UNIVERZA NA PRIMORSKEM

FAKULTETA ZA MATEMATIKO, NARAVOSLOVJE IN INFORMACIJSKE TEHNOLOGIJE

DOKTORSKA DISERTACIJA
(DOCTORAL THESIS)

DOLOČANJE UKRIVLJENIH FUNKCIJ ZUNAJ $\mathcal{M}^{\#}$ RAZREDA IN DOLOČENI REZULTATI O KORELACIJSKI IMUNOSTI FUNKCIJ

(SPECIFYING BENT FUNCTIONS OUTSIDE $\mathcal{M}^{\#}$ AND SOME RESULTS ON CORRELATION IMMUNE FUNCTIONS)

SADMIR KUDIN

KOPER, 2023

UNIVERZA NA PRIMORSKEM

FAKULTETA ZA MATEMATIKO, NARAVOSLOVJE IN INFORMACIJSKE TEHNOLOGIJE

DOKTORSKA DISERTACIJA
(DOCTORAL THESIS)

DOLOČANJE UKRIVLJENIH FUNKCIJ ZUNAJ $\mathcal{M}^{\#}$ RAZREDA IN DOLOČENI REZULTATI O KORELACIJSKI IMUNOSTI FUNKCIJ

(SPECIFYING BENT FUNCTIONS OUTSIDE $\mathcal{M}^{\#}$ AND SOME RESULTS ON CORRELATION IMMUNE FUNCTIONS)

SADMIR KUDIN

KOPER, 2023

MENTOR: PROF. DR. ENES PASALIC
SOMENTOR: DOC. DR. SAMIR HODŽIĆ

Acknowledgement

I would like to thank my supervisor Professor Enes Pasalic for his consistent guidance, patience and support during my PhD studies. I would also like to express my thanks to my co-supervisor Dr. Samir Hodžić for his support, availability and constructive suggestions. Furthermore I would like to thank the rest of the crypto group at University of Primorska for their energy, understanding and help.

I'm also grateful for having the opportunity to collaborate with: Dr. Nastja Cepak, Dr. Alexandr Polujan, Prof. Alexander Pott, Prof. Yongzhuang Wei and Prof. Fengrong Zhang in a number of occasions during my PhD studies.

Želio bih da se zahvalim mojim roditeljima i porodici na pomoći, podršci i razumijevanju. Hvala vam.

Abstract

SPECIFYING BENT FUNCTIONS OUTSIDE $\mathcal{M}^{\#}$ AND SOME RESULTS ON CORRELATION IMMUNE FUNCTIONS

Cryptographically significant properties of Boolean functions are the main subject of study in this thesis. Depending on which cryptographically significant property is the center of our attention, the thesis is split into three corresponding parts.

In the first part of the thesis we focus on providing a more accurate description (in terms of class membership) of the secondary classes of bent functions $\mathcal{D}_0$ and $\mathcal{C}$. C. Carlet in the 1990s considered bent functions in $\mathcal{D}_0$ class of the form $f(x,y) = x \cdot \pi(y) + \delta_0(x)$, where $x, y \in \mathbb{F}_2^n$, π is a permutation of $\mathbb{F}_2^n$ and $\delta_0(x)$ is the indicator (characteristic function) of the subspace $\{0_n\} \times \mathbb{F}_2^n$. He provided a sufficient condition for the functions to be outside the completed Maiorana-McFarland class of bent functions $\mathcal{M}^{\#}$, based on properties of the permutation π. Namely, if π is not affine on any linear hyperplane of $\mathbb{F}_2^n$, then f is outside $\mathcal{M}^{\#}$. We show that, when the algebraic degree of a permutation π is greater than 2, the Boolean function $f(x,y) = x \cdot \pi(y) + \delta_0(x)$, with $f : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2$, is always outside $\mathcal{M}^{\#}$ (regardless of the fact whether π is affine on some hyperplane or not). On the other hand, we will prove that the sufficient condition of C. Carlet is also necessary when $\deg(\pi) = 2$. We then explore the problem of specifying bent functions in $\mathcal{C}$, $f(x,y) = x \cdot \pi(y) + \mathbb{1}_{L^{\perp}}(x)$, where $x, y \in \mathbb{F}_2^n$, for a suitably chosen subspace $L \subseteq \mathbb{F}_2^n$, which are provably outside $\mathcal{M}^{\#}$. F. Zhang, E. Pasalic, N. Cepak, and Y. Wei recently, in 2017, provided a set of sufficient conditions for functions in $\mathcal{C}$ to be outside $\mathcal{M}^{\#}$. These conditions mainly refer to certain properties of the permutation π, including the requirement that the component functions of π do not admit linear structures. We show that modifications of the identity permutation on arbitrary subsets of suitably selected subspaces (for the purpose of defining π), are suitable for constructing bent functions provably in $\mathcal{C} \setminus \mathcal{M}^{\#}$. Moreover, some component functions of such permutations π admit linear structures. The possibility of selecting an arbitrary subset of a linear subspace for the modification of the identity permutation will give us infinite classes of bent functions in $\mathcal{C}$ which are provably outside $\mathcal{M}^{\#}$. We also pursue the opposite direction, that is, we construct a class of permutations suitable for specifying bent functions in $\mathcal{C}$, and rely on the set of sufficient conditions proved by F. Zhang *et al.*, to show that the functions are outside $\mathcal{M}^{\#}$. To illustrate the hardness of the underlying problem, we first show that coset-based permutations are not suitable for this purpose, proving that members of this family of permutations inevitably have component functions that admit linear structures. Instead, we employ a certain method of non-trivial decomposition of the vector space $\mathbb{F}_2^n$ into disjoint affine subspaces. The permutations without linear

