UNIVERZA NA PRIMORSKEM
FAKULTETA ZA MATEMATIKO, NARAVOSLOVJE IN INFORMACIJSKE TEHNOLOGIJE

DOKTORSKA DISERTACIJA
(DOCTORAL THESIS)

O UKRIVLJENIH FUNKCIJAH IZVEN POPOLNEGA MAIORANA-MCFARLAND RAZREDA IN PERMUTACIJAH, SKONSTRUIRANIH S TRANSLATORJI

(ON BENT FUNCTIONS LYING OUTSIDE THE COMPLETED MAIORANA-MCFARLAND CLASS AND PERMUTATIONS VIA TRANSLATORS)

NASTJA CEPAK

KOPER, 2018

UNIVERZA NA PRIMORSKEM
FAKULTETA ZA MATEMATIKO, NARAVOSLOVJE IN INFORMACIJSKE TEHNOLOGIJE

DOKTORSKA DISERTACIJA
(DOCTORAL THESIS)

O UKRIVLJENIH FUNKCIJAH IZVEN POPOLNEGA MAIORANA-MCFARLAND RAZREDA IN PERMUTACIJAH, SKONSTRUIRANIH S TRANSLATORJI

(ON BENT FUNCTIONS LYING OUTSIDE THE COMPLETED MAIORANA-MCFARLAND CLASS AND PERMUTATIONS VIA TRANSLATORS)

NASTJA CEPAK

KOPER, 2018

MENTOR: PROF. DR. ENES PASALIC
SOMENTOR: DOC. DR. ADEMIR HUJDUROVIĆ

Acknowledgement

First, I would like to thank Professor Enes Pasalic, who was both my PhD supervisor and the first one to introduce me to cryptography in the second year of my undergraduate studies that now seems so long ago. Throughout these four years his support and cryptographic enthusiasm were invaluable.

Zahvaljujem se tudi celotnemu matematičnemu oddelku FAMNITa za preteklih deset let, ki so me pripeljala od začetka dodiplomskega študija pa vse do zagovora doktorata, še predvsem prvemu in drugemu somentorju, Klavdiji Kutnar in Ademirju Hujduroviću.

Nič od tega pa ne bi bilo mogoče brez družine in celotne GloryBread skupine. Brez vas ne bi bila, kdor sem, in ne bi bila, kjer sem. I love you and am honoured.

Nastja Cepak

To delo sta financirala “Agencija za raziskovalno dejavnost Republike Slovenije” in raziskovalni program“Mladi raziskovalec”.

Abstract

ON BENT FUNCTIONS LYING OUTSIDE THE COMPLETED MARIORANA-MCFARLAND CLASS AND PERMUTATIONS VIA TRANSLATORS

For the first main topic of this thesis, a generalised Rothaus construction is considered when two of the three functions differ only on some suitably chosen $n/2$-dimensional subspace, which yields a significant simplification of the algebraic form of the resulting function and also gives the possibility to easily establish a connection to the Dillon's $\mathcal{PS}$ class [34]. Moreover, we show that under certain conditions, when the initial functions are taken from the class $\mathcal{D}$, the resulting bent functions provably do not belong to the completed Maiorana-McFarland class. Briefly, the so-called normality of constructed functions is considered and several examples of non-normal bent functions in 10 variables are provided.

The second topic of the thesis also focuses on the problem of inclusion in specific classes, focusing on classes $\mathcal{C}$ and $\mathcal{D}$. Apart from an explicit subclass denoted by $\mathcal{D}_0$, the bent conditions in terms of the selection of a vector subspace L and permutation π (used to define the initial function $f(x,y) = x \cdot \pi(y)$ in $\mathcal{M}$, where $x, y \in \mathbb{F}_2^n$) are rather hard to satisfy. This problem was recently addressed in [61], where some explicit bent functions $f^* \in \mathcal{C}$ were constructed. Thus, given the existence of bent functions $f^* \in \mathcal{C}$ the most fundamental issue is to determine whether these functions lie inside or outside the known primary classes.

We provide sufficient conditions on the choice of the permutation π and the corresponding linear subspace so that a bent function f^* that belongs either to $\mathcal{C}$ or $\mathcal{D}$ is outside the completed $\mathcal{M}$ class. Using these conditions we show that some instances of bent functions in $\mathcal{C}$ identified in [61] are indeed outside the completed $\mathcal{M}$ class, thus answering positively the classification issue raised in [61].

We proceed to consider some new classes of permutations over finite fields. For applicative purposes the use of sparse permutations, *i.e.* permutations which can be expressed with few terms is an important cryptographic property. For this reason, we are mainly interested in specifying design methods of sparse permutations, having a few polynomial terms.

Our work on new classes of permutations is based on the work of Kyureghyan [49], where permutations over $\mathbb{F}_{p^{rk}}$ of kind $F : x \mapsto L(x) + L(\gamma)h(f(x)), f : \mathbb{F}_{p^{rk}} \to \mathbb{F}_{p^k}, h : \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}$ are studied. Here $\gamma \in \mathbb{F}_{p^{rk}}^*$ is a so-called b-linear translator of f and L a linear permutation. Our main purpose is to emphasize that the use of functions f which have translators gives us the possibility to construct many infinite classes of permutations with a large choice of parameters. A suitable use of this method allows us also to construct linear permutations and sparse permutations of high degree and to give their compositional inverses. The connections between these constructions and *complete permutations*, *t.i.* permutations π such that $\pi + x$ is again a permutation, is also explored.

Next, the notion of a linear translator is generalised. The main problem when constructing permutations via traditional linear translators is that the set of functions that admit a linear translator is very limited. For example, we prove that the only binomial admitting a linear translator must be of the form $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^{\frac{n}{2}}}, f(x) = Tr^n_{\frac{n}{2}}(x)$. By defining the Frobenius translators we extend the family of functions admitting translator and the set of new permutations multiplies in size. With this the set of all binomials admitting a translator is, for example, extended to all functions of the form $f(x) = x^{p^i} + x^{p^i \frac{n}{2}}$. Then next step is to generalise Kyureghyan's construction of permutations in such a way that it allows the use of Frobenius translators. This opens the way to generalising various families of permutations, as well as generalising constructions of bent functions from [69].

For the last topic we present certain constructions of infinite classes of vectorial plateaued functions, permutations, and complete permutations. While there are a few known generic constructions of Boolean plateaued functions (a nice survey can be found in [11]) little is known about vectorial plateaued functions. In [11], several characterizations of those vectorial functions whose components are all plateaued (with possibly different amplitudes) were derived. In particular, it was shown that an extension of the Maiorana-McFarland class gives rise to vectorial plateaued functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$. Yet even so the component functions of F are bent and therefore they are not balanced. As a consequence this approach can never give rise to permutations. Therefore, we consider an alternative design method of vectorial plateaued functions. The framework is also extendible in terms of getting varying degree of these permutations since it is based on a suitable separation of the variable space.

Using a similar framework, we also construct complete permutations, though in this case the design of component functions is certainly more complicated.

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

Key words: bent functions, nonlinearity, Marioana-McFarland class, $\mathcal{C}$ class, $\mathcal{D}$ class, permutations, finite fields, linear translators, Frobenius translator.

Izvleček

O UKRIVLJENIH FUNKCIJAH IZVEN POPOLNEGA MIORANA-MCFARLAND RAZREDA IN PERMUTACIJAH, SKONSTRUIRANIH S TRANSLATORJI

Kot prvo temo si v tezi ogledamo posplošeno Rothausovo konstrukcijo, pri kateri se dve od treh začetnih funkcij razlikujeta samo nad določenim primerno izbranim $n/2$-dimenzionalnim podprostorm, kar vodi do konkretne poenostavitve algebraične oblike tako sestavljene funkcije. Ponuja tudi možnost enostavne povezave z Dillonovim $\mathcal{PS}$ razredom [34]. Poleg tega dokažemo, da pod določenimi pogoji, ko so začetne funkcije izbrane iz razreda $\mathcal{D}$, tako sestavljena ukrivljena funkcija leži izven popolnega Maiorana-McFarland razreda. Ogledamo si tudi tako imenovano normalnost skonstruiranih funkcij in prikažemo nekaj primerov ne-normalnih ukrivljenih funkcij na 10ih spremenljivkah.

Druga glavna tema je prav tako osredotočena na vsebovanost v specifičnih razredih, bolj natančno na vsebovanost v $\mathcal{C}$ in $\mathcal{D}$ razredu. Razen eksplicitno definiranega podrazreda $\mathcal{D}_0$ so pogoji za ukrivljenost kar se tiče izbire vektorskega podprostora L in permutacije π, ki se jih uporablja pri definiranju funkcije $f(x, y) = x \cdot \pi(y)$ v $\mathcal{M}$, kjer $x, y \in \mathbb{F}_2^n$, težko zadovoljivi. S tem problemom so se pred kratkim ukvarjali v [61], kjer so tudi eksplicitno skonstruirali določene ukrivljene funkcije $f^* \in \mathcal{C}$. S tem je najbolj temeljno vprašanje postalo, kdaj so tako sestavljene funkcije vsebovane v že poznanih primarnih razredih in kdaj ležijo izven njih.

V nadaljevanju predstavimo zadostne pogoje za izbiro takšne permutacije π in odgovarjajočega linearnega podprostora, da ukrivljena funkcija f^*, ki pripada ali $\mathcal{C}$, ali $\mathcal{D}$ razredu, leži izven popolnega $\mathcal{M}$ razreda. Z uporabo teh pogojev dokažemo, da določene ukrivljene funkcije v $\mathcal{C}$ razredu, najdene v [61], dejansko ležijo izven popolnega $\mathcal{M}$ razreda, s čimer pozitivno odgovorimo na odprto vprašanje klasifikacije, postavljeno v [61].

Nato si ogledamo tudi določene nove razrede permutacij nad končnimi polji. Za določene aplikacije je pomembno, da imajo permutacije čim manj členov. Zaradi tega nas večinoma zanimajo metode, s katerimi lahko skonstruiramo permutacijo z nizkim številom členov.

Naše delo na novih razredih permutacij temelji na delu Kyureghyan [49], ki proučuje permutacije nad $\mathbb{F}_{p^{rk}}$ oblike $F : x \mapsto L(x) + L(\gamma)h(f(x)), f : \mathbb{F}_{p^{rk}} \to \mathbb{F}_{p^k}, h : \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}$. Naš glavni namen je poudariti, da lahko z uporabo funkcij f, ki premorejo translatorje, skonstruiramo številne neskončne razrede permutacij s širokim naborom parametrov. Z uporabo te metode lahko sestavimo linearne permutacije in permutacije z malo členi visoke stopnje ter lahko najdemo njihove kompozicijske inverze. Raziščemo tudi povezavo med temi konstrukcijami in *popolnimi permutacijami*, torej takšnimi permutacijami π, da je $\pi(x) + x$ ponovno permutacija.

V četrtem poglavju je pojem linearnega translatorja posplošen. Glavni problem pri konstruiranju permutacij z uporabo tradicionalnih lienarnih translatorjev je, da je množica funkcij, ki premorejo linearni translator, zelo omejena. Na primer, dokažemo, da je edini binom, ki premore linearni translator, oblike $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^{\frac{n}{2}}}, f(x) = Tr^n_{\frac{n}{2}}(x)$. Z definicijo Frobeniusovih translatorjev razširimo družino funkcij, ki premorejo translatorje, in množica novih permutacij se pomnoži v velikosti. S tem je, na primer, množica vseh binomov, ki premorejo translator, razširjena na vse funkcije oblike $f(x) = x^{p^i} + x^{p^i \frac{n}{2}}$. Naslednji korak je posplošiti Kyureghyanino konstrukcijo permutacij na način, da dovoljuje uporabo Frobeniusovih translatorjev. S tem je odprta pot tako k posplošitvi številnih družin permutacij, kot k posplošitvi konstrukcij ukrivljenih funkcij iz [69].

Za zadnjo temo predstavimo določene konstrukcije neskončnih razredov vektorskih nivojskih funkcij, permutacij in popolnih permutacij. Kljub temu, da obstaja kar nekaj splošnih konstrukcij Boolovih nivojskih funkcij ([11] nudi dober pregled), je malo znanega o vektorskih nivojskih funkcijah. V [11] so predstavljene številne karakterizacije vektorskih funkcij, katerih komponente so nivojske (z dovoljenimi različnimi amplitudami). Dokazano je tudi, da lahko Maiorana-McFarland razred posplošimo v vektorske nivojske funkcije $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$. Vendar so komponentne funkcije od F ukrivljene in funkcija torej ni uravnovešena. Posledično Takšen pristop ne more nikoli generirati permutacije. Torej naš pristop prilagodimo in se ukvarjamo z alternativno konstrukcijo vektorskih nivojskih funkcij.

S podobnim pristopom skonstruiramo tudi popolne permutacije, pri čemer postane načrtovanje permutacije F zaradi dodatnih zahtev dosti težje.

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

Ključne besede: ukrivljene funkcije, nelinearnost, Marioana-McFarland razred, $\mathcal{C}$ razred, $\mathcal{D}$ razred, permutacije, končna polja, linearni translatorji, Frobeniusovi translatorji.

Contents

List of Figures **vii**

List of Appendices **ix**

1 Introduction **1**

2 Notations, Definitions, and Preliminary Results **9**

2.1 Boolean functions 10

2.2 Bent functions 12

2.2.1 Classes of bent functions 13

2.2.2 Vectorial bent functions 15

2.3 Other classes of highly nonlinear (vectorial) Boolean functions 16

2.4 Permutations and translators 16

3 Bent functions outside the completed Maiorana-McFarland class **19**

3.1 Constructing bent functions outside $\mathcal{M}$ using Rothau 19

3.1.1 A special case of Rothaus' construction 21

3.1.2 Using Rothaus construction iteratively 29

3.1.3 Counting bent functions in $\mathcal{PS}_{ap}$ satisfying Rothaus condition 32

3.2 Bent functions in $\mathcal{C}$ and $\mathcal{D}$ outside the extended Maiorana-McFarland class 34

3.2.1 Sufficient conditions for functions in $\mathcal{C}$ and $\mathcal{D}$ to be outside $\mathcal{M}^{\#}$ 35

3.2.2 Some examples of bent functions in $\mathcal{C}$ outside $\mathcal{M}^{\#}$ 37

3.2.3 Bent functions in $\mathcal{D}$ outside $\mathcal{M}^{\#}$ 39

3.2.4 Inclusion in other primary classes 41

4 Permutations and bent functions via translators **45**

4.1 Linear translators 45

4.1.1 On functions having linear translators 46

4.1.2 Compositional inverses 51

4.1.3 Relation with complete permutations 55

4.1.4 A special class of permutations 56

4.2 Frobenius Translators 64

4.2.1 Frobenius translators 65

4.2.2 Some existence issues 68

4.2.3 Application to bent functions 70

5 Infinite classes of vectorial plateaued functions, permutations, and complete permutations 79

5.1 Constructing permutations from $\mathcal{M}$ class 80

5.1.1 Noncubic permutations 83

5.2 Complete permutations 84

5.3 On existence of linear components and linear structures 86

5.3.1 Differential properties of the designed permutations 88

6 Conclusion 89

Bibliography 91

Index 113

7 Povzetek v slovenskem jeziku 115

Kazalo 123

List of Figures

1.1 A standard encryption scheme 2
1.2 Example of a stream cipher 3
1.3 Example of a block cipher 3
1.4 Oscar Rothaus, 1927 - 2003 5
1.5 Oleg P. Stepchenkov [82] 5

3.1 Intermediate step - subspaces of $A \oplus B$ 33

7.1 Standardna šifrirna shema 116
7.2 Primer pretočne šifre 117
7.3 Primer bločne šifre 117
7.4 Oscar Rothaus, 1927 - 2003 119
7.5 Oleg P. Stepchenkov [82] 119

List of Appendices

Proof of Theorem 3.1.2 100

Proof of Lemma 3.1.6 103

Proof of Proposition 3.1.7 106

Proof of Theorem 3.2.2 108

Chapter 1

Introduction

Cryptography's roots reach deep into our history. As soon as a king wanted to send written secret instructions to his generals, as soon as a craftsman wanted to write down a trade secret the need for *cryptography* appeared - the discipline that by today's definition enables two parties to communicate over an insecure channel. Almost everyone has heard of Julius Ceaser's simple shift cipher, but the first uses of cryptography can be traced to well over 1000 years before his time [44]. With the progress of encryption, the science of breaking the ciphers and revealing the original message, *cryptanalysis*, was also being developed. Together, cryptography and cryptanalysis form the field of *cryptology*, which has never in human history held a more important role in society at large than today.

Whereas cryptography was once dealing mainly with letters from alphabets, phrases, and signs, it now works with 0s and 1s, the symbols suited for computers and electronic communication. This modern cryptography and information theory in general were essentially invented by Calude Shannon in 1948 with his fundamental article "A Mathematical Theory of Communication" [79]. In order to satisfy today's needs there are four fundamental services that cryptography provides: confidentiality, data integrity, authentication, and non-repudiation.

Confidentiality (or *privacy*) is a service protecting the information from being revealed by unauthorized parties. *Data integrity* refers to the service designed to prevent data from being modified by unauthorized parties and to detect data modifications if they happen. The most common modifications are *insertion*, *deletion*, and *substitution*. *Authentication* refers to the ability of the two parties in communication to successfully identify each other. Finally, *non-repudiation*, ensures that neither of the two parties can deny having committed certain actions, for instance sending a transaction or signing a document.

These properties must be considered in the practical implementations of cryptosystems. Figure 1.1 depicts a standard encryption scheme designed for confidentiality. There are two parties, Alice and Bob, communicating over an insecure channel. Alice, the sender, wants to send the plaintext p to Bob, the receiver. In order to do that she encrypts it using the secret key k and encryption algorithm E, getting the ciphertext $c = E(p, k)$. She sends the ciphertext c to Bob over an insecure channel which is potentially compromised by the adversary, usually called Eve (standing for "Enemy" or "Eavesdropper") or Mallory (standing for man-in-the-

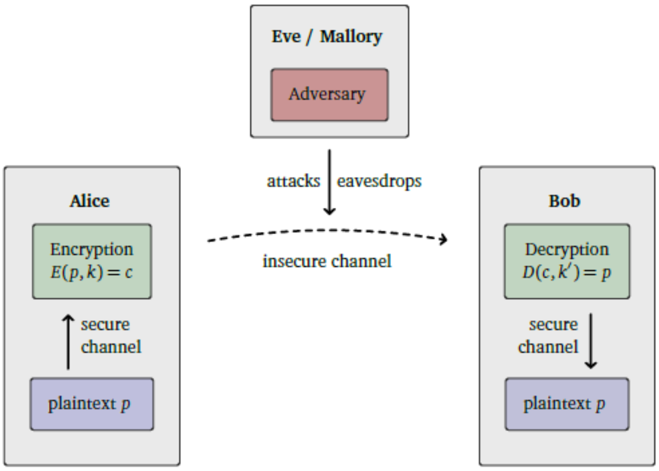

Figure 1.1: A standard encryption scheme

middle-attack) who performs cryptanalysis of the ciphertext. When Bob receives the ciphertext c he decrypts it using the secret key k' and the decryption algorithm D, getting the plaintext $p = D(c, k')$.

If the secret keys k and k' are same, this scheme is referred to as *symmetric cryptography* or *secret key cryptography*. If the keys differ, the scheme corresponds to so-called *asymmetric cryptography* or *public key cryptography*, which requires both Alice and Bob to have two keys. More precisely, they both possess a public key which is stored in a public database and accessible to anyone, and a private key which must be kept secret. Alice can therefore use Bob's public key to encrypt the plaintext and Bob then decrypts the ciphertext using his corresponding private key.

In general, symmetric key cryptography is much more computationally efficient than public key cryptography (approximately 1000 faster) and it requires shorter key length to ensure the same level of security. On the other hand, every pair of users that wants to communicate using symmetric encryption must share a common secret key. If n users want to ensure a pairwise secure communication, a total of $\frac{n(n-1)}{2}$ secret keys need to be exchanged and every user must store and keep safe $n-1$ different secret keys, which is in many cases highly impractical. In comparison, asymmetric cryptography offers a functionality of only keeping a single private key secret.

In the sequel we focus on symmetric cryptography since the main part of this thesis addresses properties of cryptographic primitives related to it. Symmetric key encryption contains two families of encryption algorithms, namely block ciphers (Figure 1.3) and stream ciphers (Figure 1.2). Stream ciphers generate a pseudo-random sequence of bits, called *keystream*, that is simply added to the plaintext modulo two to obtain the ciphertext. Among many different design rationales, a subfamily of stream ciphers (so-called filtering generator) employs a linear feedback shift register (LFSR) and a filtering Boolean function which process the content of the memory cells of LFSR to generate a single bit of the keystream [46].

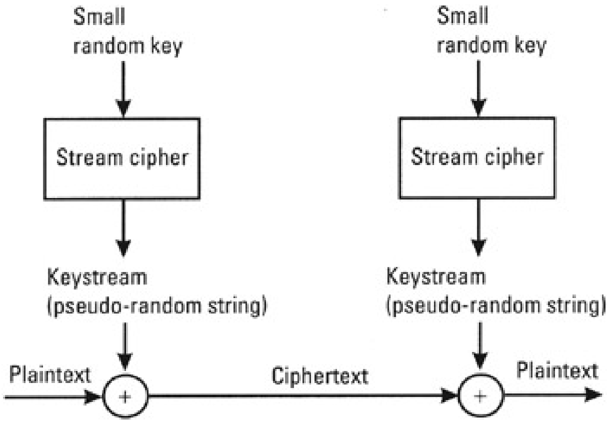

Figure 1.2: Example of a stream cipher

Some well known examples of real-life applications of LFSR-based stream ciphers include the $A5$ family of stream ciphers used in the GSM telecommunication standard [4] and the E_0 encryption algorithm used in some Bluetooth applications [59]. Some other well-known encryption algorithms that belong to the family of stream ciphers are for instance SNOW [38], RC4 [48], Trivium [8], and Grain [41].

Block ciphers represent another family of symmetric key encryption algorithms (Figure 1.3) which in general implement a pseudo-random permutation. In more detail, the plaintext is divided into blocks of data of equal length, say n, which are then consecutively processed by a block cipher to provide the output block. This process must be invertible and therefore for each different secret key (which is embedded in the encryption algorithm) block cipher implements a key specific permutation on n binary bits. The modern design of block ciphers employs an iterative application of several identical rounds to produce a ciphertext block, though their internal structure may be *Feistel-based* or alternatively *substitution-permutation network*. Nevertheless, regardless of their internal structures these iterative rounds typically implement the Shannon's concept of *confusion* through so-called *substitution-boxes* (*S-boxes*) and *difussion* through *permutation boxes* (*P-boxes*) [79]. The S-boxes can be viewed as a collection of Boolean functions (cf. Chapter 2) whereas P-boxes sim-

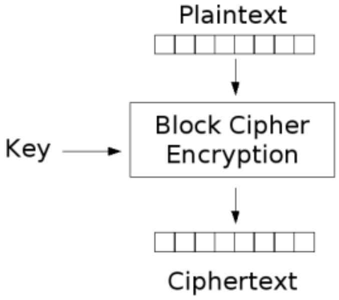

Figure 1.3: Example of a block cipher

ply permute the intermediate blocks in a linear manner though achieving the effect of the best possible diffusion of these bits so that they affect other S-boxes when processed in the subsequent round. In this context, the confusion aims at achieving a global effect of making the dependency of ciphertext bits on the key/plaintext bits as complicated as possible. One essential consequence of well designed diffusion is that changing one single bit in the plaintext should roughly cause that approximately one half of the bits in the ciphertext have flipped their values compared to the original ciphertext.

One of the earliest block ciphers was developed in 1970 by Horst Feistel and his team from IBM and was named Lucifer. Its improved version, DES (Data Encryption Standard), is one of the most prominent block ciphers and was in 1976 accepted by the USA as the Federal Information Processing Standard (FIPS). In the following years it has undergone a severe scrutiny in the academic community. Though Diffie and Hellman argued that the key length was too short to ensure long-term security [33], no serious immediate weakness of the cipher's design could have been identified. In 1992 Matsui [62] introduced a the concept of linear cryptanalysis and applied it to DES. A few years later the DESCHALL project publicly broke a coded message encrypted by DES. In the late nineties, it became clear that due to its short key length (being of size 56 bits) DES was actually susceptible to brute force attacks (today's most effective attack on DES is still the exhaustive key search), which resulted in 2001 in a new encryption standard that was named AES (Advanced Encryption Standard) and the encryption algorithm Rijndael [31] was officially selected in an open competition [71]. Some other well-known block ciphers are for instance IDEA [50], Blowfish [78], RC5 [76].

In general, when considering cryptanalytic assumptions, there are four main scenarios of applying cryptanalysis with respect to what kind of information is at the attacker's disposal.

- In the weakest *ciphertext-only* scenario, the attacker only has access to several ciphertext that were generated by a targeted block cipher using the unknown secret symmetric key. Their goal is then either to recover parts (or entire) plaintexts or alternatively to recover (a portion of) the secret key. This type of scenario is the most practical but on the other hand the cryptanalysis is hardest to perform.

- In the case of *known-plaintext* scenario, the attacker has at his disposal many plaintext/ciphertext pairs and his goal is to deduce (a portion of) the secret key.

- The *chosen-plaintext* scenario is similar to the known-plaintext attack with the difference that the attacker has the access to the encryption device and can encrypt any messages (plaintexts) of his choice. The goal is, again, to recover the secret key or a portion of it.

- The *chosen-ciphertext* scenario is similar to the latter scenario though the attacker decrypts the ciphertexts of his choice thus obtaining the corresponding plaintexts.

In the rest of this introduction, we mainly focus on the security of block ciphers. More precisely, we address the design and the security of S-boxes. Certain types of attacks, such as linear or differential cryptanalysis [5], become easier if the S-boxes (viewed as a collection of Boolean functions) have weak non-linear characteristics (*cf.* Chapter 2.2). Employing the fact that the S-boxes in DES can be approximated by suitable linear functions with certain probability, Matsui in 1993 found [64] a linear approximation for 14 rounds of DES that holds with probability 0.50000057. As a consequence, the full 16-round DES cipher could be broken in the known-plaintext scenario given 2^{47} plintext/ciphertext pairs.

To ensure high enough protection against these types of attacks the notion of *nonlinearity* was introduced, see Chapter 2 for more details. Boolean functions, which are at the largest possible distance to a set of affine functions, with the greatest possible nonlinearity are called *bent functions.* This class of Boolean functions was initially discovered by the researchers of the United States of America and the Soviet Union in separate, confidential research projects. Oscar Rothaus, Figure 1.4, is considered today to be the first researcher to publicly introduce bent functions. From 1960 to 1966, when he joined the Cornell University, he worked for Defence Department's Institute for Defence Analyses, where he first described the bent functions in his classified paper in 1966 which became available to the public only ten years later [77].

Figure 1.4: Oscar Rothaus, 1927 - 2003

Figure 1.5: Oleg P. Stepchenkov [82]

However, in the sixties, some researchers in the Soviet Union were also working on bent functions. In [82] Tokareva writes that Y. A. Vasiliev, B. M. Kloss, V. A. Eliseev, and O. P. Stepchenkov (Figure 1.5) were at that time studying properties of so called "minimal functions" whose definition coincides with that of bent functions. Most of their results, though, are still classified and not accessible to the public.

During the next decades of research on bent functions many other areas of their applications emerged. In coding theory, for instance, it was shown that determining the covering radius of a Reed-Muller code is equivalent to finding Boolean functions with highest nonlinearity [47, 60]. Bent functions are also used in the construction of famous Kerdock codes [32, 80]. They are also employed in the design of sequences with applications in certain telecommunication techniques, in particular those employing the CDMA (Code Division Multiple Access) method. In the CDMA of accessing a channel by multiple users, each user in a so-called cell must be assigned a sequence that is orthogonal to the sequences of all other users in this cell (but also to the users in all the neighboring cells). The number of users per cell is thus limited by the cardinality of the set of mutually orthogonal sequences one can construct. Bent functions and other types of Boolean functions with very high nonlinearity have been proven vital in constructing such sets. Moreover, bent functions are closely linked with Hadamard matrices, elementary Hadamard difference sets, and strongly regular Cayley graphs. In [3], it was proved that a Boolean function is bent if and only if its corresponding graph is a strongly regular Cayley graph (v, k, λ, μ), where $\lambda = \mu$.

There are still a lot of open problems related to bent functions, such as their exact number for a fixed number of variables, their design and classification. Concerning their design and classification, some primary construction methods (generating bent functions directly for any even number of input variables n) are known, see subsection 2.2.1 for their definitions. On the other hand, there are many secondary constructions which use the existing bent functions to build new ones as for instance addressed in [15, 20, 67, 95, 93]). The interested reader is referred to a nice survey on bent functions by Carlet and Mesnager. The main problem with the secondary constructions is the difficulty to answer the question about the classification of such generated bent functions. More precisely, it may happen that some of these secondary constructions simply generate bent functions which belong to the known primary classes of bent functions in which case only their explicit representation is of importance. Nevertheless, showing the non-inclusion into the completed primary classes is usually a hard task, especially in the case of the so-called $\mathcal{PS}$ class due to the lack of efficient indicators. For instance, in [61] it is shown that in many cases the functions in $\mathcal{C}$, which is a class of bent functions derived from the Marioana-McFarland primary class (denoted by $\mathcal{M}$) essentially remain in the $\mathcal{M}$ class (*cf.* Chapter 2.2.1). One of the main challenges in the area of bent functions is exactly the problem of determining whether a given bent functions lies in the completed version (completed class contains the original class and all the other bent functions that can be derived from a given class using certain affine transformations) of some primary class or it is outside of it. For the completed $\mathcal{M}$ class there exists an inclusion indicator, see [34], but even that one becomes computationally inefficient for $n > 6$. For the $\mathcal{PS}$ class there is no similar indicator, and proving exclusion from $\mathcal{PS}$ is an even more difficult problem.

Another topic that is considered in this thesis, which at the first sight does not immediately relate to bent functions, is the construction of some new classes of permutations over finite fields. A finite field of order p^n is denoted by $\mathbb{F}_{p^n}$, where p is any prime and n a positive integer. A polynomial $F \in \mathbb{F}_{p^n}[x]$ is said to be a permutation if its associated mapping $x \mapsto F(x)$ over $\mathbb{F}_{p^n}$ is bijective. Permutation polynomials received some attention already in the 19th century and due to their applications in combinatorics, coding theory, symmetric cryptography, engineering, and various other areas, the theoretical interest in these objects does not seem to fade. In general, specifying a permutation polynomial over a finite field $\mathbb{F}_{p^n}$ is not a difficult task. There are exactly $p^n!$ permutations which corresponds to the cardinality of the symmetric group on p^n elements. Once the bijection between the input space and some permuted version of the input (output) has been specified, such a permutation can be efficiently described as a univariate polynomial whose form is obtained using the Lagrange interpolation. Nevertheless, to be used in certain applications these permutation polynomials usually must possess some additional properties, such as sparseness of their representation, their differential properties, nonlinearity etc. Of course, due to a large cardinality of permutation polynomials finding some optimal classes is infeasible even for relatively small finite fields.

During the last few years there has been a tremendous progress in construction methods and characterization of many infinite classes of permutations, see a survey on recent works in [43] and the references therein. The use of permutations in applications such as coding is well-known and understood. The bijectivity is also an important cryptographic request when the design of block ciphers that use SP structure is of concern. We are mainly interested in specifying sparse permutation polynomials (due to efficient implementation), thus having a few polynomial terms. Most of the known explicit classes of permutation polynomials are of the form $X^rH(X^{\frac{p^n-1}{d}}), d < p^n - 1$, and are obtained by exploiting the multiplicative structure of the finite fields. In recent papers, ([49] and references therein) some methods to construct permutation polynomials that use the additive structure of the finite fields have been proposed. This approach is further explored in this thesis by providing several new infinite classes of permutation polynomials. At the same time, the notion *translators*, useful in designing permutation polynomials, is further extended which gives us the possibility to obtain even larger classes of permutation polynomials. Nevertheless, it turns out that the permutations based on these translators are also useful in the design of secondary classes of bent functions [69]. In this context, by introducing a notion of Frobenius translators, most of the secondary constructions of bent functions that rely on the standard linear translators can be easily generalized by employing Frobenius translators. Thus, apart from specifying new infinite classes of permutations as a by-product the generalization of certain secondary constructions of bent functions is also attained.

The rest of this thesis is structured in the following way. In Chapter 2, basic notations and definitions that are used throughout the thesis are given. In more detail, this section treats the concepts related to Boolean functions, definition of bent functions and the primary classes of these functions, as well as the notions related to permutations and translators.

Chapter 3 discusses the design of bent functions which potentially lie outside the completed Maiorana-McFarland class. In the first subsection, the construction of Rothaus is described and a special form of this design method is analysed. In the second part, sufficient conditions for bent functions within $\mathcal{C}$ and $\mathcal{D}$ class to lie outside the completed Maiorana-McFarland class are given. Some examples of such bent functions that are provably outside the completed Marioana-McFarland class are also given. Moreover, in certain cases the generated bent functions have an additional property of being non-normal which is helpful for the exclusion of these functions from some known primary classes.

Chapter 4 addresses permutations over finite fields that are constructed by means of translators. In the first subsection the linear translators are considered and the types of functions which admit linear translators are analysed. Based on this many new classes of permutations are presented. In the second subsection, the notion of linear translators is generalised through the concept of Frobenius translators which allows us to extend the design methods of permutation polynomials. As already mentioned, some secondary constructions of bent functions are then also easily generalised using the permutations obtained through Frobenius translators.

In Chapter 5, some infinite classes of vectorial plateaued functions, permutations, and complete permutations are constructed. Unlike the method used in Chapter 4, these objects are designed by considering the multivariate representation of the functions over finite fields. Roughly speaking, we considering the vector space representation of the finite field and the mappings as a collection of Boolean mappings.

The results of this PhD Thesis are published in the following articles:

- F. Zhang, E. Pasalic, Y. Wei, N. Cepak. Constructing bent functions outside the MaioranaMcFarland class using a general form of Rothaus, *IEEE Transactions on Information Theory*, 63.8 (2017), pp. 5336–5349.

- F. Zhang, E. Pasalic, N. Cepak, Y. Wei, Bent Functions in $\mathcal{C}$ and $\mathcal{D}$ outside the completed Maiorana-McFarland class." *International Conference on Codes, Cryptology, and Information Security*, Springer, Cham, 2017.

- N. Cepak, P. Charpin, E. Pasalic. Permutations via linear translators. *Finite Fields and Their Applications*, 45 (2017), pp. 19–42. Available at: https://arxiv.org/pdf/1609.09291.pdf

- N. Cepak, E. Pasalic, A. Muratović-Ribić, Frobenius linear translators giving rise to new infinite classes of permutations and bent functions, accepted for the 3rd International Workshop on Boolean Functions and their Applications

- E. Pasalic, N. Cepak, Y. Wei. Infinite classes of vectorial plateaued functions, permutations and complete permutations. *Discrete Applied Mathematics.* 215 (2016), pp. 177–184.

Chapter 2

Notations, Definitions, and Preliminary Results

Let $\mathbb{N}, \mathbb{Z}, \mathbb{R}$ denote the sets of natural numbers, integers, and real numbers, respectively, and let the ring of integers modulo r be denoted by $\mathbb{Z}_r$. Let $\mathbb{F}_q$ denote the *Galois field* of order $q = p^n$, where p is a prime number. Its cyclic group $\mathbb{F}_{p^n}^*$ is a multiplicative group with $p^n - 1$ elements, containing all the elements of the finite field $\mathbb{F}_{p^n}$ except the zero element. It is generated by a *primitive element* $\alpha \in \mathbb{F}_{p^n}^*$, and once such an element is fixed, we can use it to express the basis of the finite field as $\{\alpha^0, \alpha, \ldots, \alpha^{n-1}\}$. With this we can express any $\gamma \in \mathbb{F}_{p^n}$ as

$$\gamma = \gamma_0\alpha^0 + \gamma_1\alpha^1 + \ldots + \gamma_{n-1}\alpha^{n-1},$$

where $\gamma_0, \ldots, \gamma_{n-1} \in \mathbb{F}_p$. We see that a natural isomorphism ρ presents itself between the finite field $\mathbb{F}_{p^n}$ and *vector space* $\mathbb{F}_p^n$ of p-ary n-tuples, mapping

$$\rho : \alpha_0\gamma_0 + \ldots + \alpha_{n-1}\gamma_{n-1} \mapsto (\gamma_0, \ldots, \gamma_{n-1}).$$

In the following chapters, the binary case when $p = 2$, is the most widely considered. When we want to emphasize that an addition is over $\mathbb{F}_2$ instead of over $\mathbb{N}, \mathbb{Z}$, or $\mathbb{R}$ we denote it with "$\oplus$" instead of "$+$". We define the *Hadamard weight* of the element $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$ to be equal to the number of non-zero coordinates $w_H(x) = |\{i|x_i = 1\}| \in \mathbb{N}$, where $|A|$ denotes the cardinality of the set A. The *Hadamard distance* between two vectors $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \mathbb{F}_2^n$ is equal to the the number of coordinates where their values differ $d_H(x, y) = |\{i|x_i \neq y_i\}|$. Unless otherwise stated, we take the ordering of the vector space $\mathbb{F}_2^n$ is given as

$$\{(0, 0, \ldots, 0), (1, 0, \ldots, 0), \ldots, (1, 1, \ldots, 1)\}.$$

The *scalar/inner/dot product* of two vectors $x, y \in \mathbb{F}_2^n$ is defined as

$$x \cdot y = x_1y_1 \oplus x_2y_2 \oplus \cdots \oplus x_ny_n.$$

In the finite field, the function equivalent to the scalar product in the vector field is *trace function*. Let $x \in \mathbb{F}_{2^n}$ and $n = rk$, then the trace function from $\mathbb{F}_{2^n}$ to its subfield $\mathbb{F}_{2^k}$ is defined as

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

If $k = 1$, we denote it simply as $Tr(x)$ and call it *absolute trace*. The functions $Tr(xy)$ over a finite field is equivalent to the function $\rho(x) \cdot \rho(y)$ over a vector space.

We say that two functions $f, g \in \mathcal{B}_n$ are *affinely equivalent* if there exists a linear isomorphism $L : \mathbb{F}_2^n \to \mathbb{F}_2^n$ and a linear function $l \in \mathcal{B}_n$ such that $f(x) = g(L(x) + a) \oplus l(x) \oplus b$, where $a \in \mathbb{F}_2^n, b \in \mathbb{F}_2$.

We call functions mapping from $\mathbb{F}_2^n$ or $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ *Boolean functions* on n variables and the set of all Boolean functions is denoted by $\mathcal{B}_n$. The set of all linear functions can be described as $\{a \cdot x | a \in \mathbb{F}_2^n\}$ or $\{tr(\alpha x) | \alpha \in \mathbb{F}_{2^n}\}$. For a detailed study of Boolean functions we refer a more interested reader to Carlet [12, 13], and Cusick and Stănică [30].

2.1 Boolean functions

There exist various ways of representing Boolean functions. The *truth table* is the most straightforward. For a given Boolean function f we are given an ordered binary sequence

$$\{f(0, 0, \dots, 0), f(1, 0, \dots, 0), \dots, f(1, 1, \dots, 1)\}.$$

For higher values of n such sequences are very long and they are often presented in a hexadecimal form, as will also be the case in Chapter 3.

Boolean functions can be concatenated. The *concatenation*, denoted by "$||''$, means that the truth tables of the functions are merged. For instance, for $f_1, f_2 \in \mathcal{B}_n$ one may construct $f = f_1 || f_2 \in \mathcal{B}_{n+1}$, meaning that the upper half part of the truth table of f correspond to f_1 and the lower part to f_2.

The *support* of the function is defined as *supp*$(f) = \{x | f(x) = 1\}$. The *distance* between two Boolean function f, g on the same number of variables n is measured as the Hamming distance between their truth tables $d_H(f, g) = |\{x | f(x) \neq g(x)\}|$.

The *algebraic normal form* (ANF) is maybe the most widely used presentation in cryptography. The ANF of a function $f \in \mathcal{B}_n$ is a multivariate polynomial in $x_1, \dots, x_n$,

$$f(x_1, \dots, x_n) = \bigoplus_{I \in \mathcal{P}(N)} a_I x^I,$$

where $\mathcal{P}(N)$ denotes the power set of $N = \{1, 2, \dots, n\}$, $a_I \in \mathbb{F}_2$, and notation x^I identifies the monomial $x_{i_1} \cdots x_{i_k}$ when $I = \{i_1, \dots, i_k\} \subseteq N$. Using this form we define the *algebraic degree* of f as $\max\{|I| : a_I \neq (0, \dots, 0), I \in \mathcal{P}(N)\}$.

Then, for any $I \in \mathcal{P}(N)$ (see [12, Proposition 1]),

$$a_I = \bigoplus_{x \in \mathbb{F}_2^n / supp(x) \subseteq I} f(x), \tag{2.1}$$

where *supp*(x) denotes the support of $x = (x_1, \dots, x_n)$, i.e, the set of indices i for which $x_i \neq 0$, for $1 \leq i \leq n$. The algebraic degree is invariant under the action of the general affine group. This fact will be useful later.

The next is *univariate representation*. A univariate polynomial

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

where $\delta_i \in \mathbb{F}_{2^n}$, is a multivariate representation of a function f if and only if $\delta_0, \delta_{2^n-1} \in \mathbb{F}_2$ and $\delta_{2i \mod 2^n-1} = \delta_i^2$ for $i \in \{1, \ldots, 2^n - 2\}$. Based on this form the *polynomial degree* of f is defined as the largest such i for which $\delta_i \neq 0$.

All these three representation are unique for a given function.

The only representation that will be mentioned here that is not unique is the *trace representation.* Every Boolean function can be presented as

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

where $\delta_i \in \mathbb{F}_{2^n}$.

The *derivative* of $f \in \mathcal{B}_n$ at $a \in \mathbb{F}_2^n$, denoted by $D_a f$, is a Boolean function defined by

$$D_a f(x) = f(x+a) + f(x), \text{ for all } x \in \mathbb{F}_2^n.$$

Higher order derivatives of a Boolean function refer to k-dimensional vector subspaces, where $k > 1$. Suppose $\{a_1, a_2, \ldots, a_k\}$ is a basis of a k-dimensional subspace V of $\mathbb{F}_2^n$ (we write $\dim(V) = k$). The *k-th derivative* of f with respect to V, denoted by $D_V f$, is a Boolean function defined by

$$D_V f(x) = D_{a_k} D_{a_{k-1}} \ldots D_{a_1} f(x), \text{ for all } x \in \mathbb{F}_2^n.$$

It is to be noted that $D_V f$ is independent of the choice of the basis of V.

Cryptographically most important properties of Boolean functions are

- balancedness,
- strict avalanche criterion and propagation criterion,
- algebraic degree,
- correlation immunity, and
- nonlinearity.

Algebraic degree was already explained. A function on n variables is said to be *balanced* if exactly half of its output bits are zero; that is if $|supp(f)| = 2^{n-1}$.

The function f satisfies the *propagation criterion with respect to* α, where $\alpha \in \mathbb{F}_{2^n}$ is non-zero, if $f(x) \oplus f(x+\alpha)$ is a balanced function. It satisfies the *propagation criterion of degree k* if it satisfies the propagation criterion for every α such that $w_H(\alpha) \leq k$. It satisfies *strict avalanche criterion* (SAC) if it satisfies the propagation criterion of degree 1. If a function satisfies SAC, it means that the change of exactly one of its input bits causes the change in exactly half of the output bits.

The function f is said to be *correlation immune of order m* if the output is statistically independent of any m-subsets of the input. If the function is also balanced, it's called *m-resilient.*

Nonlinearity is the most important property for this thesis. It measures the distance between a given function $f \in \mathcal{B}_n$ and the set of all affine functions (represented as either $x \cdot \omega, \omega \in \mathbb{F}_2^n$, or $Tr(x\omega), \omega \in \mathbb{F}_{2^n}$) using the *Walsh-Hadamard transform*, which is defined as

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

for vector spaces and defined as

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

for finite fields. The *nonlinearity* of the function f is then defined as $N(f) = 2^{n-1} - \frac{1}{2} \max_{\omega \in \mathbb{F}_2^n} |W_f(\omega)|$. Nonlinearity is an affine invariant. The multiset $[W_f(\omega) | \omega \in \mathbb{F}_2^n]$ is called the *Walsh-Hadamard spectrum*. Maximum possible amplitude of a Walsh transform is $\pm 2^{\frac{n}{2}}$ and the maximum possible nonlinearity is therefore $2^{n-1} - 2^{\frac{n}{2}}$. The functions that reach it are called *bent functions*. That is, a function f is bent if $W_f(\omega) \in \{-2^{n/2}, 2^{n/2}\}$, for all $\omega \in \mathbb{F}_2^n$.

2.2 Bent functions

The term "bent function" was introduced by Rothaus [77] in 1960s' research that was officially published in 1976. These extremal combinatorial objects have several areas of application, such as coding theory, maximum length sequences, cryptography, the theory of difference sets, to name a few. Some of the most basic properties of bent functions, as already proven by Rothaus, are that they exist only for even n, they are unbalanced (either the number of zeroes or the number of ones must be equal to $2^{n-1}\left(\pm \frac{1}{2^{\frac{n}{2}}} + 1\right)$), and their algebraic degree is at most $\frac{n}{2}$, except when $\frac{n}{2} = 1$.

Every bent function has a corresponding dual function. The *dual function* f^* of a bent function f is defined in such a way that

$$W(\alpha)_f 2^{-\frac{n}{2}} = (-1)^{f^*(\alpha)}.$$

The dual is always a bent function and $(f^*)^* = f$. There also exist *self-dual* functions f for which $f = f^*$.

There exist many equivalent definitions of bent functions, connecting bent functions to other areas of mathematics such as combinatorics. Below we present some of them:

- The function f is bent.
- The nonlinearity of the functions f is $N(f) = 2^{n-1} - 2^{\frac{n}{2}}$.
- Let $\alpha \in \mathbb{F}_2^n$ be an arbitrary non-zero element. Then the derivative $f(x) \oplus f(x + \alpha)$ is balanced.
- The function $f(x) \oplus f(x) \cdot \alpha$ is bent for all $\alpha \in \mathbb{F}_2^n$.
- The matrix $|(-1)^{f(x+y)}|_{x,y \in \mathbb{F}_2^n}$ is a Hadamard matrix.

- Let S be the support of the function f. Then S is a Hadamard difference set in $\mathbb{F}_2^n$ with parameters $(2^n, 2^{n-1} \pm 2^{\frac{n}{2}} - 1, 2^{n-1} \pm 2^{\frac{n}{2}-1})$.

A $(\pm 1)_{n\times n}$ matrix is a *Hadamard matrix* if all its rows and columns and mutually orthogonal. Let G be a group with g elements and $H \leq G$ be a subgroup with h elements. If the set of differences $\{h_i - h_j | h_i, h_j \in K\}$ contains every non-zero element of G exactly t-times, then H is a (g,k,t)-*difference set* of G of order $k-t$. If $g = 4(h-t)$, it is a *Hadamard difference set.*

Bent functions are also connected to graph theory. We define a *graph* $\Gamma = (V, E)$, where V is a set of *vertices*, and $E \subseteq V \times V$ is a set of *edges*. If two vertices are connected, they are called *neighbours*. A graph is r-regular if every vertex v has exactly r neighbours. A graph is (v, r, λ, μ)-*strongly regular* if it has v vertices, is r-regular and if the following holds:

- Every pair of adjacent vertices $u, u' \in V$ has exactly λ common neighbours.
- Every pair of non-adjacent vertices $u, u' \in V$ has exactly μ common neighbours.

We define the graph Γ_f of a function $f \in \mathcal{B}_n$ as a graph with $V = \mathbb{F}_2^n$ and two vertices $v, u \in V$ are connected if and only if $f(u+v) \neq 0$. The functions f is bent if and only if its ocrresponsding graph Γ_f is strongly regular with parameters

$$(2^n, 2^{n-1} - 2^{\frac{n}{2}-1}, 2^{n-2} - 2^{\frac{n}{2}-1}, 2^{n-2} - 2^{\frac{n}{2}-1}) \quad \text{if } |supp(f)| = 2^{n-1} - 2^{\frac{n}{2}-1},$$
$$(2^n, 2^{n-1} + 2^{\frac{n}{2}-1}, 2^{n-2} + 2^{\frac{n}{2}-1}, 2^{n-2} + 2^{\frac{n}{2}-1}) \quad \text{if } |supp(f)| = 2^{n-1} + 2^{\frac{n}{2}-1}.$$

2.2.1 Classes of bent functions

Understanding the behaviour and mechanics of bent functions is a difficult task and for $n > 9$ there is no classification of bent functions under the action of general affine group on which to rely. The solution is to study constructions of bent functions. Some of these constructions rely on already known bent functions as building blocks to create new ones. These are called *secondary constructions*. *Primary constructions*, on the other hand, are direct and they are far fewer.

Definition 2.2.1 *A class of bent functions $\{f\} \in \mathcal{B}_n$ is* complete *if it is globally invariant under the action of the general affine group (the group of all invertible matrices of size $n \times n$ over $\mathbb{F}_2$ extending by a shift through $b \in \mathbb{F}_2^n$ so that $x \mapsto Ax \oplus b$) and under the addition of affine functions. The* completed class *is the smallest possible class that includes the original one.*

The first, and one of the most important, primary constructions was described in 1973, [65]. Dillon mentions in [36] that Maiorana and McFarland each discovered this same constructions independently, so it is today named the Maiorana-McFarland construction. Functions of the form

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

where $x, y \in \mathbb{F}_2^{\frac{n}{2}}$, π is a permutation, and g is an arbitrary Boolean function on $\frac{n}{2}$ variables, belong to the Maiorana-McFarland $\mathcal{M}$ class. Alternatively, the class can be described in terms of finite fields:

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

where $x, y \in \mathbb{F}_{2^{\frac{n}{2}}}$, and Tr is the absolute trace. Often, the completed $\mathcal{M}$ class, $\mathcal{M}^{\#}$, is considered.

This is one of the few classes where the explicit construction of the duals is known. For $f \in \mathcal{M}$ we have $f(x, y)^* = y \cdot \pi^{-1}(x) \oplus g(\pi^{-1}(x))$.

A useful indicator for the purpose of establishing whether a given bent function belongs to the completed Maiorana-McFarland class $\mathcal{M}^{\#}$ is given below.

Lemma 2.2.2 *[35, p. 102] An m-variable bent function f, $m = 2n$, belongs to $\mathcal{M}^{\#}$ if and only if there exists an n-dimensional linear subspace V of $\mathbb{F}_2^m$ such that the second order derivatives*

$$D_\alpha D_\beta f(x) = f(x) \oplus f(x \oplus \alpha) \oplus f(x \oplus \beta) \oplus f(x \oplus \alpha \oplus \beta)$$

vanish for any $\alpha, \beta \in V$.

The second primary construction, partial spread $\mathcal{PS}$, was introduced by Dillon [34] in his PhD thesis and the properties of this class have been studied in many recent works. This class is divided into two subclasses called $\mathcal{P}S^-$ and $\mathcal{P}S^+$ class depending on the size of the support. Any function $f \in \mathcal{B}_{2k}$ in the $\mathcal{P}S^-$ class is obtained by defining its support as a collection of 2^{k-1} disjoint k-dimensional subspaces of $\mathbb{F}_2^{2k}$ with the all zero vector discarded, where disjoint means that any pair of these subspaces intersects only in 0_{2k}. A function in the $\mathcal{P}S^+$ class is constructed by selecting $2^{k-1} + 1$ disjoint k-dimensional subspaces of $\mathbb{F}_2^{2k}$ (with the 0_{2k} vector included).

There are some fundamental differences between the two subclasses. Whereas the degree of any function $f \in \mathcal{B}_{2k}$ in $\mathcal{P}S^-$ is always equal to k, this is not the case for functions in $\mathcal{P}S^+$ whose degree may be less than k, see e.g. [34, 88]. The algebraic representation of the bent functions in the $\mathcal{P}S$ class appears to be hard. Dillon [34] exhibits one explicit representation of a subclass of $\mathcal{P}S^-$, denoted by $\mathcal{P}S_{ap}$, defined as follows:

$$\begin{aligned} f &: \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2 \\ f(x, y) &= g(xy^{2^k-2}), \ \ x, y \in \mathbb{F}_{2^k}, \end{aligned} \tag{2.2}$$

where $g \in \mathcal{B}_k$ is any balanced Boolean function such that $g(0) = 0$. If we allow that $g(0) = 1$ and furthermore that $f(x, y) = 1$ for $y = 0$, then the $\mathcal{PS}_{ap}$ class will have the cardinality $\binom{2^k+1}{2^{k-1}}$.

In 1994 Dobbertin presented the last of what is referred to as the primary constructions. It is called the $\mathcal{N}$ class, containing functions described as $f(x, \phi(y)) = g\left(\frac{x+\psi(y)}{y}\right)$, where $x, y \in \mathbb{F}_{2^{\frac{n}{2}}}$, g is a balanced Boolean function on $\mathbb{F}_2^{\frac{n}{2}}$, and ϕ, ψ are two mappings from $\mathbb{F}_{2^{\frac{n}{2}}}$ to itself such that, if T denotes an affine subspace of $\mathbb{F}_{2^{\frac{n}{2}}}$

spanned by the support of the Walsh transform of g, then, for any $a \in \mathbb{F}_{2^{\frac{n}{2}}}$, the functions ϕ, ψ are affine on aT. The mapping ϕ must also be one to one. Similarly as in the case of $\mathcal{PS}$ functions, finding an explicit form is in most cases a difficult task. The $\mathcal{N}$ class includes both $\mathcal{M}$ and $\mathcal{PS}$ classes.

