UNIVERZA NA PRIMORSKEM
FAKULTETA ZA MATEMATIKO, NARAVOSLOVJE IN INFORMACIJSKE TEHNOLOGIJE

Master's thesis
(Magistrsko delo)

On certain properties of APN and AB functions

(O določenih lastnostih APN in AB funkcij)

Ime in priimek: Amar Bapić
Študijski program: Matematične znanosti 2. stopnja
Mentor: prof. dr. Enes Pasalic
Somentorja: asist. dr. Nastja Cepak , asist. dr. Samir Hodžić

Koper, julij 2019

Ključna dokumentacijska informacija

Ime in PRIIMEK: Amar BAPIĆ

Naslov zaključne naloge: O določenih lastnostih APN in AB funkcij

Kraj: Koper

Leto: 2019

Število listov: 49 Število slik: 1 Število tabel: 12

Število prilog: 1 Število strani prilog: 7 Število referenc: 56

UDK: 512.624.95(043.2)

Mentor: prof. dr. Enes Pasalic

Somentorja: asist. dr. Nastja Cepak , asist. dr. Samir Hodžić

Ključne besede: Boolova funkcija, APN funkcija, AB funkcija

Math. Subj. Class. (2010): 06E30, 12E20, 94A60

Izvleček:

Da zagotovimo odpornost bločnih šifer na razne kriptoanalitične metode morajo te vsebovati primerne Boolove funkcije, ki zadostijo določenim kriterijem. V tezi obravnavamo eno najpomembnejših lastnosti Boolovih funkcij, vezanih na algebraične objekte, znane kot skoraj popolnoma ne-linearne (almost perfectly non-linear - APN) in skoraj ukrivljene (almost bent - AB) funkcije. Ker so te funkcije velikega pomena pri zagotavljanju varnosti bločnih šifer, še posebej proti diferencialni kriptoanalizi, opišemo nekatere njihove glavne lastnosti (in v večini primerov prilagamo tudi dokaze) ter poznane razrede. Kot glavno temo teze predstavimo določena nova opažanja o APN in AB funkcijah, vezana na Walsh podporo in duale. Verjamemo, da se bodo ti rezultati v prihodnosti izkazali za uporabne pri nadaljnji obravnavi teh kompleksnih objektov.

Key words documentation

Name and SURNAME: Amar BAPIĆ

Title of final project paper: On certain properties of APN and AB functions

Place: Koper

Year: 2019

Number of pages: 49 Number of figures: 1 Number of tables: 12

Number of appendices: 1 Number of appendix pages: 7 Number of references: 56

UDK: 512.624.95(043.2)

Mentor: Prof. Enes Pasalic, PhD

Co-Mentors: Assist. Nastja Cepak, PhD, Assist. Samir Hodžić, PhD

Keywords: boolean function, APN function, AB function

Math. Subj. Class. (2010): 06E30, 12E20, 94A60

Abstract:

In order to resist various cryptanalytic methods block ciphers have to involve suitable Boolean functions which have to meet certain criteria. In the thesis we consider some of the most important properties of Boolean functions in connection to algebraic objects known as almost perfect non-linear (APN) and almost bent (AB) functions. Since these functions are of great importance in providing the security of block ciphers, especially against the differential cryptanalysis, we recall some of their main properties (along with proof for most of them) and known classes. As a main objective of this thesis, we provide some new observations on APN and AB functions in terms of their Walsh supports and duals. We believe that these results will be useful in further analysis of these complex objects.

Contents

List of Tables

List of Figures

Appendices

Notations

p	a prime number (in most cases $p = 2$)
n	an odd number (usually odd)
$\mathbb{F}_p$	the prime field, $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$
$\mathbb{F}_{p^n}$	the finite field with p^n elements
$\mathbb{F}_{p^n}^*$	the set of all non-zero elements of the field finite field $\mathbb{F}_{p^n}$
$\mathbb{F}_p^n$	the n dimensional vector space over $\mathbb{F}_p$
$\oplus$	the sum over $\mathbb{F}_2$ (XOR operation)
$\mathbf{x} = (x_0, \ldots, x_{n-1})$	a binary vector over $\mathbb{F}_2$ of length n
$\mathbf{x} \oplus \mathbf{y}$	the sum of two binary vectors over $\mathbb{F}_2$
	$\mathbf{x} \oplus \mathbf{y} = (x_0 \oplus y_0, \ldots, x_{n-1} \oplus y_{n-1})$
$\mathbf{x} \cdot \mathbf{y}$	the standard *dot product* of vectors, where
	$\mathbf{x} \cdot \mathbf{y} = x_0 y_0 \oplus \ldots \oplus x_{n-1} y_{n-1}$
$\mathbf{x} \preceq \mathbf{y}$	the *precedence relation*: $\mathbf{x} \preceq \mathbf{y}$ if and only if for all $i = 0, \ldots, n-1$
	$x_i \leq y_i$ holds (i.e., x is *covered* by y)
$d(\mathbf{x}, \mathbf{y})$	the *Hamming distance* between vectors $\mathbf{x}$ and $\mathbf{y}$
$\mathrm{wt}(\mathbf{x})$	the *Hamming weight* of a vector $\mathbf{x}$
$f : \mathbb{F}_2^n \to \mathbb{F}_2$	a *Boolean function* in n variables
$F : \mathbb{F}_2^n \to \mathbb{F}_2^m$	a *vectorial Boolean function* in n variables
$\deg(f)$	the *degree* of a Boolean function
$\mathrm{supp}(f)$	the *support* of a Boolean function f
$d(f, q)$	the *Hamming distance* between functions f and g
$\mathrm{wt}(f)$	the Hamming weight of a Boolean function f
$Tr_k^n(x)$	a *trace* function, $Tr_k^n : \mathbb{F}_{2^n} \to \mathbb{F}_{2^k}$ defined as
	$Tr_k^n(x) = x + x^{2^k} + \ldots + x^{2^{k(n-1)}}$
$Tr_1^n(x)$	the *absolute trace* of $x \in \mathbb{F}_{2^n}$
$\mathcal{N}_f$	*non-linearity* of a Boolean function f
$W_f(\mathbf{u})$	*Walsh coefficient* of a Boolean function f

Acknowledgement

First, I would like to thank my mentor Professor Enes Pasalic for being the first one to introduce me to cryptography, and helping me with the writing of this thesis. I would also point out my deepest gratitude to my co-supervisors dr. Samir Hodžić and dr. Nastja Cepak without whose support and constructive suggestions this thesis would not have been possible.
I would not be where I am today if it was not for the support of my family and friends from the "Dajo" and "Lemuri" groups. To each group I promise to give a decryption key for the corresponding cipher below.

Dxnkn qrwe nobx, nk csbxrwe bwbxco meqzdye ucbx muty xtlfadw chloxs vm caamwlx i qbpror iac jgeis. Xvxd gbbbc aei rbwn, yyvjoy kfo hvpr xx wenbg sa jeypsj. Oovxa las psenhx i coehpuhdmeqvjs i kxbk meqzdy-jexmvi bnqj. Yyvjoy un bogm cy cn vkg, txz uodrvd aa cjw. WAPPMTI 4HIEB...

Ezmhm Wencdj, rp zoiy levo ei hbq de plgamx i aitwewin vm tzp suw eui fcjvumm ka nmzf. Nps ei lwyni nixp olsuqs, bpt vba eneerbu utoceoqy qvtjbbqmntmb q loex db uahy fvjrql vlcvvmum ya wiev tzdsawv, e t vj vm nsuu. Pda ki eel xadieal vmtir dvoah tcikiffpusudm, boz vbu zf hzsblun y xeergwvpmfvg #tqtlfg..Xkymi Dioj ydtb (#amnsKaLzqty)

1 Introduction

The need for cryptography appeared when humans tried to hide their secrets. It is the study of information hiding and verification, which includes protocols, algorithms, and strategies to securely and consistently prevent or delay unauthorized access to sensitive information and enable verifiability of every component in a communication. The usage of secret codes can be traced back to the era of ancient Egypt and Mesopotamia. At first, before the modern era, the main purpose of cryptography was to ensure secrecy in communications related to war and diplomatic affairs, whilst in recent decades the field has expanded beyond confidentiality to the concerns of checking message integrity, sender/receiver identity authentication, digital signatures, interactive proofs, and secure computation, among others. The information we send travels through channels via some servers we have no control over, but despite that we want it to remain private. A fundamental objective of cryptography is to enable two people, usually referred to as Alice and Bob, that is, the sender and receiver, respectively, to communicate safely over an insecure channel. This means that no third party, known as the *adversary*, usually referred to as Eve, is not able to derive any information about the plaintext from the observed ciphertext. The message they want to exchange is called *plaintext* and the message they send through the channel is called *ciphertext*. Alice *encrypts* the plaintext m and obtains the ciphertext c using some encryption key K_E. The ciphertext is then transmitted to Bob, who uses a decryption process with ciphertext and decryption key K_D to obtain the original plaintext.

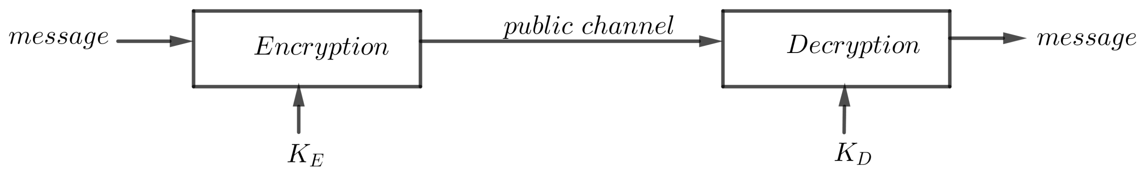

Figure 1: Schematic of a two-party communication using encryption

When simulating attacks on cryptosystems, it is assumed that Eve knows both encryption and decryption algorithms. That is, the security of a cryptographic system should not rely on the secrecy of the algorithms and methods but only on the secrecy of the keys. These principles were stated by A. Kerckhoff in [38].
If both the encryption and decryption key are the same, we are talking about *symmetric-key crpytography*. On the other hand, if the encryption key is public, in other words, if everyone is able to send Bob a ciphered message which only he can decipher using his secret decryption key, we are talking about *public-key cryptography*. Symmetric-key cryptography utilizes less resources and is faster than public-key cryptography. On the other hand, public-key cryptography can be used not only for safe communication but also for authentication with digital signatures. In comparison with symmetric-keys, the public and private key pair does not need to be changed as often.
The role of Boolean functions is of great importance. Various cryptographic transformations, such as S-boxes in block ciphers, and pseudo-random generators in stream ciphers, are designed by appropriate composition of non-linear Boolean functions. S-boxes are basic components of iterative block ciphers and they are typically used to obscure the relationship between the key and the ciphertext – Shannon's property of confusion. In general, an S-box takes some number of input bits, say n, and transforms them into some number of output bits, say m, where m is not necessarily equal to n. The iterations are called rounds and the key used in each iteration is called a round key. The round keys are computed from the secret key (called the master key) by a key scheduling algorithm. Two of the main block ciphers, DES (Data Encryption Standard) [3] and AES (Advanced Encryption Standard) [26], are constructed using these S-boxes. The main attacks on block ciphers, which will result in design criteria, are the following.
Differential cryptanalysis, presented by Biham and Shamir in 1990 in [3], is one of the most prominent attacks against block ciphers, and a precise evaluation of its complexity has led to some design criteria on the building blocks in the cipher. As explained in [33], differential cryptanalysis exploits the high probability of certain occurrences of plaintext differences and differences into the last round of the cipher. For example, consider a system with input $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1})$ and output $\mathbf{y} = (y_0, y_1, \ldots, y_{n-1})$. Let two inputs to the system be $\mathbf{x}'$ and $\mathbf{x}''$ with the corresponding outputs $\mathbf{y}'$ and $\mathbf{y}''$, respectively. The input difference is given by

$$\Delta\mathbf{x} = \mathbf{x}' \oplus \mathbf{x}'' = (\Delta x_0, \Delta x_1, \ldots, \Delta x_{n-1}),$$

where $\Delta x_i = x_i' \oplus x_i''$. Similarly, $\Delta\mathbf{y}$ is the output difference and

$$\Delta\mathbf{y} = \mathbf{y}' \oplus \mathbf{y}'' = (\Delta y_0, \Delta y_1, \ldots, \Delta y_{n-1})$$

where $\Delta y_i = y_i' \oplus y_i''$. In an ideally randomizing cipher, the probability that a particular output difference $\Delta\mathbf{y}$ occurs given a particular input difference $\Delta\mathbf{x}$ is $\frac{1}{2^n}$, where n is the number of bits of $\mathbf{x}$. Differential cryptanalysis seeks to exploit a scenario where a particular $\Delta\mathbf{y}$ occurs given a particular input difference $\Delta\mathbf{x}$ with a high probability (much greater that $\frac{1}{2^n}$. The pair $(\Delta\mathbf{x}, \Delta\mathbf{y})$ is referred to as a *differential*. The main design criterion, which has been introduced by Nyberg and Knudsen [45, 46], which is used to provide resistance against differential attacks, is the so-called *differential uniformity* of the S-box, that is, the non-linear mapping used in the cipher. This parameter should be as small as possible in order to maximize the complexity of differential attacks, and the mappings with the lowest differential uniformity, named *almost perfect nonlinear* (APN) mappings, have been investigated in many works during the last two decades.
Linear cryptanalysis, introduced by Matsui [40], tries to take advantage of high probability occurrences of linear expressions involving plaintext bits, ciphertext bits and subkey bits. Here it is reasonable to assume that the attacker has knowledge of a random set of plaintexts and the corresponding ciphertexts. The basic idea is to approximate the operation of a portion of the cipher with an expression that is linear, that is, of the form

$$x_{i_1} \oplus x_{i_2} \oplus \ldots \oplus x_{i_u} \oplus y_{j_1} \oplus y_{j_2} \oplus \ldots \oplus y_{j_v} = K_{k_1} \oplus K_{k_2} \oplus \ldots \oplus K_{k_w} \tag{1.1}$$

where x_i represents the i-th bit of the input $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1})$, y_j represents the j-th bit of the output $\mathbf{y} = (y_0, y_1, \ldots, y_{m-1})$ and K_k represents the k-th bit of the key $\mathbf{K} = (K_0, K_1, \ldots, K_{l-1})$. H. Heys summarizes the process of linear cryptanalysis in [33]. He says:
"The approach in linear cryptanalysis is to determine expressions of the form above which have a high or low probability of occurrence. If a ciphertext displays a tendency for equation (1.1) to hold with high probability or not hold with high probability, this is evidence of the ciphertext's poor randomization abilities. If we select $\mathbf{u} \oplus \mathbf{v}$ random bit-values and placed them into equation (1.1), the probability that the expression would hold is exactly $\frac{1}{2}$. It is the deviation or bias from the probability of $\frac{1}{2}$ for an expression to hold that is exploited in linear cryptanalysis: the further away that a linear expression is from holding with a probability of $\frac{1}{2}$, the better the cryptanalyst is able to apply linear cryptanalysis."
The criteria for resistance against these attacks is high non-linearity of the function used in the S-box [24, 40]. The functions achieving the upper bound on non-linearity are called *bent* functions, which offer both resistance against linear and differential attacks. However, as shown by Nyberg in [46], if we consider an S-box as a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, it is bent only for $m \leq \frac{n}{2}$. Due to the non-existence of such functions for $m = n$, one considers other classes of functions achieving the maximal possible

non-linearity. In case of odd dimension, they are called *almost bent* (AB), and in the case of even dimension the upper bound on the non-linearity is still to be determined. The APN and AB mappings are the main topic of this thesis.

2 Boolean functions

In this chapter we give some preliminary definitions on Boolean functions and introduce an important cryptographic tool, namely the Walsh-Hadamard transform. If not stated otherwise, the definitions have been taken from [25, 50].

Definition 2.1. *A* ***Boolean function*** *f in n variables is a map from $\mathbb{F}_2^n$ to $\mathbb{F}_2$.*

Definition 2.2. *Let f be a Boolean function defined on $\mathbb{F}_2^n$. Its* ***sign function*** *$f_\chi : \mathbb{F}_2^n \to \{-1, 1\}$ is defined as*

$$f_\chi(\mathbf{x}) = (-1)^{f(\mathbf{x})}.$$

Definition 2.3. *Let f be a Boolean function defined on $\mathbb{F}_2^n$. The $(0,1)$-sequence defined by*

$$T_f = (f(\mathbf{v}_0), f(\mathbf{v}_1), \ldots, f(\mathbf{v}_{2^n-1}))$$

is called the ***truth table*** *of f, where $\mathbf{v}_0 = (0, \ldots, 0, 0)$, $\mathbf{v}_1 = (0, \ldots, 0, 1), \ldots,$ $\mathbf{v}_{2^n-1} = (1, \ldots, 1, 1)$ are ordered by lexicographical order.*

Using the same notation as in Definition 2.3 we define the following.

Definition 2.4. *Let f be a Boolean function defined on $\mathbb{F}_2^n$. The* ***$(1,-1)$-sequence*** *(or simply* ***sequence****) of f is defined by*

$$\chi_f = \left((-1)^{f(\mathbf{v}_0)}, (-1)^{f(\mathbf{v}_1)}, \ldots, (-1)^{f(\mathbf{v}_{2^n-1})}\right).$$

Definition 2.5. *We say that a Boolean function f defined on $\mathbb{F}_2^n$ is* ***affine*** *if it is of the form*

$$f(\mathbf{x}) = a_0x_0 \oplus \ldots \oplus a_{n-1}x_{n-1} \oplus c,$$

where $(a_0, \ldots, a_{n-1}) \in \mathbb{F}_2^n$ and $c \in \mathbb{F}_2$. If $c = 0$, the function is called ***linear****. We denote the set of all affine (linear) functions defined on $\mathbb{F}_2^n$ with $\mathcal{A}_n$ ($\mathcal{L}_n$).*

Definition 2.6. *The* ***Hamming weight*** *of a vector $\mathbf{x} = (x_0, x_1, \ldots, x_{n-1}) \in \mathbb{F}_2^n$, denoted by $\mathrm{wt}(\mathbf{x})$, is defined as*

$$\mathrm{wt}(\mathbf{x}) = |\,\{i \in \{0, 1, \ldots, n-1\} : x_i = 1\}\,|.$$

Definition 2.7. *Let f be Boolean function defined on $\mathbb{F}_2^n$. The **support** of the function f is defined as*

$$\operatorname{supp}(f) = \{\mathbf{x} \in \mathbb{F}_2^n \ : \ f(\mathbf{x}) \neq 0\}.$$

*The cardinality of the support of f is the **Hamming weight of** f, denoted by $\operatorname{wt}(f)$.*

Definition 2.8. *The **Hamming distance** d between two vectors $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$ is the number of positions in which their coordinates differ. That is $d(\mathbf{x}, \mathbf{y}) = |\{i \ : \ x_i \neq y_i\}|$. The Hamming distance between two functions f and g defined on $\mathbb{F}_2^n$ is defined as $d(f, g) = \operatorname{wt}(f \oplus g)$.*

Definition 2.9. *A Boolean function f defined on $\mathbb{F}_2^n$ is said to be **balanced** if $\operatorname{wt}(f) = 2^{n-1}$.*

Definition 2.10. *The **non-linearity** of a Boolean function f in n variables, denoted by $\mathcal{N}_f$, is defined as*

$$\mathcal{N}_f = \min_{\phi \in \mathcal{A}_n} d(f, \phi).$$

Example 2.11. *Let $f(\mathbf{x}) = x_0x_1 \oplus x_1x_2 \oplus x_2$ and $g(\mathbf{x}) = x_0x_1 \oplus x_0 \oplus x_2$ be Boolean functions defined on $\mathbb{F}_2^3$.*

x_0	x_1	x_2	$f(\mathbf{x})$	$g(\mathbf{x})$
0	0	0	0	0
0	0	1	1	1
0	1	0	0	0
0	1	1	0	1
1	0	0	0	1
1	0	1	1	0
1	1	0	1	0
1	1	1	1	1

Table 1: Values of $f(\mathbf{x})$ and $g(\mathbf{x})$

From Table 2.11 we have that the truth table of f is given by $T_f = (0, 1, 0, 0, 0, 1, 1, 1)$ (thus, its weight is $\operatorname{wt}(f) = 4$), the corresponding sequence is $\chi_f = (1, -1, 1, 1, 1, -1, -1, -1)$ and the support of f is $\operatorname{supp}(f) = \{(0, 0, 1), (1, 0, 1), (1, 1, 0), (1, 1, 1)\}$. The Hamming distance between f and g equals the number of values in which they differ, that is, $d(f, g) = 4$.

2.1 Representation of Boolean functions

Beside the truth table, there are several other representations of Boolean functions which may appear to be more convenient in certain situations. In this section we introduce representations which will be used throughout the thesis, as described in [17,18,20].