structures are then constructed using the decomposition and suitable permutations in a smaller number of variables. The possibility of selecting different subspaces in the decomposition and different permutations in a smaller number of variables provides us with a large family of bent functions in the $\mathcal{C}$ class which are outside $\mathcal{M}^{\#}$. This approach requires that the dimension of the subspace L is less than $n/2$. In contrast with this result, we prove that when the dimension of the subspace L is relatively large and when $\pi^{-1}(a+L)$ is an affine subspace for all $a \in \mathbb{F}_2^n$, the permutation π necessarily has component functions with linear structures. Using ranks of bent functions, we then investigate the intersection of the $\mathcal{C}$ class and the partial spread class $\mathcal{PS}_{ap}$ and show that the probability that an n-variable function in $\mathcal{PS}_{ap}$ is also in $\mathcal{C}$ approaches zero as n increases.

In the second part of the thesis, we shift our focus towards vectorial Boolean functions, and we investigate various properties related to their nonlinearity. In order to describe the properties of vectorial bent functions more precisely, we introduce the concept of *weakly* and *strongly* outside a class of bent functions. The motivation for the concept of being *weakly* or *strongly* outside $\mathcal{M}^{\#}$ comes from the fact that certain infinite classes of bent functions in $\mathcal{C}$ and $\mathcal{D}$, but provably outside $\mathcal{M}^{\#}$, will be specified in the first part of the thesis. Then, employing such functions as initial bent functions, gives vectorial bent functions with certain components in $\mathcal{M}^{\#}$ and the remaining ones, belonging to $\mathcal{C}$ or $\mathcal{D}$, are provably outside $\mathcal{M}^{\#}$. In this context, the problem of constructing vectorial functions which are strictly outside the known primary classes is quite delicate, as well as the question whether these functions can be extended to the maximal output bent dimension. In this direction, we provide a way to construct vectorial bent functions which are strongly outside $\mathcal{M}^{\#}$, for various output dimensions. Then, we generalize the notion of bent-negabent functions, introduced by C. Riera and M. Parker in 2006, by introducing the notion of *vectorial bent-negabent* functions. We show that in general for a vectorial bent-negabent function $F\colon \mathbb{F}_2^{2n} \to \mathbb{F}_2^k$ we necessarily have that $k \leq n-1$, and we provide a class of vectorial bent-negabent functions with the maximal output dimension $n-1$ by using a set of linear complete mappings of cardinality $n-1$. Employing certain vector spaces of complete mappings we identify several families of vectorial bent-negabent functions having components outside $\mathcal{M}^{\#}$. We also describe a generic method for specifying vector spaces of complete mappings. The method can be efficiently used to construct vectorial bent-negabent functions having approximately half of the component functions outside the completed $\mathcal{M}$ class. We then derive an upper bound on the maximum number of bent-negabent components for mappings $F : \mathbb{F}_2^{2n} \to \mathbb{F}_2^k$, where $2 \leq k \leq 2n$, and identify some families of the functions reaching this upper bound.

In the third part of the thesis, we focus on another cryptographically significant property of Boolean functions called correlation immunity. We show that using certain weight divisibility results related to restrictions of correlation immune (CI) functions, a compact proof of Siegenthaler's bound on the algebraic degree can be deduced. In addition, we determine precisely the weight of the k-th order CI functions having (all) terms of degree $n-k$ in its algebraic normal form. Using the same divisibility results, we will also exactly determine the Walsh spectral values at vectors of weight $k+1$ for k-th order CI Boolean functions. Two efficient construc-

tions of CI functions are presented which are well-suited for designing a subclass of these functions having minimum weight, and we use them to prove the conjecture of C. Carlet and X. Chen about the minimum weight of 3-CI functions for any n of the form $n = 2^k - i$ and $n = 3 \cdot 2^k - i$, for $i = 0, 1, 2, 3$ and $k \geq 3$. Then, we investigate O'Donnell's conjecture which, translated to the Boolean setting by Q. Wang, states that: if $g : \{0,1\}^n \to \{0,1\}$ is an $(n-d-1)$-resilient Boolean function, then

$$\sum_{\substack{v \in \{0,1\}^n \\ \mathrm{wt}(v) = n-1}} W_g(v) \leq d \binom{d-1}{\lfloor \frac{d-1}{2} \rfloor} 2^{n+1-d},$$

where $W_g(v)$ is the Walsh coefficient of g at point $v \in \mathbb{F}_2^n$. We prove that the conjecture is true for all n when $d = 2$ and $d = 3$. However, when $d = 4$, we identify a 2-resilient Boolean function in 7 variables violating the conjecture, the existence of which shows that the conjecture is not true in general.