In general, secondary constructions are not direct methods and they use some known bent functions to construct new ones. In the past few years these constructions have received a lot of attention [15, 20, 67, 95, 93]. A notable example of what are usually considered secondary constructions are $\mathcal{C}$ and $\mathcal{D}$ classes by Carlet [14], derived from the Maiorana-McFarland class in 1993 by substituting the arbitrary Boolean function depending on the variable y, with suitable indicator functions depending on variable x or both y and x. Functions from $\mathcal{C}$ class are of the form $f(x, y) = x \cdot \pi(y) \oplus 1_L(x)$, where L is a linear subspace of $\mathbb{F}_2^{\frac{n}{2}}$ such that $\pi^{-1}(a + L^{\perp})$ is a flat for any $a \in \mathbb{F}_2^{\frac{n}{2}}$. The permutation ϕ and the subspace L are then said to satisfy property (C), for short (ϕ, L) *has property* (C). Functions from $\mathcal{D}$ class are of the form $f(x, y) = x \cdot \pi(y) \oplus 1_{E_1}(x)1_{E_2}(y)$, where E_1, E_2 are linear subspaces of $\mathbb{F}_2^{\frac{n}{2}}$ such that $\pi(E_2) = E_1^{\perp}$.

2.2.2 Vectorial bent functions

A function F mapping from $\mathbb{F}_2^n$ or $\mathbb{F}_{2^n}$ to $\mathbb{F}_2^m$ or $\mathbb{F}_{2^m}$ is a *vectorial Boolean function* on n variables. For a fixed F we can write $F(x) = (f_1(x), f_2(x). \cdots, f_m(x))$, where f_i are Boolean functions called coordinate functions of F. We can talk about the Walsh-Hadamard transform and nonlinearity of vectorial Boolean functions in a similar way as about the Walsh transform and nonlinearity of Boolean functions.

The *Walsh-Hadamard transform* of vectorial Boolean functions is defined as

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

for vector spaces and defined as

$$W_F(\gamma, \omega) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(F(x)\gamma) \oplus Tr(x\omega)}, \gamma \in \mathbb{F}_{2^m}^*, \omega \in \mathbb{F}_{2^n},$$

for finite fields. By adding the parameter γ the Walsh transform decomposes the vectorial function F into linear combinations of its component functions $F(x) \cdot \gamma$ or $Tr(F(x)\gamma)$, which are Boolean functions. If the Walsh spectra of every linear combination of its component functions is $\{\pm 2^{\frac{n}{2}}\}$, that is, if every linear combination of its component functions is a bent functions, then F is a *vectorial bent function*. Finding a vectorial bent functions therefore corresponds to finding an m-dimensional vector space of functions in n variables whose non-zero elements are all bent.

An alternative definition of vectorial bentness is, similarly as before, that a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is bent if and only if all its derivatives $D_aF(x) = F(x) + F(x + a)$ are balanced, where balanced means that the derivatives take every value in $\mathbb{F}_2^m$ exactly 2^{n-m} times. Another similar property is that a function F can be bent only if n is even and $m \leq \frac{n}{2}$.

2.3 Other classes of highly nonlinear (vectorial) Boolean functions

One of the problems we face when searching for cryptographically strong Boolean function is that the five desirable properties we described before cannot all be optimized at the same time. We have, for example, already seen that a bent functions $f \in \mathcal{B}_n$ cannot exceed the algebraic degree $\frac{n}{2}$ and cannot be balanced. This is one of the reasons why not only bent functions, but other classes of highly nonlienar Boolean functions are cryptographically interesting as well.

For odd n the functions with the maximum nonlinearity are those with the Walsh spectra $\{0, \pm 2^{\frac{n+1}{2}}\}$. They are known as *semi-bent functions*. A functions with the Walsh spectra $\{0, \pm 2^k\}$, where $\frac{n}{2} \geq k$, is called a *k-plateaued function* and k is its *amplitude*. *Partially-bent functions* are all functions of the form

$$f(x,y) = g(x) + h(y), x \in \mathbb{F}_2^r, y \in \mathbb{F}_2^{n-r},$$

where g is bent and h is affine. The class of partially-bent function includes, but is not limited to, all bent and semi-bent functions. Every partially-bent function is plateaued, but there exist plateaued functions which are not partially-bent.

When for any given nonzero $\alpha \in \mathbb{F}_2^n$ the set $\{f(x) + f(x+\alpha) | x \in \mathbb{F}_2^n\}$ is of cardinality 2^{n-1}, the function f is *almost perfect nonlinear* or *APN*.

There also exist some interesting classes of highly nonlinear vectorial Boolean functions. For odd n the function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is called *almost bent* if its Walsh spectra is $\{0, \pm 2^{\frac{n-1}{2}}\}$. The name implies that these functions are not quite optimal, though in this case that notion is misleading. Notice that, unlike the bent functions in case when n is even, almost bent functions are not limited with mapping to $\mathbb{F}_2^{\frac{n}{2}}$ but can freely map to the whole vector space $\mathbb{F}_2^n$ (or finite field $\mathbb{F}_{2^n}$). There still exists a bound on their algebraic degree, though, and it is always less or equal to $\frac{n+1}{2}$.

A function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is *almost perfect nonlinear* if for every $a \in \mathbb{F}_2^{n*}, b \in \mathbb{F}_2^n$ the equation $F(x) + F(x+a) = b$ has either 0 or 2 solutions. Notice that this is a direct generalisation of almost perfect nonlinear Boolean functions. Every almost bent function is also almost perfect nonlinear. The reverse is not true. Even more, any vectorial function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is almost bent if and only if F is almost perfect nonlinear and the functions $\gamma \cdot F(x), \gamma \neq 0$, are plateaued with the same amplitude. If n is odd, the condition “with the same amplitude” is not necessary.

2.4 Permutations and translators

Let $\mathbb{F}_{p^n}[x]$ denote the *polynomial ring* with coefficients from the finite field $\mathbb{F}_{p^n}$, where p is a prime. A polynomial $F \in \mathbb{F}_{p^n}[x]$ is said to be a *permutation* if its associated mapping $x \mapsto F(x)$ over $\mathbb{F}_{p^n}$ is bijective.

Here we present some properties that are used in Chapter 4. The definition of a linear translator is also provided.

Lemma 2.4.1 *Let $n = 2k$ and $L : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, $L(x) = ax + bx^{p^k}$, where $a, b \in \mathbb{F}_{p^n}^*$. Let $\mathcal{G}$ be the subgroup of $\mathbb{F}_{p^n}^*$ of order $p^k + 1$. Then we have:*

(i) *L is a permutation if and only if $ab^{-1} \notin \mathcal{G}$;*

(ii) *L is an involution if and only if $T_k^n(a) = 0$ and $b^{p^k+1} = 1 - a^2$.*

Proof. Since $L(x) = x(a + bx^{p^k-1})$, $ab^{-1} \notin \mathcal{G}$ means that the kernel of L is $\{0\}$. Now we have

$$L \circ L(x) = x(a^2 + b^{p^k+1}) + x^{p^k} b(a + a^{p^k}).$$

Thus L is an involution if and only if $a + a^{p^k} = 0$ and $a^2 + b^{p^k+1} = 1$. When p is odd, note that $a + a^{p^k} = 0$ implies $a^2 \in \mathbb{F}_{p^k}^*$. The case $p = 2$ is an instance of [26, Proposition 5]. □

A functions is said to be $\mathbb{F}_{p^k}$*-linear function* on $\mathbb{F}_{p^n}$ $(n = rk)$ if it is of the type

$$L : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n},\ L(x) = \sum_{i=0}^{r-1} \lambda_i x^{p^{ki}}\ ,\ \lambda_i \in \mathbb{F}_{p^n}.$$

Definition 2.4.2 *Let $n = rk$, $1 \leq k \leq n$. Let f be a function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^k}$, $\gamma \in \mathbb{F}_{p^n}^*$ and b fixed in $\mathbb{F}_{p^k}$. Then γ is a b-linear translator for f if*

$$f(x + u\gamma) - f(x) = ub, \quad \text{for all } x \in \mathbb{F}_{p^n} \text{ and for all } u \in \mathbb{F}_{p^k}.$$

In particular, when $k = 1$, γ is usually said to be a b-linear structure of the function f (where $b \in \mathbb{F}_p$), that is

$$f(x + \gamma) - f(x) = b \quad \text{for all } x \in \mathbb{F}_{p^n}.$$

The following general theorem about the existance of lienar translators is given in [49] without proof since the proof is an equivalent of those given in [24] and [27], when $k = 1$ and $k = n$, respectively.

Theorem 2.4.3 *A function f from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^k}$, $n = rk$, has a linear translator if and only if there is a non-bijective $\mathbb{F}_{p^k}$-linear function L on $\mathbb{F}_{p^n}$ such that*

$$f(x) = T_k^n\left(H \circ L(x) + \beta x\right)$$

for some $H : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ and $\beta \in \mathbb{F}_{p^n}$. In this case the kernel of L is contained in the subspace of linear translators (including 0 by convention).

Chapter 3

Bent functions outside the completed Maiorana-McFarland class

This chapter is composed out of two subsections, each dealing with a specific way of constructing bent functions lying outside the completed Maiorana-McFarland class. The first one considers the general form of Rothaus or, to be more precise, one of its specific forms in order to easier consider the bent properties of thus constructed functions. The second subsection focuses on bent functions within the $\mathcal{C}$ and $\mathcal{D}$ classes and considers sufficient conditions for them to lie outside the completed Maiorana-McFarland class. Some of the following proofs are very long and the reader can find them in the Appendix.

3.1 Constructing bent functions outside the Maiorana-McFarland class using a general form of Rothaus

In the past few years the secondary constructions of bent functions have received a lot of attention [15, 20, 67, 95, 93], and apart from that many attempts have been made to specify explicitly the bent conditions using the trace representation, cf. [7, 9, 22, 40, 53, 54, 57, 61, 66, 68]. A nice and exhaustive survey on bent functions can be found in [18].

In particular, the idea of using Rothaus construction to construct bent functions in $n+2$ variables by employing three bent functions in n variables whose sum is also a bent function was examined in [20]. More precisely, these triples of bent functions whose sum is also a bent function could be easily found within the $\mathcal{M}$ class [20] and the resulting function does not necessarily belong to the same class to which the initial functions belong to. In a similar manner, based on the initial work of Carlet [16], Mesnager [67] investigated thoroughly the possibilities of constructing new bent functions on the same variable space by using three suitably chosen bent functions. We also briefly address the problem of selecting three bent functions whose sum is again bent within the $\mathcal{PS}$ class and give an exact estimate on the number of possibilities of specifying such triples of bent functions (only considering the Desarguesian spread though other complete spreads may be used as well).

The main objective of this chapter is to consider the Rothaus construction in a special setting. More precisely, instead of considering three bent functions whose sum is bent, we restrict our analysis to a somewhat simplified scenario when two of these three functions differ only on some suitably chosen $n/2$-dimensional subspace. This leads to a significant simplification of the algebraic form of the resulting function and also gives the possibility to easily establish a connection to the Dillon's $\mathcal{PS}$ class [34]. This means that the initial functions are easily specified within the $\mathcal{PS}$ class and it is demonstrated that affine non-equivalent functions can be easily identified within this particular subclass of Rothaus "class" of bent functions. Moreover, we show that under certain conditions, when the initial functions are taken from the class $\mathcal{D}$, the resulting bent functions provably do not belong to the completed Maiorana-McFarland class. However, similar conditions for generating bent functions outside the completed $\mathcal{M}$ class are not easily satisfied when the initial functions are derived from $\mathcal{C}$. A further simplification then, corresponding to the case of having only one initial bent function and deriving the other two from it, relates this method to $\mathcal{C}$ and $\mathcal{D}$ classes of bent functions. It is shown that one may construct bent functions in these classes on larger variable spaces iteratively, which is a somewhat expected feature though such a precise statement is not transparent in the literature.

Bent functions derived using this special case of Rothaus construction (thus relating the initial bent functions through the complement operation or addition of the indicator of an $n/2$-dimensional subspace) exhibit some interesting properties in terms of *normality*. The *(weak) normality* of bent functions is defined as the property of a function being (affine) constant on some $n/2$-dimensional affine subspace [37]. The main primary classes of bent functions, namely $\mathcal{M}$, $\mathcal{PS}^+$ and $\mathcal{N}$ [37], were shown to be normal bent functions [10]. This is also true for the class $\mathcal{C}$ derived from the $\mathcal{M}$ class [10, Lemma 13]. Due to this, there are only a few examples known in the literature [55, 37, 17] of non-normal bent functions and some of these are also not weakly normal [55].

We provide several examples of non-normal bent functions in 10 variables (all tested functions, derived either from $\mathcal{C}$ or $\mathcal{D}$ class, appear to be non-normal) and in particular one example regards a bent function which is provably outside the completed $\mathcal{M}$ class. We notice that a weakly normal bent function (which is non-normal) can be turned into a normal bent function through addition of a suitable linear function but the converse is not always true. This is because, in certain cases, adding any linear function to a normal bent function it still might be the case that the resulting function remains normal (thus constant on some $n/2$-dimensional flat). Thus, it is of importance to investigate whether our non-normal bent functions are also not weakly normal. More precisely, there is a possibility that non-normality only disguises weak normality in which case such a non-normal function becomes normal after addition of an affine function. Our efforts to identify non-normal bent functions which are also not weakly normal have however proved unsuccessful. This also implies that we are unable to give more precise statements whether some of non-normal bent functions (which are weakly normal) identified here are actually outside the completed versions of known primary classes.

3.1.1 A special case of Rothaus' construction

Throughout this section we denote $(0, 0, \ldots, 0) \in \mathbb{F}_2^n$ by 0_n.

In the mid sixties (though published ten years later) Rothaus [77] proposed the following construction method of obtaining new bent functions in $n + 2$ variables starting with three suitable bent functions in n variables.

Rothaus' construction [77]: Let $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$ and $x_{n+1}, x_{n+2} \in \mathbb{F}_2$. Let $A(x)$, $B(x)$, $C(x)$ be bent functions on $\mathbb{F}_2^n$ such that $A(x) \oplus B(x) \oplus C(x)$ is bent as well, then the function defined for every element $(x, x_{n+1}, x_{n+2}) \in \mathbb{F}_2^{n+2}$ by:

$$\begin{aligned} & f(x, x_{n+1}, x_{n+2}) \\ = & \; A(x)B(x) \oplus A(x)C(x) \oplus B(x)C(x) \oplus x_{n+1}x_{n+2} \\ \oplus & \; [A(x) \oplus B(x)]x_{n+1} \oplus [A(x) \oplus C(x)]x_{n+2} \end{aligned} \tag{3.1}$$

is a bent function in $n + 2$ variables.

In what follows we employ the construction of Rothaus in a particular way. The following lemma gives more precision to a known result on the minimum distance of bent functions.

Lemma 3.1.1 *Let f_0, f_1 be two bent functions in n variables. Let $\Delta \subseteq \mathbb{F}_2^n$ be a set and $1_\Delta(x)$ be the function that equals 1 if x is in Δ, otherwise it equals 0. If either $\Delta \subseteq (supp(f_0) \cap supp(f_1))$ or $\Delta \subseteq (supp(1 \oplus f_0) \cap supp(1 \oplus f_1))$ and $f_0 \oplus 1_\Delta, f_1 \oplus 1_\Delta$ are also bent, then we have $|\Delta| = 2^{\frac{n}{2}}$.*

Proof. If $\Delta \subseteq supp(f_0) \cap supp(f_1)$, then $|supp(f_i)| > |supp(f_i \oplus 1_\Delta)|$, for $i = 0, 1$. Since $f_0 \oplus 1_\Delta, f_1 \oplus 1_\Delta$ are also bent, we have $|supp(f_i)| = 2^{n-1} + 2^{\frac{n}{2}-1}$ and $|supp(f_i \oplus 1_\Delta)| = 2^{n-1} - 2^{\frac{n}{2}-1}$. It implies that $|\Delta| = 2^{\frac{n}{2}}$.

Similarly, if $\Delta \subseteq supp(1 \oplus f_0) \cap supp(1 \oplus f_1)$, then $|supp(f_i)| < |supp(f_i \oplus 1_\Delta)|$, for $i = 0, 1$. Since $f_0 \oplus 1_\Delta, f_1 \oplus 1_\Delta$ are also bent, we have $|supp(f_i)| = 2^{n-1} - 2^{\frac{n}{2}-1}$ and $|supp(f_i \oplus 1_\Delta)| = 2^{n-1} + 2^{\frac{n}{2}-1}$. Thus, $|\Delta| = 2^{\frac{n}{2}}$. □

Remark 3.1.2 *If $\Delta = \Delta_1 \cup \Delta_2$ such that $\Delta_1 \subseteq supp(f_0) \cap supp(f_1)$ and $\Delta_2 \subseteq supp(1 \oplus f_0) \cap supp(1 \oplus f_1)$, thus $f_0(x) = f_1(x)$ for $x \in \Delta$, then either $|\Delta_1| = |\Delta_2|$ or $|\Delta_1| = |\Delta_2| \pm 2^{\frac{n}{2}}$ depending on the weight of f_i. This case is more general since the cardinality of $|\Delta_1|$ and $|\Delta_2|$ can be "arbitrary" and it allows us to use bent functions f_0 and f_1 from the classes $\mathcal{C}$ and $\mathcal{D}$, see also Section 3.1.2.1.*

Theorem 3.1.1 *Let $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$ and $x_{n+1}, x_{n+2} \in \mathbb{F}_2$. Let f_0, f_1 be two Boolean functions in n variables such that $f_0(x) = f_1(x)$ for $x \in \Delta$, where $\Delta \subseteq \mathbb{F}_2^n$. Then, the function f defined as*

$$\begin{aligned} & f(x, x_{n+1}, x_{n+2}) \\ = & \quad (x_{n+1} \oplus x_{n+2} \oplus 1)f_0(x) \oplus (x_{n+1} \oplus x_{n+2})f_1(x) \\ \oplus & \quad (x_{n+2} \oplus 1)1_\Delta(x) \oplus x_{n+1}x_{n+2} \oplus x_{n+1}, \end{aligned} \tag{3.2}$$

is bent if and only if all the functions f_0, f_1, $f_0 \oplus 1_\Delta$, $f_1 \oplus 1_\Delta$ are also bent. Moreover, if f is bent then we necessarily have $|\Delta| = 2^{\frac{n}{2}}$.

Proof. The sufficiency can be easily proved by setting $A(x) = f_0(x)$, $B(x) = f_1(x) \oplus 1$ and $C(x) = f_1(x) \oplus 1_\Delta(x)$ in (3.1) and verifying that we obtain (3.2). Since A, B, C, and their sum are bent functions, it suffices that f_0, f_1, $f_0 \oplus 1_\Delta$, $f_1 \oplus 1_\Delta$ are all bent, which is true by assumption, thus f is bent as well.

On the other hand, both necessary and sufficient conditions can be proved using the Walsh transform of f at point $(\alpha, \alpha_{n+1}, \alpha_{n+2}) \in \mathbb{F}_2^{n+2}$ which equals to :

$$\begin{aligned} W_f(\alpha, \alpha_{n+1}, \alpha_{n+2}) =& W_{f_0\oplus 1_\Delta}(\alpha) + (-1)^{1+\alpha_{n+1}} W_{f_1\oplus 1_\Delta}(\alpha) \\ &+ (-1)^{\alpha_{n+2}} W_{f_1}(\alpha) + (-1)^{\alpha_{n+1}+\alpha_{n+2}} W_{f_0}(\alpha), \end{aligned}$$

which is easily obtained by considering the restrictions of f with respect to (x_{n+1}, x_{n+2}), thus splitting $\sum_{(x,x_{n+1},x_{n+2})\in\mathbb{F}_2^{n+2}} (-1)^{f(x,x_{n+1},x_{n+2})\oplus(x,x_{n+1},x_{n+2})\cdot(\alpha,\alpha_{n+1},\alpha_{n+2})}$ into four sums.

We now derive the values of $W_f(\alpha, \alpha_{n+1}, \alpha_{n+2})$ for different $(\alpha_{n+1}, \alpha_{n+2}) \in \mathbb{F}_2^2$, assuming $f_0(x) = f_1(x)$ for $x \in \Delta$ which is later shown to be necessary. For $(\alpha_{n+1}, \alpha_{n+2}) = (0, 0)$, we have

$$\begin{aligned} & W_f(\alpha, 0, 0) \\ = \;& W_{f_0\oplus 1_\Delta}(\alpha) + (-1) W_{f_1\oplus 1_\Delta}(\alpha) + \; W_{f_1}(\alpha) + W_{f_0}(\alpha) \\ \\ = \;& \sum_{x\in\mathbb{F}_2^n\setminus\Delta} (-1)^{f_0(x)\oplus x\cdot\alpha} + \sum_{x\in\Delta} (-1)^{f_0(x)\oplus 1\oplus x\cdot\alpha} + W_{f_0}(\alpha) \\ + \;& (-1) \sum_{x\in\mathbb{F}_2^n\setminus\Delta} (-1)^{f_1(x)\oplus x\cdot\alpha} + \sum_{x\in\Delta} (-1)^{f_1(x)\oplus x\cdot\alpha} + W_{f_1}(\alpha) \\ = \;& 2 \sum_{x\in\mathbb{F}_2^n\setminus\Delta} (-1)^{f_0(x)\oplus x\cdot\alpha} + 2 \sum_{x\in\Delta} (-1)^{f_0(x)\oplus x\cdot\alpha}. \end{aligned}$$

Thus, $W_f(\alpha, 0, 0) = 2 \sum_{x\in\mathbb{F}_2^n} (-1)^{f_0(x)\oplus x\cdot\alpha}$ and similarly for the remaining values of $(\alpha_{n+1}, \alpha_{n+2})$:

$$\begin{aligned} & W_f(\alpha, \alpha_{n+1}, \alpha_{n+2}) \\ = & \begin{cases} 2 \sum_{x\in\mathbb{F}_2^n} (-1)^{f_1(x)\oplus 1_\Delta(x)\oplus x\cdot\alpha} & \text{if } (\alpha_{n+1}, \alpha_{n+2}) = (1, 0), \\ -2 \sum_{x\in\mathbb{F}_2^n} (-1)^{f_1(x)\oplus x\cdot\alpha} & \text{if } (\alpha_{n+1}, \alpha_{n+2}) = (0, 1), \\ 2 \sum_{x\in\mathbb{F}_2^n} (-1)^{f_0(x)\oplus 1_\Delta(x)\oplus x\cdot\alpha} & \text{if } (\alpha_{n+1}, \alpha_{n+2}) = (1, 1). \end{cases} \end{aligned}$$

Combining the above items, f is bent if and only if f_0, f_1, $f_0 \oplus 1_\Delta$ and $f_1 \oplus 1_\Delta$ are bent. The necessity that $|\Delta| = 2^{\frac{n}{2}}$ follows from the fact that both f_0 and $f_0 + 1_\Delta$ are bent. □

In Theorem 3.1.1 the given conditions are both necessary and sufficient for the subclass of the Rothaus class considered here. This raises an important question whether the conditions that the initial functions and their sum are bent are in general also necessary in the Rothaus construction.

Remark 3.1.3 *Theorem 3.1.1 can be extended to include three different functions f_0, f_1, f_2 to which some suitable characteristic functions are added. Nevertheless, the addition of the indicator Δ along with the condition that $f_0(x) = f_1(x) = f_2(x)$ for $x \in \Delta$ gives harder conditions for the choice of f_0, f_1, f_2 and the proof that f defined similarly as in (3.2) belongs to the completed Maiorana-McFarland class ($\mathcal{M}^{\#}$) would be much more complicated, see also Lemma 3.1.6. Furthermore, by setting $f_0 = f_1$ for f defined as in Theorem 3.1.1 we obtain*

$$f(x, x_{n+1}, x_{n+2}) = f_0(x) \oplus x_{n+1}x_{n+2} \oplus x_{n+1} \oplus 1_{\Delta'}, \tag{3.3}$$

which is also a bent function in $n+2$ variables, where $\Delta' = \Delta \times \{(x_{n+1}, 0) | x_{n+1} \in \mathbb{F}_2\} \in \mathbb{F}_2^n \times \mathbb{F}_2^2$.

The existence of functions satisfying the conditions in Theorem 3.1.1 is easily confirmed by considering the $\mathcal{PS}^-$ class and defining Δ to be an $\frac{n}{2}$-dimensional linear subspace. Indeed, if both f_0 and f_1 are bent functions that belong to $\mathcal{PS}^-$ then adding the characteristic function $\Delta = S$, where S is an $\frac{n}{2}$-dimensional subspace and $S \not\subset supp(f_i)$, for $i = 0, 1$, implies that the functions $f_0(x) \oplus 1_\Delta(x)$ and $f_1(x) \oplus 1_\Delta(x)$ belong to $\mathcal{PS}^+$. Nevertheless, it is not clear whether the function f belongs to the $\mathcal{PS} = \mathcal{PS}^- \cup \mathcal{PS}^+$ class.

To show the affine non-equivalence of two Boolean functions (unless it is obvious that they belong to the same class) is in general a hard problem. In what follows, we show that for suitably chosen initial bent functions f_0, f_1 and f'_0, f'_1 in Theorem 3.1.1 the functions f and f' defined by means of (3.2) (using f_0, f_1 and f'_0, f'_1, respectively) are not affine equivalent. To achieve this we consider two different functions $f_0, f_1 \in \mathcal{PS}^-$, whose sum $f_0 \oplus f_1 \in \mathcal{PS}^-$, and define f as in (3.2) using these two functions. The indicator Δ is chosen to be an $n/2$-dimensional subspace such that both $f_0 \oplus 1_\Delta$ and $f_1 \oplus 1_\Delta$ are in $\mathcal{PS}^+$. On the other hand, one can easily select $f'_0, f'_1 \in \mathcal{PS}^-$ such that $f'_0 = f'_1 = f_0$ and additionally if $f'_0 \oplus 1_\Delta$ is in $\mathcal{PS}^+$ so is $f'_1 \oplus 1_\Delta$, for the same indicator Δ. At the same time, we obviously have $f_0 \neq f_1$. Using (3.2) we get,

$$\begin{aligned} &f(x, x_{n+1}, x_{n+2}) = g(x, x_{n+1}, x_{n+2}) \\ &\oplus (x_{n+1} \oplus x_{n+2})(f_0(x) \oplus f_1(x)) \oplus x_{n+2}1_\Delta(x), \end{aligned} \tag{3.4}$$

where $g(x, x_{n+1}, x_{n+2}) = 1_\Delta(x) \oplus f_0(x) \oplus x_{n+1}x_{n+2} \oplus x_{n+1}$, and similarly we have

$$f'(x, x_{n+1}, x_{n+2}) \quad = g(x, x_{n+1}, x_{n+2}) \oplus x_{n+2}1_\Delta(x). \tag{3.5}$$

We notice that, due to the above assumptions, $g(x)$ is the same regardless of whether we use f_0, f_1 or f'_0, f'_1, and furthermore $\deg(g) \leq n/2$.

Theorem 3.1.2 *Let n be an even integer and let f and f' be defined as (3.4) and (3.5), respectively. Then there do not exist an invertible binary matrix $A = (a_{ij})$ of size $(n+2) \times (n+2)$ and a binary vector $\mathbf{b} = (b_1, b_2, \ldots, b_{n+2}) \in \mathbb{F}_2^{n+2}$ such that*

$$f'(A(x, x_{n+1}, x_{n+2}) \oplus \mathbf{b}) = f(x, x_{n+1}, x_{n+2}), \tag{3.6}$$

and hence f and f' are affine non-equivalent.

The lengthy proofs of Theorem 3.1.2 is given in the Appendix.

Remark 3.1.4 *Theorem 3.1.2 essentially claims that f' does not belong to the completed class of f. Notice that the affine equivalence in Theorem 3.1.2 does not include addition of an affine function which is irrelevant in this context (the proof establishes the non-equivalence in terms of monomials of largest degree $n/2+1$).*

3.1.1.1 Showing non-belongingness to the completed Maiorana-McFarland class

In this section we propose sufficient conditions for the bent function f defined as in Theorem 3.1.1 not to belong to the completed Maiorana-McFarland class ($\mathcal{M}^{\#}$). In [14], Carlet introduced two new classes of bent functions derived from $\mathcal{M}$ bent functions, so-called $\mathcal{C}$ and $\mathcal{D}$, by adding to the functions in the $\mathcal{M}$ class the indicators of some vector subspaces.

The class $\mathcal{D}$, used in Theorem 3.1.3 below, consists of all the functions of the form

$$\phi(x^{(2)}) \cdot x^{(1)} \oplus 1_{E_1}(x^{(1)})1_{E_2}(x^{(2)}),$$

where ϕ is any permutation on $\mathbb{F}_2^{\frac{n}{2}}$, E_1 and E_2 are two linear subspaces of $\mathbb{F}_2^{\frac{n}{2}}$ such that $\phi(E_2) = E_1^{\perp}$, and $1_{E_1}(x^{(1)})$ (resp. $1_{E_2}(x^{(2)})$ is the characteristic function of E_1 (resp. E_2). Here, $E_1^{\perp}$ denotes the orthogonal subspace of E_1, and throughout this section we use $x = (x_1, \dots, x_n) = (x^{(1)}, x^{(2)}) \in \mathbb{F}_2^{\frac{n}{2}} \times \mathbb{F}_2^{\frac{n}{2}}$. In particular, an explicit subclass of $\mathcal{D}$, denoted by $\mathcal{D}_0$, contains all elements of the form $x^{(1)} \cdot \phi(x^{(2)}) + \delta_0(x^{(1)})$. The notation $\delta_0(x^{(1)})$ means the Dirac symbol, namely $\delta_0(x^{(1)}) = 1$ if $x^{(1)} = 0_{\frac{n}{2}}$, and 0 otherwise. This implies that the linear subspace $E_1 \times E_2$ corresponds to $\{0_{\frac{n}{2}}\} \times \mathbb{F}_2^{n/2}$.

To show that Theorem 3.1.1 can generate functions that do not belong to the completed Maiorana-McFarland class ($\mathcal{M}^{\#}$), we need to use Lemma 2.2.2 and some preparatory results.

Lemma 3.1.5 *Let $h \in \mathcal{B}_n$ be an arbitrary Boolean function such that $\deg(h) \geq 2$. If V is any subspace of $\mathbb{F}_2^n$ and $\dim(V) \geq n-1$, then there exists at least one vector $\alpha \in V$ such that*

$$D_\alpha h(x) = h(x) \oplus h(x \oplus \alpha) \neq \textit{ constant}.$$

Proof. From the definition of linear structures, if $D_\beta h(x) = \textit{constant}$ then $\beta \in \mathbb{F}_2^n$ is called a linear structure of h. We also know if $\deg(h) \geq 2$, then $|\{\beta \mid D_\beta h(x) = \textit{constant},\ \beta \in \mathbb{F}_2^n\}| \leq 2^{n-2}$. Hence, there exists at least one vector $\alpha \in V$ such that

$$D_\alpha h(x) = h(x) \oplus h(x \oplus \alpha) \neq \textit{ constant},$$

because $\dim(V) \geq n-1$ and $|V| \geq 2^{n-1} > 2^{n-2}$. □

For convenience, we denote $a = (a_1, a_2, a_3, a_4), b = (b_1, b_2, b_3, b_4) \in \mathbb{F}_2^{\frac{n}{2}} \times \mathbb{F}_2^{\frac{n}{2}} \times \mathbb{F}_2 \times \mathbb{F}_2$ and let the subspace of $\mathbb{F}_2^{n+2}$ given by $\{(x^{(1)}, 0_{\frac{n}{2}}, x_{n+1}, 0) \mid x^{(1)} \in \mathbb{F}_2^{\frac{n}{2}}, x_{n+1} \in \mathbb{F}_2\}$ be denoted by Λ.

Lemma 3.1.6 *Let $n > 4$ be an even integer and let $f_0(x) = \pi(x^{(2)}) \cdot x^{(1)}$, $f_1(x) = \phi(x^{(2)}) \cdot x^{(1)}$, where π and ϕ are two permutations on $\mathbb{F}_2^{\frac{n}{2}}$. Then, $f \in \mathcal{B}_{n+2}$ defined as*

$$\begin{aligned} & f(x, x_{n+1}, x_{n+2}) \\ = & \ (x_{n+1} \oplus x_{n+2} \oplus 1) f_0(x) \oplus (x_{n+1} \oplus x_{n+2}) f_1(x) \\ \oplus & \ (x_{n+2} \oplus 1) 1_{E_1}(x^{(1)}) 1_{E_2}(x^{(2)}) \oplus x_{n+1}x_{n+2} \oplus x_{n+1}, \end{aligned} \tag{3.7}$$

is bent, where E_1, E_2 are linear subspaces of $\mathbb{F}_2^{\frac{n}{2}}$ such that $\pi(E_2) = E_1^{\perp}$ (resp. $\phi(E_2) = E_1^{\perp}$). Assume now that π and ϕ satisfy:

1. *π (or ϕ) has no nonzero linear structure;*
2. *$\nu \cdot (\pi \oplus \phi) \neq$ constant for $\nu \in \mathbb{F}_2^{\frac{n}{2}} \setminus \{0_{\frac{n}{2}}\}$;*
3. $\max_{\nu \in \mathbb{F}_2^{\frac{n}{2}}} \deg(\nu \cdot (\pi \oplus \phi)) \geq 2,$
4. *$E_1 \subset \mathbb{F}_2^{\frac{n}{2}}$ and $\dim(E_1) \leq \frac{n}{2} - 2$ (that is, $\deg(1_{E_1}(x^{(1)})) \geq 2$).*

Let V denote an arbitrary $\frac{n+2}{2}$-dimensional subspace of $\mathbb{F}_2^{n+2}$. Furthermore, assume that one of the following is satisfied:

i) There exist $(a_1, 0_{\frac{n}{2}}, a_3, 0), (b_1, 0_{\frac{n}{2}}, b_3, 0) \in \Lambda \setminus \{0_{n+2}\}$ such that $a_3 = b_3 = 1$, or $a_3 = 0, b_3 = 1$, or $a_3 = 1, b_3 = 0$.

ii) There exist $a, b \in V$ such that $(a_2, a_4) \neq (b_2, b_4)$, $D_{a_2} D_{b_2} (\pi \oplus \varphi)(x^{(2)}) \neq 0$ and $a_4 = b_4 = 0$.

iii) There is $a = (a_1, 0_{\frac{n}{2}}, a_3, 0) \in V \cap \Lambda$, such that $(a_1, a_3) \neq 0_{\frac{n}{2}+1}$, and assume the existence of $b^{(1)} = (b_1^{(1)}, b_2^{(1)}, b_3^{(1)}, b_4^{(1)}) \in V$ such that $b_2^{(1)} \neq 0_{\frac{n}{2}}$ and $b_3^{(1)} = b_4^{(1)}$, and $b^{(2)} = (b_1^{(2)}, b_2^{(2)}, b_3^{(2)}, b_4^{(2)}) \in V$ such that $b_2^{(2)} \neq 0_{\frac{n}{2}}$ and $D_{b_2^{(2)}}(\pi \oplus \phi)(x^{(2)}) \neq$ constant.

iv) There exist $a = (a_1, 0_{\frac{n}{2}}, 0, 0) \in \Lambda, b = (b_1, 0_{\frac{n}{2}}, 1, 1) \in V$ such that $D_{a_1} 1_{E_1}(x^{(1)}) \neq 0$.

v) There exist $a = (a_1, 0_{\frac{n}{2}}, 0, 0) \in \Lambda, b = (b_1, 0_{\frac{n}{2}}, 0, 1) \in V$ such that $D_{a_1} 1_{E_1}(x^{(1)}) \neq$ constant.

vi) There exist $a = (a_1, 0_{\frac{n}{2}}, 0, 0) \in \Lambda$ and $b = (b_1, b_2, b_3, b_4) \in V$ such that $D_{a_1} D_{b_1} 1_{E_1}(x^{(1)}) \neq 0$.

Then, $D_a D_b f(x, x_{n+1}, x_{n+2})$ does not vanish for the above specified $a, b \in \mathbb{F}_2^{n+2}$.

It is sufficient to show that for an arbitrary $\frac{n+2}{2}$-dimensional subspace V of $\mathbb{F}_2^{n+2}$ one can always find two vectors a, b (viewed as a basis of a 2-dimensional subspace of V) such that $D_a D_b f(x, x_{n+1}, x_{n+2}) \neq 0$. The lengthy proofs of both Lemma 3.1.6 and Proposition 3.1.7 below are given in the Appendix.

Proposition 3.1.7 *Let f be defined as in Lemma 3.1.6. Then, for any $\frac{n+2}{2}$-dimensional subspace V of $\mathbb{F}_2^{n+2}$ one can find two vectors a, b which fall under one of the forms given by items $i) - vi)$ in Lemma 3.1.6.*

From Lemma 3.1.6 and Proposition 3.1.7 we easily get the following result which essentially embeds the characterization of bent functions in $\mathcal{D}$ through the specification of the indicator $1_\Delta(x) = 1_{E_1}(x^{(1)})1_{E_2}(x^{(2)})$ so that both $f_0 \oplus 1_\Delta$ and $f_1 \oplus 1_\Delta$ belong to $\mathcal{D}$.

Theorem 3.1.3 *Let $n > 4$ be an even integer and let $f_0(x) = \pi(x^{(2)}) \cdot x^{(1)}$, $f_1(x) = \phi(x^{(2)}) \cdot x^{(1)}$, where π and ϕ are two permutations on $\mathbb{F}_2^{\frac{n}{2}}$. Then, f defined as*

$$\begin{aligned} & f(x, x_{n+1}, x_{n+2}) \\ = \;& (x_{n+1} \oplus x_{n+2} \oplus 1)f_0(x) \oplus (x_{n+1} \oplus x_{n+2})f_1(x) \\ \oplus \;& (x_{n+2} \oplus 1)1_{E_1}(x^{(1)})1_{E_2}(x^{(2)}) \oplus x_{n+1}x_{n+2} \oplus x_{n+1}, \end{aligned} \tag{3.8}$$

is bent, where E_1, E_2 are linear subspaces of $\mathbb{F}_2^{\frac{n}{2}}$ such that $\pi(E_2) = E_1^\perp$ (resp. $\phi(E_2) = E_1^\perp$). Further, if π and ϕ satisfy:

1. *π (or ϕ) has no nonzero linear structure;*
2. *$\nu \cdot (\pi \oplus \phi) \neq$ constant for $\nu \in \mathbb{F}_2^{\frac{n}{2}} \setminus \{0_{\frac{n}{2}}\}$;*
3. *$\max_{\nu \in \mathbb{F}_2^{\frac{n}{2}}} \deg(\nu \cdot (\pi \oplus \phi)) \geq 2$,*
4. *$E_1 \subset \mathbb{F}_2^{\frac{n}{2}}$ and $\dim(E_1) \leq \frac{n}{2} - 2$ (that is, $\deg(1_{E_1}(x^{(1)})) \geq 2$),*

then f does not belong to $\mathcal{M}^\#$.

Example 3.1.1 *By means of Theorem 3.1.3, we were able to specify a 10-variable bent function f of algebraic degree 5, which does not belong to $\mathcal{M}^\#$. In addition, this function and its dual are non-normal and therefore $f \notin \mathcal{N} \cup \mathcal{PS}^+$. However, this function and its dual are weakly normal.*

Let $E_1 = E_1{}^\perp = \{(0000), (0011), (1100), (1111)\}$ and $E_2 = \{(0000), (0010), (1101), (1111)\}$. The permutations π and ϕ (using hexadecimal format) are defined as

$$\begin{aligned} &\{0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ A\ B\ C\ D\ E\ F\} \overset{\pi}{\mapsto} \\ &\{3\ 1\ F\ 6\ E\ A\ 9\ 5\ 2\ 8\ 4\ B\ D\ 0\ 7\ C\}, \\ &\{0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ A\ B\ C\ D\ E\ F\} \overset{\phi}{\mapsto} \\ &\{3\ 6\ F\ 1\ A\ 2\ 9\ E\ B\ 4\ 5\ D\ 7\ 0\ 8\ C\}. \end{aligned}$$

3.1.1.2 Other bent functions derived from $\mathcal{C}$ class and non-normality

In difference to class $\mathcal{D}$, when considering the class $\mathcal{C}$ of bent functions [14] which is also derived from the $\mathcal{M}$ class, the situation is somewhat different since the sufficient conditions of Theorem 3.1.3 turn out to be harder to satisfy.

The class $\mathcal{C}$ contains all the functions of the form

$$\phi(x^{(2)}) \cdot x^{(1)} \oplus 1_{\overline{\Delta}}(x^{(1)}),$$

where $\overline{\Delta}$ is a linear subspace of $\mathbb{F}_2^{\frac{n}{2}}$ and $\phi = (\phi_1, \dots, \phi_{\frac{n}{2}})$ is any permutation on $\mathbb{F}_2^{\frac{n}{2}}$ such that, for any element a of $\mathbb{F}_2^{\frac{n}{2}}$, the set $\phi(a \oplus \overline{\Delta}^{\perp})$ is a flat.

The same arguments, as used in Lemma 3.1.6 and Proposition 3.1.7 to show that f does not belong to $\mathcal{M}^{\#}$, apply now to the case when $1_{E_1}(x^{(1)})1_{E_2}(x^{(2)})$ is replaced by $1_{\overline{\Delta}}(x^{(1)})$, provided that a similar set of conditions is satisfied.

Corollary 3.1.8 *Let $n > 4$ be an even integer and denote $x = (x^{(1)}, x^{(2)}) = (x_1, \dots, x_n) \in \mathbb{F}_2^{\frac{n}{2}} \times \mathbb{F}_2^{\frac{n}{2}}$ and $x_{n+1}, x_{n+2} \in \mathbb{F}_2$. Let $f_0(x) = \pi(x^{(2)}) \cdot x^{(1)}$ and $f_1(x) = \phi(x^{(2)}) \cdot x^{(1)}$. Then, f defined by*

$$\begin{aligned} & f(x, x_{n+1}, x_{n+2}) \\ = \; & (x_{n+1} \oplus x_{n+2} \oplus 1) f_0(x) \oplus (x_{n+1} \oplus x_{n+2}) f_1(x) \\ & \oplus (x_{n+2} \oplus 1) 1_{\overline{\Delta}}(x^{(1)}) \oplus x_{n+1}x_{n+2} \oplus x_{n+1}, \end{aligned} \tag{3.9}$$

is bent, where $\overline{\Delta}$ is any linear subspace of $\mathbb{F}_2^{\frac{n}{2}}$, π and ϕ are two permutations on $\mathbb{F}_2^{\frac{n}{2}}$ such that, $\pi(\overline{\Delta}) = \phi(\overline{\Delta})$ and for any element $\alpha^{(2)}$ of $\mathbb{F}_2^{\frac{n}{2}}$, the set $\phi(\alpha^{(2)} \oplus \overline{\Delta}^{\perp})$ (resp. $\pi(\alpha^{(2)} \oplus \overline{\Delta}^{\perp})$) is a flat. Further, if π and ϕ satisfy:

1. *π (or ϕ) has no nonzero linear structure;*

2. *$\nu \cdot (\pi \oplus \phi) \neq$ constant for $\nu \in \mathbb{F}_2^{\frac{n}{2}} \setminus \{0_{\frac{n}{2}}\}$;*

3. *$\max_{\nu \in \mathbb{F}_2^{\frac{n}{2}}} \deg(\nu \cdot (\pi \oplus \phi)) \geq 2$;*

4. *$\overline{\Delta} \subset \mathbb{F}_2^{\frac{n}{2}}$ and $\dim(\overline{\Delta}) \leq \frac{n}{2} - 2$ (that is, $\deg(1_{\overline{\Delta}}(x^{(1)})) \geq 2$),*

then f does not belong to $\mathcal{M}^{\#}$.

Remark 3.1.9 *Unfortunately, it seems that if π satisfies $\pi(\alpha^{(2)} \oplus \overline{\Delta}^{\perp})$ is a flat for any element $\alpha^{(2)}$ of $\mathbb{F}_2^{\frac{n}{2}}$, then π must have nonzero linear structures. This might be the reason that (for small n) we could not find permutations satisfying the condition $i)$ of Corollary 3.1.8, though we were unable to prove this fact.*

We also desired to study the non-normality of thus constructed functions. Checking the normality of a function is in general a difficult problem. The first non-normal bent functions were constructed in [10] in 2006. In the same article an efficient algorithm for checking the normality of a given function was also introduced. Our wish was to check the normality of functions constructed with Theorem 3.1.3 but it turned out that the actual implementation of the described algorithm was unfortunately not available.

Therefore we wrote for this purpose a new algorithm using the programming package MAGMA. We briefly describe it here. The main idea is that we construct a graph based on the function and then rely on an algorithm already implemented in the MAGMA program to search for possible cliques in the graph which correspond to the subspaces.

Lemma 3.1.10 *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function, let $c \in \mathbb{F}_2$ be a constant, and let N be the set of all such elements $x \in \mathbb{F}_2^n$ that $f(x) = c$. The graph G is constructed in the following way. Let N be its set of vertices and let $x, y \in N$ be connected if and only if $(y - x) \in N$ as well. Then any subspace of dimension k on which the function f is constant must correspond to a clique of power 2^k in the graph G. The inverse is not necessarily true.*

Proof. If there exists a subspace of dimension k on which the function f is constant, then all of its elements are contained in N. Because of the properties of the subspace all these elements will have to be pairwise connected in the graph G and therefore form a clique of size 2^k. Yet if we take an arbitrary clique of size 2^k we have no guarantee that it actually corresponds to a subspace. Let x, y be arbitrary elements of the clique. Then $y - x$ must be contained in N but we have no guarantee that it is also contained in the clique. If it is not, then the clique does not correspond to a subspace. □

The algorithm consists of three main parts and repetition:

- creating the graph G that corresponds to the function f on n variable as described in Lemma 3.1.10,
- searching for all cliques of size $2^{\frac{n}{2}}$ using MAGMA's implemented function,
- checking whether any of the found cliques corresponds to a subspace,
- repeating the process for $c = 0$ and $c = 1$.

If no such clique is found, the function f is non-normal.

One example of π and ϕ satisfying the conditions $ii), iii)$ and $iv)$ of Corollary 3.1.8 but not condition $i)$ is given below. The functions was tested using our normality algorithm and it was demonstrated that it is a non-normal bent functions which might not belong to any known primary classes (possibly to $\mathcal{M}^{\#}$) of bent functions.

Example 3.1.2 *Again, using Corollary 3.1.8, we can design a 10-variable* non-normal *bent function f with algebraic degree 4, whose dual is also a non-normal bent function, though both functions are weakly normal. Being non-normal, this function does not belong to $\mathcal{M} \cup \mathcal{PS}^+ \cup \mathcal{N}$ and furthermore since* $\deg(f) = 4$ *then $f \notin \mathcal{PS}^-$ class. Let $n = 8$ and $\overline{\Delta} = \{(0000), (0101), (1010), (1111)\}$. Further, we have $\overline{\Delta} = \overline{\Delta}^{\perp}$.*

The permutations π and ϕ satisfying $ii) - iv)$ are defined as:

$$\{0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ A\ B\ C\ D\ E\ F\} \overset{\pi}{\mapsto}$$
$$\{A\ B\ 9\ 7\ 1\ 0\ 8\ 6\ 3\ D\ F\ E\ 2\ C\ 4\ 5\},$$
$$\{0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ A\ B\ C\ D\ E\ F\} \overset{\phi}{\mapsto}$$
$$\{A\ D\ C\ E\ 2\ 0\ 1\ 6\ 9\ 4\ F\ 7\ B\ 3\ 8\ 5\}.$$

Computer simulations indicate that all 10-variable functions constructed by means of Corollary 3.1.8 are non-normal bent functions but unfortunately they are all weakly normal. It is unclear whether these functions still belong to $\mathcal{M}^{\#}$ since the item *i)* is generally not satisfied.

We remark that in Corollary 3.1.8 the choice of the subspace indicator $1_{\overline{\Delta}}(x^{(1)})$ defined on the variable space $x_1, \ldots, x_{n/2}$ appears to be crucial for ensuring that f does not belong to $\mathcal{M}^{\#}$, as illustrated in the following result. Replacing $1_{\overline{\Delta}}(x^{(1)})$ by any function g defined on the variable space $x_{n/2+1}, \ldots, x_n$ does not give bent functions outside the $\mathcal{M}^{\#}$ class.

Corollary 3.1.11 *Let $n > 4$ be even and denote $x = (x^{(1)}, x^{(2)}) = (x_1, \ldots, x_n) \in \mathbb{F}_2^{\frac{n}{2}} \times \mathbb{F}_2^{\frac{n}{2}}$ and $x_{n+1}, x_{n+2} \in \mathbb{F}_2$. Let $f_0(x) = \pi(x^{(2)}) \cdot x^{(1)}$ and $f_1(x) = \phi(x^{(2)}) \cdot x^{(1)}$. Then, f, defined as*

$$\begin{aligned} & f(x, x_{n+1}, x_{n+2}) \\ = \ & (x_{n+1} \oplus x_{n+2} \oplus 1) f_0(x) \oplus (x_{n+1} \oplus x_{n+2}) f_1(x) \\ & \oplus (x_{n+2} \oplus 1) g(x^{(2)}) \oplus x_{n+1} x_{n+2} \oplus x_{n+1}, \end{aligned} \tag{3.10}$$

is bent and belongs to $\mathcal{M}^{\#}$, where π, ϕ are two permutations on $\mathbb{F}_2^{\frac{n}{2}}$ and $g \in \mathcal{B}_{n/2}$ is arbitrary.

Proof. Clearly, f_0 and f_1, are bent. Set $\Delta = \mathbb{F}_2^{\frac{n}{2}} \times supp(g(x^{(2)})) \subset \mathbb{F}_2^n$. Thus, $1_\Delta(x) = g(x^{(2)})$. Hence, we know $f_0(x) \oplus 1_\Delta(x)$ and $f_1(x) \oplus 1_\Delta(x)$ are bent. According to Theorem 3.1.1, the function f is bent.

We prove that f belongs to $\mathcal{M}^{\#}$, by using Lemma 2.2.2. We need to find an $(\frac{n+2}{2})$-dimensional subspace V such that

$$D_{(a_1,a_2,a_3,a_4)} D_{(b_1,b_2,b_3,b_4)} f(x, x_{n+1}, x_{n+2}) = 0, \tag{3.11}$$

for any (a_1, a_2, a_3, a_4), $(b_1, b_2, b_3, b_4) \in V$.

Let $V = \{(x^{(1)}, 0_{n/2}, x_{n+1}, x_{n+1}) | x^{(1)} \in \mathbb{F}_2^{\frac{n}{2}}, x_{n+1} \in \mathbb{F}_2\}$. We have

$$D_{(a_1, 0_{\frac{n}{2}}, a_3, a_3)} D_{(b_1, 0_{\frac{n}{2}}, b_3, b_3)} f(x, x_{n+1}, x_{n+2}) = 0$$

for any (a_1, a_2, a_3, a_4), $(b_1, b_2, b_3, b_4) \in V$. Hence, f belongs to $\mathcal{M}^{\#}$. □

Open Problem 1 *The problem of providing generic methods for finding suitable permutations and related subspaces satisfying the conditions of Theorem 3.1.3 and its corollaries is of great significance. We believe that there are many more instances of non-normal bent functions (which are possibly not weakly normal) that can be specified using the results in this section.*

3.1.2 Using Rothaus construction iteratively

In this section we extend the original construction of Rothaus to be valid not only as efficient method for defining bent functions in $(n+2)$ variables but also in $(n+4)$

variables. Furthermore, we indicate the possibility of constructing bent functions in $\mathcal{C}$ and $\mathcal{D}$ iteratively.

Due to symmetry, the original class of bent functions defined by (3.1) can be easily extended by defining two additional bent functions as follows:

$$\begin{aligned} & f'(x, x_{n+1}, x_{n+2}) \\ = \; & A(x)B(x) \oplus A(x)C(x) \oplus B(x)C(x) \oplus x_{n+1}x_{n+2} \\ & \oplus [B(x) \oplus C(x)]x_{n+1} \oplus [A(x) \oplus B(x)]x_{n+2}, \end{aligned}$$

$$\begin{aligned} & f''(x, x_{n+1}, x_{n+2}) \\ = \; & A(x)B(x) \oplus A(x)C(x) \oplus B(x)C(x) \oplus x_{n+1}x_{n+2} \\ & \oplus [A(x) \oplus C(x)]x_{n+1} \oplus [B(x) \oplus C(x)]x_{n+2}. \end{aligned}$$

Using the exactly same arguments as Rothaus the functions f' and f'' are also bent assuming that A, B, C and $A \oplus B \oplus C$ are bent. Then provided that $f \oplus f' \oplus f''$ (where f is defined by (3.1)) is also bent one could use these functions as initial functions in the Rothaus construction to possibly generate an infinite sequence of bent functions on larger variable spaces. It is readily verified that

$$\begin{aligned} & (f \oplus f' \oplus f'')(x, x_{n+1}, x_{n+2}) \\ = \; & A(x)B(x) \oplus A(x)C(x) \oplus B(x)C(x) \oplus x_{n+1}x_{n+2}. \end{aligned} \tag{3.12}$$

Nevertheless, it is well-known that this particular form implies the following condition, namely $f \oplus f' \oplus f''$ is bent if and only if $A(x)B(x) \oplus A(x)C(x) \oplus B(x)C(x)$ is bent. Furthermore, it was shown in [67] that this function is bent if and only if $\tilde{A} \oplus \tilde{B} \oplus \tilde{C} = \widetilde{A \oplus B \oplus C}$, where $\tilde{A}$ denotes the dual bent function of A. Several examples of such triples of bent functions were found in [67] and consequently taking such bent functions A, B and C we can use $f, f', f'' \in \mathcal{B}_{\backslash+\in}$ as initial functions in the Rothaus construction. However, these initial functions can also be specified using suitably chosen A, B and C in the $\mathcal{PS}_{ap}$ class, see also Section 3.1.3. The main question to answer is whether the bent conditions used in Rothaus construction are automatically satisfied if we proceed with this iterative process. Thus, we analyze a set of functions defined on $\mathcal{B}_{\backslash+\triangle}$ by:

$$\begin{aligned} h(\mathrm{x}, x_{n+3}, x_{n+4}) &= (ff' \oplus ff'' \oplus f'f'')(\mathrm{x}) \oplus x_{n+3}x_{n+4} \\ & \oplus [f(\mathrm{x}) \oplus f'(\mathrm{x})]x_{n+3} \oplus [f(\mathrm{x}) \oplus f''(\mathrm{x})]x_{n+4}, \\ h'(\mathrm{x}, x_{n+3}, x_{n+4}) &= (ff' \oplus ff'' \oplus f'f'')(\mathrm{x}) \oplus x_{n+3}x_{n+4} \\ & \oplus [f'(\mathrm{x}) \oplus f''(\mathrm{x})]x_{n+3} \oplus [f(\mathrm{x}) \oplus f'(\mathrm{x})]x_{n+4}, \\ h''(\mathrm{x}, x_{n+3}, x_{n+4}) &= (ff' \oplus ff'' \oplus f'f'')(\mathrm{x}) \oplus x_{n+3}x_{n+4} \\ & \oplus [f(\mathrm{x}) \oplus f''(\mathrm{x})]x_{n+3} \oplus [f'(\mathrm{x}) \oplus f''(\mathrm{x})]x_{n+4}, \end{aligned}$$

where $\mathrm{x} = (x, x_{n+1}, x_{n+2}) \in \mathbb{F}_2^{n+2}$.