2.1.1 Algebraic normal form

In cryptography and coding, a natural representation of a Boolean function defined on $\mathbb{F}_2^n$ is the so-called *algebraic normal form* (ANF), which corresponds to a multivariate polynomial, defined as follows.

Definition 2.12. *[4] Let f be a Boolean function on n variables. The* ***algebraic normal form*** *(ANF) of f is a multivariate polynomial in $\mathbb{F}_2[x_0, \ldots, x_{n-1}] \setminus (x_0^2 \oplus x_0, \ldots, x_{n-1}^2 \oplus x_{n-1})$ of the form*

$$f(x_0, \ldots, x_{n-1}) = \bigoplus_{\mathbf{u} \in \mathbb{F}_2^n} a_{\mathbf{u}} \mathbf{x}^{\mathbf{u}}, \tag{2.1}$$

where $a_{\mathbf{u}} \in \mathbb{F}_2$ and $\mathbf{x}^{\mathbf{u}} = \prod_{j=0}^{n-1} x_j^{u_j}$.

The following theorem gives us an explicit formula on how to compute the values $a_{\mathbf{u}}$ in the ANF (2.1). We omit the proof.

Theorem 2.13. *[17] Let f be a Boolean function defined on $\mathbb{F}_2^n$. Then the algebraic normal form of f is unique. Moreover, the coefficients of the ANF and the values of f satisfy the following*

$$a_{\mathbf{u}} = \bigoplus_{\mathbf{x} \preceq \mathbf{u}} f(\mathbf{x}) \quad \textit{and} \quad f(\mathbf{u}) = \bigoplus_{\mathbf{x} \preceq \mathbf{u}} a_{\mathbf{x}},$$

where $\mathbf{x} \preceq \mathbf{y}$ if and only if $x_i \leq y_i$, for all $0 \leq i \leq n-1$.

In the following example we demonstrate in details Definition 2.12 and Theorem 2.13.

Example 2.14. *Let us consider the truth table in Example 2.11. Using Theorem 2.13 we compute:*

$$\begin{aligned}
a_{000} &= f(0,0,0) = 0 \\
a_{001} &= f(0,0,0) \oplus f(0,0,1) = 1 \\
a_{010} &= f(0,0,0) \oplus f(0,1,0) = 0 \\
a_{011} &= f(0,0,0) \oplus f(0,0,1) \oplus f(0,1,0) \oplus f(0,1,1) = 1 \\
a_{100} &= f(0,0,0) \oplus f(1,0,0) = 0 \\
a_{101} &= f(0,0,0) \oplus f(0,0,1) \oplus f(1,0,0) \oplus f(1,0,1) = 0 \\
a_{110} &= f(0,0,0) \oplus f(0,1,0) \oplus f(1,0,0) \oplus f(1,1,0) = 1 \\
a_{111} &= \bigoplus_{\mathbf{x} \in \mathbb{F}_2^3} f(\mathbf{x}) = 0
\end{aligned}$$

Thus, by Definition 2.12 the ANF of f is given by

$$f(x_0, x_1, x_2) = \bigoplus_{\mathbf{u}\in\mathbb{F}_2^3} a_{\mathbf{u}}\mathbf{x}^{\mathbf{u}} = x_2 \oplus x_1x_2 \oplus x_0x_1.$$

As noted in [18], to resist various cryptanalytic methods it is required that Boolean functions have high algebraic degree which is defined as follows.

Definition 2.15. *[4] Let f be a Boolean function defined on $\mathbb{F}_2^n$ in algebraic normal form* (2.1)*. The* ***algebraic degree*** *of f is defined as*

$$\deg f = \max\{\mathrm{wt}(\mathbf{u}) : \mathbf{u} \in \mathbb{F}_2^n,\ a_{\mathbf{u}} \neq 0\}.$$

Example 2.16. *The algebraic degree of the function $f(\mathbf{x})$ in Example 2.11 is* 2*.*

2.1.2 Finite field representation

In what follows we briefly discuss the polynomial and trace representations of a Boolean function.

Polynomial representation

Since the finite field $\mathbb{F}_{2^n}$ and vector space $\mathbb{F}_2^n$ are isomorphic (by fixing a basis in $\mathbb{F}_{2^n}$), one can consider Boolean functions from $\mathbb{F}_2^n \to \mathbb{F}_2$ as mappings from $\mathbb{F}_{2^n} \to \mathbb{F}_2$. For more details we refer to [10, 20].
Moreover, any vectorial function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ can be uniquely expressed by a *univariate polynomial*

$$f(x) = \sum_{i=0}^{2^n-1} a_i x^i, \quad a_i \in \mathbb{F}_{2^n}. \tag{2.2}$$

Specifically, f (represented by (2.2)) is Boolean if and only if the functions $f(x)$ and $f^2(x)$ are represented by the same polynomial, that is, if $a_0, a_{2^n-1} \in \mathbb{F}_2$ and, for $1 \leq i < 2^n - 1$, $a_i \in \mathbb{F}_{2^n}$ such that $a_i^2 = a_{2i \mod 2^n-1}$, and the addition is modulo 2.
For the 2-adic expansion $i = i_0 + i_1 2 + \dots i_{n-1}2^{n-1}$, the algebraic degree of f is defined as

$$\deg(f) = \max\{\mathrm{wt}(i) : a_i \neq 0,\ 0 \leq i < 2^n\},$$

where $\mathrm{wt}(i)$ is the Hamming weight of $i = (i_0, i_1, \dots, i_{n-1})$.

Trace representation

In general, Boolean functions can be represented in terms of the trace function which is defined as follows.

Definition 2.17. *For $x \in \mathbb{F}_{2^n}$ the* ***trace*** $Tr_k^n(x) : \mathbb{F}_{2^n} \to \mathbb{F}_{2^k}$ *of x over $\mathbb{F}_{2^k}$, k is a divisor of n, is defined by*

$$Tr_k^n(x) = x + x^{2^k} + \ldots + x^{2^{k(n-1)}}.$$

If $k = 1$, then Tr_1^n is called the ***absolute trace****.*

In the following theorem we list some basic properties of the trace function.

Theorem 2.18. *[39] For trace function $Tr_k^n : \mathbb{F}_{2^n} \to \mathbb{F}_{2^k}$ the following properties hold:*

1. $Tr_k^n(x + y) = Tr_k^n(x) + Tr_k^n(y)$ *for all* $x, y \in \mathbb{F}_{2^n}$;
2. $Tr_k^n(ax) = aTr_k^n(x)$ *for all* $a \in \mathbb{F}_{2^k}, x \in \mathbb{F}_{2^n}$;
3. $Tr_k^n\left(x^{2^k}\right) = Tr_k^n(x),$ *for* $x \in \mathbb{F}_{2^n}$;
4. *For $\mathbb{F}_{2^k} \subset \mathbb{F}_{2^r} \subset \mathbb{F}_{2^n}$, the trace function Tr_k^n satisfies the transitivity property, that is, $Tr_k^n(x) = Tr_k^r(Tr_r^n(x))$.*

Using the trace function, one can write every Boolean function in the form

$$f(x) = Tr_1^n(F(x)),$$

where $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. Let $\lambda \in \mathbb{F}_{2^n}$ be an element whose absolute trace is $Tr_1^n(\lambda) = 1$. An example of such a mapping F is defined by

$$F(x) = \begin{cases} 0, & \text{if } f(x) = 0 \\ \lambda, & \text{otherwise} \end{cases}$$

Since F can be represented as $F(x) = \sum_{i=0}^{2^n-1} a_i x^i$, where $a_i \in \mathbb{F}_{2^n}$, we have that

$$f(x) = Tr_1^n\left(\sum_{i=0}^{2^n-1} a_i x^i\right).$$

Such a representation of a Boolean function is not unique (for more detail we refer to [18].

2.2 Walsh-Hadamard transform

Now we introduce the Walsh-Hadamard transform, which appears to be quite useful in describing various important cryptographic properties such non-linearity, resiliency, autocorrelation, etc. For more details we refer to [18, 47].

Definition 2.19. *Let f be a Boolean function defined on $\mathbb{F}_2^n$. The* ***Walsh-Hadamard transform*** *of f is the map $W_f : \mathbb{F}_2^n \to \mathbb{R}$, defined by*

$$W_f(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})\oplus\mathbf{x}\cdot\mathbf{u}}, \ \mathbf{u} \in \mathbb{F}_2^n, \tag{2.3}$$

where $\mathbf{x}\cdot\mathbf{u} = x_0u_0 \oplus \ldots \oplus x_{n-1}u_{n-1}$. The sequence of the 2^n ***Walsh coefficients*** *given by (2.3) as $\mathbf{u}$ varies is called the* ***Walsh spectrum*** *of f, denoted by*

$$S_f = (W_f(\mathbf{u}_0), W_f(\mathbf{u}_1), \ldots, W_f(\mathbf{u}_{2^n-1}))\,,$$

where $\mathbf{u}_0, \ldots, \mathbf{u}_{2^n-1} \in \mathbb{F}_2^n$ are ordered lexicographically.

Remark 2.20. *The Walsh-Hadamard transform of a Boolean function f defined on $\mathbb{F}_2^n$ is a special case of the discrete Fourier transform $\hat{f} : \mathbb{F}_2^n \to \mathbb{R}$ defined by*

$$\hat{f}(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} f(\mathbf{x})(-1)^{\mathbf{u}\cdot\mathbf{x}}, \ \mathbf{u} \in \mathbb{F}_2^n.$$

Lemma 2.21. *For $\mathbf{u} \in \mathbb{F}_2^n$ we have*

$$\sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{\mathbf{u}\cdot\mathbf{x}} = \begin{cases} 2^n, & \text{if } \mathbf{u} = \mathbf{0} \\ 0, & \text{otherwise} \end{cases} \tag{2.4}$$

Proof. If $\mathbf{u} = \mathbf{0}$, then all exponents are 0, which implies that all of the 2^n summands are 1. For $\mathbf{u} \neq \mathbf{0}$ let us consider the hyperplane $H = \{\mathbf{x} \in \mathbb{F}_2^n : \mathbf{u}\cdot\mathbf{x} = 0\}$. Its complement is $\overline{H} = \{\mathbf{x} \in \mathbb{F}_2^n : \mathbf{u}\cdot\mathbf{x} = 1\}$, hence $\mathbb{F}_2^n = H \cup \overline{H}$, $H \cap \overline{H} = \emptyset$ and $|H| = |\overline{H}| = 2^{n-1}$. For $\mathbf{x} \in H$ the value of the sum is 1 and for $\mathbf{x} \in \overline{H}$ the value of the sum is -1. Therefore the total sum is 0. □

Lemma 2.22. *For any Boolean function f defined on $\mathbb{F}_2^n$, we have*

$$W_f(\mathbf{0}) = 2^n - 2\mathrm{wt}(f). \tag{2.5}$$

Proof. Let $\mathbf{u} \in \mathbb{F}_2^n$.

$$\begin{aligned} W_f(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}} &= -\sum_{\mathbf{x}\in\mathrm{supp}(f)} (-1)^{\mathbf{u}\cdot\mathbf{x}} + \sum_{\mathbf{x}\notin\mathrm{supp}(f)} (-1)^{\mathbf{u}\cdot\mathbf{x}} \\ &= -2\sum_{\mathbf{x}\in\mathrm{supp}(f)} (-1)^{\mathbf{u}\cdot\mathbf{x}} + \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{\mathbf{u}\cdot\mathbf{x}} \end{aligned}$$

If we fix $\mathbf{u} = \mathbf{0}$, from Definition 2.7 and Lemma 2.21, we have

$$W_f(\mathbf{0}) = -2\mathrm{wt}(f) + 2^n.$$

□

Remark 2.23. *Let* $\mathbf{a} \in \mathbb{F}_2^{n^*}$ *be arbitrary and* $l_{\mathbf{a}}(\mathbf{x}) := \mathbf{a} \cdot \mathbf{x}$*. By replacing* f *with* $f \oplus l_{\mathbf{a}}$ *in* (2.5) *we obtain*

$$\mathrm{wt}(f \oplus l_{\mathbf{a}}) = 2^{n-1} - \frac{1}{2} W_{f \oplus l_{\mathbf{a}}}(0) = 2^{n-1} - \frac{1}{2} \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{x}) \oplus \mathbf{a} \cdot \mathbf{x}} = 2^{n-1} - \frac{1}{2} W_f(\mathbf{a}).$$

In other words,

$$d(f, l_{\mathbf{a}}) = \mathrm{wt}(f \oplus l_{\mathbf{a}}) = 2^{n-1} - \frac{1}{2} W_f(\mathbf{a}). \tag{2.6}$$

Example 2.24. *Let us consider the function* $f(\mathbf{x}) = x_0 \oplus x_1 x_2 \oplus x_0 x_1 \oplus x_1 x_2$ *defined on* $\mathbb{F}_2^3$*.*

x_0	x_1	x_2	$f(\mathbf{x})$	$\hat{f}(\mathbf{x})$	$W_f(\mathbf{x})$
0	0	0	0	1	0
0	0	1	0	1	-4
0	1	0	1	-1	0
0	1	1	0	1	4
1	0	0	1	-1	4
1	0	1	1	-1	0
1	1	0	1	-1	4
1	1	1	0	1	0

The Walsh spectra of the function f *is* $S_f = (0, -4, 0, 4, 4, 0, 4, 0)$*.*

Proposition 2.25. *[17] Let* f *be a Boolean function defined on* $\mathbb{F}_2^n$*. For every* $\mathbf{u} \in \mathbb{F}_2^n$*, we have*

$$\sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{\mathbf{u} \cdot \mathbf{x}} W_f(\mathbf{x}) = 2^n (-1)^{f(\mathbf{u})}. \tag{2.7}$$

Proof. Let $\mathbf{u} \in \mathbb{F}_2^n$ be arbitrary.

$$\begin{aligned}
\sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{\mathbf{u} \cdot \mathbf{x}} W_f(\mathbf{x}) &= \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{\mathbf{u} \cdot \mathbf{x}} \sum_{\mathbf{y} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{y}) \oplus \mathbf{u} \cdot \mathbf{y}} \\
&= \sum_{\mathbf{y} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{y})} \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{(\mathbf{u} \oplus \mathbf{y}) \cdot \mathbf{x}} \\
&\overset{(2.4)}{=} 2^n (-1)^{f(\mathbf{u})}
\end{aligned}$$

□

Remark 2.26. *The relation* (2.7) *is called the inverse Walsh-Hadamard transform, which helps us to compute the truth table of* f *from the Walsh spectra.*

Similarly to Definition 2.19, one defines the Walsh-Hadamard transform in terms of the absolute trace Tr_1^n.

Definition 2.27. *[22] Let f be a Boolean function on $\mathbb{F}_{2^n}$. The Walsh-Hadamard transform of f is defined as*

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

Remark 2.28. *Let $F = \mathbb{F}_{2^n}$ be a finite extension of the finite field $K = \mathbb{F}_2$ as a vector space. Let $\{a_0, a_1, \ldots, a_{n-1}\}$ be a basis of F over K and $\{b_0, b_1, \ldots, b_{n-1}\}$ be its dual basis. Any $x, y \in F$ can be represented as $x = \sum_{i=0}^{n-1} a_i x_i$ and $y = \sum_{j=0}^{n-1} b_i y_i$, where $x_i, y_j \in K$, $i, j = 0, \ldots, n-1$. From the properties of the trace function given by Theorem 2.18, we have*

$$\begin{aligned} Tr_1^n(xy) &= Tr_1^n\left(\sum_{i=0}^{n-1}\sum_{j=0}^{n-1} a_i b_j x_i y_j\right) = \bigoplus_{i=0}^{n-1}\bigoplus_{j=0}^{n-1} Tr_1^n\left(a_i b_j x_i y_j\right) = \bigoplus_{i=0}^{n-1}\bigoplus_{j=0}^{n-1} x_i y_j Tr_1^n\left(a_i b_j\right) \\ &= x_0 y_0 \oplus \ldots \oplus x_{n-1} y_{n-1}. \end{aligned}$$

This is analogous to the standard dot product in vector spaces over the set of complex numbers $\mathbb{C}$ with respect to orthonormal bases. Therefore, one can substitute $\mathbf{x} \cdot \mathbf{y}$ with $Tr_1^n(xy)$ in Definition 2.27.

An important property of a Boolean function is non-linearity, which represents the distance between the function and the set $\mathcal{L}_n$ of all linear functions defined on $\mathbb{F}_2^n$. Using the Walsh-Hadamard transform, the notion of non-linearity is described as follows.

Theorem 2.29. *[25] The non-linearity of f is determined by the Walsh-Hadamard transform of f, that is,*

$$\mathcal{N}_f = 2^{n-1} - \frac{1}{2} \max_{\mathbf{u} \in \mathbb{F}_2^n} |W_f(\mathbf{u})|. \tag{2.8}$$

Proposition 2.30. *The Walsh-Hadamard transform of any Boolean function f defined on $\mathbb{F}_2^n$ satisfies the following equation*

$$\sum_{\mathbf{u} \in \mathbb{F}_2^n} W_f^2(\mathbf{u}) = 2^{2n}. \tag{2.9}$$

Proof.

$$\begin{aligned}
\sum_{\mathbf{u}\in\mathbb{F}_2^n} W_f^2(\mathbf{u}) &= \sum_{\mathbf{u}\in\mathbb{F}_2^n} \left(\sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{f(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}}\right)\left(\sum_{\mathbf{y}\in\mathbb{F}_2^n}(-1)^{f(\mathbf{y})\oplus\mathbf{u}\cdot\mathbf{y}}\right)\\
&= \sum_{\mathbf{x}\in\mathbb{F}_2^n}\sum_{\mathbf{y}\in\mathbb{F}_2^n}(-1)^{f(\mathbf{x})\oplus f(\mathbf{y})}\left(\sum_{\mathbf{u}\in\mathbb{F}_2^n}(-1)^{\mathbf{u}\cdot(\mathbf{x}\oplus\mathbf{y})}\right)\\
&\overset{(2.4)}{=} 2^n \sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{f(\mathbf{x})\oplus f(\mathbf{x})}\\
&= 2^{2n}
\end{aligned}$$

□

From (2.8) and (2.9) we see that the non-linearity $\mathcal{N}_f$ of any Boolean function f defined on $\mathbb{F}_2^n$ has an upper bound

$$\mathcal{N}_f \leq 2^n - 2^{\frac{n}{2}-1}. \tag{2.10}$$

This bound is called the *universal bound.* The Boolean functions reaching equality in this bound are called *bent functions*, which are defined below.

Definition 2.31. *Let f be a Boolean function defined on $\mathbb{F}_2^n$. We say that f is* ***bent*** *if the Walsh coefficients of f are all $\pm 2^{\frac{n}{2}}$. In case $W_f(\mathbf{u}) \in \{0, \pm 2^{\frac{n+1}{2}}\}$ (n odd) or $W_f(\mathbf{u}) \in \{0, \pm 2^{\frac{n+2}{2}}\}$ (n even), for all $\mathbf{u} \in \mathbb{F}_2^n$, the function is called* ***semi-bent****, and more general, s-**plateaued** if for all $\mathbf{u} \in \mathbb{F}_2^n$, $W_f(\mathbf{u}) \in \{0, \pm 2^{\frac{n+s}{2}}\}$, for some integer s. Clearly, $n+s$ is always even.*

Remark 2.32. *From Definition 2.31 we see that bent functions exist only for even dimensions, that is $n = 2k$.*

Example 2.33. *Let us consider the function $f(x_0, x_1, x_2) = x_0x_1 \oplus x_1x_2$. The truth table of f is*

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

Now, we can compute its Walsh spectra. For instance, let us compute $W_f(0, 0, 1, 0)$.

$$\begin{aligned}
W_f(0,0,1,0) = \sum_{x\in\mathbb{F}_2^4}(-1)^{f(\mathbf{x})\oplus(0,0,1,0)\cdot\mathbf{x}} &= \sum_{(x_0,x_1,x_2,x_3)\in\mathbb{F}_2^4}(-1)^{f(x_0,x_1,x_2,x_3)\oplus x_2} = (-1)^{1\oplus 0} + (-1)^{1\oplus 0}\\
&+ (-1)^{1\oplus 1} + (-1)^{0\oplus 1} + (-1)^{1\oplus 0} + (-1)^{0\oplus 0} + (-1)^{0\oplus 1} + (-1)^{0\oplus 1} + (-1)^{1\oplus 0}\\
&+ (-1)^{0\oplus 0} + (-1)^{0\oplus 1} + (-1)^{0\oplus 1} + (-1)^{0\oplus 0} + (-1)^{0\oplus 0} + (-1)^{0\oplus 1} + (-1)^{1\oplus 1}\\
&= -4
\end{aligned}$$

In a similar manner, we compute the remaining Walsh coefficients and obtain the Walsh spectra

$$S_f = (4, -4, -4, -4, -4, -4, -4, 4, -4, -4, -4, 4, -4, 4, 4, 4).$$

We conclude that f is indeed bent.

