UNIVERZA NA PRIMORSKEM
FAKULTETA ZA MATEMATIKO, NARAVOSLOVJE IN
INFORMACIJSKE TEHNOLOGIJE

Magistrsko delo
(Master thesis)

Maksimalno nelinearne Boolove funkcije

(Bent functions)

Ime in priimek: Nastja Cepak
Študijski program: Matematične znanosti 2. stopnja
Mentor: izr. prof. dr. Enes Pasalic

Koper, avgust 2014

Ključna dokumentacijska informacija

Ime in PRIIMEK: Nastja CEPAK

Naslov magistrskega dela: Maksimalno nelinearne Boolove funkcije

Kraj: Koper

Leto: 2014

Število listov: 48 Število slik: 6

Število referenc: 28
UDK:

Mentor: izr. prof. dr. Enes Pasalic

Ključne besede: kriptografija, boolove funkcije, nelinearnost

Math. Subj. Class. (2010): 94A60, 11T71, 05C62

Izvleček:

Predstavljenih je nekaj pomembnejših lastnosti Boolovih funkcij, ki so pomembne za uporabo v kriptografskih algoritmih.
Izmed naštetih lastnosti se osredotočimo na nelinearnost in uvedemo definicijo maksimalno nelinearne Boolove funkcije, kot jo je leta 1976 definiral Rothaus. Predstavimo in dokažemo nekaj ekvivalentnih definicij in najbolj uporabnih lastnosti.
Uvedemo koncepta diferenčnih množic in krepko regularnih grafov ter dokažemo nekaj njihovih lastnosti, ki jih bomo potrebovali v nadaljevanju. Nato prikažemo postopka, s katerima lahko maksimalno nelinearne Boolove funkcije pretvorimo v Hadamarjevo diferenčno množico in v krepko regularen graf. Navedemo zahtevane parametre obojih. Prikažemo dva izmed najbolj znanih postopkov konstruiranja maksimalno nelinearnih Boolovih funkcij – Maiorana-McFarland postopek in Dillonov postopek. Za konec prestavimo tudi skupino posplošenih Rothausovih funkcij, za katere sva z mentorjem Enesom Pasalicem dokazala, da so maksimalno nelinearne, in pokažemo njihovo povezavo z razredom funkcij, ki jih je predstavil Carlet.

Key words documentation

Name and SURNAME: Nastja CEPAK

Title of master thesis: Bent functions

Place: Koper

Year: 2014

Number of pages: 48 Number of figures: 6
Number of references: 28
UDK:

Mentor: Assoc. Prof. Enes Pasalic, PhD

Keywords: cryptography, boolean functions, bent functions, linearity

Math. Subj. Class. (2010): 94A60, 11T71, 05C62

Abstract:

We introduce some of the more important properties of Boolean functions, used in cryptographic algorithms.
Among these properties we focus on nonlinearity and introduce the definition of bent functions, as it was defined in 1976 by Rothaus. We introduce and prove some equivalent definitions of bent functions and their most useful properties.
We define difference sets and strongly regular graphs and prove some of their properties, which will be useful in the following proofs. We show step by step how we can turn a bent function into a Hadamard difference set and how to turn it into a strongly regular graph. In both cases we give exact required parameters.
We show two of the most well-known construction techniques for bent function - the Maiorana-McFarland construction and Dillon's construction, which gives rise to the Partial Spread class. Towards the end we introduce a generalization of Rothaus functions, for which we have together with my mentor Enes Pasalic proved that they are bent. We also show their connection to a class of bent functions introduced by Carlet.

Zahvala

Zahvaljujem se mentorju dr. Enesu Pasalicu za vso pomoč pri iskanju gradiva in pisanju magistrske naloge ter dr. Klavdiji Kutnar za vse sprotne nasvete in pomoč skozi celoten študij.

Vsem relevantnim osebam obljubljam razlago spodnje šifre in predajo dešifrirnega ključa, vsaki skupini svojega!

WOVN NRMT KDDH JIZN CRQP XOLQ OSUS BAOV TOFH TELN RVMY KKQE VATX YTMX YVWB
ZRGX YTHY TUNY TAZV TALG OZUZ FAYI SMQA SIZF ONMX YNOH CUBR BRMM EMQZ YKQE
WIVR FCMF SHFB XAVO YLVC YMQZ LNAX ORHF OOEG KLAM OVQF DEUA UEDI KSUZ KMHF
ORMQK

MTSY JJIA EIHF OXYS SWIR TEEV IOWU GPCU OIXV TYVL OWIN TLFF OPVG ULRJ ANWL
UYRF DWIU GVRK SZHV TVVL UMRL UYYS VZJB KYLM TIAK QZWS DLNB IWGU BLGE SLJS
VRQZ SXWT CIEC IJZA GPPU RKAN PIGU JZYH OXUK KFGD AMTN XRNE IKRX WRKS ZQOR
I

RADV RTAI PNAX AEPA WLRO THLF FTQZ IMNC ZVBK NOOR XKFV ERRX ASMX ILUU EGQE
FVPE CZFC QABB UMMG MFFT UPVB MVAQ IMFK AQIG FJNB BHEA TIIE FZMC ZXYE WYIE
JTMR VOJL UXBH UEXB JCJM UAAD ZPQA HTHE FRSI TSFH LBOS WROT TBPB JCFV QAMF
AAEZ IFWA PN

Contents

List of Figures

1 Introduction

Cryptography is a field of practice and study as ancient as the need for secrecy. Secret codes have been utilized by civilizations as old as those of ancient Egypt or Mesopotamia. Through the ages the codes have of course changed dramatically, while their complexity, importance in the every-day life and consequently the resources dedicated to breaking them have increased staggeringly. When once they were primarily used for exchanging relatively few information mainly linked to war and trade, today we are exchanging and storing enormous quantities of information every day. We use the Internet, wireless communications, sending out information to travel through channels and be forwarded through servers we have no control over. And despite that we want it to remain private. Secret. Accessible only to us. And for that we need cryptography.

Its main goal is to make it possible for two parties to safely communicate using an unprotected channel. When considering cryptographic systems, we usually talk about Alice as the sender of the message and Bob as the receiver. The actual message they want to exchange is called "plaintext" and its ciphered version "ciphertext". When encrypting the message Alice takes as input the plaintext and the encryption key K_E and gets as output the ciphertext. To decrypt the message Bob runs the decryption process with ciphertext and decryption key K_D as input and gets the original plaintext.

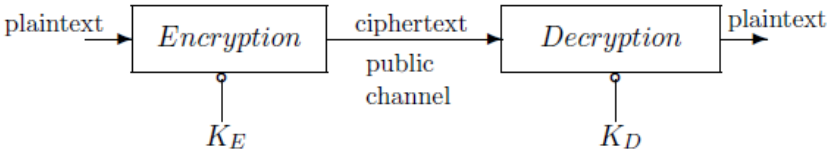

Figure 1: Cryptographic system as usually depicted. [8]

When simulating attacks on a cryptographic system it is assumed that the attacker or enemy, usually referred to as Eve, knows both encryption and decryption algorithms. That is, the security of a cryptographic system should not rely on the secrecy of the algorithms and methods but on the secrecy of the keys. As told in [24], these principles were stated already in 1883 in [5] and even before that in [18].

If both keys K_E and K_D are the same, we talk about symmetric cryptography. Some of the most famous examples of symmetric cryptography are the block ciphers DES

(Data Encryption Standard) and Rijndael, which is the current algorithm used in the AES (Advanced Encryption Standard). If, on the other hand, the encryption key K_E is public so that anyone can send Bob a ciphered message that only Bob can decipher with his private decryption key, we talk about public cryptography. Some main differences between them are that symmetric cryptography can generally be faster implemented be it in hardware or software, and that in order to ensure the same level of security symmetric cryptography requires shorter key size. Public cryptography, on the other hand, can be used not only for safe communication but also for authentication with digital signatures. Also, the key management is easier and the public and private key pair does not need to be changed as often.

All of these schemes utilise algorithms in which Boolean functions play an important role. Various cryptographic transformations, such as the S-boxes in the block ciphers or pseudo-random generators in stream ciphers, are composed out of Boolean functions with a low number of variables [8]. Yet even with limitations on the number of variables, the number of Boolean functions is extremely high. The number of Boolean functions on 7 variables is approximately 10^{38} and not all of them can be used in the construction of cryptographic algorithms. There are certain criteria a function must satisfy. Different types of algorithms require different criteria. One special class of Boolean functions, so-called bent functions, are characterized by the property of being furthest away from the set of affine functions. This class of Boolean functions is the main topic of this thesis.

2 Cryptographic criteria for Boolean functions

As we have already stated in the introduction, Boolean functions play a very important role in modern day cryptography, yet not all of them are fit to be used. Thus we will begin by taking a look at some of the most cryptographically desirable properties for a Boolean function to have, as have been listed in [14] and [8]. If not stated differently, the definitions are also derived from the same source.

First, let us formally define Boolean functions and show some basic ways of working with them. We must mention that we will denote addition over $\mathbb{Z}$, $\mathbb{R}$ and $\mathbb{C}$ with $+$, and addition over vector space $V_n = \mathbb{F}_2^n$, $n \in \mathbb{Z}$, with $\oplus$.

Definition 2.0.1. *[12] A Boolean function f on n variables is a mapping from the space V_n into $\mathbb{F}_2$.*

Definition 2.0.2. *Let f be a Boolean function mapping from V_n. Then its truth table is the $(0,1)$ sequence $(f((0,\ldots,0)), f((0,\ldots,0,1)), \cdots, f((1,\ldots,1)))$.*

Definition 2.0.3. *Let f be a Boolean function mapping from V_n. Then the following $(1,-1)$ sequence is the sequence of function f:*

$$((-1)^{f((0,\ldots,0))}, (-1)^{f((0,\ldots,0,1))}, \cdots, (-1)^{f((1,\ldots,1))})$$

.

Definition 2.0.4. *Let f be a Boolean function mapping from V_n. Then we call the $(1,-1)$-matrix M of order 2^n defined by $M_{(i,j)} = (-1)^{f(v_i \oplus v_j)}$ for each $v_i, v_j \in V_n$, the matrix of f.*

Definition 2.0.5. *A function f mapping from the vector space V_n is called an affine function if it is of the form $f(x) = c \oplus a_1x_1 \oplus \cdots \oplus a_nx_n$, where $a_1, \cdots, a_n, c \in V_n$. If $c = 0$, the function is called linear.*

Definition 2.0.6. *The support of the function f is defined as $supp(f) = \{x | f(x) \neq 0\}$.*

Another two definitions vital for operating with vectors are those for Hamming weight and Hamming distance, which are used to determine how "far" certain vectors or functions are from one another.

Definition 2.0.7. *Hamming weight w_H of a vector $u \in V_n$ is the number of positions with value 1. That is $w_H(u) =\mid \{i \mid u_i = 1\} \mid$.*

Definition 2.0.8. *Hamming distance d_H between two vectors $u, v \in V_n$ is the number of positions in which their values differ. That is $d_H(u,v) =\mid \{i \mid u_i \neq v_i\} \mid$. Hamming distance between two function f, g mapping from V_n is the value $d_H(f,g) = w_H(f(x) \oplus g(x))$, where $x \in V_n$.*

Example 2.0.9. *Let $f(x) = x_1 \oplus x_2$ be a Boolean linear function and $g(x) = x_1 x_2$, both mapping from V_2. Then the truth table of the function f is*

$$(0,1,1,0),$$

since

x_1	x_2	$f(x)$
0	0	0
0	1	1
1	0	1
1	1	0

Its sequence is $(1,-1,-1,1)$.
Its support set is $supp(f) = \{(0,1),(1,0)\}$.
Its $(1,-1)$-matrix is

$$\begin{bmatrix} 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \\ -1 & 1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}.$$

Also

$$d_H(f,g) = w_H(f(x) \oplus g(x)) = w_H((f(x_1) \oplus g(x_1), f(x_2) \oplus g(x_2), f(x_3) \oplus g(x_3))) =$$

$$= w_H((0 \oplus 0, 1 \oplus 0, 1 \oplus 0, 0 \oplus 1)) = 3.$$

We have now defined the basic concepts related to Boolean functions and can take a look at some important properties that are relevant for their use in cryptography. Those are:

- balancedness,
- strict avalanche criterion and propagation criterion,
- algebraic degree,

- correlation immunity and
- nonlinearity.

Among them the one we will be most interested in is nonlinearity. It will be left for last and it will be explored further in the next chapter.

It should also be mentioned that apart from the above listed criteria there are other important notions, especially the algebraic immunity and the resistance to fast algebraic cryptanalysis. The reader can find more information about those in [19, 28].

2.1 Balancedness

As the name already implies, balanced functions are characterized by the property that their output values are evenly distributed. The main goal of cryptography is often to disguise connections between the input and output and disperse the output values as much as possible so the balanced property is usually mandatory.

Definition 2.1.1. *A function f mapping from V_n to V_2 is called balanced if its truth table has 2^{n-1} zeros and 2^{n-1} ones.*

Example 2.1.2. *Let $f = x_1x_2 \oplus x_3$ be a function mapping from V_3. Then its truth table looks like this:*

$$(0, 1, 0, 1, 0, 1, 1, 0).$$

We see that exactly half the values are 1 *and half* 0*. The function f is therefore balanced.*

A standard way of modifying the function's output values while keeping the property of balancedness is to apply a nonsingular affine transformation as shown below.