Once again, $(h \oplus h' \oplus h'')(\mathrm{x}, x_{n+3}, x_{n+4}) = f(\mathrm{x})f'(\mathrm{x}) \oplus f(\mathrm{x})f''(\mathrm{x}) \oplus f'(\mathrm{x})f''(\mathrm{x}) \oplus x_{n+3}x_{n+4}$ and the only issue that needs to be resolved is whether $f(\mathrm{x})f'(\mathrm{x}) \oplus f(\mathrm{x})f''(\mathrm{x}) \oplus f'(\mathrm{x})f''(\mathrm{x})$ is a bent function. For convenience, we write $f(x, x_{n+1}, x_{n+2}) = d(x) \oplus u(x, x_{n+1}, x_{n+2})$ and similarly $f'(x, x_{n+1}, x_{n+2}) = d(x) \oplus u'(x, x_{n+1}, x_{n+2})$, $f''(x, x_{n+1}, x_{n+2}) = d(x) \oplus u''(x, x_{n+1}, x_{n+2})$, where $d(x) = A(x)B(x) \oplus A(x)C(x) \oplus$

$B(x)C(x)$ and u, u', u'' correspond to the remaining parts. Then, it can be readily verified that

$$(ff' \oplus ff'' \oplus f'f'')(\mathrm{x}) = d(x) \oplus x_{n+1}x_{n+2}$$
$$\oplus[x_{n+1} \oplus x_{n+2} \oplus x_{n+1}x_{n+2}][d \oplus A \oplus B \oplus C](x).$$

Denoting by $G = A \oplus B \oplus C$, the last expression can be also written in terms of concatenation so that $ff' \oplus ff'' \oplus f'f'' = d||G||G||G \oplus 1$. Thus, it is both sufficient and necessary to have $d = G$, or equivalently $AB \oplus AC \oplus BC = A \oplus B \oplus C$, for the iterative method to be efficient because then $ff' \oplus ff'' \oplus f'f''$ is a bent function as well. This is trivially satisfied if we assume that $A = B = C$ but it also reduces the Rothaus construction into a trivial method of constructing new bent functions from the known ones.

Open Problem 2 *It would be of interest to specify conditions on initial functions A, B, C along with suitably defined f, f' and f'', where f' and f'' are symmetric versions of f, that would give rise to an infinite sequence of bent functions stemming from the method of Rothaus.*

3.1.2.1 Iterative construction of bent functions in $\mathcal{C}$ and $\mathcal{D}$

Even though the classes $\mathcal{C}$ and $\mathcal{D}$ are derived from $\mathcal{M}$ class, due to the addition of a characteristic function 1_Δ the preservation of the class in an iterative manner is not completely straightforward. To the best of our knowledge, though rather elementary, the result below is not stated explicitly in the literature.

Theorem 3.1.4 *Let n and m be two even integers. Let $f_0(x) = \pi(x^{(2)}) \cdot x^{(1)}$ and its associated bent function in $\mathcal{C}$ or $\mathcal{D}$ be defined as $f_0(x) + 1_\Delta(x)$, where $\Delta = L \times \mathbb{F}_2^{\frac{n}{2}}$ or $\Delta = E_1 \times E_2$. Then, the function $f \in \mathcal{B}_{n+m}$ defined as*

$$\begin{aligned} & f(x, x_{n+1}, x_{n+2}, \ldots, x_{n+m}) \\ = \ & f_0(x) \oplus \bigoplus_{j=1}^{m/2} x_{n+2j-1}x_{n+2j} \oplus 1_{\Delta'}, \end{aligned} \tag{3.13}$$

is bent and belongs to $\mathcal{C}$ or $\mathcal{D}$ (depending on the choice of Δ), where $\Delta' = \Delta \times \{(x_{n+1}, 0)|x_{n+1} \in \mathbb{F}_2\} \times \{(x_{n+3}, 0)|x_{n+3} \in \mathbb{F}_2\} \times \cdots \times \{(x_{n+m-1}, 0)|x_{n+m-1} \in \mathbb{F}_2\} \subset \mathbb{F}_2^{\frac{n}{2}} \times \mathbb{F}_2^{\frac{n}{2}} \times \mathbb{F}_2^m$.
In particular, if f_0 belongs to $\mathcal{D}_0$ then f also belongs to $\mathcal{D}_0$.

Proof. The proof is a straightforward analysis, employing the fact that $f_0 \oplus 1_\Delta$ is bent and that the choice of Δ' indeed implies that the condition $\pi(\alpha \oplus L^\perp)$ is a flat for any α (alternatively $\pi(E_2) = E_1^\perp$ for class $\mathcal{D}$) is roughly speaking preserved on the increased variable space. The latter is due to the particular choice of the indicator Δ'. □

3.1.3 Counting bent functions in $\mathcal{PS}_{ap}$ satisfying Rothaus condition

In the context of Rothaus' construction, the issue of specifying three bent functions (whose sum is also bent) was initially addressed in [20] by employing the $\mathcal{M}$ class. Also, based on the initial work of Carlet [16], a similar idea of considering bent functions of the form $g(x) = A(x)B(x) \oplus A(x)C(x) \oplus B(x)C(x)$, where A, B, C are bent, was investigated by Mesnager [67]. Notice that in this case the variable space remains unchanged and the bent conditions are also related to the duals of the initial functions, see [67] for more details. Basically, this form corresponds to the restriction of f given by (3.1) obtained by fixing $(x_{n+1}, x_{n+2}) = (0, 0)$.

This motivates us to investigate the possibility of finding three initial bent functions for (extended) Rothaus' construction within the $\mathcal{PS}$ class. In particular, bent functions f_0 and f_1 in Theorem 3.1.1, satisfying that $f_0 \oplus 1_\Delta$ and $f_1 \oplus 1_\Delta$ are also bent (where additionally $f_0(x) = f_1(x)$ when $x \in \Delta$), can be easily specified using the $\mathcal{PS}$ class.

Remark 3.1.12 *Henceforth we deal with a fixed full (complete) spread of the space $\mathbb{F}_2^n$. For simplicity, we assume that the fixed spread is actually the Desarguesian spread, which consists of the $2^k + 1$ multiplicative cosets of $\mathbb{F}_{2^k}^*$ in $\mathbb{F}_{2^n}^*$, thus dealing with the $\mathcal{PS}_{ap}$ class which then has an efficient algebraic representation. However, there are many other full (such as e.g. Andrè's spread) and partial spreads that can be used for the same purpose.*

The main idea is to select the points (disjoint linear subspaces) from the complete spread for the bent functions A, B, and C so that they overlap and cancel each other out in such a way that their sum again consists of either $2^{\frac{n}{2}-1}$ or $2^{\frac{n}{2}-1} + 1$ points. Depending on whether the functions A, B, and C belong to the $\mathcal{PS}^+$ or $\mathcal{PS}^-$ class, we have 8 different cases if we differentiate between the three functions and four if we do not.

Our estimates on the number of functions constructed this way concerns only one cases, when all the initial function A, B, C belong to PS^-, the remaining cases being similar to analyze.

First we may select linear subspaces that constitute A in $\binom{2^{\frac{n}{2}}+1}{2^{\frac{n}{2}-1}}$ many ways. Then, assuming that exactly $|X|$ many points of B also belong to A, the total number of choices for the constituent subspaces of B is estimated as: $\sum_{|X|=0}^{2^{\frac{n}{2}-1}} \binom{2^{\frac{n}{2}-1}}{|X|}\binom{2^{\frac{n}{2}-1}+1}{2^{\frac{n}{2}-1}-|X|}$.

Figure 3.1 shows how the function $A \oplus B$ looks like after A and B have been specified. Now, the selection of $2^{\frac{n}{2}-1}$ disjoint subspaces of C must ensure that $A \oplus B \oplus C$ belongs to $\mathcal{PS}$. It implies that either these subspaces extend the support of $A \oplus B \oplus C$ (when we choose subspaces in the support of C that either belong to both A and B or that belong to neither of these - coloured white in Figure 3.1) or some subspaces are removed from $A \oplus B$ them from the final selection (when we choose subspaces in C that belong either to A or B but not both - coloured green in Figure 3.1). Depending on the specification of A and B, the impact of adding C to $A \oplus B$ is therefore the addition of $|Y|$ subspaces, $0 \le |Y| \le 2^{\frac{n}{2}-1}$, and subsequently the subtraction of exactly $2^{\frac{n}{2}-1} - |Y|$ subspaces, and additionally $A \oplus B \oplus C$ contains either $2^{\frac{n}{2}-1}$ or $2^{\frac{n}{2}-1} + 1$ many subspaces. There are two cases to be considered.

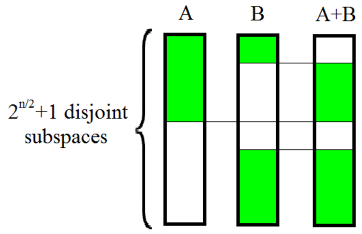

Figure 3.1: Intermediate step - subspaces of $A \oplus B$

The first one is when $A \oplus B \oplus C \in \mathcal{PS}^-$. Then $2(2^{\frac{n}{2}-1}-|X|)+|Y|-(2^{\frac{n}{2}-1}-|Y|) = 2^{\frac{n}{2}-1}$, which implies that $|Y| = |X|$. We know there are exactly $|X|$ points which belong to both A and B, exactly $|X|+1$ points which belong neither to A nor to B and therefore exactly $2^{\frac{n}{2}} - 2|X|$ points which belong to either A or B. If we select i points from $|X|$, $|Y|-i = |X|-i$ points from $|X|+1$ (these points do not belong to $supp(A) \cup sup(B)$) and $2^{\frac{n}{2}-1} - |Y| = 2^{\frac{n}{2}-1} - |X|$ points from $2^{\frac{n}{2}} - 2|X|$, then such a selection essentially defines a function $A \oplus B \oplus C$ which belongs to $\mathcal{PS}^-$.

Therefore, we have $\binom{2|X|+1}{|X|}\binom{2^{\frac{n}{2}}-2|X|}{2^{\frac{n}{2}-1}-|X|}$ possibilities for choosing subspaces that specify C. The total number of possibilities for getting $A \oplus B \oplus C \in \mathcal{PS}^-$ is

$$\binom{2^{\frac{n}{2}}+1}{2^{\frac{n}{2}-1}} \sum_{|X|=0}^{2^{\frac{n}{2}-1}} \binom{2^{\frac{n}{2}-1}}{|X|}\binom{2^{\frac{n}{2}-1}+1}{2^{\frac{n}{2}-1}-|X|}\binom{2|X|+1}{|X|}\binom{2^{\frac{n}{2}}-2|X|}{2^{\frac{n}{2}-1}-|X|}. \tag{3.14}$$

The second case, $A \oplus B \oplus C \in \mathcal{PS}^+$ for $A, B, C \in \mathcal{PS}^-$ is impossible since we have

$$2(2^{\frac{n}{2}-1} - |X|) + |Y| - (2^{\frac{n}{2}-1} - |Y|) \quad = \quad 2^{\frac{n}{2}-1} + 1,$$

and the left-hand side is divisible by 2 whereas the right-hand is not. Therefore, the total number of choices for functions $A, B, C \in \mathcal{PS}^-$ is given by (3.14), the other cases being similar to treat. This approach can be easily adopted for the purpose of counting bent functions f_0 and f_1 in the $\mathcal{PS}$ class satisfying the conditions in Theorem 3.1.1.

Though the above combinatorial results greatly resemble the problem of how many ways are there for choosing in a set of size $2^{n/2}+1$ three sets of size $2^{n/2-1}$ (resp. $2^{n/2-1}+1$) whose symmetric difference has size $2^{n/2-1}$ (resp. $2^{n/2-1}+1$), to the best of our efforts we could not find some explicit formulas in the literature. The special cases, as discussed above, also make this combinatorial problem a bit harder than the standard formulation. The above approach can be adopted for the purpose of specifying the bent functions f_0 and f_1 in Theorem 3.1.1.

In connection to the results given in Section 3.1.2, we remark that the $\mathcal{PS}_{ap}$ class is also a natural resource for identifying bent functions that apart from satisfying that $A \oplus B \oplus C$ is bent also satisfy the condition that $AB \oplus AC \oplus BC = A \oplus B \oplus C$. The latter condition is satisfied if for instance B and C have disjoint supports (thus $BC = 0$) and additionally both A and B as well as A and C intersect in exactly

$2^{n/2-2}$ many subspaces where these intersections are mutually disjoint. Clearly, when $A, B, C \in \mathcal{PS}_{ap}$ then such functions form a subset of the set whose cardinality is given by (3.14). Due to space limitations we omit combinatorial analysis regarding the cardinality of this subset.

3.2 Bent functions in $\mathcal{C}$ and $\mathcal{D}$ outside the extended Maiorana-McFarland class

The secondary classes of bent functions $\mathcal{C}$ and $\mathcal{D}$ are derived from the $\mathcal{M}$ class by adding the indicator functions of suitably chosen vector subspaces to the functions in the $\mathcal{M}$ class. Nevertheless, apart from an explicit subclass denoted by $\mathcal{D}_0$, the bent conditions in terms of the selection of a vector subspace L and permutation π (used to define the initial function $f(x, y) = x \cdot \pi(y)$ in $\mathcal{M}$, where $x, y \in \mathbb{F}_2^n$) are rather hard to satisfy. This problem was recently addressed in [61] and the hardness of satisfying the property (C) (thus identifying a suitable permutation and related vector subspace) was confirmed true since for some classes of permutation polynomials there are no suitable linear subspaces of certain dimension for which the modification of $f \in \mathcal{M}$ would give a bent function $f^* \in \mathcal{C}$. On the other hand, for some other classes of permutations and associated linear subspaces of the same dimension it could be verified that indeed we get a bent function $f^* \in \mathcal{C}$. Thus, given the existence of bent functions $f^* \in \mathcal{C}$ the most fundamental issue is to determine whether these functions are essentially contained in the known primary classes (which gives nothing new in that case) or these functions potentially lie outside the known classes. It should be remarked that certain choices of the indicator functions used to define f^* from $f \in \mathcal{M}$ are provably non-efficient in this context, thus giving rise to bent functions f^* within the class $\mathcal{M}$.

In this section we provide sufficient conditions on the choice of the permutation π and the corresponding linear subspace so that a bent function f^* that belongs either to $\mathcal{C}$ or $\mathcal{D}$ is outside the completed $\mathcal{M}$ class. This is the first step towards a better understanding of classification of bent functions in these secondary classes which also opens up for further investigation concerning a more refined classification in terms of determining whether these functions are also outside the completed $\mathcal{PS}$ and $\mathcal{H}$ class (which is intrinsically more difficult due to the absence of efficient indicators for these classes). The derived sufficient conditions are relatively simple and they roughly speaking correspond to the existence of permutations without linear structures. Then, using the sufficient conditions that the bent functions in $\mathcal{C}$ or $\mathcal{D}$ do not belong to the completed $\mathcal{M}$ class we could show that some instances of bent functions in $\mathcal{C}$ identified in [61] are indeed outside the completed $\mathcal{M}$ class, thus answering positively the classification issue raised in [61]. Furthermore, some generic methods for specifying suitable monomial permutations are given for the purpose of generating bent functions in $\mathcal{D}$ outside the completed $\mathcal{M}$ class.

3.2.1 Sufficient conditions for functions in $\mathcal{C}$ and $\mathcal{D}$ to be outside $\mathcal{M}^{\#}$

Using this criterion we firstly address the problem of deciding whether bent functions in $\mathcal{C}$ are outside the completed $\mathcal{M}$ class.

Theorem 3.2.1 *Let $m = 2n > 4$ be an even integer and let $f(x, y) = \pi(y) \cdot x \oplus 1_{L^\perp}(x)$, where L is any linear subspace of $\mathbb{F}_2^n$ and π is a permutation on $\mathbb{F}_2^n$ such that (π, L) has property (C). If π satisfies:*

1. $\dim(L) \geq 2$;

2. *π has no nonzero linear structure;*

then f does not belong to $\mathcal{M}^{\#}$.

Proof. Let $a^{(1)}, b^{(1)}, a^{(2)}, b^{(2)} \in \mathbb{F}_2^n$. We prove that f does not belong to $\mathcal{M}^{\#}$, by using Lemma 2.2.2. We need to show that there does not exist an n-dimensional subspace V such that

$$D_{(a^{(1)},a^{(2)})} D_{(b^{(1)},b^{(2)})} f = 0,$$

for any $(a^{(1)}, a^{(2)})$, $(b^{(1)}, b^{(2)}) \in V$.

The second derivative of f with respect to a and b can be written as,

$$\begin{aligned} D_{(a^{(1)},a^{(2)})} D_{(b^{(1)},b^{(2)})} f(x) &= x \cdot (D_{a^{(2)}} D_{b^{(2)}} \pi(y)) \oplus a^{(1)} \cdot D_{b^{(2)}} \pi(y \oplus a^{(2)}) \quad (3.15) \\ &\oplus b^{(1)} \cdot D_{a^{(2)}} \pi(y \oplus b^{(2)}) \oplus D_{a^{(1)}} D_{b^{(1)}} 1_{L^\perp}(x) \end{aligned}$$

We denote the set $\{(x, 0_n) \mid x \in \mathbb{F}_2^n\}$ by Δ. We will distinguish two main cases depending on whether $V = \Delta$ or $V \neq \Delta$.

For $V = \Delta$, we can find two vectors $(a^{(1)}, 0_n), (b^{(1)}, 0_n) \in \Delta$ such that

$$D_{a^{(1)}} D_{b^{(1)}} 1_{L^\perp}(x) \neq 0$$

since $\dim(L) \geq 2$ (i.e., $\deg(1_{L^\perp}) \geq 2$). Further, we know

$$D_{(a^{(1)},a^{(2)})} D_{(b^{(1)},b^{(2)})} f(x) = D_{a^{(1)}} D_{b^{(1)}} 1_{L^\perp}(x) \neq 0.$$

Let now $V \neq \Delta$. We split the proof into three cases depending on the cardinality of $V \cap \Delta$. We set $V = \left\{(v_1^{(1)}, v_2^{(1)}), (v_1^{(2)}, v_2^{(2)}), \ldots, (v_1^{(2^n)}, v_2^{(2^n)})\right\}$,

1. For $|V \cap \Delta| = 1$, we have $v_2^{(i)} \neq v_2^{(j)}$ for any $i \neq j$. If there exist two vectors $v_2^{(i_1)}, v_2^{(j_1)}$ such that $v_2^{(i_1)} = v_2^{(j_1)}$, then $v_1^{(i_1)} = v_1^{(j_1)}$, (or $(v_1^{(i_1)} \oplus v_1^{(j_1)}, 0_n) \in V \cap \Delta$), that is, $(v_1^{(i_1)}, v_2^{(i_1)}) = (v_1^{(j_1)}, v_2^{(j_1)})$. Further, $|\{v_2^{(1)}, v_2^{(2)}, \ldots, v_2^{(2^n)}\}| = |V| = 2^n$, that is, $\{v_2^{(1)}, v_2^{(2)}, \ldots, v_2^{(2^n)}\} = \mathbb{F}_2^n$ (here, if $v_2^{(i_1)} = v_2^{(i_2)}$, they are called one element).

   Now, there are two cases to be considered.

(a) If there exists one vector $\mathbf{v} = (v^{(1)}, v^{(2)}) \in V \setminus \{0_{2n}\}$ such that $v^{(1)} = 0_n$, we set $a = \mathbf{v}$. We know

$$D_{a^{(1)}} 1_{L^\perp}(x) = 0.$$

For the nonzero vector a, we have

$$\deg(D_{a^{(2)}} \pi(y)) \geq 1$$

since π has no nonzero linear structure (i.e., $\deg(\pi) \geq 2$). Further, since $\{v_2^{(1)}, v_2^{(2)}, \ldots, v_2^{(2^n)}\} = \mathbb{F}_2^n$, we are able to select $b \in V \setminus \{0_{2n}, a\}$ such that

$$D_{a^{(2)}} D_{b^{(2)}} \pi(y) \neq 0_n.$$

Thus, $D_{(a^{(1)},a^{(2)})} D_{(b^{(1)},b^{(2)})} f(x) = x \cdot (D_{a^{(2)}} D_{b^{(2)}} \pi(y)) \oplus b^{(1)} \cdot D_{a^{(2)}} \pi(y \oplus b^{(2)}) \neq 0$, since $D_{a^{(2)}} D_{b^{(2)}} \pi(y) \neq 0$ implies that $x \cdot (D_{a^{(2)}} D_{b^{(2)}} \pi(y))$ is not constant, i.e. depends on x.

(b) If there does not exist a vector $\mathbf{v} = (v^{(1)}, v^{(2)}) \in V \setminus \{0_{2n}\}$ such that $v^{(1)} = 0_n$, then we have $|\{v_1^{(1)}, v_1^{(2)}, \ldots, v_1^{(2^n)}\}| = |V| = 2^n$ (that is, $\{v_1^{(1)}, v_1^{(2)}, \ldots, v_1^{(2^n)}\} = \mathbb{F}_2^n$) since V is a subspace and $|\{v_2^{(1)}, v_2^{(2)}, \ldots, v_2^{(2^n)}\}| = |V| = 2^n$. We set $a \in V \setminus \{0_{2n}\}$ such that $a^{(1)} \in L^\perp$. From the definition of indicator functions, we know

$$D_{a^{(1)}} 1_{L^\perp}(x) = 0.$$

Further, we have

$$D_{a^{(1)}} D_{b^{(1)}} 1_{L^\perp}(x) = 0.$$

Further, since $\{v_2^{(1)}, v_2^{(2)}, \ldots, v_2^{(2^n)}\} = \mathbb{F}_2^n$, we are able to select $b \in V \setminus \{0_{2n}, a\}$ such that

$$D_{a^{(2)}} D_{b^{(2)}} \pi(y) \neq 0_n.$$

Thus, $D_{(a^{(1)},a^{(2)})} D_{(b^{(1)},b^{(2)})} f(x) = x \cdot (D_{a^{(2)}} D_{b^{(2)}} \pi(y)) \oplus a^{(1)} \cdot D_{b^{(2)}} \pi(y \oplus a^{(2)}) \oplus b^{(1)} \cdot D_{a^{(2)}} \pi(y \oplus b^{(2)}) \neq 0$, since $D_{a^{(2)}} D_{b^{(2)}} \pi(y) \neq 0$ implies that $x \cdot (D_{a^{(2)}} D_{b^{(2)}} \pi(y))$ is not constant, i.e. depends on x.

Hence, we have

$$D_{(a^{(1)},a^{(2)})} D_{(b^{(1)},b^{(2)})} f(x) \neq 0$$

for $|V \cap \Delta| = 1$.

2. For $|V \cap \Delta| \geq 2$, without loss of generality, let $(a^{(1)}, 0_n)(\neq 0_{2n}) \in V \cap \Delta$. Set $b \in V \setminus \{0_{2n}, a\}$, then $b^{(2)} \neq 0_n$. Thus,

$$D_a D_b f(x) = a^{(1)} \cdot D_{b^{(2)}} \pi(y) \oplus D_{a^{(1)}} D_{b^{(1)}} 1_{L^\perp}(x) \neq 0$$

since π has no nonzero linear structure.

Combining both cases $V = \Delta$ and $V \neq \Delta$ we deduce that f does not belong to $\mathcal{M}^{\#}$.

□

A similar set of conditions on permutation π used in the definition of $\mathcal{D}$ class of bent functions can be deduced.

Theorem 3.2.2 *Let $m = 2n > 6$ be an even integer and let $f(x,y) = \pi(y) \cdot x \oplus 1_{E_1}(x)1_{E_2}(x)$, where π is a permutation on $\mathbb{F}_2^n$, and E_1, E_2 are two linear subspaces of $\mathbb{F}_2^n$ such that $\pi(E_2) = E_1^{\perp}$. If π satisfies:*

1. $\dim(E_1) \geq 2$ *and* $\dim(E_2) \geq 2$;
2. *π has no nonzero linear structure;*
3. $\deg(\pi) \leq n - \dim(E_2)$,

then f does not belong to $\mathcal{M}^{\#}$.

The lengthy proof of Theorem 3.2.2 is given in the Appendix.

3.2.2 Some examples of bent functions in $\mathcal{C}$ outside $\mathcal{M}^{\#}$

In this section we apply the criterion derived in the previous section to those bent functions given in [61] that satisfy the property (C). Notice that the condition in Theorem 3.2.1 regards the condition imposed on $\pi(x)$ and not on $\phi(x) = \pi^{-1}(x)$ but this is of no relevance due the result of Charpin and Sarkar [27]. More precisely, it was shown that if F is a permutation then linear structures of F and F^{-1} are closely related and in particular the non-existence of linear structures for F implies the no-existence of linear structures for F^{-1}, see Lemma 2 in [27]. For convenience of the reader, we recall a few examples of bent functions satisfying the property (C), cf. [61].

Theorem 3.2.3 *[61] Suppose $\phi(x) = x^{2^r+1}$, for all $x \in \mathbb{F}_{2^n}$, where $\gcd(r,n) = e$, n/e is odd and $\gcd(2^n-1, 2^r+1) = 1$.*

(i) Then (ϕ, L) (where L is a subspace of $\dim(L) = 2$) satisfies the (C) property if and only if $L = \langle u, cu \rangle$ where $u \in \mathbb{F}_{2^n}^*$ and $1 \neq c \in \mathbb{F}_{2^e}^*$.

(ii) We assume that $e = \gcd(n,r) > 1$ and $L = \langle u_1, c_1u_1, \ldots, c_{s-1}u_1 \rangle$, $\dim(L) = s$, $c_i \in \mathbb{F}_{2^e}^*$, $1 \leq i \leq s-1$, $s \geq 2$, and $u_1 \in \mathbb{F}_{2^n}^*$. Then (ϕ, L) satisfies the (C) property.

The following example was also provided in [61], thus providing an infinite class of bent functions in $\mathcal{C}$ other than $\mathcal{D}_0$.

Example 3.2.1 *Let $n = 2p$ where p is any odd prime, $r = 2$ and $e = \gcd(n,r) = 2$. Since n/e is odd, it is known that $\gcd(2^r+1, 2^n-1) = 1$. Therefore $\phi(x) = x^{2^r+1}$ is a permutation on $\mathbb{F}_{2^n}$. Let ζ be a primitive element of $\mathbb{F}_{2^n}$. Therefore, $\lambda = \zeta^{\frac{2^n-1}{2^e-1}} =$*

$\zeta^{\frac{2^n-1}{3}}$ is a generator of $\mathbb{F}_{2^e}$. Suppose that the permutation $\pi(x) = \phi^{-1}(x) = x^\gamma$ where $\gamma(2^r+1) \equiv 1 \pmod{2^n-1}$. Given r and n, γ can be computed easily by the Euclidean algorithm. Consider the Maiorana-McFarland bent $f(x,y) = x \cdot \pi(y)$. According to Theorem 3.2.3 if we choose $L = \langle 1, \lambda\rangle$, then the function $f^*(x,y) = x \cdot \pi(y) + 1_{L^\perp}(x)$ is in $\mathcal{C}$. The bent function f^* can be explicitly written as

$$\begin{aligned} f^*(x,y) &= Tr_1^n(xy^\gamma) + (Tr_1^n(x)+1)(Tr_1^n(\lambda x)+1) && (3.16)\\ &= Tr_1^n(xy^\gamma) + Tr_1^n(x)Tr_1^n(\lambda x) + Tr_1^n((1+\lambda)x) + 1. && (3.17)\\ & && (3.18)\end{aligned}$$

Using new tools presented in this section we can answer the question of whether the function f^* defined above is outside the completed $\mathcal{M}$ class.

Lemma 3.2.4 *For $r \neq 0$ the function f^* from Example 3.2.1 does not belong to the completed $\mathcal{M}$ class.*

Proof. Using Theorem 3.2.1 we need to prove that $\dim(L) \geq 2$ and that the permutation $\pi(x) = x^\gamma$ has no linear structures. Since $L = \langle 1, \lambda\rangle$, where λ is the generator of $\mathbb{F}_{2^e} = \mathbb{F}_{2^2}$, we have $\dim(L) = 2$. By Lemma 2 in [27], instead of considering $\pi(x)$ we show the non-existence of linear structures of $\phi(x) = x^{2^r+1}$.

Suppose the mapping $\phi(x)$ has a c-linear structure a, where $a, c \in \mathbb{F}_{2^n}^*$. Then

$$(x+a)^{2^r+1} + x^{2^r+1} \quad = \quad c,$$

which implies $x^{2^r} + a^{2^r-1}x + a^{2^r} + a^{-1}c = 0$, for every $x \in \mathbb{F}_{2^n}$. Taking $x = 0$ forces $a^{2^r} + a^{-1}c = 0$ and taking $x = 1$ forces $a^{2^r-1} = 1$. This leaves us with the equation $x^{2^r} + x = 0$ for every $x \in \mathbb{F}_{2^n}$, which implies $2^r \equiv 1 \mod (2^n-1)$ and $r = 0$. It follows that for $r = 2$ the permutation π does not have linear structures and thus the function f^* from Example 3.2.1 does not belong to the completed $\mathcal{M}$ class. □

Remark 3.2.5 *Note that when $r = 0$, the function $\phi(x) = x^{2^r+1} = x^2$ obviously has linear structures since it is a linear permutation, and is not covered by Theorem 3.2.3.*

Another class of so-called bilinear split permutations (considered originally in [6, 51]) of the form

$$\phi(x) = x(Tr_l^n(x) + ax), \tag{3.19}$$

where $n = kl$, $l > 1$, $a \in \mathbb{F}_{2^l} \setminus \mathbb{F}_2$ and $Tr_l^n(x) = \sum_{i=0}^{k-1} x^{2^{li}}$, was also analyzed in [61]. It was shown that when k is odd these permutations also give rise to bent functions satisfying (C).

Lemma 3.2.6 *The above defined function $\phi(x)$ has a linear structure if and only if $l = n$.*

Proof. Let b be a c-linear structure of $\phi(x) = x(Tr_l^n(x) + ax)$. Then

$$\begin{aligned}
(x+b)(Tr_l^n(x+b) + a(x+b)) + x(Tr_l^n(x) + ax) &= c \\
x(Tr_l^n(b) + ab) + b(Tr_l^n(x) + Tr_l^n(b) + ax + ab)) &= c \\
xTr_l^n(b) + bTr_l^n(x) + bTr_l^n(b) + ab^2 &= c \\
xTr_l^n(b) + bTr_l^n(x) + (bTr_l^n(b) + ab^2 + c) &= 0,
\end{aligned}$$

for every $x \in \mathbb{F}_2^n$. Taking $x = 0$ forces $(bTr_l^n(b) + ab^2 + c) = 0$ and taking $x = 1$, since k is odd, implies that $Tr_l^n(b) = b$. We are left with the equation $Tr_l^n(x) = x$. This equation is valid for any $x \in \mathbb{F}_{2^n}$ if and only if $l = n$. □

Thus the bilinear permutations defined by (3.19) can be used in constructions of functions satisfying (C) and being outside the completed $\mathcal{M}$ class whenever we have a nontrivial factorization $n = kl$.

3.2.3 Bent functions in $\mathcal{D}$ outside $\mathcal{M}^\#$

The set of sufficient conditions related to class $\mathcal{D}$ given in Theorem 3.2.2 is harder to satisfy than those related to class $\mathcal{C}$ so we have limited ourselves to the study of monomial permutations.

Proposition 3.2.7 *Let n be even. Then any non-linear monomial permutation $\pi(y) = y^d$, where $deg(\pi) \leq n-2$, satisfies the required conditions in Theorem 3.2.2 for the 2-dimensional vector subspace $E_2 = \langle \zeta^{\frac{2^n-1}{3}}, \zeta^{\frac{2(2^n-1)}{3}} \rangle$, where ζ is a primitive element of $\mathbb{F}_{2^n}$.*

Proof. Since n is even, $3 \mid 2^n - 1$ and furthermore E_2 is not only a vector subspace but also corresponds to a subfield $\{0, 1, \zeta^{\frac{2^n-1}{3}}, \zeta^{\frac{2(2^n-1)}{3}}\}$. This is because π is a monomial permutation and it must map every subfield to itself (multiplication being closed). Therefore, $\pi(E_2) = E_2 = E_1^\perp$. The permutation π is a non-linear monomial, therefore it does not have a linear structure. The condition $\deg(\pi) \leq n - \dim(E_2)$ is satisfied as well since $\deg(\pi) \leq n-2$ and $\dim(E_2) = 2$. □

We illustrate this approach by providing an example for $n = 6$.

Example 3.2.2 *Let $n = 6$ and $d = 11$ (smaller d will be covered by Proposition 3.2.8 below). Since $(2^6 - 1, 11) = 1$ and the binary weight of 11 is 3, $\pi(x) = x^d$ is a cubic permutation. Using the programming package Magma, the vector space representation on $\mathbb{F}_2^6$ of the subspace $E_2 = \langle \zeta^{21}, \zeta^{42} \rangle$, where ζ is the generating element of the field $\mathbb{F}_{2^6}$, is :*

$$E_2 = \left\{ \begin{array}{c} (0,0,0,0,0,0) \\ (1,0,0,0,0,0) \\ (1,1,1,1,0,0) \\ (0,1,1,1,0,0) \end{array} \right\}.$$

Since $1^{11} = 1, (\zeta^{21})^{11} = \zeta^{42}$, and $(\zeta^{42})^{11} = \zeta^{21}$, the subspace E_2 is indeed mapped to itself. This gives us $E_2 = E_1^{\perp}$ and

$$E_1 = \left\langle \begin{array}{c} (0,1,0,1,0,0) \\ (0,0,1,1,0,0) \\ (0,0,0,0,1,0) \\ (0,0,0,0,0,1) \end{array} \right\rangle .$$

Thus, all the requirements of Theorem 3.2.2 are satisfied and the permutation π gives rise to a bent function $f(x,y) = \pi(y) \cdot x \oplus 1_{E_1}(x)1_{E_2}(x)$ contained in $\mathcal{D}$ but outside the $\mathcal{M}^*$ class.

The next result partially overlaps with Proposition 3.2.7 but, as shown in Example 3.2.3, it also includes cases when n is odd.

Proposition 3.2.8 *Let $\pi(y) = y^d$ be a quadratic permutation over $\mathbb{F}_{2^n}$ ($n \geq 4$), where $d = 2^i + 2^j, i > j$, and $(2^n - 1, 2^i + 2^j) = 1$. Let also $E_2 = \langle \zeta^a, \zeta^b \rangle$ be a 2-dimensional linear subspace of $\mathbb{F}_2^n$, where ζ is a primitive element of $\mathbb{F}_{2^n}$. If*

$$(a - b)(2^i - 2^j) \equiv 0 \mod (2^n - 1)$$

then π satisfies all the conditions in Theorem 3.2.2.

Proof. Since π is a quadratic permutation monomial it has no linear structures. Because $n \geq 4$ and $\deg(\pi) = 2$, it also satisfies $\deg(\pi) \leq n - \dim(E_2)$. It remains to determine when the subspace E_2 is mapped to a subspace. Noting that $\zeta^a \mapsto \zeta^{ad}$ and $\zeta^b \mapsto \zeta^{bd}$, it is required that $\zeta^a + \zeta^b$ is mapped to $(\zeta^a + \zeta^b)^d = \zeta^{ad} + \zeta^{bd}$. Therefore

$$\begin{aligned} (\zeta^a + \zeta^b)^{2^i+2^j} &= \zeta^{a(2^i+2^j)} + \zeta^{b(2^i+2^j)} \\ \zeta^{a(2^i+2^j)} + \zeta^{a2^i+b2^j} + \zeta^{b2^i+a2^j} + \zeta^{b(2^i+2^j)} &= \zeta^{a(2^i+2^j)} + \zeta^{b(2^i+2^j)} \\ \zeta^{a2^i+b2^j} &= \zeta^{b2^i+a2^j}. \end{aligned}$$

It follows that

$$a2^i + b2^j \equiv b2^i + a2^j \mod (2^n - 1),$$

which implies $(a-b)(2^i-2^j) \equiv 0 \mod (2^n-1)$, as stated. Thus, all three conditions imposed by Theorem 3.2.2 are satisfied. □

Remark 3.2.9 *It should be noted that given the set of parameters a, b, i and j satisfying the main condition in Proposition 3.2.8 we are still left with some freedom in choosing the subspace E_2 since the only constraint is on the fixed difference $a - b$ satisfying $(a - b)(2^i - 2^j) \equiv 0 \mod (2^n - 1)$. This gives multiple choices of a and b for specifying the elements ζ^a, ζ^b.*

It turns out that the conditions in Proposition 3.2.8 cannot be satisfied for relatively small n. It was confirmed (using the programming package Magma) that the smallest n for which a 2-dimensional subspace E_2 in Proposition 3.2.8 can be found is $n = 6$. Nevertheless, in order to also present a construction for odd n, we give below an example for $n = 9$.

Example 3.2.3 *Let $n = 9$ and $\pi(y) = y^9$, thus $i = 3, j = 0$. Then π is a quadratic permutation since $(2^9 - 1, 9) = 1$. Furthermore, $(a - b) = (2^9 - 1)/(2^3 - 2^0) = 73$. We choose $a = 74, b = 1$ and use Magma to get the vector space representation of the subspace $E_2 = \langle \zeta, \zeta^{74} \rangle$, where ζ is the generating element of the field $\mathbb{F}_{2^9}$:*

$$E_2 = \left\{ \begin{array}{c} (0,0,0,0,0,0,0,0,0) \\ (1,1,0,0,1,1,0,1,0) \\ (0,1,0,0,0,0,0,0,0) \\ (1,0,0,0,1,1,0,1,0) \end{array} \right\}$$

$$E_1^{\perp} = \pi(E_2) = \left\{ \begin{array}{c} (0,0,0,0,0,0,0,0,0) \\ (1,1,1,0,1,1,0,0,1) \\ (1,0,0,0,1,0,0,0,0) \\ (0,1,1,0,0,1,0,0,1) \end{array} \right\}.$$

One can readily check that all the requirements of Theorem 3.2.2 are satisfied.

Remark 3.2.10 *Finding non-monomial permutations that satisfy the conditions of Theorem 3.2.2 appears to be much harder and is still an open problem.*

3.2.4 Inclusion in other primary classes

Even though we have confirmed the existence of certain subclasses of bent functions in $\mathcal{C}$ and $\mathcal{D}$ that are provably not included in the completed $\mathcal{M}^*$ class there are some important questions that need to be answered. In the first place, it is of importance to distinguish (at least some subclasses) these classes of functions from the class $\mathcal{D}_0$. In other words, these classes may be contained in the completed class of $\mathcal{D}_0$ in which case they do not belong to either $\mathcal{M}^*$ or to the completed $\mathcal{PS}$ class (denoted by $\mathcal{PS}^*$). Therefore, we show that some instances of the classes presented previously are not included in in the completed class of $\mathcal{D}_0$ which then raises the question whether these functions are possibly outside $\mathcal{PS}^*$. We also consider this problem and provide an affirmative answer to this question.

Let $f(X) = f(x,y) = x \cdot \pi_1(y) + 1_{E_1}(x)1_{E_2}(y)$, where $x, y \in \mathbb{F}_2^n$, be a function defined as in Proposition 3.2.8. To show that f is not contained in $\mathcal{D}_0$, we consider the completed class of f given by $F(X) = f(AX + b) + c \cdot X + d$, where $A = \begin{bmatrix} A_1 & A_2 \\ A_3 & A_4 \end{bmatrix}$ is an invertible binary matrix, A_i are $n \times n$ matrices, $b = (b_1, b_2), c = (c_1, c_2), b_i, c_i \in \mathbb{F}_2^n$, and $d \in \mathbb{F}_2$. It is enough to show that the ANF of F does not equal to the representative of the $\mathcal{D}_0$ class for any choice of A, b, c and d.

Theorem 3.2.11 *Let $F(X)$ be as defined above, where f is defined as in Proposition 3.2.7 or Proposition 3.2.8. If $\deg(\pi_1) + \dim(E_1 \cap E_2) < n - 1$, then $F(X)$ is not contained in $\mathcal{D}_0$.*

Proof. Let us assume that π_1, A, b, c, d are such that

$$F(X) = f(A_1x + A_2y + b_1, A_3x + A_4y + b_2) + c \cdot (x, y) + d$$

$$= (A_1x+A_2y+b_1)\cdot\pi_1(A_3x+A_4y+b_2)+1_{E_1}(A_1x+A_2y+b_1)1_{E_2}(A_3x+A_4y+b_2)+c(x,y)+d$$

belongs to the $\mathcal{D}_0$ class. That is, let for $g(X) \in \mathcal{D}_0$ defined as $g(X) = x\cdot\pi_2(y)+\delta_0(x)$ assume that $F(X) = g(X)$.

Let now $x = 0_n$ be fixed. Then,

$$\begin{aligned} F(0_n, y) &= (A_2y + b_1) \cdot \pi_1(A_4y + b_2) + 1_{E_1}(A_2y + b_1)1_{E_2}(A_4y + b_2) + c \cdot (0_n, y) + d \\ g(0_n, y) &= x \cdot \pi_2(y) + \delta_0(x) = 1. \end{aligned}$$

We set $S_{A_2} = \{A_2y + b_1 | y \in \mathbb{F}_2^n\}, S_{A_4} = \{A_4y + b_2 | y \in \mathbb{F}_2^n\}$. Suppose there are only t vectors $\{y^{(1)}, y^{(2)}, \ldots, y^{(t)}\}$ such that

$$A_2y^{(i)} + b_1 = A_4y^{(i)} + b_2 \in S_{A_2} \cap S_{A_4} \cap E_1 \cap E_2,$$

where $i = 1, 2, \ldots, t$. Further, we know $t \in \{0, 1, 2, 2^2, \ldots, 2^{n-1-\deg(\pi)-1}\}$ since $\dim(E_1 \cap E_2) < n - 1 - \deg(\pi)$. If $F(0_n, y) = g(0_n, y) = 1$, then

$$\deg\left((A_2y + b_1) \cdot \pi_1(A_4y + b_2)\right) = \deg\left(1_{E_1}(A_2y + b_1)1_{E_2}(A_4y + b_2)\right). \tag{3.20}$$

Since $\deg(\pi_1) + \dim(E_1 \cap E_2) < n - 1$, we have that

$$\deg\left((A_2y + b_1) \cdot \pi_1(A_4y + b_2)\right) \leq \deg(\pi) + 1 \tag{3.21}$$

and

$$\deg\left(1_{E_1}(A_2y + b_1)1_{E_2}(A_4y + b_2)\right) > \deg(\pi) + 1. \tag{3.22}$$

From (3.21) and (3.22), we know (3.20) does not hold. □

Remark 3.2.12 *For any function F obtained by means of Proposition 3.2.8, we have* $\deg(\pi_1) = 2$ *and* $\dim(E_1 \cap E_2) \leq 2$*. Thus, for $n > 5$ the function F will lie outside the completed $\mathcal{D}_0$ class. For instance, the function in Example 3.2.3 lies outside the completed $\mathcal{D}_0$ class.*

3.2.4.1 Inclusion in the $\mathcal{PS}$ class

The so-called $\mathcal{PS}$ class, originally considered by Dillon [35], can be viewed as a union of $\mathcal{PS}^-$ and $\mathcal{PS}^+$. The former subclass corresponds to defining the support of f as a union of $2^{n/2-1}$ disjoint linear subspaces (intersecting trivially in 0) of dimension $n/2$ without including the all-zero vector. The latter subclass uses a support a union of $2^{n/2-1}+1$ disjoint linear subspaces of dimension $n/2$ and includes the all-zero vector. In general, proving that a given bent function does not belong to the completed $\mathcal{PS}$ class is much harder than for the $\mathcal{MM}$ class due to the lack of useful indicators. We translate the problem of determining whether a given function belongs to the $\mathcal{PS}$ class to a graph theoretical problem to show its difficulty.

In a graph, a clique is a set of vertices such that any two vertices are adjacent. A clique cover of a given undirected graph is a partition of the vertices of the graph into cliques.

Proposition 3.2.13 *Let $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ be a bent function and $G_f = (V, E)$ its corresponding graph, where $V = supp(f) \setminus \{0\}, E = \{\{x, y\} | x, y \in V, x - y \in supp(f)\}$. If the function $f \in \mathcal{PS}^-(\mathcal{PS}^+)$ then the graph G_f has a clique covering where all cliques are disjoint and of size $2^{n/2-1}(2^{n/2-1}+1)$. If the graph G_f has a clique covering where all cliques correspond to subspaces, are disjoint, and are of size $2^{n/2-1}(2^{n/2-1} + 1)$, then $f \in \mathcal{PS}^-(f \in \mathcal{PS}^+)$.*

Proof. If a subset $H \cup \{0\}, H \subseteq V$, forms a subspace of $\mathbb{F}_2^n$, then any two $x, y \in H$ must be connected and therefore vertices corresponding to elements of H must form a clique. If $f \in PS^-$, $supp(f)$ is exactly a union of $2^{n/2-1}$ disjoint $\frac{n}{2}$-linear subspaces without the 0 vector. The graph G must therefore contain exactly $2^{n/2-1}$ cliques of size $2^{\frac{n}{2}} - 1$ which cover the entire graph and are disjoint. If $f \in PS^+$, $supp(f)$ is exactly a union of $2^{n/2-1} + 1$ disjoint $\frac{n}{2}$-linear subspaces. When defining the set of vertices V the 0 vector is removed. The graph G must therefore contain exactly $2^{n/2-1} + 1$ cliques of size $2^{\frac{n}{2}} - 1$ which again cover the entire graph and are disjoint.

If all the cliques contained in such a covering also correspond to subspaces and are disjoint, the converse is true as well. □

Therefore we can translate the initial problem into graph-theoretical terms in the following way: "Given a bent function f, does the graph G_f have a clique covering where all cliques correspond to subspaces, are disjoint, and of size $2^{\frac{n}{2}} - 1$?"

In graph theory, the so-called Clique Cover Problem is very well known: "Given a graph G and an integer k, can the vertices of the graph be partitioned into k cliques?" It was proven in [45] that this is an NP-complete problem. A related problem, that of finding the minimum clique cover of a graph, that is, finding the minimum integer k for which there exists a clique cover with k cliques, is an NP-hard problem.

This, together with the fact that many other closely related problems in graph theory are proven to be either NP-hard or NP-complete, makes us believe that determining whether an arbitrary bent function f lies within the $\mathcal{PS}$ class is either an NP-hard or an NP-complete problem.

Chapter 4

Permutations and bent functions via translators

The main goal of this chapter is to contribute to the study of permutations of finite fields. During the last few years there has been a tremendous progress in construction methods and characterisation of many infinite classes of permutations, see a survey on recent works in [43] and the references therein. The use of permutations in applications such as coding is well-known and understood. The bijectivity is also an important cryptographic criterion used in the design of some block ciphers. For applicative purposes the use of sparse permutations, *i.e.,* which can be expressed with few terms, is also an important property along with the degree and the nonlinearity which are referred to as the standard cryptographic criteria. For this reason, we are mainly interested in specifying design methods of sparse permutations, having a few polynomial terms.

4.1 Linear translators

This section is based on the work of Kyureghyan, [49, Theorem 1]. This result can also be obtained by using the AGW criterion, see Section 6 in [1].

Theorem 4.1.1 [49, Theorem 1] *Let $n = rk$, with $r, k > 1$. Let L be a $\mathbb{F}_{p^k}$-linear permutation on $\mathbb{F}_{p^n}$. Let f a function from $\mathbb{F}_{p^n}$ onto $\mathbb{F}_{p^k}$, $h : \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}$, $\gamma \in \mathbb{F}_{p^n}^*$ and b is fixed in $\mathbb{F}_{p^k}$. Assume that γ is a b-linear translator of f. Then*

$$F(x) = L(x) + L(\gamma)h(f(x))$$

permutes $\mathbb{F}_{p^n}$ if and only if $g : u \mapsto u + bh(u)$ permutes $\mathbb{F}_{p^k}$.

Note that this construction is in a certain sense a generalization of the so-called *switching construction* [24, 25]. Akbary, Ghioca and Wang unified the Kyureghyan's construction for arbitrary subsets $S \subset \mathbb{F}_{p^n}$ (not only subfields of $\mathbb{F}_{p^n}$) along with proposing a few other constructions in [1]. This general criterion is now called AGW criterion [73, Theorem 8.1.39]. After these pioneering works a series of papers [84, 85, 86, 90] (among others) treated the same topic of specifying new classes of permutation polynomials of the above form. For a nice survey of recent achievements related to this particular class of permutations the reader is referred to [43]. Nevertheless, most of the recent contributions attempt to specify suitable functions h, f and L in functions F given by

$$F \ : \ x \mapsto L(x) + L(\gamma)h(f(x)), \ f : \mathbb{F}_{p^{rk}} \to \mathbb{F}_{p^k}, \ h : \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}, \tag{4.1}$$

or alternatively, for F given by

$$F : x \mapsto \gamma(f(x) + \delta)^s + L(x), \delta \in \mathbb{F}_{p^n}, \tag{4.2}$$

to specify suitable degree s, $\delta \in \mathbb{F}_{p^n}$, the function f, and also some particular field characteristic p, see for instance [84] where three classes of permutations of the form (4.2) were specified for $p = 3$.

Our main purpose is to emphasize that the use of functions f which have translators gives us the possibility to construct many infinite classes of permutations with a large choice of parameters. A suitable use of this method allows us also to construct linear permutations and sparse permutations of high degree and to give their compositional inverses. Moreover, a connection of this class of permutations to complete permutations is considered and also more general results related to an explicit specification of permutations of the form (4.2) are given (for instance valid for any degree s for suitable f and δ).

Actually, our generalized framework turns out to give another (simpler) method to prove the bijectivity of some functions studied in [86, 90, 84].

On the other hand, it turns out that the results in Section 4.1.4 can be derived from the results in [1], more precisely from Theorem 5.1 and Proposition 5.9 in [1]. Nevertheless, our proof technique may have independent significance in the analysis of similar classes of permutations and more importantly our approach may potentially give an insight in the spectra of the component functions which has a great importance in cryptographic applications.

Throughout this section p designates any prime.

4.1.1 On functions having linear translators

In this section, motivated by the possibility of specifying new classes of permutations by means of Theorem 4.1.1, we investigate the existence of linear translators for sparse polynomials $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^k}$ (the problem being difficult for arbitrary polynomials). More precisely, we show the non-existence of linear translators for monomials and derive the exact form of binomials for which there exist linear translators. The monomial trace function of the form $Tr_k^n(x^d)$ is also considered.

The following two results are frequently used throughout this section.

Theorem 4.1.2 [Lucas' theorem] *Let a, b be positive integers and $a = \sum_{i=1}^n a_i p^i$, $b = \sum_{i=1}^n b_i p^i$ their p-adic expansions, where $a_i, b_i \in \mathbb{F}_p$. Then*

$$\binom{a}{b} \pmod{p} \equiv \binom{a_1}{b_1} \cdots \binom{a_n}{b_n}.$$

It follows that $\binom{a}{b} \pmod{p} \neq 0$ if and only if $b \preceq a$, i.e., $b_i \leq a_i$ for all i.

Let now $f(x) : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, $f(x) = \sum_{i=0}^{p^n-1} b_i x^i$. In [75], a compact formula relating the coefficients b_i of f and of its derivative $f(x+u\gamma) - f(x) = \sum_{t=0}^{p^n-2} c_t x^t$ was derived. More precisely

$$c_t = \sum_{i=t+1}^{p^n-1} \binom{i}{t} (u\gamma)^{i-t} b_i, \quad t \in \{0, 1, \dots, p^n - 2\}. \tag{4.3}$$

The first application of these results regards the existence of translators for $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^k}$ which is either monomial or binomial.

Proposition 4.1.3 *Let $f(x) = x^d$, $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^k}$, where $n = rk$ and $r > 1$.*

i) Then the image set of f is in $\mathbb{F}_{p^k}$ if and only if the exponent d is of the form

$$d = j(p^{k(r-1)} + p^{k(r-2)} + \cdots + p^k + 1), \tag{4.4}$$

for some $j \in \{1, \dots, p^k - 1\}$.

ii) The function f does not have a linear translator in sense of Definition 2.4.2.

Proof. *i)* Since f maps to some subfield $\mathbb{F}_{p^k}$, $(x^d)^{p^k} = x^d$ must be true. This means $x^{d(p^k-1)} = 1$ and therefore $d(p^k - 1) \equiv 0 \pmod{p^n - 1}$. It follows that

$$d \;=\; j\frac{p^n - 1}{p^k - 1} = j(p^{k(r-1)} + p^{k(r-2)} + \cdots + 1),$$

for some $j \in \{1, \dots, p^k - 1\}$. *ii)* If a function $f(x) = \sum_{i=0}^{p^n-1} b_i x^i$ has a linear translator, it must satisfy two necessary but not sufficient conditions:

1. it must map to a subfield $\mathbb{F}_{p^k}$ as requested by the definition, and
2. its coefficients b_i must satisfy $c_t = 0$, for $t \in \{1, \dots, p^n - 2\}$ and $c_0 \neq 0$, where c_t and c_0 are defined above by (4.3).