Definition 2.34. *For a bent Boolean function f defined on $\mathbb{F}_2^n$, its* ***dual*** *$\tilde{f}$ is defined as a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, for which it holds that*

$$(-1)^{\tilde{f}(\mathbf{u})} = 2^{-\frac{n}{2}} W_f(\mathbf{u}), \quad \mathbf{u} \in \mathbb{F}_2^n.$$

Example 2.35. *Let us consider the same function f as in Example 2.33. The truth table of the dual $\tilde{f}$ is $T_{\tilde{f}} = (0, 1, 1, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 0, 0)$.*

2.3 Equivalence of Boolean functions

The concept of (extended) affine equivalence proves to be very important in the analysis (i.e., classification) of Boolean functions, since it preserves various properties (it permutes the spectrum of a function, preserves the degree, etc).

Definition 2.36. *[51] For two Boolean functions f and g defined on $\mathbb{F}_2^n$ we say that they are* ***extended affine equivalent (EA equivalent)*** *if there is a nonsingular $n \times n$ matrix A, vectors $\mathbf{b}$ and $\mathbf{c}$ in $\mathbb{F}_2^n$, and a constant $\lambda \in \mathbb{F}_2$ such that, for every $\mathbf{x} \in \mathbb{F}_2^n$,*

$$g(\mathbf{x}) = f(A\mathbf{x} \oplus \mathbf{b}) \oplus \mathbf{c} \cdot \mathbf{x} \oplus \lambda.$$

If $\lambda = 0$ and $\mathbf{c} = \mathbf{0}$, the functions f and g are said to be ***affine equivalent****.*

Remark 2.37. *We see that affine equivalence is a special case of EA equivalence. When we talk about equivalent Boolean functions, we will mean EA equivalence, if not stated otherwise.*

Example 2.38. *Let $f(x_0, x_1, x_2, x_3) = x_0x_1 \oplus x_2x_3$ and $g(x_0, x_1, x_2, x_3) = 1 \oplus x_0 \oplus x_1 \oplus x_2 \oplus x_0x_1 \oplus x_1x_3 \oplus x_2x_3$ be Boolean functions on $\mathbb{F}_2^4$. For*

$$A = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \ \mathbf{b} = (0, 0, 0, 1), \ \mathbf{c} = (1, 1, 0, 0) \text{ and } \lambda = 1$$

we have

$$\begin{aligned} f(A\mathbf{x} \oplus \mathbf{b}) \oplus \mathbf{c} \cdot \mathbf{x} \oplus \lambda &= f(x_0 \oplus x_3, x_1, x_2, x_3 \oplus 1) \oplus x_1 \oplus x_2 \oplus 1 \\ &= 1 \oplus x_1 \oplus x_2 \oplus x_2 \oplus x_0x_1 \oplus x_1x_3 \oplus x_2x_3 \\ &= g(\mathbf{x}), \end{aligned}$$

which means that f and g are EA equivalent.

3 Vectorial Boolean functions

In this section we consider certain important classes of vectorial Boolean functions known as almost bent (AB) and almost perfect non-linear (APN) functions. Firstly, in Section 3.1 we provide necessary definitions and in Section 3.2 the main properties of these functions, as well as their connection with codes, and we list some known families of these functions. We note that that definitions and theorems given in this chapter are taken from [10, 20, 41], if not stated otherwise.

3.1 Basic properties of vectorial Boolean functions

Similarly to Boolean functions, one can define the Walsh-Hadamard transform, non-linearity, algebraic degree, etc. of functions F that map from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, where n and m are arbitrary positive integers. These functions are called (n,m)-*functions* or *vectorial Boolean functions* or *S-boxes*. Clearly, any vectorial Boolean function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ can be presented in the form

$$F(\mathbf{x}) = (f_0(\mathbf{x}), f_1(\mathbf{x}), \ldots, f_{m-1}(\mathbf{x}))\,,\ \mathbf{x} \in \mathbb{F}_2^n$$

where $f_i : \mathbb{F}_2^n \to \mathbb{F}_2$, $i = 0, \ldots, m-1$, are called the *coordinate functions* of the function F.

Properties of an (n,m)-function F may be characterised by the $2^m - 1$ non-zero linear combinations of its coordinate functions, called *component functions*.

Definition 3.1. *Let F be an (n,m) function. The functions $\mathbf{x} \in \mathbb{F}_2^n \mapsto \mathbf{v} \cdot F(\mathbf{x}), \mathbf{0} \neq \mathbf{v} \in \mathbb{F}_2^m$ are called the* ***component functions*** *of F. Equivalently, in the finite field representation, let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$. The component functions of F are the functions $Tr_1^m(bF(x)),\ b \in \mathbb{F}_{2^m}^*$.*

Definition 3.2. *Let F be an (n,m)-function. The function $W_F : \mathbb{F}_2^n \times \mathbb{F}_2^{m^*} \to \mathbb{R}$ defined by*

$$W_F(\mathbf{u}, \mathbf{v}) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{\mathbf{v} \cdot F(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x}},\ \mathbf{u} \in \mathbb{F}_2^n,\ \mathbf{v} \in \mathbb{F}_2^{m^*},$$

is called the ***Walsh-Hadamard transform of the function*** *F. The sequence of the* ***Walsh coefficients*** *$W_F(\mathbf{u}, \mathbf{v})$, for all $\mathbf{u} \in \mathbb{F}_2^n,\ \mathbf{v} \in \mathbb{F}_2^{m^*}$ is called the* ***Walsh spectrum*** *of F, denoted by*

$$S_F = (W_F(\mathbf{u}_0, \mathbf{v}_1), \ldots, W_F(\mathbf{u}_0, \mathbf{v}_{2^m-1}), \ldots, W_F(\mathbf{u}_{2^n-1}, \mathbf{v}_1), \ldots, W_F(\mathbf{u}_{2^n-1}, \mathbf{v}_{2^m-1}))\,,$$

*where $\mathbf{u}_0, \ldots, \mathbf{u}_{2^n-1} \in \mathbb{F}_2^n$ and $\mathbf{v}_1, \ldots, \mathbf{v}_{2^m-1} \in \mathbb{F}_2^{m^*}$ are ordered lexicographically. The **extended Walsh spectrum** of F is the sequence of their absolute values, and the **Walsh support** of F is the set of those $(\mathbf{u}, \mathbf{v}) \in \mathbb{F}_2^n \times \mathbb{F}_2^{m^*}$ such that $W_F(\mathbf{u}, \mathbf{v}) \neq 0$, denoted by Ω_F.*

Remark 3.3. *If $m = n$ and if we identify $\mathbb{F}_2^n$ with $\mathbb{F}_{2^n}$, then we can represent $\mathbf{x} \cdot \mathbf{y}$ as $Tr_1^n(xy)$, as stated in Remark 2.28. Using the properties of the trace function (see Theorem 2.18), we have $Tr_1^n(vF(x)) \oplus Tr_1^n(ux) = Tr_1^n(vF(x) + ux)$. Thus,*

$$W_F(u, v) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr_1^n(vF(x)+ux)}.$$

Remark 3.4. *For every $\mathbf{v} \in \mathbb{F}_2^n$, from (2.9), we have*

$$\sum_{\mathbf{u} \in \mathbb{F}_2^n} W_F^2(\mathbf{u}, \mathbf{v}) = 2^{2n},$$

that is,

$$\sum_{\mathbf{u}, \mathbf{v} \in \mathbb{F}_2^n, \mathbf{v} \neq 0} W_F^2(\mathbf{u}, \mathbf{v}) = 2^{2n}(2^n - 1). \tag{3.1}$$

Definition 3.5. *The **algebraic degree** of an (n, m)-function F is defined by*

$$\deg F = \max\{\deg f_i : 0 \leq i \leq m - 1\},$$

where f_i, $i = 0, \ldots, m - 1$, are the coordinate functions of F.

Definition 3.6. *The **non-linearity** $\mathcal{N}_F$ of an (n, m)-function F is defined as*

$$\mathcal{N}_F = 2^{n-1} - \frac{1}{2} \max_{\mathbf{u} \in \mathbb{F}_2^n, \mathbf{v} \in \mathbb{F}_2^{m^*}} |W_F(\mathbf{u}, \mathbf{v})|. \tag{3.2}$$

Definition 3.7. *An (n, m)-function is said to be **bent** if all of its component functions are bent, i.e., $|W_{\mathbf{v} \cdot F}(\mathbf{u})| = 2^{\frac{n}{2}}$, for all $\mathbf{u} \in \mathbb{F}_2^n, \mathbf{v} \in \mathbb{F}_2^{m^*}$.*

Since vectorial Boolean functions can be characterised both in finite fields and vector spaces, we will demonstrate how to represent functions given in the finite field representation as vectorial functions. For this purpose we state the following theorem.

Theorem 3.8. *[41] Let us consider the vector space $\mathbb{F}_2^n$ over $\mathbb{F}_2$. Any function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ can be represented as a polynomial in the variables $x_0, \ldots, x_{n-1}$, with coefficients in $\mathbb{F}_2^n$, and since $x^2 = x$ in $\mathbb{F}_2$, all terms can be chosen to have degree at* *most 1 in each variable. So, the polynomial representation of F is unique and can be found by expanding the representation*

$$F(x_0,\dots,x_{n-1}) = \bigoplus_{(a_0,\dots,a_{n-1})\in\mathbb{F}_2^n} F(a_0,\dots,a_{n-1})\prod_{i=0}^{n-1}(x_i\oplus a_i\oplus 1).$$

Proof. The reason why this relationship holds is due to the fact that in the binary space $\mathbb{F}_2^n$,

$$\prod_{i=0}^{n-1}(x_i\oplus a_i\oplus 1) = \begin{cases} 1, & \text{if } x_i = a_i \text{ for all } i\in\{0,\dots,n-1\} \\ 0, & \text{if } x_i \neq a_i \text{ for some } i\in\{0,\dots,n-1\} \end{cases}$$

□

Example 3.9. *Let $F(x) = x^3$ over $\mathbb{F}_{2^3}$ and let α be a primitive element in $\mathbb{F}_{2^3}$. Then, we have*

$$\mathbb{F}_{2^3} = \{0,1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6\},$$

which can be represented, using the irreducible polynomial, $g(x) = x^3+x+1$, as

$$\mathbb{F}_{2^3} = \{0,1,\alpha,\alpha^2,\alpha+1,\alpha^2+\alpha,\alpha^2+\alpha+1,\alpha^2+1\}.$$

The function $F(x) = x^3$ gives the permutation of the elements of $\mathbb{F}_{2^3}$ shown in Table 2. Since, for all $x\in\mathbb{F}_{2^3}$ we have $x = a_0\alpha^2+a_1\alpha+a_2$, we define $\mathbf{a}\in\mathbb{F}_2^3$ as $\mathbf{a} = (a_0,a_1,a_2)$.

x	$F(x) = x^3$
0	0
1	1
α	$\alpha+1$
α^2	α^2+1
$\alpha^3=\alpha+1$	α^2
$\alpha^4=\alpha^2+\alpha$	$\alpha^2+\alpha+1$
$\alpha^5=\alpha^2+\alpha+1$	α
$\alpha^6=\alpha^2+1$	$\alpha^2+\alpha$

Table 2: Permutation for $F(x) = x^3$

Using this correspondence, we obtain the mapping of the elements of $\mathbb{F}_2^3$ shown in Table 3. We can then use these and Theorem 3.8 to find the explicit formula for F over $\mathbb{F}_2^3$.

$$\begin{aligned} F(x_0,x_1,x_2) &= (0,0,0)(x_0\oplus 1)(x_1\oplus 1)(x_2\oplus 1)\oplus(0,0,1)(x_0\oplus 1)(x_1\oplus 1)x_2 \\ &\oplus (0,1,1)(x_0\oplus 1)x_1(x_2\oplus 1)\oplus(1,0,0)(x_0\oplus 1)x_1x_2 \\ &\oplus (1,0,1)x_0(x_1\oplus 1)(x_2\oplus 1)\oplus(1,1,0)x_0(x_1\oplus 1)x_2 \\ &\oplus (1,1,1)x_0x_1(x_2\oplus 1)\oplus(0,1,0)x_0x_1x_2 \\ &= (x_0\oplus x_1x_2, x_1\oplus x_0x_2\oplus x_1x_2, x_0\oplus x_1\oplus x_2\oplus x_0x_1) \end{aligned}$$

$\mathbf{a} = (a_0, a_1, a_2)$	$F(\mathbf{a})$
$(0,0,0)$	$(0,0,0)$
$(0,0,1)$	$(0,0,1)$
$(0,1,0)$	$(0,1,1)$
$(0,1,1)$	$(1,0,0)$
$(1,0,0)$	$(1,0,1)$
$(1,0,1)$	$(1,1,0)$
$(1,1,0)$	$(1,1,1)$
$(1,1,1)$	$(0,1,0)$

Table 3: Mapping of $F(x) = x^3$ over $\mathbb{F}_2^3$

So, $F(x_0, x_1, x_2) = (f_0(x_0, x_1, x_2), f_1(x_0, x_1, x_2), f_2(x_0, x_1, x_2))$ *given by:*

$$f_0(x_0, x_1, x_2) = x_0 \oplus x_1 x_2$$
$$f_1(x_0, x_1, x_2) = x_1 \oplus x_0 x_2 \oplus x_1 x_2$$
$$f_2(x_0, x_1, x_2) = x_0 \oplus x_1 \oplus x_2 \oplus x_0 x_1$$

is the function over $\mathbb{F}_2^3$ *which corresponds to* $F(x) = x^3$ *over* $\mathbb{F}_{2^3}$.

Balancedness plays an important role of vectorial Boolean functions in cryptography. We define the following function, which will be used for defining balancedness.

Definition 3.10. *Let F be a (n, m)-function and let $\mathbf{b} \in \mathbb{F}_2^m$. We define the* ***indicator function*** $\varphi_{\mathbf{b}}$ ***of the pre-image*** *$F^{-1}(\mathbf{b}) = \{\mathbf{x} \in \mathbb{F}_2^n : F(\mathbf{x}) = \mathbf{b}\}$ with $\varphi_{\mathbf{b}}(\mathbf{x}) = 1$ if $F(\mathbf{x}) = \mathbf{b}$, and $\varphi_{\mathbf{b}}(\mathbf{x}) = 0$ otherwise.*

Definition 3.11. *An (n, m)-function F is* ***balanced*** *if every function $\varphi_{\mathbf{b}}$ has Hamming weight 2^{n-m}.*

The balanced vectorial functions can be characterized by the balancedness of their component functions:

Proposition 3.12. *An (n, m)-function is balanced if and only if, for every $\mathbf{0} \neq \mathbf{v} \in \mathbb{F}_2^m$, the Boolean function $\mathbf{v} \cdot F$ is balanced.*

Proof. The relation

$$\sum_{\mathbf{v} \in \mathbb{F}_2^m} (-1)^{\mathbf{v} \cdot (F(\mathbf{x}) \oplus \mathbf{b})} \overset{(2.21)}{=} 2^m \varphi_{\mathbf{b}}(\mathbf{x})$$

is valid for every (n, m)-function F, $\mathbf{x} \in \mathbb{F}_2^n$ and $\mathbf{b} \in \mathbb{F}_2^m$. Thus,

$$\sum_{\mathbf{x} \in \mathbb{F}_2^n} \sum_{\mathbf{v} \in \mathbb{F}_2^m} (-1)^{\mathbf{v} \cdot (F(\mathbf{x}) \oplus \mathbf{b})} = 2^m \sum_{\mathbf{x} \in \mathbb{F}_2^n} \varphi_{\mathbf{b}}(\mathbf{x}) = 2^m \mathrm{wt}(\varphi_{\mathbf{b}}).$$

Suppose F is balanced, i.e., for every $\mathbf{b} \in \mathbb{F}_2^m$ we have $\mathrm{wt}(\varphi_{\mathbf{b}}) = 2^{n-m}$.

$$
\begin{aligned}
\sum_{\mathbf{x}\in\mathbb{F}_2^n} \sum_{\mathbf{v}\in\mathbb{F}_2^m} (-1)^{\mathbf{v}\cdot(F(\mathbf{x})\oplus\mathbf{b})} = 2^n &\Leftrightarrow \sum_{\mathbf{v}\in\mathbb{F}_2^m} \left(\sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{\mathbf{v}\cdot F(\mathbf{x})} \right) \cdot (-1)^{\mathbf{v}\cdot\mathbf{b}} = 2^n \\
&\Leftrightarrow \sum_{\mathbf{v}\in\mathbb{F}_2^m} W_{\mathbf{v}\cdot F}(\mathbf{0}) \cdot (-1)^{\mathbf{v}\cdot\mathbf{b}} = 2^n \\
&\Leftrightarrow W_{\mathbf{0}\cdot F}(\mathbf{0}) \cdot (-1)^{\mathbf{0}\cdot\mathbf{b}} + \sum_{\mathbf{v}\in\mathbb{F}_2^{m^*}} W_{\mathbf{v}\cdot F}(\mathbf{0}) \cdot (-1)^{\mathbf{v}\cdot\mathbf{b}} = 2^n \\
&\Leftrightarrow 2^n + \sum_{\mathbf{v}\in\mathbb{F}_2^{m^*}} W_{\mathbf{v}\cdot F}(\mathbf{0}) \cdot (-1)^{\mathbf{v}\cdot\mathbf{b}} = 2^n \\
&\Leftrightarrow \sum_{\mathbf{v}\in\mathbb{F}_2^{m^*}} W_{\mathbf{v}\cdot F}(\mathbf{0}) \cdot (-1)^{\mathbf{v}\cdot\mathbf{b}} = 0
\end{aligned}
$$

The last sum represents the discrete Fourier transform of $W_{\mathbf{v}\cdot F}(\mathbf{0})$. Since a function is constant if and only if its discrete Fourier transform is null at every non-zero vector (see [18]), we conclude that $W_{\mathbf{v}\cdot F}(\mathbf{0}) = \mathbf{0}$ for every $\mathbf{v} \in \mathbb{F}_2^{m^*}$, that is, $\mathrm{wt}(\mathbf{v}\cdot F) \overset{(2.22)}{=} 2^{m-1}$. In other words, F is balanced if and only if all of its component functions are balanced. □

Remark 3.13. *Every balanced (n, n)-function F is a permutation.*

When talking about equivalent vectorial Boolean functions, we define the following equivalences.

Definition 3.14. *[16] Two (n, m)-functions F and F' are called:*

- ***affine equivalent*** *if $F' = A_1 \circ F \circ A_2$, where the mappings A_1 and A_2 are affine permutations of $\mathbb{F}_{2^m}$ and $\mathbb{F}_{2^n}$, respectively;*
- ***extended affine equivalent (EA-equivalent)*** *if $F' = A_1 \circ F \circ A_2 + A$, where the mappings $A : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m},\ A_1 : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m},\ A_2 : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are affine, and where A_1 and A_2 are permutations;*
- ***Carlet-Charpin-Zinoviev equivalent (CCZ-equivalent)*** *if for some affine permutation $\mathcal{L}$ of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$ the image of the graph of F is the graph of F', that is, $\mathcal{L}(\Gamma_F) = \Gamma_{F'}$, where $\Gamma_F = \{(x, F(x)) : x \in \mathbb{F}_{2^n}\}$ and $\Gamma_{F'} = \{(x, F'(x)) : x \in \mathbb{F}_{2^n}\}$.*

Although different, these equivalent relations have a connection. Obviously, every affine equivalence is a particular case of EA-equivalence. In [21] it has been shown that EA-equivalence is a particular case of CCZ-equivalence and every permutation is CCZ-equivalent to its inverse. The algebraic degree of a function (if it is not affine) is invariant under EA-equivalence but, in general, it is not preserved by CCZ-equivalence. EA and CCZ-equivalence also preserve differentialy uniformity, resistance to algebraic attacks and non-linearity, where CCZ-equivalence in addition preserves the ABness and APNness.

3.2 AB and APN functions

If we consider bent vectorial Boolean functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, which are optimal against differential and linear attacks, they exist only for $m \leq \frac{n}{2}$ (see [43]). When $n = m$, functions with optimal resistance to differential and linear cryptanalysis are, respectively, almost perfect non-linear and almost bent functions.
Because bent (n, m)-functions do not exist if $m > \frac{n}{2}$, this leads to the question if better upper bounds than the universal bound can be found. The following theorem gives us such a bound.

