{F}^n}}(\beta) + (-1)^{\beta_{n+1}+\cdots+\beta_{n+m}} \mathcal{W}_{g_{\mathbf{0}\restriction\mathbb{F}^n}}(\beta) + \sum_{\alpha\in\mathbb{F}^m\setminus\{\mathbf{0},\mathbf{1}\}} (-1)^{\beta'\cdot\alpha} \mathcal{W}_{g_{\alpha\restriction\mathbb{F}^n}}(\beta)$,

(b) $\mathrm{w}(f) = \sum_{\alpha\in\mathbb{F}^m} \mathrm{w}(g_{\alpha\restriction\mathbb{F}^n})$,

(c) f is balanced if all g_α's are balanced,

(d) f is $\widetilde{\Delta}$-resilient, with $\widetilde{\Delta} = \Delta \uplus P(\{n+1, ..., n+m\})$, if all g_α's are Δ-resilient functions on n variables,

(e) f is $\widehat{\Delta}$-resilient, where $\widehat{\Delta} = \widetilde{\Delta} \cup P(\sup(w))$, if $w \in \Gamma$ and for any $u \preceq w$ it holds that $\sum_{\alpha\in\mathbb{F}^m} \mathcal{W}_{g_{\alpha\restriction\mathbb{F}^n}}(u) = 0$.

Notice that not every Boolean function can be expressed in the form (2.17).

2.4 Nonlinearity of Boolean functions

In this section, we determine the nonlinearity of a splitting function given in the form (104) and we also show how the nonlinearity of a Boolean function can be related to the nonlinearities of some functions in a lower dimension.

Proposition 137. *Let $f \in B_n$, with $\deg(f) = m$ and $m > 1$, be such that*

$$f = \sum_{t=0}^{k-1} \prod_{j=1}^{m} x_{mt+j}.$$

Then $\mathcal{N}(f) = 2^{n-1} - 2^{n-mk-1}(2^m - 2)^k$.

Proof. Let $f_i = \prod_{j=1}^{m} x_{mi+j}$. Then $f = \sum_{i=0}^{k-1} f_i$. Let $l_\alpha(x) = \alpha \cdot x$, where $\alpha, x \in \mathbb{F}^n$. We know, from Proposition 104, that f is not balanced, so it is clear that $f + l_\alpha$ is balanced if l_α has some variables which are not in f (see Proposition 24) and in this case, we have $\mathcal{W}_f(\alpha) = \mathcal{F}(f + l_\alpha) = 0$. Thus, we can assume that $l_\alpha(x) = l_a(X) = a \cdot X$, with $a = (a_0, ..., a_{k-1})$ and $X = (y_0, ..., y_{k-1})$ in $(\mathbb{F}^m)^k$, so that all variables in l_a are also in f. By Corollary 17, we have

$$\mathcal{W}_f(\alpha) = \mathcal{F}(f + l_a) = 2^{n-mk} \prod_{i=0}^{k-1} \mathcal{F}([f_i + l_{a_i}]_{\restriction \mathbb{F}^m}). \tag{2.18}$$

Recall that $\mathcal{N}(f) = 2^{n-1} - \frac{1}{2} \max_{\alpha \in \mathbb{F}^n} |\mathcal{W}_f(\alpha)|$. Clearly, $|\mathcal{W}_f(\alpha)|$ is maximal if all $\mathcal{F}([g_i + l_{a_i}]_{\restriction \mathbb{F}^m})$ are maximal. Observe that

$$\mathcal{F}([f_i + l_{a_i}]_{\restriction \mathbb{F}^m}) = 2^m - 2\mathrm{w}([f_i + l_{a_i}]_{\restriction \mathbb{F}^m})$$

and it is clear that $\mathrm{w}([f_i + l_{a_i}]_{\restriction \mathbb{F}^m}) \neq 0$. So $\mathcal{F}([f_i + l_{a_i}]_{\restriction \mathbb{F}^m})$ is maximal if $a_i = (0, ..., 0)$ since in this case $\mathrm{w}([f_i + l_{a_i}]_{\restriction \mathbb{F}^m}) = \mathrm{w}(f_{i \restriction \mathbb{F}^m}) = 1$. Thus, $|\mathcal{W}_f(\alpha)|$ is maximal if, for all i, we have $\mathcal{F}([f_i + l_{a_i}]_{\restriction \mathbb{F}^m}) = \mathcal{F}(f_{i \restriction \mathbb{F}^m}) = 2^m - 2$, implying that it is maximal when $\alpha = (0, ..., 0)$. Substituting $\mathcal{F}([f_i + l_{a_i}]_{\restriction \mathbb{F}^m}) = 2^m - 2$ in Equation (2.18), we obtain $\mathcal{W}_f(\alpha) = 2^{n-mk}(2^m - 2)^k$. Hence $\mathcal{N}(f) = 2^{n-1} - 2^{n-mk-1}(2^m - 2)^k$. □

Remark 138. *We deduce from Proposition 137 that f is bent if and only if $m = 2$ and $k = n/2$, for n even, otherwise $2^{n-mk-1}2^k(2^{m-1}-1)^k$ would be equal to $2^{\frac{n}{2}-1}$, for some positive integer k, contradicting the fact that $(2^{m-1}-1) \nmid 2^{\frac{n}{2}-1}$ since $(2^{m-1}-1)$ is odd and $2^{\frac{n}{2}-1}$ cannot be divisible by an odd number.*

Theorem 139. *Let f be a Boolean function given in the form (2.3). Then*

$$\mathcal{N}(f) \geq (2^m - 1)\mathcal{N}(h_{\restriction \mathbb{F}^n}) + \mathcal{N}(g_{\restriction \mathbb{F}^n}).$$

Proof. For any two integers c and d, we use the fact that $|c+d| \leq |c| + |d|$. Let $\alpha = (a, b) \in \mathbb{F}^m \times \mathbb{F}^n$, with $a = (a_1, ..., a_m)$ and $b = (b_1, ..., b_n)$. Clearly, by Lemma 130, we have

$$|\mathcal{W}_f(\alpha)| \leq \begin{cases} (2^m - 1)|\mathcal{W}_{h_{\restriction \mathbb{F}^n}}(b)| + |\mathcal{W}_{g_{\restriction \mathbb{F}^n}}(b)| & \text{if } a = 0 \\ |\mathcal{W}_{g_{\restriction \mathbb{F}^n}}(b)| + |\mathcal{W}_{h_{\restriction \mathbb{F}^n}}(b)| & \text{otherwise.} \end{cases}$$

Since

$$|\mathcal{W}_{g_{\restriction \mathbb{F}^n}}(b)| + |\mathcal{W}_{h_{\restriction \mathbb{F}^n}}(b)| \leq (2^m - 1)|\mathcal{W}_{h_{\restriction \mathbb{F}^n}}(b)| + |\mathcal{W}_{g_{\restriction \mathbb{F}^n}}(b)|,$$

then we deduce that, for any $\alpha = (a, b)$, we have

$$|\mathcal{W}(\alpha)| \leq (2^m - 1)|\mathcal{W}_{h_{\restriction \mathbb{F}^n}}(b)| + |\mathcal{W}_{g_{\restriction \mathbb{F}^n}}(b)|.$$

So we have

$$\begin{aligned}
\mathcal{N}(f) &= 2^{n+m-1} - \frac{1}{2} \max_{\alpha \in \mathbb{F}^{n+m}} |\mathcal{W}_f(\alpha)| \\
&\geq 2^{n+m-1} - \frac{1}{2} \max_{b \in \mathbb{F}^n} \left(|(2^m - 1)\mathcal{W}_{h_{\restriction \mathbb{F}^n}}(b)| + |\mathcal{W}_{g_{\restriction \mathbb{F}^n}}(b)| \right) \\
&\geq 2^{n+m-1} - \frac{1}{2}(2^m - 1) \max_{b \in \mathbb{F}^n} |\mathcal{W}_{h_{\restriction \mathbb{F}^n}}(b)| - \frac{1}{2} \max_{b \in \mathbb{F}^n} |\mathcal{W}_{g_{\restriction \mathbb{F}^n}}(b)| \\
&= (2^m - 1)2^{n-1} + 2^{n-1} - \frac{1}{2}(2^m - 1) \max_{b \in \mathbb{F}^n} |\mathcal{W}_{h_{\restriction \mathbb{F}^n}}(b)| - \frac{1}{2} \max_{b \in \mathbb{F}^n} |\mathcal{W}_{g_{\restriction \mathbb{F}^n}}(b)| \\
&= (2^m - 1)2^{n-1} - \frac{1}{2}(2^m - 1) \max_{b \in \mathbb{F}^n} |\mathcal{W}_{h_{\restriction \mathbb{F}^n}}(b)| + 2^{n-1} - \frac{1}{2} \max_{b \in \mathbb{F}^n} |\mathcal{W}_{g_{\restriction \mathbb{F}^n}}(b)| \\
&= (2^m - 1)\mathcal{N}(h_{\restriction \mathbb{F}^n}) + \mathcal{N}(g_{\restriction \mathbb{F}^n}).
\end{aligned}$$

□

Remark 140. *If $m = 1$ then, by Theorem 139, the nonlinearity of f is related to the nonlinearities of g and h as: $\mathcal{N}(f) \geq \mathcal{N}(h_{\restriction \mathbb{F}^n}) + \mathcal{N}(g_{\restriction \mathbb{F}^n})$.*

It is immediate from Theorem 47 and Remark 140 that the following corollary holds.

Corollary 141. *Let f be as described in Theorem 109. Then*

$$\mathcal{N}(f) \geq \begin{cases} 2^{n-1} - 2^{n-k-1} & \text{if } g \text{ is quadratic and } h \text{ affine,} \\ 2^{n-1} - 2^{n-\ell-1} & \text{if } g \text{ is affine and } h \text{ quadratic,} \\ 2^{n} - 2^{n-k-1} - 2^{n-\ell-1} & \text{if both } g \text{ and } h \text{ are quadratic.} \end{cases}$$

Corollary 141 suggests a way of constructing Boolean functions with high nonlinearity.

