Diploma Thesis

Boolean Functions

Author
Christian Janson

Supervisors
Prof. Dr. Michael Hortmann, Universität Bremen
Prof. Dr. Gregor Leander, Technical University of Denmark
January 31, 2012

Acknowledgments

First of all I would like to thank Prof. Dr. Michael Hortmann for supervising this thesis. I am very grateful for him introducing me to cryptography and supporting me to attend Eurocrypt 2011 and Asiacrypt 2011.
I am also very thankful for Prof. Dr. Gregor Leander who took the part of being my second supervisor.
I am indebted to my fellow students for their camaraderie and encouragement; in particular, Matthias Gehre and Mischa Jahn for proofreading, and Simon Maier for valuable language suggestions.
Lastly, I wish to thank my family, Silvia Schlapp, my best friend Thilo Hoffeld and my girlfriend Wiebke Drop, for their support and patience.

Bremen, 31 January 2012
Christian Janson

Contents

1. Introduction **5**

2. Generalities on Boolean Functions **9**
2.1. Boolean Functions 9
2.2. The Algebraic Normal Form 13
2.3. First Considerations of Nonlinearity 17

3. The Walsh Transform **19**
3.1. Generalities of the Walsh Transform 19
3.2. Walsh Transform on Subspaces 27
3.3. The Fast Walsh Transform 28

4. Correlation Immune Boolean Functions **30**
4.1. Basic Properties 30
4.2. Construction of Correlation Immune Functions 32

5. Avalanche and Propagation Criterion **37**
5.1. The Strict Avalanche Criterion 37
5.2. The Strict Avalanche Criterion of Higher Order 39
5.3. The Propagation Criterion 44
5.4. The Propagation Criterion of Higher Order 45

6. Bent Boolean Functions **48**
6.1. Difference Sets 48
6.2. Characterizations of the Bent Property 51
6.3. Constructions of Bent Functions 56
6.3.1. Primary Constructions 56
6.3.2. Secondary Constructions 59

7. Properties of Nonlinearity **63**
7.1. Bounds of Nonlinearity 63
7.2. Highly Nonlinear Balanced Functions 67
7.3. Construction of Highly Nonlinear Balanced Functions Satisfying High Degree Propagation Criterion 70
7.3.1. Basic Construction 70
7.3.2. Improved Construction 72

8. Relationships between Cryptographic Properties **76**
8.1. Relation between Nonlinearity and Correlation Immunity 76
8.2. Relationship between Nonlinearity and the Propagation Criterion 80

9. Conclusion and Further Work **84**

A. Proof of Theorem 8.10 **85**

B. Vectorial Boolean functions **89**

Bibliography **92**

1. Introduction

He who loves practice without theory is like the sailor who boards the ship without a rudder and compass and never knows where he may cast.

Leonardo da Vinci

The usage of cryptography have tremendously increased in the last years, as the use of the internet has exploded. A basic aim of cryptography is to enable two parties to confidentially communicate over an insecure channel. This means that any adversary is unable to recover the message (also called plaintext). The most common activity in cryptography is encryption and decryption. The term encryption describes the transformation of the plaintext into the ciphertext. If the ciphertext is used as input into the reverse transformation, then we recover the plaintext. This describes the decryption of a ciphertext.
We speak of symmetric key cryptography if the encryption transformation is trivially related to the reverse decryption transformation. In case the encryption key can be made public, we speak of public key cryptography. This development came up in the mid 1970s when Diffie and Hellman published their paper *New Directions in Cryptography*. Public key cryptography is often preferable to symmetric key cryptography because it allows to communicate in a secure way without having previously shared keys.
In the late 1940s, Shannon [39] introduced the fundamental concepts of confusion and diffusion to achieve security in cryptosystems. Confusion renders the relationship between the key and the ciphertext as complex as possible. This is reflected in the nonlinearity of components of the cryptosystem. Diffusion means that the ciphertext depends on the plaintext in a complex manner. Thus, we have diffusion when changing a small part in the plaintext leads to a large change in the ciphertext.
The question arises whether there are functions that can be utilized to achieve this. We will show that suitable Boolean functions easily provide confusion as well as diffusion. Hence, we deal with Boolean functions and their cryptographic properties.

Objectives

Boolean functions play an important role in cryptography, beginning with their use in linear feedback shift registers (LFSRs). In many stream ciphers, the generation of the keystream consists of a linear part. It is usually composed of one or several LFSRs and a nonlinear filtering function f which produces the output. The main cryptographic properties required for constructing such a function f are: (1) **balancedness**, (2) **algebraic**

degree, (3) **correlation immunity**, (4) **propagation criterion** and (5) **nonlinearity**.

The property of *balancedness*, that is f outputs the same number of zeros and ones, prevents the system from leaking any statistical information about its structure. This means the system does not reveal any information about the plaintext if the ciphertext is known.

A high *algebraic degree* is needed to prevent the system against attacks by the Berlekamp-Massey algorithm. This algorithm outputs the minimal polynomial of a binary sequence in finitely many steps, thus, we know an upper bound of its algebraic degree.

Correlation immune Boolean functions were introduced by Siegenthaler [40] for their ability to resist against certain kinds of divide and conquer attacks on stream ciphers. That is, f is *correlation immune of order* k if its output is statistically independent of any combination of k input variables. A balanced Boolean function which is correlation immune of order k is called k-resilient. Siegenthaler [40] proved a fundamental relation between the order of correlation immunity and the algebraic degree of a Boolean function. On the one hand, he showed that the maximum possible algebraic degree of a Boolean function in n variables which is correlation immune of order k is at most $n-k$. On the other hand, if the function is also balanced the algebraic degree is at most $n-k-1$.

A n-variable Boolean function is said to satisfy the *propagation criterion* (PC) with respect to a nonzero vector if complementing the input coordinates results in the output of the function being complemented 50% of the time over all possible input vectors. Also a Boolean function may satisfy the generalization, the *propagation criterion of degree* k, if complementing k or less input coordinates results in the output of the function being changed 50% of the time over all possible input vectors. Another important criterion is the *strict avalanche criterion* (SAC). The strict avalanche criterion coincides with the propagation criterion of degree 1. Lloyd [19] pointed out that if a function satisfies the strict avalanche criterion of degree k, the function also satisfies the strict avalanche criterion of degree j for any $j = 0, \ldots, k-1$. We can establish the same result for the propagation criterion. Furthermore, we present a recurrence relation to obtain a result on counting SAC functions and provide construction methods to design Boolean functions which satisfy the propagation criterion.

In the mid 1970s, Rothaus [36] introduced a class of Boolean functions which he named *bent functions*. Bent functions only exist in even dimension and possess the highest nonlinearity. Furthermore, they also satisfy the propagation criterion with respect to all nonzero vectors [11]. However, their characteristic to exist only in even dimension prohibits their immediate application in practical usage. A second drawback is their unbalancedness. In cryptographic applications, e.g. the design of strong substitution boxes (S-Boxes), it is often required that the output of the function must act as a uniformly distributed random variable if the input coordinates of a Boolean function are selected

randomly independent [44]. In other words, the function has to be balanced.
Bentness is closely related to the study of difference sets, Hadamard matrices and the signs of the Walsh-coefficients. Furthermore, Rothaus [36] showed that the degree of a bent function is at most $\frac{n}{2}$ for $n > 2$.
The construction of bent functions has attracted much attention. There are *primary constructions* and *secondary constructions*. Primary constructions include bent functions that are not used as building blocks in previous constructions. As an example of primary construction, we present the Maiorana-McFarland construction [22]. We observe a non-recursive method given by Camion et al. [1] using the Maiorana-McFarland construction as a starting point to construct k-resilient functions. Moreover, we follow Carlet's approach [5] using the Maiorana-McFarland construction to design functions satisfying the propagation criterion (of degree k).
Secondary constructions lead to recursive constructions. We observe the possibility to construct bent functions based on concatenation. Dillon [11] pointed out that functions of this type may be decomposed into simpler functions on lower dimensional vector spaces. Primary constructions potentially lead to wider classes of bent functions than secondary constructions.

The *nonlinearity* of a Boolean function is yet another important cryptographic property. Pieprzyk and Finkelstein [33] introduced the notion in the late 1980s as the minimum Hamming-distance from the Boolean function f to the set of all affine functions. Thus, we can say that nonlinearity measures the ability of a system to resist against being expressed as a set of linear equations. Furthermore, a strong need exists for highly nonlinear functions to make the ciphers withstand linear attacks as introduced by Matsui [24].
Seberry et al. [38] showed that the upper bound of nonlinearity is given by $2^{n-1} - 2^{\frac{n}{2}-1}$ and only attainable by bent functions. Owing to the fact that high nonlinearity is not the only important property, bent functions may not directly be used. However, they serve as an excellent starting point to design highly (balanced) nonlinear functions which also fulfill other properties. Moreover, we observe whether there is a bound of nonlinearity for k-resilient Boolean functions for $k < n - 2$. Furthermore, we examine the impact of the algebraic degree on the bound of nonlinearity.

To sum up, our main objectives are to provide basic notions about Boolean functions and their properties. In particular, we focus on nonlinearity and the relationships between nonlinearity and correlation immunity, as well as nonlinearity and the propagation criterion.

Structure of the thesis

This thesis consists of three parts. The first part has an introductory character and serves to get used to Boolean functions and further basic terms that are used within the thesis. In particular, the Walsh transform is of central importance, as it turns out that the Walsh transform is a very powerful tool to prove many results concerning the

different properties. Chapter 2 and 3 are devoted to those preliminaries.

The second part of this thesis starts in chapter 4 and introduces correlation immunity. We provide basic definitions and observe ways to construct (balanced) correlation immune functions. This part is extended with the strict avalanche criterion and its generalization, the propagation criterion. Especially, the concept of diffusion coincides with the strict avalanche criterion. We turn our attention to the observation whether there are constructions that enable to design functions that fulfill the strict avalanche criterion (of higher order) or the propagation criterion (of higher order), respectively. These observations are part of chapter 5.

The third part starts with chapter 6 in which we introduce Bent Boolean functions. These functions only exist in an even number of variables and attain the upper bound of nonlinearity. Chapter 7 is devoted to the observations about nonlinearity and provides construction method to design highly (balanced) nonlinear functions. The last element of the third part is displayed in chapter 8, where the relationships between nonlinearity, correlation immunity and the propagation criterion are observed.

Finally, the thesis closes with a conclusion and an outlook to further work.

2. Generalities on Boolean Functions

2.1. Boolean Functions

The purpose of this section is to make some preliminary definitions on Boolean functions. Let $\mathbb{F}_2^n$ be the vector space of dimension n over the two-element Galois field $\mathbb{F}_2$. $\mathbb{F}_2^n$ consist of 2^n vectors written in a binary sequence of length n.
The vector space $\mathbb{F}_2^n$ is equipped with the scalar product $\langle \cdot, \cdot \rangle \colon \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2$ with

$$\langle a, b \rangle = \bigoplus_{i=1}^{n} a_i \cdot b_i,$$

where the multiplication and addition $\oplus$ are over $\mathbb{F}_2$.
However, if additions are performed in the real numbers, then it is clear from the context.

Definition 2.1. *A* **Boolean function** of n variables is a function $f \colon \mathbb{F}_2^n \to \mathbb{F}_2$ (or simply a function on $\mathbb{F}_2^n$). The $(0,1)$-sequence is defined by $(f(a_0), f(a_1), \ldots, f(a_{2^n-1}))$, also called the truth table of f, where $a_0 = (0, \ldots, 0, 0), a_1 = (0, \ldots, 0, 1), \ldots, a_{2^n-1} = (1, \ldots, 1, 1)$, ordered by lexicographical order.

Definition 2.2. *The logical negation or complement of a Boolean function f is defined by $\overline{f} = f \oplus 1$.*

First, we introduce affine Boolean functions.

Definition 2.3. *An* ***affine function*** *f on $\mathbb{F}_2^n$ is a function that takes the form*

$$f(x) = \langle a, x \rangle \oplus c = a_1 x_1 \oplus \cdots \oplus a_n x_n \oplus c, \tag{2.1}$$

where $a = (a_1, \ldots, a_n) \in \mathbb{F}_2^n$ and $c \in \mathbb{F}_2$. If $c = 0$, then f is a ***linear function****.*

The sequence of an affine (or linear) function is called an affine (or linear) sequence.

Definition 2.4. *The set of all Boolean functions is denoted by*

$$\mathcal{F}_n = \{f | f \colon \mathbb{F}_2^n \to \mathbb{F}_2\}.$$

The subset of all affine Boolean functions in the space $\mathcal{F}_n$ is denoted by

$$\mathcal{A}_n = \{\alpha | \alpha \text{ is affine and } \alpha \in \mathcal{F}_n\}.$$

We define the subset of all linear Boolean functions in the space $\mathcal{F}_n$ by

$$\mathcal{L}_n = \{\beta | \beta \text{ is linear and } \beta \in \mathcal{F}_n\}.$$

Remark.

1. The set of all affine functions consist of the linear functions and their negations.
2. The cardinalities of the above sets are easily observed as

$$|\mathcal{F}_n| = 2^{2^n}, \quad |\mathcal{A}_n| = 2^{n+1} \text{ and } |\mathcal{L}_n| = 2^n.$$

Every once in a while, we would like to have functions with values in the set $\{1, -1\}$. Thus, we introduce the *sign function*.

Definition 2.5. *To each Boolean function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ we associate its* **sign function**, or *character form*, denoted by $\widehat{f}\colon \mathbb{F}_2^n \to \mathbb{R}^* \subseteq \mathbb{C}^*$ and defined by

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

The $(1, -1)$-sequence (or simply sequence) is defined by $((-1)^{f(a_0)}, \ldots, (-1)^{f(a_{2^n-1})})$, where a_i as defined in definition 2.1.

The behavior of the sign function on the sum and product of Boolean functions is shown in the following proposition.

Proposition 2.6. *If f and g are Boolean functions on $\mathbb{F}_2^n$, the following statements hold:*

1. $\widehat{f \oplus g} = \widehat{f}\widehat{g}$.
2. $2\widehat{fg} = 1 + \widehat{f} + \widehat{g} - \widehat{f}\widehat{g}$.

Proof.

1. This claim is straightforward:

$$\widehat{f \oplus g} = (-1)^{f \oplus g} = (-1)^f \cdot (-1)^g = \widehat{f}\widehat{g}.$$

2. This claim is provable with the observation $\widehat{f} = 1 - 2f$, that is

$$\begin{aligned} 1 + \widehat{f} + \widehat{g} - \widehat{f}\widehat{g} &= 1 + (1 - 2f) + (1 - 2g) - (1 - 2f)(1 - 2g) \\ &= 2 - 4fg = 2(1 - 2fg) = 2\widehat{fg} \end{aligned}$$

□

Definition 2.7. *The* ***Hamming-weight*** *of a Boolean function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ is the number of 1s in the truth table of f.*

Next, we introduce the notion of distance between two Boolean functions.

Definition 2.8. *For two Boolean functions $f, g\colon \mathbb{F}_2^n \to \mathbb{F}_2$ we define the* ***Hamming-distance*** *as the number of arguments where f and g differ, that is*

$$d(f,g) = \#\{x \in \mathbb{F}_2^n | f(x) \neq g(x)\}.$$

In other words, the Hamming-distance is the number of 1s in the truth table of $f+g$.

We can also express the Hamming-distance in terms of the Hamming-weight as $d(f,g) = wt(f \oplus g)$.

It is simple to show that the Hamming-distance d is a metric on $\mathbb{F}_2^n$. It follows by noting that $d(f,g)$ equals the number of entries that are needed to turn f into g. Thus, $d(f,g)$ is zero if and only if $f = g$. It is obvious that the Hamming-distance is symmetric and the triangular inequality is shown in lemma 2.10.

Definition 2.9. *The* ***support*** *of a Boolean function f is defined as* $\mathrm{supp}(f) = \{x \in \mathbb{F}_2^n | f(x) = 1\}$.

The Hamming-weight can also be expressed in the notions of the Hamming-distance and the support of a Boolean function as $wt(f) := d(f,0) = |\mathrm{supp}(f)|$.

Let us illustrate the notions by the following example.

Example 1. Let f and g be Boolean functions in two variables:

$$f(x_1,x_2) = x_1\overline{x_2}$$
$$g(x_1,x_2) = (\overline{x_1} + \overline{x_2})$$

The truth table of the two Boolean functions is:

x_1	x_2	f	g	$f \oplus g$
0	0	0	0	0
0	1	0	1	1
1	0	1	1	0
1	1	0	0	0

Therefore, we compute

$$wt(f) = 1$$
$$wt(g) = 2$$
$$d(f,g) = wt(f \oplus g) = 1.$$

The following lemma provides us with some properties satisfied by the Hamming-distance.

Lemma 2.10. *The Hamming-distance satisfies the following properties:*

1. *Let $f, g, h \in \mathcal{F}_n$: $d(f,g) + d(g,h) \geq d(f,h)$.*

2. *Let $\overline{g} = g \oplus 1$ be the negation of g, then $d(f, \overline{g}) = 2^n - d(f,g)$. This is the number of arguments where f and g coincide.*

3. *The number of roots in f is $d(f,1) = 2^n - wt(f)$.*

Proof. 1. Let $f, g, h \in \mathcal{F}_n$: if $f(x) \neq h(x)$ so $f(x) \neq g(x)$ or $g(x) \neq h(x)$ then

$$\begin{aligned} d(f,g) + d(g,h) &= \#\{x \in \mathbb{F}_2^n | f(x) \neq g(x)\} + \#\{x \in \mathbb{F}_2^n | g(x) \neq h(x)\} \\ &\geq \#\{x \in \mathbb{F}_2^n | f(x) \neq h(x)\} = d(f,h). \end{aligned}$$

2. Let $\overline{g}$ be the negation of g then

$$\begin{aligned} d(f, \overline{g}) &= \#\{x \in \mathbb{F}_2^n | f(x) \neq \overline{g}(x)\} \\ &= \#\{x \in \mathbb{F}_2^n | f(x) = g(x)\} \\ &= 2^n - \#\{x \in \mathbb{F}_2^n | f(x) \neq g(x)\} = 2^n - d(f,g). \end{aligned}$$

3. Let $f \in \mathcal{F}_n$ then

$$d(f,1) = \#\{x \in \mathbb{F}_2^n | f(x) \neq 1\} = 2^n - d(f,0) = 2^n - wt(f).$$

□

Theorem 2.11. *If we have two affine functions $\alpha, \beta \in \mathcal{A}_n$, then the distance between them is equal to*

$$d(\alpha, \beta) = \begin{cases} 0 & \text{if } \alpha = \beta \\ 2^n & \text{if } \alpha = \overline{\beta} \\ 2^{n-1} & \text{in other cases.} \end{cases}$$

Proof.

- If $\alpha = \beta$ then there are no arguments $x \in \mathbb{F}_2^n$ where α and β differ. Therefore, the distance between them is equal to zero.

- If $\alpha = \overline{\beta} = \beta \oplus 1$ then the functions differ in every argument $x \in \mathbb{F}_2^n$. Therefore, the functions have a maximum distance which is equal to 2^n.

- If α and β are arbitrary affine functions, simultaneously $\alpha \neq \beta$ and $\alpha \neq \overline{\beta}$, then we have

$$\begin{aligned} d(\alpha, \beta) &= \#\{x \in \mathbb{F}_2^n | \alpha(x) \neq \beta(x)\} = \#\{x \in \mathbb{F}_2^n | \alpha(x) = \overline{\beta(x)}\} \\ &= 2^n - \#\{x \in \mathbb{F}_2^n | \alpha(x) \neq \overline{\beta(x)}\} = 2^{n-1}. \end{aligned}$$

□

We introduce the notion of balancedness. Moreover, we note that balancedness of a Boolean function is a significant cryptographic property in the way that the output of the function should not leak any statistical information about structure.

Definition 2.12. *A $(0,1)$-sequence ($(1,-1)$-sequence) is called* ***balanced*** *if it contains an equal number of zeros and ones (ones and minus ones). A function is balanced if its sequence is balanced i.e. $wt(f) = 2^{n-1}$.*

Next we introduce the notion of equivalence of two Boolean functions.

Definition 2.13. *Two Boolean functions f, g on $\mathbb{F}_2^n$ are called (affinely) equivalent if $f(x) = g(Ax \oplus b)$, where $a, b \in \mathbb{F}_2^n$ and A is a $n \times n$ nonsingular matrix. If no such transformation exists, then f, g are called inequivalent.*

Definition 2.14. *The* ***autocorrelation function*** *$\widehat{r}_{\widehat{f}}(a)$ with a shift $a \in \mathbb{F}_2^n$ is defined as*

$$\widehat{r}_{\widehat{f}}(a) = \sum_{x \in \mathbb{F}_2^n} \widehat{f}(x) \cdot \widehat{f}(x \oplus a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus f(x \oplus a)}.$$

We shall write $\widehat{r}(a)$ if there is no danger of confusion.

Definition 2.15. *Let f be a function on $\mathbb{F}_2^n$. $a \in \mathbb{F}_2^n$ is called a linear structure of f if*

$$|\widehat{r}(a)| = 2^n,$$

that is, if $\widehat{f}(x) \cdot \widehat{f}(x \oplus a)$ is a constant.

The set of all linear structures of a function f form a linear subspace of $\mathbb{F}_2^n$. The dimension gives a measure of linearity. This measure is upper bounded by 2^n. The bound is attainable by the allzero vector in $\mathbb{F}_2^n$ and follows from lemma 3.2. A nonzero linear structure is cryptographically undesirable.

Definition 2.16. *The* ***correlation value*** *between two Boolean functions g and h is defined by*

$$c(g,h) = 1 - \frac{d(g,h)}{2^{n-1}}.$$

2.2. The Algebraic Normal Form

We introduce the most commonly used representation of a Boolean function in cryptography and coding, namely, the n-variable polynomial representation over $\mathbb{F}_2$. This representation is also called *Algebraic Normal Form*. The benefit of this representation is that we can immediately obtain the algebraic degree. Furthermore, we still have the truth table representation of the Boolean function of which the advantage is to obtain

e.g. the Hamming-weight. Therefore, it is eligible to switch between both constructions.

Each vector $u = (u_1, \ldots, u_n)$ corresponds to the set of indices which index those coordinated of u containing its 1's, that is the set $\{i | u_i = 1\}$. This identification on $\mathbb{F}_2^n$ induces the natural (partial) order which we call the *inclusion order*.

Definition 2.17. *For any vectors $u = (u_1, \ldots, u_n)$ and $v = (v_1, \ldots, v_n)$ in $\mathbb{F}_2^n$, we say that u is contained in v (and write $u \leq v$) if $u_i \leq v_i$ for all $i = 1, \ldots, n$.*

Moreover, we need an inversion theorem which was introduced by Hall [16]. It is a specific case of "Möbius inversion in a partially ordered set".

Theorem 2.18. *Let f and g be functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ and let $\mathbb{F}_2^n$ be partially ordered by the inclusion order $\leq$. Then the following statements are equivalent:*

(i) $f(u) = \sum_{v \leq u} g(v)$ *for all* $v \in \mathbb{F}_2^n$,

(ii) $g(u) = \sum_{v \leq u} f(v)$ *for all* $v \in \mathbb{F}_2^n$.

Proof. We apply (i) on the right side of (ii) and obtain

$$\sum_{v \leq u} f(v) = \sum_{v \leq u} \sum_{w \leq v} g(w) = \sum_{w \leq v \leq u} g(w) = \sum_{w \leq u} 2^{wt(u-v)} g(w) = g(u),$$

where the last equality is a consequence of $\mathbb{F}_2$ having characteristic 2. Therefore, (i) implies (ii). By changing f and g it follows that (ii) implies (i), too. □

Theorem 2.19. *Every Boolean function $f \colon \mathbb{F}_2^n \to \mathbb{F}_2$ can be expressed as a unique polynomial in $\mathbb{F}_2[x_1, \ldots, x_n]/(x_1^2 \oplus x_1, \ldots, x_n^2 \oplus x_n)$:*

$$f(x_1, \ldots, x_n) = \sum_{u \in \mathbb{F}_2^n} a(u) x_1^{u_1} \cdots x_n^{u_n}$$

where $a(u) \in \mathbb{F}_2$ with $a(u) = \sum_{x \leq u} f(x)$ and $u = (u_1, \ldots, u_n)$. This representation is called the Algebraic Normal Form or ANF for short.

Proof. Let f be any function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. By Lagrange interpolation, f is given by the polynomial

$$\sum_{u \in \mathbb{F}_2^n} f(u) \prod_{j=1}^{n} (x_j \oplus u_j \oplus 1)$$

which we rearrange to the form

$$\sum_{u \in \mathbb{F}_2^n} g(u) x_1^{u_1} x_2^{u_2} \cdots x_n^{u_n}.$$

By using the above inversion theorem 2.18, we have $g(u) = \sum_{x \leq u} f(x) = a(u)$ which gives us the existence of the algebraic normal form for every Boolean function. This implies that the mapping, from every polynomial $\vartheta \in \mathbb{F}_2[x_1, \ldots, x_n]/(x_1^2 \oplus x_1, \ldots, x_n^2 \oplus x_n)$ to the corresponding function $x \in \mathbb{F}_2^n \mapsto \vartheta(x)$, is onto $\mathcal{F}_n$. Since the size of $\mathbb{F}_2[x_1, \ldots, x_n]/(x_1^2 \oplus x_1, \ldots, x_n^2 \oplus x_n)$ and $\mathcal{F}_n$ are equal, this correspondence is one-to-one. □

Another possible representation of the same ANF uses an indexation of subsets of $N = \{1, \ldots, n\}$. Thus, we obtain the form

$$f(x) = \sum_{I \in \mathfrak{P}(N)} a_I \left(\prod_{i \in I} x_i \right) = \sum_{I \in \mathfrak{P}(N)} a_I x^I, \tag{2.2}$$

where $\mathfrak{P}(N)$ denotes the power set of N.

Example 2. We consider the function f with the following truth table:

$x \in \mathbb{F}_2^3$	$f(x)$
000	0
001	1
010	0
011	0
100	1
101	0
110	0
111	1

It is the sum of the *atomic functions* f_1, f_2 and f_3 whose truth tables are

$x \in \mathbb{F}_2^3$	$f_1(x)$	$f_2(x)$	$f_3(x)$
000	0	0	0
001	1	0	0
010	0	0	0
011	0	0	0
100	0	1	0
101	0	0	0
110	0	0	0
111	0	0	1

Now we observe where the function $f_1(x)$ takes the value 1. The function $f_1(x)$ takes the value 1 if and only if $x_1 \oplus 1 = 1$, $x_2 \oplus 1 = 1$ and $x_3 = 1$. Thus, we obtain the ANF by expanding the product $(x_1 \oplus 1)(x_2 \oplus 1)x_3 = f_1(x)$. Similar observations provide the ANFs for $f_2(x)$ and $f_3(x)$ with $f_2(x) = x_1(x_2 \oplus 1)(x_3 \oplus 1)$ and $f_3(x) = x_1x_2x_3$. Finally, we can see that the ANF of $f(x)$ equals $(x_1 \oplus 1)(x_2 \oplus 1)x_3 \oplus x_1(x_2 \oplus 1)(x_3 \oplus 1) \oplus x_1x_2x_3 = x_1 \oplus x_2 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1x_3 \oplus x_2x_3 \oplus x_1x_2x_3$.

Definition 2.20. *The number of variables in the highest order monomial with nonzero coefficient is called the* ***algebraic degree****.*

Example 3. We take the function $f(x) = x_1 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1x_2x_3$. The highest order monomial with a nonzero coefficient is $x_1x_2x_3$. Thus, the algebraic degree is $\deg(f) = 3$.

Obviously, affine functions have at most degree one. Next, we introduce the term homogeneity of a Boolean function.

Definition 2.21. *A Boolean function is said to be* ***homogeneous*** *if its algebraic normal form only contains terms of the same degree.*

Example 4. We consider the function $f(x) = x_1x_2 \oplus x_1x_3 \oplus x_2x_3$. Then we obtain $\deg(f) = 2$ and the ANF only contains terms of the same degree. Thus, the function is homogeneous.

Remark. The algebraic normalform is not the only representation to express a Boolean function. Also the *disjunctive normal form* (DNF) is a possibility. Carlet and Guillot introduced yet another representation, the so-called *numerical normal form* (NNF).

As mentioned before, we want to evaluate the ANF. Therefore, we provide the following example which shows the utility to switch between the polynomial representation of any function and its truth table.

Example 5. Let us assume that we have an eight bit string of the algebraic normalform of a function $f \in \mathcal{F}_3$ as follows

$$(00101101).$$

Then we can interpret this as

$$a(000) = 0, a(001) = 0, a(010) = 1, a(011) = 0,$$
$$a(100) = 1, a(101) = 1, a(110) = 0, a(111) = 1,$$

and we obtain the polynomial

$$0 \cdot 1 \oplus 0 \cdot x_3 \oplus 1 \cdot x_2 \oplus 0 \cdot x_2x_3 \oplus 1 \cdot x_1 \oplus 1 \cdot x_1x_3 \oplus 0 \cdot x_1x_2 \oplus 1 \cdot x_1x_2x_3.$$

The related truth table is

$$f(000) = 0, f(001) = 0, f(010) = 1, f(011) = 1,$$
$$f(100) = 1, f(101) = 0, f(110) = 0, f(111) = 0,$$

and we write the truth table as a bit string

$$(00111000).$$

If we have given the bit string of the truth table we can achieve the following polynomial (written in short form)

$$1 \cdot x_2 \oplus 1 \cdot x_2x_3 \oplus 1 \cdot x_1.$$

We evaluate the polynomial analogue to the polynomial above and get the bit string representation of the algebraic normal form.