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

Key words: bent functions, nonlinearity, Marioana-McFarland class, $\mathcal{C}$ class, $\mathcal{D}$ class, permutations, finite fields, correlation immunity, resiliency.

Izvleček

DOLOČANJE UKRIVLJENIH FUNKCIJ ZUNAJ $\mathcal{M}^{\#}$ RAZREDA IN DOLOČENI REZULTATI O KORELACIJSKI IMUNOSTI FUNKCIJ

Glavni predmet študija doktorske disertacije so kriptografsko pomembne lastnosti Boolovih funkcij. Odvisno od tega, katera kriptografsko pomembna lastnost je v središču naše pozornosti, je disertacija razdeljena na tri ustrezne dele.

Prvi del predlagane doktorske disertacije se bo osredotočil na natančnejši opis (glede na pripadnost razredu) sekundarnega razreda ukrivljenih funkcij $\mathcal{D}_0$ in $\mathcal{C}$. C. Carlet je v devetdesetih letih preteklega stoletja zagotovil zadosten pogoj, da leži ukrivljena funkcija v razredu $\mathcal{D}_0$ oblike $f(x,y) = x \cdot \pi(y) + \delta_0(x)$ nad $\mathbb{F}_2^{2n}$, kjer je $x, y \in \mathbb{F}_2^n$, π permutacija $\mathbb{F}_2^n$ in $\delta_0(x)$ indikator (karakteristična funkcija) podprostora $\{0_n\} \times \mathbb{F}_2^n$, zunaj razreda $\mathcal{M}^{\#}$ na podlagi lastnosti permutacije π. Namreč, če permutacija π ni afina na nobeni hiperravnini prostora $\mathbb{F}_2^n$, potem funkcija f leži zunaj razreda $\mathcal{M}^{\#}$. Pokazali bomo, da, ko je stopnja permutacije π večja od 2, Boolova funkcija $f(x,y) = x \cdot \pi(y) + \delta_0(x)$, z $f : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2$, vedno leži zunaj razreda $\mathcal{M}^{\#}$ (ne glede na to, ali je permutacija π afina na neki hiperravnini ali ne). Po drugi strani pa bomo dokazali, da je zadosten pogoj Carleta nujen tudi pri $\deg(\pi) = 2$. Potem bomo obravnavali tudi problem pripadnosti sekundarnim razredom upognjenih funkcij $\mathcal{C}$. Ogledali si bomo problem določanja ukrivljenih funkcij v razredu $\mathcal{C}$, ki so oblike $f(x,y) = x \cdot \pi(y) + \mathbb{1}_{L^\perp}(x)$, kjer je $x, y \in \mathbb{F}_2^n$, za ustrezno izbran podprostor $L \subseteq \mathbb{F}_2^n$, ki so dokazljivo zunaj $\mathcal{M}^{\#}$. Pred kratkim, leta 2017, so F. Zhang, E. Pasalic, N. Cepak in Y. Wei določili niz zadostnih pogojev. Ti pogoji se v glavnem nanašajo na določene lastnosti permutacije π, ki vključujejo zahtevo, da komponentne funkcije permutacije π ne vsebujejo linearnih struktur. Pokazali bomo, da modifikacije permutacije identitete na poljubnih podmnožicah ustrezno izbranih podprostorov (za namen definiranja permutacije π), so primerne za konstruiranje ukrivljenih funkcij, ki dokazljivo ležijo v $\mathcal{C} \setminus \mathcal{M}^{\#}$. Komponentne funkcije takšnih permutacij π še vedno dopuščajo linearne strukture. Upoštevajmo, da nam bo možnost izbire poljubne podmnožice linearnega podprostora za modifikacijo permutacije identitete dala veliko neskončnih razredov ukrivljenih funkcij v $\mathcal{C}$, ki so dokazljivo zunaj $\mathcal{M}^{\#}$. Sledili bomo tudi raziskavi, ki se ukvarja z obratnim problemom. Torej, zgradili bomo razred permutacij, primernih za določanje ukrivljenih funkcij razreda $\mathcal{C}$, ki so dokazljivo zunaj dokončanega $\mathcal{M}^{\#}$ razred z zadostnimi rezultati, ki so jih dokazali F. Zhang et al., 2017. Da bi ponazorili kompleksnost osnovnega problema, bomo najprej pokazali, da permutacije, ki temeljijo na odsekih, niso primerne za naš namen, saj imajo člani te družine permutacij neizogibno komponentne funkcije, ki dopuščajo linearne strukture. Namesto tega uporabljamo določeno metodo netrivialne razdelitve vektorskega prostora $\mathbb{F}_2^n$ v disjunktne afine

podprostore. Permutacije brez linearnih struktur bodo konstruirane z uporabo dekompozicije in ustreznih permutacij v manjšem številu spremenljivk. Možnost izbire različnih podprostorov pri razgradnji in različnih permutacij v manjšem številu spremenljivk nam omogoča konstrukcijo družine ukrivljenih funkcij v razredu $\mathcal{C}$, ki so zunaj $\mathcal{M}^{\#}$. Ta pristop zahteva, da je dimenzija podprostora L manjša od $n/2$. V nasprotju s tem rezultatom dokazujemo, da, ko je dimenzija podprostora L relativno velika in komponente permutacije ne dopuščajo linearnih struktur, $\pi^{-1}(a+L)$ ne more biti afin podprostor za vse $a \in \mathbb{F}_2^n$. S pomočjo ranga ukrivljenih funkcij bomo v prvem delu doktorske naloge raziskali tudi presečišče razreda $\mathcal{C}$ in razreda delnega pokritja $\mathcal{PS}_{ap}$ ter pokazali, da se verjetnost, da je funkcija n spremenljivk, ki je v razredu $\mathcal{PS}_{ap}$, tudi v $\mathcal{C}$, približuje nič, ko se n povečuje.