Remark 142. *If $f \sim_A x_{n+1}g(x_1, ..., x_n) + (1 + x_{n+1})h(x_1, ..., x_n)$ on $\mathbb{F}^{n+1}$, where both $g_{\restriction \mathbb{F}^n}$ and $h_{\restriction \mathbb{F}^n}$ are bent, then $\mathcal{N}(f) \geq 2^{N-1} - 2^{\frac{N-1}{2}}$, with $N = n + 1$. Thus, proposition 128 can be used to construct balanced Boolean functions with high nonlinearity and trivial linear space.*

Theorem 143. *Let a Boolean function f on $n+m$ variables, with $m \geq 1$, be of the form (2.17). Then*

$$\mathcal{N}(f) \geq \sum_{\alpha \in \mathbb{F}^m} \mathcal{N}(g_{\alpha \restriction \mathbb{F}^n}).$$

Proof. Let $X = (x, x') \in \mathbb{F}^n \times \mathbb{F}^m$, with $x = (x_1, ..., x_n)$ and $x' = (x_{n+1}, ..., x_{n+m})$. From (2.17), we have $f(X) = \sum_{\alpha \in \mathbb{F}^m} \left(\prod_{i=n+1}^{n+m} x_i + \alpha \cdot x' + \prod_{i=1}^{m} \alpha_i \right) g_\alpha(x)$. Let $\tilde{\beta} = (\beta, \beta') \in \mathbb{F}^n \times \mathbb{F}^m$, with $\beta = (\beta_1, ..., \beta_n)$and $\beta' = (\beta_{n+1}, ..., \beta_{n+m})$. From Corollary 136, we deduce the following:

$$\begin{aligned} |\mathcal{W}_f(\tilde{\beta})| &= |\mathcal{W}_{g_{\mathbf{1} \restriction \mathbb{F}^n}}(\beta) + (-1)^{\beta_{n+1} + \cdots + \beta_{n+m}} \mathcal{W}_{g_{\mathbf{0} \restriction \mathbb{F}^n}}(\beta) + \sum_{\alpha \in \mathbb{F}^m \setminus \{\mathbf{0}, \mathbf{1}\}} (-1)^{\beta' \cdot \alpha} \mathcal{W}_{g_{\alpha \restriction \mathbb{F}^n}}(\beta)| \\ &\leq \sum_{\alpha \in \mathbb{F}^n} |\mathcal{W}_{g_{\alpha \restriction \mathbb{F}^n}}(\beta)| \end{aligned}$$

So we have,

$$\begin{aligned}\mathcal{N}(f) &= 2^{n+m-1} - \frac{1}{2}\max_{\tilde{\beta}\in\mathbb{F}^n\times\mathbb{F}^m} |\mathcal{W}_f(\tilde{\beta})| \\ &\geq 2^{n+m-1} - \frac{1}{2}\max_{\beta\in\mathbb{F}^n}\left(\sum_{\alpha\in\mathbb{F}^m} |\mathcal{W}_{g_{\alpha\restriction\mathbb{F}^n}}(\beta)|\right) \\ &\geq 2^{n+m-1} - \sum_{\alpha\in\mathbb{F}^m}\frac{1}{2}\max_{\beta\in\mathbb{F}^n} |\mathcal{W}_{g_{\alpha\restriction\mathbb{F}^n}}(\beta)| \\ &= \sum_{\alpha\in\mathbb{F}^m}\left(2^{n-1} - \frac{1}{2}\max_{\beta\in\mathbb{F}^n} |\mathcal{W}_{g_{\alpha\restriction\mathbb{F}^n}}(\beta)|\right) \\ &= \sum_{\alpha\in\mathbb{F}^m}\mathcal{N}(g_{\alpha\restriction\mathbb{F}^n}). \qquad \square\end{aligned}$$

Chapter 3

APN functions and their second-order derivatives

In this chapter, we discuss about the properties of some quantities derived from the behaviour of second-order derivatives of functions. Moreover, we show that these quantities can be used for characterization of quadratic and cubic APN functions. We also show that the quantities can be used to determine whether a quadratic or cubic Boolean functions is bent. Our results starts from Zaninelli's thesis [51].

3.1 The parameter $\mathcal{M}(f)$

In this section, a parameter associated with second-order derivatives of Boolean functions is defined and we study its properties.

Definition 144. *For $a \in \mathbb{F}^n$ and $f \in B_n$, let $Z_a(f) = \{b \in \mathbb{F}^n \mid D_bD_af = 0\}$, $U_a(f) = \{b \in \mathbb{F}^n \mid D_bD_af = 1\}$ and $\mathcal{M}_a(f) = |Z_a(f)| - |U_a(f)|$. Define the parameter $\mathcal{M}(f)$ by*

$$\mathcal{M}(f) := \sum_{a \neq 0 \in \mathbb{F}^n} \mathcal{M}_a(f).$$

We show in the next result that in fact $Z_a(f)$ is a vector space and $U_a(f)$ is either empty or a coset of $Z_a(f)$.

Proposition 145. *Let $f \in B_n$. Then, for any $a \in \mathbb{F}^n$,*

(i) $Z_a(f)$ is a vector space and has nonzero dimension,

(ii) $U_a(f)$ is either the empty set or a coset of $Z_a(f)$.

Proof. Let $a \in \mathbb{F}^n$ and $Z_a(f)$ and $U_a(f)$ be defined as in Definition 144.

(i) It is clear that 0 is in $Z_a(f)$ since $D_0 D_a(f) = 0$. Suppose we have $b_1, b_2 \in Z_a(f)$. Then

$$D_{b_1+b_2} D_a f(x) = D_{b_1} f(x) + D_{b_2} D_a f(x + b_1) = 0 + 0 = 0,$$

implying that $b_1 + b_2 \in Z_a(f)$ [we deduced that $D_{b_2} D_a f(x + b_1) = 0$ since, by Equation (2.11), we have $0 = D_{b_2} D_a f(x) = (D_{I \cdot b_2} D_a f) \circ \varphi = D_{b_2} D_a f(x + b_1)$, with $\varphi(x) = Ix + b_1$]. To show that it is of nonzero dimension, observe that if $a = 0$ then $Z_a(f) = \mathbb{F}^n$ and if $a \neq 0$, then we have $D_a D_a f(x) = 0$, implying that $\{0, a\} \subseteq Z_a(f)$. So the dimension of $Z_a(f)$ is at least 1.

(ii) Suppose that $U_a(f) \neq \varnothing$. For any $b_1 \in U_a(f)$, we claim that $b_1 + Z_a(f) = U_a(f)$. Let $b_2 = b_1 + d$, with $d \in Z_a(f)$. We have

$$D_{b_2} D_a f(x) = D_{b_1+d} D_a f(x) = D_{b_1} D_a f(x) + D_d D_a f(x + b_1) = 1 + 0 = 1.$$

Thus, $b_2 \in U_a(f)$. Conversely, for any $e \in U_a(f)$, we have

$$D_{b_1+e} D_a f(x) = D_{b_1} D_a f(x) + D_e D_a f(x + b_1) = 1 + 1 = 0.$$

It follows that $e + b_1 \in Z_a(f) \implies e \in b_1 + Z_a(f)$. Thus $U_a(f)$ is either empty or a coset of $Z_a(f)$ set. □

Proposition 146. *Let $f \in B_n$ be a Boolean function with* $\deg(f) \in \{2, 3\}$. *Then, for some positive even integer $j < n$, and any nonzero $a \in \mathbb{F}^n$, we have*

$$\mathcal{M}_a(f) = \begin{cases} 0 & \textit{if and only if } D_a f \textit{ balanced} \\ 2^n & \textit{if and only if } D_a f \textit{ is constant} \\ 2^{n-j} & \textit{otherwise.} \end{cases}$$

Proof. We know that $\deg(f) \in \{2, 3\}$ implies $\deg(D_af) \in \{0, 1, 2\}$. It is clear from the definition of $\mathcal{M}_a(f)$ that $\deg(D_af) = 0 \iff \mathcal{M}_a(f) = 2^n$.

Now suppose that $\deg(D_af) = 1$. Then D_af is a non-constant affine function, so it is balanced. That is, we can write $D_af(x) = v \cdot x + c$, for some $v \in \mathbb{F}^n \setminus \{0\}$ and $c \in \mathbb{F}$. Observe that

$$\begin{aligned} D_bD_af(x) &= v \cdot x + c + v \cdot (x + b) + c \\ &= v \cdot x + v \cdot x + v \cdot b \\ &= v \cdot b. \end{aligned}$$

So we have $D_bD_af(x) = 0 \iff b \in W =< v >^\perp$ and $D_bD_af(x) = 1 \iff b \in W^c$ (note that $A^\perp$ denotes the dual set and A^c denotes the complement of a set A). Thus, $Z_a(f) = W$ and $U_a(f) = W^c$. It is clear that $|W| = |W^c| = 2^{n-1}$. So we have $\mathcal{M}_a(f) = 0$.

Finally, suppose that $\deg(D_af) = 2$, that is, by Theorem 7, we know that $D_af \sim_A x_1x_2 + \cdots + x_{2i-1}x_{2i} + x_{2i+1}$, with $i \leq \lfloor (n-1)/2 \rfloor$, if D_af is balanced and $D_af \sim_A x_1x_2 + \cdots + x_{2i-1}x_{2i} + e$, with $i \leq \lfloor n/2 \rfloor$ and $e \in \mathbb{F}$, if D_af is unbalanced. Suppose that D_af is balanced. Then

$$|Z_a(f)| = |\{c = (c_1, ..., c_n) \in \mathbb{F}^n \mid c_1 = \cdots = c_{2i+1} = 0\}|$$

and

$$|U_a(f)| = |\{c = (c_1, ..., c_n) \in \mathbb{F}^n \mid c_1 = \cdots = c_{2i} = 0, c_{2i+1} = 1\}|.$$

Observe that in both cases, $|Z_a(f)| = |U_a(f)| = 2^{n-2i-1}$. Hence $\mathcal{M}_a(f) = 0$. Now suppose that D_af is unbalanced. Then we have

$$|Z_a(f)| = |\{c = (c_1, ..., c_n) \in \mathbb{F}^n \mid c_1 = \cdots = c_{2i} = 0\}|$$

and $U_a(f) = \varnothing$. It follows that $|Z_a(f)| = 2^{n-2i}$ and $|U_a(f)| = 0$. So it implies that $\mathcal{M}_a(f) = 2^{n-2i}$. □

3.2 $\mathcal{M}(f)$ and partially-bent functions

In this section, we study some properties of the parameter $\mathcal{M}(f)$ of a Boolean function f in relation to quadratic and cubic partially-bent functions.

Theorem 147. *For any quadratic function or cubic partially-bent function f, we have*

$$\mathcal{M}(f) = 2^n(2^k - 1),$$

where $k = \dim V(f)$.