We close this section with the introduction of a useful notation to obtain the functional representation of a *concatenated sequence*. Let $a = (i_1, \ldots, i_n)$ be a vector on $\mathbb{F}_2^n$ and D_a is a function on $\mathbb{F}_2^n$ given by

$$D_a(y_1, \ldots, y_n) = (y_1 \oplus i_1 \oplus 1) \cdots (y_n \oplus i_n \oplus 1).$$

With this notation we obtain the following lemma.

Lemma 2.22. *[38] Let $f_0, f_1, \ldots, f_{2^n-1}$ be functions on $\mathbb{F}_2^n$. Let ξ_i be the sequence of f_i, $i = 0, 1, \ldots, 2^n - 1$. Then $\xi = (\xi_0, \xi_1, \ldots, \xi_{2^n-1})$ is the sequence of the following function on $\mathbb{F}_2^{n+m}$*

$$f(y, x) = \bigoplus_{i=0}^{2^n-1} D_{a_i}(y) f_i(x),$$

where $y = (y_1, \ldots, y_m)$, $x = (x_1, \ldots, x_n)$ and a_i as defined in definition (2.1).

To make ourselves familiar with this notation, we observe that if ξ_1 and ξ_2 are the sequences of functions f_1 and f_2 on $\mathbb{F}_2^n$, then $\xi = (\xi_1, \xi_2)$ is the sequence of the following function g on $\mathbb{F}_2^{n+1}$

$$g(u, x_1, \ldots, x_n) = [f_1, f_2]_{n+1} = (u \oplus 1) \cdot f_1(x_1, \ldots, x_n) + u \cdot f_2(x_1, \ldots, x_n).$$

2.3. First Considerations of Nonlinearity

Nonlinearity is one of the most important cryptographic properties. It is introduced rather briefly at this point, we will however deal with nonlinearity intensely in chapter 7.

As before, we denote with $\mathcal{A}_n$ the set of all affine functions and the Hamming-distance (2.8) is the number of arguments where the Boolean functions f and g differ. In addition, Pieprzyk and Finkelstein [33] introduced the notion of nonlinearity as follows

Definition 2.23. *The nonlinearity of a Boolean function $f \in \mathcal{F}_n$ is denoted by N_f and equals*

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

It is obvious that nonlinearity of an affine function is zero. If the Boolean function f is not affine, then we have $N_f > 0$ by definition. Let us observe an example about nonlinearity.

Example 6. Let $f(x) = x_1 x_2 \in \mathcal{F}_2$ be the function and we compute its nonlinearity. The related truth table is given by:

x	f
00	0
01	0
10	0
11	1

In the next step, we have to observe the truth tables of all affine functions.

x	$f_1 = 1$	$f_2 = 0$	$f_3 = x_1$	$f_4 = x_1 \oplus 1$	$f_5 = x_2$	$f_6 = x_2 \oplus 1$	$f_7 = x_1 \oplus x_2$	$f_8 = \overline{x_1 \oplus x_2}$
00	1	0	0	1	0	1	0	0
01	1	0	0	1	1	0	1	1
10	1	0	1	0	0	1	1	1
11	1	0	1	0	1	0	0	0

Next, we have to compute all Hamming-distances between the function f and all affine functions.

$d(f, f_1)$	$d(f, f_2)$	$d(f, f_3)$	$d(f, f_4)$	$d(f, f_5)$	$d(f, f_6)$	$d(f, f_7)$	$d(f, f_8)$
3	1	1	3	1	3	3	3

From definition, the nonlinearity of the function is the minimal Hamming-distance. Therefore, it follows $N_f = d(f, f_2) = d(f, f_3) = d(f, f_5) = 1$.

High nonlinearity is essential in designing a good cryptosystem. It measures the ability of a cryptographic system using the functions to resist against being expressed as a linear set of equations and it assures resistance against linear cryptanalysis introduced by Matsui [24].

3. The Walsh Transform

3.1. Generalities of the Walsh Transform

In this chapter we introduce one of the most important tools in cryptography. Namely, the *Walsh transform* which is the characteristic 2 case of the *discrete Fourier transform*. As we shall see, the use of the Walsh transform makes the computation of nonlinearity and the other properties an easy task.
Let us recall that we have the space $\mathcal{F}_n$ of all two-valued functions on $\mathbb{F}_2^n$. The domain of $\mathcal{F}_n$ is an abelian group and its range elements 0 and 1 can be added and multiplied as complex numbers. Now we analyze $\mathcal{F}_n$ by using tools from harmonic analysis, cf. Lechner [17]. This means that we are able to construct an orthogonal basis of Fourier transform kernel functions, or also known as *group characters*, on $\mathcal{F}_n$. The kernel functions are defined in terms of a group homomorphism from $\mathbb{F}_2^n$ to the direct product of n copies of the multiplicative subgroup $\{\pm 1\}$ on the unit circle of the complex plane. Thereby, we obtain the group characters $G_u(x) = (-1)^{u_1 x_1} \cdot \cdots \cdot (-1)^{u_n x_n} = (-1)^{\langle u,x \rangle}$. In doing so, the set $\{G_u | u \in \mathbb{F}_2^n\}$ is an orthogonal basis for $\mathcal{F}_n$. Due to these observations, we define the Walsh transform of a Boolean function as follows:

Definition 3.1. *The* **Walsh transform** of a function f on $\mathbb{F}_2^n$ is a map $W \colon \mathbb{F}_2^n \longrightarrow \mathbb{R}$ defined by

$$W(f)(u) = \sum_{x \in \mathbb{F}_2^n} f(x) \cdot (-1)^{\langle u,x \rangle}, \tag{3.1}$$

where $\langle u, x \rangle$ is the canonical scalar product. The **Walsh spectrum** of f is the list of 2^n Walsh-coefficients given by (3.1) as u varies.

Lemma 3.2. *If $u \in \mathbb{F}_2^n$, we have*

$$\sum_{x \in \mathbb{F}_2^n} (-1)^{\langle u,x \rangle} = \begin{cases} 2^n & \text{if } u = 0 \\ 0 & \text{else.} \end{cases}$$

Proof. If $u = 0$, then all exponents are zero and therefore all summands are equal 1. Therefore, we have 2^n summands. Now we assume that $u \neq 0$ and consider the hyperplanes $H = \{x \in \mathbb{F}_2^n | \langle u, x \rangle = 0\}$ and $\overline{H} = \{x \in \mathbb{F}_2^n | \langle u, x \rangle = 1\}$. It is obvious that these hyperplanes generate a partition of $\mathbb{F}_2^n$. Furthermore, for any $u \in H$, the summand is equal one, and for any $u \in \overline{H}$, the summand is equal -1. In addition, the cardinalities of H and $\overline{H}$ are the same, that is 2^{n-1}. Therefore, the sum equals zero and the statement follows immediately. □

Next we analyze the effect of applying the Walsh transform on $W(f)$. Proceeding this way we get the observation

$$\begin{aligned} W(W(f))(u) &= \sum_{x\in\mathbb{F}_2^n} W(f)(x)\cdot(-1)^{\langle u,x\rangle} \\ &= \sum_{x\in\mathbb{F}_2^n}\sum_{v\in\mathbb{F}_2^n} f(v)\cdot(-1)^{\langle v,x\rangle}\cdot(-1)^{\langle u,x\rangle} \\ &= \sum_{v\in\mathbb{F}_2^n} f(v)\left[\sum_{x\in\mathbb{F}_2^n}(-1)^{\langle (v+u),x\rangle}\right] \\ &\underbrace{=}_{(3.2)} 2^n\sum_{v\in\mathbb{F}_2^n} f(v) = 2^n f(u). \end{aligned}$$

Theorem 3.3. *The* Walsh transform $W:\mathbb{F}_2^n\longrightarrow\mathbb{R}$ is bijective and the inversion is given by:

$$W^{-1} = 2^{-n}W.$$

Hence, f can be recovered by the inverse Walsh transform given by

$$f(x) = 2^{-n}\sum_{u\in\mathbb{F}_2^n} W(f)(u)\cdot(-1)^{\langle u,x\rangle}. \tag{3.2}$$

At that point we do a short insertion about Hadamard matrices. Furthermore, we define the Kronecker product which we use to introduce Sylvester-Hadamard matrices. This leads us to express the Walsh transform in terms of Sylvester-Hadamard matrices.

Definition 3.4. *A matrix H of order n taking only the values in the set $\{1,-1\}$ will be called **Hadamard matrix** if $H\cdot H^t = n\cdot I_n$, where H^t is the transpose of H and I_n is the $n\times n$ identity matrix.*
In particular, the product of two distinct rows of H is zero.

Since $H^{-1} = \frac{1}{n}H^t$, we also have $H^t\cdot H = n\cdot I_n$. Wallis, Seberry and Street [43] showed that if n is the order of an Hadamard matrix then n is divisible by 1, 2 or 4.
Next we introduce the Kronecker product of matrices.

Definition 3.5. *If $A=(a_{ij})$ is a $m\times m$ matrix and $B=(b_{ij})$ is a $n\times n$ matrix over any field, the **Kronecker product** of A and B is the $mn\times mn$ matrix obtained from A by replacing every entry a_{ij} by $a_{ij}B$. This product is written as*

$$A\otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{bmatrix} = (a_{ij}B).$$

The Kronecker product is not commutative. However, it satisfies the following properties:

1. $(A \otimes B) \otimes C = A \otimes (B \otimes C)$ (Associativity)
2. $(A + B) \otimes C = A \otimes C + A \otimes B$ (Distributivity)
3. $(A \otimes B)(C \otimes D) = (AC) \otimes (BD)$.

Using the Kronecker symbol, we can define a special kind of Hadamard matrix as follows:

Definition 3.6. *The **Sylvester-Hadamard matrix** (or Walsh-Hadamard matrix) of order 2^n, denoted by H_n, is generated by the recursive relation*

$$H_n = \begin{bmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{bmatrix} = H_1 \otimes H_{n-1},$$

for $n = 1, 2, \ldots$ and $H_0 = (1)$.

With this definition we are able to express the Walsh transform in terms of Sylvester-Hadamard matrices, giving us $W(f) = f \cdot H_n$, since $(-1)^{\langle u,v \rangle}$ is the entry on the position $(u, v) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$, in the matrix H_n. Additionally, we can easily express the inverse Walsh transform as $f = 2^{-n} W(f) \cdot H_n$.

Next we collect some properties concerning the Walsh transform.
The following lemma shows the connection between the Walsh transform of two Boolean functions where one function is obtained by an affine transformation of the input coordinates.

Lemma 3.7. *[10] If the Boolean function f can be obtained from g by an affine transformation of the input, that is*

$$g(v) = f(Av \oplus b),$$

with A an invertible matrix and $b \in \mathbb{F}_2^n$, then the Walsh transform of f and g are related by

$$W(g)(u) = \pm W(f)(uA^{-1}).$$

Proof. First,

$$W(g)(u) = \sum_{v \in \mathbb{F}_2^n} (-1)^{\langle u,v \rangle} g(v) = \sum_{v \in \mathbb{F}_2^n} (-1)^{\langle u,v \rangle} f(Av \oplus b).$$

By setting $v = A^{-1}w \oplus A^{-1}b$ and $u' = uA^{-1}$, we get

$$\begin{aligned} W(g)(u) &= \sum_{w \in \mathbb{F}_2^n} (-1)^{\langle u, A^{-1}w \rangle} (-1)^{\langle u, A^{-1}b \rangle} f(w) \\ &= \pm \sum_{w \in \mathbb{F}_2^n} (-1)^{\langle u', w \rangle} f(w) = \pm W(f)(u'). \end{aligned}$$

□

Furthermore, we observe the relationship between the Walsh transform of a Boolean function and its sign function which was introduced by Forré [14].

Lemma 3.8. *Let* $\widehat{f}(x) = (-1)^{f(x)}$*, then*

$$W(\widehat{f})(u) = -2W(f)(u) + 2^n\delta(u),$$

which is equivalent to

$$W(f)(u) = 2^{n-1}\delta(u) - \frac{1}{2}W(\widehat{f})(u),$$

where

$$\delta(u) = \begin{cases} 1 & \text{for } u = 0 \\ 0 & \text{else} \end{cases}$$

is the Dirac symbol.

Proof. We start from the left-hand side of the first equation and obtain

$$\begin{aligned} W(\widehat{f})(u) &= \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)\oplus\langle u,x\rangle} \\ &= \sum_{x\in\mathbb{F}_2^n} (1-2f(x))\cdot(-1)^{\langle u,x\rangle} \\ &= \sum_{x\in\mathbb{F}_2^n} (-1)^{\langle u,x\rangle} - 2\sum_{x\in\mathbb{F}_2^n} f(x)(-1)^{\langle u,x\rangle} \\ &= 2^n\delta(u) - 2W(f)(u) \end{aligned}$$

by definition 3.1 and lemma 3.2. □

The following lemmas provide us with some properties satisfied by the Walsh transform.

Lemma 3.9. *The following statements are true:*

1. $W(\widehat{f\oplus 1})(u) = -W(\widehat{f})(u)$.
2. *If* $g(x) = f(x)\oplus\alpha_a(x)$*, where* $\alpha_a(x) = \sum_{i=1}^n a_i x_i = \langle a, x\rangle$ *is the linear function, then* $W(\widehat{g})(u) = W(\widehat{f})(u\oplus a)$.
3. *If* $g(x) = \alpha_a(x)\oplus c$ *is the affine function, then* $W(\widehat{f\oplus g})(u) = (-1)^c W(\widehat{f})(u\oplus a)$.

Proof.

1.

$$\begin{aligned} W(\widehat{f\oplus 1})(u) &= \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)\oplus 1\oplus\langle u,v\rangle} \\ &= -\sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)\oplus\langle u,v\rangle} = -W(\widehat{f})(u). \end{aligned}$$

2.

$$W(\widehat{g})(u) = \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)\oplus\alpha_a(u)\oplus\langle u,x\rangle}$$
$$= \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)\oplus\langle (u\oplus a),x\rangle} = W(\widehat{f})(u\oplus a).$$

3.

$$W(\widehat{f\oplus g})(u) = \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)\oplus\alpha_a(u)\oplus c\oplus\langle u,x\rangle}$$
$$= (-1)^c \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)\oplus\langle (u\oplus a),x\rangle} = (-1)^c W(\widehat{f})(u\oplus a).$$

The addition of an affine function causes, except for the sign, a permutation of the spectrum.

□

Corollary 3.10. *In particular $W(\widehat{f})(u)$ is always even and we have*

$$-2^n \leq W(\widehat{f})(u) \leq 2^n.$$

A classic property of the Walsh transform is to be an isomorphism from the set of the sign functions on $\mathbb{F}_2^n$, endowed with the so-called convolution product (denoted by $*$), into this same set, endowed with the usual product. The notion of the convolution is given within the next definition.

Definition 3.11. *Let f and g be any Boolean function on $\mathbb{F}_2^n$. The convolution of f and g is defined by*

$$(f * g)(x) = \sum_{y\in\mathbb{F}_2^n} f(y)g(x\oplus y).$$

Proposition 3.12. *Let f and g be any Boolean function on $\mathbb{F}_2^n$. We have:*

$$W(f * g) = W(f)\cdot W(g). \tag{3.3}$$

Consequently:

$$W(f) * W(g) = 2^n W(f\cdot g). \tag{3.4}$$

Proof. We have

$$\begin{aligned}
W(f*g) &= \sum_{x\in\mathbb{F}_2^n} (f*g)(x)\cdot(-1)^{\langle u,x\rangle} \\
&= \sum_{x\in\mathbb{F}_2^n}\sum_{y\in\mathbb{F}_2^n} f(y)g(x\oplus y)\cdot(-1)^{\langle u,x\rangle} \\
&= \sum_{x\in\mathbb{F}_2^n}\sum_{y\in\mathbb{F}_2^n} f(y)g(x\oplus y)\cdot(-1)^{\langle u,y\rangle\oplus\langle u,(x+y)\rangle} \\
&= \left(\sum_{y\in\mathbb{F}_2^n} f(y)\cdot(-1)^{\langle u,y\rangle}\right)\cdot\left(\sum_{x\in\mathbb{F}_2^n} g(x\oplus y)\cdot(-1)^{\langle u,(x\oplus y)\rangle}\right) \\
&= \left(\sum_{y\in\mathbb{F}_2^n} f(y)\cdot(-1)^{\langle u,y\rangle}\right)\cdot\left(\sum_{x\in\mathbb{F}_2^n} g(x)\cdot(-1)^{\langle u,x\rangle}\right) \\
&= W(f)\cdot W(g).
\end{aligned}$$

Thereby, the first equality is proven.
We recall the property $W(W(f)) = 2^n f$. Therefore, we obtain $W(W(f)*W(g)) = 2^{2n} f\cdot g$. Again, using the property we get $W(f)*W(g) = 2^n W(f\cdot g)$. □

Equation (3.4) applied at $x=0$ gives

$$W(f)*W(g)(0) = 2^n W(f\cdot g)(0) = 2^n \sum_{x\in\mathbb{F}_2^n} f(x)g(x) = 2^n f*g(0). \tag{3.5}$$

Taking $f=g$ in (3.5), we obtain Parseval's equation. Parseval's equation will be a useful tool to prove some of the following results.

Corollary 3.13 (Parseval's equation)**.** *For any Boolean function f in n variables, the following equation holds*

$$\sum_{u\in\mathbb{F}_2^n}\left(W(\widehat{f})(u)\right)^2 = 2^{2n}. \tag{3.6}$$

Proof.

$$\begin{aligned}
\sum_{u\in\mathbb{F}_2^n}\left(W(\widehat{f})(u)\right)^2 &= \sum_{u\in\mathbb{F}_2^n}\sum_{x\in\mathbb{F}_2^n}\sum_{y\in\mathbb{F}_2^n}(-1)^{f(x)\oplus f(y)\oplus\langle u,(x\oplus y)\rangle} \\
&= \sum_{x\in\mathbb{F}_2^n}\sum_{y\in\mathbb{F}_2^n}(-1)^{f(x)\oplus f(y)}\underbrace{\sum_{u\in\mathbb{F}_2^n}(-1)^{\langle u,(x\oplus y)\rangle}}_{2^n\delta_x(y)} \\
&= 2^n\sum_{x\in\mathbb{F}_2^n}(-1)^{2f(x)} = 2^{2n},
\end{aligned}$$

where

$$\delta_x(y) = \begin{cases} 1 & \text{if } y = x \\ 0 & \text{if } y \neq x. \end{cases}$$

□

The following lemma is a similar result to Parseval's equation.

Lemma 3.14. $\sum_{u\in\mathbb{F}_2^n} W(\widehat{f})(u)W(\widehat{f})(u\oplus v) = \begin{cases} 2^{2n} & \text{if } v = 0 \\ 0 & \text{if } v \neq 0. \end{cases}$

Proof. The proof is straightforward and follows by lemma 3.2 and the fact $\widehat{f}(w)^2 = 1$

$$\begin{aligned} \sum_{u\in\mathbb{F}_2^n} W(\widehat{f})(u)W(\widehat{f})(u\oplus v) &= \sum_{u,w\in\mathbb{F}_2^n} (-1)^{\langle u,w\rangle}\widehat{f}(w) \sum_{x\in\mathbb{F}_2^n} (-1)^{\langle (u\oplus v),x\rangle}\widehat{f}(x) \\ &= \sum_{w,x\in\mathbb{F}_2^n} (-1)^{\langle v,x\rangle}\widehat{f}(w)\widehat{f}(x) \sum_{u\in\mathbb{F}_2^n} (-1)^{\langle u,(w\oplus x)\rangle} \\ &= 2^n \sum_{w\in\mathbb{F}_2^n} (-1)^{\langle v,w\rangle}\widehat{f}(w)^2 = 2^n \sum_{w\in\mathbb{F}_2^n} (-1)^{\langle v,w\rangle}. \end{aligned}$$

□

The case $v = 0$ gives us Parseval's equation.

As mentioned earlier we can state a relation between the Walsh transform of the autocorrelation function, c.f. definition 2.14, and the square of the Walsh transform of the real-valued function. This fact is stated by the *Wiener-Khintchine Theorem*.

Theorem 3.15. *A Boolean function on $\mathbb{F}_2^n$ satisfies*

$$W(\widehat{r})(t) = W(\widehat{f})^2(t),$$

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

Proof. According to the definition of the autocorrelation function, we obtain

$$\begin{aligned} W(\widehat{r})(t) &= \sum_{s\in\mathbb{F}_2^n} \widehat{r}(s)\cdot(-1)^{\langle t,s\rangle} = \sum_{s\in\mathbb{F}_2^n} \left(\sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)\oplus f(x\oplus s)\oplus\langle t,s\rangle} \right) \\ &= \sum_{x\in\mathbb{F}_2^n} \left(\sum_{s\in\mathbb{F}_2^n} (-1)^{f(x)\oplus f(x\oplus s)\oplus\langle t,s\rangle} \right). \end{aligned}$$

Since $\mathbb{F}_2^n$ is invariant under any transformation, we may replace s by $x \oplus s$ in the second sum. Hence, we obtain

$$\begin{aligned} W(\widehat{r})(t) &= \sum_{x \in \mathbb{F}_2^n} \left(\sum_{s \in \mathbb{F}_2^n} (-1)^{f(x) \oplus f(s) \oplus \langle t, (x \oplus s) \rangle} \right) \\ &= \left(\sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus \langle t, x \rangle} \right) \left(\sum_{s \in \mathbb{F}_2^n} (-1)^{f(s) \oplus \langle t, s \rangle} \right) \\ &= \left(\sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus \langle t, x \rangle} \right)^2 = W(\widehat{f})^2(t). \end{aligned}$$

□

Definition 3.16. *The **spectral radius** of a Boolean function $f \colon \mathbb{F}_2^n \to \mathbb{F}_2$ is defined by*

$$R_f = \max\{|W(\widehat{f})(u)| \colon u \in \mathbb{F}_2^n\}.$$

This definition provides a measure for linearity. Obviously, the linearity is upper bounded by $2^n \geq R_f$ by corollary 3.10. The upper bound is only attainable if f is affine.

Theorem 3.17. *For a Boolean function $f \colon \mathbb{F}_2^n \to \mathbb{F}_2$ the spectral radius is*

$$R_f \geq 2^{\frac{n}{2}},$$

and the equality holds if and only if $W(\widehat{f})^2 = 2^n$ is constant.

The class of functions for which equality holds are known as bent functions. We will study those functions intensively in chapter 6.

Next, we provide a result about the nonlinearity of a Boolean function in terms of their Walsh transform. Therefore, we use the result that we can deduce from the Walsh transform, being that $W(\widehat{f})(u)$ is equal to the number of zeros minus the number of ones in the binary vector $f \oplus \alpha_u$, where α_u is the linear function $\alpha_u(v) = \sum_{i=1}^n u_i v_i$ with $u = (u_1, \ldots, u_n)$ and $v = (v_1, \ldots, v_n)$. Thus, we have

$$W(\widehat{f})(u) = 2^n - 2d(f, \sum_{i=1}^n u_i v_i)$$

or

$$d(f, \sum_{i=1}^n u_i v_i) = \frac{1}{2}(2^n - W(\widehat{f})(u)).$$

We also can write,

$$d(f, 1 \oplus \sum_{i=1}^n u_i v_i) = \frac{1}{2}(2^n + W(\widehat{f})(u)).$$

This proves the following theorem.

Theorem 3.18. *The nonlinearity of f is determined by the Walsh transform of f, that is,*

$$N_f = 2^{n-1} - \frac{1}{2} \max_{u \in \mathbb{F}_2^n} |W(\widehat{f})(u)|.$$

Thus, it is possible to achieve high nonlinearity if the maximal Walsh-coefficient is of little value.

3.2. Walsh Transform on Subspaces

In this section we introduce a result which was given by Lechner [17]. The theorem states the so-called *Poisson Summation Formula*, which is an equation between the Walsh transform of a real-valued function on $\mathbb{F}_2^n$ and a function f restricted to an arbitrary subspace of $\mathbb{F}_2^n$.

Theorem 3.19. *Let f be a real-valued function on $\mathbb{F}_2^n$ and $W(f)$ be its Walsh transform. Let S be an arbitrary subspace of $\mathbb{F}_2^n$ and let $S^\perp$ be the dual (annihilator) of S, that is,*

$$S^\perp = \{x \in \mathbb{F}_2^n | \langle x, s \rangle = 0 \text{ for all } s \in S\}.$$

Then

$$\sum_{u \in S} W(f)(u) = 2^{\dim S} \sum_{u \in S^\perp} f(u).$$

Proof. We have

$$\begin{aligned} \sum_{u \in S} W(f)(u) &= \sum_{u \in S} \left(\sum_{v \in \mathbb{F}_2^n} f(v) \cdot (-1)^{\langle u,v \rangle} \right) \\ &= \sum_{v \in \mathbb{F}_2^n} f(v) \left(\sum_{u \in S} (-1)^{\langle u,v \rangle} \right) \\ &= 2^{\dim S} \sum_{v \in S^\perp} f(v), \end{aligned}$$

by using lemma 3.2. □

The following corollary was discovered independently by Duvall and Mortick [13].

Corollary 3.20. *For any Boolean function $f \colon \mathbb{F}_2^n \to \mathbb{F}_2$,*

$$\sum_{u \leq v} W(f)(u) = 2^{wt(v)} \sum_{u \leq \overline{v}} f(u),$$

where $u \leq v$ means that if $u_i = 1$, then $v_i = 1$, $1 \leq i \leq n$, and $\overline{v}$ denotes the complement of the vector v.

Proof. Analogue to theorem 3.19. □

These results will be important in chapter 6 where we discuss the degree of bent functions.

3.3. The Fast Walsh Transform

The computation of the Walsh transform requires 2^{2n} operations (additions and subtractions). Therefore, the question arises whether there is a faster way to obtain the Walsh-coefficients. MacWilliams and Sloane [21, p.422] dealt with this question and came up with a description of the fast Walsh transform, which is a discrete version of the fast Fourier transform.

Theorem 3.21. *The Sylvester-Hadamard matrix* (3.6) H_n *can be decomposed as*

$$H_n = M_n^{(1)} M_n^{(2)} \cdots M_n^{(n)},$$

where $M_n^{(i)} = I_{2^{n-i}} \otimes H_1 \otimes I_{2^{i-1}}$ *with* $1 \leq i \leq n$ *and* I_m *is the* $m \times m$ *identity matrix.*

Proof. We prove the theorem by induction on n. For $n = 1$ the result is obvious. Now we assume the result is true for n. Then for $1 \leq i \leq n$:

$$\begin{aligned} M_{n+1}^{(i)} &= I_{2^{(n+1)-i}} \otimes H_1 \otimes I_{2^{i-1}} \\ &= I_2 \otimes I_{2^{n-i}} \otimes H_1 \otimes I_{2^{i-1}} = I_2 \otimes M_n^{(i)} \end{aligned}$$

and $M_{n+1}^{(n+1)} = H_1 \otimes I_{2^n}$.
Therefore, we can calculate:

$$\begin{aligned} M_{n+1}^{(1)} \cdots M_{n+1}^{(n+1)} &= (I_2 \otimes M_{n+1}^{(1)}) \cdots (I_2 \otimes M_{n+1}^{(n)})(H_1 \otimes I_2) \\ &= H_1 \otimes (M_{n+1}^{(1)} \cdots M_{n+1}^{(n)}) \\ &= H_1 \otimes H_n = H_{n+1} \end{aligned}$$

□

Let us observe an example given by MacWilliams and Sloane [21].

Example 7. For $n = 2$ we have to compute the matrices

$$M_2^{(1)} = I_{2^1} \otimes H_1 \otimes I_{2^0} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

and

$$M_2^{(2)} = I_{2^0} \otimes H_1 \otimes I_{2^1} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}.$$

Then we can calculate

$$M_2^{(1)} M_2^{(2)} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

The above given sparse matrix method enables one to compute the Walsh spectrum of the sign function using only $n2^n$ operations [21].

4. Correlation Immune Boolean Functions

Correlation immune functions were introduced by Siegenthaler [40] in order to protect some shift register based on stream ciphers against correlation attacks.

4.1. Basic Properties

Definition 4.1. *[40] A Boolean function f in n variables is said to be correlation immune of order k, $1 \leq k \leq n$, if for any fixed subset of k variables the probability that, given the value of $f(x)$, the k variables have any fixed set of values, is always 2^{-k}, no matter what the choice of the fixed set of k values is. In other words, f is correlation immune of order k if its values are statistically independent of any subset of k input variables.*

We can formulate the definition of correlation immunity to an equivalent information theory condition.
If the chosen subset of k variables is $\{x(i_1), x(i_2), \ldots, x(i_k)\}$, then the above definition of correlation immunity of order k is equivalent to the information theory condition that the information obtained about the values of $x(i_1), x(i_2), \ldots, x(i_k)$ given $f(x)$ is zero.

Now we collect some useful equivalent conditions to correlation immunity of order 1 given by [10].

Lemma 4.2. *A function f in n variables is correlation immune of order 1 if and only if any of the following conditions hold.*

(i) *If* $\mathrm{supp}(f) = \{x \in \mathbb{F}_2^n | f(x) = 1\}$, *then for each* $1 \leq i \leq n$, *we have* $|\{x \in \mathrm{supp}(f) | x_i = 1\}| = \frac{|\mathrm{supp}(f)|}{2}$.

(ii) *For each* $1 \leq i \leq n$, $f(x) \oplus x_i$ *is a balanced function.*

(iii) *For each* $1 \leq i \leq n$, $\Pr(x_i = 1 | f(x) = 1) = \frac{1}{2} = \Pr(x_i = 0 | f(x) = 1)$.