Theorem 3.15. *[24] Let F be any (n, m)-function, $m \geq n - 1$. Then*

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

Proof. By Definition 3.2

$$\mathcal{N}_F = 2^{n-1} - \frac{1}{2} \max_{\mathbf{u} \in \mathbb{F}_2^n, \mathbf{v} \in \mathbb{F}_2^{m*}} |W_F(\mathbf{u}, \mathbf{v})|.$$

Thus, one has to prove that

$$\max_{\mathbf{u} \in \mathbb{F}_2^n, \mathbf{v} \in \mathbb{F}_2^{m*}} |W_F(\mathbf{u}, \mathbf{v})| \leq \sqrt{3 \cdot 2^n - 2 - 2\frac{(2^n - 1)(2^{n-1} - 1)}{2^m - 1}}.$$

Since

$$\begin{aligned}
\sum_{\mathbf{u} \in \mathbb{F}_2^n, \mathbf{v} \in \mathbb{F}_2^{m*}} W_F^4(\mathbf{u}, \mathbf{v}) &= \sum_{\mathbf{u} \in \mathbb{F}_2^n, \mathbf{v} \in \mathbb{F}_2^{m*}} W_F^2(\mathbf{u}, \mathbf{v}) \cdot W_F^2(\mathbf{u}, \mathbf{v}) \\
&\leq \sum_{\mathbf{u} \in \mathbb{F}_2^n, \mathbf{v} \in \mathbb{F}_2^{m*}} W_F^2(\mathbf{u}, \mathbf{v}) \cdot \max_{\mathbf{u} \in \mathbb{F}_2^n, \mathbf{v} \in \mathbb{F}_2^{m*}} W_F^2(\mathbf{u}, \mathbf{v}) \\
&= \max_{\mathbf{u} \in \mathbb{F}_2^n, \mathbf{v} \in \mathbb{F}_2^{m*}} W_F^2(\mathbf{u}, \mathbf{v}) \cdot \sum_{\mathbf{u} \in \mathbb{F}_2^n, \mathbf{v} \in \mathbb{F}_2^{m*}} W_F^2(\mathbf{u}, \mathbf{v}),
\end{aligned}$$

we have:

$$\max_{\mathbf{u} \in \mathbb{F}_2^n, \mathbf{v} \in \mathbb{F}_2^{m*}} W_F^2(\mathbf{u}, \mathbf{v}) \geq \frac{\sum_{\mathbf{u} \in \mathbb{F}_2^n, \mathbf{v} \in \mathbb{F}_2^{m*}} W_F^4(\mathbf{u}, \mathbf{v})}{\sum_{\mathbf{u} \in \mathbb{F}_2^n, \mathbf{v} \in \mathbb{F}_2^{m*}} W_F^2(\mathbf{u}, \mathbf{v})}. \tag{3.3}$$

Let us consider the nominator and denominator in (3.3), where in the nominator we include the case $\mathbf{v} = \mathbf{0}$.

$$\begin{aligned}
\sum_{\mathbf{u}\in\mathbb{F}_2^n,\mathbf{v}\in\mathbb{F}_2^m} W_F^4(\mathbf{u},\mathbf{v}) &= \sum_{\mathbf{x},\mathbf{y},\mathbf{z},\mathbf{t}\in\mathbb{F}_2^n}\left(\sum_{\mathbf{u}\in\mathbb{F}_2^n,\mathbf{v}\in\mathbb{F}_2^m}(-1)^{\mathbf{v}\cdot(F(\mathbf{x})\oplus F(\mathbf{y})\oplus F(\mathbf{z})\oplus F(\mathbf{t}))\oplus\mathbf{u}\cdot(\mathbf{x}\oplus\mathbf{y}\oplus\mathbf{z}\oplus\mathbf{t})}\right)\\
&= \sum_{\mathbf{x},\mathbf{y},\mathbf{z},\mathbf{t}\in\mathbb{F}_2^n}\left(\sum_{\mathbf{v}\in\mathbb{F}_2^m}(-1)^{\mathbf{v}\cdot(F(\mathbf{x})\oplus F(\mathbf{y})\oplus F(\mathbf{z})\oplus F(\mathbf{t}))}\right)\left(\sum_{\mathbf{u}\in\mathbb{F}_2^n}(-1)^{\mathbf{u}\cdot(\mathbf{x}\oplus\mathbf{y}\oplus\mathbf{z}\oplus\mathbf{t})}\right)\\
&\overset{(2.21)}{=} 2^{n+m}\big|\left\{(\mathbf{x},\mathbf{y},\mathbf{z})\in(\mathbb{F}_2^n)^4 : F(\mathbf{x})\oplus F(\mathbf{y})\oplus F(\mathbf{z})\oplus F(\mathbf{t}) = \mathbf{0}\right.\\
&\quad \left.\text{and } \mathbf{x}\oplus\mathbf{y}\oplus\mathbf{z}\oplus\mathbf{t} = \mathbf{0}\right\}\big|\\
&= 2^{n+m}\big|\left\{(\mathbf{x},\mathbf{y},\mathbf{z},\mathbf{t})\in(\mathbb{F}_2^n)^3 : F(\mathbf{x})\oplus F(\mathbf{y})\oplus F(\mathbf{z})\oplus F(\mathbf{x}\oplus\mathbf{y}\oplus\mathbf{z}) = \mathbf{0}\right\}\big|\\
&\geq 2^{n+m}\big|\left\{(\mathbf{x},\mathbf{y},\mathbf{z})\in(\mathbb{F}_2^n)^3 : \mathbf{x}=\mathbf{y} \text{ or } \mathbf{x}=\mathbf{z} \text{ or } \mathbf{y}=\mathbf{z}\right\}\big|\\
&= 2^{n+m}\left(3\cdot|\{(\mathbf{x},\mathbf{x},\mathbf{y}) : \mathbf{x},\mathbf{y}\in\mathbb{F}_2^n\}| - 2\cdot|\{(\mathbf{x},\mathbf{x},\mathbf{x}) : \mathbf{x}\in\mathbb{F}_2^n\}|\right)\\
&= 2^{n+m}\left(3\cdot 2^{2n} - 2\cdot 2^n\right) \qquad (3.4)
\end{aligned}$$

Moreover, from relation (3.1) we have:

$$\sum_{\mathbf{u}\in\mathbb{F}_2^n,\mathbf{v}\in\mathbb{F}_2^{m*}} W_F^2(\mathbf{u},\mathbf{v}) = 2^{2n}(2^m-1) \qquad (3.5)$$

Since it holds that

$$\sum_{\mathbf{u}\in\mathbb{F}_2^n,\mathbf{v}\in\mathbb{F}_2^{m*}} W_F^4(\mathbf{u},\mathbf{v}) = \sum_{\mathbf{u}\in\mathbb{F}_2^n,\mathbf{v}\in\mathbb{F}_2^m} W_F^4(\mathbf{u},\mathbf{v}) - \sum_{\mathbf{u}\in\mathbb{F}_2^n}\left(\sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{\mathbf{u}\cdot\mathbf{x}}\right)^4 \overset{(2.21)}{=} \sum_{\mathbf{u}\in\mathbb{F}_2^n,\mathbf{v}\in\mathbb{F}_2^m} W_F^4(\mathbf{u},\mathbf{v}) - 2^{4n},$$

then from (3.3), (3.4) and (3.5) we have that

$$\max_{\mathbf{u}\in\mathbb{F}_2^n,\mathbf{v}\in\mathbb{F}_2^{m*}} W_F^2(\mathbf{u},\mathbf{v}) \geq \frac{2^{n+m}\left(3\cdot 2^{2n} - 2\cdot 2^n\right) - 2^{4n}}{2^{2n}(2^m-1)} = 3\cdot 2^n - 2 - 2\cdot\frac{(2^n-1)(2^{n-1}-1)}{2^m-1},$$

which completes the proof. □

Remark 3.16. *As noted in [20], the condition $m \geq n-1$ is assumed in Theorem 3.15 to make the expression under the square root non-negative. For $m = n-1$ it coincides with the universal bound and for $m > n$ the square-root cannot be an integer (see [24]). In case $m = n$, functions reaching this bound with equality are of great importance and we define them as follows.*

Definition 3.17. *The (n,n)-functions F which achieve the bound of Theorem 3.15 with equality, that is, $\mathcal{N}_F = 2^{n-1} - 2^{\frac{n-1}{2}}$ (n odd), are called **almost bent**.*

Equivalently, we can define almost bent (AB) functions as follows.

Definition 3.18. *An (n,n)-function F, n odd, is **almost bent** if $W_F(\mathbf{u},\mathbf{v})$ equals 0 or $\pm 2^{\frac{n+1}{2}}$ for all $\mathbf{u}\in\mathbb{F}_2^n$ and $\mathbf{v}\in\mathbb{F}_2^{n*}$.*

For an (n,n)-function F and any elements $\mathbf{a},\mathbf{b} \in \mathbb{F}_2^n$ we denote by $\delta_F(\mathbf{a},\mathbf{b})$ the number of solutions of the equation $F(\mathbf{x}\oplus\mathbf{a}) \oplus F(\mathbf{x}) = \mathbf{b}$, that is,

$$\delta_F(\mathbf{a},\mathbf{b}) = |\{\mathbf{x} \in \mathbb{F}_2^n : F(\mathbf{x}\oplus\mathbf{a}) \oplus F(\mathbf{x}) = \mathbf{b}\}|,$$

where $D_{\mathbf{a}}F(\mathbf{x}) = F(\mathbf{x}\oplus\mathbf{a}) \oplus F(\mathbf{x})$ is the *derivative* of F in $\mathbf{a}$ and we call the set

$$\Delta_F = \{\delta_F(\mathbf{a},\mathbf{b}) : \mathbf{a},\mathbf{b} \in \mathbb{F}_2^n, \mathbf{a} \neq \mathbf{0}\}$$

the *difference spectrum* or *difference distribution table* of the function F. For any (n,n)-function F its differential uniformity $\delta_F = \max \Delta_F$ is not less than 2. Functions with the smallest possible differential uniformity contribute an optimal resistance to the differential attack. This leads to the following definition.

Definition 3.19. *A (n,n)-function F is called* ***almost perfect non-linear*** *(APN) if $\delta_F = 2$, that is, $\Delta_F = \{0,2\}$.*

Now we will characterise AB and APN functions in terms of some Boolean function γ_F associated to the (n,n)-function F. With $\delta_{\mathbf{0}}(\mathbf{a},\mathbf{b})$ we denote the Dirac symbol at $(\mathbf{a},\mathbf{b})$, whose value is 1 if $\mathbf{a} = \mathbf{b} = \mathbf{0}$ and 0 otherwise.

Definition 3.20. *For any (n,n)-function F, we denote by γ_F the Boolean function on $\mathbb{F}_2^n \times \mathbb{F}_2^n$ whose value at $(\mathbf{a},\mathbf{b})$ is 1 if $\mathbf{a} \neq \mathbf{0}$ and $\delta_F(\mathbf{a},\mathbf{b}) \neq 0$, and 0 otherwise.*

Lemma 3.21. *Let F be a (n,n)-function. Then*

$$\sum_{\mathbf{a}\in{\mathbb{F}_2^n}^*,\ \mathbf{b}\in\mathbb{F}_2^n} \delta_F(\mathbf{a},\mathbf{b}) = 2^{2n} - 2^n.$$

Proof. Let us fix $\mathbf{a} \in \mathbb{F}_2^n$ and we consider the sum $\sum_{\mathbf{b}\in\mathbb{F}_2^n} \delta_F(\mathbf{a},\mathbf{b})$. Let us denote the elements $\mathbf{b} \in \mathbb{F}_2^n$ with $\mathbf{b}_0, \mathbf{b}_1, \ldots, \mathbf{b}_{2^n-1}$. For every i the equation $F(\mathbf{x}\oplus\mathbf{a}) \oplus F(\mathbf{x}) = \mathbf{b}_i$ will have k_i solutions, $0 \leq i \leq 2^n - 1$. Since no $\mathbf{x}$ can be a solution to both $F(\mathbf{x}\oplus\mathbf{a}) \oplus F(\mathbf{x}) = \mathbf{b}_i$ and $F(\mathbf{x}\oplus\mathbf{a}) \oplus F(\mathbf{x}) = \mathbf{b}_j$, $i \neq j$, we conclude that $k_0 + \ldots + k_{2^n-1} = 2^n$. Thus,

$$\sum_{\mathbf{a},\mathbf{b}\in\mathbb{F}_2^n} \delta_F(\mathbf{a},\mathbf{b}) = \sum_{\mathbf{a}\in\mathbb{F}_2^n} 2^n = 2^{2n}.$$

Let $\mathbf{a} = \mathbf{0}$. Then

$$\delta_F(\mathbf{0},\mathbf{b}) = \begin{cases} 2^n, & \mathbf{b} = \mathbf{0} \\ 0, & \textit{otherwise} \end{cases}.$$

We conclude,

$$\sum_{\mathbf{a}\in{\mathbb{F}_2^n}^*,\mathbf{b}\in\mathbb{F}_2^n} \delta_F(\mathbf{a},\mathbf{b}) = \sum_{\mathbf{a},\mathbf{b}\in\mathbb{F}_2^n} \delta_F(\mathbf{a},\mathbf{b}) - \sum_{\mathbf{b}\in\mathbb{F}_2^n} \delta_F(\mathbf{0},\mathbf{b}) = 2^{2n} - 2^n.$$

$\square$

The definition of APN and AB functions can easily be reformulated in terms of number of solutions of a certain system of equations.

Lemma 3.22. *A function F is APN if and only if the system of equations*

$$\begin{cases} \mathbf{x} \oplus \mathbf{y} = \mathbf{a} \\ F(\mathbf{x}) \oplus F(\mathbf{y}) = \mathbf{b} \end{cases} \tag{3.6}$$

has zero or two solutions $(\mathbf{x}, \mathbf{y})$ for every $(\mathbf{a}, \mathbf{b}) \neq (\mathbf{0}, \mathbf{0})$.

Proof. $(\Rightarrow)$ Assume F is APN. Let's denote the set

$$H_{\mathbf{a}}(F) = \{F(\mathbf{x}) \oplus F(\mathbf{x} \oplus \mathbf{a}) : \mathbf{x} \in \mathbb{F}_2^n\}, \quad \mathbf{a} \in \mathbb{F}_2^n, \ \mathbf{a} \neq \mathbf{0}.$$

Then, since F is APN, $|H_{\mathbf{a}}(F)| = 2^{n-1}$. If $\mathbf{x}$ is a solution of the equation $F(\mathbf{x}) \oplus F(\mathbf{x} \oplus \mathbf{a}) = \mathbf{b}$, then $\mathbf{y} = \mathbf{x} \oplus \mathbf{a}$ is also a solution because $F(\mathbf{y}) \oplus F(\mathbf{y} \oplus \mathbf{a}) = F(\mathbf{x} \oplus \mathbf{a}) \oplus F(\mathbf{x}) = \mathbf{b}$. Furthermore, $\mathbf{x} \oplus \mathbf{y} = \mathbf{a}$ and $F(\mathbf{x}) \oplus F(\mathbf{y}) = \mathbf{b}$, that is, $(\mathbf{x}, \mathbf{y})$ is a solution of the system (3.6). By interchanging $\mathbf{x}$ and $\mathbf{y}$, we get that $(\mathbf{y}, \mathbf{x})$ is also a solution. Therefore, the system of equations can have 2 solutions, but since $|H_{\mathbf{a}}(F)| = 2^{n-1}$, the system cannot have more than 2 solutions. Thus, the system (3.6) has 0 or 2 solutions.
$(\Leftarrow)$ Assume that the system (3.6) has 0 or 2 solutions. Then, for all $\mathbf{b} \in \mathbb{F}_2^n$, either $F(\mathbf{x}) \oplus F(\mathbf{x} \oplus \mathbf{a}) = \mathbf{b}$ for two $\mathbf{x} \in \mathbb{F}_2^n$ or for no $\mathbf{x} \in \mathbb{F}_2^n$. Hence, $|H_{\mathbf{a}}(F)| \leq \frac{1}{2}|\mathbb{F}_2^n| = 2^{n-1}$. But, $\mathbf{b} \in \mathbb{F}_2^n$ and $F(\mathbf{x}) \oplus F(\mathbf{x} \oplus \mathbf{a}) = \mathbf{b}$. Thus, $|H_{\mathbf{a}}(F)| \geq \frac{1}{2}|\mathbb{F}_2^n| = 2^{n-1}$. Hence, $|H_{\mathbf{a}}(F)| = 2^{n-1}$, that is, F is APN. □

Theorem 3.23. *[21] A function F is AB if and only if for every $\mathbf{a}, \mathbf{b} \in \mathbb{F}_2^n$ the system of equations*

$$\begin{cases} \mathbf{x} \oplus \mathbf{y} \oplus \mathbf{z} = \mathbf{a} \\ F(\mathbf{x}) \oplus F(\mathbf{y}) \oplus F(\mathbf{z}) = \mathbf{b} \end{cases} \tag{3.7}$$

has $3 \cdot 2^n - 2$ solutions $(\mathbf{x}, \mathbf{y}, \mathbf{z})$, if $\mathbf{b} = F(\mathbf{a})$, and $2^n - 2$ otherwise.

Lemma 3.24. *Every AB function is APN.*

Proof. Assume that F is not APN. This implies that for some $0 \neq \mathbf{q} \in \mathbb{F}_2^n, \mathbf{b} \in \mathbb{F}_2^n$, the equation $F(\mathbf{x}) \oplus F(\mathbf{x} \oplus \mathbf{q}) = \mathbf{b}$ aside from the solutions $\mathbf{x} = \mathbf{a}$ and $\mathbf{x} = \mathbf{a} \oplus \mathbf{q}$, has another solution $\mathbf{x} = \mathbf{p}$. Thus, the equality $F(\mathbf{p}) \oplus F(\mathbf{p} \oplus \mathbf{q}) = F(\mathbf{a}) \oplus F(\mathbf{a} \oplus \mathbf{q})$ holds and the system (3.7) in addition to the "trivial" solutions has the solution $(\mathbf{x}, \mathbf{y}, \mathbf{z}) = (\mathbf{p}, \mathbf{p} \oplus \mathbf{q}, \mathbf{a} \oplus \mathbf{q})$. The system has $3 \cdot 2^n - 2$ "trivial" solutions with one variable equal to a and the other two variables equal to each other. (Since $\mathbf{a}$ is fixed, there are $2^n - 1$ solutions of the form $(\mathbf{a}, \mathbf{c}, \mathbf{c})$ and three possible ways in which $\mathbf{a}, \mathbf{c}, \mathbf{c}$ can be rearranged yielding $3 \cdot 2^n - 3$ solutions plus the solution $(\mathbf{a}, \mathbf{a}, \mathbf{a})$, for a total of $3 \cdot 2^n - 2$ "trivial" solutions.) Hence, according to Theorem 3.23, F is not AB. □

The converse is false, in general. But, if F aside from the APNess satisfies some additional properties it will also be AB.

Proposition 3.25. *Let F be an APN (n,n)-function, n odd. Then, F is AB if and only if for every $\mathbf{u},\mathbf{v} \in \mathbb{F}_2^n$, $\mathbf{v} \neq \mathbf{0}$, the Walsh coefficients $W_F(\mathbf{u},\mathbf{v})$ are divisible by $2^{\frac{n+1}{2}}$.*

Proof. Obviously, the condition is necessary.
Let us assume that F is APN and all the Walsh coefficients $W_F(\mathbf{u},\mathbf{v})$ are divisible by $2^{\frac{n+1}{2}}$. This means that, $W_F^2(\mathbf{u},\mathbf{v}) = 2^{n+1}\lambda_{\mathbf{uv}}$, where $\lambda_{\mathbf{uv}}$ are integers. Chabaud and Vaudenay [24] have proved that an (n,n)-function F is APN if and only if

$$\sum_{\mathbf{u},\mathbf{v}\in\mathbb{F}_2^n,\mathbf{v}\neq\mathbf{0}} W_F^4(\mathbf{u},\mathbf{v}) = 2^{3n+1}(2^n-1).$$

From (3.1), we have that

$$2^{n+1}\sum_{\mathbf{u},\mathbf{v}\in\mathbb{F}_2^n,\mathbf{v}\neq\mathbf{0}} W_F^2(\mathbf{u},\mathbf{v}) = 2^{n+1}2^{2n}(2^n-1) = 2^{3n+1}(2^n-1).$$

This implies that F is APN if and only if

$$\sum_{\mathbf{u},\mathbf{v}\in\mathbb{F}_2^n,\mathbf{v}\neq\mathbf{0}} \left(W_F^4(\mathbf{u},\mathbf{v}) - 2^{n+1}W_F^2(\mathbf{u},\mathbf{v})\right) = 0.$$

Thus,

$$\begin{aligned} 0 &= \sum_{\mathbf{u},\mathbf{v}\in\mathbb{F}_2^n,\mathbf{v}\neq\mathbf{0}} \left(W_F^4(\mathbf{u},\mathbf{v}) - 2^{n+1}W_F^2(\mathbf{u},\mathbf{v})\right) \\ &= \sum_{\mathbf{u},\mathbf{v}\in\mathbb{F}_2^n,\mathbf{v}\neq\mathbf{0}} \left(2^{2n+2}\lambda_{\mathbf{uv}}^2 - 2^{n+1}\cdot 2^{n+1}\lambda_{\mathbf{uv}}\right) \\ &= 2^{2n+2}\sum_{\mathbf{u},\mathbf{v}\in\mathbb{F}_2^n,\mathbf{v}\neq\mathbf{0}} \left(\lambda_{\mathbf{uv}}^2 - \lambda_{\mathbf{uv}}\right). \end{aligned}$$

Because the difference $\lambda_{\mathbf{uv}}^2 - \lambda_{\mathbf{uv}}$ is nonegative and $\lambda_{\mathbf{uv}}$ are integers, we conclude that $\lambda_{\mathbf{uv}} \in \{0,1\}$. That is, $W_F(\mathbf{u},\mathbf{v}) \in \{0, \pm 2^{\frac{n+1}{2}}\}$, in other words, F is AB. □

Now we will present alternative definitions of APN and AB functions.