Proof. We know, from Proposition 146, that $\mathcal{M}_a(f) = 0$ if and only if D_af is balanced and $\mathcal{M}_a(f) = 2^n$ if and only if D_af is a constant. Recall that all quadratic functions are partially-bent. So we deduce, from the definition, that for any quadratic function or cubic partially-bent function f, D_af is constant if and only if $a \in V(f)$ and D_af is balanced if and only if $a \notin V(f)$. Thus

$$\begin{aligned}\mathcal{M}(f) &= \sum_{a\neq 0\in\mathbb{F}^n} \mathcal{M}_a(f)\\ &= \sum_{a\neq 0\in V(f)} \mathcal{M}_a(f) + \sum_{a\notin V(f)} \mathcal{M}_a(f)\\ &= \sum_{a\neq 0\in V(f)} 2^n + \sum_{a\notin V(f)} 0\\ &= 2^n(2^k-1),\end{aligned}$$

with $k = \dim V(f)$. □

Corollary 148. *Let $f \in B_n$ be a quadratic or cubic function. Then f is bent if and only if $\mathcal{M}(f) = 0$.*

Proof. For any quadratic or cubic function f, we deduce, from Proposition 146, that $\mathcal{M}(f) = 0$ if and only if $\mathcal{M}_a(f) = 0$, for all $a \neq 0 \in \mathbb{F}^n$ if and only if D_af is balanced, for all $a \neq 0 \in \mathbb{F}^n$ if and only if f is bent (see Theorem 54). □

If a function f is bent, then $k = \dim V(f) = 0$ and so, by Proposition 147, we have $\mathcal{M}(f) = 0$. So Proposition 147 can also be used to deduce Corollary 148.

Lemma 149. *Let $f \in B_n$, with n odd, be quadratic. Then $\dim V(f) \geq 1$ and equality holds if and only if f is semi-bent.*

Proof. Recall that the size of linear space is invariant under affine equivalence (see Lemma 121). From Theorem 7, we have $f \sim_A x_1x_2 + \cdots + x_{2i-1}x_{2i} + x_{2i+1}$, with $i \leq \lfloor n/2 \rfloor$, if f is balanced and $f \sim_A x_1x_2 + \cdots + x_{2i-1}x_{2i} + e$, with $i \leq \lfloor n/2 \rfloor$ and $e \in \mathbb{F}$, if f is unbalanced. So we have

$$|V(f)| = |\{c = (c_1, ..., c_n) \in \mathbb{F}^n \mid c_1 = \cdots = c_{2i} = 0, i \leq \lfloor n/2 \rfloor\}|.$$

So it follows that $|V(f)| = 2^{n-2i}$, implying that $\dim V(f) \geq 1$. By Corollary 69, we know that f is semi-bent if and only if

$$f \sim_A x_1x_2 + \cdots + x_{n-2}x_{n-1} + x_n$$

or

$$f \sim_A x_1x_2 + \cdots + x_{n-2}x_{n-1} + e,$$

with $e \in \mathbb{F}$, from which we deduce that f is semi-bent $\iff$ $\dim V(f) = 1$. □

By Proposition 147 and Lemma 149, the following corollary holds.

Corollary 150. *For n odd, a quadratic Boolean function f is semi-bent if and only if $\mathcal{M}(f) = 2^n$.*

3.3 $\mathcal{M}(F)$ and APN functions

We extend the definition of the parameter described in Section 3.2 to vectorial Boolean functions. For a vectorial Boolean function F, we write

$$\mathcal{M}(F) = \sum_{\lambda \neq 0 \in \mathbb{F}^n} \mathcal{M}(F_\lambda). \tag{3.1}$$

It is clear that $\mathcal{M}(F)$ is defined based on the second-order derivatives of components of F. Next, we establish the link between the 4th power moment of the Walsh transform and the parameter $\mathcal{M}(F)$, and consequently a natural characterization of APN functions based on the latter quantity is derived.

Lemma 151. *Let F be a function from $\mathbb{F}^n$ to itself, with $\deg(F) \in \{2, 3\}$. Then*

$$\sum_{\lambda \neq 0, a \in \mathbb{F}^n} \mathcal{W}_F^4(a, \lambda) = 2^{3n}(2^n - 1) + 2^{2n}\mathcal{M}(F).$$

Proof. We have

$$\begin{aligned}
\sum_{\lambda \neq 0, a \in \mathbb{F}^n} \mathcal{W}_F^4(a, \lambda) &= \sum_{\lambda \neq 0 \in \mathbb{F}^n} \sum_{a \in \mathbb{F}^n} \sum_{x,y,z,w \in \mathbb{F}^n} (-1)^{F_\lambda(x)+F_\lambda(y)+F_\lambda(z)+F_\lambda(w)+a\cdot(x+y+z+w)} \\
&= \sum_{\lambda \neq 0 \in \mathbb{F}^n} \sum_{a \in \mathbb{F}^n} \sum_{x,y,z,w \in \mathbb{F}^n} (-1)^{F_\lambda(x)+F_\lambda(y)+F_\lambda(z)+F_\lambda(w)}(-1)^{a\cdot(x+y+z+w)} \\
&= \sum_{\lambda \neq 0 \in \mathbb{F}^n} \sum_{x,y,z,w \in \mathbb{F}^n} (-1)^{F_\lambda(x)+F_\lambda(y)+F_\lambda(z)+F_\lambda(w)} \sum_{a \in \mathbb{F}^n} (-1)^{a\cdot(x+y+z+w)} \\
&= \sum_{\lambda \neq 0 \in \mathbb{F}^n} \sum_{x,y,z,w \in \mathbb{F}^n | x+y+z+w=0} 2^n (-1)^{F_\lambda(x)+F_\lambda(y)+F_\lambda(z)+F_\lambda(w)} \\
&= 2^n \sum_{\lambda \neq 0 \in \mathbb{F}^n} \sum_{x,y,z,w \in \mathbb{F}^n | w=x+y+z} (-1)^{F_\lambda(x)+F_\lambda(y)+F_\lambda(z)+F_\lambda(w)} \\
&= 2^n \sum_{\lambda \neq 0 \in \mathbb{F}^n} \sum_{x,y,z \in \mathbb{F}^n} (-1)^{F_\lambda(x)+F_\lambda(y)+F_\lambda(z)+F_\lambda(x+y+z)} \\
&\text{[substituting } y = x+b \text{ and } z = x+c \text{ we have]} \\
&= 2^n \sum_{\lambda \neq 0 \in \mathbb{F}^n} \sum_{x,b,c \in \mathbb{F}^n} (-1)^{F_\lambda(x)+F_\lambda(x+b)+F_\lambda(x+c)+F_\lambda(x+b+c)} \\
&= 2^n \sum_{\lambda \neq 0 \in \mathbb{F}^n} \sum_{x,b,c \in \mathbb{F}^n} (-1)^{D_bF_\lambda(x)+D_bF_\lambda(x+c)} \\
&= 2^n \sum_{\lambda \neq 0 \in \mathbb{F}^n} \sum_{x,b,c \in \mathbb{F}^n} (-1)^{D_cD_bF_\lambda(x)} \qquad (3.2) \\
&[\deg(D_cD_bF_\lambda) = 1 \implies \sum_{x \in \mathbb{F}^n} (-1)^{D_cD_bF_\lambda(x)} = 0, \text{ so we have}]
\end{aligned}$$

$$
\begin{aligned}
&= 2^n \sum_{\lambda \neq 0 \in \mathbb{F}^n} \sum_{x,b,c \in \mathbb{F}^n \,|\, \deg(D_cD_bF_\lambda)=0} (-1)^{D_cD_bF_\lambda(x)} \\
&= 2^n \sum_{\lambda \neq 0 \in \mathbb{F}^n} 2^n \sum_{b,c \in \mathbb{F}^n \,|\, \deg(D_cD_bF_\lambda)=0} (-1)^{D_cD_bF_\lambda(0)} \\
&= 2^{2n} \sum_{\lambda \neq 0 \in \mathbb{F}^n} \left(\sum_{b,c \in \mathbb{F}^n | D_cD_bF_\lambda=0} (-1)^0 + \sum_{b,c \in \mathbb{F}^n | D_cD_bF_\lambda=1} (-1)^1 \right) \\
&= 2^{2n} \sum_{\lambda \neq 0 \in \mathbb{F}^n} (|\{b, c \in \mathbb{F}^n \mid D_cD_bF_\lambda = 0\}| - |\{b, c \in \mathbb{F}^n \mid D_cD_bF_\lambda = 1\}|) \\
&= 2^{2n} \sum_{\lambda \neq 0 \in \mathbb{F}^n} \sum_{b \in \mathbb{F}^n} (|\{c \in \mathbb{F}^n \mid D_cD_bF_\lambda = 0\}| - |\{c \in \mathbb{F}^n \mid D_cD_bF_\lambda = 1\}|) \\
&= 2^{2n} \sum_{\lambda \neq 0 \in \mathbb{F}^n} (|\{c \in \mathbb{F}^n \mid D_cD_0F_\lambda = 0\}| - |\{c \in \mathbb{F}^n \mid D_cD_0F_\lambda = 1\}|) \\
&+ 2^{2n} \sum_{\lambda \neq 0 \in \mathbb{F}^n} \sum_{b \neq 0 \in \mathbb{F}^n} \mathcal{M}_b(F_\lambda) \\
&= 2^{2n} \sum_{\lambda \neq 0 \in \mathbb{F}^n} (|\{c \in \mathbb{F}^n \mid D_c(0) = 0\}| - |\{c \in \mathbb{F}^n \mid D_c(0) = 1\}|) \\
&+ 2^{2n} \sum_{\lambda \neq 0 \in \mathbb{F}^n} \sum_{b \neq 0 \in \mathbb{F}^n} \mathcal{M}_b(F_\lambda) \\
&= 2^{2n} \sum_{\lambda \neq 0 \in \mathbb{F}^n} (2^n - 0) + 2^{2n} \sum_{\lambda \neq 0 \in \mathbb{F}^n} \sum_{b \neq 0 \in \mathbb{F}^n} \mathcal{M}_b(F_\lambda) \\
&= 2^{2n} \sum_{\lambda \neq 0 \in \mathbb{F}^n} 2^n + 2^{2n} \sum_{\lambda \neq 0 \in \mathbb{F}^n} \sum_{b \neq 0 \in \mathbb{F}^n} \mathcal{M}_b(F_\lambda) \\
&= 2^{3n}(2^n - 1) + 2^{2n} \sum_{\lambda \neq 0 \in \mathbb{F}^n} \sum_{b \neq 0 \in \mathbb{F}^n} \mathcal{M}_b(F_\lambda) \\
&= 2^{3n}(2^n - 1) + 2^{2n} \sum_{\lambda \neq 0 \in \mathbb{F}^n} \mathcal{M}(F_\lambda) = 2^{3n}(2^n - 1) + 2^{2n}\mathcal{M}(F). \qquad \square
\end{aligned}
$$

By Lemma 151 and Theorem 91, the following result is deduced.

Theorem 152. *Let F be a function from $\mathbb{F}^n$ to itself, with $\deg(F) \in \{2, 3\}$. Then*

$$\mathcal{M}(F) \geq 2^n(2^n - 1).$$

Moreover, F is APN if and only if equality holds.