Lemma 2.1.3. *Let $g(x) = f(xB \oplus b)$ be a function, where B is a nonsingular matrix of order n and b is an arbitrary vector from V_n. Then the function g is balanced if and only if the function f is balanced.*

Proof. We know that the vector x runs through all the vectors in the vector field V_n. Since the matrix B is nonsingular, the product xB must run through all the vectors as well. And as b is an arbitrary vector, the same must therefore go for $xB \oplus b$. This means that the output of functions g and f will be the same, just permuted. The number of zeros and ones remains the same. Thus the result follows. ■

Example 2.1.4. *Let f be the function from the previous example, let* $B = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$ *and $b = (1, 1, 1)$. Let now $g(x) = f(xB \oplus b)$.*

We make some quick computations and see that

$$g(x_1, x_2, x_3) = f(x_1 \oplus x_2 \oplus 1, x_1 \oplus x_3 \oplus 1, x_2 \oplus 1).$$

$$\begin{aligned} g(0,0,0) &= f(1,1,1) \\ g(0,0,1) &= f(1,0,1) \\ g(0,1,0) &= f(0,1,0) \\ g(0,1,1) &= f(0,0,0) \\ g(1,0,0) &= f(0,0,1) \\ g(1,0,1) &= f(0,1,1) \\ g(1,1,0) &= f(1,0,0) \\ g(1,1,1) &= f(1,1,0) \end{aligned}$$

The truth table of function g must therefore be just a permuted version of the truth table of function f, which means that g is balanced as well.

The following two results are well-known but we provide the proofs for self-completeness.

Lemma 2.1.5. *Let f be a Boolean function mapping from V_n and g be a function mapping from V_m. Then $f(x) \oplus g(y)$, where y is fixed, is balanced if f is balanced.*

PROOF. We know that $g(y)$ is a 0 or 1 constant. When we add that constant to the truth table of the function f either non of the values change ($g(y) = 0$) or all of the values change ($g(y) = 1$). Therefore, the function remains balanced. ■

This lemma can also be extended.

Lemma 2.1.6. *Let f be Boolean function mapping from V_n that is independent of x_i, $i \in \{1, \ldots, n\}$. That is, let the variable x_i never appear in the function's algebraic normal form (as defined in 2.3.1). Then the function $g(x) = f(x) \oplus x_i$ is balanced.*

PROOF. The function $f(x)$ will run through all possible values once the standalone variable x_i equals 0 and once it equals 1. This means that in truth table of the function $g(x) = f(x) \oplus x_i$ exactly half of the values must be 1 and the other half 0. ■

2.2 Strict avalanche criterion and propagation criterion

Let us first introduce the definition of propagation and strict avalanche criterion or SAC for short, as it is defined in [7].

Definition 2.2.1. *Let f be a Boolean function mapping from V_n. We say that f satisfies*

- *the propagation criterion with respect to α if $f(x) \oplus f(x \oplus \alpha)$, where α is a non-zero vector from V_n, is a balanced function;*
- *the propagation criterion of degree k if it satisfies the propagation criteria with respect to all $\alpha \in V_n$, where $1 \leq w_H(\alpha) \leq k$;*
- *strict avalanche criterion (SAC) if the propagation criterion degree of f is 1.*

Example 2.2.2. *We will make a quick example for the first, most straightforward criterion.*

- *Let $f = x_1x_2 \oplus x_3$ be a function mapping from V_3 and let $\alpha = (1, 1, 0)$. Then,*

$$\begin{aligned} f(x) \oplus f(x \oplus \alpha) &= (x_1x_2 \oplus x_3) \oplus ((x_1 \oplus 1)(x_2 \oplus 1) \oplus x_3) \\ &= x_1 \oplus x_2 \oplus 1 \end{aligned}$$

  and we can quickly see that it is balanced. Therefore, f satisfies the propagation criteria with respect to $\alpha = (1, 1, 0)$.

- *Let $f(x_1, x_2, x_3, x_4, x_5) = x_1 \oplus x_1x_5 \oplus x_2x_4 \oplus x_2x_5 \oplus x_2x_4x_5 \oplus x_3x_4x_5$ and let $\alpha = (0, 0, 1, 0, 0,)$. Then,*

$$\begin{aligned} f(x) \oplus f(x \oplus \alpha) &= x_3x_4x_5 \oplus (x_3 \oplus 1)x_4x_5 \\ &= x_4x_5, \end{aligned}$$

  which is obviously not balanced and it therefore does not satisfy the propagation criterion with respect to this α. In fact, this function does not satisfy the said criterion for none of the following vectors:

$$(0, 0, 0, 0, 0), (0, 0, 0, 0, 1), (0, 0, 0, 1, 0), (0, 0, 1, 0, 0), (0, 0, 1, 1, 1).$$

The strict avalanche criterion can be paraphrased into a much more intuitive form. The definition is in fact equivalent to saying that, given a Boolean function f, if you change one of the input bits from 0 to 1 or the other way around, exactly half of the output bits will change their value. Let us see why this is true.

PROOF. Let f be a Boolean function that satisfies the strict avalanche criterion as we have defined it above and let α be an arbitrary vector from V_n with $w_H(\alpha) = 1$. That means that in this case $x \oplus \alpha$ represents the input with exactly one changed input bit.

We know that, since we are operating with Boolean functions, $f(x) \oplus f(x) = 0$. By definition it is also true that $f(x) \oplus f(x \oplus \alpha)$ is a balanced function. Therefore, the

addition of α had to change the value of exactly half of the output bits, otherwise the sum of both functions would not have a balanced outcome.

The process can also be reversed, which means that both definitions are equal. ■

This is in fact the initial definition of the strict avalanche criterion, as it is directly derived from an essential demand for the output not to give away any information about the modified input [6]. That is, if the input is only slightly changed (like modifying just one bit) we need the output to drastically change. The functions that satisfy the strict avalanche criterion are the best in this category - one changed input bit causes exactly half the output bits to change, which is the optimal scenario.

We give a novel proof of the result below concerning the relation between SAC and the application of the generalized linear group acting on V_n.

Proposition 2.2.3. *Let f be a Boolean function mapping from V_n and let B be a nonsingular matrix of order n with zero-one entries. If $f(x) \oplus f(x \oplus \beta)$ is balanced for each row β of matrix B, then $g(x) = f(xB)$ satisfies the strict avalanche criteria.*

Proof. To prove that the function $g(x)$ satisfies the strict avalanche criterion we must show that $g(x) \oplus g(x \oplus \alpha_i)$ for $i = 1, \dots n$, where α_i is vector from V_n with all zeros and 1 in position i, is a balanced function.

$$\begin{aligned} g(x) \oplus g(x \oplus \alpha_i) &= f(x'B) \oplus f((x' \oplus \alpha_i)B) \text{ for some } x' \in V_n \\ &= f(x'B) \oplus f(x'B \oplus \alpha_i B) \\ &= f(x'B) \oplus f(x'B \oplus \beta_i), \end{aligned}$$

where β_i is the i-th row of the matrix B.

Since $f(x) \oplus f(x \oplus \beta)$ is a balanced function, by Lemma 2.1.3 so too must be $f(x'B) \oplus f(x'B \oplus \beta_i)$. We have therefore proven the proposition. ■

Example 2.2.4. *Here we will make an example of how we can change a function that does not satisfy the strict avalanche criterion into one that does.*

Let $f(x) = x_1x_2 \oplus x_3$ and $\alpha = (0, 0, 1)$. Clearly, the function f does not satisfy the SAC for α since $f(x) \oplus f(x \oplus \alpha) = (x_1x_2 \oplus x_3) \oplus (x_1x_2 \oplus (x_3 \oplus 1)) = 1$.

But for $\beta = (1, 0, 0), \gamma = (0, 1, 0)$ and $\delta = (1, 1, 1)$ the functions

$$f(x) \oplus f(x \oplus \beta) = f(x) \oplus f(x \oplus \gamma) = f(x) \oplus f(x \oplus \delta) = x_1 \oplus x_2 \oplus 1$$

are in fact balanced.

Let us therefore consider the matrix $B = \begin{bmatrix} \beta \\ \gamma \\ \delta \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$.

By Proposition 2.2.3 we see that the modified function $g(x) = f(xB)$ must satisfy the strict avalanche criterion.

2.3 Algebraic degree

To resist various methods of cryptanalysis, a high algebraic degree is an important cryptographic criterion in the design of Boolean functions. To properly define it we will first see what algebraic normal form or ANF is.

Definition 2.3.1 ([3]). *Let f be a Boolean function mapping from V_n, let u be a vector from $\mathbb{Z}_2^n$ and let $X_u = x_1^{u_1} \cdots x_n^{u_n}$ be a Boolean function. Algebraic normal form of a Boolean function f is*

$$f = \bigoplus_{u \in \mathbb{Z}_n} h_u X_u,$$

where $h_u \in \{0, 1\}$.

This formal definition is illustrated in the following example.

Example 2.3.2. *We get the ANF of the function $f(x) = (1 \oplus x_1)(x_2 \oplus x_1x_3)$ by multiplying the components so that our function is of the form $g(x) = a_0 \oplus a_1x_1 \oplus a_2x_2 \oplus a_3x_3 \oplus a_4x_1x_2 \oplus a_5x_1x_3 \oplus a_6x_2x_3 \oplus a_7x_1x_2x_3$. In our case that is $g(x) = x_2 \oplus x_1x_2$.*

Example 2.3.3. *We will also show a quick example of how, given the truth table of a function f, we can find its uniquely corresponding algebraic normal form.*

Let us consider the following truth table: $(0, 0, 1, 1)$ and an arbitrary polynomial on 2 variables of the form $a \oplus bx_1 \oplus cx_2 \oplus dx_1x_2$.

We have now four equations with four variables. With substitutions we quickly see that $a = 0$, $b = 0$, $c = 1$ and $d = 0$. The polynomial we were looking for must therefore be $f(x) = x_2$.

Given a truth table of an arbitrary function g on n variables we therefore have a to solve a system of 2^n equations with 2^n variables.

Definition 2.3.4. *Let f be a Boolean function written in algebraic normal form. Then its algebraic degree is the greatest number of variables in any of its monomials.*

Example 2.3.5. *The algebraic degree of the function $f(x) = 1$ is therefore 0 and the degree of $g(x) = x_1 \oplus x_1x_5 \oplus x_2x_5 \oplus x_1x_2x_5x_6$ is 4.*

2.4 Correlation immunity

The correlation immunity was first studied for its cryptographic significance in 1984 in [26]. It measures to which degree does the output correlate to a subsets of the input. It is, of course, desired that the correlation is as low as possible and the optimal situation arises when the inputs and the output are completely statistically independent. The property itself was over the years defined in various different equivalent ways. We will be using definition as provided in [10]:

Definition 2.4.1. *The Boolean function f mapping from V_n is called correlation immune of order m if for every m indices $1 \leq i_1 < i_2 < \cdots < i_m \leq n$ and for every $(a_1, \ldots, a_m) \in V_m$ we have*

$$P(f(x) = 1 | (x_{i_1}, x_{i_2}, \ldots x_{i_m}) = (a_1, a_2 \ldots, a_m)) = P(f(x) = 1).$$

That is, if the output is statistically independent of all the m-subsets of the input.

Definition 2.4.2. *If the Boolean function f mapping from V_n is correlation immune of order m and balanced it is called m-resilient.*

One interesting property that ties together the number of variables of a Boolean function, its correlation immunity and algebraic degree is the following:

Proposition 2.4.3. *[26] Let f be a Boolean function on n variables with correlation immunity of order m and algebraic degree d. Then $m + d \leq n$.*

Unfortunately we will not include the proof of this nice proposition here. A more interested reader may find the proof in [26].

2.5 Nonlinearity

The property we have left for last in this introductory chapter is nonlinearity. It measures how far away a function f is from the set of affine functions. That is, how much more complex its output is in comparison with affine functions that have the lowest cryptographic complexity excluding the constant functions.

Here we will look at only the basic definition of nonlinearity and will further develop the concept in the following chapters.

Definition 2.5.1. *[12] Let f be a Boolean function mapping from V_n and let A_n be the set of all affine functions on n variables. Then, the nonlinearity of Boolean function f is defined as*

$$N(f) = \min_{f \in A_n} d_H(f, h),$$

where d_H is the Hamming distance.

A very interesting family of Boolean functions are those functions reaching the highest possible nonlinearity. That is, compared to the simple affine functions their structure is the most complex, the most nonlinear. They are called the *bent functions* and will be the focus of this master thesis.

To properly define these, however, we first need to introduce the Fourier transformation.

3 Nonlinearity

First we will take a look at Fourier transformation and Praseval's identity, both of which will be then used to prove the connection between nonlinearity and the Walsh-Hadamard transformation. This connection is very useful, as it provides us with the easiest way of defining a bent function, as we will see in the continuation of this chapter.

3.1 Fourier transformation of Boolean functions

The content of the following chapter is in large part taken from [27].

Since [27] uses an alternative definition of Boolean function, introducing it as a function F that maps $F : V_n \longrightarrow \{1, -1\}$ instead of $f : V_n \longrightarrow \{1, 0\}$, we will for the sake of greater consistency denote the function $F(x)$ as $F(x) = (-1)^{f(x)}$, where f is a Boolean function, as defined in 2.0.1.

Our first goal is to create a basis of functions to use in the Fourier transformation. Let us recall that in our case the basis is a set of basis functions, such that any function of the form $F : V_n \longrightarrow \mathbb{R}$ can be written as a linear combination of basis functions. We will name the basis, described in the following, the Fourier basis.