Proposition 3.26. *Let F be any (n,n)-function. Then,*

(i) F is APN if and only if $\mathrm{wt}(\gamma_F) = 2^{2n-1} - 2^{n-1}$;

(ii) F is AB if and only if γ_F is bent.

Proof. (i) From Definition 3.19, F is APN if and only if $\delta_F(\mathbf{a},\mathbf{b}) \in \{0,2\}$, for all $\mathbf{a} \in \mathbb{F}_2^{n*}, \mathbf{b} \in \mathbb{F}_2^n$. Thus, if we consider the sum of all $\delta_F(\mathbf{a},\mathbf{b})$, we may interpret this in terms of the function $\gamma_F(\mathbf{a},\mathbf{b})$ as follows. F is APN if and only if

$$\sum_{\mathbf{a}\in\mathbb{F}_2^{n*},\mathbf{b}\in\mathbb{F}_2^n} \delta_F(\mathbf{a},\mathbf{b}) = 2 \sum_{\mathbf{a}\in\mathbb{F}_2^{n*},\mathbf{b}\in\mathbb{F}_2^n} \gamma_F(\mathbf{a},\mathbf{b}).$$

Thus, by Lemma 3.21, F is APN if and only if

$$\sum_{\mathbf{a},\mathbf{b}\in\mathbb{F}_2^n} \gamma_F(\mathbf{a},\mathbf{b}) = 2^{2n-1} - 2^{n-1}.$$

(ii) From Lemma 3.24, without loss of generality, we may assume that F is APN. Moreover,

$$\delta_F(\mathbf{a},\mathbf{b}) = 2^n\delta_0(\mathbf{a},\mathbf{b}) + 2\gamma_F(\mathbf{a},\mathbf{b}).$$

Since γ_F is Boolean, we have

$$(-1)^{\gamma_F(\mathbf{a},\mathbf{b})} = 1 - 2\gamma_F(\mathbf{a},\mathbf{b}).$$

Thus,

$$(-1)^{\gamma_F(\mathbf{a},\mathbf{b})} = 1 - \delta_F(\mathbf{a},\mathbf{b}) + 2^n\delta_{\mathbf{0}}(\mathbf{a},\mathbf{b}).$$

Let us compute the Walsh-Hadamard transform of γ_F.

$$\begin{aligned} W_{\gamma_F}(\mathbf{u},\mathbf{v}) &= \sum_{\mathbf{a},\mathbf{b}\in\mathbb{F}_2^n} (-1)^{\gamma_F(\mathbf{a},\mathbf{b})\oplus\mathbf{a}\cdot\mathbf{u}\oplus\mathbf{b}\cdot\mathbf{v}} = \sum_{\mathbf{a},\mathbf{b}\in\mathbb{F}_2^n} \left(1 - \delta_F(\mathbf{a},\mathbf{b}) + 2^n\delta_0(\mathbf{a},\mathbf{b})\right)(-1)^{\mathbf{a}\cdot\mathbf{u}\oplus\mathbf{b}\cdot\mathbf{v}} \\ &= \sum_{\mathbf{a},\mathbf{b}\in\mathbb{F}_2^n} (-1)^{\mathbf{a}\cdot\mathbf{u}\oplus\mathbf{b}\cdot\mathbf{v}} + 2^n \sum_{\mathbf{a},\mathbf{b}\in\mathbb{F}_2^n} \delta_0(\mathbf{a},\mathbf{b})(-1)^{\mathbf{a}\cdot\mathbf{u}\oplus\mathbf{b}\cdot\mathbf{v}} - \sum_{\mathbf{a},\mathbf{b}\in\mathbb{F}_2^n} \delta_F(\mathbf{a},\mathbf{b})(-1)^{\mathbf{a}\cdot\mathbf{u}\oplus\mathbf{b}\cdot\mathbf{v}} \\ &= 2^{2n}\delta_0(\mathbf{u},\mathbf{v}) + 2^n - \hat{\delta_F}(\mathbf{u},\mathbf{v}) \end{aligned}$$

Since $\hat{\delta_F}(\mathbf{u},\mathbf{v}) = W_F^2(\mathbf{u},\mathbf{v})$ (see [24]), where $\hat{\delta}$ is the Fourier transform of δ (Remark 2.20), we have that

$$W_{\gamma_F}(\mathbf{u},\mathbf{v}) = 2^{2n}\delta_0(\mathbf{u},\mathbf{v}) + 2^n - W_F^2(\mathbf{u},\mathbf{v}). \tag{3.8}$$

We deduce that γ_F is bent if and only if, for any $(\mathbf{u},\mathbf{v}) \neq (\mathbf{0},\mathbf{0})$, $W_F^2(\mathbf{u},\mathbf{v})$ is equal to 0 or 2^{n+1}, that is if F is AB. □

We say that some function ϕ_E is the *indicator* of a set E if it is defined in the following way: $\phi_E(x) = 1$ if $x \in E$, and $\phi_E(x) = 0$, otherwise. We now have the following corollary.

Corollary 3.27. *If F is AB, then the dual of γ_F is the indicator of the Walsh support of F, deprived of $(\mathbf{0},\mathbf{0})$.*

Proof. Since F is AB, from Proposition 3.26, we have that γ_F is bent. Let $(\mathbf{u},\mathbf{v}) \neq (\mathbf{0},\mathbf{0})$, then

$$\begin{aligned}\tilde{\gamma_F}(\mathbf{u},\mathbf{v}) = 0 &\Leftrightarrow 2^{-n}W_{\gamma_F}(\mathbf{u},\mathbf{v}) = 1\\ &\Leftrightarrow W_{\gamma_F}(\mathbf{u},\mathbf{v}) = 2^n\\ &\overset{(3.8)}{\Leftrightarrow} 2^{2n}\delta_0(\mathbf{u},\mathbf{v}) - W_F^2(\mathbf{u},\mathbf{v}) = 0\\ &\Leftrightarrow W_F^2(\mathbf{u},\mathbf{v}) = 0\\ &\Leftrightarrow W_F(\mathbf{u},\mathbf{v}) = 0\\ &\Leftrightarrow (\mathbf{u},\mathbf{v}) \notin S_F\end{aligned}$$

Hence, $\tilde{\gamma_F}$ is the indicator of the Walsh support of F, deprived of $(\mathbf{0},\mathbf{0})$. □

Example 3.28. *Let us check whether the function $F(x) = x^3$ over $\mathbb{F}_{2^3}$ is APN and AB. To check if it is APN, we need its difference distribution table (DDT), that is, we need to compute*

$$\delta_F(\mathbf{a},\mathbf{b}) = |\{\mathbf{x} \in \mathbb{F}_2^n : F(\mathbf{x}) \oplus F(\mathbf{x} \oplus \mathbf{a}) = \mathbf{b}\}|,$$

for all $\mathbf{a} \in \mathbb{F}_2^{3^*}$, $\mathbf{b} \in \mathbb{F}_2^3$. Here the function F is given in vectorial form as computed in Example 3.9. The DDT is given in Table 4.

$\delta_F(\mathbf{a},\mathbf{b})$	$(0,0,0)$	$(0,0,1)$	$(0,1,0)$	$(0,1,1)$	$(1,0,0)$	$(1,0,1)$	$(1,1,0)$	$(1,1,1)$
$(0,0,1)$	2	0	0	2	0	2	2	0
$(0,1,0)$	0	2	0	2	2	2	0	0
$(0,1,1)$	0	2	2	2	0	0	2	0
$(1,0,0)$	2	2	0	0	2	0	2	0
$(1,0,1)$	0	0	2	0	2	2	2	0
$(1,1,0)$	2	0	2	2	2	0	0	0
$(1,1,1)$	2	2	2	0	0	2	0	0

Table 4: Difference distribution table of $F(x) = x^3$ over $\mathbb{F}_{2^3}$

Since $\Delta_F = \{0,2\}$, we conclude that the function F is indeed APN. To see if F is AB, we will use Proposition 3.26. That is, we need to compute the Boolean function γ_F, as defined in Definition 3.20, and see if it is bent. The values of γ_F are given in Table 5. Let us compute the Walsh spectra of γ_F. We notice that γ_F is a Boolean function on $\mathbb{F}_2^6$. If $\mathbf{a} = (a_0,a_1,a_2)$ and $\mathbf{b} = (b_0,b_1,b_2)$, we have that $\mathbf{c} = (a_0,a_1,a_2,b_0,b_1,b_2)$. With respect to lexicographical ordering, the truth table of γ_F is

$$T_{\gamma_F} = (0,0,0,0,0,0,0,0,0,1,0,1,0,1,0,1,0,0,1,1,0,0,1,1,0,1,1,0,0,1,1,0,$$
$$0,0,1,1,1,1,0,0,0,1,1,0,1,0,0,1,0,0,0,0,1,1,1,1,0,1,0,1,1,0,1,0).$$

$\gamma_F(\mathbf{a},\mathbf{b})$	$(0,0,0)$	$(0,0,1)$	$(0,1,0)$	$(0,1,1)$	$(1,0,0)$	$(1,0,1)$	$(1,1,0)$	$(1,1,1)$
$(0,0,0)$	0	0	0	0	0	0	0	0
$(0,0,1)$	1	0	0	1	0	1	1	0
$(0,1,0)$	0	1	0	1	1	1	0	0
$(0,1,1)$	0	1	1	1	0	0	1	0
$(1,0,0)$	1	1	0	0	1	0	1	0
$(1,0,1)$	0	0	1	0	1	1	1	0
$(1,1,0)$	1	0	1	1	1	0	0	0
$(1,1,1)$	1	1	1	0	0	1	0	0

Table 5: Values of $\gamma_F(\mathbf{a},\mathbf{b})$ for all $(\mathbf{a},\mathbf{b}) \in \mathbb{F}_2^3 \times \mathbb{F}_2^3$

Now, the corresponding Walsh spectra is

$$\begin{aligned} S_{\gamma_F} =&(8,8,8,8,8,8,8,8,8,-8,8,-8,8,-8,8,-8,8,8,-8,-8,-8,-8,8\\ &8,8,-8,-8,8,-8,8,8,-8,8,8,8,8,-8,-8,-8,-8,8,-8,8,-8,\\ &-8,8,-8,8,8,8,-8,-8,8,8,-8,-8,8,-8,-8,8,8,-8,-8,8) \end{aligned}$$

and we can conclude that γ_F is indeed bent, that is, F is AB.

Remark 3.29. *One can see that computing the function γ_F from an AB function F is pretty straightforward. However, if we have a bent function with $2n$ variables, we know that it is an indicator of some AB function with n variables. Determining that function is not trivial and finding an algorithm remains an open problem.*

APN functions can also be characterized in terms of affine subspaces. Let A and B be affine subspaces over $\mathbb{F}_2$ and $F : A \to B$ an affine mapping defined by $F(\mathbf{x}) = \mathbf{u}\cdot\mathbf{x} \oplus \mathbf{v}$. Let $\mathbf{x} = \mathbf{a}_0 \oplus \mathbf{a}_1 \oplus \mathbf{a}_2$, where $\mathbf{a}_0, \mathbf{a}_1, \mathbf{a}_2 \in A$ are arbitrary. We observe that

$$\begin{aligned} F(\mathbf{a}_0 \oplus \mathbf{a}_1 \oplus \mathbf{a}_2) &= \mathbf{u}\cdot(\mathbf{a}_0 \oplus \mathbf{a}_1 \oplus \mathbf{a}_2) \oplus \mathbf{v} = \mathbf{u}\cdot\mathbf{a}_0 \oplus \mathbf{u}\cdot\mathbf{a}_1 \oplus \mathbf{u}\cdot\mathbf{a}_2 \oplus \mathbf{v} \oplus \mathbf{0}\\ &= \mathbf{u}\cdot\mathbf{a}_0 \oplus \mathbf{u}\cdot\mathbf{a}_1 \oplus \mathbf{u}\cdot\mathbf{a}_2 \oplus \mathbf{v} \oplus (\mathbf{v} \oplus \mathbf{v})\\ &= F(\mathbf{a}_0) \oplus F(\mathbf{a}_1) \oplus F(\mathbf{a}_2), \end{aligned}$$

in other words, F is affine if and only if $F(\mathbf{a}_0 \oplus \mathbf{a}_1 \oplus \mathbf{a}_2) = F(\mathbf{a}_0) \oplus F(\mathbf{a}_1) \oplus F(\mathbf{a}_2)$, for all $\mathbf{a}_0, \mathbf{a}_1, \mathbf{a}_2 \in A$.

Proposition 3.30. *[35] Let F be an (n,n)-function. Then F is APN if and only if F is not affine on any 2-dimensional affine subspace of $\mathbb{F}_2^n$.*

Proof. Assume that F is affine on a 2-dimensional subspace $A = \{\mathbf{a}_0, \mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_0 \oplus \mathbf{a}_1 \oplus \mathbf{a}_2\} \subset \mathbb{F}_2^n$ and let $F(\mathbf{a}_i) = \mathbf{b}_i$, $0 \leq i \leq 2$. Then $F(\mathbf{a}_0 \oplus \mathbf{a}_1 \oplus \mathbf{a}_2) = \mathbf{b}_0 \oplus \mathbf{b}_1 \oplus \mathbf{b}_2$. It follows that

$$F(\mathbf{x} \oplus \mathbf{a}_0 \oplus \mathbf{a}_1) \oplus F(\mathbf{x}) = \mathbf{b}_0 \oplus \mathbf{b}_1,$$

for all $\mathbf{x} \in A$. In other words, F is not APN.
On the other hand, assume that for some $\mathbf{a} \in \mathbb{F}_2^{n^*}$, there exist distinct elements $\mathbf{x}_0, \mathbf{x}_1, \mathbf{x}_2 \in \mathbb{F}_2^n$ such that $F(\mathbf{x}_i \oplus \mathbf{a}) \oplus F(\mathbf{x}_i) = F(\mathbf{x}_j \oplus \mathbf{a}) \oplus F(\mathbf{x}_j), \quad 0 \leq i, j \leq 2$. We note that $\mathbf{x}_0 \oplus \mathbf{x}_1 \neq \mathbf{a}$ or $\mathbf{x}_0 \oplus \mathbf{x}_2 \neq \mathbf{a}$ because otherwise

$$\mathbf{x}_0 \oplus \mathbf{x}_1 \oplus \mathbf{x}_0 \oplus \mathbf{x}_2 = \mathbf{a} \oplus \mathbf{a} = \mathbf{0} \Rightarrow \mathbf{x}_1 \oplus \mathbf{x}_2 = \mathbf{0} \Rightarrow \mathbf{x}_1 = \mathbf{x}_2,$$

which is impossible. Thus, without loss of generality, let us assume that $\mathbf{x}_0 \oplus \mathbf{x}_1 \neq \mathbf{a}$. $A = \{\mathbf{x}_0, \mathbf{x}_1, \mathbf{x}_0 \oplus \mathbf{a}, \mathbf{x}_1 \oplus \mathbf{a}\}$ is a 2-dimensional affine subspace of $\mathbb{F}_2^n$. It can be easily checked that $F(\mathbf{a}_0 \oplus \mathbf{a}_1 \oplus \mathbf{a}_2) = F(\mathbf{a}_0) \oplus F(\mathbf{a}_1) \oplus F(\mathbf{a}_2)$. In other words, F is affine on A. □

One can also relate APN and AB functions with codes. We will not talk about linear codes in general. For our purpose, codes are just linear subspaces of $\mathbb{F}_2^v$ (for more detail on codes we refer to [52]). We give some preliminary definitions on codes as seen in [48].

Definition 3.31. *Let F be an (n, n)-function with $F(\mathbf{0}) = \mathbf{0}$. We define the $2n \times (2^n - 1)$* ***parity-check matrix***

$$H_F := \begin{bmatrix} \alpha^0 & \alpha^1 & \dots & \alpha^{2^n-2} \\ F(\alpha^0) & F(\alpha^1) & \dots & F\left(\alpha^{2^n-2}\right) \end{bmatrix}$$

where α is a primitive element in $\mathbb{F}_{2^n}$. The finite field elements are interpreted as elements in $\mathbb{F}_2^n$. By $\mathcal{C}_F$, we denote the **code** *with parity check matrix H_F, that means*

$$\mathcal{C}_F = \{\mathbf{v} \in \mathbb{F}_2^{2^n-1} : \mathbf{v} \cdot H_F^T = \mathbf{0}\}.$$

The row space of H_F,that is, the set of all linear combinations of the rows of H_F, is the ***dual code*** *of $\mathcal{C}_F$, denoted by $\mathcal{C}_F^{\perp}$.*

Definition 3.32. *The* ***weight*** *of a codeword (an element in the code) is the number of its entries different from 0, and the* ***minimum weight*** *of a code is the minimum weight of all nonzero codewords.*

Remark 3.33. *The minimum distance d of a linear code $\mathcal{C}$ equals its minimum weight w.*

Proposition 3.34. *[20, 21] Let F be any (n, n)-function such that $F(\mathbf{0}) = \mathbf{0}$. Let $\mathcal{C}_F$ be the linear code admitting H_F for parity-check matrix. Then:*

(i) F is APN if and only if $\mathcal{C}_F$ has minimum distance 5;

(ii) F is AB if and only if the nonzero weights of $\mathcal{C}_F^{\perp}$ are $2^{n-1} - 2^{\frac{n-1}{2}}$, 2^{n-1} and $2^{n-1} + 2^{\frac{n-1}{2}}$.

Proof. Since H_F contains no zero column, $\mathcal{C}_F$ has no codeword of weight 1 and since all columns of H_F are linearly independent, $\mathcal{C}_F$ has no codeword of weight 2. Hence, $\mathcal{C}_F$ has minimum distance at least 3. The minimum distance is also at most 5 (this is known, see [21]), that is, $3 \leq d \leq 5$.

(*i*) Let $\mathbf{c} = (c_0, c_1, \ldots, c_{2^n-2}) \in \mathbb{F}_2^{2^n-1}$. By Definition 3.31, $\mathbf{c}$ belongs to $\mathcal{C}_F$ if and only if

$$\sum_{i=0}^{2^n-2} c_i \alpha^i = 0 \quad \text{and} \quad \sum_{i=0}^{2^n-2} c_i F(\alpha^i) = 0. \tag{3.9}$$

From (3.9), $\mathcal{C}_F$ has minimum weight 3 or 4 if there exist distinct elements $x, y, x', y' \in \mathbb{F}_{2^n}^*$ such that

$$x + y + x' + y' = 0 \quad \text{and} \quad F(x) + F(y) + F(x') + F(y') = 0. \tag{3.10}$$

One can see that relation (3.10) is equivalent to the definition of a 2-dimensional affine subspace. The minimum weight is 3, if one of these elements is 0; otherwise, it is 4. Suppose there exist two pairs (x, y) and (x', y'), where $x, y, x', y' \in \mathbb{F}_{2^n}^*$, which satisfy the system (3.6) (in terms of finite fields). The existence of such four elements, for some $a, b \in \mathbb{F}_{2^n}^*$, is equivalent to the existence of four elements satisfying (3.10). If (x, y) is a solution of an APN function, the other solution is of the form (y, x) (as seen in Lemma 3.22). Thus, F is APN if and only $\mathcal{C}_F$ has minimum distance $d \geq 5$. But, since $d \leq 5$, we have $d = 5$.