Proof. By Lemma 80 and Theorem 91, we have

$$\sum_{\lambda\neq 0, a\in\mathbb{F}^n} \mathcal{W}_F^4(a,\lambda) \geq 2^{3n+1}(2^n-1)$$

and equality holds if and only if F is APN. Since, by Lemma 151, we have

$$\sum_{\lambda\neq 0, a\in\mathbb{F}^n} \mathcal{W}_F^4(a,\lambda) = 2^{3n}(2^n-1) + 2^{2n}\mathcal{M}(F),$$

so must have

$$\mathcal{M}(F) \geq 2^n(2^n-1)$$

and equality holds if and only if F is APN. □

By Proposition 147, the following result is deduced.

Corollary 153. *For any quadratic function $F : \mathbb{F}^n \to \mathbb{F}^n$, we have*

$$\mathcal{M}(F) = 2^n \sum_{\lambda\neq 0\in\mathbb{F}^n} (2^{\dim V(F_\lambda)} - 1). \tag{3.3}$$

Proof. For any $\lambda \neq 0 \in \mathbb{F}^n$, we have $\mathcal{M}(F_\lambda) = 2^n(2^{\dim V_\lambda} - 1)$ (see Proposition 147). We conclude from Equation (3.1) that $\mathcal{M}(F) = 2^n \sum_{\lambda\neq 0\in\mathbb{F}^n}(2^{\dim V(F_\lambda)} - 1)$. □

Example 154. *Let $F(x_1, x_2, x_3) = (f_1, f_2, f_3)$, with $f_1 = x_1x_3 + x_2x_3 + x_1$, $f_2 = x_2x_3 + x_1 + x_2$ and $f_3 = x_1x_2 + x_1 + x_2 + x_3$ in B_3. It can be easily verified that all components are quadratic. Clearly, the dimension of their linear spaces is 1. By Corollary 153, we have $\mathcal{M}(F) = 2^3(2^3 - 1) = 56$ and so, by Theorem 152, we conclude that F is APN. Moreover, all components are balanced, implying that F is an APN permutation.*

We deduce, from Lemma 149 and Corollary 153 that the following corollary holds.

Corollary 155. *Let F be a quadratic function from $\mathbb{F}^n$ to itself, with n odd. Then F is APN if and only if, for all $\lambda \neq 0 \in \mathbb{F}^n$, $\mathcal{M}(F_\lambda) = 2^n$.*

The Walsh transform in zero of the second-order derivatives of a function can be linked to the 4th power moment, and consequently a natural characterization of APN functions based on the former is obtained. The next lemma follows directly from Equation (3.2).

Lemma 156. *For a vectorial Boolean function $F : \mathbb{F}^n \to \mathbb{F}^n$, we have*

$$\sum_{\lambda \neq 0, a \in \mathbb{F}^n} \mathcal{W}_F^4(a, \lambda) = 2^n \sum_{\lambda \neq 0, c, b \in \mathbb{F}^n} \mathcal{F}(D_b D_c F_\lambda).$$

By Theorem 91 and Lemma 156, the following result is deduced.

Theorem 157. *Let $F : \mathbb{F}^n \to \mathbb{F}^n$ be a vectorial Boolean function. Then*

$$\sum_{\lambda \neq 0, c, b \in \mathbb{F}^n} \mathcal{F}(D_b D_c F_\lambda) \geq 2^{2n+1}(2^n - 1).$$

Moreover, F is APN if and only if equality holds.

Observe that Theorem 157 can also be directly deduced from Theorem 93.

Chapter 4

APN functions in even dimension

In this chapter, we study the linear spaces of components of APN functions in even dimension. We show that for any APN function there is a component with trivial linear space. We also present a general form of the number of bent components in quadratic APN functions and provide bounds on their number. Furthermore, we count the number of bent components in any quadratic power function.

4.1 Linear spaces for components of APN functions

In this section, we mainly show that some components of any APN function in even dimension must have a trivial linear space.

Definition 158. *Let a function f on n variables be a splitting function, that is, $f \sim_A g(x_1, ..., x_i) + h(x_{i+1}, ..., x_n)$, with a positive integer $i < n$. We call i a* splitting number *of f and $S(f)$ denotes the set of all i (the splitting numbers of f). We define a* splitting index *of f by the number $\sigma(f) = \min S(f)$*

Remark 159. *Let $f \in B_n$ be a splitting function. Then*

1. *i is a splitting number $\iff$ $n - i$ is a splitting number,*

2. *$\sigma(f) \in \{1, ..., \lfloor n/2 \rfloor\}$ (we deduce from 1.).*

Our main result in this section largely depends on the following two lemmas.

Lemma 160. *Let $f \in B_n$. Then $\sigma(f) = 1$ if and only if $\dim V(f) \geq 1$.*

Proof. Suppose that $\sigma(f) = 1$, that is, $f \sim_A \tilde{f} = g(x_1) + h(x_2, ..., x_n)$. So we have $\tilde{f} = f \circ \varphi$, where $\varphi(y) = M \cdot y + w$, for some $w \in \mathbb{F}^n$ and invertible $M \in GL_n(\mathbb{F})$. Clearly $D_{e_1}\tilde{f}$ is constant. By Equation (2.11) in the proof Lemma 121, we have $D_{e_1}\tilde{f} = (D_{M \cdot e_1} f) \circ \varphi$ and since $\mathrm{w}(D_{e_1}\tilde{f}) = \mathrm{w}(D_{M \cdot e_1} f)$ (see Proposition 6), so $D_{M \cdot e_1} f$ must also be constant. Note that $M \cdot e_1 \neq 0$ since M is a linear isomorphism. Thus both 0 and $M \cdot e_1$ are in $V(f)$ which implies that $\dim V(f) \geq 1$.

Conversely, suppose that $\dim V(f) \geq 1$, that is, $\exists a \neq 0 \in V(f)$ such that $D_a f = c$, with $c \in \mathbb{F}$. We can take the $\mathbb{F}$-linear isomorphism E of $\mathbb{F}^n$ that sends $e_1 \mapsto E \cdot e_1 = a$ so that we have $\tilde{f} = f \circ E$ and thus,

$$D_{e_1}\tilde{f} = (D_{E \cdot e_1} f) \circ E = (D_a f) \circ E = (c) \circ E = c$$

which implies that $D_{e_1}\tilde{f}$ is constant. Since we have $D_{e_1}\tilde{f} = c$, we can write $\tilde{f} = cx_1 + h(x_2, ..., x_n)$. Hence we have $\sigma(f) = 1$ since $f \sim_A \tilde{f}$. □

Lemma 161. *Let $f \in B_n$, with n even. If $\sigma(f) = 1$, then $|\Gamma(f)| \leq 2^n - 4$.*

Proof. Suppose $f \in \mathbb{F}^n$ has $\sigma(f) = 1$, that is, $f \sim_A \tilde{f} = cx_1 + h(x_2, ..., x_n)$, with $c \in \mathbb{F}$. By Equation (2.11) in Lemma 121, we have $|\Gamma(f)| = |\Gamma(\tilde{f})|$, so we can simply consider $|\Gamma(\tilde{f})|$. It is clear that 0 and e_1 are both not in $\Gamma(\tilde{f})$ since $D_0\tilde{f} = 0$ and $D_{e_1}\tilde{f} = c$. Suppose that these are the only ones, that is, $|\Gamma(\tilde{f})| = 2^n - 2$. This implies that, for all $a \in \mathbb{F}^n \setminus \{0, e_1\}$, $D_a\tilde{f}$ is balanced.

Let $W =< e_2, ..., e_n >$ and denote $W^* = W \setminus \{0\}$. Clearly, W^* is contained in $\mathbb{F}^n \setminus \{0, e_1\}$, that is, $W^* \subset \Gamma(\tilde{f})$. So, for all $a \in W^*$, $D_a\tilde{f}$ is balanced. It is clear that $W \simeq \mathbb{F}^{n-1}$. Observe that, for any $a = (0, b) \in \{0\} \times (\mathbb{F}^{n-1} \setminus \{0\}) = W^*$, we have $D_a\tilde{f} = D_b h$ as the first coordinate of a is 0. Since $D_a\tilde{f}$ does not depend on x_1 then, by Remark 27, we have $2^{n-1} = \mathrm{w}(D_a\tilde{f}) = \mathrm{w}(D_b h) = 2\mathrm{w}(D_b h_{\restriction \mathbb{F}^{n-1}})$ from which we deduce that $\mathrm{w}(D_b h_{\restriction \mathbb{F}^{n-1}}) = 2^{n-2}$, that is, $D_b h_{\restriction \mathbb{F}^{n-1}}$ is balanced, for all $b \in \mathbb{F}^{n-1} \setminus \{0\}$. This implies that h, with restriction to $\mathbb{F}^{n-1}$, is bent (see Theorem 54).

But $n-1$ is odd as n is even, so this implies that we have a bent function on $\mathbb{F}$-vector space of odd dimension, which is impossible. Thus, the assumption that $|\Gamma(\tilde{f})| = 2^n - 2$ is false, and so we can say $|\Gamma(\tilde{f})| \leq 2^n - 3$.

Suppose that $d \in \mathbb{F}^n \setminus \{0, e_1\}$ is the other nonzero element such that $D_d \tilde{f}$ is unbalanced. So $D_{d+e_1}\tilde{f}(x) = D_{e_1}\tilde{f}(x) + D_d f(x+e_1) = c + D_d f(x+e_1) = (c + D_{I \cdot d} f(x)) \circ \varphi$, for $c \in \mathbb{F}$ and $\varphi(y) = Iy + e_1$, with I as an identity in $GL_n(\mathbb{F})$. That is, $D_{d+e_1}\tilde{f}(x) \sim_A D_d f(x) + c$. Since $D_d f(x)$ is unbalanced then $D_d f(x) + c$ must be unbalanced, implying that $D_{d+e_1}\tilde{f}(x)$ is also unbalanced. That is, we have $\{0, e_1, d, d+e_1\} \not\subset \Gamma(\tilde{f})$. Hence $|\Gamma(\tilde{f})| \leq 2^n - 4$. □

Theorem 162. *Let a function F from $\mathbb{F}^n$ to itself, with n even, be an APN. Then there is a $\lambda \neq 0 \in \mathbb{F}^n$ such that the linear space of F_λ is trivial.*

Proof. Since, by Lemma 160, a Boolean function has a non-zero linear structure if and only if its splitting index is 1, so we simply show that for any APN function F it is impossible to have $\sigma(F_\lambda) = 1$, for all $\lambda \neq 0 \in \mathbb{F}^n$.