V *drugem delu* disertacije se bomo osredotočili na vektorske Boolove funkcije in raziskali različne lastnosti, povezane z nelinearnostjo vektorskih Boolovih funkcij. Da bi natančneje opisali lastnosti teh vektorskih ukrivljenih funkcij, uvedemo koncept šibke izločenosti in močne izločenosti zunaj dokončanega vnaprej določenega primarnega razreda. Glavni interes našega koncepta, da smo šibko ali močno zunaj $\mathcal{M}^{\#}$, izhaja iz dejstva, da bodo v prvem delu disertacije predstavljeni določeni neskončni razredi ukrivljenih funkcij v $\mathcal{C}$ in $\mathcal{D}$, ki dokazljivo ležijo zunaj $\mathcal{M}^{\#}$. Nato z uporabo takšnih funkcij, kot so začetne ukrivljene funkcije, dobimo vektorske ukrivljene prostore, katerih določene komponente so v primarnem razredu $\mathcal{M}$, in preostale pripadajo razredoma $\mathcal{C}$ ali $\mathcal{D}$ in so dokazljivo zunaj $\mathcal{M}^{\#}$. V tem kontekstu je problem določanja vektorskih funkcij, ki so strogo izven znanih primarnih razredov, precej delikaten, kot tudi vprašanje, ali je te funkcije mogoče razširiti na največjo izhodno ukrivljeno dimenzijo. V tej smeri nudimo način za konstruiranje vektorskih upognjenih funkcij, ki so močno zunaj $\mathcal{M}^{\#}$, za različne izhodne dimenzije. Nato posplošimo pojem ukrivljene-negaukrivljene funkcije ki sta ga leta 2006 uvedla C. Riera in M. Parker, z uvedbo pojma vektorske ukrivljene-negaukrivljene funkcije. Pokazali bomo da mora, v splošnem, za ukrivljeno-negaukrivljeno funkcijo $F\colon \mathbb{F}_2^{2m} \to \mathbb{F}_2^k$ nujno veljati $k \leq m-1$. Določimo razred vektorskih ukrivljenih-negaukrivljenih funkcij z največjo izhodno dimenzijo $m-1$ z uporabo množice linearnih popolnih preslikav kardinalnosti $m-1$. Z uporabo določenih vektorskih prostorov popolnih preslikav nudimo več družin vektorskih ukrivljenih-negaukrivljenih funkcij, ki imajo komponente zunaj $\mathcal{M}^{\#}$. Z uporabo primerne dekompozicije vektorskega prostora (in alternativne identificiranje ustreznih podpolj) nudimo splošno metodo določanja vektorskih prostorov popolnih preslikav, ki se nato učinkovito uporabijo za določanje vektorskih ukrivljenih negaukrivljenih funkcij (katerih dimenzija ni maksimalna), kjer približno polovica komponentnih funkcij leži zunaj popolnega razreda $\mathcal{M}$. Potem izpeljemo zgornjo mejo za največje število ukrivljenih-negaukrivljenih komponent za preslikave $F : \mathbb{F}_2^{2m} \to \mathbb{F}_2^k$, kjer je $2 \leq k \leq 2m$, in identificiramo nekatere družine teh funkcij, ki dosežejo zgornjo mejo.

V *tretjem delu* disertacije bomo raziskali še eno kriptografsko pomembno lastnost Boolovih funkcij, imenovano korelacijsko imunost (CI). Pokazali bomo, da je z uporabo določenih rezultatov, vezanih na deljivosti uteži, povezanih z omejitvami funkcij CI, mogoče izpeljati kompakten dokaz Siegenthalerjeve meje algebraične stopnje. Poleg tega natančno določimo težo CI funkcij k-tega reda, kjer so (vsi) členi stopnje $n-k$ v svoji algebraični normalni obliki. Z uporabo istih rezultatov deljivosti

bomo tudi natančno določili Walsheve spektralne vrednosti vektorjev teže $k+1$ za CI Boolove funkcije k-tega reda. Predstavljeni bosta dve učinkoviti konstrukciji funkcij CI, ki sta primerni za načrtovanje podrazreda z minimalno težo, in jih uporabimo za dokazovanje domneve C. Carleta in X. Chena o minimalni teži 3-CI funkcij, za kateri koli n oblike $n = 2^k - i$ ali $n = 3 \cdot 2^k - i$, za $i = 0, 1, 2, 3$ in $k \geq 3$. Potem bomo raziskali O'Donnellovo domnevo o rasti vsote linearnih Fourierovih koeficientov, ki prevedeno v enakovredno domnevo o razredu odpornih Boolovih funkcij navaja, da, če je $g : \{0,1\}^n \to \{0,1\}$ $(n-d-1)$-odporna Boolova funkcija, potem