The first condition implies that d must be of the form (4.4), for $j \in \{1, \dots, p^k - 1\}$. Since $b_i = 0$ for $i \neq d$, the second condition implies that $c_t = \binom{d}{t}(u\gamma)^{d-t} = 0$, for all $t \in \{1, \dots, d-1\}$. This is satisfied only if $\binom{d}{t} \equiv 0 \pmod{p}$ for all t. Using Lucas' theorem, the only possibility is $t \not\preceq d$, for all t. But since our d satisfies (4.4), for some $j \in \{1, \dots, p^k - 2\}$, this is impossible. □

Proposition 4.1.4 *Let $f(x) = \beta x^i + x^j$, $i < j$, where $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^k}$, $\beta \in \mathbb{F}_{p^n}^*$ and $n = rk$, where $r > 1$. Then the function f has a linear translator if and only if n is even, $k = \frac{n}{2}$, and furthermore $f(x) = T_k^n(x)$.*

Proof. Let $f(x) = \beta x^i + x^j, i < j, \beta \neq 0$. The function f must satisfy the same two properties as in the proof of Proposition 4.1.3. The second property, according to Definition 2.4.2 and (4.3), implies that c_t must satisfy

$$0 = c_t = \begin{cases} 0 & \text{for } j \le t \le p^n - 2 \\ \binom{j}{t}(u\gamma)^{j-t} & \text{for } i \le t < j \\ \binom{i}{t}(u\gamma)^{i-t}\beta + \binom{j}{t}(u\gamma)^{j-t} & \text{for } 0 < t < i \end{cases}. \tag{4.5}$$

Suppose i and j are both powers of p so that $i = p^{i'}, j = p^{j'}$. Since $t \not\preceq j$ and $t \not\preceq i$ for any t in the above range, by Lucas' theorem $c_t = 0$ for all $t \neq 0$.

Assume now that i and j are not both powers of p and that (4.5) holds. First, we must have $t \not\prec j$ for $i \leq t < j$ (to have $c_t = 0$ for such t); in particular $i \not\prec j$. Then, there exists t, $0 < t < i$, such that either $t \prec j$ or $t \prec i$ for $t < i$. Since $c_t = 0$ we have:

- if $t \prec i$ then $t \prec j$, because otherwise $\beta = 0$, a contradiction;
- if $t \prec j$ then $t \prec i$, since otherwise $c_t = \binom{j}{t}(u\gamma)^{j-t} \neq 0$;

Thus, $t \prec i$ if and only if $t \prec j$, for all $t \in \{1, \ldots, i-1\}$. But, since $i \not\prec j$ there is $t' < i$ which satisfies $t' \prec i$, and $t' \not\prec j$, a contradiction.

Let us now analyze when $f(x) = \beta x^{p^{i'}} + x^{p^{j'}}$. Note that we want to have

$$f(x + \gamma u) - f(x) = f(\gamma u) = \beta(\gamma u)^{p^{i'}} + (\gamma u)^{p^{j'}} = uA(\beta, \gamma),$$

where A is some function of β, γ. Then k must divide i' and j'; set $i' = uk$ and $j' = vk$ $(0 \leq u < v \leq r-1)$. Since F maps to a subfield $\mathbb{F}_{p^k}$, the following must be satisfied for all x:

$$\begin{aligned}(\beta x^{p^{uk}} + x^{p^{vk}})^{p^k} - \beta x^{p^{uk}} - x^{p^{vk}} &= 0\\ \beta^{p^k} x^{p^{(u+1)k}} + x^{p^{(v+1)k}} - \beta x^{p^{uk}} - x^{p^{vk}} &= 0.\end{aligned}$$

Hence, the exponents $\{p^{(u+1)k}, p^{(v+1)k}, p^{uk}, p^{vk}\}$ cannot be two by two distinct. This forces $u = v + 1 \pmod r$ and further $v = u + 1 \pmod r$. This implies $u = u + 2 \pmod r$ showing that the only solution is $u = 0$ with $r = 2$ and $v = r - 1 = 1$ (using also $0 \leq u < v \leq r - 1$). Finally, we must have

$$\beta^{p^k} x^{p^k} + x - \beta x - x^{p^k} = x^{p^k}\left(\beta^{p^k} - 1\right) - x(\beta - 1) = 0, \quad \text{for all } x,$$

which implies $\beta = 1$ so that $F(x) = T_k^{2k}(x)$ completing the proof. □

Any function $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^k}$, $n = rk$, can be expressed as $f(x) = T_k^n(P(x))$, where P is some polynomial in $\mathbb{F}_{p^n}[x]$. Note that this representation is not unique. In the rest of this section we analyze the case when P has a single term, the cases with several terms being significantly more complicated. The following result further refines the choice of d for $f(x) = T_k^n(\beta x^d)$. We denote by $wt_H(d)$ the Hamming weight of d which is the number of nonzero components in the p-adic expansion of integer d.

Proposition 4.1.5 *The function $f(x) = T_k^n(\beta x^d)$, $\beta \in \mathbb{F}_{p^n}^*$, can have a linear translator only if $wt_H(d) \in \{1, 2\}$. When $wt_H(d) = 2$, then d must be equal to $p^j(1 + p^i)$ for some $0 \leq i, j \leq n - 1$, $i \notin \{0, n/2\}$. In particular, $f(x) = T_k^n(\beta x^{2p^j})$ cannot have linear translators.*

Proof. In [23, Theorem 5], it was proved that the function $T_1^n(\beta x^d)$ can have a linear structure only if $wt_H(d) \in \{1, 2\}$. Especially, when $wt_H(d) = 2$ then $d = p^j(1 + p^i)$ for some $0 \leq i, j \leq n - 1$, $i \notin \{0, n/2\}$.

Suppose now that the function $f(x) = T_k^n(\beta x^d)$ has a b-translator γ. Then,

$$\begin{aligned} T_1^n\left(\beta(x+u\gamma)^d - \beta x^d\right) &= T_1^k\left(T_k^n(\beta(x+u\gamma)^d - \beta x^d)\right) \\ &= T_1^k(bu). \end{aligned}$$

If we now fix $u \in \mathbb{F}_{p^k}$, then $u\gamma$ becomes the $T_1^k(bu)$-linear structure of $T_1^n(\beta x^d)$, which gives the result. In particular, the function $T_1^n(\beta x^{2p^j})$ (corresponding to $i = 0$ in $d = p^j(1+p^i)$) cannot have linear translators. □

The following result was mentioned by Kyureghyan in [49].

Lemma 4.1.6 *Let f be an affine function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^k}$ given by $f(x) = T_k^n(\beta x) + a$, where $\beta \in \mathbb{F}_{p^n}$ and $a \in \mathbb{F}_{p^k}$. Then, any $\gamma \in \mathbb{F}_{p^n}$ is a b-translator of f, with $b = T_k^n(\beta\gamma)$.*

Proof. For any $\gamma \in \mathbb{F}_{p^n}$ we have

$$f(x+u\gamma) - f(x) = T_k^n(\beta(x+u\gamma)) - T_k^n(\beta x) = T_k^n(\beta u\gamma) = uT_k^n(\beta\gamma),$$

for all $u \in \mathbb{F}_{p^k}$ and $x \in \mathbb{F}_{p^n}$. □

The next result regards the existence of linear translators for the trace of quadratic monomials which in general contains r polynomial terms for $n = rk$.

Lemma 4.1.7 *Let $n = rk$ and $f(x) = T_k^n(\beta x^{p^i+p^j})$, where $i < j$. Then, f has a derivative independent of x, that is, $f(x+u\gamma) - f(x) = T_k^n(\beta(u\gamma)^{p^i+p^j})$ for all $x \in \mathbb{F}_{p^n}$, all $u \in \mathbb{F}_{p^k}$, if and only if $\beta, \gamma \in \mathbb{F}_{p^n}$ are related through,*

$$\beta\gamma^{p^{i+lk}} + \beta^{p^{(r-l)k}}\gamma^{p^{i+(r-l)k}} = 0, \tag{4.6}$$

where $0 < l < r$ satisfies $j = i + kl$.
In particular, if $\beta \in \mathbb{F}_{p^k}$ then $f(x+u\gamma) - f(x) = \beta T_k^n((u\gamma)^{p^i+p^{i+kl}})$ if and only if $\gamma^{p^{2kl}-1} = -1$, which requires $\frac{r}{\gcd(r,2l)}$ is even when $p > 2$.

Proof. For $f(x) = T_k^n(\beta x^{p^i+p^j})$, we have

$$\begin{aligned} f(x+u\gamma) - f(x) &= T_k^n\left(\beta(x+u\gamma)^{p^i+p^j}\right) - T_k^n\left(\beta x^{p^i+p^j}\right) \\ &= T_k^n\left(\beta x^{p^i}(u\gamma)^{p^j} + \beta x^{p^j}(u\gamma)^{p^i} + \beta(u\gamma)^{p^i+p^j}\right) \\ &= T_k^n\left(\beta x^{p^i}(u\gamma)^{p^j}\right) + T_k^n\left(\beta x^{p^j}(u\gamma)^{p^i}\right) + T_k^n\left(\beta(u\gamma)^{p^i+p^j}\right). \end{aligned}$$

The above expression will be independent of x if and only if $T_k^n(\beta x^{p^i}(u\gamma)^{p^j}) = -T_k^n(\beta x^{p^j}(u\gamma)^{p^i})$, for all $x \in \mathbb{F}_{p^n}$ and all $u \in \mathbb{F}_{p^k}$.

We analyze this equation in terms of the congruence $i \equiv j \pmod{k}$. If $i \not\equiv j \pmod{k}$, it follows that all the exponents are pairwise different. Therefore, all the coefficients must equal 0 and so either $\beta = 0$ or $\gamma = 0$. But γ cannot be 0, following from Definition 2.4.2, and β cannot be 0, since then $f(x) = 0$.

It follows that $i \equiv j \pmod{k}$, thus $j = i + kl$ for some $0 < l < r$. Note that we exclude the case $l = 0$. Indeed, in this case, f is linear for $p = 2$ and $f(x) = x^{2p^i}$ for $p > 2$, a function which cannot have a linear translator by Proposition 4.1.5. Therefore, we have

$$\begin{aligned} f(x+u\gamma) - f(x) &= T_k^n\left(\beta x^{p^i}(u\gamma)^{p^{i+lk}}\right) + T_k^n\left(\beta x^{p^{i+lk}}(u\gamma)^{p^i}\right) + T_k^n\left(\beta(u\gamma)^{p^i+p^{i+lk}}\right) \\ &= T_k^n\left(\beta x^{p^i}(u\gamma)^{p^{i+lk}} + \beta^{p^{(r-l)k}} x^{p^i}(u\gamma)^{p^{i+(r-l)k}} + \beta(u\gamma)^{p^i+p^{i+lk}}\right) \\ &= u^{p^i} T_k^n\left(x^{p^i}\left(\beta\gamma^{p^{i+lk}} + \beta^{p^{(r-l)k}}\gamma^{p^{i+(r-l)k}}\right)\right) \\ &\quad + u^{2p^i} T_k^n\left(\beta\gamma^{p^i+p^{i+lk}}\right). \end{aligned} \tag{4.7}$$

Thus, we must have

$$\beta\gamma^{p^{i+lk}} + \beta^{p^{(r-l)k}}\gamma^{p^{i+(r-l)k}} = 0,$$

to eliminate x.

In particular, if $\beta \in \mathbb{F}_{p^k}$ then the above condition reduces to $\gamma^{p^{2lk}-1} = -1$, which for p odd has a solution exactly when $\frac{n}{\gcd(n,2kl)} = \frac{r}{\gcd(r,2l)}$ is even (see [23, Claim 4], for instance).

□

Remark 4.1.8 *It can be easily verified that*

$$T_k^n(\beta x^{p^i+p^j}) = \left(T_k^n(ax^{1+p^{j-i}})\right)^{p^i}, \ a = \beta^{p^{n-i}}, \ j > i.$$

Thus, alternatively, one can consider the mapping $x \mapsto T_k^n(ax^{1+p^s})$.

The result below specifies further the existence of translators for quadratic trace monomials.

Theorem 4.1.9 *Let $n = rk$ and $f(x) = T_k^n(\beta x^{p^i+p^j})$, where $r > 1$ and $j = i + kl$ for some $0 < l < r$. Assume that $\gamma \in \mathbb{F}_{p^n}^*$ is a b-translator of f, where $b = T_k^n(\beta\gamma^{p^i+p^{i+lk}})$. Then :*

i) If $p = 2$ the condition (4.6) in Lemma 4.1.7 must be satisfied and either

$$b = T_k^n(\beta\gamma^{2^i+2^{i+lk}}) \ \text{ and } i = sk - 1 \text{ for some } 0 < s \le r,$$

or $b = 0$. In particular, if $\beta \in \mathbb{F}_{2^k}$ then $\gamma = 1$ is a 0-translator of f if r is even and $\gamma = 1$ is a β-translator if r is odd, where in the latter case $i = sk - 1$.

ii) If $p > 2$ we necessarily have $b = 0$. In particular, if $\beta \in \mathbb{F}_{p^k}$ then n is even and γ must satisfy $\gamma^{p^{2kl}-1} = -1$ and $Tr_k^n(\gamma^{1+p^{lk}}) = 0$.

Proof. If (4.6) is satisfied then, from (4.7),

$$f(x+u\gamma) - f(x) \;=\; u^{2p^i} T_k^n\left(\beta\gamma^{p^i+p^{i+lk}}\right).$$

For f to have linear translators, we either have $u^{2p^i} = u$ or $T_k^n(\beta\gamma^{p^i+p^{i+lk}}) = 0$.

i) Let $p = 2$. The condition $u^{2p^i} = u$ gives $2^{i+1} \equiv 1 \pmod{2^k - 1}$, which implies $i = sk - 1$, for some $0 < s \leq r$. This follows from the fact that $2^k - 1 \mid 2^{i+1} - 1$ if and only if $k \mid i+1$. Otherwise, if $T_k^n(\beta\gamma^{2^i+2^{i+lk}}) = 0$ then γ is a 0-translator.

In particular, if $\beta \in \mathbb{F}_{2^k}$ then $\gamma = 1$ is a solution to (4.6). Then,

$$b = \beta T_k^n(\gamma^{2^i+2^{i+lk}}) = \beta T_k^n(1) = 0$$

if r is even and $b = \beta$ for odd r where additionally $i = sk - 1$ as above.

ii) For $p > 2$ we have $2p^i \equiv 1 \pmod{p^k - 1}$, which implies $2p^i = 1 + s(p^k - 1)$, for some s. Since p is odd the left-hand side of the equation is even and the right-hand side is odd, which is impossible. The only remaining option for γ is to be a 0-translator.

In particular, if $\beta \in \mathbb{F}_{p^k}^*$, then by Lemma 4.1.7, $\frac{n}{\gcd(n,2kl)} = \frac{r}{\gcd(r,2l)}$ is even and thus n must be even. Furthermore, (4.6) reduces to $\gamma^{p^{2kl}-1} = -1$ and the fact that $b = 0$ implies

$$T_k^n(\beta\gamma^{p^i+p^{i+lk}}) = \beta\left(T_k^n(\gamma^{1+p^{lk}})\right)^{p^i} = 0.$$

□

Remark 4.1.10 *The existence of translators for $f(x) = Tr_k^n(\beta x^{p^i+p^j})$ is more easily handled when $\beta \in \mathbb{F}_{p^k}$. For $\beta \in \mathbb{F}_{p^n}$ general solutions to (4.6) satisfying at the same time the other conditions seem to be difficult to specify explicitly. Theorem 4.1.9 may also induce some non-existence results as well, which however requires further analysis.*

The next corollary follows directly from Theorem 4.1.1 and 4.1.9.

Corollary 4.1.11 *Let $p = 2$, $n = rk$, $f(x) = T_k^n(\beta x^{p^{sk-1}+p^{(s+l)k-1}})$ for some $0 < l < r$, $0 < s \leq r$, and let γ satisfy (4.6) in Lemma 4.1.7. Then*

$$L(x) + L(\gamma)h\left(T_k^n(\beta x^{p^{sk-1}+p^{(s+l)k-1}})\right),$$

where L is a $\mathbb{F}_{p^k}$-linear permutation on $\mathbb{F}_{p^n}$ and $h : \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}$, is a permutation if and only if $g : u \mapsto u + T_k^n(\beta\gamma^{p^{sk-1}+p^{(s+l)k-1}})h(u)$ permutes $\mathbb{F}_{p^k}$.

4.1.2 Compositional inverses

The main goal of this section is to show that a lot of permutations, and some related structures can be derived from Theorem 4.1.1. In this section, we focus on the compositional inverses of these permutations. A similar initiative was taken in [87] where other classes of permutations (not of the form (4.2)) were analyzed with respect to their inverses. Related to compositional inverses of permutations of the form (4.2), we mention Corollary 3.8 in [87] which states that given $\gcd(n,k) = d > 1, s(q^k - 1) \equiv 0 \mod (q^n - 1), \delta \in \mathbb{F}_{q^n}$, the function $f(x) = x + (x^{q^k} - x + \delta)^s$ permutes $\mathbb{F}_{q^n}$ and its inverse is $f^{-1}(x) = x - (x^{q^k} - x + \delta)^s$.

Definition 4.1.12 *Let F be any function over $\mathbb{F}_{p^n}$. For any $t \geq 1$, the function*

$$F_t(x) = \underbrace{F \circ \cdots \circ F}_{t}(x)$$

is said to be the t-fold composition of F with itself.

In [49, Section 4], the author studied the functions $F : x \mapsto x + \gamma f(x)$, *i.e.,* with notation of Definition 2.4.2, the function h being the identity. Several results in [49], regarding the compositional inverses, hold for such F (only). Henceforth, we attempt to specify compositional inverses when h is not the identity.

Lemma 4.1.13 *Let $n = rk$, $k > 1$. Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^k}$, $h : \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}$ and $b \in \mathbb{F}_{p^k}$. Define*

$$F(x) = x + \gamma h(f(x)), \ \gamma \in \mathbb{F}_{p^n}^*$$

where γ is a b-linear translator of f. Then

$$F_2(x) = x + \gamma h(f(x)) + \gamma h\left(bh(f(x)) + f(x)\right).$$

Proof.

$$\begin{aligned} F \circ F(x) &= F\left(x + \gamma h(f(x))\right) \\ &= x + \gamma h(f(x)) + \gamma h\left(f(x + \gamma h(f(x)))\right) \\ &= x + \gamma h(f(x)) + \gamma h\left(bh(f(x)) + f(x)\right), \end{aligned}$$

since $f(x + \gamma h(f(x))) = bh(f(x)) + f(x)$ for all x. □

Proposition 4.1.14 *Notation is as in Lemma 4.1.13. If $b = 0$ then $F_p(x) = x$ so that*

$$F^{-1}(x) = F_{p-1}(x) = x + (p-1)\gamma h(f(x)).$$

In particular, F is an involution when $p = 2$.

Proof. Assume that $b = 0$. In this case, F is a permutation for any h (from Theorem 4.1.1), so that its compositional inverse F^{-1} exists. We get from Lemma 4.1.13:

$$F \circ F(x) = x + 2\ \gamma h(f(x)).$$

Assume that $F_{j-1}(x) = x + (j-1)\gamma h(f(x))$. We have for $2 < j \leq p$:

$$\begin{aligned} F_j(x) &= F \circ F_{j-1}(x) = F_{j-1}(x) + \gamma h(f(F_{j-1}(x))) \\ &= x + (j-1)\gamma h(f(x)) + \gamma h(f(x)) = x + j\gamma h(f(x)), \end{aligned}$$

since $f(x + (j-1)\gamma h(f(x))) = f(x)$, for all x. Thus we get $F_p(x) = x$, for all x, for $j = p$. Moreover if $p = 2$ then $F^{-1} = F$. □

Thus, according to Proposition 4.1.14 a large set of permutations can be obtained whose compositional inverse is known as illustrated below.

Corollary 4.1.15 *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^k}$, $n = rk$, $f(x) = T_k^n(\beta x)$. Choose $\beta, \gamma \in \mathbb{F}_{p^n}^*$ such that $T_k^n(\beta\gamma) = 0$. Let L be any $\mathbb{F}_{p^k}$-linear permutation. Then the functions*

$$F(x) = L(x) + L(\gamma)h\left(T_k^n(\beta x)\right)$$

are permutations for any $h : \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}$. Moreover

$$F^{-1}(x) = L^{-1}(x) + (p-1)L(\gamma)h\left(T_k^n(\beta(L^{-1}(x)))\right).$$

If $p = 2$ and $L(x) = x$, then F is an involution, i.e., $F^{-1} = F$.

Proof. From Lemma 4.1.6, γ is a 0-translator of f if and only if $T_k^n(\beta\gamma) = 0$. So, from Theorem 4.1.1, F is a permutation for any $\mathbb{F}_{p^k}$-linear permutation L and for any h. Further, set $G(x) = x + \gamma h(f(x))$ so that $F = L \circ G$. Then $F^{-1} = G^{-1} \circ L^{-1}$, where, from Proposition 4.1.14,

$$G^{-1}(x) = G_{p-1}(x) = x + (p-1)\gamma h\left(T_k^n(\beta x)\right).$$

Moreover if $p = 2$ and $L(x) = x$, then $F^{-1}(x) = G^{-1}(x)$ with $G^{-1}(x) = G(x)$. □

Taking h linear we get a large set of linear permutations. We illustrate this in the binary case when $r = 2$.

Corollary 4.1.16 *Notation is as in Corollary 4.1.15 with $n = 2k$ and $p = 2$. Assume that L is a $\mathbb{F}_{p^k}$-linear involution, i.e., $L(x) = ax + bx^{2^k}$ as defined by Lemma 2.4.1. Then, for all $\beta, \gamma \in \mathbb{F}_{p^n}^*$ such that $T_k^n(\beta\gamma) = 0$ and for any linear function h the functions*

$$F(x) = L(x) + L(\gamma)h\left(T_k^n(\beta x)\right),$$

are linear permutations of $\mathbb{F}_{p^n}$ and

$$F^{-1}(x) = L(x) + L(\gamma)h\left(T_k^n(\beta(L(x)))\right).$$

Note that for $p = 3$ the compositional inverse is obtained by adding to F its second term, as shown in the example below.

Example 4.1.1 *Let $p = 3$, $n = 3k$ and $a \in \mathbb{F}_{3^k}$.*

$$F(x) = x + \gamma(x^{3^{2k}} + x^{3^k} + x + a)^s,\ T_k^{3k}(\gamma) = 0.$$

Then, by applying Corollary 4.1.15, F is a permutation of $\mathbb{F}_{3^n}$ for any integer s in the range $[1, 3^n - 2]$. Moreover

$$F^{-1} = x + 2\gamma\left(x^{3^{2k}} + x^{3^k} + x + a\right)^s = F(x) + \gamma\left(T_k^n(x) + a\right)^s.$$

In Section 4.1.1, it was proved that a function $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^k}$, p odd, defined by $f(x) = T_k^n(x^{p^i + p^{i+\ell k}})$, can have a b-translator for $b = 0$ only (see Theorem 4.1.9). Based on this, we are able to derive a class of permutations of degree at least 2 whose compositional inverse is known.

Corollary 4.1.17 *Let p be an odd prime, $n = rk$ and ℓ be a positive integer such that $r/\gcd(r, 2\ell)$ is even. Let $f(x) = T_k^n(x^{p^i+p^{i+\ell k}})$, where $0 \le i \le k-1$. Let $\gamma \in \mathbb{F}_{p^n}^*$ such that*

$$\gamma^{p^{2k\ell}-1} = -1 \quad \textit{and} \quad T_k^n(\gamma^{1+p^{\ell k}}) = 0.$$

Then

$$x \mapsto L(x) + L(\gamma)h\left(T_k^n(\beta x^{p^i+p^{i+\ell k}})\right)$$

is a permutation of $\mathbb{F}_{p^n}$, for any $\mathbb{F}_{p^k}$-linear permutation L and any $h : \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}$. Moreover if $F(x) = x + \gamma h\left(T_k^n(x^{p^i+p^{i+\ell k}})\right)$ then

$$F^{-1}(x) = x + \gamma(p-1)h\left(T_k^n(x^{p^i+p^{i+\ell k}})\right).$$

Proof. From Theorem 4.1.9, γ is a 0-linear translator of f if and only if $T_k^n(\gamma^{1+p^{\ell k}}) = 0$. Further, we apply Theorem 4.1.1 and Proposition 4.1.14. □

We previously considered functions with a zero translator, *i.e.,* $b = 0$, to obtain permutations with their compositional inverses. When $b \neq 0$, other permutations with their compositional inverses can be obtained. In this case however, it seems that the definition of the function h has to be specified. The idea is to determine h such that

$$h(f(x)) + h(bh(f(x)) + f(x)) = g(x), \ b \neq 0,$$

(by using Lemma 4.1.13) where g allows us to compute easily the t-fold composition of F with itself. We illustrate our purpose by constructing involutions for any odd p.

Proposition 4.1.18 *Notation is as in Lemma 4.1.13. Let p be an odd prime. Assume that γ is a b-linear translator of f where $b \neq 0$. Set $h(x) = \lambda x$ where $\lambda \in \mathbb{F}_{p^k}^*$ and $\lambda \neq -b^{-1}$. Then the function F,*

$$F(x) = x + \gamma\lambda f(x),$$

permutes $\mathbb{F}_{p^n}^*$. Moreover, if $\lambda = -2b^{-1}$ then F is an involution.

Proof. From Theorem 4.1.1, F is a permutation, since

$$\ell(u) = u + bh(u) = u(1 + \lambda b) \ \text{ for } u \in \mathbb{F}_{p^k};$$

so ℓ is a permutation because $\lambda \neq -b^{-1}$ by hypothesis. Moreover

$$h(f(x)) + h(bh(f(x)) + f(x)) = 2\lambda f(x) + b\lambda^2 f(x) = \lambda f(x)(2 + b\lambda).$$

From Lemma 4.1.13, we get $F \circ F(x) = x$ if and only if $2 + b\lambda = 0$. □

4.1.3 Relation with complete permutations

The concept of complete permutations is of crucial importance for non-zero linear translators b in terms of Theorem 4.1.1, since the main condition there was that $u \mapsto u + bh(u)$ permutes $\mathbb{F}_{p^k}$.

Definition 4.1.19 *Let h be a function over $\mathbb{F}_{p^k}$. We say that h is complete with respect to b, or b-complete, when both h and $u \mapsto u + bh(u)$ permutes $\mathbb{F}_{p^k}$.*

Thus we can apply Theorem 4.1.1 as follows:

Theorem 4.1.20 *Let $n = rk$, $k > 1$. Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^k}$, $h : \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}$, $\gamma \in \mathbb{F}_{p^n}^*$ and $b \in \mathbb{F}_{p^k}^*$ such that γ is a b-linear translator of f. Let L be a $\mathbb{F}_{p^k}$-linear permutation on $\mathbb{F}_{p^n}$.*

If h is b-complete then $F(x) = L(x) + L(\gamma)h(f(x))$ permutes $\mathbb{F}_{p^n}$.

Proof. To say that h is b-complete is to say that both h and $u \mapsto u+bh(u)$ permute $\mathbb{F}_{p^k}$. We apply Theorem 4.1.1 assuming that h is a permutation. □

The characterizarion of complete permutations, especially monomials, is currently discussed in many works (see for instance [2, 85, 89] and refererences). We illustrate Theorem 4.1.20 through the example below.

Example 4.1.2 *Let $p = 3$ and h be the permutation on $\mathbb{F}_{p^3}$ defined by $h(x) = x^{p^2+p+2}$. By [2, Theorem 6] we know those $b \in \mathbb{F}_{p^3}$ such that $u \mapsto u + bh(u)$ permutes $\mathbb{F}_{p^3}$. Thus, we can apply Theorem 4.1.20 for any $n = 3r$ and for any such b. Let $\gamma \in \mathbb{F}_{p^n}$ and*

$$f \ : \ x \in \mathbb{F}_{p^n} \ \mapsto \ x + x^{p^3} + \cdots + x^{p^{(r-1)3}} \in \mathbb{F}_{p^3}.$$

Then, for any $u \in \mathbb{F}_{p^3}$

$$f(x + u\gamma) - f(x) = T_3^{3r}(u\gamma) = uT_3^{3r}(\gamma).$$

Thus, we choose γ such that $b = T_3^{3r}(\gamma)$ is suitable, according to the results of [2]. Then we obtain a new permutation F, for any $\mathbb{F}_{p^3}$-linear permutation L. In particular for $L(x) = x$:

$$F(x) \ : \ x \mapsto x + \gamma \left(T_3^{3r}(x)\right)^{p^2+p+2}$$

is a permutation of $\mathbb{F}_{p^n}$. Another example is $L(x) = ax + x^{p^3}$, where $a \in \mathbb{F}_{p^n}$ and $-a$ are not in the image set of $x \mapsto x^{p^3-1}$. Then

$$F(x) = ax + x^{p^3} + L(\gamma) \left(T_3^{3r}(x)\right)^{p^2+p+2}$$

is a permutation over $\mathbb{F}_{p^n}$.

A set of trinomials which are 1-complete over $\mathbb{F}_{2^{3m}}$ is proposed in [85, Theorem 4]. We give here a slightly different version of this result.

Theorem 4.1.21 *For any $\nu \in \mathbb{F}_{2^m} \setminus \{0,1\}$, the trinomial*

$$h(x) = x^{2^{2m}+1} + x^{2^m+1} + \nu x$$

is complete over $\mathbb{F}_{2^{3m}}$ with respect to any $b \in \mathbb{F}_{2^m} \setminus \{0, \nu^{-1}\}$.

Proof. It is proved in [85] that h is a permutation of $\mathbb{F}_{2^{3m}}$ for any such ν. Thus $x \mapsto bh(x)$ is also a permutation. If $b \in \mathbb{F}_{2^m} \setminus \{0, \nu^{-1}\}$ then $b\nu + 1 \in \mathbb{F}_{2^m} \setminus \{0,1\}$. So we have

$$g(x) = b\left(x^{2^{2m}+1} + x^{2^m+1} + \nu x\right) + x = bh(x) + x,$$

where h and g are both bijective. □

Applying Theorem 4.1.1, we obtain directly the following class of permutation.

Corollary 4.1.22 *Let $n = rk$ with $k = 3m$. Denote by L any $\mathbb{F}_{2^k}$-linear permutation on $\mathbb{F}_{2^n}$. Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^k}$ such that f has a b-translator $\gamma \in \mathbb{F}_{2^n}^*$ with $b \in \mathbb{F}_{2^m}^*$. Then the functions*

$$x \mapsto L(x) + L(\gamma)\left((f(x))^{2^{2m}+1} + (f(x))^{2^m+1} + \nu(f(x))\right)$$

permute $\mathbb{F}_{2^n}$ for all $\nu \in \mathbb{F}_{2^m} \setminus \{0, 1, b^{-1}\}$.

4.1.4 A special class of permutations

There is currently a lot of work related to the functions over $\mathbb{F}_{p^n}$ of type

$$F \; : \; x \mapsto (f(x) + \delta)^s + L(x), \;\; \delta \in \mathbb{F}_{p^n}^*, \tag{4.8}$$

where f is linear, s is any integer and L is a linearized polynomial in $\mathbb{F}_{p^n}[x]$ (see [84],[86] and [91] for the most recent articles, and their references). The problem is *to determine some (δ, s, L) such that F is a permutation.* To apply directly Theorem 4.1.1, we take $L(x) = x$ and specific functions f. According to our previous results and thanks to Theorem 4.1.1 we can treat some cases directly. Note that δ must be in the image set of f to apply Theorem 4.1.1.

Proposition 4.1.23 *Let $n = 2k$, $F(x) = \gamma(f(x))^s + x$ where $f(x) = x^{p^k} + x + \delta$ with $\delta \in \mathbb{F}_{p^k}$. Set $b = T_k^n(\gamma)$. Then*

- *If $b = 0$ then F is a permutation over $\mathbb{F}_{2^n}$ for any s as well as*

  $$x \mapsto L(\gamma)(f(x))^s + L(x) \text{ where } L \text{ is an } \mathbb{F}_{p^k}\text{-linear permutation.}$$

- *When $b = 0$, $F^{-1} = x + (p-1)\gamma(f(x))^s$. Notably, F is an involution if and only if $p = 2$.*

- *When $b \neq 0$, one can apply Theorem 4.1.1 if and only if $u \mapsto u + bu^s$ permutes $\mathbb{F}_{p^k}$. It is especially the case when $u \mapsto u^s$ is b-complete.*

Proof. First, we have from Lemma 4.1.6:

$$f(x+\gamma u)-f(x)=u(\gamma^{p^k}+\gamma),$$

for all $u \in \mathbb{F}_{p^k}$ and all x. Thus γ is a b-translator of f, with $b=\gamma^{p^k}+\gamma$.

To have $b=0$ is always possible. When $p=2$ we take $\gamma \in \mathbb{F}_{p^k}$. When p is odd it is known that $\gamma^{p^k-1}=-1$ has a solution in $\mathbb{F}_{p^n}$ as soon as $n/\gcd(n,k)$ is even (see [23, Claim 4], for instance). Here we have $2k/\gcd(2k,k)=2$. For such γ, we can apply Theorem 4.1.1 for any s. Moreover, the inverse of F is obtained by applying Proposition 4.1.14. According to Theorem 4.1.20, we can apply Theorem 4.1.1 in particular when $u \mapsto u^s$ is b-complete. □

Our purpose is to contribute to the current works on polynomials of type (4.8). Generally, to prove that F is a permutation is easier when δ is in a subfield and f has its image in this subfield. In the next subsections we study specific polynomials, taking $\delta \in \mathbb{F}_{p^n}$ where $n=2k$. The results presented by Propositions 4.1.25 and 4.1.30 (and then Corollary 4.1.34) are partly already known. The necessary and sufficient condition of bijectivity can be obtained by using the AGW criterion. More precisely, we give here instances and applications of the following result which is a direct consequence of [1, Theorem 5.1]. We first give the version of [1, Proposition 5.9] that we need in our context.

Proposition 4.1.24 *Let L be an $\mathbb{F}_{p^k}$-linear polynomial which permutes $\mathbb{F}_{p^k}$ and $g,h:\mathbb{F}_{p^n}\to\mathbb{F}_{p^n}$, where $h(x^{p^k}-x)\in\mathbb{F}_{p^k}^*$.*

Then the function $x\mapsto h(x^{p^k}-x)L(x)+g(x^{p^k}-x)$ is a permutation of $\mathbb{F}_{p^n}$ if and only if

$$x\mapsto h(x)L(x)+g(x)^{p^k}-g(x)\ \ \textit{permutes}\ \mathcal{J}=\{y^{p^k}-y|y\in\mathbb{F}_{p^n}\}.$$

We propose another way of proving the bijectivity in Propositions 4.1.25 and 4.1.30. Our main purpose is to use the component functions of F explicitly relying on the following criterion: $F:\mathbb{F}_{p^n}\mapsto\mathbb{F}_{p^n}$ *is a permutation if and only if all its component functions $F_\lambda(x)=Tr(\lambda F(x))$, $\lambda\in\mathbb{F}_{p^n}^*$, are balanced [58, Theorem 7.7].* This approach may have independent significance for establishing permutation property of other classes of functions and may be useful in the analysis of the Walsh spectra of the component functions.

4.1.4.1 Permutation polynomials for $\mathbf{p=2}$

When $p=2$, to say that the component functions $F_\lambda(x)=Tr(\lambda F(x))$ of F are *balanced* is to prove that

$$A_\lambda=\sum_{x\in\mathbb{F}_{2^n}}(-1)^{Tr(\lambda F(x))}=0,\ \forall\ \lambda\in\mathbb{F}_{2^n}^*. \tag{4.9}$$

Proposition 4.1.25 *Let $n=2k$ and $F:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ with $F(x)=x+(x+x^{2^k}+\delta)^s$, where $\delta\in\mathbb{F}_{2^n}$ and s is any integer in the range $[0,2^n-2]$. Notation F_λ and A_λ is defined above. Let us define*

$$g\ :\ y\mapsto y+(y+\delta)^s+(y+\delta)^{2^ks}\quad \textit{from}\ \mathbb{F}_{2^k}\ \textit{to}\ \mathbb{F}_{2^k}.$$

Then we have:

(i) *F is a permutation over $\mathbb{F}_{2^n}$ if and only if the function g is bijective. In particular, if s satisfies $2^k s \equiv s \pmod{2^n-1}$ then F is a permutation.*

(ii) *The Boolean functions F_λ are balanced for all $\lambda \notin \mathbb{F}_{2^k}$. If $\lambda \in \mathbb{F}_{2^k}$ then*

$$A_\lambda = 2^k \sum_{y\in\mathbb{F}_{2^k}} (-1)^{T_1^k(\lambda g(y))}.$$

Proof. Note that $s = 0, 1$ are trivial cases. So we suppose that $s \geq 2$. The item (i) comes directly from Proposition 4.1.24, by taking (with its notation) $L(x) = x$, $g(x) = (x+\delta)^s$ and h is the constant function equal to 1. Note that in this case $\mathcal{J} = \mathbb{F}_{2^k}$. Clearly, if $2^k s \equiv s \pmod{2^n-1}$ then $g(y) = y$, and thus F is a permutation.

(ii) Now, it is easy to see that F is affine on any coset of $\mathbb{F}_{2^k}$: for $x = a+y$, $y \in \mathbb{F}_{2^k}$

$$F(a+y) = y + a + (a + a^{2^k} + \delta)^s.$$

Let $\mathcal{W}$ be a set of representatives of these cosets. Thus $\mathbb{F}_{2^n} = \cup_{a\in\mathcal{W}}(a+\mathbb{F}_{2^k})$. We have for any $\lambda \in \mathbb{F}_{2^n}^*$:

$$\begin{aligned} A_\lambda &= \sum_{a\in\mathcal{W}}\sum_{y\in\mathbb{F}_{2^k}} (-1)^{Tr(\lambda F(y+a))} \\ &= \sum_{a\in\mathcal{W}}\sum_{y\in\mathbb{F}_{2^k}} (-1)^{Tr(\lambda(y+a+(a+a^{2^k}+\delta)^s))} \\ &= \sum_{a\in\mathcal{W}}\sum_{y\in\mathbb{F}_{2^k}} (-1)^{T_1^k\left((\lambda+\lambda^{2^k})y+T_k^{2k}(\lambda F(a))\right)}. \end{aligned}$$

We deduce that $A_\lambda = 0$ for any $\lambda \notin \mathbb{F}_{2^k}$, which means that F_λ is balanced for all these λ. Now assume that $\lambda \in \mathbb{F}_{2^k}^*$. Then

$$A_\lambda = 2^k \sum_{a\in\mathcal{W}} (-1)^{T_1^k\left(T_k^{2k}(\lambda F(a))\right)},$$

where

$$T_k^{2k}(\lambda F(a)) = \lambda\left(a + a^{2^k} + (a+a^{2^k}+\delta)^s + (a+a^{2^k}+\delta)^{2^k s}\right).$$

Since $a \mapsto a + a^{2^k}$ is a bijection from $\mathcal{W}$ to $\mathbb{F}_{2^k}$, to compute the values $T_k^{2k}(\lambda F(a))$ is exacly to compute $\lambda g(y)$ for $y \in \mathbb{F}_{2^k}$. Clearly, $A_\lambda = 0$ for all $\lambda \in \mathbb{F}_{2^k}^*$ if and only if g is bijective. □

Remark 4.1.26 *In a recent article [86], two classes of permutations $F(x) = x + (x + x^{2^k} + \delta)^s$ were proposed for s of the form $s = i(2^k \pm 1) + 1$. More precisely, it was shown that F is a permutation for $s = 2(2^k - 1) + 1 = 2^{k+1} - 1$ and for $s \in \{2^k + 2, 2^{2k-1} + 2^{k-1} + 1, 2^{2k} - 2^k - 1\}$ when $s = i(2^k + 1) + 1$. The above result covers the case $s = i(2^k + 1)$ for any $i \in [0, 2^k - 2]$, since in this case $s(2^k - 1) \equiv 0 \pmod{2^n - 1}$.*

It is also of interest to establish whether for $s = 2^i$, for $i = 0, \dots, n-1$, the linearized polynomial $F(x)$ is a permutation. An immediate consequence of Proposition 4.1.25 is the following.

Corollary 4.1.27 *Using the same notation as in Proposition 4.1.25, if $s = 2^i$ then $F(x) = x + (x + x^{2^k} + \delta)^s$ is a linearized permutation for any $\delta \in \mathbb{F}_{2^n}$ and any $i = 0, \dots, n-1$.*

Proof. Since F is a permutation if and only if $g(y) = y + T_k^{2k}((y + \delta)^s)$ is a permutation over $\mathbb{F}_{2^k}$, then for $s = 2^i$ we have

$$g(y) = y + T_k^n(y^{2^i}) + T_k^n(\delta^{2^i}) = y + T_k^n(\delta^{2^i})$$

which is clearly a permutation. □

Another direct consequence of Proposition 4.1.25 is the following result.

Corollary 4.1.28 *Using the same notation as in Proposition 4.1.25, if $\delta \in \mathbb{F}_{2^k}$ then $F(x) = x + (x + x^{2^k} + \delta)^s$ is a permutation for any $s \in [0, 2^k - 2]$.*

Proof. If $\delta \in \mathbb{F}_{2^k}$ then $(y+\delta)^s \in \mathbb{F}_{2^k}$ since $y \in \mathbb{F}_{2^k}$ so that $g(y) = y+T_k^n((y+\delta)^s) = y$, which is a permutation and so is F regardless of the choice of s. □

Remark 4.1.29 *Corollary 4.1.28 also follows from Proposition 4.1.23 by noting that in this case $b = 0$, that is, $\gamma = 1$ is a 0-translator. Recall that in this case F is an involution for any $\delta \in \mathbb{F}_{2^k}$.*

4.1.4.2 Permutation polynomials for odd p

Using the same technique, we deduce slightly different results when p is odd. For odd p, the function F_λ is said to be *balanced* when

$$A_\lambda = \sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{Tr(\lambda F(x))} = 0 \tag{4.10}$$

where ζ_p is a p-th root of unity, *i.e.*, $\zeta_p = e^{2\pi i/p}$ for some i. Also, F is a permutation over $\mathbb{F}_{p^n}$ if and only if (4.10) holds for any $\lambda \in \mathbb{F}_{p^n}^*$.

Proposition 4.1.30 *Let p be an odd prime, $n = 2k$ and $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$,*

$$F(x) = L(x) + (x^{p^k} - x + \delta)^s, \ \delta \in \mathbb{F}_{p^n}, \tag{4.11}$$

where $L \in \mathbb{F}_{p^k}[x]$ is a linear permutation and s is any integer in the range $[1, p^n - 2]$. Let us define

$$G(y) = -L(y) + (y + \delta)^s - (y + \delta)^{p^k s}, \ y \in \mathbb{F}_{p^n}.$$

Then we have:

(i) *F is a permutation over $\mathbb{F}_{p^n}$ if and only if the function G permutes the subspace $\mathcal{S} = \{y \in \mathbb{F}_{p^n} \mid T_k^n(y) = 0\}$. In particular, if s satisfies $p^k s \equiv s \pmod{p^n - 1}$ then F is a permutation.*

(ii) *The component functions F_λ of F are balanced for all $\lambda \in \mathbb{F}_{p^n}^*$ satisfying $T_k^n(\lambda) \neq 0$. If $T_k^n(\lambda) = 0$, then*

$$A_\lambda = p^k \sum_{y \in \mathcal{S}} \zeta_p^{T_1^k(\lambda G(y))}.$$

Proof. First, (i) comes directly from Proposition 4.1.24, by taking (with its notation) $g(x) = (x+\delta)^s$ and h is the constant function equal to 1. Obviously $\mathcal{S} = \mathcal{J}$, since $\mathcal{J}$ and $\mathcal{S}$ have the same cardinality p^k and $\mathcal{J} \subset \mathcal{S}$ because $y = u^{p^k} - u$ satisfies $T_k^{2k}(y) = 0$. Note that $L(\mathcal{S}) = \mathcal{S}$ since

$$L(y) + (L(y))^{p^k} = L(y + y^{p^k}) = L(0) = 0, \quad \text{for any } y \in \mathcal{S}.$$

If s satisfies $p^k s \equiv s \pmod{p^n - 1}$, then $G(y) = -L(y)$ implying that F is a permutation since L permutes $\mathcal{S}$ by assumption.

As in Proposition 4.1.25, $\mathcal{W}$ is a set of representatives of the p^k cosets of $\mathbb{F}_{p^k}$. Recall that $F_\lambda(x) = Tr(\lambda F(x))$. We have for any $\lambda \in \mathbb{F}_{p^n}^*$:

$$A_\lambda = \sum_{x \in \mathbb{F}_{p^n}} \zeta_p^{Tr(\lambda F(x))} = \sum_{a \in \mathcal{W}} \sum_{y \in \mathbb{F}_{p^k}} \zeta_p^{Tr(\lambda F(y+a))},$$

where

$$\begin{aligned} Tr(\lambda F(y+a)) &= Tr\left(\lambda(L(y+a) + (a^{p^k} - a + \delta)^s)\right) \\ &= T_1^k\left(L(y)(\lambda + \lambda^{p^k}) + T_k^{2k}(\lambda F(a))\right). \end{aligned}$$

Since $L \in \mathbb{F}_{p^k}[x]$ is a permutation over $\mathbb{F}_{p^n}$ and thus over $\mathbb{F}_{p^k}$ as well, we deduce that $A_\lambda = 0$ for any λ such that $\lambda + \lambda^{p^k} \neq 0$, *i.e.*, F_λ is balanced for such λ. Further, for $\lambda + \lambda^{p^k} = 0$, thus $\lambda \in \mathcal{S}$, we get

$$A_\lambda = p^k \sum_{a \in \mathcal{W}} \zeta_p^{T_1^k\left(T_k^{2k}(\lambda F(a))\right)},$$

where

$$\begin{aligned} T_k^{2k}(\lambda F(a)) &= (\lambda L(a))^{p^k} + \lambda L(a) + T_k^{2k}(\lambda(a^{p^k} - a + \delta)^s) \\ &= \lambda\left(L(a) - L(a^{p^k}) + (a^{p^k} - a + \delta)^s - (a^{p^k} - a + \delta)^{sp^k}\right) \\ &= \lambda\left(L(a - a^{p^k}) + (a^{p^k} - a + \delta)^s - (a^{p^k} - a + \delta)^{sp^k}\right). \end{aligned}$$

Recall that $\pm(z^{p^k} - z) \in \mathcal{S}$, for any $z \in \mathbb{F}_{p^n}$. Moreover $\lambda s \in \mathbb{F}_{p^k}$ for any $s \in \mathcal{S}$, since

$$(\lambda s)^{p^k} = \lambda^{p^k} s^{p^k} = (-\lambda)(-s) = \lambda s.$$

Therefore, $T_k^{2k}(\lambda F(a)) = \lambda B$ with

$$B = L(a) + (a^{p^k} - a + \delta)^s - \left(L(a) + (a^{p^k} - a + \delta)^s\right)^{p^k}, \tag{4.12}$$

which satisfies $T_k^{2k}(B) = 0$, *i.e.*, $B \in \mathcal{S}$. Clearly, the function $a \mapsto a^{p^k} - a$ is a bijection from $\mathcal{W}$ to $\mathcal{S}$. Finally, the function

$$G(y) = -L(y) + (y+\delta)^s - (y+\delta)^{sp^k},$$

can be viewed as a function from the subspace $\mathcal{S}$ to itself and $\lambda G(y) \in \mathbb{F}_{p^k}$. Consequently

$$A_\lambda = p^k \sum_{y \in \mathcal{S}} \zeta_p^{T_1^k(\lambda G(y))}.$$

Note that $A_\lambda = 0$ for any $\lambda \in \mathcal{S}$ if and only if G is a permutation of $\mathcal{S}$. □

Corollary 4.1.31 *Notation is as in Proposition 4.1.30. Assume that* $T_k^n(\delta) = 0$. *Then*

- *If s is even then F is a permutation of $\mathbb{F}_{p^n}$ for any permutation L.*
- *If s is odd then F is a permutation of $\mathbb{F}_{p^n}$ if and only if*

$$y \mapsto L(y) - 2(y+\delta)^s \quad \textit{is a permutation of } \mathcal{S}.$$

- *If s is even and $L(x) = x$, then we have $F^{-1}(x) = F_{p-1}(x)$.*

Proof. As we noticed in the previous proof, L induces a permutation of $\mathcal{S}$. The case s even was proved in [90, Theorem 3.4]. Another proof is simply derived from Proposition 4.1.30 by observing that

$$\begin{aligned} G(y) &= -L(y) + (y+\delta)^s - (-y-\delta)^s \\ &= -L(y) + (y+\delta)^s - (-1)^s(y+\delta)^s = -L(y). \end{aligned}$$

When s is odd, we get $G(y) = -L(y) + 2(y+\delta)^s$. Now consider

$$F(x) = x + (f(x))^s, f(x) = x^{p^k} - x + \delta, \text{ with } s \text{ even.}$$

Note that $f(x) \in \mathcal{S}$ when $T_k^n(\delta) = 0$, since $f(x)^{p^k} = -f(x)$. Moreover,

$$(f(x))^{sp^k} - (f(x))^s = (-f(x))^s - (f(x))^s = 0 \tag{4.13}$$

holds for any even s. To compute the inverse of F we proceed as in Section 4.1.2. We have here

$$F \circ F(x) = F(x) + \left(f(x + (f(x))^s)\right)^s, \tag{4.14}$$

where $T_k^{2k}(f(x)) = 0$. Setting $a = (f(x))^s$, we get

$$\begin{aligned} f(x+a) - f(x) &= (x+a)^{p^k} - (x+a) + \delta - x^{p^k} + x - \delta \\ &= a^{p^k} - a = 0, \quad \text{from (4.13)}. \end{aligned}$$

Hence, according to (4.14),

$$F_2(x) = F(x) + (f(x))^s = x + 2(x^{p^k} - x + \delta)^s.$$

Further, for $j > 2$, assuming that $F_{j-1}(x) = x + (j-1)(f(x))^s$

$$\begin{aligned} F_j(x) &= F_{j-1}(F(x)) = F(x) + (j-1)\left(f(x + (f(x))^s)\right)^s \\ &= x + (f(x))^s + (j-1)(f(x))^s = x + j(f(x))^s. \end{aligned}$$

So, $F_p(x) = x$, completing the proof. □

By noting that $Tr_k^n(\alpha) = 0$ if and only if there exists $\beta \in \mathbb{F}_{p^n}$ such that $\alpha = \beta - \beta^{p^k}$, we can write $\mathcal{S} = \{y \in \mathbb{F}_{p^n} \mid T_k^n(y) = 0\} = \{\beta - \beta^{p^k} | \beta \in \mathbb{F}_{p^n}\}$.

Clearly, $G : \mathcal{S} \to \mathcal{S}$ since $\mathcal{S}$ is a subspace and $(y+\delta)^s - (y+\delta)^{p^k s} \in \mathcal{S}$.

We first consider the special case when $\delta \in \mathcal{S}$.

Proposition 4.1.32 *Let p be odd, $n = 2k$, and $\mathcal{S} = \{y \in \mathbb{F}_{p^n} \mid T_k^n(y) = 0\}$. Then the mapping*

$$G(x) = -L(x) + (x+\delta)^s - (x+\delta)^{p^k s}$$

permutes the set $\mathcal{S}$ for any $\delta \in \mathcal{S}$, any linear permutation L, and any even $s \in \{2, 4, \ldots, p^n - 1\}$. Consequently,

$$F(x) = L(x) + (x^{p^k} - x + \delta)^s,$$

is a permutation for any $\delta \in \mathcal{S}$, for any L and any even $s \in \{2, 4, \ldots, p^n - 1\}$.

Proof. Since s is even, let us write $s = 2s'$ and let $a \in \mathcal{S}$ be arbitrary. Then because $a \in \mathcal{S}$ we can write $a = b - b^{p^k}$ for some $b \in \mathbb{F}_{p^n}$ and

$$\begin{aligned} (b - b^{p^k})^{2s'p^k} &= (b^{p^k} - b^{p^{2k}})^{2s'} \\ &= (b^{p^k} - b)^{2s'} \\ &= (-(b^{p^k} - b))^{2s'} \\ &= (b^{p^k} - b)^{2s'}. \end{aligned}$$

Since $x + \delta$ is an element of $\mathcal{S}$ for every $x, \delta \in \mathcal{S}$, the function $G(x)$, restricted to $\mathcal{S}$, can be also written as

$$\begin{aligned} G(x) &= -L(x) + (x+\delta)^{2s'} - (x+\delta)^{2s'p^k} \\ &= -L(x) + (x+\delta)^{2s'} - (x+\delta)^{2s'} \\ &= -L(x). \end{aligned}$$

Since $L(x)$ is a linear permutation and we already observed that it induces permutation on $\mathcal{S}$, $G(x)$ must be a permutation of $\mathcal{S}$. From Proposition 4.1.30, it then follows that $F(x) = L(x) + (x^{p^k} - x + \delta)^s$ is a permutation. □

This results provides us with many infinite classes of permutations of the form (4.11), as illustrated by the following example.

Example 4.1.3 *Let $p = 3, n = 2k, k = 3, L(x)$ be any $\mathbb{F}_{3^3}$-linear permutation polynomial of $\mathbb{F}_{3^6}$, and $\delta \in \mathbb{F}_{3^6}$ be such that $Tr_3^6(\delta) = 0$. It then follows from Proposition 4.1.32 that the mapping*

$$G(x) = -L(x) + (x+\delta)^s - (x+\delta)^{p^k s}$$

permutes the set $\mathcal{S} = \{y \in \mathbb{F}_{3^6} | Tr_3^6(y) = 0\}$ for any even s. Furthermore, by Proposition 4.1.30

$$F(x) = L(x) + (x^{3^3} - x + \delta)^s$$

is a permutation for any $\delta \in \mathcal{S}$ and any even s.

A closely related issue in this context is whether there are suitable $L(y)$ and exponents s when $\delta \notin \mathcal{S}$.