The number of functions in the Fourier basis is 2^n. Let "$\cdot$" denote the inner or dot product between two vectors. That is, let $x \cdot y = x_1y_1 \oplus \cdots \oplus x_ny_n$. Then we can create for each element $v \in V_n$ a function $\chi_v : V_n \longrightarrow \{1, -1\}$ where

$$\chi_v(x) = (-1)^{v \cdot x}.$$

Together they form the Fourier basis.

We can also quickly see that the functions are mutually orthogonal and that they in fact form a normal basis.

Definition 3.1.1. *Scalar product of Boolean functions f and g mapping from V_n is defined as*

$$\langle g, h \rangle = \frac{1}{2^n} \sum_{x \in V_n} f(x)g(x)$$

.

Corollary 3.1.2 (Fourier transformation). *For any function $F : V_n \longrightarrow \mathbb{R}$ it holds that*

$$F(x) = \sum_{v \in V_n} \hat{F}(v)\chi_v(x),$$

where

$$\hat{F}(v) = \langle F, \chi_v \rangle = \frac{1}{2^n} \sum_{x \in V_n} (-1)^{f(x) \oplus v \cdot x}$$

are the Fourier coefficients.

The Fourier transformation is introduced in more detail, which we are skipping in this thesis, and with a longer explanation in [27].

We also know of Parseval's identity, which connects Fourier coefficients with the function's values.

Theorem 3.1.3 (Parseval's identity). *For any function $F : V_n \longrightarrow \mathbb{R}$ it holds that*

$$\sum_{v \in V_n} \hat{F}^2(v) = \langle F, F \rangle.$$

Proof. Let us look at the following equation:

$$\begin{aligned} \langle F, F \rangle &= \left\langle \sum_{v \in V_n} \hat{F}(v)\chi_v(x), \sum_{u \in V_n} \hat{F}(u)\chi_u(x) \right\rangle \\ &= \sum_{v,u \in V_n} \hat{F}(v)\hat{F}(u)\langle \chi_v(x), \chi_u(x) \rangle \\ &\quad \text{we use the fact that the functions } \chi_v(x) \text{ are orthogonal for every } v \in V \\ &= \sum_{v \in V_n} \hat{F}^2(v) \end{aligned}$$

Thus the result follows. ∎

For the functions of the form $(-1)^{f(x)}$, where $f(x)$ is a Boolean function, this result can be even improved.

Corollary 3.1.4. *For every function of the form $F : V_n \longrightarrow \{1, -1\}$ it holds that*

$$\sum_{v \in V_n} \hat{F}^2(v) = 1.$$

Proof. Let us consider the following equation:

$$\begin{aligned}\sum_{v\in V_n}\hat{F}^2(v) &= \langle F,F\rangle \\ &= \frac{1}{2^n}\sum_{x\in V_n}F(x)^2 \\ &\quad \text{we use the fact that the function } F(x) \text{ maps to } \{1,-1\} \\ &= 1\end{aligned}$$

Thus the result follows. ∎

Now we have all the tools needed to proceed with further exploration of nonlinearity.

3.2 Nonlinearity of Boolean functions

We must first introduce the Walsh-Hadamard transformation, as defined in [11].

Definition 3.2.1. *Let f be a Boolean function mapping from V_n, $v \in V_n$ and let the operation $\cdot$ be the usual scalar product between the vectors in V_n. Then the Walsh-Hadamard transformation of a Boolean function f over the field V_n is*

$$W_f(v) = \sum_{x\in V_n}(-1)^{f(x)\oplus v\cdot x}.$$

We give a proof of the result below concerning the alternative way of expressing the nonlinearity of a function compared to the definition 2.5.1.

Proposition 3.2.2. *Let f be a Boolean function mapping from V_n. Then the nonlinearity of function f is equal to*

$$N(f) = 2^{n-1} - \frac{1}{2}\sup_{v\in V_n} \mid W_f(v) \mid .$$

Proof. Let us first look at the Walsh-Hadamard transformation, while considering two cases. First case is when the affine function is a linear function. Then, $W_f(v) = \sum_{x\in V_n}(-1)^{f(x)+v\cdot x}$, where $v\cdot x = v_1x_1 \oplus \cdots \oplus v_nx_n$ plays the role of our linear function.

When the values of functions $f(x)$ and $v\cdot x$ are the same, we have $(-1)^{f(x)+v\cdot x} = 1$, otherwise $(-1)^{f(x)+v\cdot x} = -1$.

The number of all elements in the space V_n is 2^n. Let k denote number of elements $x \in V_n$, such that $f(x) = v\cdot x$, and let l denote the number of elements, such that $f(x) \neq v\cdot x$. Thus, we get two equations:

$$k + l = 2^n$$

and

$$k - l = W_f(V).$$

We join both equations and get $l = 2^{n-1} - \frac{1}{2}W_f(v)$. Since we would like to get the smallest possible number of inequalities between the linear functions and the function f, we must minimize l and therefore maximize $W_f(v)$, where we take into account its absolute value.

Therefore, $2^{n-1} - \frac{1}{2}\sup_{v\in V_n} \mid W_f(v) \mid$ is the smallest possible Hamming distance between the function f and the linear functions.

Let us now consider the second case, where we are dealing with affine functions with the constant coefficient $c = 1$. These are in fact just the functions from the previous case, but with the addition of 1. Therefore, the absolute values of the Walsh coefficients remain the same and $2^{n-1} - \frac{1}{2}\sup_{v\in V_n} \mid W_f(v) \mid$ is indeed the smallest possible Hamming distance between the function f and the affine functions.

With this the lemma is proven. ■

Let us now try to find the highest nonlinearity. We must, obviously, look for the minimum supremum of Walsh-Hadamard transformation. We give a novel and simplified proof of the result below concerning the minimum supremum of absolute value of Walsh-Hadamard coefficients.

Proposition 3.2.3. *The minimum supremum of absolute values of Walsh-Hadamard transformation of a Boolean function is* $2^{\frac{n}{2}}$.

PROOF. Let f be a Boolean function mapping from V_n. Then $F(x) = (-1)^{f(x)}$ is a well defined real function that maps from V_n to $\{1, -1\}$, on which we can perform the Fourier transformation, as was introduced in 3.1.2:

$$F(x) = \sum_{v\in V_n} \hat{F}(v)\chi_v(x),$$

where

$$\begin{aligned}
\hat{F}(v) &= \langle F, \chi_v(y)\rangle \\
&= \frac{1}{2^n}\sum_{y\in V_n}(-1)^{f(y)}(-1)^{v\cdot y} \\
&= \frac{1}{2^n}\sum_{y\in V_n}(-1)^{f(y)\oplus v\cdot y} \\
&= \frac{1}{2^n}W_f(y)
\end{aligned}$$

By Corollary 3.1.4 we know that for all Boolean functions the equality $\sum_{v \in V_n} \hat{F}^2(v) = 1$ holds.

After rearranging the above equation we get

$$\sum_{v \in V_n} W_f^2(v) = 2^{2n}.$$

Since we are looking for the minimum supremum of absolute values of Walsh-Hadamard transformation, we can assume that $W_f^2(v)$ has the same value for every $v \in V_n$. Let us denote this value with k^2.

Then, it follows

$$\begin{aligned} \sum_{v \in V_n} k^2 &= 2^{2n} \\ 2^n k^2 &= 2^{2n} \\ k &= \pm 2^{\frac{n}{2}}. \end{aligned}$$

Since the value k represents the minimum supremum of absolute values of Walsh-Hadamard transformation of a Boolean function, we have proved the proposition. ■

Remark 3.2.4. *It follows from the above proposition that the maximal nonlinearity of a Boolean function is* $2^{n-1} - 2^{\frac{n}{2}-1}$. *It is reached exactly when all of the Walsh-Hadamard coefficients equal* $\pm 2^{\frac{n}{2}}$.

And finally we can give a proper definition of a bent function.

Definition 3.2.5. *[20] A bent function is a Boolean function* f, *for which all the Walsh-Hadamard coefficients equal* $\pm 2^{\frac{n}{2}}$. *That is,* $W_f(v) = \pm 2^{\frac{n}{2}}$ *for every* $v \in V_n$.

4 Bent functions

4.1 Properties of bent functions

Let us begin with the most simple and obvious property, which concerns the function's domain. The following properties were noted and proven, as describer bellow, by Rothaus [22] back in 1960s.

Lemma 4.1.1. *If the Boolean function f mapping from V_n is a bent function, then n is an even number.*

PROOF. By definition of the bent functions, the equation $W_f(v) = \pm 2^{\frac{n}{2}}$ holds for every $v \in V_n$. And by definition of the Walsh-Hadamard transformation, all its coefficients are integers. Therefore, n is an even number. ■

We can notice that if f is a bent function, we can write all its Fourier coefficients as $2^{\frac{n}{2}}\hat{F}(v) = \frac{1}{2^{\frac{n}{2}}}W_f(v) = (-1)^{q(v)}$, where the function $q(v)$ is a well defined Boolean function mapping from V_n. We name such a function q the dual function of f.

Lemma 4.1.2. *Let the function q be the dual function of bent function f. Then q is a bent function as well and f is the dual function of q.*

PROOF. We know the following holds:

$$\begin{aligned}
\frac{1}{2^{\frac{n}{2}}}W_f(v) &= (-1)^{q(v)} \\
\frac{1}{2^{\frac{n}{2}}}\sum_{x\in V_n}(-1)^{f(x)\oplus v\cdot x} &= \sum_{x\in V_n}\frac{1}{2^n}W_q(x)(-1)^{v\cdot x} \text{ since } \hat{F} = \frac{1}{2^n}W_q(x) \\
\sum_{x\in V_n}(-1)^{f(x)\oplus v\cdot x} &= \frac{1}{2^{\frac{n}{2}}}\sum_{x\in V_n}W_q(x)(-1)^{v\cdot x} \\
(-1)^{f(x)} &= \frac{1}{2^{\frac{n}{2}}}W_q(x) \text{ for all } x \in V_n
\end{aligned}$$

From this it follows that the values of $W_q(x)$ must equal $\pm 2^{\frac{n}{2}}$ for every $x \in V_n$. This means that q is a bent function. From the last line of the equation it is also obvious that the function f is the dual function of q. ■

There also exist functions which are self-dual, as we will see in the following example.

Example 4.1.3. *Let $f = x_1x_2$ be a bent function on 2 variables. Its truth table is $(0,0,0,1)$ and the Walsh coefficients are as computed bellow:*

v_1	v_2	$\frac{1}{2^{\frac{n}{2}}}W_f(v)$
0	*0*	$\frac{1}{2^{\frac{n}{2}}}((-1)^{0+0}+(-1)^{0+0}+(-1)^{0+0}+(-1)^{1+0})=1$
0	*1*	$\frac{1}{2^{\frac{n}{2}}}((-1)^{0+0}+(-1)^{0+1}+(-1)^{0+0}+(-1)^{1+1})=1$
1	*0*	$\frac{1}{2^{\frac{n}{2}}}((-1)^{0+0}+(-1)^{0+0}+(-1)^{0+1}+(-1)^{1+1})=1$
1	*1*	$\frac{1}{2^{\frac{n}{2}}}((-1)^{0+0}+(-1)^{0+1}+(-1)^{0+1}+(-1)^{1+0})=-1$

Since we are looking for the dual function of f, that is for such a function q that $\frac{1}{2^{\frac{n}{2}}}W_f(v)=(-1)^{q(v)}$, we now know that its truth table should be $(0,0,0,1)$. But that is exactly the truth table of function f. Therefore, f is a self-dual function.

The following lemma proves useful in finding the maximum degree of a bent function.

Lemma 4.1.4. *The number of zeros of a Boolean function f equals $2^{n-1}(\hat{F}(0)+1)$. If the function f is bent, the number of zeros equals $2^{n-1}\left(\pm\frac{1}{2^{\frac{n}{2}}}+1\right)$*

Proof. From the definition of the Fourier coefficient $\hat{F}(v)$ it follows that difference between the number of zeros and ones of function $f(x)+v\cdot x$ is equal to $2^n\hat{F}(v)$.

Let us now assume that $v=0$. We get that the difference between the number of zeros and ones of $f(x)$ is equal to $2^n\hat{F}(0)$. Therefore it follows that the number of zeros of $f(x)$ equals $2^{n-1}(\hat{F}(0)+1)$.

If we now assume that f is a bent function, we know that $\hat{F}(0)=\frac{1}{2^n}W_f(0)$ and that for every $W_f(v), v\in V_n$, $W_f(v)=\pm 2^{\frac{n}{2}}$. We insert this value into the previous result and see that the number of zeros in a bent function is indeed $2^{n-1}\left(\pm\frac{1}{2^{\frac{n}{2}}}+1\right)$. ■

To prove the next property of bent functions we will need the following lemma. We give a proof of the result below concerning the parity of zeros of a function.

Lemma 4.1.5. *Let f be a Boolean function mapping from V_n. Then the parity of the number of zeros equals the coefficient of the monomial term $x_1\cdots x_n$ of the function f.*

Proof. We see that the term $x_1\cdots x_n$ is the only one that changes the value of the function an odd number of times (once), since there is only one vector in V_n such that $x_1\cdots x_n=1$. All the other terms influence the value of the function an even number of times. It follows from this that we have an even number of zeros (and ones) exactly when the term $x_1\cdots x_n$ does not appear in the function. And the other way around

- we have an odd number of zeros (and ones) exactly when $x_1 \cdots x_n$ is a part of the function. ■

Proposition 4.1.6. *Let f be a bent function that maps from V_n. Then its maximum algebraic degree is $\frac{n}{2}$, except when $\frac{n}{2} = 1$.*

Proof. We have already proven that n is an even number in 4.1.1. Let us now denote $\frac{n}{2} = k$, where $k > 1$, and $k < r < n$, $r \in \mathbb{N}$.