$$\sum_{\substack{v \in \{0,1\}^n \\ \mathrm{wt}(v) = n-1}} W_g(v) \leq d \binom{d-1}{\lfloor \frac{d-1}{2} \rfloor} 2^{n+1-d},$$

kjer je $W_g(v)$ Walshev koeficient g v točki $v \in \mathbb{F}_2^n$. Dokazali bomo, da je domneva resnična za vse n, ko je $d = 2$ in $d = 3$. Ko pa je $d = 4$, bomo identificirali 2-odporno Boolovo funkcijo na 7 spremenljivkah, ki krši domnevo. To pomeni, da domneva v splošnem ne drži.

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

Ključne besede: ukrivljene funkcije, nelinearnost, Marioana-McFarland razred, $\mathcal{C}$ razred, $\mathcal{D}$ razred, permutacije, končna polja, korelacijska imunost, odporne funkcije.

Contents

List of Tables

Chapter 1

Introduction

The main subject of study in this thesis will be cryptographically significant properties of Boolean functions. Informally, Boolean functions are the functions which take as inputs strings of zeroes and ones (of fixed length) and output either zero or one, or in the even more general case of vectorial Boolean functions, they output strings of zeroes and ones. We make this intuitive notion formal by saying that Boolean functions are functions from $\{0,1\}^n$ (where n is a natural number) to $\{0,1\}$, or in the vectorial case to $\{0,1\}^k$ (where k is also some natural number, possibly different from n).

With the development and the rise of interest in modern computing machines, starting back in the first half of the 20th century, there was a parallel rise of interest of the scientific community in various properties of Boolean functions, and they became one of the basic objects of study in theoretical computer science. Quickly, the importance of secure private communication based on the new technology became apparent. In 1945 (published in 1949 in [66]) C. Shannon identified confusion and diffusion as two important properties that any secure cipher should possess. When present, confusion and diffusion hinder the application of statistics and other methods of cryptanalysis. In turn, confusion and diffusion help us to determine which properties of the Boolean functions used in a cipher are desirable, and which are undesirable. We call such properties cryptographically significant properties of Boolean functions.

Over many years of security analysis of symmetric-key ciphers, it appears that one of the significant cryptographic properties of Boolean functions is nonlinearity. For example, here are two quotes about nonlinearity that illustrate its importance: *"a high nonlinearity is surely one of the most important cryptographic criteria"* from [12], and *"linearity is the curse of the cryptographer"* from [42]. To avoid linear attacks, ideally the functions used in a cipher should be as nonlinear as possible, of course, taking into account the other desirable cryptographic properties. Motivated by this, in the 1960s (published in 1976 in [62]), O. Rothaus introduced a class of Boolean functions called bent functions, and defined them to be the Boolean functions which are as far away from linear and affine functions as possible, the distance between two functions being the Hamming distance i.e. the number of input vectors for which the output of the two functions differ (all notions used in the introduction are defined precisely and with more details in Chapter 2). That is,

bent functions are maximally nonlinear Boolean functions. This explains, if we recall the two aforementioned nonlinearity quotes, why bent functions are so important and ubiquitous in cryptography.

A significant part of research on bent functions is concerned with their constructions, i.e. searching for various ways to construct bent functions. Constructions of bent functions are split into two groups: primary constructions (constructions which do not require other bent functions in order to construct new ones, i.e. starting from scratch) and secondary constructions (constructions utilising other bent functions to construct new ones). For a detailed survey on bent functions we refer to the book of S. Mesnager [48], whereas an exhaustive survey on cryptographic (vectorial) Boolean functions can be found in [12]. Two of the best studied primary classes of bent functions are the Maiorana-McFarland ($\mathcal{M}$) class and the partial spreads ($\mathcal{PS}$) class, which were introduced in the 1970s in [43] and [21, 22], respectively. Since it is not a simple matter to construct elements of the class $\mathcal{PS}$ practically, an explicit subclass of the class, denoted by $\mathcal{PS}_{ap}$, is specified in [21] for its ease of construction. A non-exhaustive list of various secondary constructions can be found in the following works [11, 14, 28, 47, 75, 85]. The Maiorana-McFarland class $\mathcal{M}$ is the set of $2n$-variable Boolean bent functions of the form

$$f(x, y) = x \cdot \pi(y) + \rho(y), \text{ for all } x, y \in \mathbb{F}_2^n,$$

where ρ is an arbitrary Boolean function on $\mathbb{F}_2^n$, and π is a permutation of $\mathbb{F}_2^n$, and $x \cdot \pi(y)$ is the standard dot product of two vectors in $\mathbb{F}_2^n$ (here $\mathbb{F}_2^n$ denotes the n-dimensional vector space over the field with two elements $\mathbb{F}_2 = \{0, 1\}$). The completed $\mathcal{M}$ class, denoted by $\mathcal{M}^{\#}$, is the class of all bent functions affine equivalent to functions in $\mathcal{M}$. (Two functions in m variables f and g are affine equivalent if there exist an affine permutation L_1 of $\mathbb{F}_2^m$ and an affine function $l_2 : \mathbb{F}_2^m \to \mathbb{F}_2$, such that $f(x) = g(L_1(x)) + l_2(x)$, for all $x \in \mathbb{F}_2^m$.)