Proposition 4.1.33 *Let p be odd, $n = 2k$, and $\mathcal{S} = \{y \in \mathbb{F}_{p^n} \mid T_k^n(y) = 0\}$. Then the mapping*

$$G(x) = -L(x) + (x+\delta)^s - (x+\delta)^{p^k s}$$

permutes the set $\mathcal{S}$ for any δ, any linearized permutation L, and any $s = t(p^k+1)$, where t is an integer. Consequently,

$$F(x) = L(x) + (x^{p^k} - x + \delta)^{t(p^k+1)},$$

is a permutation for any δ, for any L, and any integer t.

Proof. For every $x \in \mathbb{F}_{p^n}$ we can see that

$$\begin{aligned} x^{t(p^k+1)} - x^{p^k t(p^k+1)} &= x^{t(p^k+1)} - x^{tp^{2k}+tp^k} \\ &= x^{t(p^k+1)} - x^t x^{tp^k} \\ &= x^{t(p^k+1)} - x^{t(p^k+1)} \\ &= 0. \end{aligned}$$

It follows that

$$G(x) = -L(x) + (x+\delta)^{t(p^k+1)} - (x+\delta)^{p^k t(p^k+1)} = -L(x).$$

Similarly as before, it follows from Proposition 4.1.30 that $G(x)$ is a permutation of $\mathbb{F}_{p^n}$. □

In the case when s is odd, the next corollary generalizes [84, Theorem 4] with a simple proof. Notation is as in Proposition 4.1.30.

Corollary 4.1.34 *Let p be an odd prime, $n = 2k$ and $\delta \in \mathcal{S} \setminus \{0\}$. Then*

$$F(x) = L(x) + (x^{p^k} - x + \delta)^{\ell(p^k-1)+1},\ 1 \le \ell \le p^k,$$

permutes $\mathbb{F}_{p^n}$ if and only if $y \mapsto L(y) - 2(-1)^\ell y$ permutes $\mathcal{S}$. It is especially the case when:

$$F(x) = \rho x + (x^{p^k} - x + \delta)^{\ell(p^k-1)+1},\ \rho \in \mathbb{F}_{p^n}^*,\ \rho \ne 2(-1)^\ell.$$

Proof. Since p is odd, then $\ell(p^k-1)+1$ is odd for any ℓ. From Corollary 4.1.31, F is a permutation if and only if

$$y \mapsto G(y) = L(y) - 2(y+\delta)^s, \quad s = \ell(p^k-1)+1$$

is a permutation of $\mathcal{S}$. Note that $\beta \in \mathcal{S}$ if and only if $\beta^{p^k-1} = -1$. Moreover $\beta^s \in \mathcal{S}$ for any odd s, since

$$T_k^{2k}(\beta^s) = (-\beta)^s + \beta^s = (-1)^s\beta^s + \beta^s = 0.$$

For $y \in \mathcal{S}$, we have $y+\delta \in \mathcal{S}$ and

$$(y+\delta)^s = (y+\delta)^{\ell(p^k-1)}(y+\delta) = (-1)^\ell(y+\delta).$$

So, $G(y) = L(y) - 2(-1)^\ell(y+\delta)$ and G is a permutation if and only if the linear function $y \mapsto L(y) - 2(-1)^\ell y$ is bijective on $\mathcal{S}$. Now if $L(x) = \rho x$ then $y \mapsto (\rho - 2(-1)^\ell)y$ is a permutation as soon as $\rho - 2(-1)^\ell \neq 0$. □

4.2 Frobenius Translators

The main obstacle when considering the form 4.1 is that some new classes of permutation polynomials could be specified provided the existence of suitable polynomials admitting linear translators. For instance, it was shown in the previous section that for $n = rk$ (where $r > 1$), the function $f(x) = \beta x^i + x^j$, $i < j$, where $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^k}$ and $\beta \in \mathbb{F}_{p^n}^*$, has a linear translator if and only if n is even, $k = \frac{n}{2}$, and furthermore $f(x) = T_k^n(x)$. This indicates that the class of polynomials $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^k}$ admitting linear translators is quite likely rather small. To increase its cardinality and consequently to be able to derive other classes of permutation polynomials, we extend the original definition of linear translators to cover a wider class of functions admitting such translators. We call these translators *Frobenius translators* since the derivative of f is rather expressed as $f(x+u\gamma) - f(x) = u^{p^i}b$ in contrast to standard definition $f(x+u\gamma) - f(x) = ub$. Apparently, linear translators are just a special case of Frobenius translators. To justify this extension we may for instance consider the mapping $f : x \mapsto T_k^n(x^{2^{\ell k}+1})$ over $\mathbb{F}_{2^n}$, where $n = rk$ and $1 \leq \ell \leq r-1$, which does not have linear but admits a Frobenius translator, cf. Example 4.2.1. This gives us the possibility to construct permutation polynomials whose form greatly resembles (4.1) though using Frobenius translators instead, cf. Theorem 4.2.4. In connection to the results in [21], we also address some existence issues for the classes of functions given by $f(x) = T_k^n(\beta x^{p^i+p^j})$, where $n = rk$, admitting linear translators and specify exactly the value of γ in this case.

Assuming the existence of a Frobenius translator, the main condition that $F(x) = L(x)^{p^i} + L(\gamma)^{p^i}h(f(x))$ permutes $\mathbb{F}_{p^n}$, similar to the original condition for the form (4.1), is that the mapping $g(u) = u + bh(u)$ permutes $\mathbb{F}_{p^k}$, where $n = rk$. This leads us to the problem of specifying suitable permutations over suitable subfield which we address thoroughly. In the first place, using a multivariate representation for a suitable tower of extension fields we show that $g(u) = u+bh(u)$ can be a permutation for any choice of b in a subfield of $\mathbb{F}_{p^k}$. This gives us much more freedom to identify a function $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^k}$ satisfying $f(x+u\gamma) - f(x) = u^{p^i} b$. Though our approach uses a multivariate representation, the univariate form of h can be easily recovered and furthermore there is a great range of possibility of specifying h of various degree. The case when $b = 1$ is handled separately since there are many known classes of permutations of the form $x + h(x)$ which can be used. In particular, this is the case when certain trinomials with so-called Niho exponents of the form $x + x^{n_1} + x^{n_2}$ are considered, where the exponents n_1 and n_2 are of Niho type [56].

Finally, yet another wide class of permutations of the form $F(x) = L(x) + (x^{p^k} - x + \delta)^s$ is proposed by specifying those L, s, and δ that satisfy the condition given recently in [21]. The permutation property of F is related to the condition that $G(y) = -L(y) + (y+\delta)^s - (y+\delta)^{p^k s}$ permutes the set $\mathcal{S} = \{\beta \in \mathbb{F}_{p^n} : Tr_k^n(\beta) = 0\}$, where $n = 2k$ and $p > 2$. It is shown that $F(x) = L(x) + (x^{p^k} - x + \delta)^s$ is a permutation for any $\mathbb{F}_{p^k}$-linear permutation L, any even s, and any $\delta \in \mathcal{S}$. In case that δ does not belong to $\mathcal{S}$, then F is a permutation for any $\mathbb{F}_{p^k}$-linear permutation L and $s = t(p^k + 1)$, where $t < p^k - 1$ is a nonnegative integer.

4.2.1 Frobenius translators

The main restriction of Theorem 4.1.1 is that it only gives new permutation polynomials for linear translators of f satisfying the conditions in Definition 2.4.2.

Example 4.2.1 *Let $p = 2$, $n = rk$ and $f : x \mapsto T_k^n(x^{2^{\ell k}+1})$ with $1 \le \ell \le r-1$. Let $\gamma \in \mathbb{F}_{2^n}$ and u be any element of $\mathbb{F}_{2^k}$. Then*

$$\begin{aligned} f(x) + f(x+u\gamma) &= T_k^n\left(x^{2^{\ell k}+1} + (x+\gamma u)^{2^{\ell k}+1}\right) \\ &= T_k^n\left(x^{2^{\ell k}}\gamma u + x(\gamma u)^{2^{\ell k}} + (\gamma u)^{2^{\ell k}+1}\right) \\ &= u\, T_k^n\left(x(\gamma^{2^{\ell k}} + \gamma^{2^{n-\ell k}})\right) + u^2 T_k^n\left(\gamma^{2^{\ell k}+1}\right). \end{aligned}$$

This shows that $f(x) + f(x+u\gamma) = u^2\, T_k^n(\gamma^{2^{\ell k}+1})$, for all x and all $u \in \mathbb{F}_{2^k}$, if and only if $\gamma^{2^{\ell k}} + \gamma^{2^{n-\ell k}} = 0$, which is equivalent to $\gamma^{2^{2\ell k}} = \gamma$.

In the above example $b = T_k^n(\gamma^{2^{\ell k}+1})$ is not a linear translator of f since we would obtain $f(x+\gamma u) + f(x) = u^2 b$, for γ satisfying $\gamma^{2^{2\ell k}} = \gamma$, instead of having ub on the right-hand side. To find other (not affine) functions f which have b-translators appears to be a difficult problem. The global description is given in [49, Section 2] but to have precise instances would be useful for some constructions. In particular, extending Definition 2.4.2 to cover other cases, as illustrated in the above example, would be useful for deducing other families of permutation polynomials.

To accomplish this we extend the definition of linear translators to cover the case when $f(x+\gamma u) - f(x) = u^{p^i} b$, as given below.

Definition 4.2.1 *Let $n = rk$, $1 \le k \le n$. Let f be a function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^k}$, $\gamma \in \mathbb{F}_{p^n}^*$ and b fixed in $\mathbb{F}_{p^k}$. Then γ is an (i,b)-*Frobenius translator *for f if*

$$f(x+u\gamma) - f(x) = u^{p^i} b \quad \textit{for all } x \in \mathbb{F}_{p^n} \textit{ and for all } u \in \mathbb{F}_{p^k},$$

where $i = 0, \ldots, k-1$.

Notice that in the above definition taking $i = 0$ gives a standard definition of translators. The next proposition generalizes the standard properties of linear translators to the case of Frobenius translators.

Proposition 4.2.2 *Let $\gamma_1, \gamma_2 \in \mathbb{F}_{p^n}$ be (i, b_i) and (i, b_2)-Frobenius translators, respectively, of the function $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^k}$. Then*

- *$\gamma_1 + \gamma_2$ is an $(i, b_1 + b_1)$-Frobenius translator of f,*
- *$c\gamma_1$ is a $(i, c^{p^i} b_1)$-Frobenius translator of f, for any $c \in \mathbb{F}^*_{p^k}$.*

Proof.

$$\begin{aligned} f(x + u(\gamma_1 + \gamma_2)) - f(x) &= f(x + u\gamma_1) + u^{p^i} b_2 - f(x) \\ &= f(x) + u^{p^i} b_1 + u^{p^i} b_2 - f(x) \\ &= u^{p^i}(b_1 + b_2) \end{aligned}$$

$$\begin{aligned} f(x + u(c\gamma_1)) - f(x) &= f(x + (uc)\gamma_1) - f(x) \\ &= (uc)^{p^i} b_1 \\ &= u^{p^i}(c^{p^i} b_1) \end{aligned}$$

□

The Corollary below will be useful when satisfying conditions of constructions in Section 4.2.3.

Corollary 4.2.3 *In the binary case the sum of any three (i, b)-Frobenius translators $\gamma_1, \gamma_2, \gamma_3$, such that $\gamma_1 + \gamma_2 + \gamma_3 \neq 0$, is again an (i, b)-Frobenius translator.*

Proof. By applying Proposition 4.2.2 we know that $\gamma_1 + \gamma_2 + \gamma_3$ is a $(i, b + b + b)$-Frobenius translator. Since we are considering the binary case, that is an (i, b)-Frobenius translator. □

Theorem 4.2.4 *For $n = rk$, let $h : \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}$ be an arbitrary mapping and let $\gamma \in \mathbb{F}_{p^n}$ be an (i, b)-Frobenius translator of $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^k}$, that is $f(x+u\gamma)-f(x) = u^{p^i} b$ for all $x \in \mathbb{F}_{p^n}$ and all $u \in \mathbb{F}_{p^k}$. Then, the mapping*

$$G(x) = L(x)^{p^i} + L(\gamma)^{p^i} h(f(x)), \tag{4.15}$$

where $L : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is an F_{p^k}-linear permutation, permutes $\mathbb{F}_{p^n}$ if and only if the mapping $g(u) = u + bh(u)$ permutes $\mathbb{F}_{p^k}$.

Proof. We follow the same steps as in the proof of [49, Theorem 6]. Let us first consider the special case $L(x) = x$, thus the function $F(x) = x^{p^i} + \gamma^{p^i} h(f(x))$. Assume that $x, y \in \mathbb{F}_{p^n}$ satisfy $F(x) = F(y)$. Then

$$F(x) = x^{p^i} + \gamma^{p^i} h(f(x)) = y^{p^i} + \gamma^{p^i} h(f(y)) = F(y),$$

and hence

$$x^{p^i} = y^{p^i} + \gamma^{p^i}(h(f(y)) - h(f(x))) = y^{p^i} + \gamma^{p^i} a,$$

where $a = h(f(y)) - h(f(x)) \in \mathbb{F}_q$. This is equivalent to saying that $x = y + \gamma a^{p^{n-i}}$, thus we suppose that $F(y) = F(y + \gamma a^{p^{n-i}})$. Then, using

$$\begin{aligned} F(y + \gamma a^{p^{n-i}}) &= y^{p^i} + (\gamma a^{p^{n-i}})^{p^i} + \gamma^{p^i} h(f(y + \gamma a^{p^{n-i}})) \\ &= y^{p^i} + \gamma^{p^i} a + \gamma^{p^i} h(f(y) + ab), \end{aligned}$$

we get

$$y^{p^i} + \gamma^{p^i} h(f(y)) = y^{p^i} + \gamma^{p^i} a + \gamma^{p^i} h(f(y) + ab),$$

which can be rewritten as

$$h(f(y)) = a + h(f(y) + ab). \tag{4.16}$$

The mapping F is a permutation of $\mathbb{F}_{p^n}$ if and only if the only a satisfying (4.16) is $a = 0$. Using exactly the same arguments as in [49], one can conclude that F is a permutation if and only if $g(u) = u + bh(u)$ permutes $\mathbb{F}_{p^k}$.

To show that $G(x)$ is a permutation it is enough to notice that $G(x) = L(F(x))$. □

Remark 4.2.5 *The condition imposed on h, which applies to both linear and Frobenius translators, requiring that for a given b the function $x + bh(x)$ is a permutation of $\mathbb{F}_{p^k}$ is easily satisfied. Indeed, given any permutation g over $\mathbb{F}_{p^k}$ we can define $h(x) = 1/b(g(x) - x)$ so that $x + bh(x) = g(x)$ is a permutation. Thus, the main challenge is to specify $\{f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^k}\}$ which admit linear/Frobenius translators. Each such translator then gives different permutations over $\mathbb{F}_{p^n}$ for different permutations g over $\mathbb{F}_{p^k}$.*

Apart from Example 4.2.1, one can for instance find Frobenius translators by combining trace functions, more precisely by defining $f(x) = Tr_k^n(x) + Tr_{2k}^n(x)$, for $n = 4k$, as shown below.

Proposition 4.2.6 *For $n = 4k$, the function $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^{2k}}$, defined by $f(x) = Tr_k^n(x) + Tr_{2k}^n(x)$, always has a 0-translator if $\gamma + \gamma^{p^{2k}} = 0$. In the binary case, it also has a $(k, \gamma^{p^k} + \gamma^{p^{3k}})$-Frobenius translator.*

Proof. Let $n = 4k$ and $f(x) = Tr_k^n(x) + Tr_{2k}^n(x)$. Let also $\gamma \in \mathbb{F}_{p^{4k}}^*$ and $u \in \mathbb{F}_{p^{2k}}$. Then

$$\begin{aligned} f(x + u\gamma) - f(x) &= Tr_k^{4k}(x + u\gamma) + Tr_{2k}^{4k}(x + u\gamma) - Tr_k^{4k}(x) - Tr_{2k}^{4k}(x) \\ &= Tr_k^{4k}(x + u\gamma) + Tr_k^{4k}(-x) + Tr_{2k}^{4k}(x + u\gamma) + Tr_{2k}^{4k}(-x) \\ &= Tr_k^{4k}(u\gamma) + Tr_{2k}^{4k}(u\gamma) \\ &= 2u\gamma + (u\gamma)^{p^k} + 2(u\gamma)^{p^{2k}} + (u\gamma)^{p^{3k}} \\ &= 2u(\gamma + \gamma^{p^{2k}}) + u^{p^k}(\gamma^{p^k} + \gamma^{p^{3k}}). \end{aligned}$$

For $p \neq 2$ the only possibility that f has a linear translator is $\gamma + \gamma^{p^{2k}} = 0$, which results in a 0-translator. In the binary case, we have $f(x + u\gamma) - f(x) = u^{2^k}(\gamma^{2^k} + \gamma^{2^{3k}})$, for any $x \in \mathbb{F}_{2^{4k}}$ and any $u \in \mathbb{F}_{2^{2k}}$, which means that γ is a $(k, \gamma^{p^k} + \gamma^{p^{3k}})$-Frobenius translator. □

4.2.2 Some existence issues

In this section we specify exactly Frobenius translators for certain classes of mappings $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^k}$ which gives us the possibility to specify some new infinite classes of permutations. The following existence results are similar to the ones presented in [21], with the difference that here we consider Frobenius translators by means of Definition 4.2.1.

Proposition 4.2.7 *Let $f(x) = x^d$, $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^k}$, where $n = rk$ and $r > 1$. Then the function f does not have Frobenius translators in the sense of Definition 4.2.1.*

Proof. This result follows directly from the proof of Proposition 1 in [21] by direct calculation. □

On the other hand, binomial mappings of the form $f(x) = \beta x^i + x^j$ still admit Frobenius translators as shown below.

Proposition 4.2.8 *Let $f(x) = \beta x^i + x^j$, $i < j$, where $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^k}$, $\beta \in \mathbb{F}_{p^n}^*$ and $n = rk$, where $r > 1$. Then the function f has a Frobenius translator γ if and only if n is even, and $k = \frac{n}{2}$. Furthermore, $f(x) = x^{p^{i'}} + x^{p^{i'+\frac{n}{2}}}$ and γ is an $(i', \gamma^{p^{i'}} + \gamma^{p^{i'+\frac{n}{2}}})$-Frobenius translator.*

The proof uses the same techniques as the proof of Proposition 4.1.4 and is therefore omitted.

We conclude this section by specifying exactly Frobenius translators related to quadratic mappings of the form $f(x) = T_k^n(\beta x^{p^i+p^j})$ as discussed in section 4.1, Lemma 4.1.7.

Lemma 4.2.9 *Let $n = rk$ and $f(x) = T_k^n(\beta x^{p^i+p^j})$, where $i < j$. Then, f has a derivative independent of x, that is, $f(x + u\gamma) - f(x) = T_k^n(\beta(u\gamma)^{p^i+p^j})$ for all $x \in \mathbb{F}_{p^n}$, all $u \in \mathbb{F}_{p^k}$, if and only if $\beta, \gamma \in \mathbb{F}_{p^n}^*$ are related through,*

$$\beta\gamma^{p^{i+lk}} + \beta^{p^{(r-l)k}}\gamma^{p^{i+(r-l)k}} = 0, \tag{4.17}$$

where $0 < l < r$ satisfies $j = i + kl$.

Nevertheless, the relation between β and γ imposed by (4.17) and their existence were not investigated in [21]. Below, we specify the exact relationship between β and γ, thus implying the possibility of defining some infinite classes of permutations explicitly.

Proposition 4.2.10 *Let n, r, k, l be as in Lemma 4.1.7, α be a primitive element of $\mathbb{F}_{p^n}$, and $\gamma = \alpha^a, \beta = \alpha^b \in \mathbb{F}_{p^n}$. Then*

$$\beta\gamma^{p^{i+lk}} + \beta^{p^{(r-l)k}}\gamma^{p^{i+(r-l)k}} = 0$$

if and only if

$$b = \begin{cases} -ap^{i+lk}(p^{(r-l)k} + 1) \mod (p^n - 1), & p = 2 \\ -ap^{i+lk}(p^{(r-l)k} + 1) + \frac{p^n-1}{2}(1 - p^{(r-l)k})^{-1} \mod (p^n - 1), & p \neq 2. \end{cases}$$

Proof. Expressed in terms of α, the equation

$$-\alpha^{b+ap^{i+lk}} = \alpha^{bp^{(r-l)k}+ap^{i+(r-l)k}}$$

is considered separately for the binary and non-binary case. Let $p=2$. In this case

$$\alpha^{b+ap^{i+lk}} = \alpha^{bp^{(r-l)k}+ap^{i+(r-l)k}}.$$

Therefore,

$$\begin{aligned} b+ap^{i+lk} \mod (p^n-1) &= bp^{(r-l)k}+ap^{i+(r-l)k} \mod (p^n-1)\\ b(1-p^{(r-l)k}) \mod (p^n-1) &= ap^{i+lk}(p^{2(r-l)k}-1) \mod (p^n-1)\\ b(1-p^{(r-l)k}) \mod (p^n-1) &= ap^{i+lk}(p^{(r-l)k}-1)(p^{(r-l)k}+1) \mod (p^n-1)\\ b \mod (p^n-1) &= -ap^{i+lk}(p^{(r-l)k}+1) \mod (p^n-1)\\ b &= -ap^{i+lk}(p^{(r-l)k}+1) \mod (p^n-1). \end{aligned}$$

Let $p \neq 2$. In this case $-1 = \alpha^{\frac{p^n-1}{2}}$ and

$$\alpha^{\frac{p^n-1}{2}}\alpha^{b+ap^{i+lk}} = \alpha^{bp^{(r-l)k}+ap^{i+(r-l)k}}.$$

Therefore,

$$\begin{aligned} b+ap^{i+lk}+\frac{p^n-1}{2} \mod (p^n-1) &= bp^{(r-l)k}+ap^{i+(r-l)k} \mod (p^n-1)\\ 2b(1-p^{(r-l)k}) \mod (p^n-1) &= 2a(p^{i+(r-l)k}-p^{i+lk}) \mod (p^n-1)\\ 2b(1-p^{(r-l)k}) \mod (p^n-1) &= 2ap^{i+lk}(p^{2(r-l)k}-1) \mod (p^n-1)\\ 2b(1-p^{(r-l)k}) \mod (p^n-1) &= 2ap^{i+lk}(p^{(r-l)k}-1)(p^{(r-l)k}+1) \mod (p^n-1)\\ 2b &= -2ap^{i+lk}(p^{(r-l)k}+1) \mod (p^n-1). \end{aligned}$$

□

The Frobenius translators related to the function f in Lemma 4.1.7 are further specified in the result below.

Theorem 4.2.11 *Let $n = rk$ and $f(x) = T_k^n(\beta x^{p^i+p^{i+kl}})$, where $r > 1$ and $0 < l < r$. Assume that $\gamma \in \mathbb{F}_{p^n}^*$ is an (s,b)-translator of f, where $b = T_k^n(\beta\gamma^{p^i+p^{i+lk}})$. Then:*

i) If $p = 2$ the condition (4.17) in Lemma 4.2.9 must be satisfied and $s = i+1$. In particular, if $\beta \in \mathbb{F}_{2^k}$ then $\gamma = 1$ is a 0-translator of f if r is even, and $\gamma = 1$ is an $(i+1,\beta)$-translator if r is odd.

ii) If $p > 2$ we necessarily have $b = 0$. In particular, if $\beta \in \mathbb{F}_{p^k}$ then n is even and γ must satisfy $\gamma^{p^{2kl}-1} = -1$ and $Tr_k^n(\gamma^{p^i+p^{i+lk}}) = 0$.

Proof. If (4.17) is satisfied then

$$f(x+u\gamma) - f(x) = u^{2p^i} T_k^n\left(\beta\gamma^{p^i+p^{i+lk}}\right).$$

i) Let $p = 2$. Then $u^{2p^i} = u^{p^{i+1}}$ and γ is an $(i+1, b)$-translator. In particular, if $\beta \in \mathbb{F}_{2^k}$ then $\gamma = 1$ is a solution to (4.17). Then, $b = \beta T_k^n(\gamma^{2^i+2^{i+lk}}) = \beta T_k^n(1) = 0$ if r is even and $b = \beta$ for odd r.

ii) For $p > 2$ we have $2p^i \equiv p^t \pmod{p^k - 1}$ for some positive integer t, which implies $2p^i = m(p^k - 1) + p^j$. Since p is odd, the left-hand side of the equation is even and the right-hand side is odd, which is impossible. The only remaining option is for γ to be a 0-translator.

The rest follows directly from [21, Theorem 4]. □

The following example specifies a function having a linear translator constructed in this way.

Example 4.2.2 *Let us consider $f(x) = T_k^n(\beta x^{p^i+p^j})$ given in Lemma 4.1.7, where $p = 2$. The relevant parameters are: $n = rk = 8, r = 4, k = 2$ and $i = 2, l = 1, j = i + kl = 4$. Let α be a primitive element of the field $\mathbb{F}_{2^4}$. We fix an arbitrary element $\gamma = \alpha^a$ by setting e.g. $a = 3$. Now the function $f : \mathbb{F}_{2^8} \to \mathbb{F}_{2^2}$, having a linear translator, can be specified using the condition (4.17) in Lemma 4.2.9. The element $\beta = \alpha^b$ is then computed, using Proposition 4.2.10, by specifying b to be*

$$b = -ap^{i+lk}(p^{(r-l)k}+1) \mod (p^n-1) = -3\cdot 2^{2+1\cdot 2}\cdot(2^{(4-1)\cdot 2}+1) \mod (255) = 195.$$

By Theorem 4.2.11, it follows that $f(x) = T_k^n(\beta x^{p^i+p^j}) = T_2^8(\alpha^{195}x^{2^2+2^4})$ has an $(s, b) = (3, T_2^8(\alpha^{195}\alpha^{3(2^2+2^4)}))$-Frobenius translator.

4.2.3 Application to bent functions

In this section we provide a generalization of results in [69] by using Frobenius translators instead of standard linear translators, when $p = 2$. This allows to specify some new infinite classes of permutations and their inverses similarly to the approach in [69] which in turn gives rise to suitable quadruples of permutations from which secondary classes of bent functions can be deduced. Furthermore, we also solve an open problem [42] mentioned in the introduction which concerns the existence of quadruples of bent functions whose duals sum to one.

4.2.3.1 Generalization of certain permutations using Frobenius translators

The main result of the method in [67] is the condition imposed on the duals of four bent functions $f_1, \dots, f_4$ (where $f_4 = f_1 + f_2 + f_3$) given by $f_1^* + f_2^* + f_3^* + f_4^* = 0$, where f_i^* denotes the dual of f_i. This condition was shown to be both necessary and sufficient in order that the function $H = f_1f_2 + f_1f_3 + f_2f_3$ is bent. This naturally leads to the employment of the Maiorana-McFarland class of bent functions, where a bent function $f_j : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \to \mathbb{F}_2$ in this class is defined as $f_j(x, y) = Tr_1^n(x\phi_j(y) + \theta_j(y))$, for some permutation ϕ_j over $\mathbb{F}_{2^n}$ and arbitrary function θ_j over $\mathbb{F}_{2^n}$. It was shown in [70] that the above quadruples of bent functions are easily identified using a set of permutations defined by means of linear translators. We show that this approach is easily extended to cover Frobenius translators as well, which induces larger classes of these sets of permutations suitable to define new bent functions.

Proposition 4.2.12 (Generalization of Proposition 3, [69]) *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^k}$, let $L : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be an $\mathbb{F}_{2^k}$-linear permutation of $\mathbb{F}_{2^n}$, and let $g : \mathbb{F}_{2^k} \to \mathbb{F}_{2^k}$ be a permutation. Assume $\gamma \in \mathbb{F}_{2^n}^*$ and $a \in \mathbb{F}_{2^k}^*$ are such that γ is an (a,i)-Frobenius translator of f with respect to $\mathbb{F}_{2^k}$. Then the function $\phi : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$,*

$$\phi = L(x) + L(\gamma)\left(g(f(x)) + \frac{f(x)}{a}\right)^{2^{n-i}}, \tag{4.18}$$

is a permutation polynomial of $\mathbb{F}_{2^n}$ and

$$\phi^{-1} = L^{-1}(x) + \gamma a^{2^i}\left(g^{-1}\left(\frac{f(L^{-1}(x))}{a}\right) + f(L^{-1}(x))\right)^{2^{n-i}}.$$

Proof. Let us define $h : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ as

$$h(x) = x + \gamma\left(g(f(x)) + \frac{f(x)}{a}\right)^{2^{n-i}}.$$

Then, setting $y = x + \gamma\left(g(f(x)) + \frac{f(x)}{a}\right)^{2^{n-i}}$ leads to

$$f(y) = f\left(x + \gamma\left(g(f(x)) + \frac{f(x)}{a}\right)^{2^{n-i}}\right) = f(x) + a\left(g(f(x)) + \frac{f(x)}{a}\right)^{2^{n-i}2^i} = ag(f(x)).$$

Therefore, $f(x) = g^{-1}\left(\frac{f(y)}{a}\right)$ and

$$x = y + \gamma\left(g(f(x)) + \frac{f(x)}{a}\right)^{-2^i} = y + \gamma a^{-2^{n-i}}\left(f(y) + g^{-1}\left(\frac{f(y)}{a}\right)\right)^{2^{n-i}}.$$

This means that h is a permutation of $\mathbb{F}_{2^n}$ and its inverse is

$$h^{-1}(x) = x + \gamma a^{-2^{n-i}}\left(f(x) + g^{-1}\left(\frac{f(x)}{a}\right)\right)^{2^{n-i}}.$$

Now we can define ϕ as $\phi = L \circ h$,

$$\begin{aligned}\phi(x) &= L(h(x)) = L\left(x + \gamma\left(g(f(x)) + \frac{f(x)}{a}\right)^{2^{n-i}}\right)\\ &= L(x) + L(\gamma)\left(g(f(x)) + \frac{f(x)}{a}\right)^{2^{n-i}},\end{aligned}$$

and ϕ^{-1} as

$$\phi^{-1}(x) = h^{-1} \circ L^{-1} = L^{-1}(x) + \gamma a^{-2^{n-i}}\left(f(L^{-1}(x)) + g^{-1}\left(\frac{f(L^{-1}(x))}{a}\right)\right)^{2^{n-i}}.$$

□

In order to use these permutations in constructing new secondary classes of bent functions they must satisfy the condition $(\mathcal{A}_n)$, which was first introduced by Mesnager in [67] and later employed in [70].

Definition 4.2.13 *Three pairwise distinct permutations ϕ_1, ϕ_2, ϕ_3 of $\mathbb{F}_{2^n}$ are said to satisfy $(\mathcal{A}_n)$ if the following conditions hold:*

- $\psi = \phi_1 + \phi_2 + \phi_3$ *is a permutation of* $\mathbb{F}_{2^n}$,
- $\psi^{-1} = \phi_1^{-1} + \phi_2^{-1} + \phi_3^{-1}$.

The main challenge is to define suitable permutations ϕ_i as in (4.18) so that $\psi = \phi_1 + \phi_2 + \phi_3$ is also a permutation satisfying the condition $(\mathcal{A}_n)$, quite similarly to the approach taken in [69]. To achieve this, the simplest way is to use the same L, f, g for all $\phi_j, j \in \{1, 2, 3\}$, where the functions ϕ_i only differ in the term $L(\gamma_i)$. More precisely, the function f admits different (a, i)-Frobenius translators γ_i, for some fixed i and a, with the additional condition that $\gamma_1 + \gamma_2 + \gamma_3$ is also an (a, i)-Frobenius translator of f.

In the non-binary cases, finding such triples of Frobenius translators can be difficult, but in the binary case, the sum of any three (a, i)-Frobenius translators is again an (a, i)-Frobenius translator, as Corollary 4.2.3 proves.

Then

$$\psi(x) = L(x) + L(\gamma_1 + \gamma_2 + \gamma_3)\left(g(f(x)) + \frac{f(x)}{a}\right)^{2^{n-i}},$$

$$\psi^{-1}(x) = L^{-1}(x) + (\gamma_1 + \gamma_2 + \gamma_3)a^{-2^{n-i}}\left(f(L^{-1}(x)) + g^{-1}\left(\frac{f(L^{-1}(x))}{a}\right)\right)^{2^{n-i}},$$

and it is easily verified that the permutations ϕ_j satisfy the condition $(\mathcal{A}_n)$. This approach allows us to construct new bent functions using the result from [67, 70] below.

Proposition 4.2.14 ([67, 70]) *Let ϕ_1, ϕ_2, ϕ_3 be three pairwise distinct permutations satisfying $(\mathcal{A}_n)$. Then, the Boolean function $H : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \to \mathbb{F}_2$ defined by*

$$\begin{aligned} H(x, y) \quad = \quad & Tr_1^n(x\phi_1(y))Tr_1^n(x\phi_2(y)) + Tr_1^n(x\phi_1(y))Tr_1^n(x\phi_3(y)) + \\ & + Tr_1^n(x\phi_2(y))Tr_1^n(x\phi_3(y)) \end{aligned}$$

is bent. Furthermore, its dual function H^* is given by

$$\begin{aligned} H^*(x, y) \quad = \quad & Tr_1^n(\phi_1^{-1}(x)y)Tr_1^n(\phi_2^{-1}(x)y) + Tr_1^n(\phi_1^{-1}(x)y)Tr_1^n(\phi_3^{-1}(x)y) + \\ & + Tr_1^n(\phi_2^{-1}(x)y)Tr_1^n(\phi_3^{-1}(x)y). \end{aligned}$$

Notice that H is essentially defined as $H = f_1f_2 + f_1f_3 + f_2f_3$, where $f_j(x, y) = Tr_1^n(x\phi_j(y))$ so that $\theta_j(y) = 0$.

Remark 4.2.15 *Using the same techniques the following Propositions and Theorems from [69] can be generalized as well with minor modifications.*

- *Theorems* 1, 2, 3, 4 *in [69];*
- *Propositions* 4, 5, 6 *in [69].*

Due to similarity, we only discuss a generalization of Theorem 1 in [69] and give an example of bent functions constructed using this generalization.

Theorem 4.2.16 (Generalized Theorem 1, [69]) *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^k}$, let $L : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be an $\mathbb{F}_{2^k}$-linear permutation of $\mathbb{F}_{2^n}$, and let $g : \mathbb{F}_{2^k} \to \mathbb{F}_{2^k}$ be a permutation. Assume $\gamma_1, \gamma_2, \gamma_3 \in \mathbb{F}_{2^n}^*$ are all pairwise distinct (a,i)-Frobenius translators of f with respect to $\mathbb{F}_{2^k}$ ($a \in \mathbb{F}_{2^k}^*$) such that $\gamma_1+\gamma_2+\gamma_3$ is again an (a,i)-Frobenius translator. Suppose $\gamma_1+\gamma_2+\gamma_3 \neq 0$. Set $\rho(x) = \left(g(f(x)) + \frac{f(x)}{a}\right)^{2^{n-i}}$ and $\tilde{\rho}(x) = a^{2^i}\left(g^{-1}\left(\frac{f(x)}{a}\right) + f(x)\right)^{2^{n-i}}$. Then,*

$$\begin{aligned} H(x,y) &= Tr(xL(y)) + Tr(L(\gamma_1)x\rho(y))Tr(L(\gamma_2)x\rho(y)) + \\ &\quad Tr(L(\gamma_1)x\rho(y))Tr(L(\gamma_3)x\rho(y)) + Tr(L(\gamma_2)x\rho(y))Tr(L(\gamma_3)x\rho(y)) \end{aligned}$$

is bent. Furthermore, its dual function H^* is given by

$$\begin{aligned} H^*(x,y) &= Tr(yL^{-1}(x)) + Tr(\gamma_1 y\tilde{\rho}(L^{-1}(x)))Tr(\gamma_2 y\tilde{\rho}(L^{-1}(x))) + \\ &\quad +Tr(\gamma_1 y\tilde{\rho}(L^{-1}(x)))Tr(\gamma_3 y\tilde{\rho}(L^{-1}(x))) \\ &\quad +Tr(\gamma_2 y\tilde{\rho}(L^{-1}(x)))Tr(\gamma_3 y\tilde{\rho}(L^{-1}(x))). \end{aligned}$$

Proof. The only difference between Theorem 1 [69], and the generalized version presented here is the modification to ρ and $\tilde{\rho}$. In the original approach $\rho(x) = \left(g(f(x)) + \frac{f(x)}{a}\right)$ and $\tilde{\rho}(x) = a^{2^i}\left(g^{-1}\left(\frac{f(x)}{a}\right) + f(x)\right)$. Then, raising ρ and $\tilde{\rho}$ to the power of 2^{n-i}, as it has been done in the proof of Proposition 4.2.12, the proof of Theorem 4.2.16 is the same as the proof of Theorem 1, [69]. □

Example 4.2.3 *Let $n = 8$, ω be a primitive element of $\mathbb{F}_{2^8}$, L be an arbitrary $\mathbb{F}_{2^4}$-linear permutation of $\mathbb{F}_{2^8}$ and h be an arbitrary permutation of $\mathbb{F}_{2^4}$. Suppose we want the function $f : \mathbb{F}_{2^8} \to \mathbb{F}_{2^4}$ to be a binomial and to use it in the construction of a bent function using Theorem 4.2.16. Using only the standard definition of a linear translator, we would be forced to define $f(x) = Tr_4^8(x)$ according to Proposition 2 from [21]. But using Proposition 4.2.8 we can define $f(x) = x^{2^i} + x^{2^{i+4}}$ for any i with any $\gamma \in \mathbb{F}_{2^8}$ being an $(\gamma^{2^i} + \gamma^{2^{i+4}}, i)$-Frobenius translator of f.*

To use Theorem 4.2.16, we need to define three pairwise distinct (a,i)-Frobenius translators. So we need to find three distinct $\gamma_1, \gamma_2, \gamma_3$ such that

$$\gamma_1^{2^i} + \gamma_1^{2^{i+4}} = \gamma_2^{2^i} + \gamma_2^{2^{i+4}} = \gamma_3^{2^i} + \gamma_3^{2^{i+4}} = (\gamma_1+\gamma_2+\gamma_3)^{2^i} + (\gamma_1+\gamma_2+\gamma_3)^{2^{i+4}} = a.$$

This would imply that $\gamma_1, \gamma_2, \gamma_3, \gamma_1+\gamma_2+\gamma_3$ are all (a,i)-Frobenius translators. A quick computation shows that $\gamma_1+\gamma_2, \gamma_1+\gamma_3, \gamma_2+\gamma_3 \in \mathbb{F}_{2^4}$ is required. We select $\gamma_1 = \omega, \gamma_2 = \omega^3, \gamma_3 = \omega^{16}$ and, for example, if we fix $i = 2$, we get

$$\gamma_1^{2^i} + \gamma_1^{2^{i+4}} = \gamma_2^{2^i} + \gamma_2^{2^{i+4}} = \gamma_3^{2^i} + \gamma_3^{2^{i+4}} = (\gamma_1+\gamma_2+\gamma_3)^{2^i} + (\gamma_1+\gamma_2+\gamma_3)^{2^{i+4}} = \omega^{136}$$

and $\omega + \omega^3 + \omega^{16} = \omega^{48} \neq 0$.

Let $\rho, \tilde{\rho}$ and H be defined as in Theorem 4.2.16. It follows that H is a bent function.

4.2.3.2 New bent functions from suitable quadruples of bent functions

In difference to the above approach, which preserves the variable space of input functions, another method of constructing secondary bent functions on the extended variable space was recently proposed in [42]. Nevertheless, quite a similar set of conditions on initial bent functions f_1, f_2, f_3, which was left as an open problem in [42], is imposed in order that the resulting function F defined on a larger variable space is bent.

Open Problem 3 *[42] Find such bent functions f_1, f_2, f_3 that $f_1 + f_2 + f_3 = f_4$ is again a bent function and $f_1^* + f_2^* + f_3^* + f_4^* = 1$.*

The design rationale is illustrated by Example 4.9 [42], where using $f_1, f_2, f_3 : \mathbb{F}_{2^n} \to \mathbb{F}_2$ that satisfy the above condition, implies that $F : \mathbb{F}_{2^n} \times \mathbb{F}_2 \times \mathbb{F}_2$ defined as

$$F(X, y_1, y_2) = f_1(X) + y_1(f_1 + f_3)(X) + y_2(f_1 + f_2)(X)$$

is bent.

Below we present a construction that solves this open problem and gives an example of its use.

Theorem 4.2.17 *Let $f_i(X) = f_i(x, y) = Tr(x\phi_i(y)) + h_i(y)$ for $i \in \{1, 2, 3\}$, where ϕ_i satisfy the condition $(\mathcal{A}_n)$ and $x, y \in \mathbb{F}_{2^{n/2}}$. If the functions h_i satisfy*

$$h_1(\phi_1^{-1}(x)) + h_2(\phi_2^{-1}(x)) + h_3(\phi_3^{-1})(x)) + (h_1 + h_2 + h_3)((\phi_1 + \phi_2 + \phi_3)^{-1}(x)) = 1, \tag{4.19}$$

then f_1, f_2, f_3 are solutions to Open Problem 3.

Proof. Let $f_4 = f_1 + f_2 + f_3 = Tr(x(\phi_1 + \phi_2 + \phi_3)(y)) + (h_1 + h_2 + h_3)(y)$. Since the permutations ϕ_i satisfy the condition $(\mathcal{A}_n)$, their sum is again a permutation and f_4 is a bent Maiorana-McFarland function. Its dual is

$$f_4^* = Tr(y(\phi_1 + \phi_2 + \phi_3)^{-1}(x)) + (h_1 + h_2 + h_3)((\phi_1 + \phi_2 + \phi_3)^{-1}(x)).$$

Then,

$$\begin{aligned} f_1^* + f_2^* + f_3^* + f_4^* &= Tr(y(\phi_1^{-1}(x))) + h_1(\phi_1^{-1}(x)) + Tr(y(\phi_2^{-1}(x))) + h_2(\phi_2^{-1}(x)) + \\ &\quad + Tr(y(\phi_3^{-1}(x))) + h_3(\phi_3^{-1}(x)) + Tr(y(\phi_1 + \phi_2 + \phi_3)^{-1}(x)) + \\ &\quad + (h_1 + h_2 + h_3)(\phi_1 + \phi_2 + \phi_3)^{-1}(x)) \\ &= Tr(y((\phi_1^{-1} + \phi_2^{-1} + \phi_3^{-1} + (\phi_1 + \phi_2 + \phi_3)^{-1})(x))) + \\ &\quad + h_1(\phi_1^{-1}(x)) + h_2(\phi_2^{-1}(x)) + h_3(\phi_3^{-1}(x)) + \\ &\quad + (h_1 + h_2 + h_3)((\phi_1 + \phi_2 + \phi_3)^{-1}(x)) \\ &= h_1(\phi_1^{-1}(x)) + h_2(\phi_2^{-1}(x)) + h_3(\phi_3^{-1})(x)) + \\ &\quad + (h_1 + h_2 + h_3)((\phi_1 + \phi_2 + \phi_3)^{-1}(x)) \\ &= 1. \end{aligned}$$

□

The following example illustrates the procedure of defining three suitable bent functions on $\mathbb{F}_{2^n}$ used to specify a bent function F on $\mathbb{F}_{2^n} \times \mathbb{F}_2 \times \mathbb{F}_2$. The condition

(4.19) imposed on h_i in the definition of suitable $f_i(x,y) = Tr(x\phi_i(y)) + h_i(y)$ turns out to be easily satisfied.

Example 4.2.4 *Let α be a primitive element of $\mathbb{F}_{2^6}$. For simplicity, we define the permutations ϕ_i over $\mathbb{F}_{2^6}$ as*

$$\phi_1(y) = y + \alpha, \qquad \phi_1(y) = y + \alpha^2, \qquad \phi_1(y) = y + \alpha^3,$$

which are self-inverse and it is straightforward to verify that they satisfy the condition $(\mathcal{A}_n)$. Define the Boolean functions $h_2, h_3 : \mathbb{F}_{2^6} \to \mathbb{F}_2$ as

$$h_2(y) = 0, \qquad h_3(y) = 1.$$

After, we define the Boolean function h_1 in such a way that

$$\begin{aligned} h_1(\phi_1^{-1}(y)) + h_2(\phi_2^{-1}(y)) + h_3(\phi_3^{-1})(y)) + (h_1 + h_2 + h_3)((\phi_1 + \phi_2 + \phi_3)^{-1}(y)) &= 1 \\ h_1(\phi_1^{-1}(y)) + (h_1)((\phi_1 + \phi_2 + \phi_3)^{-1}(y)) &= 1 \\ h_1(y + \alpha) + (h_1)(y + \alpha + \alpha^2 + \alpha^3) &= 1. \end{aligned}$$

This condition is easily satisfied. We just construct the truth table of the Boolean function h_1 in such a way that for every $y \in \mathbb{F}_{2^6}$ we have $h_1(y) = h_1(y + \alpha^2 + \alpha^3) + 1$. Now we construct bent Maiorana-McFarland functions $f_i : \mathbb{F}_{2^6} \times \mathbb{F}_{2^6} \to \mathbb{F}_2, f_i(x,y) = Tr(x\phi_i(y)) + h_i(y)$ and use them in the construction from Example 4.9, *[42].*

We define $F : \mathbb{F}_{2^{12}} \times \mathbb{F}_2 \times \mathbb{F}_2 \to \mathbb{F}_2$,

$$F(X, y_1, y_2) = f_1(X) + y_1(f_1 + f_3)(X) + y_2(f_1 + f_2)(X).$$

The function F was implemented and tested using the programming package Magma. It was confirmed that F is a bent function.

Remark 4.2.18 *In [81, Remark 3], a method to define anti-self-dual bent functions $f_1, f_2, f_3, f_1+f_2+f_3$ (thus $f_i^* = f_i+1$) is given which implies that $f_1^*+f_2^*+f_3^+ + f_4^* = 0$. Another construction of f_1, f_2, f_3 that satisfies this condition can be found in [94, Section 5], where f_1, f_2, f_3 all belong to the partial spread ($\mathcal{PS}$) class of Dillon [34]. It is based on a well-known property of the $\mathcal{PS}$ class that the dual f^* of a $\mathcal{PS}$ function f is defined by substituting all the disjoint $\frac{n}{2}$-dimensional subspaces in its support by their orthogonal subspaces [12]. It follows that $f_4^* = f_1^* + f_2^* + f_3^*$ and consequently $f_1^* + f_2^* + f_3^* + f_4^* = 0$.*

4.2.3.3 Some new infinite families of bent functions

In Chapter 4.1 many infinite families of permutations based on linear translators were introduced, some of which were already generalized in previous sections. It turns that in the binary case some of those families satisfy the condition $(\mathcal{A}_n)$.

Proposition 4.2.19 ([21]) *Let $k > 1 (n = rk)$, $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^k}$, $g : \mathbb{F}_{2^k} \to \mathbb{F}_{2^k}$, and let γ be a 0-linear translator. Then*

$$F(x) = x + \gamma g(f(x))$$

is an involution.

Note that if γ is a 0-translator it is irrelevant to differentiate between linear and Frobenius translators.

Proposition 4.2.20 *Let $\gamma_1, \gamma_2, \gamma_3$ be pairwise distinct 0-linear translators, and let $F_i(x) = x + \gamma_i g(f(x))$ for $i \in \{1, 2, 3\}$. Then the functions F_i satisfy the condition $\mathcal{A}_n$.*

Proof. By Proposition 4.2.2, $\gamma_1 + \gamma_2 + \gamma_3$ must again be a 0-linear translator.

$$\begin{aligned} F_1(x) + F_2(x) + F_3(x) &= x + \gamma_1 g(f(x)) + x + \gamma_2 g(f(x)) + x + \gamma_3 g(f(x)) \\ &= x + (\gamma_1 + \gamma_2 + \gamma_3) g(f(x)) \end{aligned}$$

Then, by Proposition 4.2.19, $F_1 + F_2 + F_3$ is again a permutation and an involution. This immediately implies that the second requirement of condition $(\mathcal{A}_n)$ is satisfied as well. □

It therefore follows that we can use the above presented permutations in constructing new families of bent functions, as was done in Proposition 4.2.14. Since the proof also follows the same steps it is in this case skipped.

Theorem 4.2.21 *Let $k > 1 (n = rk)$, $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^k}$, $g : \mathbb{F}_{2^k} \to \mathbb{F}_{2^k}$, and let γ_i be pairwise distinct 0-linear translators. Then*

$$\begin{aligned} H(x, y) &= Tr(xy) + Tr(\gamma_1 g(f(y)))Tr(\gamma_2 g(f(y))) + Tr(\gamma_1 g(f(y)))Tr(\gamma_3 g(f(y))) + \\ &+ Tr(\gamma_2 g(f(y)))Tr(\gamma_3 g(f(y))) \end{aligned}$$

is a self-dual bent function.

Another family of permutations that turns out to satisfy the condition $(\mathcal{A}_n)$ was introduced in [21]:

Corollary 4.2.22 ([21]) *Let $k > 1 (n = rk)$, L be any $\mathbb{F}_{2^k}$-linear permutation, $f(x) = T_k^n(\beta x)$ such that $Tr(\beta\gamma) = 0$. Then the functions*

$$F(x) = L(x) + L(\gamma) g(Tr_k^n(\beta x))$$

are permutations for any $g : \mathbb{F}_{2^k} \to \mathbb{F}_{2^k}$. Moreover,

$$F^{-1}(x) = L^{-1}(x) + L(\gamma) g(Tr_k^n(\beta L^{-1}(x))).$$

In a similar way as before we can show that $F_i(x) = L(x) + L(\gamma_i) g(Tr_k^n(\beta x))$ satisfy the condition $(\mathcal{A}_n)$ if $Tr_k^n(\gamma_i \beta) = 0$. It follows that these permutations can also be used in constructing new families of bent functions.

Theorem 4.2.23 *Let L be any $\mathbb{F}_{2^k}$-linear permutation,$f(x) = T_k^n(\beta x)$, $g : \mathbb{F}_{2^k} \to \mathbb{F}_{2^k}$, and let γ_i be such that $Tr_k^n(\gamma_i \beta) = 0$. Then*

$$\begin{aligned} H(x,y) &= Tr(xL(y)) + Tr(L(\gamma_1)g(Tr_k^n(\beta x)))Tr(L(\gamma_2)g(Tr_k^n(\beta x))) + \\ &\quad + Tr(L(\gamma_1)g(Tr_k^n(\beta x)))Tr(L(\gamma_3)g(Tr_k^n(\beta x))) + \\ &\quad + Tr(L(\gamma_2)g(Tr_k^n(\beta x)))Tr(L(\gamma_3)g(Tr_k^n(\beta x))) \end{aligned}$$

is a bent function and its dual is

$$\begin{aligned} \tilde{H}(x,y) &= Tr(yL^{-1}(x)) + Tr(L(\gamma_1)g(Tr_k^n(\beta L^{-1}(x))))Tr(L(\gamma_2)g(Tr_k^n(\beta L^{-1}(x)))) + \\ &\quad + Tr(L(\gamma_1)g(Tr_k^n(\beta L^{-1}(x))))Tr(L(\gamma_3)g(Tr_k^n(\beta L^{-1}(x)))) + \\ &\quad + Tr(L(\gamma_2)g(Tr_k^n(\beta L^{-1}(x))))Tr(L(\gamma_3)g(Tr_k^n(\beta L^{-1}(x)))). \end{aligned}$$

Chapter 5

Infinite classes of vectorial plateaued functions, permutations, and complete permutations

Boolean plateaued functions and vectorial functions with plateaued components have a significant impact in many applications such as cryptography, sequences for communications, and related combinatorics and designs. Boolean plateaued functions were introduced in [96] as a class of functions characterized by the property of having at most three values in its Walsh spectra. In particular, the semi-bent functions play a significant role in certain cryptographic primitives and additionally these functions constitute the component functions of certain mappings such as almost perfect nonlinear (APN) mappings with Gold exponent. Nevertheless, while there are a few known generic constructions of Boolean plateaued functions (a nice survey can be found in [11]) little is known about vectorial plateaued functions. In [11], several characterizations of those vectorial functions whose components are all plateaued (with possibly different amplitudes) were derived. In particular, it was shown that an extension of the Maiorana-McFarland class gives rise to a vectorial plateaued functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$. Namely, using a permutation π over $\mathbb{F}_{2^m}$ and two arbitrary functions $\phi, \psi : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ it could be shown that $F : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ defined by $F(x, y) = (x\pi(y) + \phi(y), x\pi^{2^i}(y) + \psi(y))$ is plateaued.

Even though the above approach gives an infinite class of vectorial plateaued functions the component functions of F are bent and therefore they are not balanced. As a consequence this approach can never give rise to permutations due to the property of permutations that all linear combinations of its component functions are balanced Boolean functions. Therefore, we consider an alternative design method of vectorial plateaued functions which specifies the component functions of F in such a way so that all linear combinations of them are balanced Boolean functions, thus implying that F is a permutation. This way two infinite classes of non-quadratic permutations are proposed but there are many variations of the proposed method which may give many more infinite classes. The framework is also extendible in terms of getting varying degree of these permutations since it is based on a suitable separation of the variable space. More precisely, the component functions can be seen as a concatenation of linear functions from some fixed variable space whose size can be adjusted to accommodate the design of permutations of even higher degree. The polynomial form, as a univariate representation over the corresponding finite field, appears to be complicated and it is retrieved using Lagrange interpolation. On the other hand, the algebraic normal form (ANF) description of the component functions is usually simple.

Complete mappings are a particular class of permutations characterized by the property that both $F(x)$ and $F(x)+x$ are permutation polynomials over some finite field $\mathbb{F}_{2^n}$. Complete mappings have got attention in several works [72, 52, 92, 39] and it appears to be a topic of current research interest as well, see [2, 85] and the references therein. In particular, for the well-known Even-Mansour block cipher that uses a public n-bit permutation $F(x)$ and two n-bit secret keys k_1, k_2, and encrypts an n-bit plaintext x by computing $F(x + k_1) + k_2$, it was demonstrated that this cipher usually suffered from the attacks that rely on the non-uniform behavior of $F(x) + x$. In order to resist these attacks, the distribution of $F(x) + x$ should be uniform, i.e., $F(x) + x$ should also be a permutation (see the work of [39]).