(iv) *Let* f_{0i} *and* f_{1i} *denote the functions in* $n-1$ *variables obtained from* f *by setting* $x_i = 0$ *or* 1, *respectively. Then for each* $i = 1, \ldots, n$, *the functions* f_{0i} *and* f_{1i} *have the same Hamming-weight.*

(v) *All the Walsh transforms*

$$W(\widehat{f})(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus \langle u, x \rangle}, \quad wt(u) = 1,$$

are equal to zero.

(vi) For each $i = 1, 2, \ldots, n$, $\Pr(f(x) = 1 | x_i = 1) = \Pr(f(x) = 1 | x_i = 0) = \frac{wt(f)}{2^n}$

Example 8. We take the following 3-variable Boolean function $f(x) = x_1 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus 1$. Thus, we obtain the truth table

$x \in \mathbb{F}_2^3$	$f(x)$
000	1
001	1
010	1
011	0
100	0
101	1
110	1
111	1

We use lemma 4.2 (v) and compute all Walsh-coefficients with $wt(u) = 1$. Hence, we obtain that all Walsh-coefficients are equal zero. Therefore, the given Boolean function is correlation immune of order 1.

Furthermore, we give an extension of lemma 4.2(v) with a short proof given by Brynielsson as reported in Simmons [41].

Lemma 4.3. *A function f in n variables is correlation immune of order k, $1 \leq k \leq n$, if and only if all of the Walsh transforms*

$$W(\widehat{f})(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus \langle u, x \rangle}, \;\; 1 \leq wt(u) \leq k,$$

are equal zero.

Proof. The proof is based on the fact that the Walsh transform $W(\widehat{f})(u)$ is the cross correlation between f and the linear function α_u. Let the k-vector y be defined by

$$y = (x(i_1), x(i_2), \ldots, x(i_k)),$$

where $x(i_1), x(i_2), \ldots, x(i_k)$ are the variables in α_u. Then we focus on the Walsh transform in k variables of the conditional probability $\Pr(y|z)$, where z is a possible value of $f(x)$. By the definition of the expectation follows

$$\sum_y \Pr(y|z)(-1)^{\langle u,x \rangle} = E[(-1)^{\langle u,x \rangle} | f(x) = z] = E[(-1)^{\langle u,x \rangle}] = \sum_y \Pr(y)(-1)^{\langle u,x \rangle}.$$

The equality follows by our correlation immunity hypothesis. Thus, $\Pr(y|z)$ and $\Pr(y)$ are identical since their Walsh transforms are identical. Consequently, the cross correlation between $f(x)$ and $\alpha_u(x)$ is zero, which gives the statement. □

It follows from lemma 4.3 that the functions $f(x)$ and $\alpha_u(x)$ are statistically independent if and only if the Walsh transform $W(\widehat{f})(u) = 0$.

Remark. We note that the original proof was given by Xiao and Massey [46]. Sarkar [37] gave another noteworthy proof which is based on linear algebra and combinatorics.

Now, we obtain the correlation value $c(f, \alpha_u)$. Therefore, we recall that the Hamming-distance between two Boolean functions $f, g\colon \mathbb{F}_2^n \to \{1, -1\}$ is tied up with the cross correlation between f and g which is defined as

$$c(f, g) = \frac{\#\{x \in \mathbb{F}_2^n | f(x) = g(x)\} - \#\{x \in \mathbb{F}_2^n | f(x) \neq g(x)\}}{2^n}.$$

Now we use an arbitrary linear function α_u. Hence, we get

$$c(f, \alpha_u) = 2^{-n} W(\widehat{f})(u). \tag{4.1}$$

Thus, lemma 4.3 states that achieving correlation immunity for f is the same as getting zero correlation of f with certain linear functions α_u. It is impossible to guarantee that f will not have a nonzero correlation with any linear function. This means we cannot achieve $c(f, \alpha_u) = 0$ for every u. This follows from the following lemma, which was first proven by Meier and Staffelbach [26].

Lemma 4.4. *For any Boolean function f the total square correlation of f with the set of all linear functions is equal to one, that is*

$$\sum_{u \in \mathbb{F}_2^n} c(f, \alpha_u)^2 = 1.$$

Proof. By equation (4.1) we have

$$\sum_{u \in \mathbb{F}_2^n} c(f, \alpha_u)^2 = 2^{-2n} \sum_{u \in \mathbb{F}_2^n} W(\widehat{f})(u)^2,$$

then using Parseval's equation (3.6) and the statement follows immediately. □

As a result of lemma 4.4 and equation (4.1), we shift our focus to seeking those Boolean functions of which the largest possible value of $|W(\widehat{f})(u)|$ is as small as possible. These functions are the so-called **perfect nonlinear functions** which were introduced by Meier and Staffelbach [26]. It is a well-known result that the class of perfect nonlinear functions coincides with the class of bent functions. This result can be found in 6.19.

4.2. Construction of Correlation Immune Functions

In this section we observe methods to construct correlation immune functions. First, we adopt a terminology which was introduced by Chor et al. [9].

Definition 4.5. *A Boolean function in n variables which is balanced and correlation immune of order k is said to be a k-resilient function.*

Example 9. We consider $\mathbb{F}_2^4$ and take the Boolean function $f(x) = x_1 \oplus x_2 \oplus x_3$. It is easy to verify that the function is balanced and correlation immune of order 2. Altogether, it follows that the function is a 2-resilient function.

Resiliency has been characterized by Xiao and Massey [46] through the Walsh transform.

Theorem 4.6. *Any Boolean function in n variables is k-resilient if and only if* $W(\widehat{f})(u) = 0$ *for all* $u \in \mathbb{F}_2^n$ *such that* $wt(u) \leq k$. *Equivalently, f is k-resilient if and only if it is balanced and* $W(f)(u) = 0$ *for all* $u \in \mathbb{F}_2^n$ *such that* $0 < wt(u) \leq k$.

Proof. See [2]. □

Before we start to construct correlation immune functions we recall that a Boolean function cannot simultaneously have too many cryptographically desirable properties. Siegenthaler [40] introduced a useful theorem which describes the relation between high order correlation immunity and high algebraic degree for a Boolean function, and we follow the more simple proof of Sarkar [10].

Theorem 4.7. *If f is a Boolean function in n variables, which is correlation immune of order k, then the degree of f is at most* $n - k$. *If f is also balanced and* $k < n - 1$, *then the degree is at most* $n - k - 1$.

Proof. A truth table for $f(x_1, \ldots, x_n)$ is an array with 2^n rows and $n + 1$ columns. Clearly, each of the first n columns has values for one of the variables x_i and the first n entries of the 2^n rows are the coordinates of all n-vectors in lexicographical order. The last column gives the output values $f(x_1, \ldots, x_n)$.

Let f be correlation immune of order k. If we choose any k variables and make these the leftmost ones in the truth table, then the last column of the truth table is the concatenation of 2^k strings of the length 2^{n-k} and of equal Hamming-weight (follows from generalization to order k of lemma 4.2(iv)). Now we suppose that the degree of f is $n - i$ for some $i < k$ and deduce a contradiction.

Since f is correlation immune of order k, it is also correlation immune of order i and $i + 1$. Also, by our assumption, the algebraic normal form has at least one term T of degree $n-i$ while having no terms of greater degree. Let $y_1, \ldots, y_i$ be the variables not in T and let y be any other variable from $\{x_1, \ldots, x_n\} - \{y_1, \ldots y_i\}$. We arrange the truth table for f so that the variables $y_1, \ldots, y_i, y$ appear as the leftmost variables in this order. This gives a division of the output column into 2^{i+1} strings $\sigma(0), \sigma(1), \ldots \sigma(2^{i+1} - 1)$ in which all Hamming-weights are equal. We define the strings $g(j) = \sigma(2j)\sigma(2j + 1)$ for all $0 \leq j \leq 2^i - 1$. Then

$$wt(g(j)) = wt(\sigma(2j)) + wt(\sigma(2j + 1)) = 2wt(\sigma(2j))$$

and therefore $wt(g(j))$ must be even. The string $g(0)$ of even Hamming-weight is a function of $n-i$ variables and is obtained from f by setting the variables $y_1, \ldots, y_i$ equal to 0. The term T does not contain any of the variables $y_1, \ldots, y_i$ and must thus be in the algebraic normal form of $g(0)$. Hence, $g(0)$ represents a function of $n-i$ variables with degree $n-i$. Consequently, this function must have odd Hamming-weight, which is a contradiction. Thus, the degree equals $n-k$.

Next, we suppose that f is balanced and has degree $n-k$ for $k < n-1$. Let T be a term of degree $n-k$ and let $y_1, \ldots, y_k$ be the variables not in T. If these variables are made the leftmost variables in the truth table for f, then the output column can be divided into 2^k strings $\sigma(0), \sigma(1), \ldots \sigma(2^k-1)$ in which the Hamming-weights are equal. Each of these functions has $n-k$ variables and contains the term T. Hence, each function has degree $n-k$ and odd Hamming-weight. Let w be the common Hamming-weight of all strings. Therefore, we have $wt(f) = 2^k w$ with w odd. However, f is balanced and hence $wt(f) = 2^{n-1}$. Thus, $w = 2^{n-k-1}$ which is even for $k < n-1$. This is a contradiction. Thus, the degree is equal to $n-k-1$. □

In the context of counting correlation immune functions Mitchell [29] mentioned a very simple method for constructing correlation immune functions of order 1. We define the first half $(f(a_0), \ldots, f(a_{2^{n-1}-1}))$ of the function arbitrarily and then we define the second half of the function by taking the bits of the first half in reverse order. By using lemma 4.2(i) the function f is correlation immune.
The disadvantage of such a construction is that these functions are not useful for cryptographic applications because it is not easy to obtain other cryptographic properties such as high nonlinearity. Therefore, we need more specialized constructions which are more useful for cryptographic applications. Siegenthaler [40] gives a recursive construction for correlation immune functions of order k as follows:

Theorem 4.8. *Let $x = (x_1, \ldots, x_n)$ and suppose that $f_1(x)$ and $f_2(x)$ are correlation immune functions of order k such that $\Pr(f_1(x) = 1) = \Pr(f_2(x) = 1) = p$. Then the function f of $n+1$ variables defined by*

$$f(x, x_{n+1}) = (x_{n+1} \oplus 1) f_1(x) \oplus x_{n+1} f_2(x) \tag{4.2}$$

is also correlation immune of order k and satisfies $\Pr(f(x) = 1) = p$.

Proof. Let $y = (x_{i(1)}, \ldots, x_{i(k)})$ be made up of an arbitrary choice of k of the variables x_i and let $y_0 = (y_1, \ldots, y_k)$ be any fixed binary k-vector. Since f_1 and f_2 are independent of x_{n+1} we have either fixed choice of the bit b and $i = 1$ or 2

$$\Pr(f_i = 1 | y = y_0, x_{n+1} = b) = \Pr(f_i = 1 | y = y_0) = \Pr(f_i = 1), \tag{4.3}$$

where the second equality follows from the hypothesis that f_i is correlation immune of order k. Equations (4.2) and (4.3) imply

$$\Pr(f_i = 1 | y = y_0, x_{n+1} = 1) = \Pr(f_1 = 1)$$

and

$$\Pr(f_i = 1 | y = y_0, x_{n+1} = 0) = \Pr(f_2 = 1).$$

The two right-hand-side probabilities are equal to p due to our hypotheses. Therefore, we obtain

$$\Pr(f_i = 1 | y = y_0, x_{n+1} = b) = \Pr(f = 1) = p.$$

This implies that the value of f is independent of the choice of any subset of k of the $n+1$ input variables. Thus, f is correlation immune of order at least k. □

Remark. We note that the correlation immunity order is not increased in this construction.

From a cryptographic viewpoint, theorem 4.8 is most interesting when $p = \frac{1}{2}$. The result of which is that f_1 and f_2 are k-resilient. In this case Camion et al. [1] provide a more precise formulation of theorem 4.8.

Theorem 4.9. *Let $x = (x_1, \ldots, x_n)$ and suppose that $f_1(x)$, $f_2(x)$ and $f(x, x_{n+1})$ are related by equation (4.2). Then for $k < n-1$, f is $(k+1)$-resilient if and only if the following two conditions hold:*

(i) f_1 and f_2 are k-resilient functions

(ii) for all $v \in \mathbb{F}_2^n$ with $wt(v) = k+1$ we have the Walsh transform equation

$$W(f_1)(v) + W(f_2)(v) = 0. \tag{4.4}$$

Also, if the degrees of f, f_1 and f_2 are equal (thus, the degree of $f_1 + f_2$ is less than the degree of f), then f has its maximum degree $n+1-(k+2)$ if and only if f_1 and f_2 have their maximum degree $n-(k+1)$.

Proof. Let $w = (v, d)$ be a vector in $\mathbb{F}_2^{n+1}$. Let $x = (x_1, \ldots, x_n)$. We obtain

$$\begin{aligned} W(f)(w) &= \sum_{(x, x_{n+1}) \in \mathbb{F}_2^{n+1}} f(x, x_{n+1}) \cdot (-1)^{\langle v, x \rangle \oplus d \cdot x_{n+1}} \\ &= \sum_{x \in \mathbb{F}_2^n, x_{n+1} = 0} f_1(x) \cdot (-1)^{\langle v, x \rangle} + \sum_{x \in \mathbb{F}_2^n, x_{n+1} = 1} f_2(x) \cdot (-1)^{\langle v, x \rangle \oplus d} \\ &= W(f_1)(v) + (-1)^d W(f_2)(v). \end{aligned} \tag{4.5}$$

First, we suppose that f satisfies (i) and (ii). Then from equation (4.5) and (i) we have

$$W(f)(0) = W(f_1)(0) + (-1)^0 W(f_2)(0) = 2^n,$$

therefore, f is balanced. If $w = (v, d)$ and $0 < wt(v) < k+1$, then we obtain by equation (4.5) and (i) that $W(f)(w) = 0$. Furthermore, if $w = (v, d)$ with $wt(v) = k+1$ and

$d = 0$, then we obtain by equation (4.5) and (ii) that $W(f)(w) = 0$. Hence, we have that f is $(k+1)$-resilient.

Conversely, we suppose that f is $(k+1)$-resilient. Then for all $w = (v, d)$ such that $1 \leq wt(w) \leq k+1$, equation (4.5) yields to

$$0 = W(f_1)(v) + (-1)^d W(f_2)(v). \tag{4.6}$$

For $w = (0, 1)$, equation (4.6) gives $W(f_1)(v) = W(f_2)(v)$. Since f is balanced for $w = 0$, equation (4.5) gives $W(f)(0) = wt(f) = 2^n = W(f_1)(0) + W(f_2)(0)$. Thus f_1 and f_2 are balanced.

If $0 < wt(v) < k+1$, then we obtain by equation (4.6) that $W(f_1)(v) = W(f_2)(v)$ for $d = 1$ and $W(f_1)(v) = -W(f_2)(v)$ for $d = 0$. Therefore, $W(f_1)(v) = W(f_2)(v) = 0$, so (i) is satisfied.

If $wt(v) = k+1$ and $d = 0$, then we obtain (ii) from (4.6).

The last statement of the theorem follows immediately from equation (4.2) and theorem 4.7. Each function f_1 and f_2 is k-resilient and have degree at most $n - (k+1)$. Using equation (4.2) we deduce that f has its maximum degree $n + 1 - (k+2)$. □

5. Avalanche and Propagation Criterion

The *Strict Avalanche Criterion* (*SAC* for short) was introduced by Webster and Tavares [44]. They write [44]: " If a function is to satisfy the strict avalanche criterion, then each of its output bits should change with a probability of one half whenever a single input bit x is complemented to $\overline{x}$."
The *SAC* is a useful property for Boolean functions in cryptographic applications. This means that if a Boolean function is satisfying the *SAC*, a small change in the input leads to a large change in the output (an avalanche effect). This property is essential in a cryptographic context due to the fact that we cannot infer its input from its output. In addition to *SAC* we study the so-called *Propagation Criterion* (*PC* for short) which was introduced by Preneel et al. [34].

5.1. The Strict Avalanche Criterion

Definition 5.1. *A Boolean function f in n variables is said to satisfy the* **Strict Avalanche Criterion** if changing any one of the n bits in the input x results in the output of the function being changed for exactly half of the 2^{n-1} vectors x with the changed input bit.

This property has an obvious desirability. Since knowing the function value for a given input an attacker does not gain any information about the function value of a slightly different input value.

We introduce the important notation of the directional derivative.

Definition 5.2. *For $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ and $a \in \mathbb{F}_2^n$, $a \neq 0$, we define the function $f_a\colon \mathbb{F}_2^n \to \mathbb{F}_2$ by*

$$f_a(x) = f(x) \oplus f(x \oplus a).$$

f_a is called the ***directional derivative*** *of f in the direction a.*

Now we are able to express the SAC in connection with the directional derivative.

Lemma 5.3. *A Boolean function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ satisfies the SAC if and only if the function $f(x) \oplus f(x \oplus a)$ is balanced for every a in $\mathbb{F}_2^n$ with Hamming-weight 1.*

Proof. We assume that f fulfills the SAC, then exactly half of the $x \in \mathbb{F}_2^n$ satisfy $f(x) \neq f(x \oplus a)$ for every $a \in \mathbb{F}_2^n$ with $wt(a) = 1$. This means that

$$f(x) \oplus f(x \oplus a) = 1 \text{ for half the } x \in \mathbb{F}_2^n, \text{ and}$$
$$f(x) \oplus f(x \oplus a) = 0 \text{ for the other half.}$$

Summing up over $x \in \mathbb{F}_2^n$ leads us to $\sum_{x \in \mathbb{F}_2^n} f(x) \oplus f(x \oplus a) = 2^{n-1}$. So, $f(x) \oplus f(x \oplus a)$ is balanced. For the converse we reverse the arguments. □

Lemma 5.3 provides a straightforward way to verify the SAC by computation the output values of f.

Let us focus on an example of a SAC function.

Example 10. We take the 3-variables Boolean function $f(x) = x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_1 \oplus 1$. Clearly, the vectors with Hamming-weight one are the three unit-vectors in $\mathbb{F}_2^3$. So we compute the following table.

$x \in \mathbb{F}_2^3$	$f(x)$	$f(x \oplus e_1)$	$f(x \oplus e_2)$	$f(x \oplus e_3)$
000	1	0	1	1
001	1	1	0	1
010	1	1	1	0
011	0	1	1	1
100	0	1	1	1
101	1	1	1	0
110	1	1	0	1
111	1	0	1	1

Next we compute the values for $f(x) \oplus f(x \oplus e_i)$ for $i \in \{1, 2, 3\}$.

$x \in \mathbb{F}_2^n$	$f(x) \oplus f(x \oplus e_1)$	$f(x) \oplus f(x \oplus e_2)$	$f(x) \oplus f(x \oplus e_3)$
000	1	0	0
001	0	1	0
010	0	0	1
011	1	1	1
100	1	1	1
101	0	0	1
110	0	1	0
111	1	0	0

By lemma 5.3, we see that the Boolean function fulfills the SAC because for each $i \in \{1, 2, 3\}$, $f(x) \oplus f(x \oplus e_i)$ is balanced.

Furthermore, we give an alternative formulation of lemma 5.3 using the autocorrelation function in a slightly different way as in definition 2.14

Definition 5.4. *The autocorrelation function of a Boolean function in n variables is defined as*

$$r_f(a) = \sum_{i=0}^{2^n-1} f(v_i) \oplus f(v_i \oplus a),$$

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

The autocorrelation function is simply the sum over all values of the directional derivative $f(x) \oplus f(x \oplus a)$ as x runs through $\mathbb{F}_2^n$.

Now we are able to restate lemma 5.3 in terms of the autocorrelation function.

Lemma 5.5. *A Boolean function f in n variables is SAC if and only if the autocorrelation function* $r_f(a)$ *is equal to* 2^{n-1} *for all* $a \in \mathbb{F}_2^n$ *with Hamming-weight* 1.

5.2. The Strict Avalanche Criterion of Higher Order

In this section we study a generalization of the SAC defined by Forré [14], which she named the SAC of higher order.

Definition 5.6. *A Boolean function* $f(x)$ *in n variables is said to satisfy the* Strict Avalanche Criterion of order k (*SAC(k)* for short) if fixing any k of the n bits in the input x results in a Boolean function in the remaining $n-k$ variables which satisfies the SAC, where $0 \leq k \leq n-2$.

It is required that $0 \leq k \leq n-2$ since the SAC is not defined for 1-variable functions. A function which satisfies the SAC as originally defined is a $SAC(0)$ function.
Forré did not notice that if a function is $SAC(k)$ for $k > 0$, then it is also $SAC(j)$ for any $j = 0, 1, \ldots, k-1$. This was pointed out by Lloyd [19].

Lemma 5.7. *Suppose f is a Boolean function in* $n > 2$ *variables which satisfies the SAC of order k,* $1 \leq k \leq n-2$. *Then f also satisfies the SAC of order j for any* $j = 0, 1, \ldots, k-1$.

Proof. We prove that if f satisfies the SAC of order k, then f also satisfies the SAC of order $k-1$. The proof follows by induction.
The base step is trivial. For the inductive step, let g be a function in $n-k+1$ variables obtained by fixing $k-1$ variables in f. We need to prove that g is a SAC function. By lemma 5.3 it suffices to show

$$S = \sum_{i=0}^{2^{n-k+1}-1} g(v_i) \oplus g(v_i \oplus a) = 2^{n-k}, \tag{5.1}$$

for all $a \in \mathbb{F}_2^{n-k+1}$ with Hamming-weight 1. Without loss of generality, we may take $a = (0, \ldots, 0, 1)$. Thus, v_i and $v_i \oplus a$ have the same first bit, so we may split the above sum S into two sums. One sum in which the first bit of v_i is zero and one sum in which the first bit is one. Then we denote with g_0 and g_1 the functions obtained from g by fixing the first input bit as 0 and 1, respectively, and let a^* be the vector made up of the least $n-k$ significant bits of a. Then we have

$$S = \sum_{i=0}^{2^{n-k}-1} g_0(v_i) \oplus g_0(v_i \oplus a^*) \oplus \sum_{i=0}^{2^{n-k}-1} g_1(v_i) \oplus g_1(v_i \oplus a^*).$$

Both g_0 and g_1 are obtained from f by fixing k variables, so by hypothesis they are both SAC functions. Therefore, both of the above sums are 2^{n-k-1}, and this proves equation (5.1). □

Lemma 5.8. *If f is a Boolean function in $n > 2$ variables and $deg(f) = n$, then $r_f(a)$, as defined in definition 5.4, does not take on the value 2^{n-1} for any $a \in \mathbb{F}_2^n$.*

This lemma is needed to prove the next corollary which is given by Preneel et al. [34].

Corollary 5.9. *If f is a Boolean function in $n > 2$ variables and $deg(f) = n$, then f does not satisfy the SAC.*

Proof. We prove that if $r_f(a) = 2^{n-1}$ for some $a \in \mathbb{F}_2^n$, then the Hamming-weight $wt(f)$ is even. This is a contradiction since $deg(f) = n$ implies that $wt(f)$ is odd, cf. lemma 5.8. We suppose that $r_f(a) = 2^{n-1}$. Then

$$\begin{aligned} wt(f) \equiv \sum_{i=0}^{2^n-1} f(v_i) &\equiv \sum_{i=0}^{2^n-1} f(v_i \oplus a) \\ &\equiv \frac{1}{2} \sum_{i=0}^{2^n-1} f(v_i) \oplus f(v_i \oplus a) \\ &\equiv \frac{r_f(a)}{2} \equiv 2^{n-2} (\text{mod } 2). \end{aligned}$$

Since $n > 2$, we have that $wt(f)$ is even and the contradiction follows. Then using lemma 5.8 and it follows that f does not satisfy the SAC. □

Now we turn to the issue of counting SAC functions. First, we shall prove a result conjectured by Forré [14].

Theorem 5.10. *There are 2^{n+1} $SAC(n-2)$ Boolean functions in n variables.*

To prove the theorem we need the following lemma.

Lemma 5.11. *Suppose $n \in \mathbb{Z}$, $n \geq 2$ and $f \colon \mathbb{F}_2^n \to \mathbb{F}_2$. Then f satisfies the SAC of order $(n-2)$ if and only if for all $S \subseteq \{1, 2 \ldots, n\}$,*

$$\widehat{f}(e_S) = (-1)^{\frac{|S|(|S|-1)}{2}} (\widehat{f}(0))^{(|S|+1)} \prod_{r \in S} \widehat{f}(e_{\{r\}}),$$

where e_S denotes the element of $\mathbb{F}_2^n$ which satisfies $e_i = 1 \Leftrightarrow i \in S$.

Proof. See [19]. □

Proof of theorem 5.10. By lemma 5.11, the set of functions $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ satisfying the SAC of order $(n-2)$ is the same as the set of functions $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ satisfying the set of equations

$$\widehat{f}(e_S) = (-1)^{\frac{|S|(|S|-1)}{2}} (\widehat{f}(0))^{(|S|+1)} \prod_{r\in S} \widehat{f}(e_{\{r\}}),$$

with the notation of lemma 5.11.
Now, since we can write any element in $\mathbb{F}_2^n$ as e_S for exactly one set $S \subseteq \{1, 2, \ldots n\}$, this determines the value of $g(x)$ for all values of x with Hamming-weight greater than 1 in terms of the values of $g(x)$ for values of x with Hamming-weight less than or equal to 1. In other words, if we choose values for $g(0)$ and for $g(e_{\{r\}})$ for all $r \in \{1, \ldots, n\}$, then g is completely determined on the whole of $\mathbb{F}_2^n$. Thus, there are 2^{n+1} ways to choose such a function, and so the size of the set of these functions is 2^{n+1}. □

Next, we turn to the problem of counting balanced functions satisfying SAC of higher order. Lloyd [20] first solved the problem but we follow a different approach based on the paper of Gopalakrishnan and Stinson [15].
Lloyd characterized SAC functions in terms of their algebraic normal form of the function f. Thus, a function f in $n \geq 2$ variables satisfies the SAC of order $(n-2)$ if and only if the algebraic normal form is

$$f(x) = a_0 \oplus a_1 x_1 \oplus \cdots \oplus a_n x_n \oplus \sum_{1\leq i<j\leq n} x_i x_j, \tag{5.2}$$

for some $a_0, a_1, \ldots a_n \in \mathbb{F}_2^n$.
Now, we proceed to simplify the ANF without loss of generality since $f(x)$ is balanced if and only if $f(x) \oplus 1$ is balanced. Hence, we may assume that $a_0 = 0$.
We suppose that exactly r of the coefficients $a_1, a_2, \ldots a_n$ are ones and the rest are equal to zero. Let $S_{n,r}$ denote the number of vectors $x \in \mathbb{F}_2^n$ such that $f(x) = 0$, where $0 \leq r \leq n$. The next lemma gives a recurrence relation for $S_{n,r}$.

Lemma 5.12. *For $n \geq 2$ and $0 \leq r \leq n$ we have*

$$S_{n,r} = S_{n-1,r} + S_{n-1,r-1}. \tag{5.3}$$

Proof. Renumbering the variables does not affect whether a function is balanced or not, so we may reduce (5.2) to

$$f(x) = x_1 \oplus \cdots \oplus x_r \oplus \sum_{1\leq i<j\leq n} x_i x_j, \tag{5.4}$$

for some n, $0 \leq r \leq n$.
Any vector $x \in \mathbb{F}_2^n$ has either $x_{r+1} = 0$ or $x_{r+1} = 1$. We suppose that $x_{r+1} = 0$, then the function f reduces to a function $g_0\colon \mathbb{F}_2^{n-1} \to \mathbb{F}_2$ of which the ANF is

$$g_0(x) = x_1 \oplus \cdots \oplus x_r \oplus \sum_{\substack{1\leq i<j\leq n,\\ i,j\neq r+1}} x_i x_j,$$

and the number of vectors in $\mathbb{F}_2^{n-1}$ such that $g_0(x) = 0$ is $S_{n-1,r}$. Furthermore, we suppose that $x_{r+1} = 1$, then the ANF of the induced function $g_1 \colon \mathbb{F}_2^{n-1} \to \mathbb{F}_2$ is

$$\begin{aligned} g_1(x) &= x_1 \oplus \cdots \oplus x_r \oplus \sum_{\substack{1 \le i \le n, \\ i \ne r+1}} x_i \oplus \sum_{\substack{1 \le i < j \le n, \\ i,j \ne r+1}} x_i x_j \\ &= x_{r+2} \oplus x_{r+3} \oplus \cdots \oplus x_n \oplus \sum_{\substack{1 \le i < j \le n, \\ i,j \ne r+1}} x_i x_j, \end{aligned}$$

and the number of vectors in $\mathbb{F}_2^{n-1}$ such that $g_1(x) = 0$ is $S_{n-1,n-r-1}$. Thus, we have

$$S_{n,r} = S_{n-1,r} + S_{n-1,n-r-1}. \tag{5.5}$$

Using the recurrence relation (5.5) to evaluate $S_{n-1,n-r-1}$ we get

$$\begin{aligned} S_{n-1,n-r-1} &= S_{n-2,n-r-1} + S_{n-2,n-1-(n-r-1)-1} \\ &= S_{n-2,n-r-1} + S_{n-2,r-1} \\ &= S_{n-2,r-1} + S_{n-2,(n-1)-(r-1)-1} \\ &= S_{n-1,r-1}. \end{aligned}$$

Substituting this back into (5.5) gives (5.3). □

Subsequently, we derive expressions for the boundary conditions $S_{n,0}$ and $S_{n,n}$. If $r = 0$, the ANF (5.4) reduces to

$$f(x) = \sum_{1 \le i < j \le n} x_i x_j. \tag{5.6}$$

We note that the equation (5.6) is symmetric in the n input bits and hence, the value of $f(x)$ depends only on the Hamming-weight of x. If the Hamming-weight is equal to k, then

$$wt(f(x)) = \binom{k}{2} \equiv f(x) \mod 2.$$

Since $\binom{k}{2} \equiv 0 \mod 2$ if and only if $k \equiv 0, 1 \mod 4$, we have

$$S_{n,0} = \sum_{\substack{0 \le k \le n \\ k \equiv 0,1 \mod 4}} \binom{n}{k}. \tag{5.7}$$

Now, when $r = n$, the ANF (5.4) reduces to

$$f(x) = x_1 \oplus \cdots \oplus x_n \oplus \sum_{1 \le i < j \le n} x_i x_j. \tag{5.8}$$

Once again we observe that equation (5.8) is symmetric in the n input bits and hence, we have that the value of $f(x)$ depends only on the Hamming-weight of x. If the Hamming-weight is equal to k, then

$$wt(f(x)) = k + \binom{k}{2} \equiv f(x) \mod 2.$$

Since $k + \binom{k}{2} \equiv 0 \mod 2$ if and only if $k \equiv 0, 3 \mod 4$, we have

$$S_{n,n} = \sum_{\substack{0 \le k \le n, \\ k \equiv 0,3 \mod 4}} \binom{n}{k}. \tag{5.9}$$

The recurrence relation (5.3) with the boundary conditions (5.7) and (5.9) completely describes $S_{n,r}$ for $n \ge 1$ and $0 \le r \le n$. The next theorem gives an explicit formula for $S_{n,r}$. Prior to this we need the following lemma on binomial coefficients.