The exact number of bent functions in m variables is known only when $m \leq 8$. For $m \leq 6$, all bent functions are affine equivalent to functions in the class $\mathcal{M}$. However, already for $m = 8$ the number of bent functions in the class $\mathcal{M}^{\#}$ (at most $2^{81.38}$) is negligible compared to the number of all bent functions in 8 variables (approximately $2^{106.29}$) [37]. Despite this, the class $\mathcal{M}$ is still the widest known primary class of bent functions. Therefore, in order to bridge the gap, it is important to investigate new constructions and determine how they intersect with the already known classes of bent functions, especially the class $\mathcal{M}$.

In the 1990s, C. Carlet [9] provided two new secondary constructions of bent functions using bent functions from the class $\mathcal{M}$ and adding indicators of an appropriately chosen vector subspace. The classes of bent functions obtained by the constructions are called $\mathcal{C}$ and $\mathcal{D}$. A particular subclass of both $\mathcal{C}$ and $\mathcal{D}$, called $\mathcal{D}_0$, is singled out in [9] because of a simpler form of the subspaces used and for the ease of construction. It is established in [9] that there are functions in $\mathcal{D}_0$ which are not affine equivalent to any function in the class $\mathcal{M}$, and also, that there are some functions in the class $\mathcal{D}_0$ which are not affine equivalent to any function in the class $\mathcal{PS}$. Thus showing that $\mathcal{C}$ and $\mathcal{D}$ truly are two new classes of bent functions.

In Chapter 3, we will focus on providing a more accurate description (in terms of class membership) of the secondary class of bent functions $\mathcal{D}_0$. C. Carlet in

[9] considered bent functions in the $\mathcal{D}_0$ class, which are the Boolean functions of the form $f(x,y) = x \cdot \pi(y) + \delta_0(x)$, where $x, y \in \mathbb{F}_2^n$, π is a permutation of $\mathbb{F}_2^n$ and $\delta_0(x)$ is the indicator (characteristic function) of the subspace $\{0_n\} \times \mathbb{F}_2^n$. [9, Proposition 2] provides a sufficient condition for the functions in $\mathcal{D}_0$ to be outside $\mathcal{M}^\#$, based on properties of the permutation π. Namely, if π is not affine on any linear hyperplane of $\mathbb{F}_2^n$ (i.e. $(n-1)$-dimensional subspace of $\mathbb{F}_2^n$), then f is outside $\mathcal{M}^\#$. In our characterization, we will use the notion of algebraic degree of a Boolean function. We can represent a Boolean function f as a polynomial $f(x_1, \ldots, x_n) = \sum_{a=(a_1,\ldots,a_n)\in\mathbb{F}_2^n} \mu_a x_1^{a_1} \cdots x_n^{a_n}$ over $\mathbb{F}_2$ in a unique way, and we call that representation the algebraic normal form of f. The algebraic degree of f is then defined as the degree of the polynomial, that is, the maximal length of any multivariate term $x_1^{a_1} \cdots x_n^{a_n}$ for which μ_a is nonzero. For a vectorial Boolean function, we define its algebraic degree as the maximum algebraic degree of its component functions. We will show that, when the algebraic degree of a permutation π is greater than 2, the Boolean function $f(x,y) = x \cdot \pi(y) + \delta_0(x)$, with $f : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2$, is always outside $\mathcal{M}^\#$ (regardless of the fact whether π is affine on some hyperplane or not). On the other hand, we will prove that the sufficient condition of C. Carlet is also necessary when $\deg(\pi) = 2$. Therefore, we provide a complete description of the relation between the classes $\mathcal{D}_0$ and $\mathcal{M}^\#$.

In Chapter 4, we will investigate the class membership problem for the secondary class of bent functions $\mathcal{C}$. We will consider the problem of specifying bent functions in $\mathcal{C}$, which are of the form $f(x,y) = x \cdot \pi(y) + \mathbb{1}_{L^\perp}(x)$, where $x, y \in \mathbb{F}_2^n$, for a suitably chosen subspace $L \subseteq \mathbb{F}_2^n$, which are provably outside $\mathcal{M}^\#$. In [83], a set of sufficient conditions for the functions in $\mathcal{C}$ and $\mathcal{D}$ to be outside $\mathcal{M}^\#$ is obtained. These mainly refer to certain properties of the permutation π, including the requirement that the component functions of π do not admit linear structures (for more details check Section 4.1). These sufficient conditions are quite useful when specifying bent functions in $\mathcal{C} \backslash \mathcal{M}^\#$ and $\mathcal{D} \backslash \mathcal{M}^\#$, but it was demonstrated that they are not necessary, see e.g. [84]. In particular, certain modifications of the identity permutation π (swapping two output values) was shown to provide bent functions in $\mathcal{D}$ which are provably outside $\mathcal{M}^\#$, even though the component functions of π admit linear structures. In this context, related to bent functions in $\mathcal{C}$, we will show a stronger result which enables modifications of the identity permutation on arbitrary subsets of suitably selected subspaces (for the purpose of defining π), while at the same time the resulting bent functions will provably be in $\mathcal{C} \setminus \mathcal{M}^\#$. The component functions of such permutations π still admit linear structures which again indicate that there is a possibility of relaxing the set of sufficient conditions in [83]. Notice that the possibility of selecting an arbitrary subset of a linear subspace for the modification of the identity permutation will give us many infinite classes of bent functions in $\mathcal{C}$ which are provably outside $\mathcal{M}^\#$.