Due to the additional requirement that $F(x) + x$ is a permutation as well, the design of component functions of F is certainly more complicated. However, we demonstrate that even complete permutations can be generated using the same framework as in the case of ordinary permutations. We exhibit one infinite class of complete permutations but nevertheless the same method may give many more (affinely non-equivalent) classes, though we do not pursue this issue further. The polynomial form of this class of permutations is again retrieved through Lagrange interpolation and it is very complex, though the ANF of the component functions is somewhat simple.

5.1 Constructing permutations from $\mathcal{M}$ class

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ and $F = (f_1, \dots, f_n)$, where f_i are component functions of F. It is well-known [58, Theorem 7.7] that F is a permutation over $\mathbb{F}_{2^n}$ if and only if,

$$\sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(\lambda F(x))} = 0, \tag{5.1}$$

for any $\lambda \in \mathbb{F}_{2^n}^*$, where Tr denotes the absolute trace function. In terms of the vector space representation this is equivalent to the requirement that $F_\lambda = \lambda_1 f_1 \oplus \dots \oplus \lambda_n f_n$ is a balanced function for any $\lambda = (\lambda_1, \dots, \lambda_n) \in \mathbb{F}_2^{n*}$. Our goal is to specify the component functions $f_1, \dots, f_n$ of F so that the above condition is satisfied. To achieve this we use the Maiorana-McFarland class of Boolean functions in $n = s + k$ variables defined as,

$$f(y, x) = \phi(y) \cdot x \oplus g(y), \quad x \in \mathbb{F}_2^k, y \in \mathbb{F}_2^s, \tag{5.2}$$

where ϕ is any mapping from $\mathbb{F}_2^s$ to $\mathbb{F}_2^k$, and $g \in \mathcal{B}_s$ is arbitrary. Note that for fixed y, the restriction of f (also called a subfunction of f) is an affine function in x. The following result is well-known and the interested reader can find the proof in e.g. [19].

Theorem 5.1.1 *[19] Let $n = s + k$ and $f(y, x) = \phi(y) \cdot x \oplus g(y)$, for $x \in \mathbb{F}_2^k, y \in \mathbb{F}_2^s$, where $\phi : \mathbb{F}_2^s \to \mathbb{F}_2^k$ and $g \in \mathcal{B}_s$ is arbitrary. Then, if $\phi : \mathbb{F}_2^s \to \mathbb{F}_2^k$ is injective the Walsh spectra of f is three valued, that is, $W_f(\omega) \in \{0, \pm 2^k\}$. In other words, f is a plateaued function.*

In terms of algebraic degree we recall the result from [29].

Theorem 5.1.2 *The notation is the same as in Theorem 5.1.1. Assuming ϕ is injective, the degree of f is $s+1$ if and only if $\bigoplus_{y\in\mathbb{F}_2^s} \phi(y) \neq \mathbf{0}$, where $\mathbf{0} = (0, \dots, 0) \in \mathbb{F}_2^s$.*

For the rest of this section we fix $(y, x) \in \mathbb{F}_2^n, x \in \mathbb{F}_2^{n-2}, y \in \mathbb{F}_2^2$, and consider the specification of the Maiorana McFarland component functions f_i of the function F, where $f_i(y, x) = \phi_i(y) \cdot x \oplus g_i(y), \phi_i : \mathbb{F}_2^2 \to \mathbb{F}_2^{n-2}$ and $g_i : \mathbb{F}_2^2 \to \mathbb{F}_2$ for $i = 1, \dots, n$, so that F_λ is balanced. In the following constructions we further specify the functions ϕ_i and g_i.

For simplicity we assume $g_i(y) = 0$ though it is formally true only for $f_1, \dots, f_{n-2}$. Our first approach gives a class of permutations over $\mathbb{F}_2^n$, whose component functions are all plateaued and non-quadratic (their algebraic degree is 3). This method employs the rotation of the standard basis of $\mathbb{F}_2^{n-2}$, that is, $\{e_1, \dots, e_{n-2}\}$, where e_i has its only non-zero value (equal to 1) at position i.

Construction 1 *Let $e_i \in \mathbb{F}_2^{n-2}$, for $i = 1, \dots, n-2$, form the canonical basis of $\mathbb{F}_2^{n-2}$, where $n \geq 7$. For any $y \in \mathbb{F}_2^2$ define $\phi(y)$ as below,*

y	$\phi_1(y)$	$\phi_2(y)$	$\cdots$	$\phi_{n-2}(y)$	$\phi_{n-1}(y)$	$\phi_n(y)$
$(0,0)$	e_1	e_2	$\cdots$	e_{n-2}	$(\phi_{n-2} \oplus \phi_1)(y)$	$(\phi_{n-2} \oplus \phi_1)(y)$
$(0,1)$	e_2	e_3	$\cdots$	e_1	$(\phi_{n-2} \oplus \phi_1)(y)$	$(\phi_{n-2} \oplus \phi_1)(y) + 1$
$(1,0)$	e_3	e_4	$\cdots$	e_2	$(\phi_{n-2} \oplus \phi_1)(y) + 1$	$(\phi_{n-2} \oplus \phi_1)(y) + 1$
$(1,1)$	e_4	e_5	$\cdots$	e_3	$(\phi_{n-2} \oplus \phi_1)(y) + 1$	$(\phi_{n-2} \oplus \phi_1)(y)$

Let $f_i(y, x) = \phi_i(y) \cdot x \oplus g_i(y)$ for $i = 1, \dots, n$, where $g_i(y) = 0$, for $i = 1, \dots, n-2$. In particular, "$(\phi_{n-2} \oplus \phi_1)(y) + 1$" means that for some fixed y we have $f_i(y, x) = (\phi_{n-2} \oplus \phi_1)(y) \cdot x + 1$, for $i = n-1, n$. In other words, the functions f_{n-1} and f_n have some component functions which are affine. For instance, the function $g_n(y) \neq 0$ since $g_n(0, 1) = g_n(1, 0) = 1$ and consequently $f_n(y, x) = \phi_n(y) \cdot x \oplus g_n(y)$ is affine function for fixed $y \in \{(0, 1), (1, 0)\}$.

Remark 5.1.1 *The use of the above notation appears to be simpler and more compact than fully specifying subfunctions in terms of both $\phi_i(y)$ and $g_i(y)$.*

Theorem 5.1.3 *Let f_i be defined as in Construction 1. Then, each f_i is a plateaued function with spectra $\{0, \pm 2^{n-2}\}$. Furthermore, the algebraic degree of each f_i is 3 and the same is true for any non-zero linear combination of f_i apart from $f_{n-1} \oplus f_n, f_1 \oplus f_{n-2} \oplus f_{n-1}$, and $f_1 \oplus f_{n-2} \oplus f_n$ in which case the degree is 1. Also, $F = (f_1, \dots, f_n)$ is a permutation over $\mathbb{F}_2^n$, i.e., F_λ is balanced for any $\lambda \in \mathbb{F}_2^{n*}$.*

Proof. It is clear that each ϕ_i is injective and by Theorem 5.1.1 it follows that f_i is plateaued with spectra $\{0, \pm 2^{n-2}\}$. Moreover, $deg(f_i) = s+1 = 3$ by Theorem 5.1.2, since $\bigoplus_{y \in \mathbb{F}_2^s} \phi_i(y) \neq \mathbf{0}$ for any i. For each fixed y, the values $\phi_1(y), \ldots, \phi_{n-2}(y)$ form the standard basis of $\mathbb{F}_2^{n-2}$. For any $\alpha \in \mathbb{F}_2^{n-2*}$, consider the linear combinations of the form,

$$\alpha_1 f_1(y,x) \oplus \ldots \oplus \alpha_{n-2} f_{n-2}(y,x) = (\alpha_1 \phi_1(y) \oplus \ldots \oplus \alpha_{n-2}\phi_{n-2}(y)) \cdot x = \phi_\alpha(y) \cdot x.$$

Clearly, $\phi_\alpha(y)$ is by construction injective and $\phi_\alpha(y) \neq \mathbf{0}$ for any $y \in \mathbb{F}_2^2$. Thus, as a concatenation of non-zero linear functions any F_α is balanced.

The functions ϕ_{n-1} and ϕ_n are defined in such a way as to preserve the balance property. Indeed, by specifying ϕ_{n-1} and ϕ_n through ϕ_1 and ϕ_{n-2} along with taking a complement of certain linear functions, one can readily check that F_λ is balanced for any $\lambda \in \mathbb{F}_2^{n*}$. Thus, $F = (f_1, \ldots, f_n)$ is a permutation. Finally, we notice that $f_{n-1} \oplus f_n$ is a concatenation of four constant functions, namely $\mathbf{0}||\mathbf{1}||\mathbf{0}||\mathbf{1}$, where $\mathbf{0}, \mathbf{1}$ are constant vectors of length 2^{n-2}. Therefore, $\deg(f_{n-1} \oplus f_n) = 1$ and the same is true for $f_1 \oplus f_{n-2} \oplus f_{n-1}$ and $f_1 \oplus f_{n-2} \oplus f_n$.

□

Notice that by permuting component functions $f_1, \ldots, f_n$ along with permuting $\phi(y)$ (row-wise) we easily get $n!4!$ many permutations, for any $n \geq 4$ (since we need f_n, f_{n-1} and at least 2 more component functions with which to compose them). Nevertheless, we can find many such constructions and below we consider (only) one different approach.

Let the function l denote the left shift by one coordinate, i.e., $l((u_n, u_{n-1}, \ldots, u_1)) = (u_{n-1}, \ldots, u_1, 0)$. Furthermore, in the construction below we adopt the convention that $l^{n-4}(a) = l^{n-4}(b) = l^{n-4}(c) = l^{n-4}(d) = (10\ldots0)$.

For convenience, we define a set of vectors of length $n-2$ needed in the construction by,

$$a = (0\cdots010),\;\; b = (0\cdots0110),\;\; c = (0\cdots01110),\;\; d = (0\cdots011110),\;\; e_1 = (00\cdots01).$$

Construction 2 *For any $y \in \mathbb{F}_2^2$ define $\phi(y)$ as below,*

y	$\phi_1(y)$	$\phi_2(y)$	$\phi_3(y)$	$\phi_4(y)$	$\ldots$	$\phi_{n-3}(y)$	$\phi_{n-2}(y)$	$\phi_{n-1}(y)$	$\phi_n(y)$
$(0,0)$	a	$l(a)$	$l^2(a)$	$l^3(a)$	$\ldots$	$l^{n-4}(a)$	e_1	$(\phi_{n-2}+\phi_1)(y)$	$(\phi_{n-2}+\phi_2)(y)$
$(0,1)$	e_1	b	$l(b)$	$l^2(b)$	$\ldots$	$l^{n-5}(b)$	$l^{n-4}(b)$	$(\phi_{n-2}+\phi_1)(y)$	$(\phi_{n-2}+\phi_2)(y)+1$
$(1,0)$	$l^{n-4}(c)$	e_1	c	$l(c)$	$\ldots$	$l^{n-6}(c)$	$l^{n-5}(c)$	$(\phi_{n-2}+\phi_1)(y)+1$	$(\phi_{n-2}+\phi_2)(y)+1$
$(1,1)$	$l^{n-5}(d)$	$l^{n-4}(d)$	e_1	d	$\ldots$	$l^{n-7}(d)$	$l^{n-6}(d)$	$(\phi_{n-2}+\phi_1)(y)+1$	$(\phi_{n-2}+\phi_2)(y)$

Finally, let $f_i(y,x) = \phi_i(y) \cdot x + g_i(y)$ for $i = 1, \ldots, n$, where $g_i(y) = 0$, for $i = 1, \ldots, n-2$, and $g_i(y)$, for $i = n-1, n$, is as specified above. In particular, "$(\phi_{n-2} \oplus \phi_1)(y) + 1$" means that for some fixed y we have $f_i(y,x) = (\phi_{n-2} \oplus \phi_1)(y) \cdot x + 1$, for $i = n-1, n$.

Theorem 5.1.4 *Let f_i be defined as in Construction 2. Then, each f_i is a plateaued function with spectra $\{0, \pm 2^{n-2}\}$. Furthermore, the algebraic degree of any F_λ is 3 apart from $f_1 \oplus f_{n-2} \oplus f_{n-1}$, $f_2 \oplus f_{n-2} \oplus f_n$, and $f_{n-1} \oplus f_n$ which are linear. Also, $F = (f_1, \ldots, f_n)$ is a permutation over $\mathbb{F}_2^n$.*

Proof. The proof follows the same lines of reasoning as the proof of Theorem 5.1.3 by checking the balancedness of F_λ. □

Example 5.1.1 *Let $n = 7$. Then the component functions f_i of our permutation are defined through ϕ_i as follows:*

y	$\phi_1(y)$	$\phi_2(y)$	$\phi_3(y)$	$\phi_4(y)$	$\phi_5(y)$	$\phi_6(y)$	$\phi_7(y)$
$(0,0)$	(00010)	(00100)	(01000)	(10000)	(00001)	(00011)	(00101)
$(0,1)$	(00001)	(00110)	(01100)	(11000)	(10000)	(10001)	$(10110)+1$
$(1,0)$	(10000)	(00001)	(01110)	(11100)	(11000)	$(01000)+1$	$(11001)+1$
$(1,1)$	(11000)	(10000)	(00001)	(11110)	(11100)	$(00100)+1$	$(01100).$

Using MAGMA software to perform the Lagrange interpolation and a primitive polynomial $p(z) = z^7+z+1$ over $\mathbb{F}_2$, the univariate polynomial form of F specified above is given as :

$$\begin{aligned} F(y) \quad = \quad & g^{20}y^{112} + g^{99}y^{104} + g^{34}y^{100} + g^{58}y^{98} + g^{63}y^{97} + g^{49}y^{96} + g^{61}y^{88} + g^{10}y^{84} + \\ & g^{23}y^{81} + g^{24}y^{80} + g^{77}y^{76} + g^{99}y^{74} + g^{116}y^{73} + g^{60}y^{72} + g^{48}y^{70} + g^{22}y^{69} + \\ & g^{95}y^{68} + g^{61}y^{67} + g^{123}y^{66} + g^{118}y^{65} + g^{77}y^{64} + g^{123}y^{56} + g^{8}y^{52} + g^{78}y^{50} + \\ & g^{25}y^{49} + g^{122}y^{48} + g^{43}y^{44} + g^{58}y^{42} + g^{7}y^{41} + y^{40} + g^{83}y^{38} + g^{37}y^{37} + g^{67}y^{36} + \\ & g^{101}y^{35} + g^{25}y^{34} + g^{102}y^{33} + g^{39}y^{32} + g^{116}y^{28} + g^{119}y^{26} + g^{63}y^{25} + g^{126}y^{24} + \\ & g^{68}y^{22} + g^{39}y^{21} + g^{77}y^{20} + g^{81}y^{19} + g^{48}y^{18} + g^{29}y^{17} + g^{91}y^{16} + g^{37}y^{14} + g^{26}y^{13} + \\ & g^{123}y^{12} + g^{52}y^{11} + g^{50}y^{10} + g^{104}y^{9} + g^{119}y^{8} + g^{13}y^{7} + g^{18}y^{6} + g^{10}y^{5} + \\ & g^{117}y^{4} + g^{32}y^{3} + g^{27}y^{2} + g^{35}y, \end{aligned}$$

where g is the primitive root of $p(z)$. Notice that the maximum Hamming weight of the exponents is equal to 3, thus the algebraic degree of $\deg_{alg}(F) = 3$.

5.1.1 Noncubic permutations

When y is of dimension larger than 2 there exist many different ways to generalize the construction and increase the degree of the derived permutations. One of the methods is presented below.

Construction 3 *Let $e_i \in \mathbb{F}_2^{n-3}$, for $i = 1, \dots, n-3$. For any $y \in \mathbb{F}_2^3$ define $\phi(y)$ as below,*

y	$\phi_1(y)$	$\phi_2(y)$	$\cdots$	$\phi_{n-3}(y)$	$\phi_{n-2}(y)$	$\phi_{n-1}(y)$	$\phi_n(y)$
$(0,0,0)$	e_1	e_2	$\cdots$	e_{n-3}	$(\phi_{n-3}\oplus\phi_1)(y)$	$(\phi_{n-3}\oplus\phi_1)(y)$	$(\phi_{n-2}\oplus\phi_1)(y)$
$(0,0,1)$	e_2	e_3	$\cdots$	e_1	$(\phi_{n-3}\oplus\phi_1)(y)$	$(\phi_{n-3}\oplus\phi_1)(y)$	$(\phi_{n-3}\oplus\phi_1)(y)+1$
$(0,1,0)$	e_3	e_4	$\cdots$	e_2	$(\phi_{n-3}\oplus\phi_1)(y)$	$(\phi_{n-3}\oplus\phi_1)(y)+1$	$(\phi_{n-3}\oplus\phi_1)(y)$
$(0,1,1)$	e_4	e_5	$\cdots$	e_3	$(\phi_{n-3}\oplus\phi_1)(y)$	$(\phi_{n-3}\oplus\phi_1)(y)+1$	$(\phi_{n-3}\oplus\phi_1)(y)+1$.
$(1,0,0)$	e_5	e_6	$\cdots$	e_4	$(\phi_{n-3}\oplus\phi_1)(y)+1$	$(\phi_{n-3}\oplus\phi_1)(y)$	$(\phi_{n-3}\oplus\phi_1)(y)$
$(1,0,1)$	e_6	e_7	$\cdots$	e_5	$(\phi_{n-3}\oplus\phi_1)(y)+1$	$(\phi_{n-3}\oplus\phi_1)(y)$	$(\phi_{n-3}\oplus\phi_1)(y)+1$
$(1,1,0)$	e_7	e_8	$\cdots$	e_6	$(\phi_{n-3}\oplus\phi_1)(y)+1$	$(\phi_{n-3}\oplus\phi_1)(y)+1$	$(\phi_{n-3}\oplus\phi_1)(y)$
$(1,1,1)$	e_8	e_9	$\cdots$	e_7	$(\phi_{n-3}\oplus\phi_1)(y)+1$	$(\phi_{n-3}\oplus\phi_1)(y)+1$	$(\phi_{n-3}\oplus\phi_1)(y)+1$

Let $f_i(y,x) = \phi_i(y) \cdot x \oplus g_i(y)$ for $i = 1, \ldots, n$, where $g_i(y) = 0$, for $i = 1, \ldots, n-3$, and $g_i(y)$, for $i = n-2, n-1, n$, is as specified above. In particular, "$(\phi_{n-2} \oplus \phi_1)(y) + 1$" means that same as in constructions 1 and 2.

Note that in case $n - |y| = |x| < 9$, where by $|y|$ we mean the dimension of the vector, $e_{(i \mod |x|)}$ is used instead of e_i.

Theorem 5.1.5 *Let f_i be defined as in Construction 3. Then, each f_i is a plateaued function with spectra $\{0, \pm 2^{n-3}\}$. Furthermore, the algebraic degree of any F_λ is 4 apart from some linear combinations of $f_1, f_{n-3}, f_{n-2}, f_{n-1}, f_n$ which are linear. Also, $F = (f_1, \ldots, f_n)$ is a permutation over $\mathbb{F}_2^n$.*

Proof. The proof follows the same lines of reasoning as the proof of Theorem 5.1.3 by checking the balancedness of F_λ. □

Example 5.1.2 *Let $n = 8$ and y be of length 3. Defining the component functions f_i as in Construction 3 and using MAGMA software to perform the Lagrange interpolation (with a primitive polynomial $p(z) = z^8 + z^4 + z^3 + z^2 + 1$ over $\mathbb{F}_2$), the univariate polynomial form of F can be found. It can be verified that $\deg_{alg}(F) = 4$. Due to space limitation we do not list the polynomial terms of F.*

Remark 5.1.2 *Using the similar approach as in Constructions 1 to 3, one can design permutations $F = (f_1, \ldots, f_n)$ over $\mathbb{F}_2^n$, where each f_i is a plateaued function with spectra $\{0, \pm 2^{n-j}\}, (4 \leq j < n/2)$.*

5.2 Complete permutations

Whereas any permutation over finite field can be specified by properly assigning 2^n tuples $(x, F(x))$ and its polynomial form can be retrieved using Lagrange interpolation, the situation is not the same when complete permutations are considered. However, we show that the above construction methods can be used for specifying the component functions in such a way that F is a complete permutation. Apart from requiring that F_λ is balanced for $F = (f_1, \ldots, f_n)$ the additional request is that $F(x) + x$ is a permutation, when F is considered as a polynomial over finite field. In vector space representation, viewing $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, the latter condition means that,

$$\sum_{x \in \mathbb{F}_2^n} (-1)^{\lambda \cdot (F(x) \oplus x)} = \sum_{x \in \mathbb{F}_2^n} (-1)^{\lambda_1 (f_1(x) \oplus x_1) \oplus \cdots \oplus \lambda_n (f_n(x) \oplus x_n)} = 0,$$

for any $\lambda \in \mathbb{F}_2^{n*}$. In other words, we must ensure that all linear combinations of $f_1(x) \oplus x_1, \ldots, f_n(x) \oplus x_n$ are balanced as well. Since we are using two variables to represent f_i, we denote these functions as $f_i(y,x) \oplus (y,x)_i$, where$(y,x)_i$ denotes that the i-th variable in $(y_1, \ldots, y_s, x_1, \ldots, x_k)$.

The construction method described below relies heavily on the fact that the following three sets of vectors belonging to $\mathbb{F}_2^{n-2}$ are all linearly independent (the independence within each distinct set).

$$\left\{\begin{array}{c} a_1 = (0\ldots00110) \\ a_2 = (0\ldots01100) \\ a_3 = (0\ldots01110) \\ a_4 = e_5 \\ a_5 = l^4(a_1) \\ a_6 = l^5(a_1) \\ \vdots \\ a_{n-3} = l^{n-4}(a_1) \\ a_{n-2} = (0\ldots0111) \end{array}\right\} \quad \left\{\begin{array}{c} b_1 = (0\ldots001100) \\ b_2 = (0\ldots011000) \\ b_3 = (0\ldots011010) \\ b_4 = e_5 \\ b_5 = e_6 \\ \vdots \\ b_{n-3} = e_{n-2} \oplus e_3 \\ b_{n-2} = (0\ldots01101) \end{array}\right\} \quad \left\{\begin{array}{c} c_1 = (0\ldots0011000) \\ c_2 = (0\ldots0110000) \\ c_3 = (0\ldots0110010) \\ c_4 = e_3 \\ c_5 = e_6 \\ \vdots \\ c_{n-3} = e_{n-2} \oplus e_3 \\ c_{n-2} = (0\ldots011001) \end{array}\right\}$$

It can be easily verified that for $a'_i = a_i \oplus e_i$ (where e_i corresponds to the variable x_i) the three sets containing a'_i-s, b'_i-s, and c'_i-s respectively are sets of linearly independent vectors.

These vectors will present the values of $\phi_i(y)$ for $i \in \{1, \ldots, n-2\}$. The last two component functions ϕ_{n-1} and ϕ_n will be defined as slightly modified versions of ϕ_{n-2} and ϕ_3. The construction is presented below.

y	$\phi_1(y)$	$\phi_2(y)$	$\phi_3(y)$	$\ldots$	$\phi_{n-2}(y)$	$\phi_{n-1}(y)$	$\phi_n(y)$
$(0,0)$	a_1	a_2	a_3	$\ldots$	a_{n-2}	a_{n-2}	a_3
$(0,1)$	a_1	a_2	a_3	$\ldots$	a_{n-2}	a_{n-2}	a_3+1
$(1,0)$	b_1	b_2	b_3	$\ldots$	b_{n-2}	$b_{n-2}+1$	b_3+1
$(1,1)$	c_1	c_2	c_3	$\ldots$	c_{n-2}	$c_{n-2}+1$	c_3

The component functions of $f(y,x)+(y,x)$ will therefore be

y	$\phi'_1(y)$	$\phi'_2(y)$	$\phi'_3(y)$	$\ldots$	$\phi'_{n-2}(y)$	$\phi'_{n-1}(y)$	$\phi'_n(y)$
$(0,0)$	a'_1	a'_2	a'_3	$\ldots$	a'_{n-2}	$a_{n-2} = a'_1$	$a_3 = a'_2$
$(0,1)$	a'_1	a'_2	a'_3	$\ldots$	a'_{n-2}	$a_{n-2}+1 = a'_1+1$	$a_3+1 = a'_2+1$.
$(1,0)$	b'_1	b'_2	a'_3	$\ldots$	b'_{n-2}	$b_{n-2}+1 = b'_1+1$	$b_3 = b'_2$
$(1,1)$	c'_1	c'_2	a'_3	$\ldots$	c'_{n-2}	$c_{n-2} = c'_1$	$c_3+1 = c'_2+1$

Notice that $\phi'_1 = \phi_{n-2}$ and $\phi'_2 = \phi_3$. Using this and the addition of 1 in the appropriate coordinates in functions ϕ_{n-1} and ϕ_n we can ensure that all the linear combinations of functions ϕ'_i will be linearly independent as well.

Example 5.2.1 *Let us present an example of a complete permutation constructed using the above presented method for $n = 8$. Note that because of the way vectors c_i are defined the above construction does not work for smaller n.*

y	$\phi_1(y)$	$\phi_2(y)$	$\phi_3(y)$	$\phi_4(y)$	$\phi_5(y)$	$\phi_6(y)$	$\phi_7(y)$	$\phi_8(y)$
$(0,0)$	(000110)	(001100)	(001110)	(010000)	(100000)	(000111)	(000111)	(001110)
$(0,1)$	(000110)	(001100)	(001110)	(010000)	(100000)	(000111)	(000111)	$(001110)+1$
$(1,0)$	(001100)	(011000)	(011010)	(010000)	(100100)	(001101)	$(001101)+1$	$(011010)+1$
$(1,1)$	(011000)	(110000)	(110010)	(000100)	(100100)	(011001)	$(011001)+1$	(110010)

Notice that ϕ_7 differ from ϕ_6 by a constant and the same is true for ϕ_8 and ϕ_3. If we add the $(y,x)_i$ component, we get the following scheme:

y	$\phi'_1(y)$	$\phi'_2(y)$	$\phi'_3(y)$	$\phi'_4(y)$	$\phi'_5(y)$	$\phi'_6(y)$	$\phi'_7(y)$	$\phi'_8(y)$
$(0,0)$	(000111)	(001110)	(001010)	(011000)	(110000)	(100111)	(000111)	(001110)
$(0,1)$	(000111)	(001110)	(001010)	(011000)	(110000)	(100111)	$(000111)+1$	$(001110)+1$
$(1,0)$	(001101)	(011010)	(011110)	(011000)	(110100)	(101101)	$(001101)+1$	(011010)
$(1,1)$	(011001)	(110010)	(110110)	(001100)	(110100)	(111001)	(011001)	$(110010)+1$

In this scheme ϕ'_7 differ from ϕ'_1 by a constant and the same is true for ϕ'_8 and ϕ'_2. Therefore, every linear combination will yield a balanced function in a similar way as before. Similarly as before, the Lagrange interpolation gives the univariate polynomial form of F specified above as:

$$\begin{aligned}
F(y) \quad = \quad & g^{186}y^{224} + gy^{208} + g^{57}y^{200} + g^{139}y^{196} + g^{104}y^{194} + g^{229}y^{193} + g^{246}y^{192} + g^{2}y^{176} + \\
& + g^{195}y^{168} + g^{38}y^{164} + g^{171}y^{162} + g^{26}y^{161} + g^{19}y^{160} + g^{174}y^{152} + g^{74}y^{148} + g^{205}y^{146} + \\
& + g^{28}y^{145} + g^{43}y^{144} + g^{38}y^{140} + g^{151}y^{138} + g^{139}y^{137} + g^{210}y^{136} + g^{36}y^{134} + g^{200}y^{133} + \\
& + g^{152}y^{132} + g^{232}y^{131} + g^{83}y^{130} + g^{184}y^{129} + g^{120}y^{128} + g^{86}y^{112} + g^{139}y^{104} + g^{23}y^{100} + \\
& + g^{76}y^{98} + g^{100}y^{97} + g^{189}y^{96} + g^{177}y^{88} + g^{247}y^{84} + g^{222}y^{82} + g^{31}y^{81} + g^{247}y^{80} + g^{175}y^{76} + \\
& + g^{73}y^{74} + g^{142}y^{73} + g^{63}y^{72} + g^{116}y^{70} + g^{152}y^{69} + g^{146}y^{68} + g^{65}y^{67} + g^{42}y^{66} + g^{45}y^{65} + \\
& + g^{14}y^{64} + g^{83}y^{56} + g^{107}y^{52} + g^{184}y^{50} + g^{192}y^{49} + g^{92}y^{48} + g^{148}y^{44} + g^{191}y^{42} + g^{48}y^{41} + \\
& + g^{144}y^{40} + g^{96}y^{38} + g^{66}y^{37} + g^{190}y^{36} + g^{72}y^{35} + g^{8}y^{34} + g^{206}y^{33} + g^{50}y^{32} + g^{80}y^{28} + \\
& + g^{95}y^{26} + g^{34}y^{24} + g^{209}y^{22} + g^{189}y^{21} + g^{88}y^{20} + g^{204}y^{19} + g^{191}y^{18} + g^{158}y^{17} + g^{140}y^{16} + \\
& + g^{98}y^{14} + g^{45}y^{13} + g^{183}y^{12} + g^{60}y^{11} + g^{16}y^{10} + g^{147}y^{8} + g^{189}y^{7} + g^{252}y^{6} + g^{69}y^{5} + \\
& + g^{52}y^{4} + g^{99}y^{3} + g^{224}y^{2} + g^{122}y,
\end{aligned}$$

where g is the primitive root of $p(z) = z^8 + z^4 + z^3 + z^2 + 1$.

5.3 On existence of linear components and linear structures

In this section, the existence of linear components of certain nonzero linear combinations in a generalized framework of the design rationales behind Constructions 1 and 2 is investigated (the same reasoning applies to Construction 3). More precisely, we show that specifying $\phi_1, \dots, \phi_{n-2}$ to build a vector space basis of $\mathbb{F}_2^{n-2}$, then whatever is the choice of ϕ_{n-1} and ϕ_n there will exist some linear combinations of the component functions $f_1, \dots, f_n$ which are linear.

Construction 4 *Let $e_i \in \mathbb{F}_2^{n-2}$, for $i = 1, \dots, n-2$, form the canonical basis of $\mathbb{F}_2^{n-2}$, where $n \geq 7$. For any $y \in \mathbb{F}_2^2$ define $\phi(y)$ as below,*

y	$\phi_1(y)$	$\phi_2(y)$	$\cdots$	$\phi_{n-2}(y)$	$\phi_{n-1}(y)$	$\phi_n(y)$
$(0,0)$	e_1	e_2	$\cdots$	e_{n-2}	$L_1(\phi_1, ..., \phi_{n-2})(y)$	$L_1^*(\phi_1, ..., \phi_{n-2})(y)$
$(0,1)$	e_2	e_3	$\cdots$	e_1	$L_2(\phi_1, ..., \phi_{n-2})(y)$	$L_2^*(\phi_1, ..., \phi_{n-2})(y)$
$(1,0)$	e_3	e_4	$\cdots$	e_2	$L_3(\phi_1, ..., \phi_{n-2})(y)$	$L_3^*(\phi_1, ..., \phi_{n-2})(y)$
$(1,1)$	e_4	e_5	$\cdots$	e_3	$L_4(\phi_1, ..., \phi_{n-2})(y)$	$L_4^*(\phi_1, ..., \phi_{n-2})(y)$

Let $f_i(y,x) = \phi_i(y) \cdot x \oplus g_i(y)$ for $i = 1, \dots, n$, where $g_i(y) = 0$, for $i = 1, \dots, n-2$, and both L_i and L_i^* are affine functions of ϕ_j, $(i = 1, \dots, 4, j = 1, \dots, n-2)$.

Remark 5.3.1 *For convenience and shortness of notation, we use in this section "+" instead of more correct $\oplus$ to denote vector addition modulo two.*

Theorem 5.3.1 *If $F = (f_1, \dots, f_n)$ is a permutation over $\mathbb{F}_2^n$, then there exists at least one non-zero linear combination of $f_1, \dots, f_n$ which is linear.*

Proof. Note that the functions ϕ_{n-1}, ϕ_n must be defined in such a way so that f_{n-1}, f_n and $f_{n-1} + f_n$ are balanced functions. Clearly,

y	$\phi_{n-1}(y)$	$\phi_n(y)$	$(\phi_{n-1} + \phi_n)(y)$
$(0,0)$	$L_1(\phi_1, ..., \phi_{n-2})(y)$	$L_1^*(\phi_1, ..., \phi_{n-2})(y)$	$L_1(\phi_1, ..., \phi_{n-2})(y) + L_1^*(\phi_1, ..., \phi_{n-2})(y)$
$(0,1)$	$L_2(\phi_1, ..., \phi_{n-2})(y)$	$L_2^*(\phi_1, ..., \phi_{n-2})(y)$	$L_2(\phi_1, ..., \phi_{n-2})(y) + L_2^*(\phi_1, ..., \phi_{n-2})(y)$
$(1,0)$	$L_3(\phi_1, ..., \phi_{n-2})(y)$	$L_3^*(\phi_1, ..., \phi_{n-2})(y)$	$L_3(\phi_1, ..., \phi_{n-2})(y) + L_3^*(\phi_1, ..., \phi_{n-2})(y)$
$(1,1)$	$L_4(\phi_1, ..., \phi_{n-2})(y)$	$L_4^*(\phi_1, ..., \phi_{n-2})(y)$	$L_4(\phi_1, ..., \phi_{n-2})(y) + L_4^*(\phi_1, ..., \phi_{n-2})(y)$

where

$$L_i(\phi_1, \dots, \phi_{n-2}) = \sum_{j=1}^{n-2} \delta_j^i \phi_j + \delta_0^i; \qquad L_i^*(\phi_1, \dots, \phi_{n-2}) = \sum_{j=1}^{n-2} \gamma_j^i \phi_j + \gamma_0^i,$$

for $(\delta_1^i, \dots, \delta_{n-2}^i) \in \mathbb{F}_2^{n-2}$, $(\gamma_1^i, \dots, \gamma_{n-2}^i) \in \mathbb{F}_2^{n-2}$, $\delta_0^i, \gamma_0^i \in \mathbb{F}_2$, and $i = 1, \dots, 4$.

(1) To preserve the balancedness property of any non-zero linear combination of $f_1, \dots, f_{n-1}$, we define L_is by reasoning as follows. For each L_i, there must exist L_t such that (L_i, L_t) is a pair of complement functions so that $L_t = 1 + L_i$, where $1 \le i \ne t \le 4$. Assume on contrary that for some L_i there is no L_t, $i \ne t$, such that $L_t = 1 + L_i$. Then, for a fixed $(\delta_1^i, \dots, \delta_{n-2}^i) \in \mathbb{F}_2^{n-2}$ which defines L_i, let us w.l.o.g. suppose that $i = 1$ and observe the linear combination $\sum_{j=1}^{n-2} \delta_j^1 f_j + f_{n-1}$ which in terms of concatenation can be written as,

$$\sum_{j=1}^{n-2} \delta_j^1 f_j + f_{n-1} = \delta_0^1 || \sum_{j=1}^{n-2} (\delta_j^1 + \delta_j^2)\phi_j + \delta_0^2 || \sum_{j=1}^{n-2} (\delta_j^1 + \delta_j^3)\phi_j + \delta_0^3 || \sum_{j=1}^{n-2} (\delta_j^1 + \delta_j^4)\phi_j + \delta_0^4.$$

Since it needs to be balanced at least one $\sum_{j=1}^{n-2} (\delta_j^1 + \delta_j^t)\phi_j + \delta_0^t$, $t = 2, 3, 4$ needs to be a constant function equal to $\delta_0^1 + 1$, which would imply $L_t + L_1 + \delta_0^1 = \delta_0^1 + 1$, a contradiction.

(2) Similarly, to preserve the balancedness property of any non-zero linear combination of $f_1, \dots, f_{n-2}, f_n$, for each L_i^*, there must exist L_t^*, $i \ne t$, such that $(L_t^* = 1 + L_i^*)$, $1 \le i \ne t \le 4$.

(3) Finally, to preserve the balancedness property of any non-zero linear combination of $f_1, \dots, f_{n-2}, f_{n-1} + f_n$, for each $L_i + L_i^*$, we necessarily have that $(L_i + L_i^* = 1 + L_t + L_t^*)$ for some $t \ne i$.

(4) W.l.o.g, we assume that $L_2(y) = L_1(y) + 1, L_4(y) = L_3(y) + 1, L_2^*(y) = L_1^*(y) + 1$, and $L_4^*(y) = L_3^*(y) + 1$, i.e.,

y	$\phi_{n-1}(y)$	$\phi_n(y)$	$(\phi_{n-1} + \phi_n)(y)$
$(0,0)$	$L_1(y)$	$L_1^*(y)$	$(L_1 + L_1^*)(y)$
$(0,1)$	$L_1(y) + 1$	$L_1^*(y) + 1$	$(L_1 + L_1^*)(y)$
$(1,0)$	$L_3(y)$	$L_3^*(y)$	$(L_3 + L_3^*)(y)$
$(1,1)$	$L_3(y) + 1$	$L_3^*(y) + 1$	$(L_3 + L_3^*)(y)$

To preserve the balancedness property of $\phi_{n-1}+\phi_n$ as well, we must have $(L_3+L_3^*)(y) = (L_1+L_1^*)(y)+1$, i.e.,

y	$(\phi_{n-1}+\phi_n)(y)$
$(0,0)$	$(L_1+L_1^*)(y)$
$(0,1)$	$(L_1+L_1^*)(y)$
$(1,0)$	$(L_1+L_1^*)(y)+1$
$(1,1)$	$(L_1+L_1^*)(y)+1$

Let $(L_1+L_1^*)(\phi_1,\ldots,\phi_{n-2}) = \sum_{i=1}^{n-2}\tau_i\phi_i$, where $(\tau_1,\ldots,\tau_{n-2}) \in \mathbb{F}_2^{n-2^*}$. Moreover, we have $\sum_{i=1}^{n-2}\tau_i f_i + f_{n-1} + f_n = \mathbf{0}||\mathbf{0}||\mathbf{1}||\mathbf{1}$. Therefore, $\deg(\sum_{i=1}^{n-2}\tau_i f_i + f_{n-1} + f_n) = 1$.
□

5.3.1 Differential properties of the designed permutations

Due to the nature of the presented constructions, the differential properties of the proposed permutations are rather poor and therefore these permutations are not useful in cryptographic applications such as the design of substitution boxes (S-boxes) in block ciphers.

Proposition 5.3.2 *The functions F in Construction 1 admit linear structures, that is,*

$$\delta(F) = \max_{a\neq 0, b\in\mathbb{F}_2^n}(\#\{x\in\mathbb{F}_2^n \mid F(x+a)+F(x)=b\}) = 2^n.$$

Proof. Let $a = (0,0,1,\ldots,1)$. Notice that in general

$$\begin{aligned} F(x+a)+F(x) &= (f_1(x+a),\ldots,f_n(x+a)) + (f_1(x),\ldots,f_n(x)) \\ &= (f_1(x+a)+f_1(x),\ldots,f_n(x+a)+f_n(x)). \end{aligned}$$

Since our component functions f_i are defined as $f_i(y,x) = \phi_i(y)\cdot x$ we notice that $f_i((y,x)+a)+f_i(y,x) = \phi_i(y)\cdot(x+(1,1,\ldots,1))+\phi_i(y)\cdot x = \phi_i(y)\cdot(1,1,\ldots,1) = 1$, for any $y\in\mathbb{F}_2^2$ and $i = 1,\ldots,n-2$. In a similar manner, $f_i((y,x)+a)+f_i(y,x) = 0$ for all x, y, when $i\in\{n-1,n\}$. Thus, $F(x+a)+F(x) = b$ has 2^n solutions for $b = (1,1,\ldots,1,0,0)$. □

In a similar manner, the differential properties of the functions in Construction 2 can be analyzed. Here, however, we could not show the existence or linear structures and computer simulations indicate that for small values of n we either have $\delta(F) = 2^{n-1}$ or $\delta(F) = 2^{n-2}$. The class of complete permutations seems to admit linear structures which was checked by computer simulations.

Chapter 6

Conclusion

The results of the PhD Thesis represent a significant contribution to a number of the standing open problems in cryptography which have been an active topic of research in mathematical community in the last decades.

In the study of special Rothaus constructions, certain methods from linear algebra and the analysis of the Walsh-Hadamard spectra are important tools. The bent functions thus acquired are presented as mappings over vector spaces and the affine non-equivalence of their classes is proved by considering their possible algebraic degrees. When creating the algorithm to test the normality of these bent functions we first transformed the functions into graphs and utilized certain optimized search algorithms for finding all possible cliques of size $2^{\frac{n}{2}}$. It is proved that under certain conditions these functions do not belong to the completed Maiorana Mc-Farland class using a careful and detailed analysis of their double derivatives over all possible $\frac{n}{2}$-dimensional vector subspaces.

The sufficient conditions for $\mathcal{C}$ and $\mathcal{D}$ functions to lie outside of the completed Maiorana-McFarland class are derived in a similar way, by considering how to ensure that the double derivatives over all possible $\frac{n}{2}$-dimensional vector subspaces never completely vanish. The examples for functions in $\mathcal{C}$ outside the $\mathcal{M}^{\#}$ class are derived from [61] using certain finite field and primitive element properties. The examples for functions in $\mathcal{D}$ outside the $\mathcal{M}^{\#}$ class are found by relying on algebraic properties of finite fields and the help of programming package Magma.

The existence of linear translators for certain classes of functions over finite fields is explored relying on properties of polynomials over finite fields, Lucas's Theorem, and, specifically, the linear properties of trace functions. Properties of finite fields, lienar translators, and linearised polynomials are, together with applications of results from [49], then used in finding compositional inverses of a number of polynomials, as well as several new families of permutations of form $x \mapsto (x^{p^m} - x + \delta)^s$, for even and odd n separately.

When constructing permutations using Frobenius translators, similar techniques are used as when constructing them using linear translators. When applying the Frobenius translator in the construction of bent functions, these are represented as mappings over finite fields. Examples of these generalized constructions are then verified using the programming package Magma. Magma is used in verifying the solution to the Open Problem from [42], as well.

When constructing infinite classes of vectorial plateaued functions, permutations and complete permutations these are all represented as mappings over binomial vector spaces. All the constructions required a combinatorial approach, where we often searched for large sets of linearly independent vectors. The construction of complete permutations especially relied heavily on intuition-based approach where a very strict set of combinatorial conditions needed to be satisfied.

The basic tools used in the research range from combinatorial to algebraic cryptographic methods. In addition, we used the computer package Computational Algebra System Magma to test the results and form new conjectures.

Bibliography

[1] A. Akbary, D. Ghioca, and Q. Wang, On constructing permutations of finite fields, *Finite Fields Appl.*, vol. 17(1) (2011), pp. 51–67.

[2] L. A. Bassalygo, and V. A. Zinoviev, Permutation and complete permutation polynomials, *Finite Fields Appl.*, vol. 33 (2015), pp. 198–211.

[3] A. Bernasconi, B. Codenotti, J. M. VanderKam, A characterization of bent functions in terms of strongly regular graphs, IEEE Trans Comput, 50(9), (2001), pp. 984–5.

[4] E. Biham, O. Dunkelman, Cryptanalysis of the $A5/1$ GSM stream cipher, International Conference on Cryptology in India, Springer, Berlin, Heidelberg, (2000).

[5] E. Biham, A. Shamir, Differential cryptanalysis of the full 16-round DES, *Differential Cryptanalysis of the Data Encryption Standard*, Springer, New York, (1993), pp. 79–88).

[6] A. Blokhuis, R. S. Coulter, M. Henderson, and C. M. O'Keefe, Permutations amongst the Dembowski-Ostrom polynomials, *Proceedings of the fifth international conference on Finite Fields and Applications* F_{q5}, Springer, Berlin, (2001), pp. 37–42.

[7] L. Budaghyan, A. Kholosha, C. Carlet, and T. Helleseth, Niho bent functions from quadratic o-monomials, *Information Theory (ISIT), 2014 IEEE International Symposium*, (2014), pp. 1827–1831

[8] C. De Canniere, Trivium: A stream cipher construction inspired by block cipher design principles, International Conference on Information Security, Springer, Berlin, Heidelberg (2006), pp. 171–186.

[9] A. Canteaut, P. Charpin, and G. Kyureghyan, A new class of monomial bent functions, *F*inite Fields and Their Applications, vol. 14, no. 1 (2008), pp. 221–241.

[10] A. Canteaut, M. Daum, H. Dobbertin, and G. Leander, Finding nonnormal bent functions, *D*iscrete Applied Math., vol. 154 (2006), pp. 202–218.

[11] C. Carlet, Boolean and vectorial plateaued functions, and APN functions, *I*EEE Trans. Inform. Th., vol. 61, no. 11 (2015), pp. 6272–6289.

[12] C. Carlet, Boolean functions for cryptography and error correcting codes, *Boolean models and methods in mathematics, computer science, and engineering 2* (2010), pp.257-397.

[13] C. Carlet, Vectorial Boolean Functions for Cryptography, *C*hapter of the monograph: Boolean Models and Methods in Mathematics, Computer Science, and Engineering, Cambridge University Press, (2010), pp. 398–469.

[14] C. Carlet, Two New Classes of Bent Functions, *Procedings of Eurocrypt '93, LNCS, vol. 765*, (1994), pp. 77–101.

[15] C. Carlet, On the secondary constructions of resilient and bent functions, *Proceedings of Coding, Cryptography and Combinatorics, Progress in Computer Science and Applied Logic*, vol. 23, Birkhauser Verlag, Basel, (2004), pp. 3-28.

[16] C. Carlet, On bent and highly nonlinear balanced/resilient functions and their algebraic immunities, *Proceedings of AAECC, Lecture Notes in Computer Science 3857*, (2006), pp. 1–28.

[17] C. Carlet, and P. Gaborit, Hyper-bent functions and cyclic codes, *J.* Combinatorial Theory, Ser. A, vol. 113(3) (2006), pp. 466–482.

[18] C. Carlet, and S. Mesnager, Four decades of research on bent functions, *Designs, Codes and Cryptography*, vol. 78 (1) (2016), pp. 5–50.

[19] C. Carlet, and E. Prouff, On Plateaued Functions and Their Constructions, *F*ast Software Encryption: 10th International Workshop, Lund (2003), pp. 54–73.

[20] C. Carlet, F. Zhang, and Y. Hu, Secondary constructions of bent functions and their enforcements, *A*dvances in Mathematics and Communications, vol. 6, no. 3 (2012), pp. 305–314.

[21] N. Cepak, P. Charpin, and E. Pasalic, Permutations via linear translators, *Finite Fields and Their Applications*, vol. 45 (2017), pp.19-42.

[22] P. Charpin, and G. Kyureghyan, Cubic monomial bent functions: a subclass of $\mathcal{M}$, *SIAM Journal of Discrete Math.*, vol. 22, no. 2 (2008), pp.650–665.

[23] P. Charpin, and G. M. Kyureghyan, Monomial functions with linear structure and permutation polynomials, *Finite Fields: Theory and Applications-Fq9-Contemporary Mathematics*, AMS, 518 (2010), pp.99–111.

[24] P. Charpin, and G. M. Kyureghyan, When does $G(x) + \gamma Tr(H(x))$ permute $\mathbb{F}_{2^n}$?, *Finite Fields Appl.*, vol. 15 (5) (2009), pp. 615–632.

[25] P. Charpin, G. M. Kyureghyan and V. Suder, Sparse permutations with low differential uniformity, *Finite Fields Appl.*, vol. 28 (2014), pp. 214–243.

[26] P. Charpin, S. Mesnager, and S. Sarkar, Involutions over the Galois field $GF(2^n)$, *IEEE Trans. Inf. Theory*, vol. 62 (4) (2016), pp. 2266–2276.

[27] P. Charpin, S. Sarkar, Polynomials with linear structure and Maiorana–McFarland construction, *IEEE Transactions on Information Theory*, IT-57(6) (2011), pp. 3796–3804.

[28] P. Charpin, E. Pasalic, and C. Tavernier, On bent and semi-Bent quadratic Boolean functions, *IEEE Transactions on Information Theory*, vol. 51, no.12 (2005), pp. 4286–4298.

[29] S. Chee, S. Lee, D. Lee, and H. S. Sung, On the correlation immune functions and their nonlinearity, *ASIACRYPT '96*, LNCS 1163, Springer-Verlag (1996), pp. 232–243.

[30] T. W. Cusick, P. Stănică, Cryptographic Boolean functions and applications, Elsevier–Academic Press, (2017).

[31] J. Daemen, V. Rijmen, AES proposal: Rijndael, (1999).

[32] P. Delsarte, An algebraic approach to the association schemes of coding theory, PhD thesis, 1973.

[33] W. Diffie, M. E. Hellman, Exhaustive Cryptanalysis of the NBS Data Encryption Standard, *Computer*, (1977), pp. 74–84.

[34] J. F. Dillon, Elementary Haddamard Difference Sets, PhD thesis, University of Maryland, U.S.A., 1974.

[35] J. F. Dillon, Elementary Hadamard difference sets, *Proceedings of 6th S. E. Conference of Combinatorics, Graph Theory, and Computing*, Utility Mathematics, Winnipeg, (1975), pp. 237–249.

[36] J. F. Dillon, A survey of bent functions, *NSA Techical Journal 1972*; special issue, pp.191–215.

[37] H. Dobbertin, Construction of bent functions and balanced Boolean functions with high nonlinearity, *Proceedings of Fast Software Encryption*, Leuven 1994 (1995), LNCS 1008, Springer-Verlag, pp. 61–74.

[38] P. Ekdahl, T. Johansson, SNOW-a new stream cipher Proceedings of First Open NESSIE Workshop, KU-Leuven (2000), pp. 167–168.

[39] S. Gilboa, S. Gueron, and M. Nandi, Balanced permutations Even-Mansour ciphers, Cryptography 1, no. 1 (2016), pp. 2

[40] G. Gong, T. Helleseth, H. Hu, and A. Kholosha, On the dual of certain ternary weakly regular bent functions, *IEEE Transactions on Information Theory*, vol. 58, no. 4 (2012), pp. 2237–2243.

[41] M. Hell, T. Johansson, W. Meier, Grain: a stream cipher for constrained environments, International Journal of Wireless and Mobile Computing, 2(1) (2007), pp. 86–93.

[42] S. Hodžić, E. Pasalic, and Y. Wei, A general framework for secondary constructions of bent and plateaued functions, Submitted manuscript.

[43] X. Hou, Permutation polynomials over finite fields A survey of recent advances, *Finite Fields Appl.*, vol. 32 (2015), pp. 82–119.

[44] D. Kahn, The Codebreakers: A Comprehensive History of Secret Communication from Ancient Times to the Internet, Revised and Updated. Scribner Simon and Schuster, (1996).

[45] R.M. Karp, Reducibility among combinatorial problems, *Complexity of computer computations*, Springer, Boston, MA, 1972, pp. 85–103.

[46] J. Katz, A. J. Menezes, P. C. Van Oorschot, S. A. Vanstone, Handbook of applied cryptography, CRC press. (1996).

[47] S. Kavut, S. Maitra, M.D. Yucel, Search for Boolean functions with excellent profiles in the rotation symmetric class, *IEEE Trans Inform Theory* 53.5 (2007), pp. 1743–1751.

[48] A. Klein, Attacks on the RC4 stream cipher, *Designs, Codes and Cryptography*, 48(3) (2008), pp. 269–286.

[49] G. M. Kyureghyan. Constructing permutations of finite fields via linear translators, *Journal of Combinatorial Theory*, Series A vol. 118 (2011), pp. 1052–1061.

[50] X. Lai, J. L. Massey, A proposal for a new block encryption standard, *Workshop on the Theory and Application of of Cryptographic Techniques*, Springer, Berlin, Heidelberg (1990), pp. 389–404.

[51] Y. Laigle-Chapuy, A note on a class of quadratic permutations over $\mathbb{F}_{2^n}$, *In International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes*, Springer, Berlin, Heidelberg, (2007), pp. 130–137.

[52] Y. Laigle-Chapuy, Permutation polynomials and applications to coding theory, *Finite Fields and Their Applications 13*, no. 1 (2007), pp. 58–70.

[53] N. G. Leander, Monomial bent functions, *IEEE Trans. on Inform. Theory*, vol.52, no. 2 (2006), pp. 738–743.

[54] N. G. Leander, and A. Kholosha, Bent functions with 2^r Niho exponents, *IEEE Trans. on Inform. Theory*, vol. 52, no. 12 (2006), pp. 5529–5532.

[55] N. G. Leander, and G. McGuire, Construction of bent functions from near-bent functions, *J. Combinatorial Theory, Ser. A,* vol. 116(4) (2009), pp. 960–970.

[56] N. Li, and T. Helleseth, New permutation trinomials from Niho exponents over finite fields with even characteristic, *arXiv preprint arXiv:1606.03768* (2016)

[57] N. Li, T. Helleseth, X. Tang, and A. Kholosha, Several new classes of bent functions from Dillon exponents, *IEEE Transactions on Information Theory*, vol. 59, no. 3 (2013), pp. 1818–1831.

[58] R. Lidl, and H. Niederreiter, Finite Fields, Encyclopedia Math. Appl., vol. 20, Addison-Wesley, Reading, 1983.

[59] Y. Lu, S. Vaudenay Faster correlation attack on Bluetooth keystream generator E0, Annual International Cryptology Conference, Springer, Berlin, Heidelberg, (2004).

[60] S. Maitra, P. Sarkar, Maximum nonlinearity of symmetric Boolean functions on odd number of variables *IEEE Trans Inform Theory* 48(9) 2002, pp. 2626–30.