Suppose, by contradiction, that F is APN and $\sigma(F_\lambda) = 1$, for all $\lambda \neq 0 \in \mathbb{F}^n$. By Lemma 161, we can suppose that, for any $\lambda \neq 0 \in \mathbb{F}^n$, there are non-zero v, u and w not $\Gamma(F_\lambda)$ such that $D_v F_\lambda$ is constant, $D_u F_\lambda$ and $D_w F_\lambda$ are both unbalanced. So we have $\mathcal{F}^2(D_0 F_\lambda) = \mathcal{F}^2(D_v F_\lambda) = 2^{2n}$, and both $\mathcal{F}^2(D_u F_\lambda)$ and $\mathcal{F}^2(D_w F_\lambda)$ are non-zero positive integers (recall that, for any Boolean function f, $\mathcal{F}(f) = 0$ if and only if f is balanced). Thus, we have

$$\begin{aligned}\sum_{a \in \mathbb{F}^n} \mathcal{F}^2(D_a F_\lambda) &\geq \mathcal{F}^2(D_0 F_\lambda) + \mathcal{F}^2(D_v F_\lambda) + \mathcal{F}^2(D_u F_\lambda) + \mathcal{F}^2(D_w F_\lambda) \\ &= 2^{2n} + 2^{2n} + \mathcal{F}^2(D_u F_\lambda) + \mathcal{F}^2(D_w F_\lambda) > 2^{2n+1}\end{aligned}$$

from which we deduce that

$$\sum_{\lambda \neq 0 \in \mathbb{F}^n} \sum_{a \in \mathbb{F}^n} \mathcal{F}^2(D_a F_\lambda) > 2^{2n+1}(2^n - 1).$$

Thus, by Theorem 93, it is impossible for F to be an APN function. So it follows that if F is an APN function in even dimension then there is a component whose linear space is trivial. $\square$

Theorem 163. *Let F be an APN permutation over $\mathbb{F}^n$, with n even. Then $\dim V(F_\lambda) \leq 1$, for all $\lambda \neq 0 \in \mathbb{F}^n$.*

Proof. Suppose, by contradiction, that there is $\mu \neq 0 \in \mathbb{F}^n$ such that $\dim V(F_\mu) > 1$. It follows that $V(F_\mu)$ contains at least three nonzero elements. Let $a, b \in V(F_\mu)$ be nonzero and distinct. Then, by Proposition 97, we have $D_aF_\lambda = D_bF_\lambda = 1$. Clearly, $a+b$ is also a nonzero element in $V(F_\mu)$ different from a and b. Note that $D_{a+b}F_\mu(x) = D_aF_\mu(x) + D_bF_\mu(x+a)$, $x \in \mathbb{F}^n$. By Equation (2.11) in the proof of Lemma 121, $D_bF_\mu(x+a) = (D_{I\cdot b}F_\mu)\circ\varphi \sim_A D_bF_\mu$, with $\varphi(x) = I\cdot x + a$ and I being the identity matrix of $GL_n(\mathbb{F})$. Since $D_bF_\mu = 1$, so we must have $D_bF_\mu(x+a) = 1$. Thus, $D_{a+b}F_\mu(x) = 0$, which is impossible by Proposition 97. Thus, we must have $\dim V(F_\lambda) \leq 1$, for all $\lambda \neq 0 \in \mathbb{F}^n$. $\square$

4.2 Quadratic APN functions

A quadratic vectorial Boolean function from $\mathbb{F}^n$ to itself is denoted by Q, the linear space $V(Q_\lambda)$ of a component Q_λ is denoted by V_λ and we let $V_\lambda^* = V_\lambda \setminus \{0\}$. Since an APN function cannot contain linear components, we assume that Q is pure quadratic. Recall that all quadratic functions are partially-bent, so by Theorem 162 quadratic APN functions must have bent components since they are the only quadratics with trivial linear space. In this section, we are mainly counting how many these bent components are in quadratic APN functions.

First, we characterize quadratic APN functions based on the dimensions of linear spaces for their components.

Proposition 164. *For any quadratic $Q : \mathbb{F}^n \to \mathbb{F}^n$, we have*

$$\sum_{\lambda\neq 0\in\mathbb{F}^n} (2^{\dim V_\lambda} - 1) \geq 2^n - 1. \tag{4.1}$$

Moreover, equality holds if and only if Q is APN.

Proof. Since $\mathcal{F}^2(D_0Q_\lambda) = 2^{2n}$, so we have

$$\sum_{\lambda\neq 0\in\mathbb{F}^n}\sum_{a\in\mathbb{F}^n}\mathcal{F}^2(D_aQ_\lambda) = 2^{2n}(2^n-1) + \sum_{\lambda\neq 0,\in\mathbb{F}^n}\sum_{a\neq 0\in\mathbb{F}^n}\mathcal{F}^2(D_aQ_\lambda). \tag{4.2}$$

By Theorem 93 and Equation (4.2), we deduce that

$$\sum_{\lambda\neq 0,\in\mathbb{F}^n}\sum_{a\neq 0\in\mathbb{F}^n}\mathcal{F}^2(D_aQ_\lambda) \geq 2^{2n}(2^n-1) \tag{4.3}$$

and equality holds if and only if Q is APN.

For any quadratic Q, $\deg(D_aQ_\lambda) = 0$ if $a \in V_\lambda$ and $\deg(D_aQ_\lambda) = 1$ if $a \notin V_\lambda$. So we have $\mathcal{F}^2(D_aQ_\lambda) = 2^{2n}$ if $a \in V_\lambda$ and $\mathcal{F}^2(D_aQ_\lambda) = 0$ if $a \notin V_\lambda$. Thus, we have

$$\begin{aligned}\sum_{\lambda\neq 0\in\mathbb{F}^n}\sum_{a\neq 0\in\mathbb{F}^n}\mathcal{F}^2(D_aQ_\lambda) &= \sum_{\lambda\neq 0\in\mathbb{F}^n}\sum_{a\in V_\lambda^*}\mathcal{F}^2(D_aQ_\lambda)\\ &= \sum_{\lambda\neq 0\in\mathbb{F}^n} 2^{2n}|V_\lambda^*|\\ &= 2^{2n}\sum_{\lambda\neq 0\in\mathbb{F}^n}(2^{\dim V_\lambda}-1). \end{aligned}\tag{4.4}$$

We deduce, from the relation (4.3) and Equation (4.4), that

$$\sum_{\lambda\neq 0\in\mathbb{F}^n}(2^{\dim V_\lambda}-1) \geq 2^n - 1$$

and equality holds if and only if Q is APN. □

For any quadratic Boolean function f in odd dimension we have $\dim V(f) \geq 1$ and equality holds if and only if f is a semi-bent (see Lemma 149). This implies that the equality in the relation (4.1) happens if and only if Q is an AB function. So it implies that a quadratic function is APN if and only if it is AB (this is a well-known result). It follows that all components of any quadratic APN function in odd dimension have non-trivial linear space, implying that the result in Theorem 162 cannot be extended to quadratic APN functions in odd dimension.

Now we focus on quadratic functions from $\mathbb{F}^n$ to $\mathbb{F}^n$ in even dimensions. It is clear, from Theorem 7, that any quadratic Boolean function in even dimension has a splitting index 1 or 2. By Corollary 69, we deduce that a quadratic Boolean function is bent if and only if the splitting index is 2.

Definition 165. *For any quadratic Q, define*

$$\Delta_i = \{\lambda \in \mathbb{F}^n \mid \lambda \neq 0, \sigma(Q_\lambda) = i\}, \quad N = |\Delta_1| \quad \textit{and} \quad B = |\Delta_2|.$$

Remark 166. *From Definition 165, N is the number of non-bent compoments and B is the number of bent components in Q and so we have $N + B = 2^n - 1$.*

As proved by Nyberg in [42], bent functions exist only from $\mathbb{F}^n$ to $\mathbb{F}^m$, with $m \leq n/2$, so it follows that no function from $\mathbb{F}^n$ to itself can be bent. However, we can talk about bent components in functions from $\mathbb{F}^n$ to itself. Recall, from Remark 86, that the number of bent components in any function from $\mathbb{F}^n$ to itself is at most $2^n - 2^{\frac{n}{2}}$ [45]. It was shown in [39] that no plateaued APN function can contain the maximum possible number of bent components. Since the quadratic functions are plateaued, no quadratic APN function contains $2^n - 2^{\frac{n}{2}}$ bent components.

In the next result, we determine B when Q is an APN function and contains only bent and semi-bent components.

Proposition 167. *Let $Q : \mathbb{F}^n \to \mathbb{F}^n$, with n even, be such that Q_λ, with $\lambda \neq 0$, is bent or semi-bent. Then Q is APN if and only if there are exactly $\frac{2}{3}(2^n - 1)$ bent components.*

Proof. For any quadratic APN function Q, by Theorem 162, we have $B > 0$, that is, some components of Q must be bent (as we require that the linear space of some components must be trivial). Since n is even, then $\dim V_\lambda$ is even (see Remark 63). From Theorem 7 and Corollary 69, we can deduce that $\dim V_\lambda = 0$ if and only if Q_λ is bent. That is, $\dim V_\lambda \neq 0$ if $\lambda \in \Delta_1$ and $\dim V_\lambda = 0$ if $\lambda \in \Delta_2$. For any quadratic APN function Q, by Proposition 164, we must have

$$\sum_{\lambda\neq 0\in\mathbb{F}^n}(2^{\dim V_\lambda}-1)=2^n-1. \tag{4.5}$$

Since $\dim V_\lambda = 0$ if $\lambda\in\Delta_2$, then Equation (4.5) can be reduced to

$$\sum_{\lambda\in\Delta_1}(2^{\dim V_\lambda}-1)=2^n-1. \tag{4.6}$$

That is, Q is APN if and only if Equation (4.6) holds.

If Q is such that Q_λ, with $\lambda\neq 0$, is bent or semi-bent, then N is the number of semi-bent components (i.e., $\dim V_\lambda = 2$, for any $\lambda\in\Delta_1$). Thus, Equation (4.6) holds if and only if $(2^2-1)|\Delta_1| = 3N = 2^n-1$ if and only if $N=(2^n-1)/3$. Since $N+B=2^n-1$, so $B=2(2^n-1)/3$. □

It follows from Proposition 167 that any quadratic APN function in even dimension with the set $\{0,\pm 2^{\frac{n}{2}},\pm 2^{\frac{n+2}{2}}\}$ as its Walsh spectrum has $2(2^n-1)/3$ bent components. It is well-known that Gold APN functions (all functions of the form x^{2^k+1} with $\gcd(k,n)=1$) in even dimension have such Walsh spectrum, so they have $2(2^n-1)/3$ bent components.

Theorem 168. *Let a quadratic $Q:\mathbb{F}^n\to\mathbb{F}^n$, with n even, be APN. Then*

$$2(2^n-1)/3\leq B\leq 2^n-2^{n/2}-2,$$

where $B=2(2^n-1)/3+4t$, for some integer $t\geq 0$.