Let us now look at the polynomial $f(x_1, \ldots, x_r, 0, \ldots, 0) = g(x_1, \ldots, x_r)$ and the Fourier transformation

$$(-1)^{g(x)} = \sum_{v \in V_r} \hat{G}((v_1, \ldots, v_r))(-1)^{v_1 x_1 + \cdots + v_r x_r}.$$

We also know

$$(-1)^{f(x)} = \sum_{v \in V_n} \hat{F}((v_1, \ldots, v_n))(-1)^{v_1 x_1 + \cdots + v_r x_r}.$$

We compare the two equations. Since the Fourier transformation is unique, it follows

$$\hat{G}((v_1, \ldots, v_r)) = \sum_{u \in V_{n-r}} \hat{F}((v_1, \ldots, v_r, u_1, \ldots, u_{n-r})).$$

Now we look at the number of zeros of function $f((x_1, \ldots, x_r, 0, \cdots, 0))$, that is function $g(x_1, \ldots, x_r)$. By Lemma 4.1.4 the following holds:

$$\begin{aligned} \text{number of zeros} &= 2^{r-1}(\hat{G}(0) + 1) \\ &= 2^{r-1}\left(\sum_{u \in V_{n-r}} \hat{F}((0, \ldots, 0, u_1, \ldots, u_{n-r})) + 1\right) \end{aligned}$$

We have 2^{n-r} summands, all of which equal $\pm\frac{1}{2^{\frac{n}{2}}}$. Therefore the number of zeros equals $z2^{r-1-\frac{n}{2}} + 2^{r-1}$ for some $z \in \mathbb{N}$.

That means that for every $r > \frac{n}{2}$ the number of zeros will be even. By Lemma 4.1.5 this means that any monomial term of the form $x_1 \cdots x_r$ will not be present in the function. Therefore, the maximum possible algebraic degree of a bent function is $\frac{n}{2}$. ■

4.2 Equivalent definitions

Bent functions themselves can be defined in different ways, all of them equivalent to the definition from the previous chapter. Here we will take a brief look at six such definitions, as listed in [14]. These are:

1. The function f is bent.
2. Let ξ be a sequence of function f and let l be sequence of an arbitrary linear function L. Then $\langle \xi, l \rangle = \pm 2^{\frac{n}{2}}$.
3. Let α be an arbitrary non-zero vector from the vector space V_n. Then $f(x) \oplus f(x \oplus \alpha)$ is a balanced function.
4. Let M be the associated $(1, -1)$ matrix of the function f of size $2^n \times 2^n$. M is a Hadamard matrix (for the definition of the Hadamard matrix see Definition 4.2.1 bellow).
5. Nonlinearity $N(f)$ of function f satisfies $N(f) = 2^{n-1} - 2^{\frac{1}{2}n-1}$.
6. Let D be the support set of the bent function f. Then D is a Hadamard difference set in V_n with parameters $(2^n, 2^{n-1} \pm 2^{\frac{1}{2}n-1}, 2^{n-2} \pm 2^{\frac{1}{2}n-1})$.

For some of these definitions we can already prove that they are equivalent to our initial definition. For Definition 6 we will wait until Chapter 5 where we define difference sets. Definition 5 was proven in the previous chapter, as this is exactly what we observed in Remark 3.2.4.

Let us first prove the equivalence of Definitions 1 and 2.

PROOF.[1 $\Leftrightarrow$ 2] We must first note that the sequence $\langle \xi, l \rangle$ is in fact the sequence of the function $f \oplus L$. This can be easily verified as follows. Let $\xi_i = (-1)^{f(x_i)}$ and $l_i = (-1)^{L(x_i)}$. It follows that $\xi_i l_i = (-1)^{f(x_i) \oplus L(x_i)} = (-1)^{(f \oplus L)(x_i)}$.

Let us now suppose that f is indeed a bent function. This means that all of its Walsh-Hadamard coefficients equal $\pm 2^{\frac{n}{2}}$. If we choose for vector v the sequence of coefficients of the function L we get

$$W_f(v_L) = \sum_{x \in V_n} (-1)^{f(x) \oplus v_L \cdot x} = \sum_{x \in V_n} (-1)^{(f \oplus L)(x)}.$$

Now we use the above stated observation and see that we have proved the equivalence in one direction.

Let us now assume 2. As we have shown above, the vector product $\langle \xi, l \rangle$ can be directly translated into the Walsh-Hadamard coefficients. By Remark 3.2.4 the function

f is indeed bent. ■

The proof of the equivalence of Definitions 1 and 3 is omitted here, and the interested reader can find the proof in [8].

To prove the equivalence of the Definition 4 we must first define the Hadamard matrix and show some of its properties.

Definition 4.2.1. *Let H be a $(1,-1), n \times n$ matrix. If all of its rows and columns and mutually orthogonal, we call it a Hadamard matrix.*

Example 4.2.2. *A generic method of constructing Hadamard matrices recursively is using the Sylvester's construction, first introduced in [17].*

We take a Hadamard matrix H of order n. Then the matrix $\begin{bmatrix} H & H \\ H & -H \end{bmatrix}$ *is again a Hadamard matrix of order $2n$, which by itself is an easily observable fact. If two rows H_i and H_j are mutually orthogonal, then $[H_i, H_i]$ and $[H_j, H_j]$ will be orthogonal as well. The same is true for $[H_i, -H_i]$ (since the first and second part of summands will neutralize each-other) and $[H_j, -H_j]$. The same reasoning applies to the columns of H.*

With this construction we get a special class of Hadamard matrices, sometimes also called the Walsh matrices. We start with matrix [1] *and then step by step produce more matrices. Here we have listed the first three:*

$$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix}$$

Definition 4.2.3. *Let M be a matrix of order $n \times m$. Then M^T is its transposed matrix of order $m \times n$, where $M^T_{i,j} = M_{j,i}$.*

Lemma 4.2.4. *The matrix H of order n is a Hadamard matrix if and only if $HH^T = n\mathbb{I}$, where $\mathbb{I}$ is the identity matrix.*

PROOF. When multiplying HH^T we are in fact multiplying the rows of matrix H. Since all of them are mutually orthogonal, it is obvious that our result will always be

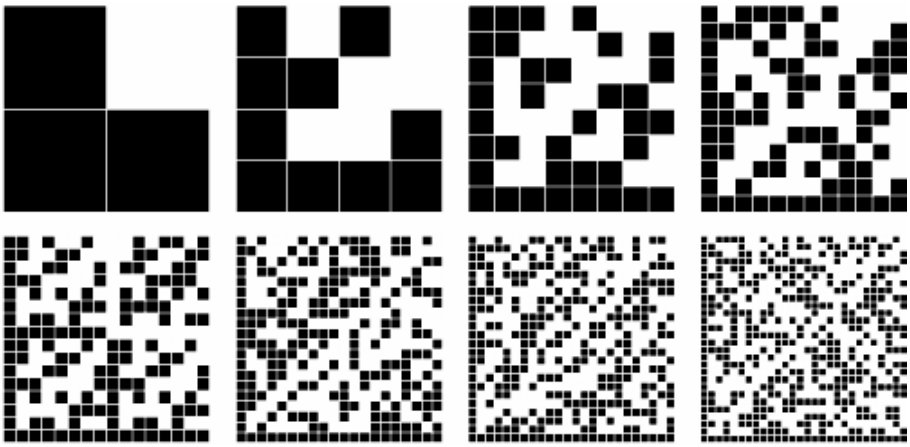

Figure 2: Some more Hadamard matrices, where entries with value 1 are coloured black and those with value -1 are coloured white, as depicted on the Wolfram Mathwolrd's webpage.

zero. Except, of course, when we multiply a row with itself when we are computing a value of the result matrix's diagonal. In that case we get n.

It is similarly evident that the only way to get the matrix $n\mathbb{I}$ is for all columns and rows to be mutually orthogonal. ■

At this point we are ready to prove the equivalence between Definition 1 and 4. We give bellow a novel proof.

PROOF.[$1 \Leftrightarrow 4$] What we need to prove is that the function f is bent if and only if the vector product of any two of the rows or columns in its matrix M equals zero. Let us pick the product of two arbitrary rows i and j and see what their product looks like.

$$\begin{aligned} M_i \cdot M_j &= \left[(-1)^{f(x_i \oplus x_k)}\right]_{k=1,\ldots,2^n} \cdot \left[(-1)^{f(x_j \oplus x_k)}\right]_{k=1,\ldots 2^n} \\ &= \sum_{k=1,\ldots,2^n} (-1)^{f(x_i \oplus x_k) \oplus f(x_j \oplus x_k)} \\ &= \sum_{k=1,\ldots,2^n} (-1)^{f(x_i \oplus x_k) \oplus f((x_i \oplus x_k) \oplus (x_j \oplus x_i))} \end{aligned}$$

At this point we take a look at the last line of the above equation and remember the equivalent Definition 3 of a bent function. Since x_k spans across all the vectors in V_n, we take the vector $x_i \oplus x_k$ as our x and the vector $x_j \oplus x_i$ as our α. From this we see that if f is a bent function, then exactly half of the values in the sum will be 1 (when the value of the function $f(x_i \oplus x_k) \oplus f((x_i \oplus x_k) \oplus (x_j \oplus x_i))$ will equal 0) and the other half -1, which means the two rows i and j will be orthogonal to each other and the matrix M will be a Hadamard matrix.

The opposite obviously holds as well. Thus the equivalence of the definitions follows. ■

Remark 4.2.5. *One more interesting property that relates the bentness of a Boolean function f and the strict avalanche criterion, as defined in 2.2.1, is the fact that f is bent if and only if the function f satisfies SAC of order n. This follows directly from the Definition 3.*

5 Difference sets and their relation to bent functions

In the following two chapters we will introduce two new combinatorial objects, difference sets and strongly regular graphs, and discuss some interesting relationships between these structures and bent functions.

We will first take a look at the representation of bent functions in terms of difference sets, as was shown by Dillon [15].

Let us first introduce the following definition.

Definition 5.0.6. *Let H be an abelian group with h elements and $K \subseteq H$ be a set of k elements of H. If the set of differences $k_i - k_j$, $k_i, k_j \in K$, contains every nonzero element of H exactly α times, then K is an (h, k, α)-difference set in H of order $n = k - \alpha$.*

From here on we will be focusing on difference sets on additively written abelian 2-groups.

It is obvious that the parameters h, k, α of the difference set cannot be independently chosen. The following lemma shows some of their dependencies.

Lemma 5.0.7. *Let K be an (h, k, α)-difference set. Then $k(k-1) = \alpha(h-1)$.*

Proof. We use double counting on the number of all possible ways to write any non-zero element of the group H as a difference between elements k_i and k_j, $k_i, k_j \in K$.

On the one hand, we know we have $h - 1$ non-zero elements in the group H and each can be written as a difference in α different ways.

On the other hand, we have k elements in K that we can subtract in $k(k-1)$ ways to get a non-zero difference.

Therefore, the equality holds. ∎

To make operating with a difference set easier we can represent it with a matrix $D(K)$. We define it in the following way:

$$D(K)_{h_i,h_j} = \begin{cases} 1 & \text{if } h_i - h_j \in K \\ 0 & \text{otherwise} \end{cases}.$$

We can easily identify some particular entries in the matrix D whose value equals 1. For example, the column belonging to the neutral element in the group H will have entries 1 in precisely those rows indexed by elements from the set K.

The matrix D itself also has a very useful property as stated by Dillon [15].

Lemma 5.0.8. *K is an (h, k, α)-difference set if and only if the following equation holds:*

$$D(K)^2 = \alpha\mathbb{J} + (k - \alpha)\mathbb{I}.$$

Proof. Let us look at the following equation:

$$\begin{aligned}
(D(K)^2)_{h_i,h_j} &= \sum_{g\in H} D(K)_{h_i,g} D(K)_{g,h_j} \\
&= \sum_{k\in H} \begin{cases} 1 & \text{if } h_i - g = k' \in H \text{ and } g - h_j = k' \in H \\ 0 & \text{otherwise} \end{cases} \\
&= \sum_{h\in H} \begin{cases} 1 & \text{if } h_i - h_j = k' - k'' \\ 0 & \text{otherwise} \end{cases} \\
&= \begin{cases} \alpha & \text{if } h_i - h_j \neq 0 \\ k & \text{otherwise} \end{cases}.
\end{aligned}$$

The lemma therefore holds. ∎

There is a special family of difference sets, the Hadamard difference sets, that will be especially useful in this and the following sections.

Definition 5.0.9. *If an (h, k, α)-difference set K satisfies the condition $h = 4(k - \alpha)$, it is called a Hadamard difference set.*

Let us briefly explain the reasons for calling such a set the Hadamard difference set.