(*ii*) All codewords of the dual code $\mathcal{C}_F^\perp$ correspond some linear combination of the rows of H_F. Let us consider the elements of $\mathbb{F}_2^n$ as binary vectors and define $\psi(\mathbf{x}) = \mathbf{a} \cdot \mathbf{x} \oplus \mathbf{b} \cdot F(\mathbf{x})$. The vector $\mathbf{c_{ab}} = (\psi(\mathbf{x}) : \mathbf{x} \in \mathbb{F}_2^{n^*})$ is actually a linear combination of the rows of H_F for some $\mathbf{a}, \mathbf{b} \in \mathbb{F}_2^n$. Hence, $\mathcal{C}_F^\perp = \{\mathbf{c_{ab}} : \mathbf{a}, \mathbf{b} \in \mathbb{F}_2^n\}$. The numbers

$$w_{\mathbf{ab}} = |\{\mathbf{x} \in \mathbb{F}_2^n : \psi(\mathbf{x}) = 1\}| = \mathrm{wt}(\psi) \overset{(2.6)}{=} 2^{n-1} - \frac{1}{2} W_F(\mathbf{a}, \mathbf{b})$$

are the weights of the codewords $\mathbf{c_{ab}}$. We note the following:

- $W_F(\mathbf{a}, \mathbf{b}) = 0 \Leftrightarrow w_{\mathbf{ab}} = 2^{n-1}$
- $W_F(\mathbf{a}, \mathbf{b}) = \pm 2^{\frac{n+1}{2}} \Leftrightarrow w_{\mathbf{a},\mathbf{b}} = 2^{n-1} \mp 2^{\frac{n-1}{2}}$

Thus, F is *AB* if and only if the nonzero weights of the dual $\mathcal{C}_F^\perp$ are $2^{n-1}, 2^{n-1} \pm 2^{\frac{n-1}{2}}$.

□

The Walsh spectrum of a Boolean function and its derivatives are related by the so-called *sum-of-square indicator*, introduced in [55], and defined as follows.

Definition 3.35. *[1] Let f be a Boolean function defined on $\mathbb{F}_2^n$. The sum-of-square indicator of f is defined by:*

$$\nu(f) = \sum_{\mathbf{a}\in\mathbb{F}_2^n} \mathcal{F}^2(D_{\mathbf{a}}f), \tag{3.11}$$

where $\mathcal{F}(f) := W_f(\mathbf{0})$.

The next lemma gives a connection between the Walsh coefficients and the derivatives of a Boolean function f.

Lemma 3.36. *[19] Let f be a Boolean function on $\mathbb{F}_2^n$. Then, for any $\mathbf{u} \in \mathbb{F}_2^n$, we have:*

$$W_f^2(\mathbf{u}) = \sum_{\mathbf{a}\in\mathbb{F}_2^n} (-1)^{\mathbf{u}\cdot\mathbf{a}} \mathcal{F}(D_{\mathbf{a}}f). \tag{3.12}$$

Proof.

$$\begin{aligned} W_f^2(\mathbf{u}) &= \left(\sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}}\right)^2 = \left(\sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}}\right) \cdot \left(\sum_{\mathbf{y}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{y})\oplus\mathbf{u}\cdot\mathbf{y}}\right) \\ &= \sum_{\mathbf{x},\mathbf{y}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})\oplus f(\mathbf{y})\oplus\mathbf{u}\cdot(\mathbf{x}\oplus\mathbf{y})} = \sum_{\mathbf{x},\mathbf{a}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})\oplus f(\mathbf{x}\oplus\mathbf{a})\oplus\mathbf{u}\cdot\mathbf{a}} \\ &= \sum_{\mathbf{a}\in\mathbb{F}_2^n} (-1)^{\mathbf{u}\cdot\mathbf{a}} \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{D_{\mathbf{a}}f(\mathbf{x})} = \sum_{\mathbf{a}\in\mathbb{F}_2^n} (-1)^{\mathbf{u}\cdot\mathbf{a}} \mathcal{F}(D_{\mathbf{a}}f) \end{aligned}$$

□

In terms of Walsh coefficients, the sum-of-square indicator is characterized as follows.

Proposition 3.37. *[56] Let f be a Boolean function defined on $\mathbb{F}_2^n$. Then*

$$\nu(f) = 2^{-n} \sum_{\mathbf{u}\in\mathbb{F}_2^n} W_f^4(\mathbf{u}). \tag{3.13}$$

Proof.

$$
\begin{aligned}
\sum_{\mathbf{u}\in\mathbb{F}_2^n} W_f^4(\mathbf{u}) &\overset{(3.12)}{=} \sum_{\mathbf{u}\in\mathbb{F}_2^n}\left(\sum_{\mathbf{a}\in\mathbb{F}_2^n}(-1)^{\mathbf{u}\cdot\mathbf{a}}\mathcal{F}(D_{\mathbf{a}}f)\right)^2 = \sum_{\mathbf{u}\in\mathbb{F}_2^n}\left(\sum_{\mathbf{a},\mathbf{b}\in\mathbb{F}_2^n}(-1)^{\mathbf{u}\cdot(\mathbf{a}\oplus\mathbf{b})}\mathcal{F}(D_{\mathbf{a}}f)\cdot\mathcal{F}(D_{\mathbf{b}}f)\right)\\
&= \sum_{\mathbf{u}\in\mathbb{F}_2^n}\left(\sum_{\mathbf{a},\mathbf{b},\mathbf{x},\mathbf{y}\in\mathbb{F}_2^n}(-1)^{f(\mathbf{x})\oplus f(\mathbf{x}\oplus\mathbf{a})\oplus f(\mathbf{y})\oplus f(\mathbf{y}\oplus\mathbf{b})\oplus\mathbf{u}\cdot(\mathbf{a}\oplus\mathbf{b})}\right)\\
&= \sum_{\mathbf{u}\in\mathbb{F}_2^n}\left(\sum_{\mathbf{a},\mathbf{b}\in\mathbb{F}_2^n}(-1)^{\mathbf{u}\cdot(\mathbf{a}\oplus\mathbf{b})}\sum_{\mathbf{x},\mathbf{y}\in\mathbb{F}_2^n}(-1)^{f(\mathbf{x})\oplus f(\mathbf{x}\oplus\mathbf{a})\oplus f(\mathbf{y})\oplus f(\mathbf{y}\oplus\mathbf{b})}\right)\\
&\overset{(2.4)}{=} \sum_{\mathbf{a}\in\mathbb{F}_2^n} 2^n \sum_{\mathbf{x},\mathbf{y}\in\mathbb{F}_2^n}(-1)^{f(\mathbf{x})\oplus f(\mathbf{x}\oplus\mathbf{a})\oplus f(\mathbf{y})\oplus f(\mathbf{y}\oplus\mathbf{a})}\\
&= 2^n\sum_{\mathbf{a}\in\mathbb{F}_2^n}\left(\sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{f(\mathbf{x})\oplus f(\mathbf{x}\oplus\mathbf{a})}\right)^2\\
&= 2^n\sum_{\mathbf{a}\in\mathbb{F}_2^n}\mathcal{F}^2(D_{\mathbf{a}}f) = 2^n\nu(f)
\end{aligned}
$$

□

The following theorem gives us a full characterization of APN functions by means of the derivatives of their component functions.

Theorem 3.38. *[1,46] Let F be an (n,n)-function and let $F_{\mathbf{v}} = \mathbf{v}\cdot F$, $\mathbf{v}\in{\mathbb{F}_2^n}^*$ denote its components. Then, for any $\mathbf{a}\in{\mathbb{F}_2^n}^*$:*

$$\sum_{\mathbf{v}\in{\mathbb{F}_2^n}^*}\mathcal{F}^2(D_{\mathbf{a}}F_{\mathbf{v}}) \geq 2^{n+1}\cdot(2^n-1). \tag{3.14}$$

Moreover, F is APN if and only if for all $\mathbf{a}\in{\mathbb{F}_2^n}^*$:

$$\sum_{\mathbf{v}\in{\mathbb{F}_2^n}^*}\mathcal{F}^2(D_{\mathbf{a}}F_{\mathbf{v}}) = 2^{n+1}\cdot(2^n-1) \tag{3.15}$$

Proof. Let $\mathbf{a}\in{\mathbb{F}_2^n}^*$ be arbitrary.

$$
\begin{aligned}
\sum_{\mathbf{v}\in{\mathbb{F}_2^n}^*}\mathcal{F}^2(D_{\mathbf{a}}F_{\mathbf{v}}) &= \sum_{\mathbf{v}\in{\mathbb{F}_2^n}^*}\left(\sum_{\mathbf{x},\mathbf{y}\in\mathbb{F}_2^n}(-1)^{\mathbf{v}\cdot(F(\mathbf{x})\oplus F(\mathbf{y})\oplus F(\mathbf{x}\oplus\mathbf{a})\oplus F(\mathbf{y}\oplus\mathbf{a}))}\right)\\
&\overset{for:sum-ux}{=} (2^n-1)\cdot\left|\left\{(\mathbf{x},\mathbf{y})\in(\mathbb{F}_2^n)^2 : F(\mathbf{x})\oplus F(\mathbf{x}\oplus\mathbf{a}) = F(\mathbf{y})\oplus F(\mathbf{y}\oplus\mathbf{a})\right\}\right|\\
&= (2^n-1)\cdot(|\{(\mathbf{x},\mathbf{x}):\mathbf{x}\in\mathbb{F}_2^n\}| + |\{(\mathbf{x},\mathbf{x}+\mathbf{a}):\mathbf{x}\in\mathbb{F}_2^n\}| +\\
&+ \underbrace{\left|\left\{(\mathbf{x},\mathbf{y})\in(\mathbb{F}_2^n)^2 : D_{\mathbf{a}}F(\mathbf{x}) = D_{\mathbf{a}}F(\mathbf{y}), \mathbf{x}\neq\mathbf{y}, \mathbf{y}\neq\mathbf{x}\oplus\mathbf{a}\right\}\right|}_{=\lambda})\\
&= (2^n-1)\cdot\left(2^{n+1}+\lambda\right)
\end{aligned}
$$

Obviously, $\lambda \geq 0$, confirming relation (3.14), and $\lambda = 0$ if and only if F is APN, confirming relation (3.15). □

Corollary 3.39. *Let F be an (n,n)-function with components $F_{\mathbf{v}}$, $\mathbf{v} \in \mathbb{F}_2^{n^*}$. Then,*

$$\sum_{\mathbf{v}\in\mathbb{F}_2^{n^*}} \nu(F_{\mathbf{v}}) \geq 2^{2n+1} \cdot (2^n - 1). \tag{3.16}$$

Moreover, F is APN if and only if

$$\sum_{\mathbf{v}\in\mathbb{F}_2^{n^*}} \nu(F_{\mathbf{v}}) = 2^{2n+1} \cdot (2^n - 1). \tag{3.17}$$

Consequently, if $\nu(F_{\mathbf{v}}) = 2^{2n+1}$ for all $\mathbf{v} \in \mathbb{F}_2^{n^*}$, then F is APN.

Proof. From Definition 3.11 we have $\nu(F_{\mathbf{v}}) = \sum_{\mathbf{a}\in\mathbb{F}_2^n} \mathcal{F}^2(D_{\mathbf{a}}F_{\mathbf{v}})$. Thus,

$$\sum_{\mathbf{v}\in\mathbb{F}_2^{n^*}} \nu(F_{\mathbf{v}}) = \sum_{\mathbf{v}\in\mathbb{F}_2^{n^*}} \sum_{\mathbf{a}\in\mathbb{F}_2^n} \mathcal{F}^2(D_{\mathbf{a}}F_{\mathbf{v}}) = \sum_{\mathbf{a}\in\mathbb{F}_2^n} \left(\sum_{\mathbf{v}\in\mathbb{F}_2^{n^*}} \mathcal{F}^2(D_{\mathbf{a}}F_{\mathbf{v}}) \right). \tag{3.18}$$

The relations (3.16) and (3.17) follow immediately from relations (3.14), (3.15) and (3.18). Moreover, the last statement is trivial to observe. □

One can easily check the APNess of a function if the Walsh spectrum is known. The following example shows a function which is APN, but not AB.

Example 3.40. *Let us consider the function $F(x) = x^{15}$ defined on $\mathbb{F}_{2^5}$. When computed, its Walsh coefficients are $0, \pm 4, \pm 8$ or 12, that is, F is not AB. But, for every $\mathbf{v} \in \mathbb{F}_2^{5^*}$ we have that*

$$\nu(F_{\mathbf{v}}) \overset{(3.13)}{=} 2^{-n} \sum_{\mathbf{u}\in\mathbb{F}_2^5} W_{F_{\mathbf{v}}}^4(\mathbf{u}) = 2^{11},$$

which by Corollary 3.39 means that F is APN.

Regarding the balancedness of AB and APN functions, we have the following.

Remark 3.41. *Let F be an AB (n,n)-function and let us denote with $F_i = \mathbf{v}_i \cdot F$, $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_{2^n-1} \in \mathbb{F}_2^{n^*}$ the component functions of F. With Ω_i we denote the Walsh support of F_i. From Parseval's relation (2.9) we have*

$$\sum_{\mathbf{u}\in\mathbb{F}_2^n} W_{F_i}^2(\mathbf{u}) = 2^{2n} \Leftrightarrow \sum_{\mathbf{u}\in\Omega_i} W_{F_i}^2(\mathbf{u}) = 2^{2n}$$

Since F is AB, we have that $W_{F_i}^2(\mathbf{u}) \in \{0, 2^{n+1}\}$. Hence,

$$\sum_{\mathbf{u}\in\Omega_i} W_{F_i}^2(\mathbf{u}) = \sum_{\mathbf{u}\in\Omega_i} 2^{n+1} = |\Omega_i| 2^{n+1},$$

that is, $|\Omega_i| = 2^{n-1}$. From Proposition 3.12 and Remark 3.13, we deduce that every AB function is a permutation. Moreover, because of Lemma 3.24, ***every APN (n,n)-function (n odd) is a permutation****.*

In the case of n even, the existence of APN permutations is still an important research area. If F is a permutation on $\mathbb{F}_{2^{2k}}$, then it is *not* APN, if one of the following conditions hold:

1. k is even and $F \in \mathbb{F}_{2^4}[x]$ [35];
2. F is a polynomial with coefficients in $\mathbb{F}_{2^k}$ [35];
3. F is a power function [20];
4. F is quadratic [46].

In [27] **the Big APN Problem** was formulated: Does there exist an APN permutation on $\mathbb{F}_{2^n}$ if n is even?
In 2009 the first example of an APN permutation on dimension six was presented by Dillon *et al.* in [8]. The function was constructed by finding a permutation in the CCZ-equivalence class of a certain quadratic APN function, namely the *Kim function* or κ *function* which is defined as

$$\kappa(x) = x^3 + x^{10} + \alpha x^{24},$$

where α is a primitive element of $\mathbb{F}_{2^6}$ whose minimal polynomial over $\mathbb{F}_2$ is $x^6 + x^4 + x^3 + x + 1$. The existence of APN function on dimension greater than six remains still open.
Although APN and AB functions are intensively studied, it is very hard to give complete descriptions of these classes. Checking the ABness or APNess of *power functions*, that is, functions over $\mathbb{F}_{2^n}$ of the form $F(x) = x^d$, is the easiest. Table 6 gives the list of all known APN and AB power functions up to EA-equivalence and inverse. Dobertin conjectured in [29] that this list is complete.
Also, there are eleven known infinite families of quadratic APN polynomials which are CCZ-inequivalent to power functions. They are listed in Table 7.
Complete classification over EA and CCZ-equivalence up to dimension 5 was obtained by M. Brinkmann and G. Leander in [7]. For $n = 6$ there are also known all 13 CCZ-inequivalent quadratic APN functions (found in [9], and proven in [31]). For $n = 7$ and $n = 8$, as shown in [53], there are, respectively, more than 470 and more than a thousand CCZ-inequivalent quadratic APN functions.
The functions listed in Table 6 have been intensively studied in the previous years, but some *open problem* still exist, as listed by C. Carlet in [20]:

1. Find classes of AB functions using CCZ-equivalence with Kasami (respectively, Welch, Niho) function.

Functions	Exponents d	Conditions	Degree	AB	Proven in
Gold	2^i+1	$\gcd(i,n)=1,\ 1\leq i\leq\frac{n-1}{2}$	2	for odd n	[32, 44]
Kasami	$2^{2i}-2^i+1$	$\gcd(i,n)=1,\ 1\leq i\leq\frac{n-1}{2}$	$i+1$	for odd n	[36, 37]
Welch	2^t+3	$n=2t+1$	3	yes	[30]
Niho	$2^t+2^{\frac{t}{2}}-1,\quad t$ even $2^t+2^{\frac{3t+1}{2}}-1,\quad t$ odd	$n=2t+1$	$t+1$ $\frac{t+1}{2}$	yes	[29, 34]
Inverse	$2^{2t}-1$	$n=2t+1$	$n-1$	no	[2, 44]
Dobbertin	$2^{4t}+2^{3t}+2^{2t}+2^t-1$	$n=5t$	$t+3$	no	[28]

Table 6: Known AB and APN power functions x^d defined on $\mathbb{F}_{2^n}$ up to EA-equivalence and inverse

Remark 3.42. *In [12] new classes of AB functions, which are by construction CCZ-equivalent to Gold functions, have been found.*

2. Find infinite classes of AB functions CCZ-equivalent to power functions and to quadratic functions.

3. Find classes of APN functions by using CCZ-equivalence with Kasami (respectively, Welch, Niho, Dobbertin, inverse) functions.

4. Classify APN functions, or at least their extended Walsh spectra, or at least their non-linearities.

Remark 3.43. *For n odd, as recalled by A. Canteaut in her "Habilitation à diriger des recherches", the APN functions can have three possible extended Walsh spectra:*

- *the spectrum of the AB functions which gives a non-linearity of* $2^{n-1}-2^{\frac{n-1}{2}}$,
- *the spectrum of the inverse function, which takes any value divisible by 4 in the interval* $\left(-2^{\frac{n}{2}+1}+1, 2^{\frac{n}{2}+1}+1\right)$ *and gives a non-linearity close to* $2^{n-1}-2^{\frac{n}{2}}$,
- *the spectrum of the Dobbertin function which is more complex (it is divisible by* $2^{\frac{n}{5}}$ *and not divisible by* $2^{\frac{2n}{5}+1}$*); its non-linearity seems to be bounded below by approximately* $2^{n-1}-2^{\frac{3n}{5}-1}-2^{\frac{2n}{5}-1}$ *– maybe equal, but this has yet to be proven (or disproven).*

For n even, the spectra may be more diverse:

	Function	Conditions	References
1-2	$x^{2^s}+1+\alpha^{2^k-1}x^{2^{ik}+2^{mk+s}}$	$n=pk,\ \gcd(k,p)=\gcd(s,pk)=1,\ p\in\{3,4\},\ i=sk \mod p,\ m=p-i,\ n\geq 12,\ \alpha$ primitive in $\mathbb{F}_{2^n}^*$	[13]
3	$x^{2^{2i}+2^i}+bx^{q+1}+cx^{q\left(2^{2i}+2^i\right)}$	$q=2^m,\ n=2m,\ \gcd(i,m)=1,\ \gcd(2^i+1,q+1)\neq 1,\ cb^q+b\neq 0,\ c\notin\{\lambda^{\left(2^i+1\right)(q-1)}:\lambda\in\mathbb{F}_{2^n}\},\ c^{q+1}=1$	[11]
4	$x\left(x^{2^i}+x^q+cx^{2^iq}\right)+x^{2^i}\left(c^qx^q+sx^{2^iq}\right)+x^{\left(2^i+1\right)q}$	$q=2^m,\ n=2m,\ \gcd(i,m)=1,\ x\in\mathbb{F}_{2^n},\ s\in\mathbb{F}_{2^n}\setminus\mathbb{F}_q,\ X^{2^i+1}+cX^{2^i}+x^qX+1$ is irreducible over $\mathbb{F}_{2^n}$	[11]
5	$x^3+a^{-1}Tr_1^n(a^3x^9)$	$a\neq 0$	[14,15]
6	$x^3+a^{-1}Tr_3^n(a^3x^9+a^6x^{18})$	$3\|n,\ a\neq 0$	[14]
7	$x^3+a^{-1}Tr_3^n(a^6x^{18}+a^{12}x^{36})$	$3\|n,\ a\neq 0$	[14]
8-10	$ux^{2^s+1}+u^{2^k}x^{2^{-k}+2^{k+s}}+vx^{2^{-k}+1}+wu^{2^k+1}x^{2^s+2^{k+s}}$	$n=3k,\ \gcd(k,3)=\gcd(s,3k)=1,\ v,w\in\mathbb{F}_{2^k},\ vw\neq 1,\ 3\|(k+s),\ u$ primitive in $\mathbb{F}_{2^n}^*$	[5]
11	$\alpha x^{2^s+1}+\alpha^{2^k}x^{2^{k+s}+2^k}+\beta x^{2^k+1}+\sum_{i=1}^{k-1}\gamma_i x^{2^{k+i}+2^i}$	$n=2k,\ \gcd(s,k)=1,\ s,k$ odd, $\beta\notin\mathbb{F}_{2^k},\ \gamma_i\in\mathbb{F}_{2^k},\ \alpha$ not a cube	[5,6]

Table 7: Known classes of quadratic APN polynomials CCZ-inequivalent to power functions on $\mathbb{F}_{2^n}$

- *the Gold functions whose component functions are bent for a third of them and have non-linearity $2^{n-1}-2^{\frac{n}{2}}$ for the rest of them; the Kasami functions which have the same extended spectra,*
- *the Dobbertin function (same observation as above),*
- *as soon as $n\geq 6$, we find (quadratic) functions with different spectra.*

5. The non-linearities of the known APN functions do not seem to be very week; is this situation general to all APN functions or specific to the APN functions found so far?