Lemma 5.13. *We have the following identities:*

$$\sum_{\substack{0 \le k \le n, \\ k \equiv 0 \mod 4}} \binom{n}{k} = 2^{n-2} + 2^{\frac{n-2}{2}} \cos\left(\frac{n\pi}{4}\right)$$

$$\sum_{\substack{0 \le k \le n, \\ k \equiv 1 \mod 4}} \binom{n}{k} = 2^{n-2} + 2^{\frac{n-2}{2}} \sin\left(\frac{n\pi}{4}\right)$$

$$\sum_{\substack{0 \le k \le n, \\ k \equiv 3 \mod 4}} \binom{n}{k} = 2^{n-2} - 2^{\frac{n-2}{2}} \sin\left(\frac{n\pi}{4}\right)$$

Theorem 5.14. *For $n \ge 2$ and $0 \le r \le n$ we have*

$$S_{n,r} = 2^{n-1} - 2^{\frac{n-1}{2}} \sin\left(\left(r + \frac{7n-1}{2}\right)\frac{\pi}{2}\right). \tag{5.10}$$

Proof. From lemma 5.13, the two conditions (5.7) and (5.9) become

$$S_{n,0} = 2^{n-1} + 2^{\frac{n-2}{2}} \left(\cos\left(\frac{n\pi}{4}\right) + \sin\left(\frac{n\pi}{4}\right)\right) \tag{5.11}$$

$$S_{n,n} = 2^{n-1} + 2^{\frac{n-2}{2}} \left(\cos\left(\frac{n\pi}{4}\right) - \sin\left(\frac{n\pi}{4}\right)\right). \tag{5.12}$$

If $r = 0$, equation (5.11) is the same as equation (5.10); and if $r = n$, equation (5.12) is the same as equation (5.10).
An easy computation shows that $S_{n,r}$ as given in (5.10) satisfies the recurrence relation (5.3), and this suffices the theorem. □

Now we are able to prove the main result on counting SAC functions given by Forré [20].

Theorem 5.15. *If n is even, then there are no balanced $SAC(n-2)$ functions in n variables.*
If n is odd, then exactly the half of the 2^{n+1} $SAC(n-2)$ functions in n variables are balanced.

Proof. With no loss of generality we can reduce the function to the form (5.4). The function f is balanced if and only if $S_{n,r} = 2^{n-1}$. By theorem 5.14, this is true if and only if

$$\sin\left(\left(r + \frac{7n-1}{2}\right)\frac{\pi}{2}\right) = 0. \tag{5.13}$$

Now, (5.13) holds if and only if $r + \frac{7n-1}{2}$ is an even integer, which is impossible for n even, since then we do not have an even integer. If n is odd, then we get an even integer for exactly the half of the $n+1$ values $r = 0, 1, \ldots, n$, namely, even r if $\frac{7n-1}{2}$ is even, that is if $n \equiv 3 \mod 4$; and odd r if $\frac{7n-1}{2}$ is odd, that is if $n \equiv 1 \mod 4$. □

5.3. The Propagation Criterion

This section generalizes the notion of the strict avalanche criterion to the propagation criterion.

Definition 5.16. *A Boolean function f in n variables is said to satisfy the propagation criterion of degree k ($PC(k)$ for short) if changing any i ($1 \leq i \leq k$) of the n bits in the input x results in the output of the function being changed for exactly half of the 2^n vectors x.*

By definition, we conclude that SAC is identical to PC(1). The function given in example 10 satisfies PC(2).

The propagation criterion is strongly connected to properties of the autocorrelation function $r_f(a)$ as defined in definition 5.4.

Lemma 5.17. *A Boolean function f in n variables satisfies $PC(k)$ if and only if all of the given values*

$$r_f(a) = \sum_{x \in \mathbb{F}_2^n} f(x) \oplus f(x \oplus a), \quad 1 \leq wt(a) \leq k,$$

of the autocorrelation function are equal 2^{n-1}.

Proof. From the definition of the autocorrelation function $r_f(a)$ we have

$$Pr(f(x) \neq f(x \oplus a)) = \frac{r_f(a)}{2^n} = \frac{1}{2},$$

so the statement follows from the definition of the $PC(k)$. □

The next lemma restates lemma 5.17 in terms of these directional derivatives (5.2).

Lemma 5.18. *A Boolean function f in n variables satisfies $PC(k)$ if and only if all directional derivatives*

$$f_a(x) = f(x) \oplus f(x \oplus a), \;\; 1 \leq wt(a) \leq k,$$

are balanced functions.

Proof. With lemma 5.17 and the definition of $PC(k)$ the statement follows immediately. □

The following lemma shows the connection that if f satisfies the propagation criterion, then also the concatenation of f with any affine function satisfies the propagation criterion of the same degree.

Lemma 5.19. *If a Boolean function f in n variables satisfies $PC(k)$ for some k, $1 \leq k \leq n$, then so does $f \oplus g$, where g is any affine function in n variables.*

5.4. The Propagation Criterion of Higher Order

We can generalize the definition of high order SAC given in section 5.2 to define high order propagation criterion. The following definitions were introduced by Preneel et al. [34].

Definition 5.20. *A Boolean function f in n variables is said to satisfy the propagation criterion of degree k and order m if $k + m \leq n$ and fixing any m of the n bits in the input x results in a Boolean function in the remaining $n - m$ variables which satisfies $PC(k)$. For brevity, we may say that such a function is $PC(k)$ of order m.*

Clearly, the condition $k + m \leq n$ is imposed because if m bits are fixed, there are only $n - m$ variable bits left which can be changed, as the definition of $PC(k)$ requires. If we removed the condition $k + m \leq n$, we could allow m bits to be fixed and the subsequently k bits to be changed.

Definition 5.21. *A Boolean function f in n variables is said to satisfy the* ***extended propagation criterion*** *of degree k and order m (EPC(k) of order m for short) if knowledge of m bits of x gives no information about $f(x) \oplus f(x \oplus a)$ for all $a \in \mathbb{F}_2^n$ with $1 \leq wt(a) \leq k$.*

It follows from the above definitions and lemma 5.18 that $PC(k)$, $PC(k)$ of order 0 and $EPC(k)$ of order 0 all refer to essentially the same. A function which satisfies $PC(k)$ or $EPC(k)$ of order m also satisfy the corresponding criterion for all orders less than m.

We can use terms of correlation immunity, cf. section 4.1, to express $EPC(k)$ of order $m > 0$.

Lemma 5.22. *A Boolean function f in n variables satisfies $EPC(k)$ of order $m > 0$ if and only if all of the directional derivatives*

$$f_a(x) = f(x) \oplus f(x \oplus a), \;\; 1 \leq wt(a) \leq k,$$

are m-resilient.

Proof. The proof follows by the definitions of $EPC(k)$ of order m and correlation immunity of order m by using lemma 5.18. □

Lemma 5.23. *Let f be a Boolean function in n variables. If f satisfies $EPC(k)$ of order $m > 0$, then f satisfies $PC(k)$ of order $m > 0$. On one hand, the converse is true for $k = 1$ and any $m > 0$. On the other hand, the converse is also true for any k if $m = 1$, but is false for $k = m = 2$.*

Proof. [10] The first assertion follows from the definitions.
First, we prove the converse for $k = 1$. We observe that if f satisfies $PC(1)$ of order m, then by lemma 5.18 and 5.22 f satisfies $EPC(1)$ of order m if and only if

$$\sum_{x \in \mathbb{F}_2^n,\, x_{i(1)} = a_{i(1)}, \ldots, x_{i(m)} = a_{i(m)}} f(x) \oplus f(x \oplus e_i) = 2^{n-1} \tag{5.14}$$

for each unit vector e_i, $1 \leq i \leq n$, and for all choices of the variables $x_{i(1)}, \ldots, x_{i(m)}$ and fixed values $a_{i(1)}, \ldots, a_{i(m)}$. If none of the indices $i(j)$ equals i then, according to lemma 5.18, equation (5.14) is exactly the condition $PC(1)$ of order m. If the index $i(j)$ is equal to i, then equation (5.14) is exactly the condition for $PC(1)$ of order $m - 1$, and this is true by our assumption that f satisfies $PC(1)$ of order m.
To prove the second converse for any k if $m = 1$, the proof is similar to the one above based on equation (5.14), which is, however, more simple because one variable x_i is fixed.
Finally, we prove the converse is false for $k = m = 2$. Therefore we define the function

$$q_n = q_n(x_1, \ldots, x_n) = \sum_{1 \leq i < j \leq n} x_i x_j \tag{5.15}$$

and show that for $n \geq 4$ the function satisfies $PC(2)$ of order 2 but does not satisfy $EPC(2)$ of order 2. To verify the former condition, we need to examine the directional derivatives of q_n when any two bits are fixed. By symmetric reasons, we may suppose that the fixed bits are x_{n-1} and x_n. Therefore, the directional derivative is a function $g(x_1, \ldots, x_{n-2})$ of the form

$$g = q_{n-2} \oplus h(x_1, \ldots, x_{n-2}), \tag{5.16}$$

where h is an affine function. Now all of the directional derivatives

$$g_a(x) = g(x) \oplus g(x \oplus a), \;\; 1 \leq wt(a) \leq 2,$$

are non-constant affine functions and therefore balanced. By using lemma 5.18, q_n satisfies $PC(2)$ of order 2. However, q_n does not satisfy $EPC(2)$ of order 2 because

if $a \in \mathbb{F}_2^n$ of Hamming-weight 2 has a one in position i and j, then we write for the directional derivative of q_n

$$q_n(x) \oplus q_n(x \oplus a) = x_i \oplus x_j \oplus 1.$$

This function is correlation immune of order 1 but not of order 2. By using lemma 5.22 the function q_n does not satisfy $EPC(2)$ of order 2. □

The next target obviously is to construct $SAC(k)$ and $PC(k)$ functions. A well-known fact is that bent functions in n variables are exactly those functions which satisfy $PC(n)$ because of lemma 5.18 and theorem 6.20(vi). We will construct such functions in section 6.3.1

6. Bent Boolean Functions

In his paper [36], Rothaus introduced a class of Boolean functions which he named "bent" functions. These functions are called bent because they are as different as possible from all affine and linear functions. Bent functions have been extensively studied for their applications in cryptography and their relations in coding theory.

Definition 6.1. *A Boolean function f in n variables is called* ***bent*** *if and only if the Walsh-coefficients of $\widehat{f}$ are all $\pm 2^{\frac{n}{2}}$, that is, $W(\widehat{f})^2$ is constant.*

Remark. We immediately notice that bent functions exist only for even dimension, so that is $n = 2k$.

Let us observe two little examples about bent functions.

Example 11.

1. $f(x) = x_1x_2$ on $\mathbb{F}_2^2$. Then $W(\widehat{f})(u) = \pm 2$.
2. $f(x) = 1 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1x_4 \oplus x_2x_3 \oplus x_2x_4 \oplus x_3x_4$ on $\mathbb{F}_2^4$. Then $W(\widehat{f})(u) = \pm 4$.

Further we note the obvious fact that if f is affine, then f cannot be bent, since the spectral radius is $R_f = 2^n$.

Remark. We note that bent functions also play an important role in coding theory, especially in the area of Reed-Muller codes.

6.1. Difference Sets

A vast body of work has been devoted to the study of *difference sets*. Consequently, this section can only present some basic terminology and is thus mainly based on results from Dillon [11].

Definition 6.2. *Let G be an abelian group of order v and D a subset of G of order k. D is a (v, k, λ, n)- difference set in G if for every nonzero element g in G the equation $g = d_i - d_j$ (or $d_i d_j^{-1}$ in multiplicative notation) has exactly λ different pairs $(d_i, d_j) \in D \times D$, and we define $n = k - \lambda$.*

We note that the parameters v, k and λ cannot be independently chosen. By definition, all of the $v-1$ nontrivial elements in G are represented in λ different ways as the difference of two elements in D. Simultaneously, there are $k(k-1)$ possible different ordered pairs

of elements in D whose difference is not equal zero. Hence, the parameters of a difference set must satisfy the fundamental relation given by

$$\lambda(v-1) = k(k-1). \tag{6.1}$$

We can represent a difference set by an integer matrix $[M_D]$, the so-called *incidence matrix*.

Definition 6.3. *The* **incidence matrix** associated with the subset D is the $v \times v$-matrix $[M_D]$ with entries over $\mathbb{F}_2$ defined by

$$[M_D](x,y) = \begin{cases} 1, & \text{if } x - y \in D \\ 0, & \text{otherwise.} \end{cases}$$

As a consequence of the definition for the incidence matrix, Dillon [11] stated a helpful lemma.

Lemma 6.4. *D is a (v,k,λ,n)- difference set if and only if the incidence matrix $[M_D]$ satisfies*

$$[M_D]^2 = n \cdot I_v + \lambda J,$$

where I_v is the $v \times v$-unit matrix and J is the $v \times v$-matrix with all entries 1.

Proof. See [11]. □

The following lemma shows that the complement of a difference set is also a difference set.

Lemma 6.5. *If D is a (v,k,λ,n)- difference set in G, then its complement $\overline{D} = G - D$ is a $(v, v-k, v-2k+\lambda, n)$-difference set in G.*

Proof. We show that $[M_{\overline{D}}]$ is an incidence matrix. We get

$$\begin{aligned} [M_{\overline{D}}]^2 = (J - [M_D])^2 &= J^2 - 2[M_D]J + [M_D]^2 \\ &= vJ - 2kJ + (nI_v + \lambda J) \\ &= nI_v + (v - 2k + \lambda)J. \end{aligned}$$

Thus, $[M_{\overline{D}}]$ is an incidence matrix. Therefore, the statement follows by using lemma 6.4. □

Without loss of generality, this result allows us to assume that $k < \frac{v}{2}$. Furthermore, we are interested in a specific class of difference sets, the so-called *Hadamard difference sets*.

Definition 6.6. *A (v,k,λ,n)-difference set D satisfying the condition $v = 4n = 4(k-\lambda)$ is called* ***Hadamard difference set****.*

Let us shortly motivate the condition $v = 4n$ as well as the name Hadamard difference set.
We consider the matrix $[M_{D^*}] = J - 2[M_D]$ with entries in the set $\{-1, 1\}$. Those entries are obtained by replacing the value zero in $[M_D]$ by one and one by minus one. The matrix $[M_{D^*}]$ satisfies

$$\begin{aligned}[M_{D^*}]^2 &= (J - 2[M_D])^2 \\ &= J^2 - 2J[M_D] - 2[M_D]J + 4[M_D]^2 \\ &= vJ - 2kJ - 2kJ + 4(nI_v + \lambda J) \\ &= 4nI_v + (v - 4n)J.\end{aligned}$$

Thus, if $v = 4n$, then the matrix $[M_{D^*}]$ has the property $[M_{D^*}]^2 = v \cdot I_v$. As we know, in general, a matrix A with entries in the set $\{-1, 1\}$ of size $b \times b$ with the property $A^2 = b \cdot I$ is known as a Hadamard matrix. Therefore, we have

Lemma 6.7. *A (v, k, λ, n)-difference set is Hadamard if and only if $[M_{D^*}] = J - 2[M_D]$ is a Hadamard matrix.*

The Hadamard condition essentially determines the size of such a difference set in any group. The next result was first noted by Menon [28].

Theorem 6.8. *A Hadamard difference set has parameters of the form*

$$(v, k, \lambda, n) = (4N^2, 2N^2 - N, N^2 - N, N^2) \text{ or } (4N^2, 2N^2 + N, N^2 + N, N^2).$$

Proof. See [28]. □

This leads us to the result that a Hadamard difference set can only exist in a group of square order.

There are different generalizations of theorem 6.8. We conclude another generalization presented by Mann [23] in the following form:

Theorem 6.9. *Let G be an abelian group of order 2^n, $D \subset G$ a (v, k, λ, n)-difference set. Then one of the following holds*

$D = \emptyset$,	$k = 0$	and $\lambda = 0$
$D = \{e\}$,	$k = 1$	and $\lambda = 0$
$D = G \setminus \{e\}$	$k = v - 1$	and $\lambda = v - 2$
	$k = 2^{n-1} - 2^{\frac{n}{2}-1}$	and $\lambda = 2^{n-2} - 2^{\frac{n}{2}-1}$
	$k = 2^{n-1} + 2^{\frac{n}{2}-1}$	and $\lambda = 2^{n-2} + 2^{\frac{n}{2}-1}$.

Proof. See [23]. □

Clearly, if D is a particular difference set in the group G, it is easy to obtain many other difference sets from D. The following observation provides us with some difference sets which require further definition of the terms *equivalent difference sets* and *multiplier*.

If D is a (v, k, λ, n)-difference set in the group G, then for all $g \in G$ and all automorphisms α of G the sets

$$D + g = \{d + g | d \in D\}$$

and

$$D^\alpha = \{d^\alpha | d \in D\}$$

are also (v, k, λ, n)-difference sets in G.

This motivates the following definition.

Definition 6.10. *The difference sets D_1 and D_2 in the abelian group G are **equivalent** if there exists an automorphism α of G such that*

$$D_1^\alpha = D_2 + g \tag{6.2}$$

*for some $g \in G$. In particular, if equation (6.2) holds for $D_1 = D_2 = D$, then the group automorphism α is said to be a **multiplier** of D. A multiplier of the form*

$$g \mapsto g^t, \quad t \in \mathbb{Z}$$

*is called a **numerical multiplier**.*

Mann and McFarland have shown that every multiplier of a difference set must fix at least one translate of that difference set. We denote with $M(D)$ the subgroup of multipliers of D in the group of automorphisms in G. It is easy to see that equivalent difference sets have isomorphic multiplier groups. Indeed, if $D_1^\alpha = D_2 + g$ then $M(D_1) = \alpha M(D_2)\alpha^{-1}$, that is D_1 and D_2 are isomorphic.

6.2. Characterizations of the Bent Property

If it is not mentioned otherwise we use the convention $n = 2k$ in the rest of this chapter. We present different equivalent definitions of the bent property. Prior to this we want to assemble some basic results.

Definition 6.11. *For a bent function f we define a Boolean function $\mathfrak{F}$ such that*

$$\frac{W(\widehat{f})(u)}{2^{\frac{n}{2}}} = (-1)^{\mathfrak{F}(u)} = \widehat{\mathfrak{F}}(u).$$

We call $\mathfrak{F}$ **the dual** of f.

That is to say we consider the dual as the signs of the Walsh-coefficients of f. Thus, an obvious question is whether the dual is also a bent function.

Theorem 6.12. *Let f be a Boolean function on $\mathbb{F}_2^n$. Then f is bent if and only if the dual $\mathfrak{F}$ is bent.*

Proof. The Walsh-coefficients of $\mathfrak{F}$ are $\pm 2^{\frac{n}{2}}$, thus $\mathfrak{F}$ is bent. □

Therefore, we can conclude that bent functions always occur in pairs.

Definition 6.13. *For each real-valued function $f\colon \mathbb{F}_2^n \to \mathbb{R}$ we associate the $2^n \times 2^n$ matrix $[M_f]$ of which the (u,v)th entry is $f(u \oplus v)$, i.e. $[M_f] = (f(u \oplus v))_{u,v}$.*

The next result is given by McFarland [25].

Theorem 6.14. *Let the Sylvester-Hadamard matrix H_n be defined as in definition 3.6, and a_i, $0 \leq i \leq 2^n - 1$, as in definition 2.1. If $f\colon \mathbb{F}_2^n \to \mathbb{R}$, then*

$$H_n[M_f]H_n^{-1} = diag\left(W(f)(a_0), W(f)(a_1), \ldots, W(f)(a_{2^n-1})\right).$$

Proof. We recall that $H_n^{-1} = 2^{-n}H_n^t$. The (u,v)-th entry in the matrix $H_n[M_f]H_n^{-1}$ is

$$\begin{aligned} 2^{-n} \sum_{(s,t)\in\mathbb{F}_2^n\times\mathbb{F}_2^n} H_n(u,s)f(s\oplus t)H_n(t,v) &= 2^{-n} \sum_{w\in\mathbb{F}_2^n} f(w) \sum_{s\in\mathbb{F}_2^n} H_n(u,s)H_n(s\oplus w,v) \\ &= 2^{-n} \sum_{w\in\mathbb{F}_2^n} f(w)H_n(w,v) \sum_{s\in\mathbb{F}_2^n} H_n(u,s)H_n(v,s) \\ &= \begin{cases} W(f)(u) & \text{if } u = v \\ 0 & \text{otherwise,} \end{cases} \end{aligned}$$

since we use the relation between Sylvester-Hadamard matrices and the Walsh transform. □

Furthermore, we establish some more equivalent characterizations of the bent property.

Theorem 6.15. *Let $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function and let ξ be the $(1,-1)$-sequence. Then f is bent if and only if $\langle \xi, l\rangle = \pm 2^{\frac{n}{2}}$ for any affine sequence of length 2^n.*

Proof. This equivalence is a restatement of definition 6.1. □

Theorem 6.16. *Let f be a Boolean function on $\mathbb{F}_2^n$. Then f is bent if and only if the matrix $[M_{\widehat{f}}] = \left(\widehat{f}(u \oplus v)\right)_{u,v}$ is a Hadamard matrix.*

Proof. First, we assume that f is bent. From theorem 6.14 we know that

$$H_n[M_{\widehat{f}}]H_n^{-1} = diag\left(W(\widehat{f})(a_0), W(\widehat{f})(a_1), \ldots, W(\widehat{f})(a_{2^n-1})\right). \tag{6.3}$$

By applying the transposition operation we get

$$\left(H_n^{-1}\right)[M_{\widehat{f}}]^t H_n^t = H_n[M_{\widehat{f}}]^t H_n^{-1} = diag\left(W(\widehat{f})(a_0), W(\widehat{f})(a_1), \ldots, W(\widehat{f})(a_{2^n-1})\right). \tag{6.4}$$

Multiplying (6.3) and (6.4), we immediately get

$$H_n[M_{\widehat{f}}][M_{\widehat{f}}]^t H_n^{-1} = 2^n I_{2^n},$$

which leads to

$$[M_{\widehat{f}}][M_{\widehat{f}}]^t = 2^n I_{2^n},$$

that is, the matrix $[M_{\widehat{f}}]$ is Hadamard.
Conversely, we assume that $[M_{\widehat{f}}]$ is Hadamard. Immediately, we can conclude that $[M_{\widehat{f}}]^2$ is Hadamard. We multiply H_n and H_n^{-1} which gives us $H_n[M_{\widehat{f}}]H_n^{-1}$ and this is still Hadamard. Therefore, it follows that f is bent. □

If we regard the Boolean function f as the characteristic function of the set $D = f^{-1}(1)$, then the matrices $[M_f]$ and $[M_{\widehat{f}}]$ coincide with the incidence matrix $[M_D]$ and its associate matrix $[M_{D^*}]$, respectively. This leads to the following characterization of bentness.

Theorem 6.17. *Let f be a Boolean function on $\mathbb{F}_2^n$. Then f is bent if and only if $f^{-1}(1)$ is a Hadamard difference set in $\mathbb{F}_2^n$.*

Proof. We use lemma 6.7 to conclude the statement. The (u, v)-th entries of the matrix $J - 2[M_D]$ are

$$\begin{cases} -1 & \text{if } u - v \in D \\ 1 & \text{otherwise} \end{cases} = \begin{cases} -1 & \text{if } u \oplus v \in f^{-1}(1) \\ 1 & \text{otherwise} \end{cases}$$
$$= \begin{cases} -1 & \text{if } f(u \oplus v) = 1 \\ 1 & \text{otherwise} \end{cases} = (-1)^{f(u \oplus v)},$$

where $D = f^{-1}(1)$ is a Hadamard matrix. By theorem 6.7, D is also a Hadamard difference set. Finally, we use theorem 6.16 and so it follows that f is bent.
For the converse we reverse the arguments. □

Theorem 6.18. *Let f be a Boolean function on $\mathbb{F}_2^n$. Then f is bent if and only if $f(x) \oplus \langle \alpha, x \rangle$ has $2^{n-1} \pm 2^{\frac{n}{2}-1}$ zeros for all $\alpha \in \mathbb{F}_2^n$.*

Proof. Let us denote with Z_v the number of zeros of $g(x) = f(x) \oplus \langle v, x \rangle$. Then

$$W(\widehat{f})(v) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus \langle v, x \rangle} = Z_v - (2^n - Z_v) = 2Z_v - 2^n$$

or

$$Z_v = 2^{n-1} + 2^{-1} W(\widehat{f})(v).$$

Since f is bent, we have $W(\widehat{f})(v) = \pm 2^{\frac{n}{2}}$. Therefore, it follows that $Z_v = 2^{n-1} \pm 2^{\frac{n}{2}-1}$.
For the converse we reverse the arguments. □

For the next characterization of bentness we use the directional derivative.

Theorem 6.19. *Let f be a Boolean function on $\mathbb{F}_2^n$. Then f is bent if and only if the directional derivative f_v is balanced for all nonzero v in $\mathbb{F}_2^n$.*

Proof. We use theorem 6.16 with $[M_{\widehat{f}}] = \left(\widehat{f}(u \oplus v)\right)_{u,v}$ and know that f is bent if and only if $[M_{\widehat{f}}]$ is Hadamard. It follows that $[M_{\widehat{f}}]$ is Hadamard if and only if

$$\sum_{w \in \mathbb{F}_2^n} (-1)^{f(u \oplus w) \oplus f(w \oplus v)} = 0,$$

for any $u \neq v$. If w runs through $\mathbb{F}_2^n$, $w \oplus v$ runs through $\mathbb{F}_2^n$ as well. Thus, we can write the above equation as

$$\sum_{w \in \mathbb{F}_2^n} (-1)^{f(u \oplus v \oplus w) \oplus f(w)} = 0, \tag{6.5}$$

for any $u \neq v$. And that is that $f_{u \oplus v}$ is balanced.
For the converse we reverse the arguments. □

The result of this theorem is that the classes of perfect nonlinear functions [26] and bent functions coincide.
Let us stop for a moment and gather the various characterizations of bent functions in the following theorem.

Theorem 6.20. *Let $f \colon \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function. The following statements are equivalent:*

(i) *f is bent.*

(ii) *Let ξ be the $(1,-1)$-sequence of f. Then $\langle \xi, l \rangle = \pm 2^{\frac{n}{2}}$ for any affine sequence of length 2^n.*

(iii) *The matrix $[M_{\widehat{f}}] = \left(\widehat{f}(u \oplus v)\right)_{u,v}$ is a Hadamard matrix.*

(iv) *$f^{-1}(1)$ is a Hadamard difference set in $\mathbb{F}_2^n$.*

(v) *The dual $\mathfrak{F}$ is bent.*

(vi) *The directional derivative $f_v(x) = f(x \oplus v) \oplus f(x)$ is balanced for all nonzero v in $\mathbb{F}_2^n$.*

(vii) *$f(x) \oplus \langle \alpha, x \rangle$ assumes the value one $2^{n-1} \pm 2^{\frac{n}{2}-1}$ times for any $\alpha \in \mathbb{F}_2^n$.*

There is yet another important characterization of bent functions concerning the nonlinearity of Boolean functions. This will, however, be discussed in chapter 7, where we show that the function f is bent if and only if f attains the upper bound of nonlinearity.