By Definition 4.2.1, Hadamard matrix H is a square matrix of size $n \times n$ where entries are either 1 or -1, where all the rows and columns are mutually orthogonal and with the property that $HH^T = n\mathbb{I}$. Let us now take the matrix $D(K)$, replace the values 0 by 1 and 1 by -1, denote it by $\tilde{D}(K)$ and take a look at its square.

$$\begin{aligned}
\tilde{D}(K)^2 &= (\mathbb{J} - 2D(K))^2 \\
&= \mathbb{J}^2 - 2\mathbb{J}D(K) - 2D(K)\mathbb{J} + 4D(K)^2 \\
&= h\mathbb{J} - 2k\mathbb{J} - 2k\mathbb{J} + 4(\alpha\mathbb{J} + (k - \alpha)\mathbb{I}) \\
&= 4(k - \alpha)\mathbb{I} + (h - 4(k - \alpha))\mathbb{J}
\end{aligned}$$

We see that if K was a Hadamard difference set, then $\tilde{D}(K)^2$ would equal $h\mathbb{I}$. Since it follows from the definition of $\tilde{D}(K)$ that in our case $\tilde{D}(K) = \tilde{D}(K)^T$, this also means

that $\tilde{D}(K)$ is a Hadamard matrix, as $\tilde{D}(K)\tilde{D}(K)^T = \tilde{D}(K)^2 = h\mathbb{I}$. This can in fact be used as an alternative definition of a Hadamard difference set:

Lemma 5.0.10. *An (h, k, α)-difference set is Hadamard if and only if $\tilde{D}(K)^2 = h\mathbb{I}$ and is therefore a Hadamard matrix.*

The next theorem demonstrates how the added restriction on the cardinality of our group $h = 2^n$, since we have already stated that we are dealing with abelian 2-groups, determines the parameters of the difference set. Since these groups can be in fact considered V_n vector spaces, they can have Boolean functions defined on them.

Theorem 5.0.11. *Let H be an elementary abelian 2-group with cardinality 2^n and $K \subseteq H$ an (h, k, α)-Hadamard difference set. Then n is even, $k = 2^{n-1} \pm 2^{\frac{n}{2}-1}$ and $\alpha = 2^{n-2} \pm 2^{\frac{n}{2}-1}$.*

Proof. K is a Hadamard difference set therefore $k = \frac{h}{4} + \alpha$. We insert this into the equation from Lemma 5.0.7:

$$\begin{aligned} 0 &= k(k-1) - \alpha(h-1) \\ &= \left(\frac{h}{4} + \alpha\right)\left(\frac{h}{4} + \alpha - 1\right) - \alpha(h-1) \\ &= \alpha^2 - \frac{h}{2}\alpha + \left(\frac{h^2}{16} - \frac{h}{4}\right) \end{aligned}$$

The solutions of this quadratic equation are $\alpha = \frac{h}{4} \pm \frac{1}{2}\sqrt{h}$.

Consequently h must be a square. If we now insert $h = 2^n$, as H is an elementary abelian 2-group, we see that n must be an even number. The values for the parameters k and α also follow directly. ■

The knowledge of the possible values of the parameters that define Hadamard difference sets in elementary abelian 2-groups enables a nice connection between these sets and bent functions.

Theorem 5.0.12. *Let $K \subseteq H$ be a Hadamard difference set in an elementary abelian 2-group H of order 2^n. Then there exists a bent function f mapping from V_n, such that $K = supp(f)$. The opposite also holds. The support of any bent function mapping from some V_n is a Hadamard difference set for an elementary abelian 2-group.*

Proof. As we have already noted before, the group H can in this case be considered as a vector space V_n. Since K, the Hadamard difference set, is a subset of the group H, we can construct a Boolean function f such that $K = supp(f)$.

Now we have to prove that the function f is bent. Let us therefore consider the Hadamard matrix $\tilde{D}(K)_{k_1,k_2} = \begin{cases} -1 & \text{if } \mathrm{k_1 + k_2 = k_1 - k_2 \in K} \\ 1 & \text{otherwise} \end{cases} = (-1)^{f(k_1+k_2)}$.

We see that the Hadamard matrix $\tilde{D}(K)$ is exactly the matrix of the function f. By the 4-th equivalency above, we now know that f must be a bent function. Since the opposite is also true (that is, if f is bent, then $\tilde{D}(K)$ is a Hadamard matrix), we have proved the theorem. ■

The above result also implies the 6-th equivalence introduced in the beginning of Section 4.2.

6 Strongly regular graphs and bent functions

In this section we will show how a bent function is connected to and how it can be represented by a strongly regular graph. The connection itself was first noted and proven in [1], [2].

Let us begin by defining some of the basic concepts from the graph theory.

Definition 6.0.13. *Let V be a set of vertices and $E \subseteq V \times V$ be a set of edges. Then $G = (V, E)$ is a graph where two vertices $u, u' \in V$ are connected precisely when $(u, u') \in E$.*

In general, a graph $G = (V, E)$ can contain multiple edges between two vertices and it can contain loops (an edge where the starting vertex and the ending vertex are the same). The graphs we will use will be finite graphs without loops and multiple edges.

If a graph has no edges, we call it an empty graph. If a graph $G = (V, E)$ has all possible edges ($E = V \times V$), we call it a full graph.

If the vertices u and u' are connected, we write $u \sim u'$.

Definition 6.0.14. *Let $G = (V, E)$ be a graph. Then its complementary graph $\overline{G} = \overline{(V, E)}$ is a graph where the set of vertices remains the same but two vertices are connected if and only if they are not connected in the original graph G.*

We note at this point that if we look at the complementary graph of the complement of graph G, we get the original graph G. That is $\overline{\overline{G}} = G$.

Definition 6.0.15. *We denote the degree of a vertex u in the graph G by $deg_G(u)$ and it is equal to the number of edges for which vertex u is a starting vertex.*

Definition 6.0.16. *We say that the graph G is regular if every vertex of the graph has the same degree. If $r = deg_G(u)$ for every $u \in V$, then the graph G is r-regular.*

Having defined regular graphs, we can take a look at which conditions must be met for it to be strongly regular.

Definition 6.0.17. *The graph $G = (V, E)$ is strongly regular with parameters (v, r, λ, μ) if it is r-regular on v vertices and if the following holds:*

1. *every pair of connected vertices $u, u' \in V$ has exactly λ common neighbours;*

2. *every pair of non-connected vertices $u, u' \in V$ has exactly μ common neighbours.*

Example 6.0.18. *Let us look at an example of a strongly regular graph. The graph in Figure 3 is called the Petersen graph and possesses many nice properties, with strong regularity being just one of them.*

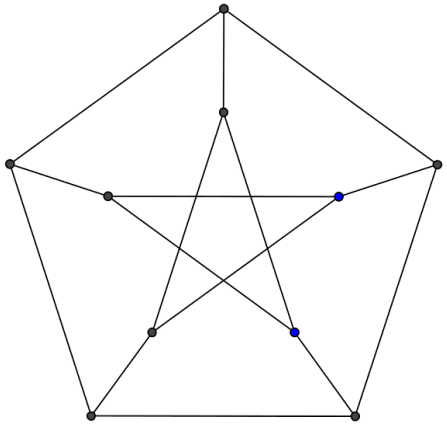

Figure 3: The Petersen graph.

The Petersen graph is a graph on 10 *vertices and we see that each of them has valency* 3*. Because of its symmetries we can quickly check that any two connected vertices have zero common neighbours, as there are no triangles in the graph. We also see that any two unconnected vertices have exactly* 1 *common neighbour.*

That means that the Petersen graph is a $(10, 3, 0, 1)$*-strongly regular graph.*

Next we define certain structures and prove some of their properties that will help us in showing how a bent function can be represented by a strongly regular graph.

In our case the easiest way to operate with the graph will be by looking at its adjacency matrix.

Definition 6.0.19. *The adjacency matrix of graph the G is a square $(0, 1)$-matrix $A(G)$ of order $\mid V \mid$ where*

$$(A(G))_{u,u'} = \begin{cases} 1 & \text{if } (u, u') \in E \\ 0 & \text{otherwise} \end{cases} .$$

Since we can freely choose in which way to enumerate the vertices, a graph usually has more than one adjacency matrix. Any of them, however, completely defines the original graph.

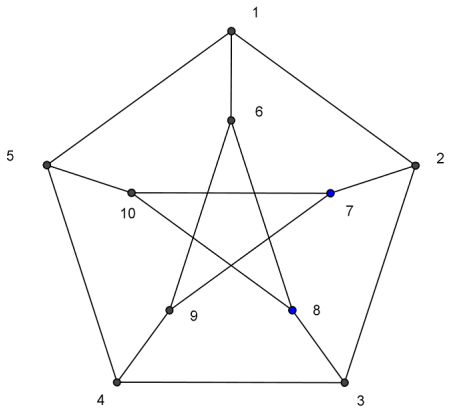

Figure 4: Petersen graph G_1 with enumerated vertices.

Example 6.0.20. *Here we take a look at the graph G in the Figure 4 and show two possible adjacency matrices.*

Using the enumeration as we see it in Figure 4, we get the bellow adjacency matrix.

$$A(G_1) = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \end{bmatrix}$$

If, on the other hand, we use different enumeration, we also get a different adjacency matrix that is still describing the same, that is, an isomorphic graph.

Now we get a different adjacency matrix:

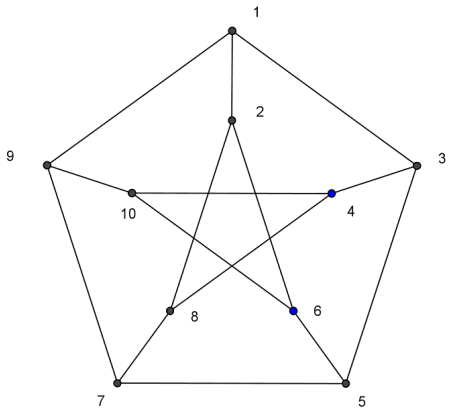

Figure 5: Petersen graph G_2 with enumerated vertices.

$$A(G_2) = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Definition 6.0.21. *A walk of length k between vertices u and w is a sequence of k edges $(u,x)(x,y)\dots(t,z)(z,w)$. If all of the visited vertices are distinct from one another, we call this a path.*

Definition 6.0.22. *The distance between two vertices u and v is the length of the shortest existing path between them. In case there exists no path between them, we write $dist(u,v) = \infty$.*

Now to show a property of the adjacency matrix that gives us more information about the number of different paths between vertices that will be used later.

Lemma 6.0.23. *Let $G = (V,E)$ be graph, $u, u' \in V$ and $k \in \mathbb{N}$. Then the number $((A(G))^k)_{u,u'}$ is the number of different paths between vertices u and u' of length k.*

Proof. Let us first denote the number of paths of length k between vertices u and u' by $p_k(u,u')$.

We will use induction on k. For $k = 1$, our claim is trivial and by the definition of the adjacency matrix it obviously holds.

Let us now assume that the following is true: $p_{k-1}(u, u') = ((A(G))^{k-1})_{u,u'}$. Therefore, since a path of length k between vertices u and u' must be constructed from a path of length $k-1$ between vertices u and some w and from a path of length 1 between w and u', the following holds:

$$\begin{aligned} p_k(u, u') &= \sum_{w \in V} p_{k-1}(u, w) p_1(w, u') \\ &= \sum_{w \in V} ((A(G))^{k-1})_{u,w} ((A(G)))_{w,u'} \\ &= ((A(G))^k)_{u,u'} \end{aligned}$$

Thus the result follows. ■

The adjacency matrix of a strongly regular graph also has some additional useful properties.

Lemma 6.0.24. *A graph G is strongly regular with parameters (n, r, λ, μ) if and only if the following is true:*

$$A(G)^2 = (\lambda - \mu)A(G) + \mu\mathbb{J} + (r - \mu)\mathbb{I}.$$

Proof. By Lemma 6.0.23 we know that $A(G)^2_{u,v}$ represents the number of different paths of length 2 between vertices u and v. Wee need to consider three different cases.

The first case is $u = u'$.

$$\begin{aligned} A(G)^2_{u,u} &= (\lambda - \mu)A(G)_{u,u} + \mu\mathbb{J}_{u,u} + (r - \mu)\mathbb{I}_{u,u} \\ &= 0 + \mu + r - \mu \\ &= r \end{aligned}$$

Since the graph G is r-regular, this must be true.

The second case is $u \neq u'$, $u \sim u'$.

$$\begin{aligned} A(G)^2_{u,u'} &= \lambda - \mu + \mu \\ &= \lambda, \end{aligned}$$

which is again true, since by the definition of a strongly regular graph, two connected vertices always have exactly λ common neighbours.

The last case arises when $u \neq u'$, $u \nsim u'$.

$$A(G)^2_{u,u'} \quad = \quad \mu$$

By the definition of a strongly regular graph, this again holds.

Thus, we see that the theorem holds for every possible pair of points, which completes the proof. ■

Lemma 6.0.25. *Let G be a (v, r, λ, μ)-strongly regular graph. Then, its complementary graph $\overline{G}$ is a $(v, v-r-1, v-2-2r+\mu, v-2r+\lambda)$-strongly regular graph.*

Proof. The number of vertices in the graph must obviously remain the same so $\overline{v} = v$.

Since every vertex is now connected exactly to the vertices to which it was not connected to in the original graph, it is connected to all the vertices apart from the vertices it was connected to originally including the connection to itself. Therefore, $\overline{r} = v - r - 1$.

To get the parameter $\overline{\lambda}$ we must take two unconnected vertices u and u' from the original graph G and count those vertices to which neither u nor u' are connected to. By using the inclusion-exclusion principle, the number of these vertices is exactly $v - 2 - 2r + \mu$.