[61] B. Mandal, P. Stănică, S. Gangopadhyay, and E. Pasalic, An analysis of $\mathcal{C}$ class of bent functions, *Fundamenta Informaticae*, vol. 147 (3) (2016), pp. 271–292.

[62] M. Matsui, On correlation between the order of S-boxes and the strength of DES, *Workshop on the Theory and Application of of Cryptographic Techniques*, Springer, Berlin, Heidelberg, (1994), pp. 366–375.

[63] R. L. McFarland, A family of noncyclic difference sets, *J. Combinatorial Theory, Ser. A,* vol. 15 (1973), pp.1–10.

[64] M. Matsui, Linear cryptanalysis method for DES cipher, Advances in cryptologyEUROCRYPT93, workshop on the theory and application of cryptographic techniques, Lecture notes in computer science, vol. 765 (1994), p.386–97.

[65] R. L. McFarland, A family of difference sets in non-cyclic groups, *Journal of Combinatorial Theory*, Series A, 15(1), 1973, pp. 1–10.

[66] S. Mesnager, Bent and Hyper-bent functions in polynomial form and their link with some exponential sums and Dickson Polynomials, *IEEE Trans. on Inform. Theory*, vol.57, no. 9 (2011), pp. 5996–6009.

[67] S. Mesnager, Several New Infinite Families of Bent Functions and Their Duals, *IEEE Trans. on Inform. Theory*, vol. 60, no. 7 (2014), pp. 4397–4407.

[68] S. Mesnager, Bent functions from spreads, *Journal of the American Mathematical Society*, vol. 632 (2015), pp. 295–316.

[69] S. Mesnager, P. Ongan, and F. Özbudak, New bent functions from permutations and linear translators, *C2SI 2017: Codes, Cryptology and Information Security*, pp. 282–297.

[70] S. Mesnager, P. Ongan, and F. Özbudak, Further constructions of infinite families of bent functions from new permutations and their duals, *Cryptography and Communications* 8.2, (2016), pp.229–246

[71] F. P. Miller, A. F. Vandome, J. McBrewster, Advanced encryption standard, (2009).

[72] G. L. Mullen, and H. Niederreiter, Dickson polynomials over finite fields and complete mappings, *Canad. Math. Bull.*, vol. 30(1) (1987), pp. 19–27.

[73] G. L. Mullen, and Q. Wang, Permutation polynomials in one variable, Chapter 8 in *Handbook of Finite Fields*, Chapman and Hall/CRC, Boca Raton, FL (2013), pp. 215–230.

[74] A. Muratović-Ribić, and E. Pasalic, A note on complete polynomials over finite fields and their applications in cryptography, *Finite Fields and Their Applications*, 25 (2014), pp. 306–315.

[75] E. Pasalic, A. Muratović-Ribić, S. Hodžić, and S. Gangopadhyay. On derivatives of polynomials over finite fields through integration, *Discrete Applied Mathematics*, 217 (2017), pp. 294–303.

[76] R. L. Rivest, The RC5 encryption algorithm, *International Workshop on Fast Software Encryption*, Springer, Berlin, Heidelberg, (1993), pp. 86–96.

[77] O. S. Rothaus, On Bent Functions, *J. Combinatorial Theory, Ser. A*, vol. 20 (1976), pp. 300–305.

[78] B. Schneier, *Description of a new variable-length key, 64-bit block cipher (Blowfish)*, *International Workshop on Fast Software Encryption*, Springer, Berlin, Heidelberg, (1993), pp. 191–204.

[79] C. E. Shannon A mathematical theory of communication, *Bell system technical journal*, 27.3 (1948), pp. 379–423.

[80] V. M. Sidelnikov, On extremal polynomials used to estimate the size of codes, *Probl. Inform. Transm*, 16 (1980), pp. 174–186.

[81] C. Tang, Z. Zhou, Y. Qi, X. Zhang, C. Fang, and T. Helleseth, Generic construction of bent functions and bent idempotents with any possible algebraic degree, *IEEE Transactions on Information Theory* 63.10 (2017), pp. 6149-6157.

[82] N. Tokareva, Bent functions: results and applications to cryptography, Academic Press, 2015.

[83] Z. Tu, and Y. Deng, A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity, *Des. Codes Cryptogr.*, vol. 60 (2011), pp. 1–14.

[84] Z. Tu, X. Zeng, C. Li, and T. Helleseth, Permutation polynomials of the form $(x^{p^m} - x + \delta)^s + L(x)$ over the finite field $\mathbb{F}_{p^{2m}}$ of odd characteristic, *Finite Fields Appl.*, vol. 31 (2015), pp. 12–24.

[85] Z. Tu, X. Zeng, and L. Hu, Several classes of complete permutation polynomials, *Finite Fields Appl.*, vol. 25 (2014), pp. 182–193.

[86] Z. Tu, X. Zeng, and Y. Jiang, Two classes of permutation polynomials having the form $(x^{2^m} + x + \delta)^s + x$, *Finite Fields Appl.*, vol. 31 (2015), pp. 12–24.

[87] A. Tuxanidy, and Q. Wang. On the inverses of some classes of permutations of finite fields, *Finite Fields Appl.*, vol. 28 (2014), pp. 244–281.

[88] G. Vega, Some precisions on $\mathcal{PS}$ bent functions, *International Mathematical Forum*, vol. 5 (2010), pp.537–544.

[89] G. Wu, N. Li, T. Helleseth, and Y. Zhang, Some classes of monomial complete permutation polynomials over finite fields of characteristic two, *Finite Fields Appl.*, vol. 28 (2014), pp. 148–165.

[90] P. Yuan, and C. Ding, Further results on permutation polynomials over finite fields, *Finite Fields Appl.*, vol. 27 (2014), pp. 88–103.

[91] P. Yuan, C. Ding, H. Wang and J. Pieprzyk, Permutation polynomials of the form $(x^p - x + \delta)^s + L(x)$, *Finite Fields and Their Applications* 14, no. 2 (2008), pp. 482–493.

[92] Y. Yuan, Y. Tong, and H. Zhang, Complete mapping polynomials over finite field $\mathbb{F}_{16}$, *Proceedings of the 1st international workshop on Arithmetic of Finite Fields*, WAIFI '07 (2007), pp.147–158.

[93] F. Zhang, C. Carlet, Y. Hu, and W. Zhang, New secondary constructions of bent functions, *Applicable Algebra in Engineering, Communication and Computing* 27, no. 5 (2016), pp. 413–434.

[94] F. Zhang, E. Pasalic, Y. Wei, and N. Cepak, Constructing bent functions outside the MaioranaMcFarland class using a general form of Rothaus, IEEE Transactions on Information Theory 63, no. 8 (2017), pp. 5336–5349.

[95] F. Zhang, Y. Wei, and E. Pasalic, Constructions of bent-negabent functions and their relation to the completed Maiorana-McFarland class, *IEEE Trans. on Inform. Theory*, vol. 61, no. 3 (2015), pp. 1496–1506.

[96] Y. Zheng, and X. M. Zhang, On plateaued functions. *IEEE Trans. Inform. Th.*, vol. 47, no. 3 (2001), pp. 1215–1223.

Appendix

Proof of Theorem 3.1.2:

Proof. Both $\mathbf{x} = (x, x_{n+1}, x_{n+2})$ and $\mathbf{b}$ are considered as column vectors of length $n{+}2$. Also, let A_i denote the i-th row of A, $i = 1, 2, \ldots, n{+}2$. Our goal is to show the non-existence of A and $\mathbf{b}$ such that the terms of algebraic degree $n/2{+}1$ in $f'(A\mathbf{x}\oplus\mathbf{b})$ and $f(x, x_{n+1}, x_{n+2})$ cannot be equal, which implies affine non-equivalence between f and f'.

Let $p(x)$ and $q(x)$ denote a collection of monomials of degree $n/2$ in the ANF of $1_\Delta(x)$ and of $f_0(x) \oplus f_1(x)$, respectively. Since $f_0 \oplus f_1 \in \mathcal{PS}^-$ then $q(x)$ is non-empty. Before applying affine transformation, the terms of algebraic degree $n/2{+}1$ in $f'(x, x_{n+1}, x_{n+2})$ and $f(x, x_{n+1}, x_{n+2})$ are $x_{n+2}p(x)$ and $x_{n+2}p(x) \oplus (x_{n+1} \oplus x_{n+2})q(x)$, respectively.

For shortness, we denote the terms of algebraic degree $n/2 + 1$ in $(A_{n+2} \cdot \mathbf{x} \oplus b_{n+2})p(A_1 \cdot \mathbf{x} \oplus b_1, \ldots, A_n \cdot \mathbf{x} \oplus b_n)$ (after applying affine transformation) by $\Im(x, x_{n+1}, x_{n+2})$. Furthermore, the terms of degree $n/2$ in $p(A_1 \cdot \mathbf{x} \oplus b_1, \ldots, A_n \cdot \mathbf{x} \oplus b_n)$ are denoted by

$$\begin{aligned}\wp(x, x_{n+1}, x_{n+2}) = {} & c_1 x_{n+1} \Re_1(x) \oplus c_2 x_{n+2} \Re_2(x) \\ & \oplus c_3 x_{n+1} x_{n+2} \Re_3(x) \oplus c_4 \Re_4(x),\end{aligned}$$

where $c_i \in \mathbb{F}_2, i = 1, \ldots, 4$. It is easy to deduce that

$$\begin{aligned}&\deg(\Re_1) = \deg(\Re_2) = n/2 - 1, \\ &\deg(\Re_3) = n/2 - 2, \deg(\Re_4) = n/2.\end{aligned} \tag{6.1}$$

Clearly, the terms of degree $n/2 + 1$ in $f'(A\mathbf{x} \oplus \mathbf{b})$ correspond to $\Im(x, x_{n+1}, x_{n+2})$. If (3.6) holds, then

$$\begin{aligned}\Im(x, x_{n+1}, x_{n+2}) &= x_{n+2}p(x) \oplus (x_{n+1} \oplus x_{n+2})q(x) \\ &= x_{n+2}(p(x) \oplus q(x)) \oplus x_{n+1}q(x).\end{aligned} \tag{6.2}$$

We denote $A_{n+2} = (\mathbf{a'}, a_{n+2,n+1}, a_{n+2,n+2})$, and the terms of degree $n/2$ in $\Re_i(x)(\mathbf{a'} \cdot x)$ by $\Re'_i(x)$ for $i = 1, 2$, the terms of degree $n/2 - 1$ in $\Re_3(x)(\mathbf{a'} \cdot x)$ by $\Re'_3(x)$. There are four cases to be considered.

1. Assuming that $A_{n+2} = (\mathbf{a'}, 0, 1)$, we have

$$\begin{aligned}&(A_{n+2} \cdot \mathbf{x} \oplus b_{n+2})\wp(x, x_{n+1}, x_{n+2}) \\ =&c_4(\mathbf{a'} \cdot x)\Re_4(x) \oplus c_1 x_{n+1}\Re_1(x)(\mathbf{a'} \cdot x) \\ &\oplus c_2 x_{n+2}\Re_2(x)(\mathbf{a'} \cdot x) \oplus c_3 x_{n+1}x_{n+2}\Re_3(x)(\mathbf{a'} \cdot x) \\ &\oplus c_1 x_{n+1}x_{n+2}\Re_1(x) \oplus c_2 x_{n+2}\Re_2(x) \oplus c_3 x_{n+1}x_{n+2}\Re_3(x) \\ &\oplus c_4 x_{n+2}\Re_4(x) \oplus b_{n+2}\wp(x, x_{n+1}, x_{n+2}).\end{aligned}$$

   Combining (6.1) and (6.2), we know there is no term $x_{n+1}x_{n+2}r(x)$ in $x_{n+2}p(x) \oplus (x_{n+1} \oplus x_{n+2})q(x)$, where $\deg(x_{n+1}x_{n+2}r(x)) = n/2 + 1$. Hence, we must have

$$q(x) = c_1\Re'_1(x) \quad \textit{and} \quad c_3\Re'_3(x) = c_1\Re_1(x). \tag{6.3}$$

Further, we have $c_1 = c_3 = 1$ and from (6.3)

$$\begin{aligned}&(\Re'_3(x) = \Re_3(x)(\mathbf{a'} \cdot x) \oplus \ell'(x) = \Re_1(x))\\ \Longleftrightarrow\ &(\Re_3(x)(\mathbf{a'} \cdot x) \oplus \ell'(x)(\mathbf{a'} \cdot x) = \Re_1(x)(\mathbf{a'} \cdot x)),\end{aligned}$$

where $\deg(\ell') \leq n/2 - 2$. It is easy to deduce that $\deg(\Re_3(x)(\mathbf{a'} \cdot x) \oplus \ell'(x)(\mathbf{a'} \cdot x)) \leq n/2 - 1$. However, $\deg(\Re_1(x)(\mathbf{a'} \cdot x)) = \deg(q(x)) = n/2$. Thus, if $A_{n+2} = (\mathbf{a'}, 0, 1)$ then there do not exist an invertible matrix A and a vector $\mathbf{b} \in \mathbb{F}_2^{n+2}$ such that $\Im(x, x_{n+1}, x_{n+2})$ equals $x_{n+2}p(x) \oplus (x_{n+1} \oplus x_{n+2})q(x)$.

2. Assuming that $A_{n+2} = (\mathbf{a'}, 1, 1)$, we have

$$\begin{aligned}&(A_{n+2} \cdot \mathbf{x} \oplus b_{n+2})\wp(x, x_{n+1}, x_{n+2}) = c_4(\mathbf{a'} \cdot x)\Re_4(x)\\ &\oplus c_1 x_{n+1}\Re_1(x)(\mathbf{a'} \cdot x) \oplus c_2 x_{n+2}\Re_2(x)(\mathbf{a'} \cdot x)\\ &\oplus c_3 x_{n+1}x_{n+2}\Re_3(x)(\mathbf{a'} \cdot x) \oplus c_1 x_{n+1}\Re_1(x)\\ &\oplus c_2 x_{n+1}x_{n+2}\Re_2(x) \oplus c_3 x_{n+1}x_{n+2}\Re_3(x) \oplus c_4 x_{n+1}\Re_4(x)\\ &\oplus c_1 x_{n+1}x_{n+2}\Re_1(x) \oplus c_2 x_{n+2}\Re_2(x) \oplus c_3 x_{n+1}x_{n+2}\Re_3(x)\\ &\oplus c_4 x_{n+2}\Re_4(x) \oplus b_{n+2}\wp(x, x_{n+1}, x_{n+2}).\end{aligned}$$

Moreover, combining (6.1) and (6.2), we have

$$\begin{aligned}c_1\Re'_1(x) \oplus c_4\Re_4(x) &= q(x);\\ c_2\Re'_2(x) \oplus c_4\Re_4(x) &= q(x) \oplus p(x);\\ x_{n+1}x_{n+2}(c_3\Re'_3(x) \oplus c_2\Re_2(x) \oplus c_1\Re_1(x)) &= 0.\end{aligned}$$

From the above relationships, we have

$$\begin{aligned}p(x) &= c_1\Re'_1(x) \oplus c_2\Re'_2(x)\\ &= (c_1\Re_1(x) \oplus c_2\Re_2(x))(\mathbf{a'} \cdot x) \oplus \ell(x)\\ &= c_3\Re'_3(x)(\mathbf{a'} \cdot x) \oplus \ell(x)\\ &= c_3\left(\Re_3(x)(\mathbf{a'} \cdot x) \oplus \ell'(x)\right)(\mathbf{a'} \cdot x) \oplus \ell(x)\\ &= c_3\Re_3(x)(\mathbf{a'} \cdot x) \oplus c_3\ell'(x)(\mathbf{a'} \cdot x) \oplus \ell(x),\end{aligned} \tag{6.4}$$

where $\deg(\ell) \leq n/2 - 1$, $\Re'_3(x) = \Re_3(x)(\mathbf{a'} \cdot x) \oplus \ell'(x), \deg(\ell') \leq n/2 - 2$. However, from (6.4), we find $\deg(p) \leq n/2 - 1$ since $\deg(\Re_3) = n/2 - 2$, $\deg(\ell') \leq n/2 - 2$ and $\deg(\ell) \leq n/2 - 1$.

Thus, for $A_{n+2} = (\mathbf{a'}, 1, 1)$ there do not exist an invertible matrix A and a vector $\mathbf{b} \in \mathbb{F}_2^{n+2}$ such that $\Im(x, x_{n+1}, x_{n+2})$ equals $x_{n+2}p(x) \oplus (x_{n+1} \oplus x_{n+2})q(x)$.

3. Assuming that $A_{n+2} = (\mathbf{a'}, 1, 0)$, we have

$$\begin{aligned}&(A_{n+2} \cdot \mathbf{x} \oplus b_{n+2})\wp(x, x_{n+1}, x_{n+2}) = c_4(\mathbf{a'} \cdot x)\Re_4(x)\\ &\oplus c_1 x_{n+1}\Re_1(x)(\mathbf{a'} \cdot x) \oplus c_2 x_{n+2}\Re_2(x)(\mathbf{a'} \cdot x) \oplus c_1 x_{n+1}\Re_1(x)\\ &\oplus c_3 x_{n+1}x_{n+2}\Re_3(x)(\mathbf{a'} \cdot x) \oplus c_2 x_{n+1}x_{n+2}\Re_2(x)\\ &\oplus c_3 x_{n+1}x_{n+2}\Re_3(x) \oplus c_4 x_{n+1}\Re_4(x) \oplus b_{n+2}\wp(x, x_{n+1}, x_{n+2}).\end{aligned}$$

Moreover, combining (6.1) and (6.2), we have $p(x) \oplus q(x) = c_2\Re'_2(x)$ and $c_3\Re'_3(x) = c_2\Re_2(x)$. Further, we have $c_2 = c_3 = 1$ and

$$\begin{aligned}&(\Re_3(x)(\mathbf{a'} \cdot x) \oplus \ell'(x) = \Re_2(x))\\ \Longleftrightarrow\quad &(\Re_3(x)(\mathbf{a'} \cdot x) \oplus \ell'(x)(\mathbf{a'} \cdot x) = \Re_2(x)(\mathbf{a'} \cdot x)),\end{aligned}$$

where $\deg(\ell') \leq n/2 - 2$. It is easy to find $\deg(\Re_3(x)(\mathbf{a'} \cdot x) \oplus \ell'(x)(\mathbf{a'} \cdot x)) \leq n/2 - 1$. However, $\deg(\Re_2(x)(\mathbf{a'} \cdot x)) = \deg(p(x) \oplus q(x)) = n/2$. Thus, if $A_{n+2} = (\mathbf{a'}, 1, 0)$ then there do not exist an invertible matrix A and a vector $\mathbf{b} \in \mathbb{F}_2^{n+2}$ such that $\Im(x, x_{n+1}, x_{n+2})$ equals $x_{n+2}p(x) \oplus (x_{n+1} \oplus x_{n+2})q(x)$.

4. Assume that $A_{n+2} = (\mathbf{a'}, 0, 0)$. If the relationship (3.6) holds, then we have

$$\begin{aligned} & f'(A\mathbf{x} \oplus \mathbf{b}) \\ = {} & 1_\Delta(A\mathbf{x} \oplus \mathbf{b}) \oplus f_0(A\mathbf{x} \oplus \mathbf{b}) \\ \oplus {} & (\mathbf{a'} \cdot x \oplus b_{n+2}) 1_\Delta(A\mathbf{x} \oplus \mathbf{b}) \\ \oplus {} & (A_{n+1} \cdot \mathbf{x} \oplus b_{n+1})(\mathbf{a'} \cdot x \oplus b_{n+2}) \oplus A_{n+1} \cdot \mathbf{x} \oplus b_{n+1} \\ = {} & f(x, x_{n+1}, x_{n+2}). \end{aligned}$$

The above relationship also implies the following,

$$\begin{aligned} & (\mathbf{a'} \cdot x) f'(A\mathbf{x} \oplus \mathbf{b}) \\ = {} & (\mathbf{a'} \cdot x) f_0(A_1 \cdot \mathbf{x} \oplus b_1, \ldots, A_n \cdot \mathbf{x} \oplus b_n) \\ \oplus {} & (\mathbf{a'} \cdot x) b_{n+2} 1_\Delta(A_1 \cdot \mathbf{x} \oplus b_1, \ldots, A_n \cdot \mathbf{x} \oplus b_n) \\ \oplus {} & (\mathbf{a'} \cdot x)(A_{n+1} \cdot \mathbf{x} \oplus b_{n+1})(\mathbf{a'} \cdot x \oplus b_{n+2}) \\ \oplus {} & (\mathbf{a'} \cdot x)(A_{n+1} \cdot \mathbf{x} \oplus b_{n+1}) \\ = {} & (\mathbf{a'} \cdot x)(x_{n+1} \oplus x_{n+2})(f_0(x) \oplus f_1(x)) \\ \oplus {} & (\mathbf{a'} \cdot x) x_{n+2} 1_\Delta(x) \oplus (\mathbf{a'} \cdot x) 1_\Delta(x) \\ \oplus {} & (\mathbf{a'} \cdot x) f_0(x) \oplus (\mathbf{a'} \cdot x) x_{n+1} x_{n+2} \oplus (\mathbf{a'} \cdot x) x_{n+1}. \end{aligned}$$

It is easy to deduce that $\deg((\mathbf{a'} \cdot x) f'(A\mathbf{x} \oplus \mathbf{b})) \leq n/2 + 1$. It is sufficient to show that $\deg((\mathbf{a'} \cdot x) f(x, x_{n+1}, x_{n+2})) > n/2 + 1$.

Since the algebraic immunity of any bent function is strictly greater than 1 [83], we know $(\mathbf{a'} \cdot x)\ (f_0(x) \oplus f_1(x)) \neq$ *constant*, that is,

$$\deg\left((\mathbf{a'} \cdot x)(x_{n+1} \oplus x_{n+2})(f_0(x) \oplus f_1(x))\right) \geq 3.$$

Now we show that $\deg\left((\mathbf{a'} \cdot x)(f_0(x) \oplus f_1(x))\right) = n/2+1$. Since $f_0 \oplus f_1 \in \mathcal{PS}^-$, we have $supp(f_0 \oplus f_1) = \bigcup_{i=1}^{2^{n/2-1}} H_i^*$, where H_i is an $n/2-$dimensional subspace of $\mathbb{F}_2^n$, $H_i \cap H_j = \{0_n\}$ for $1 \leq i < j \leq 2^{n/2-1}$ and $H_i^* = H_i \setminus \{0_n\}$. Thus, since $(\mathbf{a'} \cdot x)(f_0(x) \oplus f_1(x)) \neq$ *constant*, there exists at least one $H_{i_1}^*$ such that $E \cap H_{i_1}^* \neq \emptyset$,where $E = \{x \mid \mathbf{a'} \cdot x = 1, x \in \mathbb{F}_2^n\}$. It is clear that $E \cap H_{i_1}^* = E \cap H_{i_1}$.

From (2.1), $\deg\left((\mathbf{a'} \cdot x)(f_0(x) \oplus f_1(x))\right)$ equals the maximum dimension of all the linear (resp. affine) subspaces of $\mathbb{F}_2^n$ on which $(\mathbf{a'} \cdot x)(f_0(x) \oplus f_1(x))$ takes the value 1 an odd number of times [12]. We know $(E \cap H_i^*) \cup (\overline{E} \cap H_i) = H_i$ for any $i \in \{1, 2, \ldots, n\}$, where $\overline{E} = \{x \mid \mathbf{a'} \cdot x = 0, x \in \mathbb{F}_2^n\}$. For $i = i_1$, set $D_{i_1} = \overline{E} \cap H_{i_1}$, so we have $E \cap H_i^* = \alpha \oplus D_{i_1} = \{\alpha \oplus y \mid y \in \overline{E} \cap H_{i_1}\}$, where $\alpha \in E \cap H_{i_1}^*$.

Let $D_{i_1}^\perp$ denote a subspace of $\mathbb{F}_2^n$ such that $\dim(D_{i_1}) + \dim(D_{i_1}^\perp) = n$ and $D_{i_1} \cap D_{i_1}^\perp = \{0_n\}$. It is easy to deduce that $|(E \cap H_i^*) \setminus D_{i_1}^\perp| \geq 2^{n/1-1} - 1$. Set $\alpha \in (E \cap H_i^*) \setminus D_{i_1}^\perp$, we have $E \cap H_i^* = \alpha \oplus D_{i_1} (= \{\alpha \oplus y \mid y \in \overline{E} \cap H_{i_1}\})$.

Thus, D_{i_1} is a subspace of H_{i_1}, and its dimension is $n/2-1$. The dimension of the flat $E\cap H_{i_1}^*$ is equal to $n/2-1$. Further, we have

$$(\alpha\oplus D_{i_1})\cap(\alpha\oplus D_{i_1}^{\perp})=\{\alpha\}. \tag{6.5}$$

In addition, we have $|(E\cap H_j^*)\cap(\alpha\oplus D_{i_1}^{\perp})|$ is even, where $j\neq i_1, E\cap H_j^*\neq\emptyset$. In fact, if there exists one vector γ such that $\gamma\in(E\cap H_j^*)\cap(\alpha\oplus D_{i_1}^{\perp})$, then $\gamma\oplus(E\cap H_j^*)$ is a subspace and $(\alpha\oplus\gamma)\oplus D_{i_1}^{\perp}(=D_{i_1}^{\perp})$ is also a subspace. Thus, we have

$$|(\gamma\oplus(E\cap H_j^*))\cap D_{i_1}^{\perp}|=|(E\cap H_j^*)\cap(\gamma\oplus D_{i_1}^{\perp})| \tag{6.6}$$

is even. Combining (6.5) and (6.6), we find an affine subspace $\gamma\oplus D_{i_1}^{\perp}$ on which $(\mathbf{a'}\cdot x)(f_0(x)\oplus f_1(x))$ takes value 1 an odd number of times, that is, $\deg((\mathbf{a'}\cdot x)(f_0(x)\oplus f_1(x)))\geq\dim(\gamma\oplus D_{i_1}^{\perp})=n-\dim(D_{i_1})=n/2+1$.

□

Proof of Lemma 3.1.6:

Proof. The fact that f defined by (3.7) is bent follows directly from Theorem 3.1.1 by noting that f_0, f_1, $f_0\oplus 1_\Delta$, $f_1\oplus 1_\Delta$ are also bent, where $\Delta=E_1\times E_2$.

Using the definition of f and the above existence assumptions we need to show that $D_aD_bf(x)\neq 0$, for the above specified vectors. The second derivative of f with respect to a and b can be written as,

$$\begin{aligned}
&D_{(a_1,a_2,a_3,a_4)}D_{(b_1,b_2,b_3,b_4)}f(x,x_{n+1},x_{n+2})\\
&=(x_{n+1}\oplus x_{n+2})\big[D_{a_2}D_{b_2}(\pi\oplus\phi)(x^{(2)})\cdot x^{(1)}\\
&\oplus D_{b_2}(\pi\oplus\phi)(x^{(2)}\oplus a_2)\cdot a_1\oplus D_{a_2}(\pi\oplus\phi)(x^{(2)}\oplus b_2)\cdot b_1\big]\\
&\oplus(a_3\oplus a_4)\big[D_{b_2}(\pi\oplus\phi)(x^{(2)}\oplus a_2)\cdot(x^{(1)}\oplus a_1)\\
&\oplus b_1\cdot(\pi\oplus\phi)(x^{(2)}\oplus a_2\oplus b_2)\big]\\
&\oplus(b_3\oplus b_4)\big[D_{a_2}(\pi\oplus\phi)(x^{(2)}\oplus b_2)\cdot(x^{(1)}\oplus b_1)\\
&\oplus a_1\cdot(\pi\oplus\phi)(x^{(2)}\oplus a_2\oplus b_2)\big]\\
&\oplus\big[D_{a_2}D_{b_2}(\pi)(x^{(2)})\cdot x^{(1)}\oplus D_{b_2}\pi(x^{(2)}\oplus a_2)\cdot a_1\\
&\oplus D_{a_2}\pi(x^{(2)}\oplus b_2)\cdot b_1\big]\oplus a_3b_4\oplus a_4b_3\\
&\oplus(x_{n+2}\oplus 1)D_{(a_1,a_2)}D_{(b_1,b_2)}[1_{E_1}(x^{(1)})1_{E_2}(x^{(2)})]\\
&\oplus a_4D_{(b_1,b_2)}[1_{E_1}(x^{(1)}\oplus a_1)1_{E_2}(x^{(2)}\oplus a_2)]\\
&\oplus b_4D_{(a_1,a_2)}[1_{E_1}(x^{(1)}\oplus b_1)1_{E_2}(x^{(2)}\oplus b_2)].
\end{aligned} \tag{6.7}$$

We first notice the following facts regarding $D_aD_bf(x,x_{n+1},x_{n+2})$. It is sufficient that $D_{a_2}D_{b_2}(\pi\oplus\phi)(x^{(2)})\neq 0$ so that $D_aD_bf(x,x_{n+1},x_{n+2})\neq 0$ due to the involvement of the variables x_{n+1},x_{n+2} (the first term in the second equality above). Thus, $a_2\neq b_2\neq 0_{\frac{n}{2}}$ gives $D_aD_bf(x,x_{n+1},x_{n+2})\neq 0$ immediately. Let us consider this derivative for the different cases.

1. Let $a=(a_1,0_{\frac{n}{2}},a_3,0), b=(b_1,0_{\frac{n}{2}},b_3,0)\in\Lambda\setminus\{0_{n+2}\}$ such that $a_3=b_3=1$, or $a_3=0,b_3=1$, or $a_3=1,b_3=0$. In this case the only term that depends

exclusively on $x^{(2)}$ in (6.7) is $a_3\left((\pi\oplus\phi)(x^{(2)})\cdot b_1\right)\oplus b_3\left((\pi\oplus\phi)(x^{(2)})\cdot a_1\right)$ since $\nu\cdot(\pi\oplus\phi)\neq \mathit{constant}$ for $\nu\in\mathbb{F}_2^{\frac{n}{2}}\setminus\{0_{\frac{n}{2}}\}$. Therefore,

$$D_{(a_1,0_{\frac{n}{2}},a_3,0)}D_{(b_1,0_{\frac{n}{2}},b_3,0)}f(x,x_{n+1},x_{n+2})\neq 0.$$

2. Assume there exist $a,b\in V$ such that $(a_2,a_4)\neq(b_2,b_4)$, $D_{a_2}D_{b_2}(\pi\oplus\varphi)(x^{(2)})\neq 0$ and $a_4=b_4=0$ (their existence is proven in Proposition 3.1.7). Then, $D_{a_2}D_{b_2}(\pi\oplus\phi)(x^{(2)})\neq 0$ and consequently $D_aD_bf(x,x_{n+1},x_{n+2})\neq 0$.

3. In this case there always exists $a=(a_1,0_{\frac{n}{2}},a_3,0)\in V$, where $(a_1,a_3)\neq 0_{\frac{n}{2}+1}$. By assumption we can find $b^{(1)}=(b_1^{(1)},b_2^{(1)},b_3^{(1)},b_4^{(1)})\in V$ such that $b_2^{(1)}\neq 0_{\frac{n}{2}}$ and $b_3^{(1)}=b_4^{(1)}$, and $b^{(2)}=(b_1^{(2)},b_2^{(2)},b_3^{(2)},b_4^{(2)})\in V$ such that $b_2^{(2)}\neq 0_{\frac{n}{2}}$ and $D_{b_2^{(2)}}(\pi\oplus\phi)(x^{(2)})\neq$ *constant*. There are two cases to consider.

   i) If $a_3=0$ and consequently $a_1\neq 0_{\frac{n}{2}}$, we find $b^{(1)}=(b_1^{(1)},b_2^{(1)},b_3^{(1)},b_4^{(1)})\in V$ such that $b_2^{(1)}\neq 0_{\frac{n}{2}}$ and $b_3^{(1)}=b_4^{(1)}$. Then, (6.7) gives

$$\begin{aligned}&D_aD_{b^{(1)}}f(x,x_{n+1},x_{n+2})\\ =&(x_{n+1}\oplus x_{n+2})[D_{b_2^{(1)}}(\pi\oplus\phi)(x^{(2)})\cdot a_1]\oplus D_{b_2^{(1)}}\pi(x^{(2)})\cdot a_1\\ &\oplus(x_{n+2}\oplus 1)D_{(a_1,a_2)}D_{(b_1^{(1)},b_2^{(1)})}[1_{E_1}(x^{(1)})1_{E_2}(x^{(2)})]\\ &\oplus b_4D_{(a_1,a_2)}[1_{E_1}(x^{(1)}\oplus b_1^{(1)})1_{E_2}(x^{(2)}\oplus b_2^{(1)})],\end{aligned}$$

   which is nonconstant assuming that π has no linear structures (i.e., $D_{b_2^{(1)}}\pi(x^{(2)})\cdot a_1$ does not equal a constant and only depends on $x^{(2)}$).

   ii) If $a_3=1$ and consequently $a_3\oplus a_4=1$, we find $b^{(2)}=(b_1^{(2)},b_2^{(2)},b_3^{(2)},b_4^{(2)})\in V$ such that $b_2^{(2)}\neq 0_{\frac{n}{2}}$ and $D_{b_2^{(2)}}(\pi\oplus\phi)(x^{(2)})\neq$ *constant*. There are also two cases to consider.

   (a) If $a_1\neq 0_{\frac{n}{2}}$, (6.7) gives,

$$\begin{aligned}&D_aD_{b^{(2)}}f(x,x_{n+1},x_{n+2})\\ =&(x_{n+1}\oplus x_{n+2})[D_{b_2^{(2)}}(\pi\oplus\phi)(x^{(2)})\cdot a_1]\\ &\oplus D_{b_2^{(2)}}(\pi\oplus\phi)(x^{(2)})\cdot(x^{(1)}\oplus a_1)\oplus b_1^{(2)}\cdot(\pi\oplus\phi)(x^{(2)}\oplus b_2^{(2)})\\ &\oplus(b_3^{(2)}\oplus b_4^{(2)})[D_{a_2}(\pi\oplus\phi)(x^{(2)}\oplus b_2^{(2)})\cdot(x^{(1)}\oplus b_1^{(2)})\\ &\oplus a_1\cdot(\pi\oplus\phi)(x^{(2)}\oplus b_2^{(2)})]\oplus D_{b_2^{(2)}}\pi(x^{(2)})\cdot a_1\\ &\oplus(x_{n+2}\oplus 1)D_{(a_1,a_2)}D_{(b_1^{(2)},b_2^{(2)})}[1_{E_1}(x^{(1)})1_{E_2}(x^{(2)})]\\ &\oplus b_4D_{(a_1,a_2)}[1_{E_1}(x^{(1)}\oplus b_1^{(2)})1_{E_2}(x^{(2)}\oplus b_2^{(2)})]\oplus a_3b_4^{(2)},\end{aligned}$$

   which is nonconstant since $(x_{n+1}\oplus x_{n+2})(D_{b_2^{(2)}}(\pi\oplus\phi)(x^{(2)})\cdot a_1)$ does not equal a constant and depends on $(x_{n+1}\oplus x_{n+2})$.

(b) If $a_1 = 0_{\frac{n}{2}}$, (6.7) gives,

$$\begin{aligned}&D_a D_{b^{(2)}} f(x,x_{n+1},x_{n+2}) = D_{b_2^{(2)}}(\pi\oplus\phi)(x^{(2)})\cdot x^{(1)}\\&\oplus b_1^{(2)}\cdot(\pi\oplus\phi)(x^{(2)}\oplus b_2^{(2)})\oplus b_4^{(2)},\end{aligned}$$

which is nonconstant since $D_{b_2^{(2)}}(\pi\oplus\phi)(x^{(2)})\cdot x^{(1)}$ does not equal a constant and depends on $x^{(1)}$ and $x^{(2)}$.

4. Since there exist $a = (a_1, 0_{\frac{n}{2}}, 0, 0) \in \Lambda$ and $b = (b_1, 0_{\frac{n}{2}}, 1, 1) \in V$ such that $D_{a_1}1_{E_1}(x^{(1)}) \neq 0$, then (6.7) gives,

$$\begin{aligned}&D_{(a_1,0_{\frac{n}{2}},0,0)}D_{(b_1,0_{\frac{n}{2}},1,1)}f(x,x_{n+1},x_{n+2})\\=\ &(x_{n+2}\oplus 1)D_{(a_1,0_{\frac{n}{2}})}D_{(b_1,0_{\frac{n}{2}})}[1_{E_1}(x^{(1)})1_{E_2}(x^{(2)})]\\\oplus\ &b_4 D_{(a_1,0_{\frac{n}{2}})}[1_{E_1}(x^{(1)}\oplus b_1)1_{E_2}(x^{(2)})]\\=\ &(x_{n+2}\oplus 1)1_{E_2}(x^{(2)})D_{a_1}D_{b_1}(1_{E_1}(x^{(1)}))\\\oplus\ &1_{E_2}(x^{(2)})D_{a_1}(1_{E_1}(x^{(1)}\oplus b_1))\neq 0.\end{aligned}$$

5. Since there exist $a = (a_1, 0_{\frac{n}{2}}, 0, 0) \in \Lambda$ and $b = (b_1, 0_{\frac{n}{2}}, 0, 1) \in V$, then (6.7) gives,

$$\begin{aligned}&D_{(a_1,0_{\frac{n}{2}},0,0)}D_{(b_1,0_{\frac{n}{2}},0,1)}f(x,x_{n+1},x_{n+2})\\&=(\pi\oplus\varphi)(x^{(2)})\cdot a_1\oplus(x_{n+2}\oplus 1)1_{E_2}(x^{(2)})D_{a_1}D_{b_1}1_{E_1}(x^{(1)})\\&\oplus 1_{E_2}(x^{(2)})D_{a_1}1_{E_1}(x^{(1)}\oplus b_1)\neq 0,\end{aligned}$$

since $D_{a_1}1_{E_1}(x^{(1)}) \neq$ *constant* and
$1_{E_2}(x^{(2)})D_{a_1}[1_{E_1}(x^{(1)}\oplus b_1)]$ depends on $x^{(1)}$ and $x^{(2)}$.

6. Since there exist $a = (a_1, 0_{\frac{n}{2}}, 0, 0) \in \Lambda$ and $b = (b_1, b_2, b_3, b_4) \in V$ such that $D_{a_1}D_{b_1}1_{E_1}(x^{(1)}) \neq 0$, then (6.7) gives,

$$\begin{aligned}&D_{(a_1,a_2,a_3,a_4)}D_{(b_1,b_2,b_3,b_4)}f(x,x_{n+1},x_{n+2})\\&=(x_{n+1}\oplus x_{n+2})(D_{b_2}(\pi\oplus\varphi)(x^{(2)})\cdot a_1)\\&\oplus(b_3\oplus b_4)\big[(\pi\oplus\varphi)(x^{(2)}\oplus b_2)\cdot a_1\big]\oplus D_{b_2}\pi(x^{(2)})\cdot a_1\\&\oplus(x_{n+2}\oplus 1)D_{(a_1,0_{\frac{n}{2}})}D_{(b_1,b_2)}[1_{E_1}(x^{(1)})1_{E_2}(x^{(2)})]\\&\oplus b_4 D_{(a_1,0_{\frac{n}{2}})}(1_{E_1}(x^{(1)}\oplus b_1)1_{E_2}(x^{(2)}\oplus b_2)).\end{aligned}$$

From the above relation, we know if $D_{a_1}D_{b_1}1_{E_1}(x^{(1)}) \neq\ 0$, then

$$\begin{aligned}&D_{(a_1,0_{\frac{n}{2}})}D_{(b_1,b_2)}(1_{E_1}(x^{(1)})1_{E_2}(x^{(2)}))\\&=1_{E_2}(x^{(2)})D_{a_1}D_{b_1}1_{E_1}(x^{(1)})\\&\oplus D_{b_2}1_{E_2}(x^{(2)})D_{a_1}1_{E_1}(x^{(1)}\oplus b_1)\neq\ 0.\end{aligned}$$

Hence, $(x_{n+2}\oplus 1)D_{(a_1,0_{\frac{n}{2}})}D_{(b_1,b_2)}(1_{E_1}(x^{(1)})1_{E_2}(x^{(2)}))$ depends on x_{n+2}, and does not depend on x_{n+1}. If $D_{b_2}\big((\pi\oplus\varphi)(x^{(2)})\cdot a_1\big)\neq 0$, then $(x_{n+1}\oplus x_{n+2})D_{b_2}\big((\pi\oplus\varphi)(x^{(2)})\cdot a_1\big)$ depends on $x_{n+2}\oplus x_{n+1}$. Hence, we have

$$D_{(a_1,a_2,a_3,a_4)}D_{(b_1,b_2,b_3,b_4)}f(x,x_{n+1},x_{n+2})\neq 0.$$

□

Proof of Proposition 3.1.7:

Proof. Let, as before, V be an arbitrary $\frac{n+2}{2}$-dimensional subspace of $\mathbb{F}_2^{n+2}$ and $\Lambda = \{(x^{(1)}, 0_{\frac{n}{2}}, x_{n+1}, 0) \mid x^{(1)} \in \mathbb{F}_2^{\frac{n}{2}}, x_{n+1} \in \mathbb{F}_2\}$. Also, any $a \in \mathbb{F}_2^{n+2}$ is written as $a = (a_1, a_2, a_3.a_4) \in \mathbb{F}_2^{\frac{n}{2}} \times \mathbb{F}_2^{\frac{n}{2}} \times \mathbb{F}_2 \times \mathbb{F}_2$.

1. The case $V = \Lambda$ is trivial since we can always find nonzero vectors $(a_1, 0_{\frac{n}{2}}, a_3, 0)$, $(b_1, 0_{\frac{n}{2}}, b_3, 0) \in \Lambda$ such that $a_3 = b_3 = 1$, or $a_3 = 0, b_3 = 1$, or $a_3 = 1, b_3 = 0$.

2. If $\dim(V \cap \Lambda) = 0$, (so that these subspaces intersect in $\{0_{n+2}\}$), then we want to show the existence of $a, b \in V$ such that $(a_2, a_4) \neq (b_2, b_4)$, $D_{a_2} D_{b_2}(\pi \oplus \varphi)(x^{(2)}) \neq 0$ and $a_4 = b_4 = 0$. The condition $(a_2, a_4) \neq (b_2, b_4)$ is actually true for any two vectors $a, b \in V$. Indeed, assuming $(a_2, a_4) = (b_2, b_4)$ implies that $a \oplus b = (a_1 \oplus b_1, 0_{\frac{n}{2}}, a_3 \oplus b_3, 0) \in \Lambda$, a contradiction. It is also easy to verify that we can find $a, b \in V$ such that $a_4 = b_4 = 0$, $a_2 \neq b_2$ and $D_{a_2} D_{b_2}(\pi \oplus \varphi)(x^{(2)}) \neq 0$. This comes from the fact that $|V| = 2^{\frac{n+2}{2}}$ and $(a_2, a_4) \neq (b_2, b_4)$ for any $a, b \in V$, which implies $\{(v_2^{(1)}, v_4^{(1)}), (v_2^{(2)}, v_4^{(2)}), \ldots, (v_2^{(2^{\frac{n+2}{2}})}, v_4^{(2^{\frac{n+2}{2}})})\} = \mathbb{F}_2^{\frac{n}{2}} \times \mathbb{F}_2$.

3. If $|V \cap \Lambda| = 2$, then there exists $a \neq 0_{n+2}$ such that $a = (a_1, 0_{\frac{n}{2}}, a_3, 0) \in V \cap \Lambda$ for which $(a_1, a_3) \neq 0_{\frac{n}{2}+1}$. We need to show the existence of $b^{(1)} = (b_1^{(1)}, b_2^{(1)}, b_3^{(1)}, b_4^{(1)}) \in V$ such that $b_2^{(1)} \neq 0_{\frac{n}{2}}$ and $b_3^{(1)} = b_4^{(1)}$, and $b^{(2)} = (b_1^{(2)}, b_2^{(2)}, b_3^{(2)}, b_4^{(2)}) \in V$ such that $b_2^{(2)} \neq 0_{\frac{n}{2}}$ and $D_{b_2^{(2)}}(\pi \oplus \phi)(x^{(2)}) \neq$ *constant*.

   To show this, we first prove $|\{v_2^{(1)}, v_2^{(2)}, \ldots, v_2^{(2^{\frac{n+2}{2}})}\}| \geq 2^{\frac{n}{2}-1}$. Suppose cardinality $|\{v_2^{(1)}, v_2^{(2)}, \ldots, v_2^{(2^{\frac{n+2}{2}})}\}|$ is strictly less than $2^{\frac{n}{2}-1}$ (counting different elements in the multiset). Then, there must exist at least 8 vectors $v^{(j_1)}, v^{(j_2)}, \ldots, v^{(j_8)}$ such that $v_2^{(j_1)} = v_2^{(j_2)} = \ldots = v_2^{(j_8)}$. Further, without loss of generality, let $v_4^{(j_1)} \neq v_4^{(j_2)}$. Since $v_4^{(i)} \in \mathbb{F}_2$, for $i = 1, 2, \ldots, 2^{\frac{n+2}{2}}$, there are at least three vectors $v^{(j_{t1})}, v^{(j_{t2})}, v^{(j_{t3})}$, which belong to $\{v^{(j_3)}, \ldots, v^{(j_8)}\}$, such that $v_4^{(j_{t1})} = v_4^{(j_{t2})} = v_4^{(j_{t3})}$. Thus, we have $v_4^{(j_1)} = v_4^{(j_{t1})} = v_4^{(j_{t2})} = v_4^{(j_{t3})}$ (or $v_4^{(j_2)} = v_4^{(j_{t1})} = v_4^{(j_{t2})} = v_4^{(j_{t3})}$), that is, $v^{(j_1)} \oplus v^{(j_{t1})}, v^{(j_1)} \oplus v^{(j_{t2})}, v^{(j_1)} \oplus v^{(j_{t3})}$ (or $v^{(j_2)} \oplus v^{(j_{t1})}, v^{(j_2)} \oplus v^{(j_{t2})}, v^{(j_2)} \oplus v^{(j_{t3})}$) belong to $V \cap \Lambda$. This is in contradiction with $|V \cap \Lambda| = 2$. Hence, $|\{v_2^{(1)}, v_2^{(2)}, \ldots, v_2^{(2^{\frac{n+2}{2}})}\}| \geq 2^{\frac{n}{2}-1} > 4$ (since $n > 4$). Further, it is easy to find $b^{(1)} \in V$ such that $b_2^{(1)} \neq 0_{\frac{n}{2}}$ and $b_3^{(1)} = b_4^{(1)}$. By assumption, $\max_{\nu \in \mathbb{F}_2^{\frac{n}{2}}} \deg(\nu \cdot (\pi \oplus \phi)) \geq 2$. Thus, according to Lemma 3.1.5, we are able to find $b^{(2)} \in V$ such that $b_2^{(2)} \neq 0_{\frac{n}{2}}$ and $D_{b_2^{(2)}}(\pi \oplus \phi)(x^{(2)}) \neq$ *constant*.

4. If $|V \cap \Lambda| = t > 2$, then we write $V \cap \Lambda = \{v^{(1)}, \ldots, v^{(t)}\}$, where $t = 2^r$ for $r = 2, \ldots, n/2$. There are two cases to be considered.

(a) If there exist at least two vectors $(a_1, 0_{\frac{n}{2}}, a_3, 0), (b_1, 0_{\frac{n}{2}}, b_3, 0) \in V \cap \Lambda$ such that $a_3 = b_3 = 1$, or $a_3 = 0, b_3 = 1$, or $a_3 = 1, b_3 = 0$ (that is, there exists $i \in \{1, 2, \ldots, t\}$ such that $v_3^{(i)} \neq 0$), then a, b fall under item $i)$ in Lemma 3.1.6.

(b) If $v_3^{(i)} = 0$ for $i = 1, 2, \ldots, t$, then there are three cases to be considered.

i. If $v_2^{(i)} = 0_{\frac{n}{2}}$ for $i = 1, 2, \ldots, 2^{\frac{n}{2}+1}$, we have two cases:

- If $v_3^{(i)} = v_4^{(i)}$ (i.e., $v_3^{(i)} = v_4^{(i)} = 1$) for $i = t+1, \ldots, 2^{\frac{n}{2}+1}$, since $|V| = 2^{\frac{n}{2}+1}$, then $\{v_1^{(1)}, v_1^{(2)}, \ldots, v_1^{(2^{\frac{n}{2}+1})}\} = \mathbb{F}_2^{\frac{n}{2}}$. Thus, there exists one vector $(v_1^{(j_1)}, 0_{\frac{n}{2}}, 0, 0)$ such that $D_{v_1^{(j_1)}} 1_{E_1}(x^{(1)}) \neq 0$ since $\deg(1_{E_1}(x^{(1)})) \geq 2$.
  Set $(a_1, a_2, a_3, a_4) = (v_1^{(j_1)}, 0_{\frac{n}{2}}, 0, 0) \in V \cap \Lambda, (b_1, b_2, b_3, b_4) = (b_1, 0_{\frac{n}{2}}, 1, 1) \in V$. Then, a, b fall under item $iv)$ in Lemma 3.1.6.

- If there exists a vector $v^{(j_1)}$ such that $v_3^{(j_1)} \neq v_4^{(j_1)}$ for $j_1 \in \{t+1, \ldots, 2^{\frac{n}{2}+1}\}$, then $v_3^{(j_1)} = 0, v_4^{(j_1)} = 1$ since $v_3^{(i)} = 0$ for $i = 1, 2, \ldots, t$. Further, we have $v_3^{(i)} = 0, v_4^{(i)} = 1$, for $i = t+1, \ldots, 2^{\frac{n}{2}+1}$. Similarly, if there exists a vector $v^{(j_2)}$ such that $v_3^{(j_2)} = 1, v_4^{(j_2)} = 1$, then there must exist a vector $v^{(j_3)}$ such that $v_3^{(j_3)} = 1, v_4^{(j_2)} = 0$, where $j_2, j_3 \in \{t+1, \ldots, 2^{\frac{n}{2}+1}\}$. However, it is in contradiction with $v_3^{(i)} = 0$, for $i = 1, 2, \ldots, t$. Hence, $\{v_1^{(1)}, v_1^{(2)}, \ldots, v_1^{(2^{\frac{n}{2}+1})}\} = \mathbb{F}_2^{\frac{n}{2}}$. Thus, there exists one vector $(v_1^{(\ell)}, 0_{\frac{n}{2}}, 0, 0)$ such that $D_{v_1^{(\ell)}} 1_{E_1}(x^{(1)}) \neq 0$ since $\deg(1_{E_1}(x^{(1)})) \geq 2$. We set $(a_1, a_2, a_3, a_4) = (v_1^{(\ell)}, 0_{\frac{n}{2}}, 0, 0) \in V \cap \Lambda, (b_1, b_2, b_3, b_4) = (v_1^{(j_1)}, 0_{\frac{n}{2}}, 0, 1) \in V$. Then, a, b fall under item $v)$ in Lemma 3.1.6.

ii. For $|\{v_2^{(1)}, v_2^{(2)}, \ldots, v_2^{(2^{\frac{n+2}{2}})}\}| = 2$, without loss of generality, let the set $\{v_2^{(1)}, v_2^{(2)}, \ldots, v_2^{(2^{\frac{n+2}{2}})}\} = \{0_{\frac{n}{2}}, d_2\}$, where $d_2 \in \mathbb{F}_2^{\frac{n}{2}} \setminus \{0_{\frac{n}{2}}\}$.

- If there exists one vector $(v_1^{(i_1)}, v_2^{(i_1)}, v_3^{(i_1)}, v_4^{(i_1)}) \in V$ such that $v_2^{(i_1)} \neq 0_{\frac{n}{2}}$ and $v_3^{(i_1)} = v_4^{(i_1)}$, then set $(a_1, a_2, a_3, a_4) = (a_1, 0_{\frac{n}{2}}, 0, 0) \in (V \cap \Lambda), (b_1, b_2, b_3, b_4) = (v_1^{(i_1)}, v_2^{(i_1)}, v_3^{(i_1)}, v_4^{(i_1)}) \in V$. Then, a, b fall under item $iii)$ in Lemma 3.1.6.

- If for any vector $v \in V$ such that $v_2 = d_2 \neq 0_{\frac{n}{2}}$, we always have $v_3 \neq v_4$, we denote these vectors such that $v_2 = d_2$ and $v_3 \neq v_4$ by $\{v^{(k_1)}, v^{(k_2)}, \ldots, v^{(k_\eta)}\}$. We consider two cases: $v_3^{(k_i)} = constant$ and $v_3^{(k_i)} \neq constant$ for $i = 1, 2, \ldots, \eta$.
  - If $v_3^{(k_i)} = constant$ for $i = 1, 2, \ldots, \eta$, then $v_2^{(k_i)} = d_2$ and $v_4^{(k_i)} = constant$ for $i = 1, 2, \ldots, \eta$. Thus, we have

$$\{(v_2^{(1)}, v_3^{(1)}, v_4^{(1)}), \ldots, (v_2^{(2^{\frac{n+2}{2}})}, v_3^{(2^{\frac{n+2}{2}})}, v_4^{(2^{\frac{n+2}{2}})})\} = \{(0_{\frac{n}{2}}, 0, 0), (d_2, v_3^{(k_1)}, v_4^{(k_1)})\}.$$

Also, $|\{v_1^{(1)},v_1^{(2)},\dots,v_1^{(2^{\frac{n+2}{2}})}\}|\cdot|\{(v_2^{(1)},v_3^{(1)},v_4^{(1)}),\dots,(v_2^{(2^{\frac{n+2}{2}})},v_3^{(2^{\frac{n+2}{2}})},v_4^{(2^{\frac{n+2}{2}})})\}|$ $\geq |\{v^{(1)},v^{(2)},\dots,v^{(2^{\frac{n+2}{2}})}\}|$, that is, $|\{v_1^{(1)},\dots,v_1^{(2^{\frac{n+2}{2}})}\}| = 2^{\frac{n}{2}}$. Thus, we are able to choose two vectors $a = (a_1, 0_{\frac{n}{2}}, 0, 0) \in V \cap \Lambda$ and $b = (b_1, d_2, b_3, b_4) \in V$ such that $D_{a_1}D_{b_1}1_{E_1}(x^{(1)}) \neq 0$ since $\deg(1_{E_1}(x^{(1)})) \geq 2$. Then, a, b fall under item $vi)$ in Lemma 3.1.6.