We use corollary 3.20 and $\widehat{f}$ instead of f to obtain information about the degree of a bent function. By corollary 3.20, we have

$$\sum_{u\leq v}\widehat{f}(u)=2^{-wt(v)}\sum_{u\leq\overline{v}}W(\widehat{f})(u).$$

For a Boolean function we have $\widehat{f}(u)=(-1)^{f(u)}=1-2f(u)$, where we interpret the functions as real functions. Furthermore, if f is bent, by using the definition 6.11 of the dual $\mathfrak{F}$ we have

$$W(\widehat{f})(u)=2^{\frac{n}{2}}\widehat{\mathfrak{F}}=2^{\frac{n}{2}}\left(1-2\mathfrak{F}(u)\right).$$

We obtain

$$\begin{aligned}\sum_{u\leq v}\widehat{f}(u)=2^{-wt(v)}\sum_{u\leq\overline{v}}W(\widehat{f})(u)&\Leftrightarrow\sum_{u\leq v}(1-2f(u))=2^{-wt(v)}\sum_{u\leq\overline{v}}2^{\frac{n}{2}}\left(1-2\mathfrak{F}(u)\right)\\&\Leftrightarrow 2^{wt(v)}-2\sum_{u\leq v}f(u)=2^{-wt(v)}\sum_{u\leq\overline{v}}2^{\frac{n}{2}}-2^{-wt(v)+1\frac{n}{2}}\sum_{u\leq\overline{v}}\mathfrak{F}(u)\\&\Leftrightarrow\sum_{u\leq v}f(u)=2^{wt(v)-1}-2^{\frac{n}{2}-1}+2^{-wt(v)+\frac{n}{2}}\sum_{u\leq\overline{v}}\mathfrak{F}(u).\end{aligned}$$

This proves the next lemma.

Lemma 6.21. *If f is a bent function on $\mathbb{F}_2^n$, then regarding f as a real-valued function we have*

$$\sum_{u\leq v}f(u)=2^{wt(v)-1}-2^{\frac{n}{2}-1}+2^{-wt(v)+\frac{n}{2}}\sum_{u\leq\overline{v}}\mathfrak{F}(u).\tag{6.6}$$

Now we are able to phrase and prove the theorem on the degree of a bent function.

Theorem 6.22. *For $n=2$, the degree of a bent function on $\mathbb{F}_2^2$ is 2. For $n>2$, the degree of a bent function is at most $\frac{n}{2}$.*

Proof. The first part is obvious. For the second part, let f be a bent function and $n>2$. As we know, every Boolean function is given by a unique polynomial, so we have

$$f(x)=\sum_{v\in\mathbb{F}_2^n}g(v)x_1^{v_1}\cdots x_n^{v_n},$$

where the coefficients are given by

$$g(v)=\sum_{u\leq v}f(u).$$

The monomial $x_1^{v_1}\cdots x_n^{v_n}$ is present in the polynomial $f(x)$ if and only if $g(v)$ is odd. However, if $wt(v)>\frac{n}{2}$ and $n>2$, then the right side of equation (6.6) is even. Thus, $g(v)$ is zero in $\mathbb{F}_2$ and $f(x)$ does not contain the monomial $x_1^{v_1}\cdots x_n^{v_n}$. Therefore, f has at most degree $\frac{n}{2}$. □

Corollary 6.23. *If f is bent of degree $\frac{n}{2}$, then its dual $\mathfrak{F}$ is also bent of degree $\frac{n}{2}$.*

Xia et al [45] have observed that the homogeneity influences the degree of bent functions. They proved that homogeneous bent functions of degree k in $2k$ variables, for $k > 3$, do not exist. The proof is based on the use of difference sets.
This approach was generalized by Meng et al. [27]. They showed that for any nonnegative integer m, there exists a positive integer N such that for $k \geq N$ there exist no $2k$-variable homogeneous bent function having degree $k - m$ or more, where N is the least integer such that $2^{N-1} > \binom{N+1}{0} + \binom{N+1}{1} + \cdots + \binom{N+1}{m+1}$.
The problem of constructing homogeneous bent functions of degree four and higher is still a open problem. In this context we present the following conjecture given by Meng et al [27].

Conjecture. For any integer $k > 1$, there exists a positive integer N such that when $m > N$, there exist homogeneous bent functions of degree k in $2m$ variables.

6.3. Constructions of Bent Functions

For a better understanding of bent functions we want to construct such functions. We differentiate between *primary constructions* and *secondary constructions*. Primary constructions include bent functions that are not used as building blocks in previous constructions and secondary constructions lead to recursive constructions. Thus, primary constructions lead potentially to wider classes of functions than secondary constructions.

6.3.1. Primary Constructions

Maiorana and McFarland's Construction

The following definition were introduced by Maiorana [22].

Definition 6.24. *Let $\pi\colon \mathbb{F}_2^k \longrightarrow \mathbb{F}_2^k$ be a permutation and $g\colon \mathbb{F}_2^k \longrightarrow \mathbb{F}_2$ an arbitrary Boolean function. Then $f : \mathbb{F}_2^k \times \mathbb{F}_2^k \longrightarrow \mathbb{F}_2$ with*

$$f(x, y) = \langle \pi(x), y \rangle \oplus g(x)$$

is called a Maiorana-McFarland function.

Remark. Dillon [11] points out that Maiorana and McFarland independently came up with the same construction. Therefore, we call it the Maiorana and McFarland construction or MM-functions.

The following theorem shows that all MM-functions are bent.

Theorem 6.25. *The MM-functions as defined in definition 6.24 are bent.*

Proof. For any $u, v \in \mathbb{F}_2^k$, we have

$$\begin{aligned} W(\widehat{f})(u,v) &= \sum_{x,y\in\mathbb{F}_2^k} (-1)^{\langle\pi(x),y\rangle\oplus g(x)\oplus\langle u,x\rangle\oplus\langle v,y\rangle} \\ &= \sum_{x,y\in\mathbb{F}_2^k} (-1)^{g(x)\oplus\langle u,x\rangle\oplus\langle\pi(x),y\rangle\oplus\langle v,y\rangle} \\ &= \sum_{x\in\mathbb{F}_2^k} (-1)^{g(x)\oplus\langle u,x\rangle} \cdot \underbrace{\sum_{y\in\mathbb{F}_2^k} (-1)^{\langle(\pi(x)\oplus v),y\rangle}}_{=\begin{cases} 2^m, & \text{if } \pi(x)=v \\ 0, & otherwise \end{cases}} \\ &= \pm 2^m, \end{aligned}$$

where the last equality follows from (6.9) and $x = \pi^{-1}(v)$. Thus, f is bent. □

The above given construction was generalized by Carlet [2] in the following way.

Proposition 6.26. *Let $n = r + s$ $(r \leq s)$ be even. Further, let Φ be any mapping from $\mathbb{F}_2^s$ to $\mathbb{F}_2^r$, such that, for every $a \in \mathbb{F}_2^r$, the set $\Phi^{-1}(a)$ is an $(n-2r)$-dimensional affine subspace of $\mathbb{F}_2^s$. Let g be any Boolean function on $\mathbb{F}_2^s$ whose restriction to $\Phi^{-1}(a)$ (viewed as a Boolean function on $\mathbb{F}_2^{n-2r}$ via an isomorphism between $\Phi^{-1}(a)$ and this vector space) is bent for every $a \in \mathbb{F}_2^r$, if $n > 2r$ (no restriction is imposed if $n = 2r$). Then the function $f_{\Phi,g}(x,y) = \langle x, \Phi(y)\rangle \oplus g(y)$ is bent on $\mathbb{F}_2^n$.*

Proof. [2] We start with the fact that every function $x \mapsto f_{\Phi,g}(x,y) \oplus \langle a,x\rangle \oplus \langle b,y\rangle$ is affine and thus constant or balanced. This contributes for a nonzero value in the sum $\sum_{x\in\mathbb{F}_2^r,\, y\in\mathbb{F}_2^s}(-1)^{f_{\Phi,g}(x,y)\oplus\langle a,x\rangle\oplus\langle b,y\rangle}$ only if $\Phi(y) = a$. By rewriting the equality, we obtain

$$W(\widehat{f_{\Phi,g}})(a,b) = 2^r \sum_{y\in\Phi^{-1}(a)} (-1)^{g(y)\oplus\langle b,y\rangle}.$$

According to this, the function $f_{\Phi,g}$ is bent if and only if $r \leq \frac{n}{2}$ and $\sum_{y\in\Phi^{-1}(a)}(-1)^{g(y)\oplus\langle b,y\rangle} = \pm 2^{\frac{n}{2}-r}$ for every $a \in \mathbb{F}_2^r$ and $b \in \mathbb{F}_2^s$. □

Other known primary constructions of bent functions are the Partial Spread class given by Dillon [12] and the class $\mathcal{N}$ introduced by Dobbertin.

Application of the Maiorana-McFarland Construction

Next we use the Maiorana-McFarland construction to construct correlation immune- and $PC(k)$ functions. Therefore, we start to construct correlation immune functions of order at least k applying a non-recursive method given by Camion et al. [1].

Theorem 6.27. *Given m and n with $1 \leq m < n$ and define $x = (x_1, \dots x_n)$ and $r = n - m$, $u = (x_1, \dots, x_m)$ and $v = (x_{m+1}, \dots, x_n)$. Further, let $g(u)$ be an arbitrary Boolean function in m variables and let $\Phi(u)$ be any function $\Phi \colon \mathbb{F}_2^m \to \mathbb{F}_2^r$ with*

$$w = \min\{wt(\Phi(u)) | u \in \mathbb{F}_2^m\} \geq 1. \tag{6.7}$$

We define a Boolean function f on $\mathbb{F}_2^n$ by

$$f(x) = f(u, v) = \langle v, \Phi(u) \rangle \oplus g(u).$$

Then $f(x)$ is balanced and correlation immune of order k with $k \geq w - 1$.

Proof. We have

$$\sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)} = \sum_{u \in \mathbb{F}_2^m} (-1)^{g(u)} \sum_{v \in \mathbb{F}_2^r} (-1)^{\langle v, \Phi(u) \rangle} = 0,$$

since the sums over v are always 0 because by equation (6.7) $\Phi(u) \neq 0$. Thus, $f(x)$ is balanced.

For any choice of $b \in \mathbb{F}_2^m$, $a \in \mathbb{F}_2^r$ and for any $k \leq w - 1$ with $1 \leq wt(b, a) \leq k$, we have

$$\begin{aligned} W(f)(b, a) &= \sum_{u \in \mathbb{F}_2^m,\, v \in \mathbb{F}_2^r} (-1)^{f(u,v) \oplus \langle (b,a), (u,v) \rangle} \\ &= \sum_{u \in \mathbb{F}_2^m,\, v \in \mathbb{F}_2^r} (-1)^{\langle \Phi(u), v \rangle \oplus g(u) \oplus \langle b, u \rangle \oplus \langle a, v \rangle} \\ &= \sum_{u \in \mathbb{F}_2^m} (-1)^{\langle b, u \rangle \oplus g(u)} \sum_{v \in \mathbb{F}_2^r} (-1)^{\langle (\Phi(u) \oplus a), v \rangle}. \end{aligned}$$

We get $\Phi(u) \oplus a \neq 0$ by the fact that $wt(a) \leq k$ and $wt(\Phi(u)) \geq w \geq k + 1$. Thus, the sums over v are equal 0. Therefore, it follows that $W(f)(b, a) = 0$. By lemma 4.3 f is correlation immune of order k. □

Remark. Carlet discusses in [6] that one virtue of the MM-functions is their possibility to retain control of some properties, for example the nonlinearity and the propagation characteristics.

Moreover, we use the Maiorana-McFarland construction to construct functions satisfying the propagation criterion. We follow Carlet's approach [5] and confine the observation on functions which satisfy $PC(k)$ of order m for $k > 1, m \geq 1$.

Theorem 6.28. *We define a MM-function $f(x, y) = \langle \Phi(x), y \rangle \oplus g(x)$ in $n = s + t$ variables such that*

(i) for each j, $1 \leq j \leq k$, the sum of any j of the coordinate functions $\Phi_i(x)$ is a balanced function;

(ii) for every nonzero $a \in \mathbb{F}_2^s$ with $wt(a) \leq k$, and for any x in $\mathbb{F}_2^s$, we have $\Phi(x \oplus a) \neq \Phi(x)$.

Then $f(x, y)$ satisfies $PC(k)$.

Proof. For any $a \in \mathbb{F}_2^s$ and $b \in \mathbb{F}_2^t$, we have

$$f(x, y) \oplus f(x \oplus a, y \oplus b) = \langle(\Phi(x) \oplus \Phi(x \oplus a)), y\rangle \oplus \langle\Phi(x \oplus a), b\rangle \oplus g(x) \oplus g(x \oplus a) \tag{6.8}$$

If $a = 0$ and $1 \leq wt(b) \leq k$, then equation (6.8) becomes $\langle\Phi(x), b\rangle$ which is balanced by equation (i). If $1 \leq wt(a) \leq k$, then for every fixed x condition (ii) implies that the function of y given by (6.8) is a non-constant affine function and hence the function is balanced. Furthermore, for every a, b with $1 \leq wt(a) + wt(b) \leq k$, it follows that (6.8) is balanced. Therefore, it follows by using lemma 5.18 that $f(x, y)$ satisfies $PC(k)$. □

Now we use the term of resiliency and obtain the following

Theorem 6.29. *We define a MM-function $f(x, y) = \langle\Phi(x), y\rangle \oplus g(x)$ in $n = s + t$ variables such that*

(i) for each j, $1 \leq j \leq k$, the sum of any j of the coordinate functions $\Phi_i(x)$ is a k-resilient function;

(ii) for every nonzero $a \in \mathbb{F}_2^s$ with $wt(a) \leq k$, and for any x in $\mathbb{F}_2^s$, we have that at least $m + 1$ coordinates of the vectors $\Phi(x \oplus a)$ and $\Phi(x)$ are different.

Then $f(x, y)$ satisfies $PC(k)$ of order m.

Proof. Any restriction of a MM- function obtained by fixing some of the input bits in x and y is still a MM-function. So any restriction of the above given MM-function has the form $f'(x', y') = \langle\Phi'(x'), y'\rangle \oplus g'(x')$ by fixing at most m of the input bits in x and y. Furthermore, the sum of any at least 1 and at most k of the $\Phi_i'(x')$ is equal to the sum of any at least 1 and at most k of the $\Phi_i(x)$.
Therefore, by condition (i), theorem 6.28 (i) is satisfied by $f'(x', y')$. By condition (ii), it follows that for every nonzero a' with $wt(a') \leq k$ and for any $x' \in \mathbb{F}_2^s$ we have $\Phi'(x' \oplus a') \neq \Phi'(x')$. Thus, we have that condition (ii) of theorem 6.28 is also satisfied by $f'(x', y')$ and it follows that $f(x, y)$ satisfies $PC(k)$ of order m. □

6.3.2. Secondary Constructions

In the remaining part, we focus on secondary constructions. First, we start to construct bent functions on $\mathbb{F}_2^{n+m}$ based on concatenation.

Theorem 6.30. *Let f and g be Boolean functions on $\mathbb{F}_2^m$ and $\mathbb{F}_2^n$, respectively. Then the Boolean function $h\colon \mathbb{F}_2^{m+n} \to \mathbb{F}_2$ is defined by $h(x, y) = f(x) \oplus g(y)$ is bent if and only if f and g are bent.*

Proof. Let $z \in \mathbb{F}_2^{m+n}$, $z = (x, y)$, where $x \in \mathbb{F}_2^m$ and $y \in \mathbb{F}_2^n$. Then we have

$$\begin{aligned} W(\widehat{h})(z) &= \sum_{t \in \mathbb{F}_2^{m+n}} (-1)^{\langle z,t\rangle \oplus h(t)} \\ &= \sum_{r \in \mathbb{F}_2^m} \sum_{s \in \mathbb{F}_2^n} (-1)^{\langle x,r\rangle \oplus \langle y,s\rangle \oplus f(r) \oplus g(s)} \\ &= W(\widehat{f})(x) W(\widehat{g})(y) \end{aligned}$$

If f and g are bent, then we have $W(\widehat{f})(x) = \pm 2^{\frac{m}{2}}$ and $W(\widehat{g})(y) = \pm 2^{\frac{n}{2}}$. Thus, we have $W(\widehat{h})(z) = \pm 2^{\frac{m+n}{2}}$ and so h is bent.
Conversely, we assume that h is bent. We have to prove that f and g are bent. For instance, we suppose that f is not bent. Therefore, it follows that there exists $u \in \mathbb{F}_2^m$ such that $|W(\widehat{f})(u)| > 2^{\frac{m}{2}}$. Since h is bent and $2^{\frac{m+n}{2}} = |W(\widehat{f})(u)||W(\widehat{g})(v)|$, thus for any $v \in \mathbb{F}_2^n$ we have $|W(\widehat{g})(v)| < 2^{\frac{n}{2}}$. Using Parseval's equation (3.6), we get a contradiction and so f has to be bent. □

As Dillon [11] pointed out, functions of this type constructed within the previous theorem are rather uninteresting because they may be "decomposed" into simpler functions on lower dimensional vector spaces.

Definition 6.31. *A Boolean function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ is decomposable if it is linearly equivalent to a sum of functions in disjoint sets of variables. That is, there exists a nonsingular $n \times n$ matrix T, $n = m + k$, $1 \leq m < n$, and two functions $g\colon \mathbb{F}_2^m \to \mathbb{F}_2$, $h\colon \mathbb{F}_2^k \to \mathbb{F}_2$ such that*

$$f(xT) = g(x_1, \ldots, x_m) \oplus h(x_{m+1}, \ldots, x_n).$$

Lemma 6.32. *For $n \geq 6$, every bent function of degree $k = \frac{n}{2}$ on $\mathbb{F}_2^n$ is indecomposable.*

Proof. [36] If the bent function f of degree k is linearly equivalent to the sum of two functions g and h in disjoint variables, then both g and h must be bent by theorem 6.30. Their degrees are less than k, which means that their sum cannot have degree k. This is a contradiction and the bent function is indecomposable. □

It is easy to see that the above lemma is not true for $n = 4$. For example we take the bent function $h(x) = x_1x_2 \oplus x_3x_4$. Obviously, we can write $h(x) = f(x_1, x_2) \oplus g(x_3, x_4)$ and therefore the function is decomposable.

Corollary 6.33. *The function*

$$f(x) = x_1x_2 \oplus x_3x_4 \oplus \cdots \oplus x_{2k-1}x_{2k}, \quad k \geq 1,$$

is bent.

Proof. The proof follows by induction on k. The base step is trivial, as we have seen in example 11 the function $f(x) = x_1x_2$ is bent because the Walsh-coefficients of $\widehat{f}$ equals ± 2. For the inductive step we have

$$\begin{aligned} g(x) &= x_1x_2 \oplus x_3x_4 \oplus \cdots \oplus x_{2k-1}x_{2k} \oplus x_{2k+1}x_{2k+2} \\ &= f(x_1, \ldots, x_{2k}) \oplus x_{2k+1}x_{2k+2} = f(x_1, \ldots, x_{2k}) \oplus h(x_{2k+1}, x_{2k+2}). \end{aligned}$$

By our hypothesis, we have that $f(x)$ is bent and obviously $h(x_{2k+1}, x_{2k+2})$ is bent due to the base step. By theorem 6.30, it follows that $g(x)$ is bent. □

An interesting question is whether the class of bent functions is stable under addition of affine functions. This question is to be answered in the affirmative as we shall prove within the next theorem.

Theorem 6.34. *If f is bent, then $f \oplus \alpha$ is bent for any affine function α.*

Proof. It suffices to consider the linear case $\alpha_a(x) = \langle a, x\rangle$, since adding 1 to a function will complement the truth table. Then, we note $g(x) = f(x) \oplus \alpha_a(x)$ and obtain

$$\begin{aligned} W(\widehat{g})(u) &= \sum_{x \in \mathbb{F}_2^n} (-1)^{g(x) \oplus \langle u, x\rangle} \\ &= \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus \langle x, (u \oplus a)\rangle} \\ &= W(\widehat{f})(u \oplus a). \end{aligned}$$

Thus, if f is bent, then g is bent for any $a \in \mathbb{F}_2^n$. □

Now a valid question is whether by applying an affine transformation on the variables of a bent function also produce bent functions. To answer this question, let A be an $n \times n$ invertible matrix over $\mathbb{F}_2$ and b a vector in $\mathbb{F}_2^n$. We write $g(x) = f(Ax \oplus b)$ and obtain

$$\begin{aligned} W(\widehat{g})(u) &= \sum_{x \in \mathbb{F}_2^n} (-1)^{g(x) \oplus \langle u, x\rangle} \\ &= \sum_{x \in \mathbb{F}_2^n} (-1)^{f(Ax \oplus b) \oplus \langle u, x\rangle}. \end{aligned}$$

By setting $x = A^{-1}w \oplus A^{-1}b$, we get

$$\begin{aligned} W(\widehat{g})(u) &= \sum_{x \in \mathbb{F}_2^n} (-1)^{f(w) \oplus \langle uA^{-1}, w\rangle \oplus \langle u, A^{-1}b\rangle} \\ &= (-1)^{\langle u, A^{-1}b\rangle} \cdot W(\widehat{f})(uA^{-1}) \\ &= \pm W(\widehat{f})(uA^{-1}). \end{aligned} \tag{6.9}$$

Thus, if f is bent, then g is also bent.
For this reason we can answer the above question positive if the transformation is non-singular. Finally, we have proven the following theorem.

Theorem 6.35. *Let A be an $n \times n$ invertible matrix over $\mathbb{F}_2$ and b a vector in $\mathbb{F}_2^n$. If f is bent, then $g(x) = f(Ax \oplus b)$ is also bent.*

Remark. The nonsingularity of the transformation is a requirement for good cryptographic functions.

7. Properties of Nonlinearity

Nonlinearity is an important cryptographic criterion. It measures the ability of a cryptographic system using the functions to resist against being expressed as a linear set of equations.

The purpose of this chapter is to examine properties of nonlinearity. In detail, we present the basics about nonlinearity and introduce some results concerning the upper and lower bound of nonlinearity. Furthermore, we observe ways to construct highly (balanced) nonlinear functions. A vast body of work has focused on nonlinearity. Thus, this section is mainly based on results from Seberry, Zhang and Zheng [38].

7.1. Bounds of Nonlinearity

In this section, we observe the upper bound of nonlinearity which is only attainable by bent functions. Moreover, we present some results about the lower bound of nonlinearity of a function obtained by concatenating sequences of functions.

First, we phrase a lemma that is very useful in calculating nonlinearity of a function.

Lemma 7.1. *Let f and g be functions on $\mathbb{F}_2^n$ whose $(1,-1)$-sequences are ξ_f and ξ_g. Then the distance between f and g can be calculated by $d(f,g) = 2^{n-1} - \frac{1}{2}\langle \xi_f, \xi_g \rangle$.*

Proof.

$$\begin{aligned}\langle \xi_f, \xi_g \rangle &= \sum_{f(x)=g(x)} 1 - \sum_{f(x)\neq g(x)} 1 \\ &= 2^n - 2\sum_{f(x)\neq g(x)} \\ &= 2^n - 2d(f,g).\end{aligned}$$

By rearranging the terms, the statement follows immediately. □

The valid question is whether we find an upper bound of nonlinearity.

Theorem 7.2. *[38] For any function f on $\mathbb{F}_2^n$, the nonlinearity N_f of f satisfies $N_f \leq 2^{n-1} - 2^{\frac{n}{2}-1}$.*

To prove the theorem we need the following lemma. The lemma presents how closely Sylvester-Hadamard matrices (3.6) are related to linear functions (2.3).

Lemma 7.3. *[38] If the Sylvester-Hadamard matrix H_n is given by*

$$H_n = \begin{bmatrix} l_0 \\ l_1 \\ \vdots \\ l_{2^n-1} \end{bmatrix},$$

where l_i is a row of H_n, $i = 0, \ldots, 2^n - 1$, then l_i is the $(1, -1)$-sequence of $h_i = \langle a_i, x\rangle$, a linear function, where a_i is defined before in (2.1) and $x = (x_1, \ldots, x_n)$. Conversely, the $(1, -1)$-sequence of any linear function on $\mathbb{F}_2^n$ is a row of H_n.

Proof. The lemma follows by induction on n. Let $n = 1$, then we have the following Sylvester-Hadamard matrix $H_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$. The first row of H_1, $l_0 = (1, 1)$, is the sequence of $h_0 = \langle a_0, x\rangle$, while the second row of H_1, $l_1 = (1, -1)$, is the sequence of $h_1 = \langle a_1, x\rangle$, where $x = x_1$, $a_0 = 0$ and $a_1 = 1$. Now, we suppose that the first half of the lemma is true for $n = 1, 2, \ldots, k - 1$. Since $H_k = H_1 \otimes H_{k-1}$, each row of H_k can be expressed as $\delta \otimes l$ where $\delta = (1, 1)$ or $(1, -1)$, and l is a row of H_{k-1}. By the assumption that l is the $(1, -1)$-sequence of a linear function $h_{k-1}(x) = \langle a, x\rangle$ for some $a \in \mathbb{F}_2^{k-1}$ and $x = (x_1, \ldots, x_{k-1})$, it follows that $\delta \otimes l$ is the sequence of a linear function on $\mathbb{F}_2^k$ defined by $h_k(y) = \langle b, y\rangle$, where $y = (y_1, \ldots, y_k)$, $b = (0, a)$ if $\delta = (1, 1)$ and $b = (1, a)$ otherwise. Thus, the first half is also true for $n = k$.
The second half follows from the discussion above as well as the fact that H_n has 2^n rows, and there are exactly 2^n linear functions on $\mathbb{F}_2^n$. □

We note that the rows of H_n comprise the $(1, -1)$-sequences of all linear functions. Consequently, the rows of $\pm H_n$ comprise the sequences of all affine functions.

Proof of theorem 7.2. [38] We recall that H_n is a $2^n \times 2^n$ matrix. Likewise to lemma 7.3, we denote by l_i the i-th row of H_n with $i = 0, 1, \ldots, 2^n - 1$. Furthermore, for each row l_i, we define $l_{i+2^n} = -l_i$. As a consequence of lemma 7.3, we get that all affine sequences are among the rows $\pm H_n$, that is, $l_0, \ldots, l_{2^{n+1}-1}$. Let f be a Boolean function on $\mathbb{F}_2^n$ of which the sequence is $\xi_f = (a_1, \ldots, a_n)$, and let α_i be an affine function whose sequence is l_i. Thus, from lemma 7.1 we infer that

$$\langle \xi_f, l_i\rangle^2 = 2^n + 2\sum_{j<k} a_j a_k h_{ij} h_{ik}.$$

Summing up for $i = 1, \ldots, 2^n$, leads to a variant of Parseval's equation [21, p. 416] as follows

$$\begin{aligned} \sum_{i=1}^{2^n} \langle \xi_f, l_i\rangle^2 &= 2^{2n} + 2\sum_{i=1}^{2^n}\sum_{j<k} a_j a_k h_{ij} h_{ik} \\ &= 2^{2n} + 2\sum_{j<k} a_j a_k \sum_{i=1}^{2^n} h_{ij} h_{ik} = 2^{2n}. \end{aligned} \tag{7.1}$$

Consequently, there exists an integer $1 \leq i \leq 2^n$ such that $\langle \xi_f, l_i \rangle^2 = \langle \xi_f, l_{i+2^n} \rangle^2 \geq 2^n$. With the fact that $\langle \xi_f, l_i \rangle = -\langle \xi_f, l_{i+2^n} \rangle$, we have either $\langle \xi_f, l_i \rangle \geq 2^{\frac{n}{2}}$ or $\langle \xi_f, l_{i+2^n} \rangle \geq 2^{\frac{n}{2}}$. Without loss of generality we assume that $\langle \xi_f, l_i \rangle \geq 2^{\frac{n}{2}}$. Therefore, by lemma (7.1), we get

$$d(f, \alpha_i) = 2^{n-1} - \frac{1}{2}\langle \xi_f, l_i \rangle \leq 2^{n-1} - 2^{\frac{n}{2}-1}. \tag{7.2}$$

□

Remark. In this chapter, we use an alternative notation. That is $|\langle \xi, l_i \rangle| = \left| W(\widehat{f})(a_i) \right|$ for $i = 0, \ldots 2^n - 1$ and l_i is the ith row of the Sylvester-Hadamard matrix H_n.

Due to the remark, we give an equivalent formulation of theorem 3.18.

Theorem 7.4. *The nonlinearity of a Boolean function f on $\mathbb{F}_2^n$ can be expressed by*

$$N_f = 2^{n-1} - \frac{1}{2}\max\{|\langle \xi, l_i \rangle| : 0 \leq i \leq 2^n - 1\},$$

where ξ is the $(1, -1)$-sequence of f and $l_0, \ldots . l_{2^n-1}$ are the rows of H_n, namely, the $(1, -1)$-sequences of linear functions on $\mathbb{F}_2^n$.

It is known that for n is even, the bound in theorem 7.2 is attained by the bent functions. This result will be shown in the next theorem. For odd n the right-hand side of the inequality of theorem 7.2 is not an integer. Clearly, equality is impossible. However, the important question how close N_f can get to the right-hand side if n is odd is not completely answered to this day.