To get the parameter $\overline{\mu}$ we must take two connected vertices w and w' in the original graph G and count all the vertices neither of them are connected to. We use the same principle as before and get $\overline{\mu} = v - 2r + \lambda$. ■

Now we have all the necessary tools to create a graph defined by a bent function and prove it is strongly regular.

Definition 6.0.26. *Let f be a bent function on n variables. Then, we define the graph G_f with $V = V_n$ and two vertices u and u' are connected if and only if $f(u + u') \neq 0$.*

Now we can use the previously defined structures and their properties to prove the main theorem of this section. The proof largely follows the procedure used in [25].

Theorem 6.0.27. *Let f be a bent function mapping from V_n. The the graph G_f is a strongly regular graph with one the following parameters:*

$$(n, r, \lambda, \mu) = (2^n, 2^{n-1} - 2^{\frac{n}{2}-1}, 2^{n-2} - 2^{\frac{n}{2}-1}, 2^{n-2} - 2^{\frac{n}{2}-1}) \text{ if } \mid supp(f) \mid = 2^{n-1} - 2^{\frac{n}{2}-1},$$

$$(n, r, \lambda, \mu) = (2^n, 2^{n-1} + 2^{\frac{n}{2}-1}, 2^{n-2} + 2^{\frac{n}{2}-1}, 2^{n-2} + 2^{\frac{n}{2}-1}) \text{ if } \mid supp(f) \mid = 2^{n-1} + 2^{\frac{n}{2}-1}$$

or its complementary graph with the added loops.

PROOF. We will divide the proof into two parts. The first part will deal with bent functions f with the property $f(0) = 0$, the second with functions where $f(0) = 1$.

Let us first suppose that $f(0) = 0$. By Theorem 5.0.12, the $supp(f)$ must be a Hadamard difference set in V_n. By the definitions of the adjacency matrix and the matrix D it then follows that $A(G_f) = D(supp(f))$. Further, by Theorem 5.0.11 we know that it is a $(2^n, k = 2^{n-1} \pm 2^{\frac{n}{2}-1}, \alpha = 2^{n-2} \pm 2^{\frac{n}{2}-1})$-Hadamard difference set.

Therefore, by Lemma 5.0.8, $A(G_f)^2 = \alpha\mathbb{J} + (k-\alpha)\mathbb{I}$. Then, by Lemma 6.0.24, this means that G_f is a strongly regular graph with parameters $(2^n, r, \mu, \mu)$ where $r = k$, $\lambda = \mu = \alpha$ if the graph is without loops. Since $f(0) = 0$, graph G does not have loops and the first statement follows.

Now we will see when we get its complementary graph with the added loops. Let us suppose that $f(0) = 1$. First we must note that the graph G_f now has a loop on every vertex since $f(u - u) = f(0) = 1$, for any vertex u.

We define a new function $\tilde{f} = f + 1$ so that $\tilde{f}(0) = 0$, and analyse its adjacency matrix. It is easily verified that by adding 1 to the bent function f in the matrix $A(G_f)$ the zeros and ones exchange places since if $f(u+v) = 0$, then $\tilde{f}(u+v) = 1$. Therefore, $A(G_{\tilde{f}}) = A(\overline{G_f})$ and $G_{\tilde{f}} = \overline{G_f}$. If we now look at the complements of both graphs we get $\overline{G_{\tilde{f}}} = G'_f$, where G'_f is the graph G_f but without the loops that were "lost" in the process because the standard definitions of complements hold for simple graphs.

With this we have proved the theorem. ■

Remark 6.0.28. *Notice that the graph G_f for which $f(0) = 1$ is a strongly regular graph with parameters*

$$(n, r, \lambda, \mu) = (2^n, 2^{n-1}+2^{\frac{n}{2}-1}, 2^{n-2}+2^{\frac{n}{2}-1}-2, 2^{n-2}+2^{\frac{n}{2}-1}) \text{ if } \mid supp(f) \mid = 2^{n-1}-2^{\frac{n}{2}-1},$$

$$(n, r, \lambda, \mu) = (2^n, 2^{n-1}+2^{\frac{n}{2}-1}, 2^{n-2}+3\cdot 2^{\frac{n}{2}-1}-2, 2^{n-2}+3\cdot 2^{\frac{n}{2}-1}) \text{ if } |supp(f)| = 2^{n-1}+2^{\frac{n}{2}-1}$$

with the added loops. This can be shown directly with the use of Lemma 6.0.25 and the knowledge that in our case G_f will be the complement of a graph of a bent function g where $g(0) = 0$.

Example 6.0.29. *We now consider a small example of representing a bent function on V_4 in terms of difference sets and strongly regular graphs.*

Let $f = x_1x_2 \oplus x_3x_4$ be a bent function mapping from V_4.

Its support set is

$$supp(f) = \{(0,0,1,1), (0,1,1,1), (1,0,1,1), (1,1,0,0), (1,1,0,1), (1,1,1,0)\}.$$

We now wish to make certain that $supp(f)$ is a $(16, 6, 2)$-difference set (since the number of elements in V_4 is 16, the number of elements in the support set is 6 and

since we are looking for a Hadamard difference set $h = 4(k-a)$ must hold). With such small numbers the fastest way would be to take a look at $\tilde{D}(supp(f))^2$.

$$\tilde{D}(supp(f)) = \begin{bmatrix}
1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 \\
1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 \\
1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 \\
-1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 \\
1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 \\
1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 \\
1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 \\
-1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 \\
1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 \\
1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 \\
1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 \\
-1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 \\
-1 & -1 & -1 & 1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 \\
-1 & -1 & 1 & -1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 \\
-1 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 \\
1 & -1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & 1
\end{bmatrix}$$

$$\tilde{D}(supp(f))^2 = \begin{bmatrix}
16 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 16 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 16 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 16 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 16 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 16 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 16 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 16 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 16 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 16 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 16 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 16 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 16 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 16 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 16 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 16
\end{bmatrix}$$

So we see that $supp(f)$ is indeed a Hadamard difference set.

Now we can also draw a strongly regular graph with the incidence matrix $A = D(supp(f))$. *Its parameters are, as we can quickly compute,* $(16, 6, 2, 2)$.

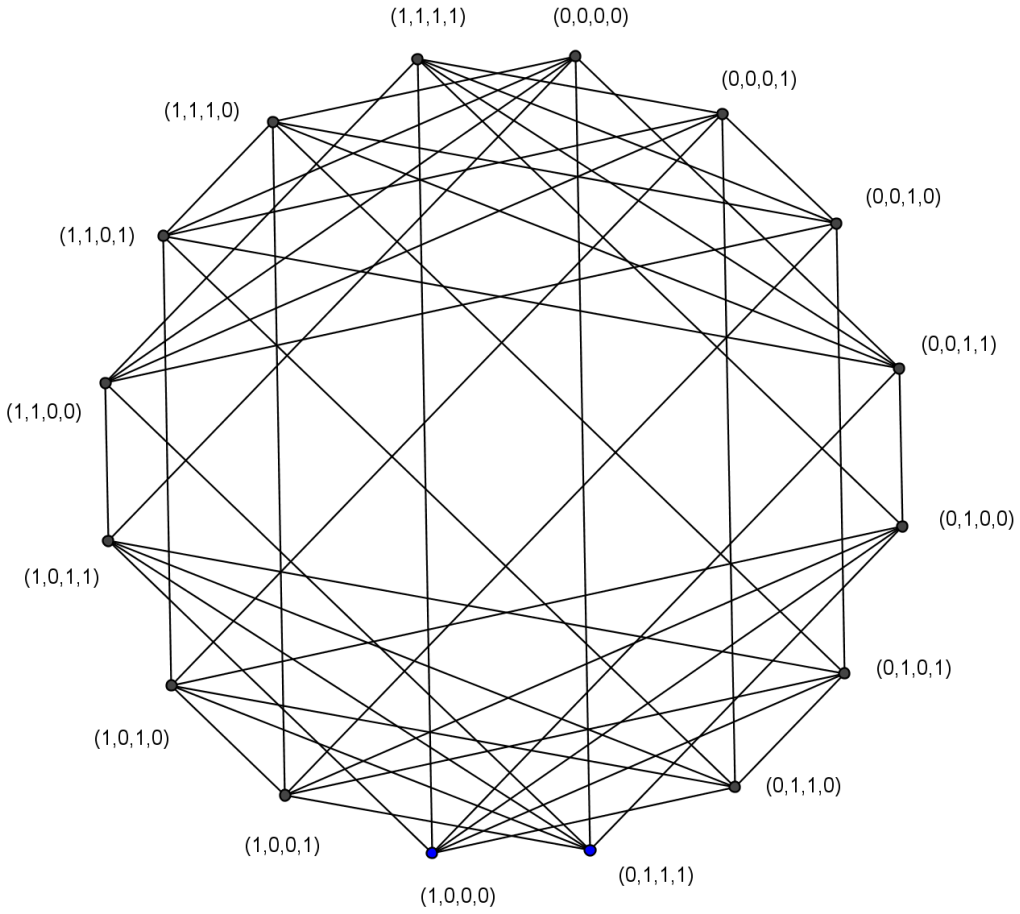

Figure 6: Strongly regular graph of the function $f(x) = x_1x_2 \oplus x_3x_4$.

7 Some generic classes of bent functions

At this point we know some things about how bent functions behave, what their most important properties are and how we can represent them. Nevertheless, the design of bent functions has not been discussed yet.

Even though there exist a few generic classes of bent functions, a complete characterization of bent functions seems to be elusive. The secondary constructions of bent functions construct new bent functions from the known ones (for instance on a larger variable space), whereas the generic classes provide an explicit design method for any n. Here we will present two of the latter, which are the most important and well known construction families, as they were described in 2010 by Carlet [8].

In the end we will also present a generalization of bent functions of Rothaus-type, which turns out to give an efficient way of defining an infinite class of bent functions. These results are to be extended to cover vectorial bent functions as well [13].

7.1 Maiorana-McFarland construction

The Maiorana-McFarland class of bent functions $\mathcal{M}$ contains functions mapping from V_n, presented as $V_{\frac{n}{2}} \times V_{\frac{n}{2}}$, to V_2. It is composed from an arbitrary permutation π on $V_{\frac{n}{2}}$ and an arbitrary Boolean function g mapping from $V_{\frac{n}{2}}$ and is of the following form:

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

where $x, y \in V_{\frac{n}{2}}$.

Let us first prove that a function of such a form is indeed a bent function.

Proposition 7.1.1. *Let x, y, π and g be as defined above. Then the function $f(x, y) = x \cdot \pi(y) \oplus g(y)$ is a bent function.*

Proof. Let us look at a Walsh-Hadamard coefficient of the function f.

$$\begin{aligned} W_f(u,v) &= \sum_{x,y\in V_{\frac{n}{2}}} (-1)^{x\cdot\pi(y)\oplus g(y)\oplus(x,y)\cdot(u,v)} \\ &= \sum_{x,y\in V_{\frac{n}{2}}} (-1)^{x\cdot\pi(y)\oplus g(y)\oplus x\cdot u\oplus y\cdot v} \\ &= \sum_{y\in V_{\frac{n}{2}}} (-1)^{g(y)\oplus y\cdot v} \left(\sum_{x\in V_{\frac{n}{2}}} (-1)^{x\cdot\pi(y)\oplus x\cdot u} \right) \\ &= \sum_{y\in V_{\frac{n}{2}}} (-1)^{g(y)\oplus y\cdot v} \left(\sum_{x\in V_{\frac{n}{2}}} (-1)^{x\cdot(\pi(y)\oplus u)} \right) \end{aligned}$$

Here we see that, since for every fixed y and u the vector x runs over the entire field $V_{\frac{n}{2}}$, $x\cdot(\pi(y)\oplus u)$ will have a balanced output except for the case when $\pi(y)=u$. This happens exactly once, that is when $y=\pi^{-1}(u)$. It therefore follows that

$$\begin{aligned} W_f(u,v) &= (2^{\frac{n}{2}}-1)0+1(-1)^{g\cdot(\pi^{-1}(u))\oplus(\pi^{-1}(u))u}\cdot 2^{\frac{n}{2}} \\ &= 2^{\frac{n}{2}}(-1)^{g(\pi^{-1}(u))\oplus(\pi^{-1}(u))u}, \end{aligned}$$

which means that W_f always equals $\pm 2^{\frac{n}{2}}$. The function f is therefore bent. ■

We would also like to mention that the above proposition, where the input is divided into two parts of equal length, holds if and only if π is a permutation. Otherwise the function $x\cdot\pi(y)\oplus g(y)$ is not bent.

The original Maiorana-McFarland construction was then extended to include constructions which do not require for the vectors x and y to be of equal length. The extension was first introduced in 1991 in [23]. We will show the result here, as it was presented in [8].