Proof. Suppose that Q is APN. Since the dimension of the linear space of any quadratic in even dimension is even (see Remark 63), so it follows that for any Q_λ, with $\lambda\in\Delta_1$, we have $\dim V_\lambda\geq 2$. If, for any $\lambda\in\Delta_1$, Q_λ is semi-bent then we are in Proposition 167, that is, $B=2(2^n-1)/3$. If some components are neither bent nor semi-bent, then we must have $B>2(2^n-1)/3$ for Equation (4.6) to be satisfied.

If Q has a component Q_μ, with $\mu \in \Delta_1$, which is not semi-bent, then $\dim V_\mu = 2k$, for some $k \geq 2$. So, for Equation (4.6) to be satisfied, the presence of Q_μ in Q implies that the number of bent components must be increased by

$$\frac{2^{2k}-1}{2^2-1} - 1 = \frac{2^{2k}-4}{3} = 4\left(\frac{2^{2k-2}-1}{3}\right)$$

which clearly is divisible by 4. This implies that the number of bent components in Q is $B = 2(2^n-1)/3 + 4t$, for some integer $t \geq 0$.

By Remark 86, we have $B \leq 2^n - 2^{n/2}$. Now we show that it is not possible to have $B = 2^n - 2^{n/2}$. For some $t \geq 0$, we have $B = 2(2^n-1)/3 + 4t = 2[(2^n-1)/3 + 2t] \not\equiv 0 \pmod 4$ since $(2^n-1)/3+2t$ is odd. Thus, $B \neq 2^n - 2^{n/2}$ since $2^n - 2^{n/2} \equiv 0 \pmod 4$. Hence we must have $B \leq 2^n - 2^{n/2} - 2$. □

For any quadratic APN function Q in dimension 4, by Theorem 168, we only have one possibility, that is, $B = 10$ (this satisfies Proposition 167). We state this result in the following.

Corollary 169. *A pure quadratic $Q : \mathbb{F}^4 \to \mathbb{F}^4$ is APN if and only if $B = 10$.*

Not long time ago, only quadratic APN functions with $B = 2(2^n-1)/3$ were known. We have shown in Proposition 167 that such functions contain only bent and semi-bent components. As noted earlier, Gold functions are example of such functions. It had been conjectured that all quadratic APN functions are equivalent to Gold functions (i.e., all quadratic APN functions have the same number of bent components) until Dillon in 2006 gave an example of quadratic APN function with different number of bent components and inequivalent to Gold APN functions. The Dillon's Example:

$$F(x) = x^3 + z^{11}x^5 + z^{13}x^9 + x^{17} + z^{11}x^{33} + x^{48}$$

is defined over $\mathbb{F}_{2^6}$, with z primitive. Using MAGMA, we found that F has 46 bent components. That is, it is an example of quadratic APN function with $B = 2(2^n-1)/3 + 4$ (i.e., $t = 1$ in Theorem 168). Also by computer search, we found the function:

$$G(x) = x^3 + z^{53}x^{10} + z^{41}x^{18} + z^{59}x^{33} + z^{43}x^{34} + z^{31}x^{48}$$

over $\mathbb{F}_{2^6}$, with z primitive, which has the same number of bent components as F, the Dillon's Example. From Theorem 168, we deduce that, in dimension 6, all the possibilities for the number of bent components in any quadratic APN function are: 42, 46, 50 and 54. So far we only know the existence of quadratic APN functions with 42 (Gold functions and others) and 46 (Dillon's example) bent components but we are uncertain whether those with 50 and 54 exist.

In [50], Yu and others constructed some quadratic APN functions in dimension 8 which have the Walsh spectrum: $\{-64, -32, -16, 0, 16, 32, 64\}$ (different from the Walsh spectrum of Gold functions). These functions are further classified in terms of the distribution of their Walsh coefficients and two classes are found. One class has 487 functions and the other one has 12 functions. In the class of 487 functions, we considered the function:

$$\begin{aligned} G'(x) = {} & z^{249}x^{192} + z^{24}x^{160} + z^{210}x^{144} + z^{69}x^{136} + z^{46}x^{132} + z^{164}x^{130} + z^{43}x^{129} \\ & + z^{31}x^{96} + z^{30}x^{80} + z^{115}x^{72} + z^{228}x^{68} + z^{16}x^{66} + z^{228}x^{65} + z^{217}x^{48} + z^{9}x^{40} \\ & + z^{251}x^{36} + z^{151}x^{34} + z^{77}x^{33} + z^{189}x^{24} + z^{109}x^{20} + z^{191}x^{18} + z^{249}x^{17} + z^{175}x^{12} \\ & + z^{130}x^{10} + z^{91}x^{9} + z^{59}x^{6} + z^{60}x^{5} + z^{121}x^{3}, \end{aligned}$$

where z is primitive and by checking with MAGMA, we found that it contains $2(2^8-1)/3+4 = 174$ bent components (i.e., $t = 1$ in Theorem 168) and in the other class, we considered the function:

$$\begin{aligned} G''(x) = {} & z^{130}x^{192} + z^{160}x^{160} + z^{117}x^{144} + z^{230}x^{136} + z^{228}x^{132} + z^{162}x^{130} + z^{25}x^{129} \\ & + z^{79}x^{96} + z^{204}x^{80} + z^{83}x^{72} + z^{159}x^{68} + z^{234}x^{66} + z^{36}x^{65} + z^{67}x^{48} + z^{151}x^{40} \\ & + z^{17}x^{36} + z^{81}x^{34} + z^{52}x^{33} + z^{9}x^{24} + z^{116}x^{20} + z^{102}x^{18} + z^{97}x^{17} + z^{74}x^{12} \\ & + z^{48}x^{10} + z^{144}x^{9} + z^{58}x^{6} + z^{146}x^{5} + z^{123}x^{3} \end{aligned}$$

which was found to have $2(2^8-1)/3+8 = 178$ bent components (i.e., $t = 2$ in Theorem 168). Thus, in dimension 8, we only know the existence of quadratic APN functions with 170, 174 and 178 bent components and it is yet to be known whether a quadratic APN functions with $B = 2(2^8-1)/3+4t$, with $3 \leq t \leq 17$, exists.

Proposition 170. *Let a quadratic function $Q : \mathbb{F}^n \to \mathbb{F}^n$ be APN with $B = 2(2^n - 1)/3 + 4t$, for some integer $t \geq 0$, as described in Theorem 168. Then*

$$\mathcal{N}(Q) = \begin{cases} 2^{n-1} - 2^{n/2} & \text{if } t = 0, n \geq 4 \\ 2^{n-1} - 2^{n/2+1} & \text{if } 1 \leq t \leq 4, n \geq 6 \end{cases}$$

Proof. We first need to recall, from Remark 63, that for any quadratic Boolean function on n variables, with even n, the dimension k of its linear space is even and the Walsh spectrum is $\{0, 2^{(n+k)/2}\}$.

If $t = 0$ then, by Proposition 167, all components of Q are bent and semi-bent, that is, the Walsh spectrum of Q is $\{0, \pm 2^{(n+2)/2}, \pm 2^{n/2}\}$. So it is clear that we have $\mathcal{N}(Q) = 2^{n-1} - 2^{n/2}$.

To prove that $\mathcal{N}(Q) = 2^{n-1} - 2^{n/2+1}$ if $1 \leq t \leq 4$, we need to show that for this range of t we have $\dim V_\lambda \in \{0, 2, 4\}$, for all $\lambda \neq 0 \in \mathbb{F}^n$, that is, that the Walsh spectrum of Q is $\{0, \pm 2^{(n+4)/2}, \pm 2^{(n+2)/2}, \pm 2^{n/2}\}$.

It is clear from Theorem 168 that for $t \geq 1$, we have $B > 2(2^n - 1)/3$, and so Proposition 167 allows us to conclude that there must be $\lambda \neq 0 \in \mathbb{F}^n$ such that $\dim V_\lambda > 2$. We claim that if $1 \leq t \leq 4$, then we have $\dim V_\lambda \in \{0, 2, 4\}$, for $\lambda \neq 0 \in \mathbb{F}^n$. Suppose, by contradiction, that there is $\mu \neq 0 \in \mathbb{F}^n$ such that $\dim V_\mu = 6$. Then, as noted in the proof of Theorem 168, the presence of Q_μ implies that the number of bent components is increased by

$$4\left(\frac{2^{6-2} - 1}{3}\right) = 4(5),$$

implying that $B \geq 2(2^n - 1)/3 + 4(5)$. So it follows that if, for some $\lambda \neq 0 \in \mathbb{F}^n$, $\dim V_\lambda = 6$, then we have $t \geq 5$. This implies that, if $1 \leq t \leq 4$, then we must have $\dim V_\lambda \in \{0, 2, 4\}$, for all $\lambda \neq 0 \in \mathbb{F}^n$. So in this case the Walsh spectrum of Q is $\{0, \pm 2^{(n+4)/2}, \pm 2^{(n+2)/2}, \pm 2^{n/2}\}$, implying that $\mathcal{N}(Q) = 2^{n-1} - 2^{n/2+1}$. □

From Proposition 170, it seems like the nonlinearity of any quadratic APN function decreases as the number of bent components increases and it is the highest when the number of bent components is the lowest possible.

4.3 Quadratic power functions

Pott et al. in [45] say that the question to determine all monomial bent functions $Tr(\alpha x^d)$ on $\mathbb{F}_{2^n}$, with $\alpha \in \mathbb{F}_{2^n}^*$ and n even, has attracted quite a lot of research interest. In this section, we study the Walsh spectrum and enumerate bent components for any quadratic power functions. Recall that a function $F = x^d$ is a quadratic power function if $d = 2^j + 2^i$, with $j > i \geq 0$. It is known that a function with the power $d = 2^i(2^{j-i} + 1)$ is affine equivalent to the one with power $d' = 2^{j-i} + 1$ [29, 30]. So we simply consider the power $2^k + 1$, for some positive integer k.

Theorem 171. *Let $F(x) = x^{2^k+1}$ be a function in $\mathbb{F}_{2^n}[x]$, with n even and some integer $k \geq 1$. Let $m = (n, k)$, $s = (n, 2k)$ and $e = 1$ if n/m is odd and $e = 2^m + 1$ if n/m is even. Then*

(a) F is an e-to-1 function on $\mathbb{F}_{2^n}^*$,

(b) F_α is bent if and only if $\alpha \notin \mathrm{Im}(F)$.

(c) the number of bent components for F is $\frac{(e-1)(2^n-1)}{e}$,

(d) the Walsh spectrum of F is $\{0, \pm 2^{(n+s)/2}\}$ if $e = 1$, and $\{0, \pm 2^{(n+s)/2}, \pm 2^{n/2}\}$ if $e = 2^m + 1$,

(e) $\mathcal{N}(F) = 2^{n-1} - 2^{(n+s)/2-1}$.