Theorem 7.5. *A function f on $\mathbb{F}_2^n$ attains the upper bound of nonlinearities, $2^{n-1} - 2^{\frac{n}{2}-1}$, if and only if f is bent.*

Proof. From theorem 6.20, we have that since f is bent, it follows that

$$\langle \xi_f, l_i \rangle = \pm 2^{\frac{n}{2}}, \tag{7.3}$$

where l_i is the corresponding sequence of the affine function α_i. Using equation (7.3) and the relation $d(f, g) = 2^{n-1} - \frac{1}{2}\langle \xi_f, \xi_g \rangle$ from lemma 7.1, we deduce

$$d(f, \alpha_i) = 2^{n-1} \pm 2^{\frac{n}{2}-1},$$

which implies $N_f = 2^{n-1} - 2^{\frac{n}{2}-1}$.
Conversely, we suppose that f attains the upper bound of nonlinearity. Then $\langle \xi_f, l_i \rangle^2 = 2^n$ for $i = 1, 2, \ldots, 2^{n+1}$. Now we suppose that this is not the case. Thus, from Parseval's equation, there would exist i_1 and i_2, $1 \leq i_1, i_2 \leq 2^n$, such that $\langle \xi_f, l_{i_1} \rangle^2 > 2^n$ and $\langle \xi_f, l_{i_2} \rangle^2 < 2^n$. This implies that either $\langle \xi_f, l_{i_1} \rangle > 2^{\frac{n}{2}}$ or $\langle \xi_f, l_{i_1+2^n} \rangle > 2^{\frac{n}{2}}$. Moreover, we suppose without loss of generality that $\langle \xi_f, l_{i_1} \rangle^2 > 2^{\frac{n}{2}}$. Furthermore, we infer that $d(f, l_{i_1}) < 2^{n-1} - 2^{\frac{n}{2}-1}$ and as a consequence we have $N_f = 2^{n-1} - 2^{\frac{n}{2}-1}$. This is a contradiction to the assumption that f attains the maximum nonlinearity. Furthermore, we must have $\langle \xi_f, l_i \rangle = \pm 2^{\frac{n}{2}}$, $i = 1, 2, \ldots, 2^{n+1}$, which implies that f is bent, c.f. theorem 6.15. □

Corollary 7.6. *Let f be a balanced function on $\mathbb{F}_2^n$ ($n \geq 3$). Then the nonlinearity N_f of f is given by*

$$N_f \leq \begin{cases} 2^{n-1} - 2^{\frac{n}{2}-1} - 2 & \text{if } n \text{ is even} \\ \lfloor\lfloor 2^{n-1} - 2^{\frac{n}{2}-1} \rfloor\rfloor & \text{if } n \text{ is odd,} \end{cases}$$

where $\lfloor\lfloor x \rfloor\rfloor$ denotes the maximum even integer less than or equal to x.

Proof. See [38]. □

So far, we observed that there is a upper bound of nonlinearity. Therefore, we turn our attention to the question whether there is also a lower bound of nonlinearity. We obtain the lower bound of nonlinearity by concatenating sequences of functions.

Lemma 7.7. *Let f_1 and f_2 be functions on $\mathbb{F}_2^n$, and let g be a function on $\mathbb{F}_2^{n+1}$ defined by*

$$g(u, x_1, \ldots, x_n) = [f_1, f_2]_{n+1} = (1 \oplus u) f_1(x_1, \ldots, x_n) + u f_2(x_1, \ldots, x_n). \tag{7.4}$$

Suppose that ξ_1 and ξ_2, the sequences of f_1 and f_2 respectively, satisfy $\langle \xi_1, l \rangle \leq P_1$ and $\langle \xi_2, l \rangle \leq P_2$ for any affine sequence l of length 2^n, where P_1 and P_2 are positive integers. Then the nonlinearity of g satisfies $N_g \geq 2^n - \frac{1}{2}(P_1 + P_2)$.

Proof. Let $\xi = (\xi_1, \xi_2)$ be the sequence of g. Further, let α be an arbitrary affine function on $\mathbb{F}_2^{n+1}$ and we denote the sequence of α with L. Then L have to take the form of $L = (l, \pm l)$, where l is an affine sequence of length 2^n. Next, we note that $\langle \xi, L \rangle = \langle \xi_1, l \rangle \pm \langle \xi_2, l \rangle$ and thus $|\langle \xi, L \rangle| \leq P_1 + P_2$. By lemma 7.1, we have $d(g, \alpha) = 2^n - \frac{1}{2}\langle \xi, L \rangle$. From these discussions we have $d(g, \alpha) \geq 2^n - \frac{1}{2}(P_1 + P_2)$. Since α is arbitrary, we have $N_g \geq 2^n - \frac{1}{2}(P_1 + P_2)$. □

Bent functions do not exist for odd dimension. Thus, an interesting question is whether there are highly nonlinear functions on $\mathbb{F}_2^{2k+1}$. The following corollary is a special case from the previous lemma. It shows that such functions can be obtained by concatenating bent sequences.

Corollary 7.8. *In the construction (7.4), if both f_1 and f_2 are bent functions on $\mathbb{F}_2^{2k}$, then $N_g \geq 2^{2k} - 2^k$.*

Proof. In the proof of lemma 7.7, let $P_1 = P_2 = 2^k$. This proves the corollary. □

We provide yet another result concerning the concatenation of four functions.

Lemma 7.9. *[38] Let f_0, f_1, f_2 and f_3 be functions on $\mathbb{F}_2^n$ whose sequences are ξ_0, ξ_1, ξ_2 and ξ_3 respectively. Assume that $\langle \xi_i, l \rangle \leq P_i$ for each $0 \leq i \leq 3$ and for each affine sequence l of length 2^n, where each P_i is a positive integer. Let g be a function on $\mathbb{F}_2^{2n}$ defined by*

$$g(y, x) = \bigoplus_{i=0}^{3} D_{a_i}(y) f_i(x), \tag{7.5}$$

where $y = (y_1, y_2)$, $x = (x_1, \ldots, x_n)$ *and* a_i *as defined in definition* (2.1). *Then* $N_g \geq 2^{n+1} - \frac{1}{2}(P_0 + P_1 + P_2 + P_3)$. *In particular, if* n *is even and* f_0, f_1, f_2 *and* f_3 *are bent functions on* $\mathbb{F}_2^n$, *then* $N_g \geq 2^{n+1} - 2^{\frac{n}{2}+1}$.

Proof. Analogue to lemma 7.7. □

Furthermore, we generalize the previous lemma in the following way. Let $f_0, f_1, \ldots, f_{2^t-1}$ be functions on $\mathbb{F}_2^n$. We denote with ξ_i the sequence of f_i. Thus, we assume that $\langle \xi_i, l \rangle \geq P_i$ for each $0 \geq i \geq 2^t - 1$ and for each sequence l of length 2^n, where P_i is a positive integer. Hence, we define a function g on $\mathbb{F}_2^{n+t}$ by

$$g(y, x) = \bigoplus_{i=0}^{2^t-1} D_{a_i}(y) f_i(x), \tag{7.6}$$

where $y = (y_1, \ldots, y_n)$, $x = (x_1, \ldots, x_n)$ and a_i as defined in definition (2.1). Then $N_g \geq 2^{n+t-1} - \frac{1}{2}\sum_{i=0}^{2^t-1} P_i$. And in particular, when n is even and f_i, $i = 0, 1, \ldots, 2^t - 1$, are all bent functions on $\mathbb{F}_2^n$, then we have $N_g \geq 2^{n+t-1} - 2^{\frac{n}{2}+t-1}$.

We note that if we select proper starting functions in (7.4), (7.5) and (7.6), the resulting functions can be balanced. For instance, in (7.4), if both functions f_1 and f_2 are balanced, or the number of times that f_1 takes the value one is equal to that f_2 takes the value zero, hence the resulting function g is balanced.

7.2. Highly Nonlinear Balanced Functions

Bent functions have maximum nonlinearity and satisfy the SAC. They are not balanced and, hence, cannot be used directly in many cryptosystems, where balancedness is needed. We note that a bent function on $\mathbb{F}_2^n$ contains $2^{2k-1}+2^{k-1}$ ones and $2^{2k-1}-2^{k-1}$ zeros, or vice versa. Meier and Staffelbach [26] observed that by changing 2^{k-1} positions in a bent function, we get a balanced function having a nonlinearity of at least $2^{2k-1} - 2^k$. This nonlinearity is the same as that by concatenating four bent functions of length 2^{2k-2} (cf. lemma 7.9). First, we present a useful lemma.

Lemma 7.10. *Let* f_1 *be a function on* $\mathbb{F}_2^n$ *and* f_2 *be a function on* $\mathbb{F}_2^m$. *Then* $f_1(x_1, \ldots, x_n) \oplus f_2(y_1, \ldots, y_m)$ *is a balanced function on* $\mathbb{F}_2^{n+m}$ *if either* f_1 *or* f_2 *is balanced.*

Proof. Let $g(x_1, \ldots, x_n, y_1, \ldots, y_m) = f_1(x_1, \ldots, x_n) \oplus f_2(y_1, \ldots, y_m)$. Without loss of generality, we suppose that f_1 is balanced. Then for any vector $a \in \mathbb{F}_2^m$,

$$g(x_1, \ldots, x_n, a_1, \ldots, a_t) = f_1(x_1, \ldots, x_n) \oplus f_2(a_1, \ldots, a_t)$$

is a balanced function on $\mathbb{F}_2^n$. Thus, it follows immediately that g is a balanced function on $\mathbb{F}_2^{n+m}$. □

So far, we have constructed several (balanced) functions with several nonlinearity bounds. Let us turn our attention to construct SAC functions with high nonlinearity. Thus, we split our examination between odd and even dimensional vector spaces.

On odd dimensional vector space

Let $k \geq 1$ and we consider a bent function f and a non-constant affine function α. Both functions are on $\mathbb{F}_2^{2k}$ and $x = (x_1, \ldots, x_{2k})$. From theorem 6.34, we know that $f \oplus \alpha$ is also bent.
Without loss of generality, we may assume that f takes the value zero $2^{2k-1} + 2^{k-1}$ times (otherwise we replace f by $f \oplus 1$). By the same reasoning, we may assume that $f \oplus \alpha$ takes the value zero $2^{2k-1} - 2^{k-1}$ times. Let g be a function on $\mathbb{F}_2^{2k+1}$ defined by

$$\begin{aligned} g(u, x_1, \ldots, x_{2k}) &= (u \oplus 1) f(x_1, \ldots, x_{2k}) \oplus u \left(f(x_1, \ldots, x_{2k}) \oplus \alpha(x_1, \ldots, x_{2k}) \right) \\ &= f(x_1, \ldots, x_{2k}) \oplus u\alpha(x_1, \ldots, x_{2k}). \end{aligned} \tag{7.7}$$

Lemma 7.11. *The function g defined by (7.7) is a balanced function on $\mathbb{F}_2^{2k+1}$.*

Proof. We note that $g(0, x) = f(x)$ has $2^{2k-1} + 2^{k-1}$ zeros and $g(1, x) = f(x) \oplus \alpha(x)$ has $2^{2k-1} - 2^{k-1}$ zeros. Thus, the number of times g takes the value zero is $(2^{2k-1} + 2^{k-1}) + (2^{2k-1} - 2^{k-1}) = 2^{2k}$. Moreover, g has also 2^{2k} ones. Therefore, g is a balanced function. □

Lemma 7.12. *The function g defined by (7.7) has nonlinearity $N_g \geq 2^{2k} - 2^k$.*

Proof. Since $g(u, x) = f(x) \oplus u\alpha(x) = (u \oplus 1) f(x) \oplus u(f(x) \oplus \alpha(x))$ with f and $f \oplus \alpha$ are bent functions and $x = (x_1, \ldots, x_{2k})$. Then using lemma 7.7 and corollary 7.8, we deduce that $N_g \geq 2^{2k} - 2^k$. □

Lemma 7.13. *The function g defined by (7.7) satisfies the SAC.*

Proof. Let $e = (a_0, \ldots, a_{2k})$ be an arbitrary vector in $\mathbb{F}_2^{2k+1}$ with $wt(e) = 1$, $a = (a_1, \ldots, a_{2k})$, $z = (u, x_1, \ldots, x_{2k})$ and $x = (x_1, \ldots x_{2k})$. Then

$$g(z \oplus e) = f(x \oplus a) \oplus (u \oplus a_0)\alpha(x \oplus a)$$

and

$$g(z) \oplus g(z \oplus e) = f(x) \oplus f(x \oplus a) \oplus u(\alpha(x) \oplus \alpha(x \oplus a)) \oplus a_0\alpha(x \oplus a),$$

which we show to be balanced, that is equivalent to fulfill the SAC. We consider the following two cases:

(i) If $a_0 = 0$ and hence $wt(a) = 1$. Then $g(z) \oplus g(z \oplus e) = f(x) \oplus f(x \oplus a) \oplus u(\alpha(x) \oplus \alpha(x \oplus a))$. Since α is a non-constant affine function, so $\alpha(x) \oplus \alpha(x \oplus a) = c$, where c is a constant from $\mathbb{F}_2$. Thus, we have $g(z) \oplus g(z \oplus e) = f(x) \oplus f(x \oplus a) \oplus cu$. By (vi) of lemma 6.20, $f(x) \oplus f(x \oplus a)$ is a balanced function on $\mathbb{F}_2^{2k}$ and hence by lemma 7.10, $g(z) \oplus g(z \oplus e)$ is a balanced function on $\mathbb{F}_2^{2k+1}$.

(ii) If $a_0 = 1$ and hence $wt(a) = 0$, i.e. $a = (0, \ldots, 0)$, then $g(z) \oplus g(z \oplus e) = \alpha(x)$. Since α is a non-constant affine function on $\mathbb{F}_2^{2k}$, $\alpha(x)$ and $g(z) \oplus g(z \oplus e)$ are balanced.

Therefore, the function g satisfies the SAC. □

Summarizing the previous lemmas, we have

Theorem 7.14. *For $k \geq 1$, g defined by (7.7) is a balanced function on $\mathbb{F}_2^{2k+1}$, having $N_g \geq 2^{2k} - 2^k$ and satisfying the SAC.*

Example 12. [38] We consider the vector space $\mathbb{F}_2^5$. As we know, $f(x) = x_1x_2 \oplus x_3x_4$ is a bent function on $\mathbb{F}_2^4$. Furthermore, we choose the non-constant affine function $\alpha(x) = 1 \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_4$. We note that $f(x)$ takes the value zero $2^{4-1} + 2^{2-1} = 10$ times and $f(x) \oplus \alpha(x)$ takes the value zero $2^{4-1} - 2^{2-1} = 6$ times. According to (7.7) we have $g(u, x) = f(x) \oplus u\alpha(x) = x_1x_2 \oplus x_3x_4 \oplus u(1 \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_4)$. By theorem 7.14, it follows that g is balanced with $N_g \geq 2^4 - 2^2 = 12$ and satisfying the SAC. On the other hand we have corollary 7.6. By this corollary the nonlinearity of balanced functions is bounded from the above by $\lfloor\lfloor 2^4 - 2^{2-\frac{1}{2}}\rfloor\rfloor = \lfloor\lfloor 13, 1818\ldots\rfloor\rfloor = 12$. Therefore, the nonlinearity of g attains the upper bound for balanced functions on $\mathbb{F}_2^5$.

On even dimensional vector space

Let $k \geq 2$ and f be a bent function on $\mathbb{F}_2^{2k-2}$. We consider three non-constant affine functions α_1, α_2 and α_3 on $\mathbb{F}_2^{2k-2}$ such that $\alpha_i \oplus \alpha_j$ is non-constant for any $i \neq j$. Such affine functions exist for all $k \geq 2$. Moreover, we note that $x = (x_1, \ldots, x_{2k-2})$ and $f(x) \oplus \alpha_j(x)$ is bent. Without loss of generality, we may assume that both $f(x)$ and $f(x) \oplus \alpha_1(x)$ take the value one $2^{2k-3} + 2^{k-2}$ times while both $f(x) \oplus \alpha_2(x)$ and $f(x) \oplus \alpha_3(x)$ take the value one $2^{2k-3} - 2^{k-2}$ times. This assumption is reasonable because $f(x) \oplus \alpha_j(x)$ takes the value one $2^{2k-3} + 2^{k-2}$ times if and only if $f(x) \oplus \alpha_j(x) \oplus 1$ takes the value one $2^{2k-3} - 2^{k-2}$ times. Additionally, $\alpha_j(x) \oplus 1$ is also a non-constant affine function. Therefore, we can choose either $f(x) \oplus \alpha_j(x)$ or $f(x) \oplus \alpha_j(x) \oplus 1$ and the assumption is satisfied. Now, let g be a function on $\mathbb{F}_2^{2k}$ defined by

$$\begin{aligned} g(u, v, x_1, \ldots, x_{2k-2}) =& (u \oplus 1)(v \oplus 1)f(x) \oplus (u \oplus 1)v(f(x) \oplus \alpha_1(x)) \\ & \oplus u(v \oplus 1)(f(x) \oplus \alpha_2(x)) \oplus uv(f(x) \oplus \alpha_3(x)) \\ =& f(x) \oplus v\alpha_1(x) \oplus u\alpha_2(x) \oplus uv(\alpha_1(x) \oplus \alpha_2(x) \oplus \alpha_3(x)). \end{aligned} \tag{7.8}$$

Lemma 7.15. *The function g defined by (7.8) is a balanced function on $\mathbb{F}_2^{2k}$.*

Proof. We note that $g(0, 0, x) = f(x)$ and $g(0, 1, x) = f(x) \oplus \alpha_1(x)$ take the value zero $2^{2k-3} + 2^{k-2}$ times. Furthermore, $g(1, 0, x) = f(x) \oplus \alpha_2(x)$ and $g(1, 1, x) = f(x) \oplus \alpha_3(x)$ take the value zero $2^{2k-3} - 2^{k-2}$ times. Thus, the function g takes the value zero 2^{k-2} times and hence g is a balanced function on $\mathbb{F}_2^{2k}$. □

Lemma 7.16. *The function g defined by (7.8) has nonlinearity $N_g \geq 2^{2k-1} - 2^k$.*

Proof. Analogue to the proof of lemma 7.12. □

Lemma 7.17. *The function g defined by (7.8) satisfies the SAC.*

Proof. The proof is similar to the proof of lemma 7.13. Let $e = (b, c, a_1, \ldots a_{2k-2})$ be an arbitrary vector in $\mathbb{F}_2^{2k}$ with $wt(e) = 1$, $a = (a_1, \ldots, a_{2k-2})$, $z = (u, v, x_1, \ldots, x_{2k-2})$ and $x = (x_1, \ldots, x_{2k-2})$. Then

$$\begin{aligned} g(z \oplus e) =& f(x \oplus a) \oplus (v \oplus c)\alpha_1(x \oplus a) \oplus (u \oplus b)\alpha_2(x \oplus a) \\ & \oplus (v \oplus c)(u \oplus b)(\alpha_1(x \oplus a) \oplus \alpha_2(x \oplus a) \oplus \alpha_3(x \oplus a)). \end{aligned}$$

We consider the balancedness of $g(z) \oplus g(z \oplus e)$ in the following three cases.

(i) If $b = 1$, $c = 0$ and hence $wt(a) = 0$. Therefore, we have $g(z) \oplus g(z \oplus e) = \alpha_2(x) \oplus v(\alpha_1(x) \oplus \alpha_2(x) \oplus \alpha_3(x))$.
If $v = 0$, then $g(z) \oplus g(z \oplus e) = \alpha_2(x)$. And if $v = 1$, then $g(z) \oplus g(z \oplus e) = \alpha_1(x) \oplus \alpha_3(x)$. Both functions $\alpha_2(x)$ and $\alpha_1(x) \oplus \alpha_3(x)$ are non-constant affine functions on $\mathbb{F}_2^{2k-2}$ and hence $g(z) \oplus g(z \oplus e)$ is a balanced function on $\mathbb{F}_2^{2k}$.

(ii) If $b = 0$, $c = 1$ and hence $wt(a) = 0$. The proof of balancedness is similar to (i).

(iii) If $b = 0$, $c = 0$ and hence $wt(a) = 1$. Since α_j is an affine function we have that $\alpha_j(x) \oplus \alpha_j(x \oplus a) = a_j$, where a_j is a constant from $\mathbb{F}_2$. Therefore, we have $g(z) \oplus g(z \oplus e) = f(x) \oplus f(x \oplus a) \oplus va_1 \oplus ua_2 \oplus uv(a_1 \oplus a_2 \oplus a_3)$. By lemma 6.20($vi$), we have that $f(x) \oplus f(x \oplus a)$ is a balanced function on $\mathbb{F}_2^{2k-2}$ and hence by lemma 7.10 we have that $g(z) \oplus g(z \oplus e)$ is a balanced function on $\mathbb{F}_2^{2k}$.

This proves that g satisfies the SAC. □

Summarizing the previous lemmas we have

Theorem 7.18. *For $k \geq 2$, the function g defined by* (7.8) *is a balanced function on $\mathbb{F}_2^{2k}$, having $N_g \geq 2^{2k-1} - 2^k$ and satisfying the SAC.*

Example 13. [38] We consider the vector space $\mathbb{F}_2^6$. We choose the bent function $f(x) = x_1x_2 \oplus x_3x_4$. Moreover, we choose the affine functions $\alpha_1(x) = x_1$, $\alpha_2(x) = x_2 \oplus 1$ and $\alpha_3(x) = x_3 \oplus 1$. We obtain that $f(x)$ and $f(x) \oplus \alpha_1(x)$ take the value one $2^{4-1} - 2^{2-1} = 6$ times while both $f(x) \oplus \alpha_2(x)$ and $f(x) \oplus \alpha_3(x)$ take the value one $2^{4-1} + 2^{2-1} = 10$ times. According to (7.8), we have $g(u, v, x) = f(x) \oplus v\alpha_1(x) \oplus u\alpha_2(x) \oplus uv(\alpha_1(x) \oplus \alpha_2(x) \oplus \alpha_3(x))$. By theorem 7.18, it follows that g is balanced with $N_g \geq 2^5 - 2^3 = 24$ and satisfying the SAC. We can compare N_g with the upper bound for the nonlinearities of balanced functions on $\mathbb{F}_2^6$ which is $2^5 - 2^2 - 2 = 26$.Therefore, the function g does not attain the upper bound of nonlinearity.

7.3. Construction of Highly Nonlinear Balanced Functions Satisfying High Degree Propagation Criterion

7.3.1. Basic Construction

Preneel et al. [35] suggested that a Boolean function $\mathbb{F}_2^n$ which has a zero point in its Walsh spectrum can be modified into a balanced function by adding a suitable linear

function α on $\mathbb{F}_2^n$. The problem is that α has to be found by an exhaustive search over all the linear functions on $\mathbb{F}_2^n$. Obviously, this method is infeasible when n is large. Furthermore, this method is not applicable to the functions which do not have zero points in its Walsh spectra. These functions include bent functions.
Seberry et al. [38] introduced a new method for systematically constructing highly nonlinear balanced functions satisfying the propagation criterion. The starting point of this construction are bent functions. We split our examination for odd and even dimensional vector spaces. If n is odd, we construct balanced functions satisfying the propagation criterion with respect to all nonzero vectors expect $\omega = (1, 0, \ldots, 0)$. And if n is even, we construct balanced functions that satisfying the propagation criterion with respect to all but three nonzero vectors, that is $\omega_1 = (1, 0, \ldots, 0)$, $\omega_2 = (0, 1, 0, \ldots, 0)$ and $\omega_3 = \omega_1 \oplus \omega_2 = (1, 1, 0, \ldots, 0)$.

On odd dimensional vector space

Let $n = 2k$ and $k \geq 1$. We consider a bent function f on $\mathbb{F}_2^{2k}$ and let g be a function on $\mathbb{F}_2^{2k+1}$ defined by

$$\begin{aligned} g(x_1, \ldots, x_{2k+1}) &= (x_1 \oplus 1) f(x_2, \ldots, x_{2k+1}) \oplus x_1 (1 \oplus f(x_2, \ldots, x_{2k+1})) \\ &= x_1 \oplus f(x_2, \ldots, x_{2k+1}). \end{aligned} \tag{7.9}$$

The following lemma presents the result that the defined function g satisfies the propagation criterion

Lemma 7.19. *The function g defined in* (7.9) *satisfies the propagation criterion with respect to all nonzero vectors $\omega \in \mathbb{F}_2^{2k+1}$ with $\omega \neq (1, 0, \ldots, 0)$.*

Proof. Let $\omega = (a_1, a_2, \ldots, a_{2k+1}) \neq (1, 0, \ldots, 0)$ and let $x = (x_1, \ldots, x_{2k+1})$. Then we have $g(x) \oplus g(x \oplus \omega) = a_1 \oplus f(x_2, \ldots, x_{2k+1}) \oplus f(x_2 \oplus a_2, \ldots, x_{2k+1} \oplus a_{2k+1})$. By (vi) of theorem 6.20, we have that since f is bent the directional derivative $f(x_2, \ldots, x_{2k+1}) \oplus f(x_2 \oplus a_2, \ldots, x_{2k+1} \oplus a_{2k+1})$ is balanced for all $(a_2, \ldots, a_{2k+1}) \neq (0, \ldots, 0)$. Thus, $g(x) \oplus g(x \oplus \omega)$ is balanced for all $\omega = (a_1, a_2, \ldots, a_{2k+1}) \neq (1, 0 \ldots, 0)$. □

Corollary 7.20. *The function g defined by* (7.9) *is balanced and satisfies the propagation criterion with respect to all nonzero vectors $\omega \in \mathbb{F}_2^{2k+1}$ with $\omega = (1, 0, \ldots, 0)$. The nonlinearity of g satisfies $N_g \geq 2^{2k} - 2^k$.*

Proof. The function g is balanced by lemma 7.10. That g satisfies the propagation criterion with respect to all nonzero vectors $\omega \in \mathbb{F}_2^{2k+1}$ with $\omega \neq (1, 0, \ldots, 0)$ follows from the previous lemma 7.19. And the nonlinearity follows from corollary 7.8. □

On even dimensional vector space

Let $n = 2k$ and $k \geq 2$ and f be a bent function on $\mathbb{F}_2^{2k-2}$. Let g be a function on $\mathbb{F}_2^{2k}$ defined by

$$\begin{aligned} g(x_1, x_2, \ldots, x_{2k}) =& (x_1 \oplus 1)(x_2 \oplus 1) f(x_3, \ldots x_{2k}) \oplus (x_1 \oplus 1) x_2 (1 \oplus f(x_3, \ldots, x_{2k})) \oplus \\ & x_1 (x_2 \oplus 1)(1 \oplus f(x_3, \ldots, x_{2k})) \oplus x_1 x_2 f(x_3, \ldots, x_{2k}) \\ =& x_1 \oplus x_2 f(x_3, \ldots, x_{2k}). \end{aligned} \tag{7.10}$$

The following lemma shows that the defined function g satisfies the propagation criterion

Lemma 7.21. *The function g defined by* (7.10) *satisfies the propagation criterion with respect to all but three nonzero vectors in $\mathbb{F}_2^{2k}$. The three vectors are $\omega_1 = (1, 0, \ldots, 0)$, $\omega_2 = (0, 1, 0, \ldots 0)$ and $\omega_3 = \omega_1 \oplus \omega_2 = (1, 1, 0, \ldots, 0)$.*

Proof. Let $\omega = (a_1, \ldots, a_{2k})$ be a nonzero vector in $\mathbb{F}_2^{2k}$ differing from ω_1, ω_2 and ω_3. Furthermore, let $x = (x_1, \ldots, x_{2k})$ and we have $g(x) \oplus g(x \oplus \omega) = a_1 \oplus a_2 \oplus f(x_3, \ldots x_{2k}) \oplus f(x_3 \oplus a_3, \ldots x_{2k} \oplus a_{2k})$. By (vi) of theorem 6.20, we have that since f is bent on $\mathbb{F}_2^{2k-2}$ and $(a_3, \ldots, a_{2k}) \neq (0, \ldots, 0)$, the directional derivative $f(x_3, \ldots x_{2k}) \oplus f(x_3 \oplus a_3, \ldots x_{2k} \oplus a_{2k})$ is balanced. Thus, $g(x) \oplus g(x \oplus \omega)$ is balanced for any nonzero vector in $\mathbb{F}_2^{2k}$ differing from ω_1, ω_2 and ω_3. □

Corollary 7.22. *The function g defined by* (7.10) *is balanced and satisfies the propagation criterion to all nonzero vectors $\omega \in \mathbb{F}_2^{2k}$ with $\omega \neq (c_1, c_2, 0, \ldots, 0)$ with $c_1, c_2 \in \mathbb{F}_2$. The nonlinearity of g satisfies $N_g \geq 2^{k-1} - 2^k$.*

Proof. Balancedness follows from the fact that since $x_1 \oplus x_2$ is balanced on $\mathbb{F}_2^2$, then g is balanced on $\mathbb{F}_2^{2k}$. g satisfies the propagation criterion with respect to all nonzero vectors $\omega \in \mathbb{F}_2^{2k}$ differing from ω_1, ω_2 and ω_3, that follows from the previous lemma 7.21. The statement about nonlinearity follows from corollary 7.8. □

The functions constructed in (7.9) and (7.10) satisfy the propagation criterion with respect to all but one or three nonzero vectors. Thus, they only fulfill the propagation criterion of degree zero. Therefore, these functions are not interesting in practical applications. Moreover, we introduce a method given by Seberry et al. [38] that transforms the vectors where the propagation criterion is not satisfied into vectors with high Hamming-weight. This provides the possibility to obtain functions satisfying high degree propagation criterion.

7.3.2. Improved Construction

We recall that balancedness, nonlinearity and the number of vectors where the propagation criterion is satisfied are all invariant under an affine transformation of the coordinates.
Seberry et al. [38] used such a transformation for the vectors where the propagation criterion is not satisfied to obtain vectors having a high Hamming-weight. In this way, we obtain highly nonlinear balanced functions satisfying high degree propagation criterion.