Proposition 7.1.2. *Let $n=r+s$, where $r\leq s$, be even. Let ϕ be such an arbitrary function mapping from V_s to V_r that for every $a\in V_r$ the set $\phi^{-1}(a)$ is an $(n-2r)$-dimensional affine subspace of V_s. Let g be an arbitrary Boolean function on V_s, whose restriction to $\phi^{-1}(a)$ (viewed as a Boolean function on V_{n-2r} via an affine isomorphism between $\phi^{-1}(a)$ and this vectorspace) is bent for every $a\in V_r$ if $n>2r$ (no condition on g being imposed if $n=2r$). Then the function $f_{\phi,g}=x\cdot\phi(y)\oplus g(y)$ is bent on V_{2n}.*

Proof. We again take a look at the Walsh coefficient of the function $f_{\phi,g}$. The initial transformations can be done the same as in the previous proof:

$$W_{f_{\phi,g}}(u,v) = \sum_{y\in V_s}(-1)^{g(y)\oplus y\cdot v}\left(\sum_{x\in V_r}(-1)^{x\cdot(\phi(y)\oplus u)}\right)$$

We again see that the only possibility for the sum to take a non-zero value is if $\phi(y) = u$ and, similarly, then above, we have

$$W_{f_{\phi,g}}(u,v) \;=\; 2^r \sum_{y\in\phi^{-1}(a)} (-1)^{g(y)\oplus yv}$$

Since the function $f_{\phi,g}$ is bent if and only if $W_{f_{\phi,g}}(u,v) = 2^{\frac{n}{2}}$, we see that a necessary condition for $f_{\phi,g}$ to be bent is that $r \leq \frac{n}{2}$ and $\sum_{y\in\phi^{-1}(a)}(-1)^{g(y)\oplus yv} = \pm 2^{\frac{n}{2}-r}$.

Because $r \leq s$, it holds that $r \leq \frac{n}{2}$, and because g is bent for every $a \in V_r$ if $n > 2r$, it holds that $\sum_{y\in\phi^{-1}(a)}(-1)^{g(y)\oplus yv} = \pm 2^{\frac{n}{2}-r}$. ∎

Remark 7.1.3. *In [21] it has also been observed that in a bent function of the form as described in the previous proposition, the function ϕ must be uniformly distributed over V_r (must be balanced).*

7.2 Partial Spreads Class

The Partial Spreads class $\mathcal{PS}$ is another class of bent functions, introduced in 1974 by Dillon in his PhD thesis [16]. This class is, in short, the set of all sums modulo 2 of the indicators of $2^{\frac{n}{2}-1}$ or $2^{\frac{n}{2}-1}+1$ disjoint $\frac{n}{2}$-dimensional subspaces of V_n. Let us now see what this in fact means, starting with the titular partial spread.

Definition 7.2.1. *[25] Let V_n be vector space where n is even. A set S of $\frac{n}{2}$-dimensional subspaces $H \subset V$ is called a partial spread if any two distinct subspaces H and H', $H, H' \in S$, are disjoint. That is $H \cap H' = \{0\}$.*

Definition 7.2.2. *[25] A partial spread is called maximal if there exists no partial spread in which it is strictly contained.*

It is also to be mentioned that we refer to the number of subspaces H in S as size of the partial spread. A partial spread of maximum possible size $(2^{\frac{n}{2}}+1)$ is then simply called a spread.

The disjoint $\frac{n}{2}$-dimensional subspaces of V_n we mentioned before are therefore parts of the partial spreads.

And we have already encountered functions similar to indicators:

Definition 7.2.3. *The indicator function, also called the characteristic function, i of a subset S on a set X is defined as*

$$i_S(x) = \begin{cases} 1 & \text{if } x \in S \\ 0 & \text{otherwise} \end{cases}.$$

Now we can more properly define the Partial Spread class. It is divided into two subclasses: $\mathcal{PS}^+$ and $\mathcal{PS}^-$.

Proposition 7.2.4. *[25] Let S be a partial spread on the vector space V_n of size $2^{\frac{n}{2}-1}$. We define the subset W to be*

$$W = \left(\bigcup_{k=1}^{2^{\frac{n}{2}-1}} H_k \right) \setminus \{0\},$$

where $H_k \in S$.

Then, i_W is a bent function on V_n of cardinality $2^{n-1} - 2^{\frac{n}{2}-1}$.

We denote this class of function with $\mathcal{PS}^-$.

Proposition 7.2.5. *[25] Let S be a partial spread on the vector space V_n of size $2^{\frac{n}{2}-1}+1$. We define the subset W to be*

$$W = \left(\bigcup_{k=1}^{2^{\frac{n}{2}-1}+1} H_k \right) \setminus \{0\},$$

where $H_k \in S$.

Then i_W is a bent function on V_n of cardinality $2^{n-1} + 2^{\frac{n}{2}-1}$.

We denote this class of function with $\mathcal{PS}^+$.

The proof to these two propositions is omitted here, as it would, to be presented in its entirety, require an introduction of a lot of new definitions and propositions related to vector spaces, but a more interested reader can find the proof in [15].

The duals of the functions in the $\mathcal{PS}$ class are also quite easy to find. If during the construction of the function $f \in \mathcal{PS}$ we joined together the subspaces $H_k \in S$ to create the union W, we now in order to create its dual join together subspaces $H_k^\perp$. That is, subspaces orthogonal to the originally chosen subspaces from S. By orthogonal we mean that

$$H_k^\perp = \{v \in V_n | vh = 0 \text{ for } \forall h \in H_k\}.$$

One can easily verify that the duals are again included in the $\mathcal{PS}$ class.

In his work [16] Dillon has also noted that all the elements of the class $\mathcal{PS}^-$ are of algebraic degree exactly $\frac{n}{2}$, yet the same is not true for the class $\mathcal{PS}^+$.

In the same work it is also shown that when $\frac{n}{2}$ is even, all quadratic bent functions are equal to some $\mathcal{PS}^+$ functions or their complements.

7.3 A generalization of bent functions of Rothaus-type

Together with my mentor Enes Pasalic we have considered an extension of a bent function introduced by Rothaus [22], mapping from V_6 $f(x) = x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5 \oplus x_3x_6$. The set of Boolean functions we considered was of the form $f : V_n \longrightarrow V_1$, $f(x) = x_1x_2 \cdots x_{\frac{n}{2}} \oplus x_1x_{\frac{n}{2}+1} \oplus x_2x_{\frac{n}{2}+2} \oplus \cdots \oplus x_{\frac{n}{2}}x_n$, where n is even, and have proven that all functions of this form are bent. The result is yet unpublished. Let us look at the proof.

Theorem 7.3.1. *Let n be an even number and $f_n : V_n \longrightarrow V_2$, $f_n(x) = x_1x_2 \cdots x_{\frac{n}{2}} \oplus x_1x_{\frac{n}{2}+1} \oplus x_2x_{\frac{n}{2}+2} \oplus \cdots \oplus x_{\frac{n}{2}}x_n$ a Boolean function. Then the function f is bent.*

Proof. To prove this theorem we will use the equivalent property 3, which says that for an arbitrary non-zero vector $\alpha \in V_n$ a function f is bent if and only if $f(x) \oplus f(x \oplus \alpha)$ is a balanced function.

Let us assume that $\alpha = (0_1, \ldots, 0_{\frac{n}{2}}, b)$ where $b \in V_{\frac{n}{2}}$ is a non-zero vector.

$$\begin{aligned} f(x) \oplus f(x \oplus \alpha) &= x_1 \cdots x_{\frac{n}{2}} \oplus x_1x_{\frac{n}{2}+1} \oplus \cdots \oplus x_{\frac{n}{2}}x_n \oplus x_1 \cdots x_{\frac{n}{2}} \oplus x_1(x_{\frac{n}{2}+1} \oplus b_1) \oplus \\ &\quad \oplus \cdots \oplus x_{\frac{n}{2}}(x_n \oplus b_{\frac{n}{2}}) \\ &= x_1(x_{\frac{n}{2}+1} \oplus x_{\frac{n}{2}+1} \oplus b_1) \oplus \cdots \oplus x_{\frac{n}{2}}(x_n \oplus x_n \oplus b_{\frac{n}{2}}) \\ &= x_1b_1 \oplus \cdots \oplus x_{\frac{n}{2}}b_{\frac{n}{2}} \end{aligned}$$

We see that what we got is a linear function where each variable has the coefficient either 0 or 1. Therefore it is a balanced function.

Let us now assume that $\alpha = (0_1, \ldots, 1_i, \ldots, 0_{\frac{n}{2}}, b)$ where $b \in V_{\frac{n}{2}}$ and $i \in \{1, \ldots, \frac{n}{2}\}$.

$$\begin{aligned} f(x) \oplus f(x \oplus \alpha) &= x_1 \cdots x_{\frac{n}{2}} \oplus x_1x_{\frac{n}{2}+1} \oplus \cdots \oplus x_{\frac{n}{2}}x_n \oplus x_1 \cdots (x_i + 1) \cdots x_{\frac{n}{2}} \oplus \\ &\quad \oplus x_1(x_{\frac{n}{2}+1} + b_1) \oplus \cdots \oplus (x_i + 1)(x_{\frac{n}{2}+i} \oplus b_i) \oplus \cdots \oplus x_{\frac{n}{2}}(x_n \oplus b_{\frac{n}{2}}) \\ &= x_1 \cdots x_{\frac{n}{2}} \oplus x_1x_{\frac{n}{2}+1} \oplus \cdots \oplus x_{\frac{n}{2}}x_n \oplus x_1 \cdots x_{\frac{n}{2}} \oplus x_1 \cdots x_{i-1}x_{i+1} \cdots \\ &\quad \cdots x_{\frac{n}{2}} \oplus x_1x_{\frac{n}{2}+1} \oplus x_1b_1 \oplus \cdots \oplus x_ix_{\frac{n}{2}+i} \oplus x_ib_i \oplus x_{\frac{n}{2}+i} \oplus b_i \oplus \cdots \\ &\quad \cdots \oplus x_{\frac{n}{2}}x_n \oplus x_{\frac{n}{2}}b_{\frac{n}{2}} \\ &= x_1 \cdots x_{i-1}x_{i+1} \cdots x_{\frac{n}{2}} \oplus x_1b_1 \oplus \cdots \oplus x_{\frac{n}{2}}b_{\frac{n}{2}} \oplus x_{\frac{n}{2}+i} \oplus b_i \end{aligned}$$

We see now that the variable $x_{\frac{n}{2}+i}$ appears exactly once in the function and it is a standalone summand. We quickly see that every time that any $\alpha_J = 1$, $J \subseteq \{1, \ldots, \frac{n}{2}\}$, the variables $x_{\frac{n}{2}+j}$ will appear exactly once and as standalone summand. By Lemma

2.1.6 the function $f(x) \oplus f(x \oplus \alpha)$ will be balanced for any nonzero α. Thus the result follows. ■

We can connect this result to one of the two classes $\mathcal{C}$ and $\mathcal{D}$ that Carlet introduced in [9], more precisely, we can connect it to a subclass $\mathcal{D}_0$ of the class $\mathcal{D}$. It includes functions of the form $x \cdot \pi(y) \oplus \delta_0(x)$, where $\delta_0(x)$ is the Dirac symbol and equals 1 if $x = 0$ and 0 of $x \neq 0$. The classes we introduced before, the Maiorana-McFarland class $\mathcal{M}$ and the partial spread class $\mathcal{PS}$, are both included in this subclass.

Let us now substitute the variables $x_{\frac{n}{2}+1}, \ldots, x_n$ with $y_1, \ldots y_{\frac{n}{2}}$. We can then write the generalized Rothaus bent functions as

$$f(x, y) = \prod_{i=1}^{\frac{n}{2}} x_i \oplus x \cdot y.$$

Also, if we set $\pi(y) = y$, we can write the functions in the subclass $\mathcal{D}_0$ as

$$f_{\mathcal{D}_0} = \prod_{i=1}^{\frac{n}{2}} (x_i + 1) \oplus x \cdot y.$$

Note that the addition of 1 in the product is necessary for the value of the whole product to equal $\delta_0(x)$. At this point we easily verify see that the generalized Rothaus bent functions are in fact affinely equivalent to the $\mathcal{D}_0$ function by applying the transformation $f(x \oplus (1, \ldots, 1), y) \oplus g(y)$, where $g(y) = y_1 \oplus \cdots \oplus y_{\frac{n}{2}}$. The addition of $g(y)$ is necessary to neutralize the effect of addition of $(1, \ldots, 1)$ in the second part of the function.

8 Conclusion

In the beginning of the thesis we have briefly presented cryptography and its main goals. We have described how a cryptographic system works and how algorithms used in these systems utilize Boolean functions. Since it is necessary for these functions to have certain properties, we have proceeded to describe some of them in general. Then we have focused on Boolean function that are bent.

We have introduced and proven six equivalent definitions of bentness and some of the more important properties. After that we have introduced two new combinatorial objects: difference sets and strongly regular graphs. We have proven some of their properties and then shown how a bent function can be transformed into a difference set and into a strongly regular graph.

In the end we have described two of the most widely known constructions of bent functions, the Maiorana-McFarland construction and Dillon's partial spread classes. We have also extended a function first introduced by Rothaus in 1976 on 6 variables into an infinite set of functions and have proven their bentness.

There remain a lot of open problems in the field of bent functions and generalized bent functions, mainly dealing with various methods for their construction.

Bibliography

[1] A. Bernasconi in B. Codenotti, Spectral Analysis of Boolean Functions as a Graph Eigenvalue Problem, *IEEE Transactions on Computers* 48 (1999).

[2] A. Bernasconi, B. Codenotti in J. M. Vanderkam, A characterization of bent functions in terms of strongly regular graphs, *IEEE Transactions on Computers* 50 (2001), 984–985.

[3] A. Braeken in I. Semaev The ANF of the Composition of Addition and Multiplication mod 2. V *Fast Software Encryption: 12th International Workshop*, 2005, 21–23.

[4] A. Canteaut, C. Carlet, P. Charpin in C. Fontatine Propagation Characteristics and Correlation-Immunity of Highly Nonlinear Boolean Functions. V *Eurocrpyt*, 2000.