Proof. Let $S = \mathrm{Im}(F) \setminus \{0\} = \{\xi^{2^k+1} \mid \xi \in \mathbb{F}_{2^n}^*\}$. It can be easily shown that S is a multiplicative subgroup of $\mathbb{F}_{2^n}^*$.

(a) Clearly, F maps $\mathbb{F}_{2^n}^*$ onto S. So we only need to show that S has the order $(2^n-1)/e$. Now we need to find the order of S. First observe that every element ζ in S satisfies $\zeta^{(2^n-1)/e} = 1$, where $e = (2^n - 1, 2^k + 1)$. By Lemma 94, $e = 1$ if n/m is odd and $e = 2^m + 1$ if n/m is even. If ν is a primitive element in $\mathbb{F}_{2^n}$, then the order of ν^{2^k+1} is $\mathrm{ord}(\nu^{2^k+1}) = \mathrm{ord}(\nu^e) = (2^n - 1)/e$. Clearly, ν^{2^k+1} has the highest order in S. It is well-known that $\mathbb{F}_{2^n}^*$ is a cyclic group, so S being its subgroup must be cyclic with ν^{2^k+1} as a generator. Thus, it follows that the order of S is $(2^n-1)/e$, implying that F is an e-to-1 function on $\mathbb{F}_{2^n}^*$.

(b) It is equivalent to show that F_α is non-bent if and only if $\alpha \in \mathrm{Im}(F)$. F_α is bent if its linear space is trivial, so we need to prove that the dimension of the linear space of F_α is non-trivial, that is, $\dim V_\alpha \geq 1$ if and only if $\alpha \in \mathrm{Im}(F)$.

A component F_α, with $\alpha \in \mathbb{F}_{2^n}$, is non-bent if there exists β in $\mathbb{F}_{2^n}^*$ such that $D_\beta F_\alpha$ is constant. Suppose that F_α, with $\alpha \in \mathbb{F}_{2^n}^*$, is non-bent and $D_\beta F_\alpha$ is constant, where $\beta \in \mathbb{F}_{2^n}$. So we have

$$\begin{aligned}
D_\beta F_\alpha(x) = F_\alpha(x) + F_\alpha(x+\beta) &= Tr\left(\alpha x^{2^k+1}\right) + Tr\left(\alpha(x+\beta)^{2^k+1}\right) \\
&= Tr\left(\alpha x^{2^k+1}\right) + Tr\left(\alpha(x^{2^k} + \beta^{2^k})(x+\beta)\right) \\
&= Tr\left(\alpha x^{2^k+1}\right) + Tr\left(\alpha(x^{2^k+1} + \beta x^{2^k} + \beta^{2^k} x + \beta^{2^k+1})\right) \\
&= Tr\left(\alpha\beta x^{2^k}\right) + Tr\left(\alpha\beta^{2^k} x\right) + Tr\left(\alpha\beta^{2^k+1}\right) \\
&= Tr\left((\alpha\beta + \alpha^{2^k}\beta^{2^{2k}})x^{2^k}\right) + Tr\left(\alpha\beta^{2^k+1}\right). \qquad (4.7)
\end{aligned}$$

Observe that $D_\beta F_\alpha$ is constant if and only if, in Equation (4.7), we have

$$Tr\left((\alpha\beta + \alpha^{2^k}\beta^{2^{2k}})x^{2^k}\right) = 0.$$

This happens if and only if

$$\alpha\beta + \alpha^{2^k}\beta^{2^{2k}} = \alpha\beta\left(1 + \alpha^{2^k-1}\beta^{2^{2k}-1}\right) = 0.$$

So either $\beta = 0$ or

$$\alpha^{2^k-1}\beta^{2^{2k}-1} = (\alpha\beta^\ell)^{2^k-1} = 1, \qquad (4.8)$$

with $\ell = \frac{2^{2k}-1}{2^k-1} = 2^k+1$. Suppose that ζ is a primitive element in $\mathbb{F}_{2^n}$. Then we can write $\alpha = \zeta^r$ and $\beta = \zeta^t$, for some integers r and t. So it follows that Equation (4.8) becomes $\zeta^{(r+t\ell)(2^k-1)} = 1$ which implies that

$$(r+t\ell)(2^k-1) = r(2^k-1) + t(2^{2k}-1) = c(2^n-1),$$

for some integer c. Thus, we have

$$r = \frac{c(2^n-1)}{2^k-1} - \frac{t(2^{2k}-1)}{2^k-1} = \frac{c(2^n-1)}{2^k-1} - t(2^k+1) = e\left(\frac{c(2^n-1)}{e(2^k-1)} - \frac{t(2^k+1)}{e}\right).$$

Recall that $e = (2^n-1, 2^k+1)$. So all α's which satisfy $(\alpha\beta^\ell)^{2^k-1} = 1$ must be those which satisfy $\alpha^{(2^n-1)/e} = 1$. These are elements whose orders are divisors of $(2^n-1)/e$. It implies that $\alpha \in S$. Including $\alpha = 0$, it follows that F_α has a non-trivial linear space if and only if $\alpha \in \mathrm{Im}(F)$.

(c) By part (b), we deduce that the number of bent components is $2^n - |\mathrm{Im}(F)|$. Since $|\mathrm{Im}(F)| = 1 + |S| = 1 + (2^n-1)/e$, then the number of bent components is
$$2^n - |\mathrm{Im}(F)| = \frac{(e-1)(2^n-1)}{e}.$$

(d) We first determine V_α, for any $\alpha \in \mathbb{F}_{2^n}^*$, and then use Theorem 48 to deduce the Walsh spectrum of F. In part (b), we showed that $V_\alpha = \{0\}$ if $\alpha \notin \mathrm{Im}(F)$ (i.e., F_α is bent) and $|V_\alpha| > 1$ if $\alpha \in \mathrm{Im}(F)$. For any $\alpha \in S = \mathrm{Im}(F) \setminus \{0\}$, we also showed, in part (b), that $D_\beta F_\alpha$ is constant if either β is equal to 0 or satisfies $(\alpha\beta^{2^k+1})^{2^k-1} = 1$. Thus, we have $\beta^{2^{2k}-1} = (\alpha^{-1})^{2^k-1}$. If $\alpha \in \mathbb{F}_{2^m}^*$, with $m = (n,k)$, then we have $\beta^{2^{2k}-1} = 1$ and so $\beta \in \mathbb{F}_{2^s}^*$, with $s = (n, 2k)$, otherwise we have $\beta \in \mu\mathbb{F}_{2^s}^*$, where μ is ℓ-th root of α^{-1}. So it follows that $|V_\alpha| = 2^s$.

By Lemma 94, we have $e = 1$ if n/m is odd and $e = 2^m+1$ if n/m is even. If $e = 1$ then, by part (a), F is a permutation which implies that it has no bent components and so we have $|V_\alpha| = 2^s$, for all $\alpha \in \mathbb{F}_{2^n}^*$. This implies that the Walsh spectrum of F is $\{0, \pm 2^{(n+s)/2}\}$ (see Theorem 48). If $e = 2^m+1$, then

F contains bent components and as shown above, all the linear spaces of non-bent components have the same order 2^s, implying that the Walsh spectrum of F is $\{0, \pm 2^{(n+s)/2}, \pm 2^{n/2}\}$.

(e) This directly follows from definition of nonlinearity and part (d). □

Corollary 172. *Let $F(x) = x^{2^k+1}$ be a power function in $\mathbb{F}_{2^n}[x]$, with positive integer $k \geq 1$ and let $e = (2^n - 1, 2^k + 1)$ and $s = (n, 2k)$. Then F is APN if and only if $e = 3$ and $s = 2$. Equivalently, F is APN if and only if there are exactly $2(2^n - 1)/3$ bent components and the rest are semi-bent.*

Proof. By Theorem 171, there are $(2^n - 1)/e$ (non-trivial) non-bent components for F and their linear spaces have the same order 2^s. Since n is even then $s = 2t$, where $t = (k, n/2)$. Thus, by Proposition 164, F is APN if and only if

$$\left(\frac{2^n - 1}{e}\right)(2^s - 1) = 2^n - 1. \tag{4.9}$$

Notice that Equation (4.9) holds if and only if $e = 2^s - 1$, so we conclude that $(2^s - 1)|(2^k + 1)$ since $e \mid (2^k + 1)$. Since $t|s$ then $(2^t - 1)|(2^s - 1)$, implying that $(2^t - 1)|(2^k + 1)$. But also $(2^t - 1)|(2^k - 1)$ (recall that $t|k$), so it implies that we must have $t = 1$ as clearly $2^k - 1$ and $2^k + 1$ are relatively prime. Observe that $t = 1$ implies $s = 2$, so it follows that F is APN if and only if $s = 2$ and $e = 2^s - 1 = 3$. In other words, F is APN if and only if the number of bent components is exactly $2(2^n - 1)/3$ and the other components are semi-bent (see Theorem 171). □

From Theorem 171, we observe that a quadratic power function has some bent components if $e \geq 3$ and equality gives the lowest number of bent components we can get and also equality happens when F is APN. So we state this in the following.

Corollary 173. *If a quadratic power function, in even dimension, has some bent components, then they are at least $2(2^n - 1)/3$.*

Conclusion and future work

In this thesis, we studied some cryptographic properties of Boolean functions which include weight, balancedness, nonlinearity and resiliency. We constructed balanced functions with trivial linear space and some resilient functions with respect to monotone sets.

Based on the behaviour of second order derivatives, we derived some quantities used for characterization of quadratic and cubic APN functions. We showed that these quantities can also be used to characterize quadratic and cubic bent functions.

Some properties of APN functions with respect to linear spaces of their components, in even dimension, were studied. We showed that there must be at least a component whose linear space is trivial. In particular, we determined the possible size of the linear space of any component of an APN permutation. We established a simple characterization of quadratic APN functions based on the dimensions of linear spaces for their components. A general form for the number of bent components in any quadratic APN functions was proved. We completely enumerated bent components in any quadratic power functions.

Next, we present some problems which emanated from our work. We would like to investigate the following:

- Do quadratic APN functions with nonlinearity $> 2^{n-1} - 2^{n/2+1}$ exist?
- For $t \geq 3$, construct (or prove existence of) quadratic APN functions with $2(2^n - 1)/3 + 4t$ bent components. More specific, construct quadratic APN functions over $\mathbb{F}_{2^6}$ with 50 or 54 bent components.

- Find a tighter upper bound on the number of bent components in any quadratic APN function in dimension $n \geq 6$.
- Can Theorem 168 be extended to plateaued APN functions?

References

[1] Berger T.P., Canteaut A., Charpin P. and Laigle-Chapuy Y.: On almost perfect nonlinear functions over $\mathbb{F}_2^n$. *IEEE Trans. Inf. Theory* 52,9, (2006), 4160-4170.