On odd dimensional vector space

Theorem 7.23. *Let $k \geq 1$ and for any nonzero vector $\omega^* \in \mathbb{F}_2^{2k+1}$, there exist balanced functions on $\mathbb{F}_2^{2k+1}$ satisfying the propagation criterion with respect to all nonzero vectors $\omega \in \mathbb{F}_2^{2k+1}$ with $\omega \neq \omega^*$. The nonlinearity of the functions are at least $2^{2k} - 2^k$.*

Proof. Let f be a bent function and let g be the function constructed by (7.9). From linear algebra, we know that there exists a unique nonsingular matrix A of order $2k+1$ with entries from $\mathbb{F}_2$ such that $\alpha_j \cdot A = \beta_j$, $j = 1, \ldots, 2^k + 1$, where we have the bases B_1 and B_2 of the vector space $\mathbb{F}_2^{2k+1}$ with $B_1 = \{\alpha_j | j = 1, \ldots, 2k+1\}$ and $B_2 = \{\beta_j | j = 1, \ldots, 2k+1\}$. In particular, this is true when $\alpha = \omega^*$ and $\beta_1 = (1, 0, \ldots, 0)$. Furthermore, let $x = (x_1, \ldots, x_{2k+1})$ and we denote with g^* the function obtained from g by a affine transformation on the input of g, that is

$$g^*(x) = g(Ax).$$

Since the matrix A is nonsingular, the function g^* is balanced and has the same nonlinearity as g.This follows from the invariance of nonlinearity and balancedness of an affine transformation of the input coordinates. By corollary 7.20 the nonlinearities of the functions are at least $2^{2k} - 2^k$. In the next step we show that g^* satisfies the propagation criterion with respect to all nonzero vectors except ω^*.
Now let ω be a nonzero vector in $\mathbb{F}_2^{2k+1}$ with $\omega \neq \omega^*$. We consider the following function $g^*(x) \oplus g^*(x \oplus \omega) = g(Ax) \oplus g(Ax \oplus A\omega)$. Since A is nonsingular Ax runs through $\mathbb{F}_2^{2k+1}$ while x runs through $\mathbb{F}_2^{2k+1}$. Furthermore, since $\omega \neq \omega^*$ we have $A\omega \neq (1, 0, \ldots, 0)$. Using lemma 7.19, we obtain that $g(Ax) \oplus g(Ax \oplus A\omega)$ takes the value zero and one an equal number of times. Therefore, it follows that $g^*(x) \oplus g^*(x \oplus \omega)$ is balanced. Consequently, we have that g^* satisfies the propagation criterion with respect to all nonzero vectors in $\mathbb{F}_2^{2k+1}$ but ω^*. □

By letting $\omega^* = (1, \ldots, 1)$, we obtain highly nonlinear balanced functions on $\mathbb{F}_2^{2k+1}$ satisfying the propagation criterion of degree $2k$.

Corollary 7.24. *Let $k \geq 1$ and f be a bent function on $\mathbb{F}_2^{2k}$ and let $g^*(x_1, \ldots, x_{2k+1}) = x_1 \oplus f(x_1 \oplus x_2, x_1 \oplus x_3, \ldots, x_1 \oplus x_{2k+1})$. Then g^* is a balanced function on $\mathbb{F}_2^{2k+1}$ and satisfies the propagation criterion of degree $2k$. The nonlinearity of g^* satisfies $N_g \geq 2^{2k} - 2^k$.*

Proof. We denote with e_j the vector in $\mathbb{F}_2^{2k+1}$ whose jth coordinate is one and all the other coordinates are zero, $j = 1, \ldots, 2k+1$. Furthermore, we use the conditions of theorem 7.23. Let $\alpha_1 = \omega_0 = (1, \ldots, 1)$, $\alpha_j = e_j$ for $j = 2, \ldots, 2k+1$, and $\beta_j = e_j$ for $j = 1, \ldots, 2k+1$. Then there is a unique nonsingular matrix A of order $2k+1$ such that $\alpha_j \cdot A = \beta_j$, $j = 1, \ldots, 2k+1$, where A has the following form

$$A = \begin{bmatrix} \omega_0 \\ e_2 \\ \vdots \\ e_{2k+1} \end{bmatrix}.$$

We have $x = (x_1, \ldots, x_{2k+1})$. Furthermore, we obtain $g^*(x) = g(Ax) = g(x_1, x_1 \oplus x_2, \ldots, x_1 \oplus x_{2k+1}) = x_1 \oplus f(x_1 \oplus x_2, \ldots, x_1 \oplus x_{2k+1})$, where $g(x) = x_1 \oplus f(x_2, \ldots, x_{2k+1})$, cf. (7.9). From theorem 7.23, we know that g^* satisfies the propagation criterion with respect to all nonzero vectors in $\mathbb{F}_2^{2k+1}$ except the all-one vector $\omega^* = (1, \ldots, 1)$. Consequently, we have that g^* satisfies the propagation criterion of degree $2k$. The nonlinearity follows from the invariance of the transformation and corollary 7.20. □

On even dimensional vector space

Theorem 7.25. *Let $k \geq 2$ and for any nonzero vector $\omega_1^*, \omega_2^* \in \mathbb{F}_2^{2k}$ with $\omega_1^* \neq \omega_2^*$, there exist balanced functions on $\mathbb{F}_2^{2k}$ satisfying the propagation criterion with respect to all but three nonzero vectors in $\mathbb{F}_2^{2k}$. The three vectors where the propagation criterion is not satisfied are ω_1^*, ω_2^* and $\omega_3^* = \omega_1^* \oplus \omega_2^*$. The nonlinearities of the functions are at least $2^{2k-1} - 2^k$.*

Proof. The proof is basically analogue to theorem 7.23. The main difference is the choice of the bases. We choose the bases $B_1 = \{\alpha_j | j = 1, \ldots, 2k\}$ and $B_2 = \{\beta_j | j = 1, \ldots, 2k\}$. Let $\alpha_1 = \omega_1^*$, $\alpha_2 = \omega_2^*$, $\beta_1 = (1, 0, \ldots, 0)$ and $\beta_2 = (0, 1, 0 \ldots, 0)$. Analogue to theorem 7.23, it is obvious g^* defined by $g^*(x) = g(Ax)$ satisfies the propagation criterion with respect to all but the following three nonzero vectors ω_1^*, ω_2^* and $\omega_3^* = \omega_1^* \oplus \omega_2^*$ in $\mathbb{F}_2^{2k}$. Now $x = (x_1, \ldots, x_{2k})$, we have $g(x) = x_1 \oplus x_2 \oplus f(x_3, \ldots, x_{2k})$, and f is bent on $\mathbb{F}_2^{2k-2}$, are the same as in (7.10). Furthermore, A is a nonsingular matrix such that $\alpha_j \cdot A = \beta_j$, $j = 1, \ldots, 2k$. The nonlinearity follows by the invariance of the transformation and corollary 7.22. □

Corollary 7.26. *Suppose that $2k = 3t + c$ where $c = 0, 1$ or 2. Then there exist balanced functions on $\mathbb{F}_2^{2k}$ that satisfy the propagation criterion of degree $2t - 1$ (when $c = 0$ or 1), or $2t$ (when $c = 2$). The nonlinearities of the functions are at least $2^{2k-1} - 2^k$.*

Proof. We set $c_1 = 0$, $c_2 = 1$ if $c = 1$ and we set $c_1 = c_2 = \frac{1}{2}c$ otherwise. Further let $\omega_1^* = (a_1, \ldots, a_{3t+c})$ and $\omega_2^* = (b_1, \ldots, b_{3t+c})$, where

$$a_j = \begin{cases} 1 & \text{for } j = 1, \ldots, 2t + c_1 \\ 0 & \text{for } j = 2t + c_1 + 1, \ldots, 3t + c \end{cases}$$

and

$$b_j = \begin{cases} 0 & \text{for } j = 1, \ldots, t + c_1 \\ 1 & \text{for } j = t + c_1 + 1, \ldots, 3t + c. \end{cases}$$

We know from theorem 7.25 that there exists a balanced function g^* on $\mathbb{F}_2^{2k}$ satisfying the propagation criterion with respect to all but three nonzero vectors. The vectors are ω_1^*, ω_2^* and $\omega_3^* = \omega_1^* \oplus \omega_2^*$ and the nonlinearity of g^* satisfies $N_{g^*} \geq 2^{2k-1} - 2^k$.
Furthermore, we have the Hamming-weights $wt(\omega_1^*) = 2t + c_1$, $wt(\omega_2^*) = 2t + c_2$ and $wt(\omega_3^*) = 2t + c$. The minimum Hamming-weight among the three Hamming-weights is

$2t+c_1$. Therefore, it follows that for any nonzero vector $\omega \in \mathbb{F}_2^{2k}$ with $wt(\omega) \leq 2t+c_1-1$, we have $\omega \neq \omega_1^*$, ω_2^* or ω_3^*. From theorem 7.25 we know that $g^*(x) \oplus g^*(x \oplus \omega)$ is balanced. Thus, we conclude that g^* satisfies the propagation criterion of order $2t+c_1-1$. If $c = 0$ or 1 we have $c_1 = 0$, and if $c = 2$ then $c_1 = 1$. This completes the proof. □

8. Relationships between Cryptographic Properties

8.1. Relation between Nonlinearity and Correlation Immunity

In this section, we obtain the relationship between nonlinearity and correlation immunity. First of all, we show two results given by Chee et al.[8] for arbitrary Boolean functions. Afterwards, we give a much stronger result using balanced functions.

Lemma 8.1. *Let f be a Boolean function in n variables and we define*

$$\eta(f) = \left|\left\{w \in \mathbb{F}_2^n : W(\widehat{f})(w) \neq 0\right\}\right|.$$

Then $N_f \leq 2^{n-1} - 2^{n-1}\eta(f)^{-\frac{1}{2}}$.

Proof. By Parseval's equation (3.6) we have

$$2^{2n} = \sum_{w\in\mathbb{F}_2^n} W(\widehat{f})(w)^2 \leq \eta(f) \max_{w\in\mathbb{F}_2^n} \left|W(\widehat{f})(w)\right|^2,$$

so it follows that $\max_{w\in\mathbb{F}_2^n} \left|W(\widehat{f})(w)\right|^2 \geq 2^n\eta(f)^{-\frac{1}{2}}$. Using theorem 3.18 we have

$$N_f = 2^{n-1} - \frac{1}{2}\max_{w\in\mathbb{F}_2^n}\left|W(\widehat{f})(w)\right| \leq 2^{n-1} - 2^{n-1}\eta(f)^{-\frac{1}{2}}.$$

□

Lemma 8.2. *If f is any Boolean function in n variables which is correlation immune of order k and $\mu(n,k) = 2^n - \sum_{i=1}^{k}\binom{n}{i}$, then $N_f \leq 2^{n-1} - 2^{n-1}\mu(n,k)^{-\frac{1}{2}}$.*

Proof. Since f is correlation immune of order k, lemma 4.3 implies that

$$\begin{aligned}\eta(f) &= 2^n - \left|\left\{w \in \mathbb{F}_2^n : W(\widehat{f})(w) = 0\right\}\right| \\ &\leq 2^n - |\{w \in \mathbb{F}_2^n : 1 \leq wt(w) \leq k\}| = \mu(n,k).\end{aligned}$$

Thus, $N_f \leq 2^{n-1} - 2^{n-1}\mu(n,k)^{-\frac{1}{2}}$ follows from lemma 8.1. □

The result of lemma 8.1 is given independently by Zhang and Zheng [49]. Moreover, they proved the case when even equality holds in the inequality of lemma 8.1. Therefore, they introduced a new class of functions which they named *plateaued functions.*

Definition 8.3. *Let f be a Boolean function on $\mathbb{F}_2^n$ and ξ_f denote the $(1,-1)$-sequence of f. If there exists an even integer r, $0 \leq r \leq n$, such that $\left|\left\{w \in \mathbb{F}_2^n : W(\widehat{f})(w) \neq 0\right\}\right| = 2^r$ and each integer $W(\widehat{f})(w)^2$ has the value 0 or 2^{2n-r}, then f is called a* **plateaued function** of order r on $\mathbb{F}_2^n$. *f is also simply called a plateaued function on $\mathbb{F}_2^n$ if reference to the order r is not needed.*

Lemma 8.4. *Let f be a Boolean function on $\mathbb{F}_2^n$. Equality holds in the inequality of lemma 8.1 if and only if the function f is plateaued.*

Proof. For convenience, we define

$$\Theta_f = \max_{w \in \mathbb{F}_2^n} \left| W(\widehat{f})(w) \right|.$$

We assume that f is a plateaued function. Thus, there exists an even integer r, $0 \leq r \leq n$, such that $\eta(f) = 2^r$ and each $W(\widehat{f})(w)^2$ takes either the value 0 or 2^{2n-r}. Hence, we have $\Theta_f = 2^{n-\frac{r}{2}}$. Using theorem 3.18, we have

$$N_f = 2^{n-1} - \frac{1}{2} \cdot 2^{n-\frac{r}{2}} = 2^{n-1} - 2^{n-1}\eta(f)^{-\frac{1}{2}}.$$

Conversely, we assume that the equality holds in lemma 8.1. From theorem 3.18, we have also $N_f = 2^{n-1} - \frac{1}{2}\Theta_f$. Hence, it follows $2^n = \Theta_f \cdot \eta(f)^{\frac{1}{2}}$. Since both $\eta(f)^{\frac{1}{2}}$ and Θ_f are integers and in fact powers of 2, it follows that $\eta(f) = 2^r$ for some even integer r, $0 \leq r \leq n$, and $\Theta_f = 2^{n-\frac{r}{2}}$. Using Parseval's equation (3.6), we can conclude that the only nonzero value of $W(\widehat{f})(w)$ is 2^{2n-r}. This proves that f is a plateaued function. □

The following lemma is a restatement of a relation given by Carlet [4]. It will be useful proving some of the following results.

Lemma 8.5. *For every Boolean function f on $\mathbb{F}_2^n$, we have*

$$(r_f(a_0), r_f(a_1), \ldots, r_f(a_{2^n-1})) \cdot H_n = \left(\langle \xi_f, l_0 \rangle^2, \langle \xi_f, l_1 \rangle^2, \ldots, \langle \xi_f, l_{2^n-1} \rangle^2\right), \tag{8.1}$$

where ξ denotes the $(1,-1)$-sequence of f, l_i is the ith row of H_n, and a_i as defined in definition 2.1, $i = 0, 1, \ldots, 2^n - 1$.

We present an important inequality given by Zhang and Zheng [49] which is helpful to understand properties of plateaued functions.

Theorem 8.6. *Let f be a Boolean function on $\mathbb{F}_2^n$ whose $(1,-1)$- sequence is denoted by ξ_f. Then*

$$\sum_{j=0}^{2^n-1} r_f^2(a_j) \geq \frac{2^{3n}}{\eta(f)},$$

where the equality holds if and only if f is a plateaued function on $\mathbb{F}_2^n$.

Proof. See [49]. □

The next result relates the autocorrelation function to nonlinearity.

Theorem 8.7. *Let f be a Boolean function on $\mathbb{F}_2^n$ whose $(1,-1)$-sequence is ξ_f. Then the nonlinearity of f satisfies*

$$N_f \leq 2^{n-1} - 2^{-\frac{n}{2}-1} \left(\sum_{j=0}^{2^n-1} r_f^2(a_j) \right)^{\frac{1}{2}},$$

where a_j is defined in (2.1)*. Equality holds if and only if f is a plateaued function on $\mathbb{F}_2^n$.*

Proof. Let $\Theta_f = \max\{|\langle \xi_f, l_j \rangle|, j = 0, 1, \ldots, 2^n - 1\}$, and we multiply equation (8.1) by itself and obtain

$$2^n \sum_{j=0}^{2^n-1} r_f^2(a_j) = \sum_{j=0}^{2^n-1} \langle \xi_f, l_j \rangle^4 \leq \Theta_f^2 \sum_{j=0}^{2^n-1} \langle \xi_f, l_j \rangle^2.$$

Using Parseval's equation (7.1), we have

$$\sum_{j=0}^{2^n-1} r_f^2(a_j) \leq 2^n \Theta_f^2.$$

Hence, we have

$$\Theta_f \geq 2^{-\frac{n}{2}} \left(\sum_{j=0}^{2^n-1} r_f^2(a_j) \right)^{\frac{1}{2}}.$$

Using theorem 3.18, we proved the inequality $N_f \leq 2^{n-1} - 2^{-\frac{n}{2}-1} \left(\sum_{j=0}^{2^n-1} r_f^2(a_j) \right)^{\frac{1}{2}}$. The equality follows by using lemma 8.4 and theorem 8.6. □

In the next theorem, we use the property of balancedness to obtain a kind of trade-off between nonlinearity and correlation immunity. This theorem is given by Tarannikov [42] and we follow his proof.

Theorem 8.8. *Let f be a balanced and correlation immune function of order k, $k \leq n-2$, then*

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

Proof. We start with the case $k = n-2$. By using theorem 4.7, we obtain that f is affine and thus $N_f = 0$.
We denote with $f(x|x_{i(1)} = c_1, \ldots, x_{i(t)} = c_t)$ the function in $n-t$ variables obtained from

$f(x)$ by setting $x_{i(1)}, \ldots, x_{i(t)}$ equal to $c_1, \ldots, c_t$. We call such a function a subfunction of f.

Now, we consider the case $k \leq n-3$. We may assume that the function is correlation immune of order k but not of order $k+1$. The generalization of lemma 4.2(iv) gives that the function f has a subfunction $f(x|x_{i(1)} = a_1, \ldots, x_{i(k+1)} = a_{k+1}) = g$ in $n-k-1$ variables such that $wt(g) = w \neq 2^{n-k-2}$. We may assume $w < 2^{n-k-2}$ since

$$wt(f) = 2^{n-1} = \sum_{(c_1,\ldots,c_{k+1})} wt(f(x|x_{i(1)} = c_1, \ldots, x_{i(k+1)} = c_{k+1})),$$

where the sum is over all the 2^{k+1} possible choices of $c_1, \ldots, c_{k+1}$. If this sum has a term greater than 2^{n-k-2}, then it also has a term less than 2^{n-k-2}. Furthermore, we consider a subfunction $f(x|x_{i(1)} = b_1, \ldots, x_{i(k+1)} = b_{k+1}) = h$, where the given fixed vector $a = (a_1, \ldots, a_{k+1})$ and the vector $b = (b_1, \ldots, b_{k+1})$ only differ in the jth coordinate. Since f is correlation immune of order k, we have with the generalization of lemma 4.2(iv) that

$$\begin{aligned} wt(g) + wt(h) &= wt(f(x|x_{i(1)} = a_1, \ldots, x_{i(j-1)} = a_{j-1}, x_{i(j+1)} = a_{j+1}, \ldots, x_{i(k+1)} = a_{k+1})) \\ &= 2^{n-k-1}. \end{aligned}$$

This gives

$$wt(h) = 2^{n-k-1} - w. \tag{8.2}$$

Moreover, we consider a subfunction $h_1 = f(x|x_{i(1)} = b_1, \ldots, x_{i(k+1)} = b_{k+1})$, where the vector b differs from the given vector a in exactly two coordinates $j(1)$ and $j(2)$. Thus, we have $x_{j(1)} = c$ and $x_{j(2)} = d$ in vector a and $x_{j(1)} = c \oplus 1$ and $x_{j(2)} = d \oplus 1$ in vector b. Furthermore, we denote with h_2 and h_3 the subfunctions with the same values as in h_1 expect that $x_{j(1)} = c$ in h_2 and $x_{j(2)} = d$ in h_3. Using the same argument which gives (8.2) we have

$$wt(h_2) = wt(h_3) = 2^{n-k-1} - w. \tag{8.3}$$

Since f is correlation immune of order k, we have

$$wt(h_1) + wt(h_3) = 2^{n-k-1}. \tag{8.4}$$

Using (8.3) and (8.4) together gives $wt(h_1) = w$. Thus, it follows that we have for any vector b

$$wt(f(x|x_{i(1)} = b_1, \ldots, x_{i(k+1)} = b_{k+1})) = \begin{cases} h, & \text{if } d(a,b) \text{ is even} \\ 2^{n-k-1} - h, & \text{if } d(a,b) \text{ is odd.} \end{cases}$$

Moreover, we define an affine function l in n variables by

$$l = \sum_{j=1}^{k+1} x_{i(j)} \oplus A,$$

where $A \equiv wt(a) \mod 2$ is 0 or 1. Then, we compute

$$\begin{aligned} d(f,l) &= \sum_{(b_1,\ldots,b_{k+1})} d\left(f(x|x_{i(1)}=b_1,\ldots,x_{i(k+1)}=b_{k+1}), \sum_{j=1}^{k+1} b_{i(j)} \oplus A\right) \\ &= \sum_{b\in\mathbb{F}_2^n,\ d(a,b) \text{ even}} wt\left(f(x|x_{i(1)}=b_1,\ldots,x_{i(k+1)}=b_{k+1})\right) \\ &+ \sum_{b\in\mathbb{F}_2^n,\ d(a,b) \text{ odd}} 2^{n-k-1} - wt\left(f(x|x_{i(1)}=b_1,\ldots,x_{i(k+1)}=b_{k+1})\right) \\ &= 2^k w + 2^k w = 2^{k+1} w, \end{aligned}$$

where the second equality is true by the fact that $\sum_{j=1}^{k+1} b_{i(j)} \oplus A$ is 1 if $d(a,b)$ is odd and the sum vanishes if $d(a,b)$ is even. Hence, we have

$$N_f \le d(f,l) = 2^{k+1} w \le 2^{k+1}\left(2^{n-k-2}-1\right) = 2^{n-1} - 2^{k+1}.$$

□

Zhang and Zheng [47] independently arrived to the same result as Tarannikov [42]. Their proof is more complicated because they also proved when equality can occur and further they showed that under certain conditions the inequality holds even the function is not balanced.
We can refine theorem 8.8 and show that equality is possible if the Boolean function has its maximum possible algebraic degree, cf. 4.7.

Theorem 8.9. *Let f be a balanced Boolean function in n variables which is correlation immune of order $k \le n-2$. Then equality is possible in theorem 8.8 only if f has its maximum possible degree $n-k-1$. If $\deg f < n-k-1$, then $N_f \le 2^{n-1} - 2^{k+2}$.*

Proof. We use the same subfunction g as in the proof of theorem 8.8. So $f(x|x_{i(1)} = a_1,\ldots,x_{i(k+1)} = a_{k+1}) = g$ which has $wt(g) = w < 2^{n-k-2}$. By theorem 4.7, we know that $\deg g \le \deg f \le n-k-1$. Thus, equality is possible in theorem 8.8.
If $\deg f < n-k-1$, then the subfunction g must have even Hamming-weight because g is a function in $n-k-1$ variables. Therefore, we have $w \le 2^{n-k-2} - 2$. By the same proof of theorem 8.8, it follows that $N_f \le 2^{k+1} w \le 2^{n-1} - 2^{k+2}$. □

8.2. Relationship between Nonlinearity and the Propagation Criterion

In this section we observe the relationship between nonlinearity and the propagation criterion. Before we observe the relationship, we provide a precise description of the functions satisfying the propagation criterion for the highest degrees k, namely, $k = n-2$, $n-1$ or n. These functions were characterized by Carlet [5].

Theorem 8.10. *Let $n \geq 4$ be even. The Boolean functions in n variables which satisfy $PC(n-2)$ are the bent functions, thus in fact they satisfy $PC(n)$.*

Let $n \geq 3$ be odd. The Boolean functions in n variables which satisfy $PC(n-1)$ are the functions of the form

$$f(x_1, \ldots, x_n) = g(x_1 \oplus x_n, \ldots, x_{n-1} \oplus x_n) \oplus h(x_1, \ldots, x_n), \tag{8.5}$$

where g is any bent function in $n-1$ variables and h is any affine function in n variables. The functions which satisfy $PC(n-2)$ are those of the form (8.5) and of the forms

$$g(x_1 \oplus x_n, \ldots, x_{i-1} \oplus x_n, x_i, x_{i+1} \oplus x_n, \ldots, x_{n-1} \oplus x_n) \oplus h(x_1, \ldots, x_n) \tag{8.6}$$

or

$$g(x_1 \oplus x_{n-1}, \ldots, x_{n-2} \oplus x_{n-1}, x_n) \oplus h(x_1, \ldots, x_n), \tag{8.7}$$

where g and h are as in (8.5).

Equivalently, for odd $n \geq 3$, the functions which satisfy $PC(n-2)$ are the functions satisfying the conditions: there exists a nonzero vector a with Hamming-weight $wt(a) \geq n-1$ such that

$$f(x) \oplus f(x \oplus a) \text{ is constant}; \tag{8.8}$$

and for every $b \neq 0$ or a, the function

$$f(x) \oplus f(x \oplus b) \text{ is balanced.} \tag{8.9}$$

Proof. See A. □

Let us illustrate theorem 8.10 by the following example.

Example 14. We use the same 3-variable Boolean function $f(x) = x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_1 \oplus 1$ as in example 10. The given function satisfies $PC(2)$ and we verify that theorem 8.10 confirms this. Hence,

$$\begin{aligned} f(x) &= x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_1 \oplus 1 \\ &= (x_1 \oplus x_2)(x_1 \oplus x_3) \oplus 1 \\ &= g(x_1 \oplus x_2, x_1 \oplus x_3) \oplus 1, \end{aligned}$$

where $g(y_1, y_2) = y_1y_2$ is bent. Then in accordance with (8.5) and by renumbering the variables we obtain that f satisfy $PC(2)$.

Finally, we present a relationship between nonlinearity and the propagation criterion given by Zhang and Zheng [48]. First, we provide three useful lemmas which we use to prove the main result about the aforementioned relationship.

The following lemma can be viewed as a refined version of the Walsh transform.

Lemma 8.11. *Let $(a_0, a_1, \ldots, a_{2^n-1})$ and $(b_0, b_1, \ldots, b_{2^n-1})$ be two real-valued sequences of length 2^n, satisfying*

$$(a_o, a_1, \ldots, a_{2^n-1})\, H_n = (b_0, b_1, \ldots, b_{2^n-1})\,. \tag{8.10}$$

Let k be an integer with $1 \leq k \leq n-1$. For any fixed i with $0 \leq i \leq 2^{n-k}-1$ and any fixed j with $0 \leq j \leq 2^k - 1$, let $\chi_i = (a_{i\cdot 2^k}, a_{1+i\cdot 2^k}, \ldots a_{2^k-1+i\cdot 2^k})$ and $\lambda_j = \left(b_j, b_{j+2^k}, b_{j+2\cdot 2^k}, \ldots, b_{j+(2^{n-p}-1)2^k}\right)$. Then we have

$$2^{n-k}\langle \chi_i, e_j\rangle = \langle \lambda_j, l_i\rangle, \tag{8.11}$$

with $i = 0, 1, \ldots, 2^{n-k}-1$ and $j = 0, 1, \ldots, 2^k - 1$, where l_i denotes the ith row of H_{n-k} and e_j denotes the jth row of H_k.

Proof. See [48] □

Lemma 8.12. *Let f be a non-bent function on $\mathbb{F}_2^n$, satisfying the propagation criterion of degree k. Denote the $(1,-1)$-sequence of f by ξ. If there exists a row l^* of H_n such that $|\langle \xi, l^*\rangle| = 2^{n-\frac{1}{2}k}$, then $\alpha_{2^{t+k}+2^k-1}$ is a non-zero linear structure of f, where $\alpha_{2^{t+k}+2^k-1}$ is the vector in $\mathbb{F}_2^n$ corresponding to the integer $2^{t+k}+2^k-1$, $t = 0, 1, \ldots, n-k-1$.*

Proof. See [48]. □

Lemma 8.13. *Let f be a non-bent function on $\mathbb{F}_2^n$, satisfying the propagation criterion of degree k. Denote the $(1,-1)$-sequence of f by ξ. If there exists a row l^* of H_n, such that $|\langle \xi, l^*\rangle| = 2^{n-\frac{1}{2}k}$, then $k = n-1$ and n is odd.*

Proof. See [48]. □

The following theorem presents the main result about the relationship between nonlinearity and the propagation criterion.

Theorem 8.14. *Let f be a Boolean function on $\mathbb{F}_2^n$. Further f satisfies the propagation criterion of degree k. Then*

(i) the nonlinearity N_f of f satisfies $N_f \geq 2^{n-1} - 2^{n-1-\frac{1}{2}k}$,

(ii) the equality in (i) holds if and only if one of the following two conditions holds:

a) $k = n-1$, n is odd and the function f is given by equation (8.5) in theorem 8.10.

b) $k = n$, f is bent and n is even.

Proof. Let $k > 0$ and since f is not bent $k \leq n-1$. We rewrite the equation in lemma 8.5 as follows

$$(r_f(a_0), r_f(a_1), \ldots, r_f(a_{2^n-1}))\cdot H_n = \left(\langle \xi_f, l_0\rangle^2, \langle \xi_f, l_1\rangle^2, \ldots, \langle \xi_f, l_{2^n-1}\rangle^2\right), \tag{8.12}$$

where a_i is the vector in $\mathbb{F}_2^n$ corresponding to the integer i, and l_i is the ith row of H_n, $i = 0, \ldots, 2^n - 1$. We set $i = 0$ in (8.11). Thus, we have $2^{n-k}\langle \chi_0, e_j \rangle = \langle \lambda_j, l_0 \rangle$. We obtain by applying $2^{n-k}\langle \chi_0, e_j \rangle = \langle \lambda_j, l_0 \rangle$ to (8.12)

$$\sum_{u=0}^{2^{n-k}-1} \langle \xi, l_{j+u\cdot 2^k} \rangle^2 = 2^{2n-k}. \tag{8.13}$$

Due to (8.13), we have $\langle \xi, l_{j+u\cdot 2^k} \rangle^2 \leq 2^{2n-k}$. Since u and j are arbitrary, we use theorem 7.4, so we have $N_f \geq 2^{n-1} - 2^{n-1-\frac{1}{2}k}$.
For the second part, we assume that the equality holds, that is

$$N_f = 2^{n-1} - 2^{n-1-\frac{1}{2}k}. \tag{8.14}$$

From theorem 7.4, we know that there exists a row l^* of H_n such that $|\langle \xi, l^* \rangle| = 2^{n-\frac{1}{2}k}$. We have to consider two cases. First, f is not bent and secondly f is bent. If f is not bent then lemma 8.13 gives us $k = n - 1$ and n is odd. Then using theorem 8.10, we have that f must take the form of (8.5). In the case that f is bent, we have that $k = n$ and n is even. Thus, the equality holds and f attains the upper bound of nonlinearity, cf. theorem 7.5.
Conversely, we assume that f takes the form (8.5) in a). Since g is bent on $\mathbb{F}_2^{n-1}$, we have $N_g = 2^{n-2} - 2^{\frac{n}{2}-2}$. We apply a nonsingular transformation on the variables and consider a result of Nyberg [32], so we have $N_f = 2N_g$. Thus, $N_f = 2^{n-1} - 2^{\frac{n}{2}-1} = 2^{n-1} - 2^{n-1-\frac{1}{2}k}$, where the second equality holds because $k = n-1$. Furthermore, it is obvious that (8.14) holds when $n = k$, n even and f is bent. □

9. Conclusion and Further Work

This thesis provides an overview of the use of Boolean functions in cryptography.