[5] A. Kerckhoffs, La Cryptographie Militaire, *Journal des Sciences Militaires* (1883).

[6] A.F. Webster in S.E. Tavares, *Advances in Cryptology - Proceedings CRYPTO85*, Springer Verlag, 1986.

[7] B. Preneel, W.V. Leekwijck, L.V. Linden, R. Govaerts in J. Vandewalle, *Advances in Cryptology*, Springer, 1991.

[8] C. Carlet, Boolean Functions for Cryptography and Error Correcting Codes, *Boolean Models and Methods in Mathematics, Computer Science, and Engineering* (2010), 257–397.

[9] C. Carlet, Two New Classes of Bent Functions, *Euroctypt '93* 765 (1994), 77–101.

[10] C.K. Wua in E. Dawson, Correlation immunity and resiliency of symmetric Boolean functions, *Theoretical Computer Science* 312 (2004), 721–335.

[11] D. Tang, C. Carlet in X. Tang, Highly Nonlinear Boolean Functions with Optimal Algebraic Immunity and Good Behaviour Against Fast Algebraic Attacks, *IEEE Transactions on Information Technology* 59 (2013), 653–664.

[12] E. Férard in F. Rodier The complexity of the approximation of the bandwidth problem. V *International Workshop on Boolean Functions : Cryptography and Applications*, 2006, 51–58.

[13] E. Pasalic in N. Cepak, On Rothaus bent functions and its generalization, *To be submitted* .

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

[15] J.F. Dillon, A survey of bent functions, *NSA Technological Journal* Special issue (1972), 191—215.

[16] J.F. Dillon, *Elementary Hadamard Difference sets*, 1974.

[17] J.J. Sylvester, Thoughts on inverse orthogonal matrices, simultaneous sign successions, and tessellated pavements in two or more colours, with applications to Newton's rule, ornamental tile-work, and the theory of numbers, *Philosophical Magazine* 34 (1867), 461—475.

[18] J.R. Du Carlet, *La Cryptographie, contenant une très subtile manière descrire secrètement, composée par Maistre Jean Robert Du Carlet*, A manuscript exists at the Bibliothèque Nationale in Paris, 1644.

[19] N. Courtois, *Higher Order Correlation Attacks, XL algorithm and Cryptanalysis of Toyocrypt*, Springer, 2002.

[20] N. Tokareva, Generalizations of bent functions - A survey, *Journal of Applied and Industrial Mathematics* Volume 5, Issue 1 (January 2011), 110–129.

[21] O.A. Logachev, A.A. Salnikov in V.V. Yashchenko, Bent functions on a finite Abelian group, *Discrete Mathematics Appl* 7 (1997), 547–564.

[22] O.S. Rothaus, On "Bent" Functions, *Journal of Combinatorial Theory (A)* 20 (1976), 300—305.

[23] P. Camion, C. Carlet, P. Charpin in N. Sendrier, On correlation-immune functions, *Advances in Cryptology: Crypto '91* 576 (1991), 86–100.

[24] S. Singh, *Knjiga Šifer*, Učila International, 2006.

[25] T. Neumann, *Bent functions*, 2006.

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

[27] Y. Mansour, Learning Boolean Functions via the Fourier Transform, *Theoretical Advances in Neural Computation and Learning* 24 (1994), 391—424.

[28] W. Meier, E. Pasalic in C. Carlet, Algebraic attacks and decomposition of Boolean functions, *Advances in Cryptology – EUROCRYPT* 3027 (2004), 474–491.

Povzetek

Uporaba kriptografije je vgrajena v naše vsakodnevno življenje. Vsakič, ko se povežemo na internet, vsakič, ko uporabimo mobilno telefonijo, naši podatki potujejo po povezavah in preko strežnikov, nad katerimi nimamo nikakršnega nadzora, kljub temu pa bi si želeli, da naši podatki ostanejo skriti in dostopni le nam. In za to potrebujemo kriptografijo.

Tip funkcij, ki je zelo pogosto uporabljen v kriptografskih algoritmih, so funkcije, ki slikajo iz prostora V_n v V_1, imenovane boolove funkcije. Niso pa vse boolove funkcije primerne. Tako v zaključni nalogi najprej predstavimo pet glavnih kriptografskih lastnosti boolovih funkcij: uravnoteženost, propagacijski kriterij, algebraičnp stopnjp, korelacijskp imunost in nelinearnost.

Če je boolova funkcija uravnotežena, pomeni, da je natančno polovica njenih izhodnih vrednosti enaka 0 in druga polovica enaka 1. Takšne funkcije so uporabne, ker dobro prikrivajo povezanost med vhodnimi in izhodnimi podatki, saj so izhodni podatki enakomerno razdeljeni med možnimi izhodnimi vrednostmi.

Propagacijski kriteriji merijo, koliko se izhodni podatki funkcije spremenijo glede na spremenjene vhodne podatke. Idealen primer je, ko se ob enem samem spremenjenem vhodnem bitu spremeni natanko polovica vseh izhodnih bitov.

Algebraična stopnja funkcije je maksimalno število njenih spremenljivk, ki nastopajo v enem členu.

Korelacijska imunost meri stopnjo statistične odvisnosti med izhodnimi podatki in podmnožicami vhodnih podatkov. Želimo si, da je povezanost kar se da majhna, pri čemer je idealen primer, če so vhodni in izhodni podatki statistično neodvisni.

Nelinearnost je lastnost, s katero se v zaključni nalogi največ ukvarjamo. Meri oddaljenost neke boolove funkcije od množice afinih funkcij. Naj bo f boolova funkcija, ki slika iz prostora V_n, naj bo A_n množica vseh afinih funkcij z n spremenljivkami in naj d_H označuje Hammingovo razdaljo. Potem nelinearnost funkcije f definiramo kot

$$N(f) = \min_{f \in A_n} d_H(f, h).$$

Boolove funkcije, ki dosegajo maksimalno možno nelinearnost, imenujemo v angleščini "bent functions", v slovenščini pa se nanašamo nanje kot na maksimalno nelinearne boolove funkcije. V zaključni nalogi je predstavljena njihova definicija z enakim postopkom, kot ga je uporabil Rothaus [22], ki je te funkcije prvič opisal leta 1976. Uvedemo pojem Fourierove baze, Fourierove transformacije boolovih funkcij in dokažemo Parsevalovo identiteto. Definiramo tudi Walsh-Hadamarjevo transformacijo boolovih funkcij W_f in s pomočjo teh transformacij dokažemo, da lahko izrazimo nelinearnost boolove funkcije f tudi kot

$$N(f) = 2^{n-1} - \frac{1}{2} \sup_{v \in V_n} \mid W_f(v) \mid .$$

Dokažemo, da je maksimalna nelinearnost, ki jo lahko doseže boolova funkcija, enaka $2^{n-1} - 2^{\frac{n}{2}-1}$ in je dosežena natanko takrat, ko so vsi Walsh-Hadamarjevi koeficienti $W_f(v)$ enaki $\pm 2^{\frac{n}{2}}$. To vzamemo za našo uradno definicijo maksimalno nelinearnih boolovih funkcij.

Nato predstavimo nekaj lastnosti maksimalno nelinearnih boolovih funkcij. Da mora biti število spremenljivk n sodo število, lahko hitro vidimo. Predstavimo pojem duala maksimalno nelinearne funkcije in pokažemo, da je dual ponovno maksimalno nelinearna funkcija. Dokažemo, da je število ničel takšne funkcije vedno enako $2^{n-1}\left(\pm\frac{1}{2^{\frac{n}{2}}} + 1\right)$ in da je njihova maksimalna algebraična stopnja $\frac{n}{2}$.

Predstavimo in z izjemo ene dokažemo pet ekvivalentnih definicij maksimalno nelinearnih boolovih funkcij:

1. Boolova funkcija f je maksimalno nelinearna.
2. Naj bo ξ zaporedje funkcije f in naj bo l zaporedje poljubne linearne funkcije L. Potem je $\langle \xi, l \rangle = \pm 2^{\frac{n}{2}}$.
3. Naj bo α poljubni neničelni vektor iz vektorskega prostora V_n. Potem je $f(x) \oplus f(x \oplus \alpha)$ uravnotežena funkcija.
4. Naj bo M $(1, -1)$ matrika, asociirana funkciji f, velikosti $2^n \times 2^n$. Potem je matrika M Hadamarjeva matrika.
5. Nelinearnost $N(f)$ funkcije f je enaka $N(f) = 2^{n-1} - 2^{\frac{1}{2}n-1}$.
6. Naj bo množica D podporna množica funkcije f. Potem je množica D Hadamarjeva diferenčna množica v prostoru V_n s parametri $(2^n, 2^{n-1} \pm 2^{\frac{1}{2}n-1}, 2^{n-2} \pm 2^{\frac{1}{2}n-1})$.

Nato opišemo postopek pretvarjanja maksimalno nelinearne boolove funkcije v Hadamarjevo diferenčno množico. Strukturo najprej dobro definiramo in dokažemo določene lastnosti, ki pokažejo odvisnosti med parametri diferenčne množice in ki bodo uporabne pri pretvarjanju. Glede na to, da se tu omejimo na diferenčne množice na abelovih 2-grupah, pokažemo tudi, kako omejitev na kardinalnost grupe še nadaljnjo vpliva na parametre diferenčne množice. Z uporabo tako dokazanih lastnosti in četrte odzgoraj naštete ekvivalentne definicije pretvorimo maksimalno nelinearno boolovo funkcijo v diferenčno množico in sproti dokažemo šesto ekvivalentno definicijo.

Nadaljujemo s pretvorbo maksimalno nelinearnih boolovih funkcij v strogo regularen graf. Ponovno pričnemo z uvajanjem potrebnih definicij: graf, regularnost, krepko

regularen graf, komplement grafa, sosednostna matrika. Podobno kot prej dokažemo nekaj lastnosti sosednostne matrike, ki jih bomo potrebovali v nadaljevanju. Na koncu poglavja pokažemo, da lahko maksimalno nelinearno boolovo funkcijo f pretvorimo v prirejeni krepko regularni graf G_f s parametri

$$(n, r, \lambda, \mu) = (2^n, 2^{n-1} - 2^{\frac{n}{2}-1}, 2^{n-2} - 2^{\frac{n}{2}-1}, 2^{n-2} - 2^{\frac{n}{2}-1}), \text{ če je } \mid supp(f) \mid = 2^{n-1} - 2^{\frac{n}{2}-1},$$

$$(n, r, \lambda, \mu) = (2^n, 2^{n-1} + 2^{\frac{n}{2}-1}, 2^{n-2} + 2^{\frac{n}{2}-1}, 2^{n-2} + 2^{\frac{n}{2}-1}), \text{ če je } \mid supp(f) \mid = 2^{n-1} + 2^{\frac{n}{2}-1}$$

ali pa njegov komplement z dodanimi zankami. Dodamo tudi primer, v katerem dokažemo, da je funkcija $f = x_1x_2 \oplus x_3x_4$ maksimalno nelinearna, ter jo nato pretvorimo v diferenčno množico in krepko regularni graf.

Nato prikažemo dve izmed najbolj poznanih konstrukcij maksimalno nelinearnih boolovih funkcij. Osnovni Maiorana-McFarland razred vsebuje funkcije oblike $f(x, y) = x \cdot \pi(y) \oplus g(y)$, kjer je π permutacija, x in y sta enako dolga vektorja in g je boolova funkcija. Ta razred je bil kasneje razširjen v [23]: Naj bo $n = r + s$, kjer je $r \leq s$, sodo. Naj bo ϕ takšna poljubna funkcija, ki slika iz prostora V_s v V_r, da je za vsak vektor $a \in V_r$ množica $\phi^{-1}(a)$ $(n-2r)$-dimenzionalen afin podprostor prostora V_s. Naj bo funkcija g poljubna boolova funkcija, ki slika iz V_s in je pri omejitvi na $\phi^{-1}(a)$ maksimalno nelinearna za vsak $a \in V_r$, če je $n > 2r$. Potem je funkcija $f_{\phi,g} = x \cdot \phi(y) \oplus g(y)$ maksimalno nelinearna na prostoru V_{2n}.

Naslednjo predstavljeno konstrukcijo je prvi opisal Dillon v [16]. Temelji na združevanju $2^{\frac{n}{2}-1}$ ali $2^{\frac{n}{2}-1} + 1$ disjunktnih $\frac{n}{2}$-dimenzionalnih podprostorov prostora V_n. Glede na število dodanih podprostorov dobimo družino funkcij $\mathcal{PS}^-$ oziroma $\mathcal{PS}^+$.

Za konec predstavimo še posplošitev maksimalno nelinearnih boolovih funkcij tipa Rothaus. Z mentorjem Enesom Pasalicem sva vzela funkcijo $f(x) = x_1x_2x_3 \oplus x_1x_4 \oplus x_2x_5 \oplus x_3x_6$, ki jo je predstavil Rothaus v [22], jo razširila v neskončno družino boolovih funkcijo oblike $f : V_n \longrightarrow V_1$, $f(x) = x_1x_2 \cdots x_{\frac{n}{2}} \oplus x_1x_{\frac{n}{2}+1} \oplus x_2x_{\frac{n}{2}+2} \oplus \cdots \oplus x_{\frac{n}{2}}x_n$, kjer je n sod, in dokazala, da so maksimalno nelinearne. Rezultat še ni objavljen.