4 Observations on AB functions

In this section we provide various observations (in terms of duals and Walsh supports) of several well-known classes of AB functions, known as Gold, Welch and Kasami functions (see Table 6). Firstly, we start by defining the dual of a (vectorial) Boolean function in general.

Definition 4.1. *Let f be a Boolean function defined on $\mathbb{F}_2^n$. We define its **dual** f^* as*

$$f^*(\mathbf{x}) = \begin{cases} 1, & W_f(\mathbf{x}) \neq 0 \\ 0, & otherwise \end{cases}.$$

If $F = (f_0, \dots, f_{n-1})$ is a (n,n)-function, we define its dual F^* as $F^* = (f_0^*, \dots, f_{n-1}^*)$.

Remark 4.2. *Suppose F is an AB (n,n)-function and let us denote with $F_i = \mathbf{v}_i \cdot F$ its component functions, where the vectors $\mathbf{v}_1, \dots, \mathbf{v}_{2^n-1} \in \mathbb{F}_2^{n^*}$ are ordered lexicographically. With Ω_i we denote the Walsh support of F_i and with $\mathcal{D}_{ij}$ the intersection of the Walsh supports of the components F_i and F_j, that is*

$$\mathcal{D}_{ij} = \Omega_i \cap \Omega_j.$$

Moreover, we suppose that the vectors in $\mathcal{D}_{ij}$, Ω_i and Ω_j are ordered lexicographically, and denote with $\mathbf{v}_{ij}$, $\mathbf{v}_i$, $\mathbf{v}_j$ the first vector of $\mathcal{D}_{ij}$, Ω_i and Ω_j, respectively.

In Table 8 we give the values of the exponents d of the Gold, Kasami and Welch functions x^d defined on $\mathbb{F}_{2^n}$, for $n \leq 15$.

Example 4.3. *Let us consider the function x^3 over $\mathbb{F}_{2^3}$ (Gold case). Its ANF form is $F(x_0, x_1, x_2) = (f_0(x_0, x_1, x_2), f_1(x_0, x_1, x_2), f(x_0, x_1, x_2))$, where*

$$f_0(x_0, x_1, x_2) = x_0 \oplus x_0x_1 \oplus x_1x_2$$
$$f_1(x_0, x_1, x_2) = x_1 \oplus x_0x_2 \oplus x_1x_2$$
$$f_2(x_0, x_1, x_2) = x_1 \oplus x_0x_1 \oplus x_2 \oplus x_1x_2$$

In Table 9 we list the truth tables of the component functions of F as well as their dual functions and corresponding Walsh spectra, and in Table 10 we give the Walsh supports of the component functions F_i.

Dimension n	Gold exponents d	Kasami exponents d	Welch exponents d
3	3	3	5
5	3, 5	13	7
7	3, 5, 9	13, 57	11
9	3, 5, 17	13, 241	19
11	3, 5, 17, 33	13, 57, 241, 993	35
13	3, 5, 9, 17, 33, 65	13, 57, 241, 993, 4033	67
15	3, 5, 17, 129	13, 241, 16257	131

Table 8: List of exponents d of the Gold, Welch and Kasami functions x^d defined on $\mathbb{F}_{2^n}$

$\mathbf{v}_i$	T_{F_i}	S_{F_i}	F_i^*	$S_{F_i^*}$
$(0,0,1)$	$(0,1,1,0,1,0,1,0)$	$(0,-4,0,4,0,4,0,4)$	$(0,1,0,1,0,1,0,1)$	$(0,8,0,0,0,0,0,0)$
$(0,1,0)$	$(0,0,1,0,0,1,1,1)$	$(0,0,4,4,4,-4,0,0)$	$(0,0,1,1,1,1,0,0)$	$(0,0,0,0,0,0,8,0)$
$(0,1,1)$	$(0,1,0,0,1,1,0,1)$	$(0,4,-4,0,4,0,0,4)$	$(0,1,1,0,1,0,0,1)$	$(0,0,0,0,0,0,0,8)$
$(1,0,0)$	$(0,0,0,1,1,1,1,0)$	$(0,0,0,0,4,4,4,-4)$	$(0,0,0,0,1,1,1,1)$	$(0,0,0,0,8,0,0,0)$
$(1,0,1)$	$(0,1,1,1,0,1,0,0)$	$(0,4,0,4,-4,0,4,0)$	$(0,1,0,1,1,0,1,0)$	$(0,0,0,0,0,8,0,0)$
$(1,1,0)$	$(0,0,1,1,1,0,0,1)$	$(0,0,4,-4,0,0,4,4)$	$(0,0,1,1,0,0,1,1)$	$(0,0,8,0,0,0,0,0)$
$(1,1,1)$	$(0,1,0,1,0,0,1,1)$	$(0,4,4,0,0,4,-4,0)$	$(0,1,1,0,0,1,1,0)$	$(0,0,0,8,0,0,0,0)$

Table 9: Component functions and their duals for $(n,d)=(3,3)$.

i	Ω_i
1	$\{(0,0,1),(0,1,1),(1,0,1),(1,1,1)\}$
2	$\{(0,1,0),(0,1,1),(1,0,0),(1,0,1)\}$
3	$\{(0,0,1),(0,1,0),(1,0,0),(1,1,1)\}$
4	$\{(1,0,0),(1,0,1),(1,1,0),(1,1,1)\}$
5	$\{(0,0,1),(0,1,1),(1,0,0),(1,1,0)\}$
6	$\{(0,1,0),(0,1,1),(1,1,0),(1,1,1)\}$
7	$\{(0,0,1),(0,1,0),(1,0,1),(1,1,0)\}$

Table 10: Walsh supports of the component functions for $(n,d)=(3,3)$

Let us consider Ω_1 and Ω_2. We observe the following:

$$\begin{aligned}
\mathcal{D}_{12} = \{(0,1,1),(1,0,1)\} &\Rightarrow \mathcal{D}_{12} \oplus (0,1,1) = \{(0,0,0),(1,1,0)\}\\
\Omega_1 \setminus \mathcal{D}_{12} = \{(0,0,1),(1,1,1)\} &\Rightarrow \Omega_1 \setminus \mathcal{D}_{12} \oplus (0,0,1) = \{(0,0,0),(1,1,0)\}\\
\Omega_2 \setminus \mathcal{D}_{12} = \{(0,1,0),(1,0,0)\} &\Rightarrow \Omega_2 \setminus \mathcal{D}_{12} \oplus (0,1,0) = \{(0,0,0),(1,1,0)\}
\end{aligned}$$

i.e., if we denote with $V = \{(0,1,0),(1,0,0)\}$, then $\mathcal{D}_{12} = (0,1,1) \oplus V$, $\Omega_1 \setminus \mathcal{D}_{12} = (0,0,1) \oplus V$ and $\Omega_2 \setminus \mathcal{D}_{12} = (0,1,0) \oplus V$. This holds for any $\mathcal{D}_{ij}$, $1 \le i,j \le 7, i \ne j$.

Remark 4.4. *In [23] it is proved that for any n, the Walsh support of any quadratic function on $\mathbb{F}_2^n$ is a flat on $\mathbb{F}_2^n$ of even dimension. Since all Gold functions are quadratic, the observations about $\mathcal{D}_{ij}$ are straightforward. Moreover, each $\mathcal{D}_{ij}$ is of dimension $n-2$.*

By observing the Walsh spectra of duals of component functions in the Gold case we obtained the following result.

Proposition 4.5. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be an AB function. Suppose that the Walsh supports Ω_i of the component functions F_i of F are affine subspaces of dimension $n-1$. Then the component functions of the dual F^* are linear functions defined on $\mathbb{F}_2^n$.*

Proof. First we consider the Walsh-Haddamard transform of an arbitrary component function of F^*.
Case I: Suppose that $\mathbf{u} \neq \mathbf{0}$.

$$\begin{aligned}
W_{F_i^*}(\mathbf{u}) &= \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{F_i^*(\mathbf{x})\oplus \mathbf{u}\cdot\mathbf{x}} = \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{F_i^*(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}} = \sum_{\mathbf{x}\notin\Omega_i} (-1)^{\mathbf{u}\cdot\mathbf{x}} - \sum_{\mathbf{x}\in\Omega_i} (-1)^{\mathbf{u}\cdot\mathbf{x}}\\
&= \sum_{\mathbf{x}\notin\Omega_i} (-1)^{\mathbf{u}\cdot\mathbf{x}} + \sum_{\mathbf{x}\in\Omega_i} (-1)^{\mathbf{u}\cdot\mathbf{x}} - \sum_{\mathbf{x}\in\Omega_i} (-1)^{\mathbf{u}\cdot\mathbf{x}} - \sum_{\mathbf{x}\in\Omega_i} (-1)^{\mathbf{u}\cdot\mathbf{x}} = \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{\mathbf{u}\cdot\mathbf{x}} - 2\sum_{\mathbf{x}\in\Omega_i} (-1)^{\mathbf{u}\cdot\mathbf{x}}\\
&\overset{(2.4)}{=} -2\sum_{\mathbf{x}\in\Omega_i} (-1)^{\mathbf{u}\cdot\mathbf{x}},
\end{aligned}$$

Since every AB function is a permutation (Remark 3.41), then $\mathbf{0} \notin \Omega_i$. Now, if we represent Ω_i as $\Omega_i = \mathbf{a} + V$, where $\mathbf{a} \notin V$ and V is a linear subspace in $\mathbb{F}_2^n$ of dimension $n-1$, then $\Omega_i^C = V$. Thus,

$$\begin{aligned}
-2\sum_{\mathbf{x}\in\Omega_i} (-1)^{\mathbf{u}\cdot\mathbf{x}} &= 2\sum_{\mathbf{x}\notin\Omega_i} (-1)^{\mathbf{u}\cdot\mathbf{x}} - 2\sum_{\mathbf{x}\notin\Omega_i} (-1)^{\mathbf{u}\cdot\mathbf{x}} - 2\sum_{\mathbf{x}\in\Omega_i} (-1)^{\mathbf{u}\cdot\mathbf{x}} = 2\sum_{\mathbf{x}\notin\Omega_i} (-1)^{\mathbf{u}\cdot\mathbf{x}} - 2\sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{\mathbf{u}\cdot\mathbf{x}}\\
&\overset{(2.4)}{=} 2\sum_{\mathbf{x}\notin\Omega_i} (-1)^{\mathbf{u}\cdot\mathbf{x}} = 2\sum_{\mathbf{x}\in\Omega_i^C} (-1)^{\mathbf{u}\cdot\mathbf{x}} = 2\sum_{\mathbf{x}\in V} (-1)^{\mathbf{u}\cdot\mathbf{x}} = \begin{cases} 0, & \mathbf{u} \notin V^\perp \\ 2\cdot 2^{\dim V}, & \textit{otherwise} \end{cases}\\
&= \begin{cases} 0, & \mathbf{u} \notin V^\perp \\ 2^n, & \textit{otherwise} \end{cases}
\end{aligned}$$

where $V^{\perp} = \{\mathbf{x} \in \mathbb{F}_2^n : \mathbf{x} \cdot \mathbf{v} = 0, \forall \mathbf{v} \in V\}$.
Case II: Suppose that $\mathbf{u} = \mathbf{0}$.

$$W_{F_i^*}(\mathbf{0}) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{F_i^*(\mathbf{x})} = \sum_{\mathbf{x} \in \Omega_i^c} 1 - \sum_{\mathbf{x} \in \Omega_i} 1 = |\Omega_i^c| - |\Omega_i| = 0.$$

So, for every $\mathbf{u} \in \mathbb{F}_2^n$ we have

$$W_{F_i^*}(\mathbf{u}) = \begin{cases} 0, & \mathbf{u} \notin V^{\perp} \vee \mathbf{u} = \mathbf{0} \\ 2^n, & otherwise \end{cases}$$

Since V is of dimension $n-1$, $V^{\perp}$ is of dimension 1, i.e., $W_{F_i^*}$ is non-zero at only one vector. □

Let us consider the Welch case:

1. For $F(x) = x^5$ on $\mathbb{F}_{2^3}$, the observations are the same as in the case of $(n, d) = (3, 3)$.

2. For $F(x) = x^7$ on $\mathbb{F}_{2^5}$ we observed that the duals F_i^* of the component functions are also AB. The intersection $\Omega_i \cap \Omega_j$ of any two Walsh supports of the component functions F_i and F_j, contains exactly 8 elements, but $\mathcal{D}_{ij} \oplus \mathbf{v}_{ij}$, $\Omega_i \setminus \mathcal{D}_{ij} \oplus \mathbf{v}_i$ and $\Omega_j \setminus \mathcal{D}_{ij} \oplus \mathbf{v}_j$ are distinct. However, when we considered the Walsh supports Ω_i^* of the duals, we observed that
$$\mathcal{D}_{ij}^* \oplus \mathbf{v}_{ij}^* = \Omega_i^* \setminus \mathcal{D}_{ij}^* \oplus \mathbf{v}_i^* = \Omega_j^* \setminus \mathcal{D}_{ij}^* \oplus \mathbf{v}_j^*.$$

3. For $F(x) = x^{11}$ on $\mathbb{F}_{2^7}$ we observed that the duals F_i^* of the component functions are also AB. The intersection $\Omega_i \cap \Omega_j$ of any two Walsh supports of the component functions F_i and F_j, contains exactly 32 elements, but $\mathcal{D}_{ij} \oplus \mathbf{v}_{ij}$, $\Omega_i \setminus \mathcal{D}_{ij} \oplus \mathbf{v}_i$ and $\Omega_j \setminus \mathcal{D}_{ij} \oplus \mathbf{v}_j$ are distinct. However, when we considered the Walsh supports Ω_i^* of the duals, we observed that
$$\mathcal{D}_{ij}^* \oplus \mathbf{v}_{ij}^* = \Omega_i^* \setminus \mathcal{D}_{ij}^* \oplus \mathbf{v}_i^* = \Omega_j^* \setminus \mathcal{D}_{ij}^* \oplus \mathbf{v}_j^*.$$

4. For $F(x) = x^{19}$ on $\mathbb{F}_{2^9}$ we observed that the Walsh coefficients of the duals F_i^* of the component functions are $0, \pm 32, \pm 64$, i.e. the dual F^* has 5-value Walsh spectra. The intersections of the Walsh supports of F_i are not the same, $|\mathcal{D}_{ij}| \in \{116, 120, 124, 128, 132, 136, 140\}$. The observation about affine subspaces does not hold for the component functions nor their duals.

From these observations, we see that characterisations regarding the Walsh support of the Welch function are not trivial, mostly because of the fact that the intersections of the supports of the component functions do not have to be the same. Moreover, the question of the ABness of their duals arises and according to Table 11 we give the following conjecture.

n	d	Walsh coefficients of F^*	Comment
3	5	$\{0, 8\}$	linear
5	7	$\{0, \pm 8\}$	AB
7	11	$\{0, \pm 16\}$	AB
9	19	$\{0, \pm 2^5, \pm 2^6\}$	5-valued Walsh spectra
11	35	$\{0, \pm 2^6, \pm 2^7\}$	5-valued Walsh spectra
13	67	$\{0, \pm 2^7, \pm 2^8\}$	5-valued Walsh spectra
15	131	$\{0, \pm 2^8, \pm 2^9\}$	5-valued Walsh spectra
17	259	$\{0, \pm 2^9, \pm 2^{10}\}$	5-valued Walsh spectra

Table 11: Walsh coefficients of duals of the Welch functions

Conjecture 4.6. *Let $F(x) = x^{2^{\frac{n-1}{2}}+3}$ be the Welch function defined on $\mathbb{F}_{2^n}$, $n \geq 9$. Then the Walsh coefficients of its dual F^* are $\{0, \pm 2^{\frac{n+1}{2}}, \pm 2^{\frac{n+3}{2}}\}$.*

Regarding the Kasami case, we made the following observations:

1. For $F(x) = x^{13}$ on $\mathbb{F}_{2^5}$ the observations are the same as in the Welch case $(n, d) = (5, 7)$.
2. For $F(x) = x^{13}$ on $\mathbb{F}_{2^7}$ the observations are the same as in the Welch case $(n, d) = (7, 11)$.
3. For $F(x) = x^{57}$ on $\mathbb{F}_{2^7}$ we observed that the duals F_i^* of the component functions are also AB. The intersection $\Omega_i \cap \Omega_j$ of any two Walsh supports of the component functions F_i and F_j, contain either 28, 32 or 36 vectors, but the intersection of the Walsh supports of the duals always contains 32 vectors. The observation about affine subspaces does not hold in either case.
4. For $F(x) = x^{13}$ on $\mathbb{F}_{2^9}$ we observed that the Walsh coefficients of the duals F_i^* of the component functions are $\{0, \pm 32, -64\}$, i.e. F^* has a 4-value Walsh spectra. For any two component functions, the intersection of their Walsh supports has either 120, 124, 128, 132, 136 or 140 vectors. The intersection of the Walsh supports of their duals is not unique either. The observation about affine subspaces does not hold in either case.
5. For $F(x) = x^{241}$ on $\mathbb{F}_{2^9}$ we observed that the Walsh coefficients of the duals F_i^* of the component functions are $\{0, \pm 32, \pm 64\}$, i.e. F^* has a 5-valued Walsh spectra. For any two component functions, the intersection of their Walsh supports has either 116, 120, 124, 128, 132 or 136 vectors. The intersection of the Walsh sup-

ports of their duals is not unique either. The observation about affine subspaces does not hold in either case.

These observations tell us that characterising Kasami functions with respect to their Walsh supports and duals is not easy. The reason for that can be many things: the degree of these functions is not unique, the intersections of the Walsh supports, in the case of both the component functions and their duals, are of different sizes, their Walsh spectra are not consistent, etc. In Table 12 we give some comments regarding the Walsh spectra of duals of the components of Kasami functions.

n	d	Walsh coefficients of F^*	Comment	Degree of x^d on $\mathbb{F}_{2^n}$
5	13	$\{0, \pm 8\}$	AB	3
7	13	$\{0, \pm 16\}$	AB	3
7	57	$\{0, \pm 16\}$	AB	4
9	13	$\{0, \pm 2^5, -2^6\}$	4-valued Walsh spectra	3
9	241	$\{0, \pm 2^5, \pm 2^6\}$	5-valued Walsh spectra	5
11	13	$\{0, \pm 2^6, \pm 2^7\}$	5-valued Walsh spectra	3
11	57	$\{0, \pm 2^6\}$	AB	4
11	241	$\{0, \pm 2^6\}$	AB	5
11	993	$\{0, \pm 2^6, \pm 2^7\}$	5-valued Walsh spectra	6
13	13	$\{0, \pm 2^7, \pm 2^8\}$	5-valued Walsh spectra	3
13	57	$\{0, \pm 2^7\}$	AB	4
13	241	$\{0, \pm 2^7\}$	AB	5
13	993	$\{0, \pm 2^7, \pm 2^8\}$	5-valued Walsh spectra	6
13	4033	$\{0, \pm 2^7, \pm 2^8\}$	5-valued Walsh spectra	7
15	13	$\{0, \pm 2^8, \pm 2^9\}$	5-valued Walsh spectra	3
15	241	$\{0, \pm 2^8, \pm 2^{10}, 2^{11}\}$	6-valued Walsh spectra	5
15	16257	$\{0, \pm 2^8, \pm 2^9\}$	5-valued Walsh spectra	8

Table 12: Walsh coefficients of the duals of the Kasami function

5 Conclusion

In this thesis we have briefly introduced cryptography and main goals that one has to achieve in the design of block ciphers, as the main representative of symmetric-key cryptography. Throughout the thesis we have discussed Boolean functions, some of their important properties and defined the Walsh-Hadamard transform. The application of vectorial Boolean functions in the construction of block ciphers is of great importance, even more, finding such functions which will be resistant to various attacks (especially differential cryptanalysis). Because of this the APN and AB functions have been studied intensively in the past 25 years. We have defined these functions, listed some of their main properties as well as their different characterizations and observed the classes of power APN and AB functions. In the last chapter of the thesis we discussed some observations we made in terms of duals of some power AB functions (Gold, Kasami and Welch), where we have proven that under certain conditions the component functions of the dual of a vectorial Boolean function, defined on $\mathbb{F}_2^n$, are linear and we conjecture that the dual of the Welch function, for $n \geq 5$, has 5-valued Walsh spectra.