We characterized the most important properties of Boolean functions and show how they can be constructed. Especially, we focused on nonlinearity and its relationships to correlation immunity and the propagation criterion. We used bent functions as a starting point to design highly (balanced) nonlinear functions. Thus, we established lower bounds on nonlinearity, where the functions also fulfill the strict avalanche criterion.
Furthermore, we presented methods to construct balanced functions satisfying the propagation criterion of higher order. More precisely, we constructed balanced nonlinear functions satisfying the propagation criterion with respect to all but one or three nonzero vectors.

Finally, we established relationships between nonlinearity and correlation immunity, as well as between nonlinearity and the propagation criterion.
For the first relationship, we obtained a upper bound on nonlinearity for balanced and correlation immune functions of order k with $k \leq n-2$. Additionally, we observed the influence of the algebraic degree on the nonlinearity.
For the second relationship, we obtained a lower bound on nonlinearity over all Boolean functions satisfying the propagation criterion of degree k. We also characterized the functions having minimum nonlinearity.

Further Work

Further work on the relationship between nonlinearity and correlation immunity would be needed to examine an upper bound on nonlinearity of a kth correlation immune function on $\mathbb{F}_2^n$ for the case $k < \frac{n}{2}$.

It would be also worthwhile to study the relationship between the correlation immunity and the propagation criterion. Zhang and Zheng gave some results [48] concerning this question. They proved that in general the sum of the degree of the propagation criterion and the order of correlation immunity of Boolean functions on $\mathbb{F}_2^n$ is less than or equal to $n-2$. This leads to the result that we cannot expect a Boolean function to achieve a high degree of propagation criterion as well as a high order correlation immunity.
One should examine whether the algebraic degree has a further impact on these observations.

A. Proof of Theorem 8.10

Theorem A.1. *Let $n \geq 4$ be even. The Boolean functions in n variables which satisfy $PC(n-2)$ are the bent functions, thus in fact they satisfy $PC(n)$.*

Let $n \geq 3$ be odd. The Boolean functions in n variables which satisfy $PC(n-1)$ are the functions of the form

$$f(x_1, \ldots, x_n) = g(x_1 \oplus x_n, \ldots, x_{n-1} \oplus x_n) \oplus h(x_1, \ldots, x_n), \tag{A.1}$$

where g is any bent function in $n-1$ variables and h is any affine function in n variables. The functions which satisfy $PC(n-2)$ are those of the form (A.1) *and of the forms*

$$g(x_1 \oplus x_n, \ldots, x_{i-1} \oplus x_n, x_i, x_{i+1} \oplus x_n, \ldots, x_{n-1} \oplus x_n) \oplus h(x_1, \ldots, x_n) \tag{A.2}$$

or

$$g(x_1 \oplus x_{n-1}, \ldots, x_{n-2} \oplus x_{n-1}, x_n) \oplus h(x_1, \ldots, x_n), \tag{A.3}$$

where g and h are as in (A.1).

Equivalently, for odd $n \geq 3$, the functions which satisfy $PC(n-2)$ are the functions satisfying the conditions: there exists a nonzero vector a with Hamming-weight $wt(a) \geq n-1$ such that

$$f(x) \oplus f(x \oplus a) \text{ is constant;} \tag{A.4}$$

and for every $b \neq 0$ or a, the function

$$f(x) \oplus f(x \oplus b) \text{ is balanced.} \tag{A.5}$$

To prove this intense theorem we need the following lemmas.

Lemma A.2. *Suppose that $0 \leq k \leq n$. A Boolean function in n variables satisfies $PC(k)$ if and only if for every n-vector u with $wt(u) = k$ and for every n-vector v we have*

$$\sum_{w \leq \overline{u}} W(\widehat{f})(w \oplus v)^2 = 2^{wt(\overline{u})+n}.$$

The same equality holds for every u with $wt(u) \leq k$.

Proof. The proof is straightforward.

$$\begin{aligned}
\sum_{w\leq\overline{u}} W(\widehat{f})(w\oplus v)^2 &= \sum_{w\leq\overline{u}} \left(\sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)\oplus\langle x,(w\oplus v)\rangle} \right)^2 \\
&= \sum_{w\leq\overline{u}} \sum_{x,y\in\mathbb{F}_2^n} (-1)^{f(x)\oplus f(y)\oplus\langle (x\oplus y),(w\oplus v)\rangle} \\
&= \sum_{x,y\in\mathbb{F}_2^n} (-1)^{f(x)\oplus f(y)\oplus\langle (x\oplus y),v\rangle} \sum_{w\leq\overline{u}} (-1)^{\langle (x\oplus y),w\rangle} \\
&= 2^{wt(\overline{u})} \sum_{x,y\in\mathbb{F}_2^n,\ x\oplus y\leq u} (-1)^{f(x)\oplus f(y)\oplus\langle (x\oplus y),v\rangle} \\
&= 2^{wt(\overline{u})} \sum_{s\leq u} (-1)^{\langle s,v\rangle} \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)\oplus f(x\oplus s)} \\
&= 2^{wt(\overline{u})+n}
\end{aligned}$$

The final equality follows from the equation

$$\sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)\oplus f(x\oplus s)} = 0 \ \text{ for nonzero } s\leq u.$$

The last statement of the theorem follows immediately by the same proof. □

Lemma A.3. *We assume that for every nonnegative integer m we have $2^m = a^2+b^2+c^2+d^2$, where a,b,c,d are nonnegative integers.*
Then for m even, either one a,b,c,d is $2^{\frac{m}{2}}$ and the others are 0, or each of a,b,c,d is $2^{\frac{m}{2}-1}$. For m is odd, two of the a,b,c,d are $2^{\frac{m-1}{2}}$ and the other two are 0.

Proof. The proof follows by induction on m for $m\geq 3$ and we have to differ between the case m is odd or even. Furthermore, we use the fact that if a,b,c,d are not all even, then 8 does not divide $a^2+b^2+c^2+d^2$. □

Proof of theorem 8.10. [10] We start to prove the assertions about the functions which satisfy $PC(n-2)$. In the first case with n even, any bent function satisfies $PC(n)$ and so they satisfy $PC(n-2)$. Secondly, n is odd. By using lemmas 5.18 and 5.19 it follows that any function of the form (A.1), (A.2) and (A.3) satisfies (A.4) and (A.5) (due to the fact that g is bent), and therefore must satisfy $PC(n-2)$. Next, we show that the converse is also true in both cases. Thus, we use lemma A.2. If f satisfies $PC(n-2)$, then for every n-vector u with Hamming-weight $n-2$ and every n-vector v we have

$$W(\widehat{f})(v)^2 + W(\widehat{f})(v\oplus e_i)^2 + W(\widehat{f})(v\oplus e_j)^2 + W(\widehat{f})(v\oplus e_i\oplus e_j)^2 = 2^{n+2}, \quad \text{(A.6)}$$

where i and j are the positions in $\overline{u}$ where 1 appears and e_k is the unit vector in $\mathbb{F}_2^n$, i.e. the vector whose only nonzero entry is in position k. Thus, it follows that equation (A.6) holds for any distinct i and j.

First, we assume that n is even. Thus, lemma A.3 provides two possibilities for the summands in (A.6). We start with the first possibility. If this possibility holds then we would have $W(\widehat{f})(v) = \pm 2^{\frac{n}{2}+1}$ for some $v \in \mathbb{F}_2^n$. Furthermore, for every z of Hamming-weight 1 or 2 we have $W(\widehat{f})(v \oplus z) = 0$ by lemma 3.2. Now, let $w = e_i \oplus e_j \oplus e_k$ be any vector of Hamming-weight 3. By using lemma A.3 with v replaced by $v \oplus e_k$ we obtain that $W(\widehat{f})(v \oplus w) = \pm 2^{\frac{n}{2}+1}$. Hence, we conclude that if $n \geq 4$ and i, j, k, t are four distinct indices, then both Walsh transforms $W(\widehat{f})(v \oplus e_i \oplus e_j \oplus e_k)$ and $W(\widehat{f})(v \oplus e_i \oplus e_j \oplus e_t)$ are equal to $\pm 2^{\frac{n}{2}+1}$. This contradicts (A.6) with v replaced by $v \oplus e_i \oplus e_k$ and $\{e_i, e_j\}$ replaced by $\{e_k, e_t\}$, since then the left-hand side would be $\geq 2^{n+3}$. Hence, the second possibility in lemma A.3 must hold, that is $W(\widehat{f})(v) = \pm 2^{\frac{n}{2}}$ for every v. Therefore, it follows that f is bent.

Next we assume that n is odd and f satisfies $PC(n-2)$. By using lemma A.3, for every vector v and any distinct i and j we obtain that two of the integers $W(\widehat{f})(v)$, $W(\widehat{f})(v \oplus e_i)$, $W(\widehat{f})(v \oplus e_j)$ and $W(\widehat{f})(v \oplus e_i \oplus e_j)$ are equal to $\pm 2^{\frac{n+1}{2}}$ and the other two are 0.
First, we assume that for some i, $1 \leq i \leq n$, and for some v in $\mathbb{F}_2^n$ we have $W(\widehat{f})(v)$ and $W(\widehat{f})(v \oplus e_i)$ are equal to $\pm 2^{\frac{n+1}{2}}$. Since we can replace $f(x)$ by $f(x) \oplus \langle v, x \rangle$, we may assume without loss of generality that $v = 0$. Moreover, we can deduce by induction on $wt(w)$ that for every vector $w = (w_1, \ldots, w_n)$ with $w_i = 0$ the numbers $W(\widehat{f})(w)$ and $W(\widehat{f})(w \oplus e_i)$ are equal to $2^{\frac{n+1}{2}}$ if $wt(w)$ is even, and are equal to 0 otherwise.

We suppose that $i < n$ and define

$$E_i = \left\{ w : \bigoplus_{j \neq i} w_j = 0 \right\}.$$

By our assumptions it follows that for all $w \notin E_i$ we have $W(\widehat{f})(w) = 0$ and for all $w \in E_i$ we have $W(\widehat{f})(w) = \pm 2^{\frac{n+1}{2}}$. Thus, by the inverse Walsh transform (3.2) we obtain for all $u \in \mathbb{F}_2^n$

$$\widehat{f}(u) = 2^{-n} \sum_{w \in E_i} W(\widehat{f})(w)(-1)^{\langle w,u \rangle}. \tag{A.7}$$

We can express every element of E_i as $(w', h_i(w'))$, where $w' = (w'_1, \ldots, w'_n) \in \mathbb{F}_2^{n-1}$ and $h_i(w') = \sum_{j \neq i} w'_j$. Then it follows from (A.7) that

$$\widehat{f}(u) = 2^{-n} \sum_{w' \in \mathbb{F}_2^{n-1}} W(\widehat{f})(w', h_i(w'))(-1)^{\langle w', u' \rangle \oplus u_n h_i(w')}, \tag{A.8}$$

where $u' = (u_1, \ldots, u_{n-1})$. We denote the vector in $\mathbb{F}_2^{n-1}$ in which the only nonzero entry is in position i with e'_i. Thus, we have

$$\langle w', u' \rangle \oplus u_n h_i(w') = \langle w, (u' \oplus u_n \overline{e'_i}) \rangle.$$

It follows that the right-hand side of the equation (A.8) is $g(u' \oplus u_n \overline{e'_i})$ for some function g in n variables.
To complete the proof in the case $i < n$ we need to show that g is bent, that is, f has the form (A.2). Let us suppose that f is not bent. Then we have by lemma 5.18 that there exists a nonzero $b \in \mathbb{F}_2^{n-1}$ such that $g(u') \oplus g(u' \oplus b)$ is not balanced. Thus, we have that the functions $f(u) \oplus f(u \oplus (b, 0))$ and $f(u) \oplus f(u \oplus (b \oplus e'_i, 1))$ are also not bent. This follows by the fact that each function $f(u) = g(u' \oplus u_n \overline{e'_i})$, for all $u \in \mathbb{F}_2^n$, is unbalanced in u' with the same unequal count of zeros and ones if we fix $u_n = 0$ or $u_n = 1$. Since the function f satisfies $PC(n-2)$, the vectors $(b, 0)$ and $(b \oplus \overline{e'_i}, 1)$ must both have Hamming-weight $\geq n-1$ (by lemma 5.18). This is a contradiction if $n \geq 5$ and if $n \geq 3$ we have that g is a quadratic non affine function in four variables and such functions are bent. The proof for the case $i = n$ follows by exchanging n and $n-1$ in (A.2) with $i = n-1$. This gives us the functions of the form (A.3).

To complete the proof, for any function f satisfying $PC(n-2)$ the function must have one of the forms (A.1), (A.2) and (A.3). The only remaining case is the case in which no i and v exist such that $W(\widehat{f})(v)$ and $W(\widehat{f})(v \oplus e_i)$ are equal to $\pm 2^{\frac{n+1}{2}}$. We choose the vector v such that $W(\widehat{f})(v) = 2^{\frac{n+1}{2}}$. Without loss of generality, we can take $v = 0$ and hence it follows by our assumptions that $W(\widehat{f})(e_i) = 0$ for every i. Once again, we can deduce by induction on $wt(w)$ that for every w we have $W(\widehat{f})(w) = \pm 2^{\frac{n+1}{2}}$ is $wt(w)$ is even and $W(\widehat{f})(w) = 0$ if $wt(w)$ is odd. Now we define $E = \{w | wt(w) \text{ is even}\}$. With $u' = (u_1, \ldots, u_{n-1}) \in \mathbb{F}_2^{n-1}$ and for every $u \in \mathbb{F}_2^n$ we can replace E_i by E in (A.7) and we get

$$\widehat{f}(u) = 2^{-n} \sum_{w' \in \mathbb{F}_2^{n-1}} W(\widehat{f})(w', h(w'))(-1)^{\langle w', u' \rangle \oplus u_n h(w')},$$

where $h(w') = \sum_{i=1}^{n-1} w'_i$. Therefore, we have

$$\widehat{f}(u) = 2^{-n} \sum_{w' \in \mathbb{F}_2^{n-1}} W(\widehat{f})(w', h_i(w'))(-1)^{\langle w', (u' \oplus u_n(1, \ldots, 1)) \rangle},$$

and this implies that $f(u) = g(u' \oplus u_n(1, \ldots, 1)$, where $g(u') = f(u', 0)$ must be bent by the fact that it is a function in an even number $n-1$ variables and satisfies $PC(n-2)$. Hence, we have a function f of the form (A.1).

The last statement that for n odd the only functions which satisfy $PC(n-1)$ are those of the form (A.1) was proved by Preneel et al. [35, Theorem 2]. □

B. Vectorial Boolean functions

In this chapter we observe multi-output Boolean functions. This section is mainly based on Carlet [3].
Multi-output Boolean functions are functions from the vector space $\mathbb{F}_2^n$ to the vector space $\mathbb{F}_2^m$, for some positive integers n and m. Obviously, the functions include the (single-output) Boolean functions which is the case $m = 1$.
Our aim is to give an introduction to multi-output Boolean functions and show similarities to results given in the previous chapters for Boolean functions. Due to the similarity we abdicate the proofs.

Definition B.1. *Let n and m be positive integers. The function $F\colon \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^m$ given by $F(x) = (f_1(x), \ldots, f_m(x))$, at every $x \in \mathbb{F}_2^n$, is called a n-*input *m-*output Boolean function *((n,m)-function for short) and f_i is called the coordinate function for $i = 1, \ldots, m$. When the numbers n and m are not specified, (n,m)-functions are called multi-output Boolean functions, vectorial Boolean functions or S-Boxes.

Remark. The last term is often used in cryptography. This term is assigned to vectorial Boolean functions whose role is to provide confusion into the cryptosystem.

Definition B.2. *The component function is the nonzero linear combination of the coordinate functions of F.*

We can easily extend the notion of the algebraic normal form of Boolean functions to (n,m)-functions. Obviously, each coordinate function of a functions F is uniquely represented as a polynomial on n variables with coefficients in $\mathbb{F}_2$. We can express the function F as a polynomial of the same form with coefficients in $\mathbb{F}_2^m$. Thus F can be expressed as a unique polynomial in $\mathbb{F}_2^m [x_1, \ldots, x_n] / (x_1^2 \oplus x, \ldots, x_n^2 \oplus x)$ as

$$F(x) = \sum_{I \in \mathfrak{P}(N)} a_I x^I, \tag{B.1}$$

where $\mathfrak{P}(N)$ denotes the power set of $N = \{1, \ldots, n\}$ and a_I belongs to $\mathbb{F}_2^m$. So by keeping the ith coordinate of each coefficient in the expression (B.1) we obtain the ANF of the ith coordinate function of F.

The condition of balancedness for multi-output functions is as important as for Boolean functions. Unbalanced multi-output functions have an irregular probability distribution on the ciphertext which give space for statistical attacks.

Definition B.3. *The vectorial Boolean function F is said to be a balanced (n,m)-function if $\#\{x|F(x) = a\} = 2^{n-m}$ for any $a \in \mathbb{F}_2^m$ and $x \in \mathbb{F}_2^n$.*

Lidl and Niederreiter [18] characterized balanced multi-output Boolean functions by the balancedness of their coordinate functions.

Proposition B.4. *An (n, m)-function is balanced if and only if all nonzero linear combinations of $f_1, \ldots, f_m$ are balanced.*

In the next step we want to introduce the useful Walsh transform for multi-output Boolean functions.

Definition B.5. *The Walsh transform of an (n, m)-function F is a map $W : \mathbb{F}_2^n \times \mathbb{F}_2^m \longrightarrow \mathbb{R}$ defined by*

$$W(F)(u, v) = \sum_{x \in \mathbb{F}_2^n} (-1)^{\langle v, F(x) \rangle \oplus \langle u, x \rangle},$$

where $u \in \mathbb{F}_2^n$ and $v \in \mathbb{F}_2^m \setminus \{0\}$.

Now we turn our attention to the cryptographic properties, in particular to nonlinearity. Nyberg [31] introduced the notion of nonlinearity for multi-output functions.

Definition B.6. *The nonlinearity N_F of an (n, m)-function F is the minimum nonlinearity of all the component functions $x \in \mathbb{F}_2^n \mapsto \langle v, F(x) \rangle$, where $v \in \mathbb{F}_2^m \setminus \{0\}$.*

In other words, the nonlinearity N_F is equal to the minimum Hamming-distance between all the component functions of F and all affine functions on $\mathbb{F}_2^n$. According to the theorem 3.18, we also can express the nonlinearity in term to the maximal magnitude of its Walsh transform of F. We have

$$N_F = 2^{n-1} - \frac{1}{2} \max_{u \in \mathbb{F}_2^n,\, v \in \mathbb{F}_2^m \setminus \{0\}} \left| \sum_{x \in \mathbb{F}_2^n} (-1)^{\langle v, F(x) \rangle \oplus \langle u, x \rangle} \right|$$

The upper bound of nonlinearity given in theorem 7.2 is also valid for every (n, m)-function. Thus

$$N_F \leq 2^{n-1} - 2^{\frac{n}{2}-1}. \tag{B.2}$$

In addition to (B.2) we can characterize (n, m)-bent functions.

Definition B.7. *An (n, m)-function is called bent if it achieves* (B.2) *with equality.*

We note that an equivalent definition is given by an (n, m)-function is bent if and only if all the component functions are bent. The algebraic degree of any (n, m)-bent function is at most $\frac{n}{2}$.
We recall from (vi) of theorem 6.20 that any Boolean function f on $\mathbb{F}_2^n$ is bent if and only if its directional derivative $f_v(x) = f(x) \oplus f(x \oplus v)$ is balanced for all nonzero v in $\mathbb{F}_2^n$. Thus, we can give a similar description for (n, m)-functions.

Proposition B.8. *An (n, m)-function is bent if and only if all of its derivatives $F_v(x) = F(x) \oplus F(x \oplus v)$ is balanced for all nonzero v in $\mathbb{F}_2^n$.*

As we have seen bent functions only exist for n is even. An (n, m)-bent function exist only under the same condition, but Nyberg [30] showed that this condition is not sufficient for the existence of (n, m)-bent functions. Therefore she introduced the following result.

Proposition B.9. *An (n, m)-bent function exist only if n is even and $m \leq \frac{n}{2}$.*

The next result is given by Chabaud and Vaudenay [7]. They show that under certain conditions, there is a better upper bound than (B.2).

Theorem B.10. *Let n and m be any positive integer such that $m \geq n - 1$. Let F be any (n, m)-function. Then*

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

Bibliography

[1] P. Camion, C. Carlet, P. Charpin, and N. Sendrier. On correlation-immune functions. In *Advances in cryptology—CRYPTO '91 (Santa Barbara, CA, 1991)*, volume 576 of *Lecture Notes in Comput. Sci.*, pages 86–100. Springer, Berlin, 1992.

[2] C. Carlet. Boolean functions for cryptography and error correcting codes.

[3] C. Carlet. Vectorial boolean functions for cryptography.

[4] C. Carlet. Partially-bent functions. *Des. Codes Cryptography*, 3(2):135–145, 1993.

[5] C. Carlet. On the propagation criterion of degree l and order k. In *EUROCRYPT*, pages 462–474, 1998.

[6] C. Carlet. A larger class of cryptographic Boolean functions via a study of the Maiorana-McFarland construction. In *Advances in cryptology—CRYPTO 2002*, volume 2442 of *Lecture Notes in Comput. Sci.*, pages 549–564. Springer, Berlin, 2002.

[7] F. Chabaud and S. Vaudenay. Links between differential and linear cryptoanalysis. In *EUROCRYPT*, pages 356–365, 1994.

[8] S. Chee, S. Lee, D. Lee, and S. H. Sung. On the correlation immune functions and their nonlinearity. In *ASIACRYPT'96*, pages 232–243, 1996.

[9] B. Chor, O. Goldreich, J. Hastad, J. Freidmann, S. Rudich, and R. Smolensky. The bit extraction problem or t-resilient functions. 1985.

[10] T. W. Cusick and P. Stănică. *Cryptographic Boolean functions and applications*. Elsevier/Academic Press, Amsterdam, 2009.

[11] J. F. Dillon. A survey of bent functions. 1972.

[12] J. F. Dillon. Elementary Hadamard difference sets, PhD thesis. 1974.

[13] P. Duvall and J. Mortick. Some symptoms of boolean functions. 1970.

[14] R. Forré. The strict avalanche criterion: Spectral properties of boolean functions and an extended definition. In *Advances in Cryptology (CRYPTO '88)*, pages 450–468, Berlin - Heidelberg - New York, Aug. 1990. Springer.

[15] K. Gopalakrishnan and D. R. Stinson. A short proof of the non-existence of certain cryptographic functions. *J. Combin. Math. Combin. Comput.*, 20:129–137, 1996.

[16] M. H. Jr. *Combinatorial Theory*. Ginn-Blaisdell, Waltham, 1967.

[17] R. Lechner. *Harmonic analysis of switching functions. In: Recent developments in switching theory. Edited by Amar Mukhopadhyay.* Academic Press, New York,, 1971.

[18] R. Lidl and H. Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1997. With a foreword by P. M. Cohn.

[19] S. Lloyd. Counting functions satisfying a higher order strict avalanche criterion. In *Advances in cryptology—EUROCRYPT '89 (Houthalen, 1989)*, volume 434 of *Lecture Notes in Comput. Sci.*, pages 63–74. Springer, Berlin, 1990.

[20] S. Lloyd. Balance, uncorrelatedness and the strict avalanche criterion. *Discrete Applied Mathematics*, 41(3):223 – 233, 1993.

[21] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes. II.* North-Holland Publishing Co., Amsterdam, 1977. North-Holland Mathematical Library, Vol. 16.

[22] J. Maiorana. A class of bent functions. 1970.

[23] H. B. Mann. Difference sets in elemantary abelian groups. *Illinois J. Math.*, 9:212–219, 1965.

[24] M. Matsui. Linear cryptoanalysis method for DES cipher. In *EUROCRYPT*, pages 386–397, 1993.

[25] R. L. McFarland. A discrete fourier theory for binary functions. *R41 Technical paper*, 1971.

[26] W. Meier and O. Staffelbach. Nonlinearity criteria for cryptographic functions. In *EUROCRYPT*, pages 549–562, 1989.

[27] Q. Meng, H. Zhang, M. Yang, and J. Cui. On the degree of homogeneous bent functions. *Discrete Applied Mathematics*, 155(5):665–669, 2007.

[28] P. K. Menon. On difference sets whose parameters satisfy a certain relation. In *Proceedings of the A.M.S. 13*, pages 739–745, 1962.

[29] C. J. Mitchell. Enumerating boolean functions of cryptographic significance. *J. Cryptology*, 2(3):155–170, 1990.

[30] K. Nyberg. Perfect nonlinear s-boxes. In *EUROCRYPT*, pages 378–386, 1991.

[31] K. Nyberg. Differentially uniform mappings for cryptography. In *EUROCRYPT*, pages 55–64, 1993.

[32] K. Nyberg. On the construction of highly nonlinear permutations. In *Proceedings of the 11th annual international conference on Theory and application of cryptographic techniques*, EUROCRYPT'92, pages 92–98, Berlin, Heidelberg, 1993. Springer-Verlag.

[33] J. Pieprzyk and G. Finkelstein. Towards effective nonlinear cryptosystem design. *IEE Proceedings Part E*, 35(6):325–335, 1988.

[34] Preneel, V. Leekwijk, V. Linden, Govaerts, and Vandewalle. Propagation characteristics of boolean functions. In *EUROCRYPT: Advances in Cryptology: Proceedings of EUROCRYPT*, 1990.

[35] B. Preneel, R. Govaerts, and J. Vandewalle. Boolean functions satisfying higher order propagation criteria. In *Proceedings of the 10th annual international conference on Theory and application of cryptographic techniques*, EUROCRYPT'91, pages 141–152, Berlin, Heidelberg, 1991. Springer-Verlag.

[36] O. S. Rothaus. On "bent" functions. *J. Comb. Theory, Ser. A*, 20(3):300–305, 1976.

[37] P. Sarkar. A note on the spectral characterization of correlation immune boolean functions. *Inf. Process. Lett.*, 74(5-6):191–195, 2000.

[38] J. Seberry, X. M. Zhang, and Y. Zheng. Nonlinearity and propagation characteristics of balanced Boolean functions. *Inform. and Comput.*, 119(1):1–13, 1995.

[39] C. E. Shannon. Communication theory of secrecy systems. *Bell System Tech. J.*, 28:656–715, 1949.

[40] T. Siegenthaler. Correlation-immunity of nonlinear combining functions for cryptographic applications. *IEEE Trans. Inform. Theory*, 30(5):776–780, 1984.

[41] G. J. Simmons, editor. *Contemporary cryptology.* IEEE Press, New York, 1992. The science of information integrity.

[42] Y. Tarannikov. On resilient boolean functions with maximal possible nonlinearity. In *Proceedings of INDOCRYPT 2000, Lecture Notes in Computer Science.* Springer-Verlag, 2000.

[43] W. D. Wallis, A. P. Street, and J. S. Wallis. *Combinatorics: Room squares, sum-free sets, Hadamard matrices.* Lecture Notes in Mathematics, Vol. 292. Springer-Verlag, Berlin, 1972.

[44] A. F. Webster and S. E. Tavares. On the design of S-boxes. In H. C. Williams, editor, *Advances in Cryptology — Crypto '85*, pages 523–534, New York, 1986. Springer-Verlag.

[45] T. Xia, J. Seberry, J. Pieprzyk, and C. Charnes. Homogeneous bent functions of degree n in 2n variables do not exist for n ¿ 3. *Discrete Applied Mathematics*, 142(1-3):127 – 132, 2004. ¡ce:title¿Boolean and Pseudo-Boolean Functions¡/ce:title¿.

[46] G. Z. Xiao and J. L. Massey. A spectral characterization of correlation-immune combining functions. *IEEE Trans. Inform. Theory*, 34(3):569–571, 1988.

[47] Y. Zheng and X.-M. Zhang. Improved upper bound on the nonlinearity of high order correlation immune functions. In *Selected Areas in Cryptography*, pages 262–274, 2000.

[48] Y. Zheng and X.-M. Zhang. On relationship among avalanche, nonlinearity, and correlation immunity. In *LNCS 1976, ASIACRYPT'2000*, pages 470–483. Springer-Verlag, 2000.

[49] Y. Zheng and X.-M. Zhang. On plateaued functions. *IEEE Transactions on Information Theory*, 47(3):1215–1223, 2001.