In Chapter 4, we will also pursue the opposite direction compared to the one in the previous paragraph, that is, we will construct a class of permutations suitable for specifying bent functions in $\mathcal{C}$, and rely on the set of sufficient conditions from [83] to prove that the functions are outside $\mathcal{M}^\#$. To illustrate the hardness of the underlying problem, we will first show that coset-based permutations are not suitable for the purpose, since the members of this family of permutations inevitably have com-

ponent functions that admit linear structures. Instead, we employ a certain method of non-trivial decomposition of the vector space $\mathbb{F}_2^n$ into disjoint affine subspaces, originally considered by L.E. Baum and L.P. Neuwirth in [2]. The permutations are constructed using the decomposition and suitable permutations in a smaller number of variables. The possibility of selecting different subspaces in the decomposition and different permutations in a smaller number of variables provides us with a large family of bent functions in the $\mathcal{C}$ class which are outside $\mathcal{M}^{\#}$. This approach requires that the dimension of the subspace L is less than $n/2$. In contrast with this result, we prove that when the dimension of the subspace L is relatively large and when $\pi^{-1}(a+L)$ is an affine subspace for all $a \in \mathbb{F}_2^n$, the permutation π necessarily has component functions with linear structures. This result gives a further insight into what is likely a trade-off of using the sufficient, but not necessary, conditions from [83] for distinguishing the bent functions in $\mathcal{C}$ which are outside $\mathcal{M}^{\#}$.

Using ranks of bent functions, in Chapter 4 we will also investigate the intersection of the $\mathcal{C}$ class and the partial spread class $\mathcal{PS}_{ap}$ and we will show that the probability that an n-variable function in $\mathcal{PS}_{ap}$ is also in $\mathcal{C}$ approaches zero as n increases.

Then, we will shift our focus towards vectorial Boolean functions, and we will investigate various properties related to nonlinearity of vectorial Boolean functions. The bent property of Boolean functions has been extended to vectorial Boolean functions by requesting that all the nonzero linear combinations of its coordinate functions are bent Boolean functions. Such vectorial functions are called vectorial bent. In the literature, methods to construct new vectorial bent functions are again divided into two classes: those building functions from scratch are called primary; those using known vectorial bent functions are called secondary. For primary constructions, K. Nyberg firstly presented the constructions of vectorial bent functions based on some special classes of bent functions such as the Maiorana-McFarland class and the partial spreads class.

In Chapter 5, we will define and investigate the class of vectorial bent-negabent functions. C. Riera and M. Parker [61] introduced the class of negabent functions, motivated by their applications to quantum computing. A Boolean function is said to be negabent, if its absolute nega-Hadamard spectrum is flat (or equivalently, f is negabent if $f + s_2$ is bent, where s_2 denotes the elementary symmetric quadratic Boolean function, i.e., $s_2(x) = \sum_{1 \le i < j \le n} x_i x_j$, for $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$). For an even number of variables, a function is called bent-negabent if it is both bent and negabent. The problem of constructing Boolean functions, which are simultaneously bent and negabent, was considered in [53, 65, 69, 71, 82]. M. Parker and A. Pott [53] considered the problem of determining the number of quadratic bent–negabent functions in n variables. It was consequently resolved by A. Pott *et al.* [59], who used a characterization of quadratic bent–negabent Boolean functions obtained in [53].

There are several design methods of bent-negabent functions given in e.g. [65, 71, 82]. In [71], a set of necessary and sufficient conditions for a Boolean function to be negabent (regardless the parity of the number of variables) was derived, which also allowed the design of a broader class of n-variable bent-negabent functions (n even) of the algebraic degree ranging from 2 to $n/2$. These functions are

however contained in the completed Maiorana-McFarland class. In difference to the standard employment of the Maiorana-McFarland class, it was shown in [82] that bent-negabent functions outside $\mathcal{M}^{\#}$ could be constructed using the indirect sum method and suitable complete mappings. Bent-negabent functions have recently received renewed attention due to the work in [70], where the connection between bent-negabent functions and Kerdock codes was established.

Nevertheless, all known methods so far only considered the Boolean case and the possibility of building vector spaces of bent-negabent functions has not been addressed in the literature. We will introduce the notion of *vectorial bent-negabent* functions and show that in general for a bent-negabent function $F\colon \mathbb{F}_2^{2n} \to \mathbb{F}_2^k$ we necessarily have that $k \leq n-1$. We provide a class of vectorial bent-negabent functions with the maximal output dimension $n-1$ by using a set of linear complete mappings of cardinality $n-1$. However, due to the linearity of these mappings, this approach only gives functions whose components are contained in the $\mathcal{M}^{\#}$ class. We then show that the so-called b-complete mappings on $\mathbb{F}_{2^n}$ considered in e.g. [18], which are permutations $x + bF(x)$ for many $b \in \mathbb{F}_{2^n}$, can be used for the purpose of designing non-quadratic vectorial bent-negabent functions. In a similar fashion as for vectorial bent functions [60, 85], we investigate and derive an upper bound on the maximum number of bent-negabent components for mappings $F : \mathbb{F}_2^{2n} \to \mathbb{F}_2^k$, where $2 \leq k \leq 2n$, and identify some families of the functions reaching this upper bound.