6 Povzetek naloge v slovenskem jeziku

Potreba po kriptografiji se je pojavila takoj, ko so prvi ljudje poskusili prikrivati skrivnosti. Ko se povežemo na internet, ko uporabljamo katerokoli mobilno napravo, pošiljamo informacije po omrežjih in preko serverjev, nad katerimi nimamo nikakršnega nadzora. Kljub temu želimo, da poslane informacije ostanejo zasebne. V kriptografiji pogosto uporabljamo tako imenovane Boolove funkcije, ki slikajo $\mathbb{F}_2^n \to \mathbb{F}_2$. V zaključnem delu bomo obravnavali tudi funkcije, ki slikajo iz $\mathbb{F}_2^n$ v $\mathbb{F}_2^m$, tako imenovane vektorske Boolove funkcije. Uporabljene so v številnih kriptografskih transformacijah, kot so na primer S-škatle, ki v iterativne bločne šifre uvajajo Shannonov princip zmede. Glavni napadi na takšne šifre so linearni in diferenčni. Zaradi tega morajo funkcije, uporabljene v takšnih šifrah, imeti visoko nelinearnost oziroma nizko diferenčno uniformnost. Funkcije, ki zadostijo tem pogojem in nudijo optimalno odpornost na takšne napade, imenujemo skoraj popolnoma ne-linearne funkcije (almost perfect non-linear - APN) in skoraj ukrivljene funkcije (almost bent - AB). Ti dve družini sta glavni predmet zaključne naloge.

Najprej so predstavljene uvodne definicije in lastnosti, ki bodo v uporabi skozi celotno zaključno nalogo, kot so ne-linearnost, ravnovesje, Walsh-Hadamard transformacija, različne reprezentacije Boolovih funkcij in ekvivalenca Boolovih funkcij. Vsi pojmi so predstavljeni tudi za vektorske Boolove funkcije. Sledi uvod v APN in AB preslikave, ki so definirane na sledeči način. Za funkcijo $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ in poljubna elementa $\mathbf{a}, \mathbf{b} \in \mathbb{F}_2^n$ z $\delta_F(\mathbf{a}, \mathbf{b})$ označimo število rešitev enačbe $F(\mathbf{x} \oplus \mathbf{a}) \oplus F(\mathbf{x}) = \mathbf{b}$ in z $\Delta_F = \{\delta_F(\mathbf{a}, \mathbf{b}) : \mathbf{a}, \mathbf{b} \in \mathbb{F}_2^n\}$ označimo *diferencialno porazdelitveno tabelo* funkcije F. Če je $\Delta_F = \{0, 2\}$, imenujemo funkcijo F *skoraj popolnoma nelinearna* (APN). Če pa so Walshovi koeficienti $W_F(\mathbf{u}, \mathbf{v})$ funkcije F enaki 0 ali $\pm 2^{\frac{n+1}{2}}$, imenujemo funkcijo F *skoraj ukrivljena* (AB). Vsaka AB funkcija je APN, obrat pa ne drži vedno. V nadaljevanju zaključne naloge predstavimo različne karkterizacije APN funkcij glede na rešitve sistema enačb in indikator vsote kvadratov ter tudi karakterizacijo AB funkcij. Obravnavamo APN permutacije in opišemo enega od velikih odprtih problemov s področja, ki ga je predstavil Dillon v [27]: ”Ali obstaja APN permutacija nad poljem $\mathbb{F}_{2^n}$, če je n sodo število?´´ Danes poznamo samo eno takšno permutacijo in to za $n = 6$. Za

$n \geq 8$ je vprašanje še vedno odprto. Podamo tudi seznam odprtih problemov, kot jih je opisal Carlet v [20].

V zadnjem poglavju zaključne naloge obravnavamo določena opažanja, vezana na duale določenih potenčnih AB funkcij (Gold, Kasami in Welch), kjer je dokazano, da so pod določenimi pogoji komponentne funkcije duala vektorske Boolove funkcije, definirane nad $\mathbb{F}_2^n$, linearne. Postavimo domnevo, da ima dual Welch funkcije za $n \geq 5$ Walsh spekter s petimi vrednostmi. V prihodnjem delu bomo domnevo poskusili dokazati in se nasplošno posvetili Walshevemu spektru s petimi vrednostmi, njegovi strukturi in karakterizaciji.

7 Bibliography

[1] T.P. Berger, A. Canteaut, P. Charpin, and Y. Laigle-Chapuy, On Almost Perfect Nonlinear Functions Over $\mathbb{F}_2^n$. *IEEE Trans. Inform. Theory* 52(9) (2006) 4160–4170.

[2] T. Beth and C. Ding, On almost perfect non-linear permutations. In: T. Helleseth (ed.), *Advances in Cryptology — EUROCRYPT '93, Lecture Notes in Computer Science*, Springer-Verlag, New York, 1993, 65–76.

[3] E. Biham and A. Shamir, Differential Cryptanalysis of DES-like Cryptosystems. *Journal of Cryptology* 4(1) (1991) 3–72.

[4] C. Boura and A. Canteaut, On the Influence of the Algebraic Degree of F^{-1} on the Algebraic Degree of $G \circ F$. In *IACR Cryptology ePrint Archive*, 2013.

[5] C. Bracken, E. Byrne, E. Markin, and N. McGuire, A Few More Quadratic APN Functions. *Cryptography and Communications* 3(1) (2011) 43–53.

[6] C. Bracken, E. Byrne, E. Markin, and N. McGuire, New Families of Quadratic Almost Perfect non-linear Trinomials and Multinomials. *Finite Fields and Their Applications* 14(3) (2008) 703–714.

[7] M. Brinkmann and G. Leander, On the classification of APN functions up to dimension five. *Designs, Codes and Cryptography* 49 (2008) 273–288.

[8] K.A. Browning, J.F. Dillon, M.T. McQuistan, and A.J. Wolfe, An APN permutation in dimension six. *Contemporary Mathematics* 518 (2010) 33–42.

[9] K.A. Browning, J.F. Dillon, R.E. Kibler, and M.T. McQuistan, APN Polynomials and Related Codes. *Journal of Combinatorics, Information & System Sciences* 34 (2009) 135–159.

[10] L. Budaghyan, *Construction and Analysis of Cryptographic Functions*, Springer International Publishing, First Edition, 2014.

[11] L. Budaghyan and C. Carlet, Classes of Quadratic APN Trinomials and Hexanomials and Related Structures. *IEEE Trans. Inform. Theory* 54(5) (2008) 2354–2357.

[12] L. Budaghyan, C. Carlet, and A. Pott, New classes of almost bent and almost perfect non-linear functions. *IEEE Trans. Inform. Theory* 52(3) (2006) 1141–1152.

[13] L. Budaghyan, C. Carlet, and G. Leander, Two Classes of Quadratic APN Binomials Inequivalent to Power Functions. *IEEE Trans. Inform. Theory* 54(9) (2008) 4218–4229.

[14] L. Budaghyan, C. Carlet, and G. Leander, Constructing New APN Functions from Known Ones. *Finite Fields and Their Applications* 15(2) (2009) 150–159.

[15] L. Budaghyan, C. Carlet, and G. Leander, On a Construction of Quadratic APN Functions. *IEEE Information Theory Workshop* (2009) 374–378.

[16] L. Budaghyan, T. Helleseth, N. Li and B. Sun, Some Results on the Known Classes of Quadratic APN Functions. In *IACR Cryptology ePrint Archive*, 2016.

[17] A. Canteaut, *Lecture Notes on Cryptographic Boolean Functions*, `https://www.rocq.inria.fr/secret/Anne.Canteaut/poly.pdf`. (Viewed on: 15/2/2019.)

[18] C. Carlet, Boolean Functions for Cryptography and Error Correcting Codes. In: Y. Crama, P.L. Hammer (eds.), *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, Cambridge University Press , 2010, 257–397.

[19] C. Carlet, Partially-bent functions. *Designs, Codes and Cryptography* 3 (1993) 135–145.

[20] C. Carlet, Vectorial Boolean Functions for Cryptography. In: Y. Crama, P.L. Hammer (eds.), *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, Cambridge University Press , 2010, 398–470.

[21] C. Carlet, P. Charpin, and V. Zinoviev, Codes, Bent Functions and Permutations Suitable For DES-like Cryptosystems. *Designs, Codes and Cryptography* 15 (1998) 125–156.

[22] C. Carlet and S. Mesnager, A Note on Semi-bent Boolean Functions. In *IACR Cryptology ePrint Archive*, 2010.

[23] C. Carlet and S. Mesnager, On the Supports of the Walsh transform of Boolean Functions. In *IACR Cryptology ePrint Archive*, 2015.

[24] F. Chabaud and S. Vaudenay, Links between differential and linear cryptanalysis. In: A. De Santis (eds.), *Advances in Cryptology – EUROCRYPT'94. Lecture Notes in Computer Science, Volume 950.*, Springer, 1994, 356–365.

[25] T.W. Cusick and P. Stănică, *Cryptographic Boolean Functions and Applications.* Elsevier, 1981.

[26] J. Daemen and V. Rijmen, *The Design of Rijndael. AES – The Advanced Encryption Standard.* Springer Berlin Heidelberg, First Edition, 2002.

[27] J.F. Dillon, APN Polynomials and Related Codes. In *Workshop on Polynomials over Finite Fields and Their Applictions, Banff International Research Station (BIRS)*, Banff, Alberta, Canada, 2015.

[28] H. Dobbertin, Almost Perfect non-linear Power Functions on $GF(2^n)$: A New Case for n Divisible by 5.. In: D. Jungnickel, H. Niederreiter (eds.), *Finite Fields and Applications*, Springer Berlin Heidelberg, 2001, 113–121.

[29] H. Dobbertin, Almost perfect non-linear power functions over $GF(2^n)$: the Niho case. *Inform. and Comput.* 151 (1999) 57–72.

[30] H. Dobbertin, Almost perfect non-linear power functions over $GF(2^n)$: the Welch case. *IEEE Trans. Inform. Theory* 45 (1999) 1271–1275.

[31] Y. Edel, Quadratic APN Functions as Subspaces of Alternating Bilinear Forms. *Contact Forum Coding Theory and Cryptography III 2009* (2011) 11–24.

[32] R. Gold, Maximal recursive sequences with 3–valued recursive crosscorrelation functions. *IEEE Trans. Inform. Theory* 14 (1968) 154–156.

[33] H.M. Heyes, A tutorial on linear and differential cryptanalysis. *Cryptologia* 26(3) (2002) 189–221.

[34] H. Hollmann and Q. Xiang, A proof of the Welch and Niho conjectures on crosscorrelations of binary m-sequences. *Finite Fields and Their Applications* 7 (2001) 253–286.

[35] X. Hou, Affinity of permutations of $\mathbb{F}_2^{n^*}$. *Discrete Applied Mathematics* 154 (2006) 313–325.

[36] H. Janwa and R. Wilson, Hyperplane sections of Fermat varieties in P3 in char. 2 and some applications to cyclic codes.. In: G. Cohen, T. Mora, O. Moreno (eds.), *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Lecture Notes in Computer Science*, Springer Berlin Heidelberg , 1993, 180–194.

[37] T. Kasami, The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes.. *Inform. and Control* 18 (1971) 369–394.

[38] A. Kerckhoffs, La cryptographie militaire. *Journal des sciences militaires* 9 (1883) 5–83.

[39] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications.* Cambridge University Press, First Edition, 1986.

[40] M. Matsui, Linear cryptanalysis method for DES cipher. In: T. Helleseth (ed.), *Advances in Cryptology — EUROCRYPT '93, Lecture Notes in Computer Science*, Springer Berlin Heidelberg, 1994, 55–64.

[41] M. Maxwell, *Almost Perfect non-linear functions and related combinatorial structures*, Ph.D. dissertation, Iowa State University, 2005.

[42] S. Mesnager, *Bent Functions Fundamentals and Results*, Springer International Publishing Switzerland, 2016.

[43] K. Nyberg, Perfect non-linear S-boxes. In: D.W. Davies (ed.), *Advances in Cryptology — EUROCRYPT '91, Lecture Notes in Computer Science*, Springer Berlin Heidelberg, 1991, 378–386.

[44] K. Nyberg, Differentially uniform mappings for cryptography. In: T. Helleseth (ed.), *Advances in Cryptology — EUROCRYPT '93, Lecture Notes in Computer Science*, Springer Berlin Heidelberg, 1994, 55–64.

[45] K. Nyberg and L.R. Knudsen, Provable security against differential cryptanalysis(rump session). In: E.F. Brickell (ed.), *Advances in Cryptology — CRYPTO' 92, Lecture Notes in Computer Science*, Springer Berlin Heidelberg, 1993, 566–576.

[46] K. Nyberg, S-boxes and round functions with controllable linearity and differential uniformity. In: B. Preneel (ed.), *Proceedings of Fast Software Encryption 1994, LNCS 1008*, Springer Berlin Heidelberg, 1995, 111–130.

[47] K. Pommering, *Fourier Analysis of Boolean Maps – A Tutorial*, `https://www.staff.uni-mainz.de/pommeren/Kryptologie/Bitblock/A_Nonlin/Fourier.pdf`. (Viewed on: 15/2/2019.)

[48] A. Pott, Almost perfect and planar functions. *Designs, Codes and Cryptography* 78 (2016) 141–195.

[49] S. Sağdiçoğlu, *Cryptological Viewpoinnt of Boolean Functions*, Ph.D. dissertation, Graduate School of Natural and Applied Sciences of the Middle East Technical University, 2003.

[50] J. Seberry and X. Zhang, Hadamard matrices, bent functions and cryptography. In *Technical report, University of Wollongong*, 1995.

[51] N. Tokareva, *Bent Functions Results and Applications to Cryptography*, Elsevier, 2015.

[52] Lint, J.H. Van, *Introduction to Coding Theory*, Springer Berlin Heidelberg , 1998.

[53] Y. Yu, M. Wang and Y. Li, Matrix Approach for Constructing Quadratic APN Functions. In *Pre-proceedings of the International Conference WCC 2013*, Bergen, Norway, 2013.

[54] X. Yuwei and W. Chuankun, On the Primary Constructions of Vectorial Boolean Bent Functions. In *IACR Cryptology ePrint Archive*, 2015.

[55] X.M. Zhang and Y. Zheng, GAC – the criterion for global avalanche characteristics of cryptographic functions. *Journal of Universal Computer Science* 1(5) (1995) 320–337.

[56] Y. Zheng and X.M. Zhang, Plateaued Functions. In: V. Varadharajan, M. Yi (ed.), *ICICS 1999: Information and Communication Security*, Springer Berlin Heidelberg, 1999, 284–300.

Appendices

A Programs in MAGMA

Program A.1. *Computing the coordinate functions of the power function x^d over $\mathbb{F}_{2^n}$.*

INPUT: n, d
OUTPUT: $(f_1, f_2, \ldots, f_n)$

```
n:=?;
d:=?;

F2n<g> :=GF(2^n);
F2:=GF(2);
V:=VectorSpace(F2,n);
SetPowerPrinting(F2n,false);
listF2n:=[];
listV:=[];
listFun:=[];
listVFun:=[];
finListVFun:=[];
listBinary:=[];
F:=[];

for i in [0..(2^n-1)] do
Append(~listBinary,Reverse(Intseq(i,2,n)));
end for;

for x in F2n do
if x ne 0 then
Append(~listFun,x^d);
end if;
end for;
listFun:=Reverse(Append(Reverse(listFun),0));

for x in F2n do
```

```
if x ne 0 then
Append(~listF2n,x);
end if;
end for;
listF2n:=Reverse(Append(Reverse(listF2n),0));

for x in listF2n do
Append(~listV,Reverse(Eltseq(x)));
end for;

for x in listF2n do
Append(~listVFun,Reverse(Eltseq(x^d)));
end for;

for i in [1..2^n] do
for j in [1..2^n] do
if (listBinary[i] eq listV[j]) then
Append(~finListVFun,listVFun[j]);
end if;
end for;
end for;

for i in [1..n] do
temp:=[];
for j in [1..2^n] do
Append(~temp,finListVFun[j,i]);
end for;
Append(~F,temp);
end for;
F;
```

Program A.2. *Computing the Walsh spectra of a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ using the function* ***WalshSpectra(f)***.

INPUT: *n and truth table of f*
OUTPUT: *Walsh spectra of f*

```
n:=?;
```

```
TruthTable:=?;

F:=GF(2);
V:=VectorSpace(F,n);
function WalshSpectra(ttable)
walsh:=0;
polartt:=[];
max:=0;

for k:=1 to 2^n do
polartt:=Append(polartt,(-1)^(ttable[k]));
end for;

j:=1;
walsh:=polartt;
while j lt 2^n do
for i:=0 to 2^n-1 do

listA:=Intseq(i,2,n);
listB:=Intseq(j,2,n);
sol:=[0:a in [1..n]];

for a:=1 to n do
sol[a]:=listA[a]*listB[a];
end for;

x:=Seqint(sol,2);

if(x eq 0) then
temp:=walsh[i+1];
walsh[i+1]:=walsh[i+1]+walsh[i+j+1];
walsh[i+j+1]:=temp-walsh[i+j+1];
end if;
end for;
j:=2*j;
end while;

return walsh;
```

```
end function;

WalshSpectra(TruthTable);
```

Program A.3. *Computing the extended walsh spectra of a (n, n)-function F, that is, the Walsh spectra of all the non-zero linear combinations of the coordinate functions of F.*

INPUT: *n, function F (array of its coordinate functions)*
OTUPUT: *Extended Walsh spectra of F*

*Firstly one needs to load the function **`WalshSpectra()`** from Program 2 (copy everything except **`TruthTable:=[];`** and **`WalshSpectra(TruthTable);`**) and insert the code below.*

```
SetColumns(0);
SetAutoColumns(false);

n:=?;
Fun:=?;

v:=[];
for i in Fun do
Append(~v,Matrix(2^n,i));
end for;

linearCombinations:=[];
for i in [1..2^n-1] do
bin:=Reverse(Intseq(i,2,n));
Append(~linearCombinations,&+[(bin[i]*v[i]) :i in [1..n]]) ;
end for;

listFun:=[];
for i in [1..2^n-1] do
temp:=[];
for j in [1..2^n] do
Append(~temp,(linearCombinations[i])[1,j] mod 2);
end for;
Append(~listFun,temp);
```

```
end for;

W:=[];
for i in listFun do
Append(~W,WalshSpectra(i));
end for;
W;
```

Program A.4. *To compute the dual F_i^* of all the component functions F_i of a (n, n)-function F, one can use Program 3 and add the code below. (One can leave out `W;` from Program 3.)*

```
dual:=[];
for i in [1..2^n-1] do
temp:=[];
for j in [1..2^n] do
if W[i,j] eq 0 then
Append(~temp,0);
else
Append(~temp,1);
end if;
end for;
Append(~dual,temp);
end for;
dual;
```

Program A.5. *To compute the Walsh suport of a (n, n)-function F, one uses the function `WalshSpectra` from Program 2 with the code below.*

INPUT: *n, coordinate functions of F*
OUTPUT: *Walsh support of F*

```
SetColumns(0);
SetAutoColumns(false);
n:=?;
F:=?;

v:=[];
for i in F do
```

```
Append(~v,Matrix(2^n,i));
end for;

linearCombinations:=[];

for i in [1..2^n-1] do
bin:=Reverse(Intseq(i,2,n));
Append(~linearCombinations,&+[(bin[i]*v[i]) :i in [1..n]]) ;
end for;

listFun:=[];
for i in [1..2^n-1] do
temp:=[];
for j in [1..2^n] do
Append(~temp,(linearCombinations[i])[1,j] mod 2);
end for;
Append(~listFun,temp);
end for;

W:=[];
for i in listFun do
Append(~W,WalshSpectra(i));
end for;

wsupp:=[];
for i in [1..2^n-1] do
temp:=[];
for j in [1..2^n] do
if W[i,j] ne 0 then
Append(~temp,Reverse(Intseq(j-1,2,n)));
end if;
end for;
Append(~wsupp,temp);
temp:=[];
end for;
wsupp;
```

Program A.6. *Computing the DDT of the power function x^d over $\mathbb{F}_2^n$ using Program 1 in combination with the code below.*

```
DDT:=[];
for a in F2n do
if a ne 0 then
row:=[];
for b in F2n do
s:=0;
for x in F2n do
if x^d+(x+a)^d eq b then
s:=s+1;
end if;
end for;
Append(~row,s);
end for;
Append(~DDT,row);
end if;
end for;
DDT;
```