[2] Beth T. and Ding C.: On almost perfect nonlinear permutations. *Advances in Cryptology* - EUROCRYPT '93 (1993), 65-76.

[3] Braeken A., Borissov Y., Nikova S. and Preneel B.: Classification of cubic $(n-4)$-resilient Boolean functions. *IEEE Transactions on Information Theory*, 52, 4, (2006), 1670-1676.

[4] Braeken A., Nikov V., Nikova S. and Preneel B.: On Boolean functions with generalized cryptographic properties. In: Preneel B. and Logachev O.A. (Eds) *Boolean Functions in Cryptology and Information Security.* IOS Press, Amsterdam, (2008), 73-96.

[5] Browning K.A., Dillon J.F., McQuistan M.T. and Wolfe A.J.: An APN permutation in dimension six. *Finite Fields: theory and applications*, 518 (2010), 33-42.

[6] Budaghyan L., Helleseth T., Li N. and Sun B.: Some Results on the Known Classes of Quadratic APN Functions. In: El Hajji S., Nitaj A., Souidi E. (eds) Codes, *Cryptology and Information Security, C2SI 2017.* Lecture Notes in Computer Science, Springer, Cham, vol 10194 (2017), 3-16.

[7] Calderini M., Sala M. and Villa I.: A note on APN permutations in even dimension. *Finite Fields and Their Applications*, 46 (2017), 1-6.

[8] Camion P., Carlet C., Charpin P. and Sendrier, N.: On Correlation-Immune functions. *Proc. of Crypto 1991*, LNCS 576 (1992), Springer-Verlag, pp 86-100.

[9] Canteaut A.: Cryptographic Functions and Design Criteria for Block Ciphers. In: Rangan C.P., Ding C. (eds) *Progress in Cryptology - INDOCRYPT 2001.* INDOCRYPT 2001. Lecture Notes in Computer Science, vol 2247, (2001), pp 1-16. Springer, Berlin, Heidelberg.

[10] Canteaut, A., Perrin, L.: On CCZ-equivalence, extended-affine equivalence, and function twisting, *Finite Fields and Their Applications,* 56, (2018), 209-246.

[11] Canteaut, A., Carlet, C., Charpin, P., Fontaine, C.: Propagation Characteristics and Correlation-Immunity of Highly Nonlinear Boolean Functions, Eurocrypt 2000, LNCS 1807, Springer-Verlag, pp. 507-522, 2000.

[12] Caranti A., Volta D. and Sala M.: On some block ciphers and imprimitive groups. *Appl.Algebra Eng. Commun. Comput.*, 20, 5-6, (2009), 229-350.

[13] Carlet C.: Vectorial Boolean Functions for Cryptography. *Boolean models and methods in mathematics, computer science and engineering*, Cambridge Univ. Press, 2,(2010), 398-470.

[14] Carlet C.: *Characterization of the differential uniformity of vectorial functions by the Walsh transform.* Available at: https://eprint.iacr.org/2017/516.pdf.

[15] Carlet C. and Mesnager S.: On Semi-bent Boolean Functions. *IEEE Transactions of Information Theory,* 58, 5, (2012) 3287-3292.

[16] Carlet C.: A transformation on boolean functions, its consequences on some problems related to Reed-Muller codes. In: *Adv. in crypt.*-Eurocrypt'90. LNCS, Berlin: Springer; 473, (1991), 42-50.

[17] Carlet C. and Codes P.: More correlation-immune and resilient functions over Galois fields and Galois ring. In *Advances in Cryptology-EUROCRYPT'98*, Volume 1233 of *Lecture Notes in Computer Science,* pp 422-433. Springer-Verlag, Berlin, Heidelberg, New York, 1997.

[18] Carlet C., Guillot P.: A New Representation of Boolean Functions. In: Fossorier M., Imai H., Lin S., Poli A. (eds) Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. AAECC 1999. Lecture Notes in Computer Science, vol 1719, (1999), pp 94-103. Springer, Berlin, Heidelberg.

[19] Carlet, C.: Boolean Functions for Cryptography and Error-Correcting Codes. In Y. Crama & P. Hammer (Eds.), *Boolean Models and Methods in Mathematics, Computer Science, and Engineering* (Encyclopedia of Mathematics and its Applications, (2010), pp. 257-397). Cambridge: Cambridge University Press. doi:10.1017/CBO9780511780448.011

[20] Carlet, C., Charpin, P., and Zinoviev, V.: Codes, bent functions and permutations suitable for DES-like cryptosystems. *Design Codes Cryptography*, 15(2):125-156, 1998.

[21] Çeşmelioğlu A., Meidl W. and Topuzoğlu A.: *Partially bent functions and their properties.* In: Applied Algebra and Number Theory, Cambridge University Press, United Kingdom (2014), 22-38.

[22] Chabaud, F. and Vaudenay, S.: Links between differential and linear cryptanalysis. In *Advances in Cryptology* - EUROCRYPT'94, pages 356–365, Springer,Berlin, 1995.

[23] Chakrabarty K. and Hayes J.P.: Balanced Boolean functions. *IEE Proc-Comput. Digit. Tech.*, 145, 1 (1998),52-62.

[24] Chee S., Lee S. and Kim K.: Semi-bent Functions: In: *Advances in Cryptology-ASIACRYPT94.* Proc. 4th Int. Conf. on the Theory and Applications of Cryptology, Wollongong, Australia. Pieprzyk, J. and Safavi-Naini, R., Eds., Lect. Notes Comp. Sci, 917, (1994), 107-118.

[25] Courtois N. and Meier W.: Algebraic attacks on stream ciphers with linear feedback. In Advances in Cryptology - EUROCRYPT 2003, number 2656 in Lecture Notes in Computer Science, pages 345–359. Springer Verlag, 2003.

[26] Cusick, T. W. and Cheon Y.: Counting balanced Boolean functions in n variables with bounded degree. *Exp. Math.*, 16, 1, (2007), 101-105.

[27] Cusick, T. W.: Affine equivalence of cubic homogeneous rotation symmetric functions. Inform Sci 181, (2011), 5067–83.

[28] Dobbertin, H.: Almost perfect nonlinear power functions on $GF(2^n)$: the Welch case. *IEEE Trans. Inf. Theory*, 45 (4) (1999), 1271-1275.

[29] Dobbertin, H.: Almost perfect nonlinear power functions on $GF(2^n)$: the Niho case. *Inf. Comput.*, 151 (1-2) (1999), 57-72.

[30] Dobbertin, H.: Almost perfect nonlinear power functions on $GF(2^n)$: a new case for n divisible by 5. In Jungnickel, D.Niederreiter, H. (Eds.): *Proceedings of the Conference on Finite Fields and Applications*. Augsburg, 1999, Springer-Verlag, Berlin (2001), pp. 113-121.

[31] Erickson, M., Vazzana, A.: Introduction to number theory. Chapman & Hall/CRC, 1st edition, 2007.

[32] Fehr, S., Maurer, U.: Linear VSS and Distributed Commitments Based on Secret Sharing and Pairwise Checks. *Crypto 2002*, LNCS 2442, Springer-Verlag, pp. 565-580, 2002.

[33] Gold, R.: Maximal recursive sequences with 3-valued recursive cross-correlation functions. *IEEE Trans. Inf. Theory*, 14 (1968), 377-385.

[34] Göloğlu, F.: Almost perfect nonlinear trinomials and hexanomials. *Finite Fields and Their Applications*, 33 (2015) 258-282.

[35] Kasami,T.: The weight enumerators for several classes of subcodes of the 2nd order binary Reed–Muller codes. *Inf. Control*, 18 (1971), 369-394

[36] Khoo, K., Gong, G.: New Construction for Balanced Boolean Functions with Very High Nonlinearity. *IEICE Trans. Fundamentals,* Vol.E90-A No.1 (2007), pp.29-35

[37] MacWilliams F.J. and Sloane N.J.A.: *The Theory of Error-Correcting Codes.* New York, Elsevier (1977).

[38] Maitra S.: Boolean Functions on Odd Number of Variables Having Nonlinearity Greater Than the Bent Concatenation Bound. In Preneel B. and Logachev O. (Eds): *Boolean Functions in Cryptology and Information Security.* IOS Press, Amsterdam, (2008), 173-182.

[39] Mesnager, S., Zhang, F., Tang, C., Zhou,Y.: Further study on the maximum number of bent components of vectorial functions. CoRR, abs/1801.06542, (2018).

[40] Mullen G.L. and Panario D.: *Handbook of Finite Fields: Discrete Mathematics and its Applications.* London CRC press, (2013).

[41] Nikov, V., Nikova, S.: On a Relation Between Verifiable Secret Sharing Schemes and a Class of Error-Correcting Schemes, Cryptology e-print archive, http://eprint.iacr.org/2003/210.

[42] Nyberg K.: S-boxes and round functions with controllable linearity and differential uniformity. In: *Fast Software Encryption-FSE'94* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, vol. 1008, (1995), pp. 111–130.

[43] Nyberg K.: Differentially uniform mappings for cryptography. In Helleseth, T. (Ed.): *Advances in Cryptology - EUROCRYPT'93*, LNCS 765. Springer-Verlag Berlin Heidelberg, (1994), pp. 55-64.

[44] Nyberg K.: Perfect non-linear S-boxes. *Proceedings of EUROCRYPT'91.* Lecture Notes in Computer Science 547, pp. 378-386, 1992.

[45] Pott, A., Pasalic, E., Muratović-Ribić, A., Bajrić S.: On the Maximum Number of Bent Components of Vectorial Functions. IEEE Transactions on Information Theory **64**(1), (2018), 403-411.

[46] Seberry J., Zhang XM., Zheng Y.: Nonlinearly Balanced Boolean Functions and Their Propagation Characteristics. In: Stinson D.R. (Eds) *Advances in Cryptology-CRYPTO 93. CRYPTO'1993.* Lecture Notes in Computer Science, 773, (1994). Springer, Berlin, Heidelberg.

[47] Siegenthaler T.: Correlation-Immunity of nonlinear combining functions for cryptography Applications. *IEEE Trans. Information Theory* (1984), 776-780.

[48] Tang D., Zhang W., Tang X.: Construction of balanced Boolean functions with high nonlinearity and good autocorrelation properties. *Designs, Codes and Cryptography*, 60, (2010), 77-91.

[49] Wu C.K. and Feng D.: Boolean Functions and Their Applications in Cryptography. *Advances in Computer Science and Technology*, New York, Springer, (2016) 78-83.

[50] Yu, Y., Wang, M., Li, Y.: A matrix approach for constructing quadratic APN functions. Des. Codes Crypt. 73(27), (2014), 587–600.

[51] Zaninelli, M.: On cryptographic properties of cubic Boolean functions. MSc. Dissertation, University of Trento, (2017).