- If $v_3^{(k_i)} \neq \mathit{constant}$ for $i = 1, 2, \dots, \eta$, then there exist two vectors $v^{(j_1)}, v^{(j_2)} \in V$ such that $v_2^{(j_1)} = v_2^{(j_2)} = d_2$ and $v_3^{(j_1)} \neq v_3^{(j_2)}$. Thus, we have $v^{(j_1)} \oplus v^{(j_2)} = (v_1^{(j_1)} \oplus v_1^{(j_2)}, 0_{\frac{n}{2}}, 1, 1)$.

  From conditions $v_3^{(i)} = 0$ for $i = 1, \dots, t$, $|\{v_2^{(1)}, v_2^{(2)}, \dots, v_2^{(2^{\frac{n+2}{2}})}\}| = 2$, and we always have $v_3^{(l)} \neq v_4^{(l)}$ for $v_2^{(l)} = d_2 \neq 0_{\frac{n}{2}} \in V$, we know $|\{(v_2^{(1)}, v_3^{(1)}, v_4^{(1)}), \dots, (v_2^{(2^{\frac{n+2}{2}})}, v_3^{(2^{\frac{n+2}{2}})}, v_4^{(2^{\frac{n+2}{2}})})\} = \{(0_{\frac{n}{2}}, 0, 0),$ $(0_{\frac{n}{2}}, 1, 1), (d_2, 1, 0), (d_2, 0, 1)\}| = 4$. Further, $|\{v_1^{(1)}, v_1^{(2)}, \dots, v_1^{(2^{\frac{n+2}{2}})}\}|\cdot$ $|\{(v_2^{(1)}, v_3^{(1)}, v_4^{(1)}), \dots, (v_2^{(2^{\frac{n+2}{2}})}, v_3^{(2^{\frac{n+2}{2}})}, v_4^{(2^{\frac{n+2}{2}})})\}| \geq |\{v^{(1)}, v^{(2)}, \dots,$ $v^{(2^{\frac{n+2}{2}})}\}|$, that is, $|\{v_1^{(1)}, v_1^{(2)}, \dots, v_1^{(2^{\frac{n+2}{2}})}\}| \geq 2^{\frac{n}{2}-1}$. Thus, due to Lemma 3.1.5 and using $\deg(1_{E_1}(x^{(1)})) \geq 2$, we are able to choose one vector $a = (a_1, 0_{\frac{n}{2}}, 0, 0) \in V$ such that $D_{a_1}1_{E_1}(x^{(1)}) \neq \mathit{constant}$. Further, we are able to choose $b = (b_1, 0_{\frac{n}{2}}, 1, 1) \in V$. Then, a, b fall under item $iv)$ in Lemma 3.1.6.

iii. For $|\{v_2^{(1)}, v_2^{(2)}, \dots, v_2^{(2^{\frac{n+2}{2}})}\}| > 2$, there must exist $b \in V$ such that $b_2 \neq 0_{\frac{n}{2}}$ and $b_3 = b_4$. Since $|\{v_2^{(1)}, v_2^{(2)}, \dots, v_2^{(2^{\frac{n+2}{2}})}\}| > 2$, there must exist three vectors $v^{(i_1)}, v^{(i_2)} \in V$ and $v^{(i_1)} \oplus v^{(i_2)} \in V$. If $v^{(i_1)} \in V$ is such that $v_2^{(i_1)} \neq 0_{\frac{n}{2}}$ and $v_3^{(i_1)} = v_4^{(i_1)}$, then set $b = v^{(i_1)}$. If $v^{(i_2)} \in V$ is such that $v_2^{(i_2)} \neq 0_{\frac{n}{2}}$ and $v_3^{(i_2)} = v_4^{(i_2}$, then set $b = v^{(i_2)}$. Otherwise, set $b = v^{(i_1)} \oplus v^{(i_2)}$ (since if $u_3, v_3, u_4, v_4 \in \mathbb{F}_2$ such that $u_3 \neq u_4$ and $v_3 \neq v_4$, we have $u_3 \oplus v_3 = u_4 \oplus v_4$). We set $(a_1, a_2, a_3, a_4) = (a_1, 0_{\frac{n}{2}}, 0, 0) \in V \cap \Lambda$ such that $(a_1, a_3) \neq 0_{\frac{n}{2}+1}$. Then, a, b fall under item $iii)$ in Lemma 3.1.6.

□

Proof of Theorem 3.2.2:

Proof. Let $a^{(1)}, b^{(1)}, a^{(2)}, b^{(2)} \in \mathbb{F}_2^n$. We prove that f does not belong to $\mathcal{M}^{\#}$, by using Lemma 2.2.2. We need to show that there does not exist an $(\frac{n}{2})$-dimensional subspace V such that

$$D_{(a^{(1)},a^{(2)})}D_{(b^{(1)},b^{(2)})}f = 0,$$

for any $(a^{(1)}, a^{(2)})$, $(b^{(1)}, b^{(2)}) \in V$.

The second derivative of f with respect to a and b can be written as,

$$\begin{aligned}
& D_{(a^{(1)},a^{(2)})}D_{(b^{(1)},b^{(2)})}f(x) \\
= \;& x\cdot(D_{a^{(2)}}D_{b^{(2)}}\pi(y))\oplus a^{(1)}\cdot D_{b^{(2)}}\pi(y\oplus a^{(2)}) \\
& \oplus b^{(1)}\cdot D_{a^{(2)}}\pi(y\oplus b^{(2)})\oplus D_aD_b1_{E_1}(x)1_{E_2}(y) \\
= \;& x\cdot(D_{a^{(2)}}D_{b^{(2)}}\pi(y))\oplus a^{(1)}\cdot D_{b^{(2)}}\pi(y\oplus a^{(2)})\oplus b^{(1)}\cdot D_{a^{(2)}}\pi(y\oplus b^{(2)}) \quad (6.8) \\
& \oplus 1_{E_1}(x)D_{a^{(2)}}D_{b^{(2)}}1_{E_2}(y)\oplus 1_{E_2}(y\oplus a^{(2)})D_{a^{(1)}}1_{E_1}(x) \\
& \oplus 1_{E_2}(y\oplus b^{(2)})D_{b^{(1)}}1_{E_1}(x)\oplus 1_{E_2}(y\oplus a^{(2)}\oplus b^{(2)})D_{a^{(1)}\oplus b^{(1)}}1_{E_1}(x).
\end{aligned}$$

We denote the set $\{(x,0_n)\mid x\in\mathbb{F}_2^n\}$ by Δ, and consider two cases $V=\Delta$ and $V\neq\Delta$.

1. For $V=\Delta$, we can find two vectors $(a^{(1)},0_n),(b^{(1)},0_n)\in\Delta$ such that

   $$D_{a^{(1)}}D_{b^{(1)}}1_{E_1}(x)\neq 0$$

   since $\dim(E_1)\geq 2$. Further, we have

   $$\begin{aligned}
   D_{(a^{(1)},a^{(2)})}D_{(b^{(1)},b^{(2)})}f(x) &= 1_{E_2}(y)(D_{a^{(1)}}1_{E_1}(x)\oplus D_{b^{(1)}}1_{E_1}(x) \\
   &\quad \oplus D_{a^{(1)}\oplus b^{(1)}}1_{E_1}(x)) \\
   &= 1_{E_2}(y)D_{a^{(1)}}D_{b^{(1)}}1_{E_1}(x)\neq 0.
   \end{aligned}$$

2. For $V\neq\Delta$, we split the proof into three cases depending on the cardinality of $V\cap\Delta$. We set $V=\left\{(v_1^{(1)},v_2^{(1)}),(v_1^{(2)},v_2^{(2)}),\ldots,(v_1^{(2^n)},v_2^{(2^n)})\right\}$,

   (a) For $|V\cap\Delta|=1$, we have $v_2^{(i)}\neq v_2^{(j)}$ for any $i\neq j$. If there exist two vectors $v_2^{(i_1)},v_2^{(j_1)}$ such that $v_2^{(i_1)}=v_2^{(j_1)}$, then $v_1^{(i_1)}=v_1^{(j_1)}$, (or $(v_1^{(i_1)}\oplus v_1^{(j_1)},0_n)\in V\cap\Delta$), that is, $(v_1^{(i_1)},v_2^{(i_1)})=(v_1^{(j_1)},v_2^{(j_1)})$. Further, $|\{v_2^{(1)},v_2^{(2)},\ldots,v_2^{(2^n)}\}|=|V|=2^n$, that is, $\{v_2^{(1)},\, v_2^{(2)},\ldots,v_2^{(2^n)}\}=\mathbb{F}_2^n$ (here, if $v_2^{(i_1)}=v_2^{(i_2)}$, they are called one element). Thus, we can find two vectors $a,b\in V$ such that

   $$D_{a^{(2)}}D_{b^{(2)}}1_{E_2}(y)\neq 0$$

   since $\dim(E_2)\geq 2$.

   Now, there are four cases to be considered.

   i. If $a^{(1)}=b^{(1)}=0_n$, from (6.8), we have

   $$\begin{aligned}
   & D_{(a^{(1)},a^{(2)})}D_{(b^{(1)},b^{(2)})}f(x) \\
   = \;& x\cdot(D_{a^{(2)}}D_{b^{(2)}}\pi(y))\oplus 1_{E_1}(x)D_{a^{(2)}}D_{b^{(2)}}1_{E_2}(y)\neq 0 \quad (6.9)
   \end{aligned}$$

   since $\dim(E_1)+\dim(E_2)=n$ and $\dim(E_2)\geq 2$, that is, $\deg(1_{E_1}(x))\geq 2$.

ii. If $a^{(1)} = 0_n, b^{(1)} \neq 0_n$, from (6.8), we have

$$\begin{aligned} & D_{(a^{(1)},a^{(2)})}D_{(b^{(1)},b^{(2)})}f(x) \\ = \;& x \cdot (D_{a^{(2)}}D_{b^{(2)}}\pi(y)) \oplus b^{(1)} \cdot D_{a^{(2)}}\pi(y \oplus b^{(2)}) \\ & \oplus 1_{E_1}(x)D_{a^{(2)}}D_{b^{(2)}}1_{E_2}(y) \\ \oplus \;& 1_{E_2}(y \oplus b^{(2)})D_{b^{(1)}}1_{E_1}(x) \oplus 1_{E_2}(y \oplus a^{(2)} \oplus b^{(2)})D_{b^{(1)}}1_{E_1}(x) \\ = \;& x \cdot (D_{a^{(2)}}D_{b^{(2)}}\pi(y)) \oplus b^{(1)} \cdot D_{a^{(2)}}\pi(y \oplus b^{(2)}) \\ \oplus \;& 1_{E_1}(x)D_{a^{(2)}}D_{b^{(2)}}1_{E_2}(y) \oplus D_{b^{(1)}}1_{E_1}(x)D_{a^{(2)}}1_{E_2}(y \oplus b^{(2)}). \end{aligned}$$

We know $\dim(E_1)+\dim(E_2) = n$ and $\dim(E_2) \geq 2$, thus $\deg(1_{E_1}(x)) \geq 2$. Further, $\deg(1_{E_1}(x)) > \deg(D_{b^{(1)}}1_{E_1}(x))$. Thus, we have

$$D_{(a^{(1)},a^{(2)})}D_{(b^{(1)},b^{(2)})}f(x) \neq 0.$$

iii. If $a^{(1)} \neq 0_n, b^{(1)} = 0_n$, from (6.8), we have

$$\begin{aligned} & D_{(a^{(1)},a^{(2)})}D_{(b^{(1)},b^{(2)})}f(x) \\ = \;& x \cdot (D_{a^{(2)}}D_{b^{(2)}}\pi(y)) \oplus a^{(1)} \cdot D_{b^{(2)}}\pi(y \oplus a^{(2)}) \qquad (6.10) \\ \oplus \;& 1_{E_1}(x)D_{a^{(2)}}D_{b^{(2)}}1_{E_2}(y) \oplus D_{a^{(1)}}1_{E_1}(x)D_{b^{(2)}}1_{E_2}(y \oplus a^{(2)}). \end{aligned}$$

We know $\dim(E_1)+\dim(E_2) = n$ and $\dim(E_2) \geq 2$, thus $\deg(1_{E_1}(x)) \geq 2$. Further, $\deg(1_{E_1}(x)) > \deg(D_{a^{(1)}}1_{E_1}(x))$. Thus, we have

$$D_{(a^{(1)},a^{(2)})}D_{(b^{(1)},b^{(2)})}f(x) \neq 0.$$

iv. If $a^{(1)} \neq 0_n, b^{(1)} \neq 0_n$, from (6.8), we have

$$D_{(a^{(1)},a^{(2)})}D_{(b^{(1)},b^{(2)})}f(x) \neq 0.$$

Since $\dim(E_1) + \dim(E_2) = n$ and $\dim(E_2) \geq 2$, then $\deg(1_{E_1}(x)) \geq 2$. Furthermore, $\deg(1_{E_1}(x)) > \deg(D_{b^{(1)}}1_{E_1}(x))$, $\deg(1_{E_1}(x)) > \deg(D_{a^{(1)}}1_{E_1}(x))$ and $\deg(1_{E_1}(x)) > \deg(D_{a^{(1)}\oplus b^{(1)}}1_{E_1}(x))$.

Hence, we have

$$D_{(a^{(1)},a^{(2)})}D_{(b^{(1)},b^{(2)})}f(x) \neq 0$$

for $|V \cap \Delta| = 1$.

(b) For $|V \cap \Delta| = 2$, without loss of generality, let $(a^{(1)}, 0_n) \in V \cap \Delta$, $a^{(1)} \neq 0_n$. We know $\{v_2^{(1)}, v_2^{(2)}, \ldots, v_2^{(2^n)}\}$ is a subspace of $\mathbb{F}_2^n$ which is denoted by $\mathcal{V}'$. We first prove $\dim(\mathcal{V}') = n - 1$ by showing that $|\{v_2^{(1)}, v_2^{(2)}, \ldots, v_2^{(2^n)}\}| = 2^{n-1}$, where we only count distinct vectors (e.g. if $v_2^{(i_1)} = v_2^{(i_2)}$ only one vector is counted). If $|\{v_2^{(1)}, v_2^{(2)}, \ldots, v_2^{(2^n)}\}| = 2^n$, then it is clear that V is not a subspace. If $|\{v_2^{(1)}, v_2^{(2)}, \ldots, v_2^{(2^n)}\}| < 2^{n-1}$, there must exist three vectors $v_2^{(i_1)} = v_2^{(i_2)} = v_2^{(i_3)}$, where $i_1 \neq i_2 \neq i_3$. Thus, we will have $(v_1^{(i_1)}, v_2^{(i_1)}) \oplus (v_1^{(i_2)}, v_2^{(i_2)}) \in V \cap \Delta$, $(v_1^{(i_1)}, v_2^{(i_1)}) \oplus (v_1^{(i_3)}, v_2^{(i_3)}) \in V \cap \Delta$

and $(v_1^{(i_3)}, v_2^{(i_3)}) \oplus (v_1^{(i_2)}, v_2^{(i_2)}) \in V \cap \Delta$, which contradicts the fact that $|V \cap \Delta| = 2$.

We now show that $|E_2 \cap \mathcal{V}'| \geq 1$ by using a well-known fact that

$$\dim(E_2 \cap \mathcal{V}') = \dim(E_2) + \dim(\mathcal{V}') - \dim(E_2 \boxplus \mathcal{V}'),$$

where $E_2 \boxplus \mathcal{V}' = \{\alpha \oplus \beta | \alpha \in E_2, \beta \in \mathcal{V}'\}$. Since by assumption $\dim(E_2) \geq 2$ and we have shown that $\dim(\mathcal{V}') = n-1$, then $\dim(E_2 \cap \mathcal{V}') \geq 1$.

We now choose one vector $b^{(2)}$ from $(\mathcal{V}' \cap E_2) \backslash \{0_n\}$, then $b^{(2)} \neq 0_n$ and $1_{E_2}(y) = 1_{E_2}(y \oplus b^{(2)})$ (since $b^{(2)} \in E_2$). Set $b = (b^{(1)}, b^{(2)}) \in V$. From (6.8), we have

$$\begin{aligned} & D_{(a^{(1)},a^{(2)})} D_{(b^{(1)},b^{(2)})} f(x) \\ = \; & a^{(1)} \cdot D_{b^{(2)}} \pi(y) \oplus 1_{E_2}(y) D_{a^{(1)}} 1_{E_1}(x) \qquad (6.11) \\ \oplus \; & 1_{E_2}(y \oplus b^{(2)}) D_{b^{(1)}} 1_{E_1}(x) \oplus 1_{E_2}(y \oplus b^{(2)}) D_{a^{(1)} \oplus b^{(1)}} 1_{E_1}(x) \\ = \; & a^{(1)} \cdot D_{b^{(2)}} \pi(y) \oplus 1_{E_2}(y) D_{a^{(1)}} D_{b^{(1)}} 1_{E_1}(x). \end{aligned}$$

Now, there are three cases to be considered. If $D_{a^{(1)}} D_{b^{(1)}} 1_{E_1}(x) \neq$ *const.* or $D_{a^{(1)}} D_{b^{(1)}} 1_{E_1}(x) = 0$, then it is clear that

$$D_{(a^{(1)},a^{(2)})} D_{(b^{(1)},b^{(2)})} f(x) \neq 0$$

since π has no nonzero linear structure and $b^{(2)} \neq 0_n$.

If $D_{a^{(1)}} D_{b^{(1)}} 1_{E_1}(x) = 1$, then it is clear that

$$D_{(a^{(1)},a^{(2)})} D_{(b^{(1)},b^{(2)})} f(x) = a^{(1)} \cdot D_{b^{(2)}} \pi(y) \oplus 1_{E_2}(y) \neq 0$$

since $\deg(\pi) \leq n - \dim(E_2)$, that is, $\deg(a^{(1)} \cdot D_{b^{(2)}} \pi(y)) < n - \dim(E_2) = \deg(1_{E_2}(y))$.

(c) For $|V \cap \Delta| > 2$ (i.e., $|V \cap \Delta| \geq 4$), without loss of generality, let $a = (a^{(1)}, 0_n) (\neq 0_{2n}) \in V \cap \Delta$. Here, there are two cases to be considered.

i. If there exists one vector $v = (0_n, v_2) \in V \setminus \{0_{2n}\}$, then we set $b = v$. Further, using that $b^{(1)} = 0_n$, we have

$$D_{(a^{(1)},a^{(2)})} D_{(b^{(1)},b^{(2)})} f(x) = a^{(1)} \cdot D_{b^{(2)}} \pi(y) \oplus D_{b^{(2)}} 1_{E_2}(y) D_{a^{(1)}} 1_{E_1}(x).$$

If $D_{a^{(1)}} 1_{E_1}(x) \neq$ *constant* or $D_{a^{(1)}} 1_{E_1}(x) = 0$, then again

$$D_{(a^{(1)},a^{(2)})} D_{(b^{(1)},b^{(2)})} f(x) \neq 0,$$

since π has no nonzero linear structure.

We now show that $D_{a^{(1)}} 1_{E_1}(x) = 1$ is impossible. We have that $D_{a^{(1)}} 1_{E_1}(x) = 0$ if $a^{(1)} \in E_1$, or alternatively if $a^{(1)} \notin E_1$

$$\deg(D_{a^{(1)}} 1_{E_1}(x)) = n - \dim(E_1) - 1,$$

since $E_1 \cup (a^{(1)} \oplus E_1)$ is a subspace of dimension $\dim(E_1) + 1$. Since $n - \dim(E_1) - 1 > 0$ and by assumption $\dim(E_1) < n - 1$, we have $D_{a^{(1)}} 1_{E_1}(x) \neq 1$.

ii. Let $v = (v_1, v_2) \in V \setminus \{0_{2n}\}$. If we always have $v = (v_1, v_2)$ such that $v_1 \neq 0_n$ for every $v_2 \neq 0_n$, then we set $b = v \in V \setminus \{0_{2n}\}$ such that $v_2 \neq 0_n$. Further, we have

$$\begin{aligned}
&D_{(a^{(1)},a^{(2)})}D_{(b^{(1)},b^{(2)})}f(x) = a^{(1)} \cdot D_{b^{(2)}}\pi(y) \oplus 1_{E_2}(y)D_{a^{(1)}}1_{E_1}(x)\\
&\oplus 1_{E_2}(y \oplus b^{(2)})D_{b^{(1)}}1_{E_1}(x) \oplus 1_{E_2}(y \oplus b^{(2)})D_{a^{(1)}\oplus b^{(1)}}1_{E_1}(x)\\
&= a^{(1)} \cdot D_{b^{(2)}}\pi(y) \oplus 1_{E_2}(y)D_{a^{(1)}}1_{E_1}(x) \qquad (6.12)\\
&\oplus 1_{E_2}(y \oplus b^{(2)})D_{a^{(1)}}1_{E_1}(x \oplus b^{(1)}).
\end{aligned}$$

There are two cases to be considered.
If $b^{(2)} \in E_2$, then we have

$$\begin{aligned}
D_{(a^{(1)},a^{(2)})}D_{(b^{(1)},b^{(2)})}f(x) \;&=\; a^{(1)} \cdot D_{b^{(2)}}\pi(y) \oplus 1_{E_2}(y)(D_{a^{(1)}}1_{E_1}(x)\\
&\oplus D_{a^{(1)}}1_{E_1}(x \oplus b^{(1)})) \neq 0,
\end{aligned}$$

since $\deg(1_{E_2}(y)) > \deg(a^{(1)} \cdot D_{b^{(2)}}\pi(y))$.
If $b^{(2)} \notin E_2$, then we have three cases to be considered.

A. For $a^{(1)} \in E_1$ we have

$$D_{(a^{(1)},a^{(2)})}D_{(b^{(1)},b^{(2)})}f(x) = a^{(1)} \cdot D_{b^{(2)}}\pi(y) \neq 0.$$

B. For $a^{(1)} \notin E_1, b^{(1)} \in E_1$ we have

$$\begin{aligned}
D_{(a^{(1)},a^{(2)})}D_{(b^{(1)},b^{(2)})}f(x) \;&=\; a^{(1)} \cdot D_{b^{(2)}}\pi(y)\\
&\oplus D_{b^{(2)}}1_{E_2}(y)D_{a^{(1)}}1_{E_1}(x) \neq 0,
\end{aligned}$$

since $D_{a^{(1)}}1_{E_1}(x) \neq$ *constant*.

C. For $a^{(1)} \notin E_1, b^{(1)} \notin E_1$ we have

$$\begin{aligned}
D_{(a^{(1)},a^{(2)})}D_{(b^{(1)},b^{(2)})}f(x) \;&=\; a^{(1)} \cdot D_{b^{(2)}}\pi(y)\\
&\oplus D_{b^{(2)}}1_{E_2}(y)D_{a^{(1)}}1_{E_1}(x)\\
&\oplus 1_{E_2}(y \oplus b^{(2)})D_{a^{(1)}}D_{b^{(1)}}1_{E_1}(x) \neq 0,
\end{aligned}$$

since $D_{a^{(1)}}1_{E_1}(x) \neq$ *constant* and furthermore $\deg(D_{a^{(1)}}1_{E_1}(x)) > \deg(D_{a^{(1)}}D_{b^{(1)}}1_{E_1}(x))$.

Combining items 1 and 2, we deduce that f does not belong to $M^{\#}$.

□

Index

affine equivalence, 10
almost bent functions, 16
almost perfect nonlinear function, 16

balancedness, 11
bent classes
  $\mathcal{C}$ class, 15, 26, 29, 34, 37
  complete class, 13
  $\mathcal{D}$ class, 15, 24, 29, 34, 39
  Maiorana-McFarland class, 13, 22, 34
  $\mathcal{N}$ class, 14
  $\mathcal{PS}$ class, 14, 42
bent function, 12
  vectorial bent function, 15
Boolean functions, 10
  vectorial, 15

concatenation, 10
coordinate functions, 15
correlation immunity, 11

degree
  algebraic, 10
  polynomial, 11
difference set, 13
  Hadamard, 13
dual function, 12, 70

Galois field, 9
graph, 13
  strongly regular, 13

Hadamard
  difference set, 13
  distance, 9
  matrix, 13
  weight, 9
Hamming
  distance, 10

linear functions, 17
linear structure, 17, 25, 35

nonlinearity, 12
normality, 20, 26
  weak normality, 20

partially-bent functions, 16
permutation, 16
  complete permutation, 55, 84
plateaued function, 16, 79
primary construction, 13
primitive element, 9
propagation criterion, 11
property (C), 15, 34, 37

representation
  algebraic normal form, 10
  trace representation, 11
  univariate representation, 10
resiliency, 11
Rothaus construction, 19

secondary constructions, 13
self-dual functions, 12
semi-bent functions, 16
strict avalanche criterion, 11
support, 10

trace function, 9
  absolute trace, 10
translator
  Frobenius translator, 64, 65
  linear translator, 17, 45

Walsh-Hadamard
  spectrum, 12
  transform, 12, 15

Chapter 7

Povzetek v slovenskem jeziku

Začetki kriptografije segajo daleč v našo preteklost. Čim je kralj želel poslati tajna navodila svojim generalom, čim je obrtnik želel varno zapisati skrivno recepturo ali postopek, se je pojavila potreba po *kriptografiji*; disciplini, ki po današnji definiciji omogoča dvema stranema, da varno komunicirata preko nezavarovanega kanala. Skoraj vsi so že slišali za Cezarjevo preprosto zamenjalno šifro, vendar začetki kriptografije segajo še več kot 1000 let v preteklost [44]. Z napredkom šifriranja se je razvijala tudi veda o dešifriranju in iskanju skritih sporočil, *kriptoanaliza.* Kriptografija in kriptoanaliza skupaj tvorita področje *kriptologije*, ki ni bila še nikdar v zgodovini tako velikega pomena za našo širšo družbo, kot danes.

Nekoč se je kriptografija večinoma ubadala s črkami abeced, frazami in znaki, danes pa dela z enicami in ničlami; simboli, ki so primerni za računalnike in elektronsko komunikacijo. Takšna moderna kriptografija in informacijska teorija nasplošno sta se v bistvu pričeli leta 1948 s prebojnim člankom Clauda Shannona "A Mathematical Theory of Communication" [79] (Matematična teorija komunikacij). Da bi zadovoljila današnjim potrebam, mora kriptografija zagotoviti štiri osnovne storitve: zaupnost, integriteto podatkov, avtentikacijo in ne-odklonskost.

Zaupnost (ali *zasebnost*) je storitev, ki ščiti informacije pred tem, da bi do njih dostopale nepooblaščene osebe. *Integriteta podatkov* pomeni, da storitev preprečuje, da bi podatke spreminjala nepooblaščena oseba, in da so spremembe, če se zgodijo, zaznane. Najpogostejše spremembe podatkov so *vstavljanje* podatkov, *izbris* in *zamenjava. Avtentikacija* se nanaša na to, da lahko dve strani, ki želita komunicirati, uspešno identificirata ena drugo. Nazadnje, *ne-odklonskost*, zagotavlja, da nobena stran ne more zanikati, da je naredila določena dejanja, kot na primer, da je poslala transakcijo ali podpisala dokument.

Vse te lastnosti je potrebno upoštevati pri praktični implementaciji kriptosistema. Slika 7.1 prikazuje shemo za zagotavljanje zaupnosti. Dve strani oz. osebi, Alica in Bob, bi radi komunicirali preko nezavarovanega kanala. Alica, pošiljatelj, želi Bobu, prejemniku, poslati sporočilo p (plaintext). Z uporabo tajnega ključa k in šifrirnega algoritma E ga zašifrira v kodirano sporočilo $c = E(p, k)$ (ciphertext). Kodirano sporočilo c pošlje Bobu preko nezavarovanega kanala, kateremu lahko prisluškuje nasprotnik, ponavadi imenovan Eva (kar stoji za "Enemy" ali "Eavesdropper") ali Mallory (kar stoji za man-in-the-middle napad), ki nad kodi-

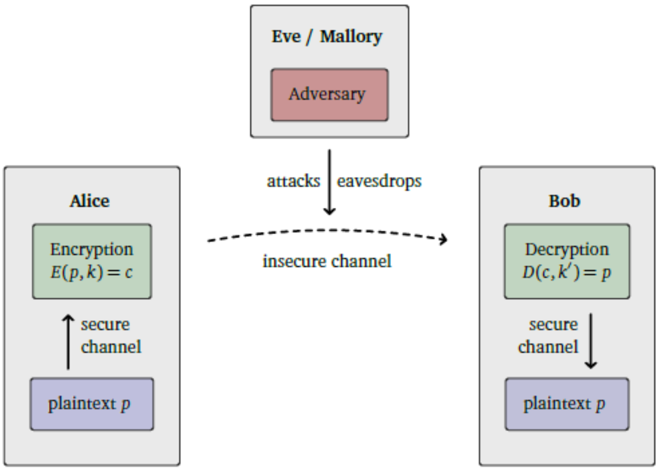

Figure 7.1: Standardna šifrirna shema

ranim sporočilom izvaja kriptoanalizo. Ko Bob prejme kodirano sporočilo c, ga dešifrira z uporabo tajnega ključa k' in dešifrirnega algoritma D. S tem dobi sporočilo $p = D(c, k')$.

Če sta tajna ključa k in k' enaka, shema uporablja *simetrično kriptografijo* oz. *kriptografijo tajnega ključa*. Če se ključa razlikujeta, je to shema *asimetrične kriptografije* ali *kriptografije javnega ključa*, ki zahteva, da imata oba Alica in Bob dva ključa. Natančneje, oba morata imeti javni ključ, ki je shranjen v javni bazi podatkov in dosegljiv vsem, in zasebni ključ, ki ga morata varovati. Alica tako uporabi Bobov javni ključ, da zašifrira sporočilo, Bob pa ga neto dešifrira s svojim odgovarjajočim zasebnim ključem.

V splošnem je simetrična kriptografija računsko približno 1000-krat hitrejša od kriptografije javnega ključa in zahteva ključe krajše dolžine za zagotavljanje enake ravni varnosti. Po drugi strani pa mora vsak par oseb, ki želi komunicirati z uporabo simetrične kriptografije, hraniti skupni tajni ključ. Če želi n oseb zagotoviti medsebojno paroma varno komunikacijo, mora biti skupno izmenjanih $\frac{n(n-1)}{2}$ tajnih ključev in vsak uporabnik mora hraniti in varovati $n-1$ različnih tajnih ključev, kar je v mnogih primerih zelo nepraktično. Če primerjamo z asimetrično kriptografijo, je za njeno uporabo potrebno hraniti samo en tajni ključ.

V nadaljevanju se posvetimo simetrični kriptografiji, saj glavni del teze obravnava lastnosti kriptografskih primitivov, ki so vezani nanjo. Simetrično šifriranje obsega dva glavni družini šifrirnih algoritmov; bločne šifre (Slika 7.3) in pretočne šifre (Slika 7.2). Pretočne šifre generirajo psevdo-naključno zaporedje bitov, imenovano *tok ključa* (keystream), ki je prišteto osnovnemu sporočilu modulo 2. Tako dobimo kodirano sporočilo. Med mnogimi načini načrtovanja ena od poddružin pretočnih šifer (tako imenovani filtrirni generator) uporablja register linearnih povratnih premikov (linear feedback shift register - LFSR) in filtrirno Boolovo funkcijo, ki procesira vsebino spominski celic registra in s tem generira bite toka ključa [46].

Dva dobro poznana primera uporabe LFSR pretočnih šifer sta družini šifer $A5$,

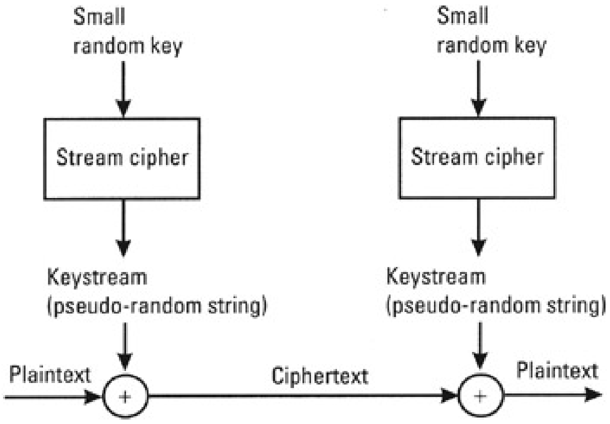

Figure 7.2: Primer pretočne šifre

ki se uporabljajo v GSM telekomunikacijskem standardu [4], in šifrirni algoritem E_0, ki ga uporabljajo nekatere Bluetooth aplikacije [59]. Nekateri drugi dobro poznani šifrirni algoritmi, ki pripadajo družini pretočnih šifer, so na primer SNOW [38], RC4 [48], Trivium [8] in Grain [41].

Bločne šifre predstavljajo drugo veliko družino simetričnih šifrirnih algoritmov (Slika 7.3), ki v splošnem implementirajo psevdo-naključne permutacije. Osnovno sporočilo je razdeljeno na bloke podatkov enake velikosti, na primer n, ki jih bločna šifra nato zaporedoma procesira v izhodni blok. Ta postopek mora biti obrnljiv in tako bločna šifra za vsak tajni ključ (ki je vgrajen v šifrirni algoritem) implementira specifično permutacijo n binarnih bitov. Moderno načrtovanje bločnih šifer uporablja iterativno aplikacijo številnih identičnih rund, katerih rezultat je blok kodiranega sporočila. Pri tem lahko njihova notranja struktura temelji ali na *Feistel omrežju*, ali na *substitucijsko-permutacijskem omrežju.* Ne glede na interno strukturo pa iterativne runde običajno implementirajo Shannonova koncepta *zmede* z uporabo tako imenovanih *substitucijskih škatel* (*S-škatel*) in koncept *difuzije* z uporabo *permutacijskih škratel* (*P-škatel*) [79]. Na S-škatle lahko gledamo kot na zbirko Boolovih funkcij (glej Chapter 2), medtem ko P-škatle preprosto linearno permutirajo bloke in dosežejo najboljšo možno difuzijo bitov, tako da pri naslednji rundi vplivajo na

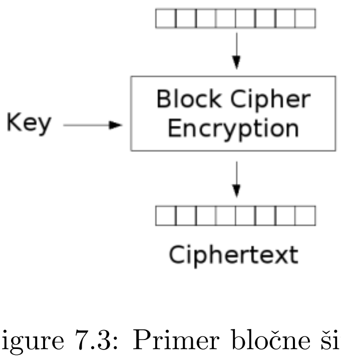

Figure 7.3: Primer bločne šifre

različne S-škatle. V tem kontekstu je cilj zmede, da doseže, da je globalna odvisnost bitov šifriranega sporočila glede na bite ključa in osnovnega sporočila kar se da kompleksna. Ena bistvenih posledic dobro zastavljene difuzije je, da sprememba enega bita osnovnega sporočila vpliva na približno eno polovico bitov šifriranega sporočila, ki spremenijo vrednost glede na prvotno šifrirano sporočilo.

Ena od prvih bločnih šifer, ki jih je leta 1970 razvil Horst Feistel s svojo IBM ekipo, je bila imenovana Lucifer. Njena izboljšana verzija, DES (Data Encryption Standard), je ena najbolj znanih blošnih šifer in ZDA jo je leta 1976 sprejela za Federalni standard za procesiranje informacij (Federal Information Processing Standard - FIPS). V sledečih letih je bila podvržena natančnemu proučevanju s strani akademske javnosti. Čeprav sta Diffie in Hellman opozorila, da je dolžina tajnega ključa prekratka, da bi zagotovila dolgoletno varnost [33], niso bile ugotovljene nobene neposredne šibke točke v načrtu šifre. Leta 1992 je Matsui [62] predstavil koncept linearne kriptoanalize in jo uporabil na šifri DES. Nekaj let za tem je project DESCHALL javno zlomil tajno sporočilo, šifrirano z DES šifro. V poznih devetdesetih je postalo jasno, da DES zaradi prekratke dolžine ključa (56 bitov) ni odporen na napade s surovo močjo (še dandanes je najučinkovitješi napad na DES izčrpno iskanje ključa). Zaradi tega je bil leta 2001 sprejet nov šifrirni standard, imenovan AES (Advanced Encryption Standard) in v odprtem tekmovanju [71] je bil izbran šifrirni algoritem Rijndael [31].

Nekatere druge dobro znane bločne šifre so IDEA [50], Blowfish [78] in RC5 [76].

V splošnem obstajajo štirje glavni scenariji za uporabo kriptoanalize glede na to, katere informacije so na razpolago napadalcu.

- V najšibkejšem, *scenariju kodiranega sporočila*, ima napadalec dostop samo do nekaj kodiranih sporočil, ki jih je generirala ciljna bločna šifra z uporabo neznanega tajnega simetričnega ključa. Napadalčev cilj je najti nekodirano sporočilo (ali njegove dele), ali pa najti tajni ključ (ali njegove dele). Ta scenarij je najbolj praktičen, vendar je izvajanje kriptoanalize najtežje.

- V primeru *scenarija s poznanim nekodiranim sporočilom* ima napadalec na razpolago pare kodiranih in dekodiranih sporočil in njegov cilj je najti tajni ključ (ali njegove dele).

- *Scenarij izbranih nekodiranih sporočil* je podoben scenariju s poznanim nekodiranim sporočilom, vendar ima zdaj napadalec dostop do šifrirne naprave in lahko šifrira poljubno sporočilo. Cilj je ponovno najti tajni ključ (ali njegove dele).

- *Scenarij izbranih kodiranih sporočil* je podobne prejšnjemu, vendar tu napadalec dešifrira poljubna kodirana sporočila in tako dobi odgovarjajoča nekodirana sporočila.

V nadaljevanju uvoda se bomo večinoma posvetili varnosti bločnih šifer. Bolj natančno, ogledali si bomo načrtovanje in varnost S-škatel. Določeni tipi napadov, kot sta lienarna in diferenčna kriptoanaliza [5], postanejo lažji, če imajo S-škatle šibke ne-linearne lastnosti (glej Poglavje 2.2). Z uporabo dejstva, da se da z določeno verjetnostjo najti približek S-škatel šifreDES, sestavljen iz linearnih funkcij, je Matsui [64] leta 1993 uspel najti približek 14 rund šifre DES, ki drži z verjetnostjo 0.50000057. Posledično se da celih 16 rund šifre DES zlomiti s scenarijem s poznanim nekodiranim sporočilom in 2^{47} pari kodiranih in nekodiranih sporočil.

Da bi zagotovili dovolj visoko stopnjo varnosti pred takšnim tipom napadov, je bil uveden koncept *nelinearnosti*, glej Poglavje 2 za več podrobnosti. Boolove funkcije, ki ležijo na največji možni razdalji od množice vseh afinih funkcij, torej funkcije z največjo možno nelinearnostjo, se imenujejo *ukrivljene funkcije* (*bent functions*). Ta razred Boolovih funkcij so prvi odkrili raziskovalci Združenih držav Amerike in Sovjetske zveze v sklopu ločenih vzporednih tajnih raziskovalnih projektov. Danes se obravnava Oscarja Rothausa, Slika 7.4, kot prvega raziskovalca, ki je svetu javno predstavil ukrivljene funkcije. Od leta 1960 do 1966, ko se je pridružil Univerzi Cornell, je delal na Inštitutu obrambnega oddelka za obrambne analize (Defence Department's Institute for Defence Analyses), kjer je prvič opisal ukrivljene funkcije v klasificiranem članku leta 1966, ki je šele čez deset let postal dostopen širši javnosti [77].

Figure 7.4: Oscar Rothaus, 1927 - 2003

Figure 7.5: Oleg P. Stepchenkov [82]

V šestdesetih letih pa so tudi raziskovalci Sovjetske zvete delali na ukrivljenih funkcijah. V [82] Tokareca piše, da so Y. A. Vasiliev, B. M. Kloss, V. A. Eliseev in O. P. Stepchenkov (Slika 7.5) v tem času proučevali tako imenovane "minimalne funkcije", katerih definicija se ujema z definicijo ukrivljenih funkcij. Kljub temu pa je večina njihovih rezultatov še vedno klasificiranih in ni dostopna javnosti.

V naslednjih desetletjih raziskovanja ukrivljenih funkcij so se pokazala mnoga področja njihove uporabe. V teoriji kodiranja je, na primer, pokazano, da je iskanje radiusa pokritja Reed-Muller kode ekvivalentno iskanju Boolove funkcij z najvišjo nelinearnostjo [47, 60]. Ukrivljene funkcije se uporabljajo tudi za konsturkcijo znanih Kerdockovih kod [32, 80]. Uporabljajo se tudi za načrtovanje zaporedij, ki se jih uporablja v sklopu določenih telekomunikacijskih tehnik, ki uporabljajo CDMA metodo (Code Division Multiple Access). Pri CDMA, ko več uporabnikov hkrati dostopa do kanala, je vsakemu uporabniku v tako imenovani celici dodeljeno zporedje, ki je ortogonalno na zaporedja vseh drugih uporabnikov v celici in hkrati ortogonalno na zaporedje vseh uporabnikov v sosednjih celicah. Število uporabnikov na celico je tako omejeno s kardinalnostjo množice paroma ortogonalnih zaporedij, ki jo lahko skonsturiramo. Tako ukrivljene funkcije, kot ostali tipi Boolovih funkcij z visoko nelinearnostjo, so se izkazali bistvenega pomena za konstruiranje takšnih množic. Poleg tega so ukrivljene funkcije tesno povezane s Hadamarjevimi matrikami, elementarnimi Hadamarjevimi diferenčnimi množicami in krepko regularnimi Cayleyjevimi grafi. V [3] je dokazano, da je ukrivljena funkcija ukrivljena, če in samo če je njen odgovarjajoči graf krepko regularen Cayleyjev graf s parametri (v, k, λ, μ), kjer je $\lambda = \mu$.

Na področju ukrivljenih funkcij ostajajo številna odprta vprašanja, kot je njihovo točno število za fiksno število spremenljivk, njihovo načrtovanje in klasifikacija. Kar se tiče njihovega načrtovanja in klasifikacije so poznane določene primarne konstrukcije, ki neposredno generirajo ukrivljene funkcije za poljubno sodo število spremenljivk n, glej podpoglavje 2.2.1 za natančnejše definicije. Po drugi strani obstajajo tudi številne sekundarne konstrukcije, ki iz že znanih ukrivljenih funkcij konstruirajo nove, kot je, na primer, opisano v [15, 20, 67, 95, 93]). Zainteresiran bralec si lahko pogleda tudi lep pregled ukrivljenih funkcij, ki sta ga napisala Carlet in Mesnager [18].

Glavni problem pri sekundarnih konsturkcijah je, da je ukrivljene funkcije, ki so generirane na ta način, težko klasificirati. Natančneje, lahko se zgodi, da nekatere sekundarne konstrukcije generirajo funkcije, ki pripadajo kateremu od primarnih razredov ukrivljenih funkcij. V tem primeru je pomembna samo njihova eksplicitna reprezentacija. Kljub temu je dokazovati, da ležijo izven popolnih primarnih razredov (popoln razred vsebuje osnovni razred in vse ukrivljene funkcije, ki jih lahko dobimo z določenimi afinimi transformacijami), običajno težka naloga, še posebej za razred $\mathcal{PS}$, za katerega ne obstajajo učinkoviti indikatorji. V [61] je, na primer, dokazano, da v mnogih primerih funkcije iz $\mathcal{C}$ razreda, ki je razred, izpeljan iz Marioana-McFarland primarnega razreda ukrivljenih funkcij (iznačujemo ga z $\mathcal{M}$), še vedno ležijo v $\mathcal{M}$ razredu (glej Poglavje 2.2.1). Tako je eden glavnih izzivov na področju ukrivljenih funkcij problem odločanja, če dana ukrivljena funkcija leži v katerem od popolnih primarnih razredov, ali izven njih. Za popoln $\mathcal{M}$ razred obstaja učinkovit indikator vsebovanosti, glej [34], vendar tudi ta postane računsko neučinkovit za $n > 6$. Za razred $\mathcal{PS}$ ne poznamo še nobenega podobnega indikatorja in problem vsebovanosti v tem razredu je še težji.

Druga tema, ki bo prav tako obravnavana v tezi in ki na prvi pogled nima bistvene povezave z ukrivljenimi funkcijami, je konstrukcija novih razredov permutacij nad končnimi polji. Končno polje reda p^n označimo z $\mathbb{F}_{p^n}$, kjer je p poljubno praštevilo in n pozitivno celo število. Polinom $F \in \mathbb{F}_{p^n}[x]$ je permutacija, če je njegova odgovarjajoča preslikava $x \mapsto F(x)$ nad $\mathbb{F}_{p^n}$ bijektivna. Permutacijski polinomi so bili deležni večje pozornosti že v 19. stoletju in zaradi njihovi uporabnosti v kombinatoriki, teoriji kodiranja, simetrični kriptografiji, inženiringu in na številnih drugih področij teoretično zanimanje za te objekte še vedno ne pojenja. V splošnem določanje permutacijskega polinoma nad končnim poljem $|\mathbb{F}_{p^n}$ ni težka naloga. Obstaja natanko $p^n!$ permutacij, ki odgovarjajo kardinalnosti simetrične grupe s p^n elementi. Ko določimo bijekcijo med vhodnim prostorom in permutiranimi vhodnimi elementi, lahko takšno permutacijo učinkovito opišemo s polinomom z eno spremenljivko, ki ga dobimo z uporabo Langrangove interpolacije. Vendar uporaba v določenih aplikacijah zahteva, da imajo ti permutacijski polinomi tudi dodatne lastnosti, kot na primer kompaktno reprezentacijo, dobre diferenčne lastnosti, nelinearnost in podobno. Zaradi velike kardinalnosti permutacijskih polinomov je iskanje optimalnih razredov na takšen način seveda nemogoče, tudi za majhna končna polja.

V zadnjih nekaj letih je prišlo do velikega napredka v konsturkcijskih metodah in karakterizaciji številnih razredov permutacij, glej pregled nedavnih del [43] in tam navedene reference. Uporaba permutacij v aplikacijah, kot je kodiranje, je dobro znana. Bijektivnost je tudi ena od pomembnih kriptografskih zahtev pri načrtovanju bločnih šifer, ki uporabljajo SP strukturo. Zaradi učinkovite implementacije nas še posebej zanima konstrukcija polinomov z majhnim številom členov. Večina poznanih eksplicitnih razredov permutacijskih polinomov je oblike $X^r H(X^{\frac{p^n-1}{d}}), d < p^n - 1$ in so dobljeni z uporabo multiplikativne strukture končnih polj. V nedavnih člankih (glej [49] in reference) so bile predstavljene tudi tehnike konstrukcij permutacijskih polinomov, ki izkoriščajo aditivno strukturo končnih polj. V sklopu teze nadaljujemo z razvojem tega pristopa in najdemo številne nove razrede permutacijskih polinomov. Hkrati je posplošen koncept *translatorjev*, ki se je izkazal za uporabnega pri načrtovanju permutacijskih polinomov, kar nam omogoči konstrukcijo še večjih razredov permutacijskih polinomov. Poleg tega se izkaže, da so permutacije, skonstruirane s translatorji, uporabne tudi pri načrtovanju sekundarnih razredov ukrivljenih funkcij [69]. V tem kontekstu lahko z uvedbo koncepta Frobeniusovega translatorja posplošimo večino sekundarnih konstrukcij, ki se zanašajo na obstoj standardnega linearnega translatorja. Tako poleg definiranja novih neskončnih razredov permutacij dosežemo tudi posplošitev določenih sekundarnih konstrukcij ukrivljenih funkcij.

Preostanek teze je sestavljen na sledeči način. V Poglavju 2 so predstavljene osnovne notacije in definicije, ki se bodo pojavljale skozi vso tezo. Natančneje, to poglavje obravnava koncepte, vezane na Boolove funkcije, definira ukrivljene funkcije in primarne razrede teh funkcij ter predstavi permutacije in translatorje.

Poglavje 3 se posveti načrtovanju ukrivljenih funkcij, ki potencialno ležijo izven popolnega Maiorana-McFarland razreda. V prvem podpoglavju je opisana Rothaus konstrukcija in analizirana je ena od njenih posebnih oblik. V drugem delu so podani zadostni pogoji, da ukrivljena funkcija, ki leži znotraj $\mathcal{C}$ oziroma $\mathcal{D}$ razreda hkrati leži izven popolnega Maiorana-McFarland razreda. Prikazani so določeni primeri takšnih ukrivljenih funkcij, ki dokazljivo ležijo izven popolnega Maiorana-McFarland razreda. Poleg tega imajo v nekaterih primerih funkcije, ki jih generiramo, tudi lastnosti ne-normalnosti, kar je zelo uporabno za dokazovanje ne-vsebovanosti v določenih poznanih primarnih razredih.

Poglavje 4 naslovi permutacije nad končnimi polji, ki so konstruirane z uporabo translatorjev. V prvem podpoglavju obravnavamo linearne translatorje in analiziramo tipe funkcij, ki jih premorejo. S pomočjo teh ugotovitev predstavimo številne nove razrede permutacij. V drugem podpoglavju posplošimo koncept linearnega translatorja in uvedemo koncept Frobeniusovega translatorja, kar nam omogoča razširiti načrtovalske metode permutacijskih polinomov. Kot že omenjeno, z uporabo polinomov, pridobljenih s Frobeniusovimi translatorji, posplošimo tudi nekatere sekundarne konstrukcije ukrivljenih funkcij.

V Poglavju 5 prikažemo konstrukcije neskončnih razredov vektorskih nivojskih funkcij, permutacij in popolnih permutacij. Za razliko od metod, uporabljenih v Poglavju 4, so ti objekti načrtovani glede na multivariabilno reprezentacijo funkcij nad končnimi polji. Grobo povedano gledamo na končno polje kot na vektorski prostor in na obravnavane preslikave kot na zbirko Boolovih funkcij.

Rezultati doktorske disertacije so bili objavljeni v sledečih člankih:

- F. Zhang, E. Pasalic, Y. Wei, N. Cepak. Constructing bent functions outside the MaioranaMcFarland class using a general form of Rothaus, *IEEE Transactions on Information Theory*, 63.8 (2017), pp. 5336–5349.

- F. Zhang, E. Pasalic, N. Cepak, Y. Wei, Bent Functions in $\mathcal{C}$ and $\mathcal{D}$ outside the completed Maiorana-McFarland class." *International Conference on Codes, Cryptology, and Information Security*, Springer, Cham, 2017.

- N. Cepak, P. Charpin, E. Pasalic. Permutations via linear translators. *Finite Fields and Their Applications*, 45 (2017), pp. 19–42. Available at: https://arxiv.org/pdf/1609.09291.pdf

- N. Cepak, E. Pasalic, A. Muratović-Ribić, Frobenius linear translators giving rise to new infinite classes of permutations and bent functions, sprejeto na tretjo mednarodno delavnico o Boolovih funkcijah in njihovih aplikacijah (3rd International Workshop on Boolean Functions and their Applications)

- E. Pasalic, N. Cepak, Y. Wei. Infinite classes of vectorial plateaued functions, permutations and complete permutations. *Discrete Applied Mathematics*. 215 (2016), pp. 177–184.

Kazalo

Seznam slik **vii**

Seznam prilog **ix**

1 Uvod **1**

2 Notacije, definicije in uvodni rezultati **9**

2.1 Boolove funkcije 10

2.2 Ukrivljene funkcije 12

2.2.1 Razredi ukrivljenih funkcij 13

2.2.1 Vektorske ukrivljene funkcije 15

2.3 Ostali razredi visoko nelinearnih (vektorskih) Boolovih funkcij 16

2.4 Permutacije in translatorji 16

3 Ukrivljene funkcije izven popolnega Maiorana-McFarland razreda **19**

3.1 Konstruiranje ukrivljenih funkcij izven popolnega Maiorana-McFarland razreda z uporabo splošne Rothaus oblike 19

3.1.1 Poseben primer Rothausove konstrukcije 21

2.1.2 Iterativna uporaba Rothausove konstrukcije 29

3.1.3 Štetje ukrivljenih funkcij v razredu $\mathcal{PS}_{ap}$, ki zadostijo Rothausovi zahtevi 32

3.2 Ukrivljene funkcije znotraj razredov $\mathcal{C}$ in $\mathcal{D}$, ki ležijo izven popolenga Maiorana-McFarland razreda 34

3.2.1 Zadostni pogoji, da funkcije v razredu $\mathcal{C}$ in $\mathcal{D}$ ležijo izven popolenga Maiorana-McFarland razreda 35

3.2.2 Nekaj primerov funkcij iz razreda $\mathcal{C}$, ki ležijo izven $\mathcal{M}^{\#}$ 37

3.2.3 Ukrivljene funkcije iz razreda $\mathcal{C}$, ki ležijo izven $\mathcal{M}^{\#}$ 39

3.2.4 Vsebovanost v drugih primarnih razredih 41

4 Permutacije in ukrivljene funkcije, skonstruirane s translatorji **45**

4.1 Linearni translatorji 45

4.1.1 O funkcijah z linearnimi translatorji 46

4.1.2 Kompozicijski inverzi 51

4.1.3 Povezava s popolnimi permutacijami 55

4.1.3 Poseben razred permutacij 56

4.1 Frobeniusovi translatorji 64

4.1.1 Frobeniusovi translatorji 65
4.1.2 O določenih problemih obstoja 68
4.1.3 Uporaba pri ukrivljenih funkcijah 70

5 Neskončni razredi vektorskih nivojskih funkcij, permutacij in popolnih permutacij 79

5.1 Konstrukcija razredov z uporabo $\mathcal{M}$ razreda 80
4.1.1 Nekubične permutacije 83
5.2 Popolne permutacije 84
5.3 O obstoju linearnih komponent in linearnih struktur 86
5.3.1 Diferencialne lastnosti skonstruiranih permutacij 88

6 Zaključek 89

Literatura 91

Stvarno kazalo 113

7 Povzetek v slovenskem jeziku 115

7.1 Kazalo v sloveščini 123

Declaration

I declare that this thesis does not contain any materials previously published or written by another person except where due reference is made in the text.

Nastja Cepak