To describe the properties of vectorial bent functions more precisely, in Chapter 6 we introduce the concept of *weakly* and *strongly* outside a pre-specified class of bent functions. The main reason for this is that for the Maiorana-McFarland class one can easily deduce that its vectorial bent functions have the property that their (nonzero) component functions are bent functions in $\mathcal{M}$. This is in general not true for vectorial functions having its coordinates in $\mathcal{C}$ or $\mathcal{D}$. In fact, the motivation for the concept of being weakly or strongly outside $\mathcal{M}^{\#}$ comes from the fact that certain infinite classes of bent functions in $\mathcal{C}$ and $\mathcal{D}$, but provably outside $\mathcal{M}^{\#}$, will be specified in the first part of the thesis. Then, employing such functions as initial bent functions, gives vectorial bent functions with certain components in the primary class $\mathcal{M}$ and the remaining ones, belonging to $\mathcal{C}$ or $\mathcal{D}$, are provably outside $\mathcal{M}^{\#}$. This means that for the first time we provide evidence of infinite classes of vectorial bent functions having such a peculiar feature. On the other hand, the problem of specifying vectorial functions which are strictly outside the known primary classes is quite delicate as well as the question whether these functions can be extended to the maximal output bent dimension (being n for the input space of size $2n$). In this direction, we provide a way to construct vectorial bent functions which are strongly outside $\mathcal{M}^{\#}$, for various output dimensions (but not for the maximal one).

In Chapter 6, we will also combine the notion of weakly outside the $\mathcal{M}^{\#}$ class and the notion of vectorial bent-negabent functions introduced in Chapter 5. To provide families of vectorial bent-negabent functions, additionally having components outside $\mathcal{M}^{\#}$, we employ vector spaces of complete mappings of the form $F(x) = x^d + b_1 a_1 x + \cdots + b_t a_t x$, where F is a permutation of $\mathbb{F}_{2^n}$ for a set of linearly independent (over $\mathbb{F}_2$) elements $a_1, \ldots, a_t \in \mathbb{F}_{2^n}$ and for any choice of binary coefficients $b_i \in \mathbb{F}_2$. Notice that in the case that $1 \in \langle a_1, \ldots, a_t \rangle$, we have that F is

also a standard complete mapping since both $F(x)$ and $F(x)+x$ are permutations over $\mathbb{F}_{2^m}$. Nevertheless, it is not necessary that F is a permutation itself and this case is considered separately. Namely, using a suitable decomposition of the vector space (alternatively identifying suitable subfields) we provide a generic method of specifying vector spaces of complete mappings which are then efficiently used to construct vectorial bent-negabent functions (whose dimension is not maximal) having approximately half of the component functions outside the completed $\mathcal{M}$ class.

In Chapter 7, we will shift our focus from nonlinearity, and we will investigate another cryptographically significant property of Boolean functions called correlation immunity. An n-variable Boolean function f is called correlation immune of order d (in brief, d-CI) if the output distribution of f does not change when at most d input variables are fixed. For cryptographic applications, the notion of correlation immunity is commonly related to the so-called nonlinear combiner model, a representative of a certain family of stream ciphers [46]. This property is crucial for this model in order to withstand correlation attacks [30, 31, 45, 68]. A closely related notion of resiliency is often used as a cryptographic criterion which, apart from a certain order of correlation immunity of the combining Boolean function, also requires its balancedness. Apart from this, a subclass of minimum weight CI functions has received a lot of attention recently due to their use as masking primitives for the purpose of hardware protection of certain encryption algorithms [4], see also [16]. In addition, CI functions are closely related to secret-sharing schemes and error-correcting codes [6, 23, 26].

A tight bound for the achievable algebraic degree of correlation immune functions was given by T. Siegenthaler in [67]. We will show that using certain weight divisibility results related to restrictions of CI functions (taken from [73]), a compact proof of Siegenthaler's bound on the algebraic degree can be deduced. In addition, we determine precisely the weight of the d-th order CI functions having (all) terms of degree $n-d$ in its algebraic normal form. Using the same divisibility results we will also exactly determine the Walsh spectral values at vectors of weight $d+1$ for d-th order CI Boolean functions.

Two efficient constructions of correlation immune functions, which are well-suited for designing a subclass of these functions having minimum weight, will be presented. Such functions have an immediate application as masking schemes for protecting ciphers against side-channel cryptanalysis [16]. As remarked in [15], for an efficient hardware implementation, CI functions need to have low Hamming weight. However, most of the known constructions (primary constructions like the Maiorana-McFarland construction and secondary constructions like the indirect sum, etc., see for example [12], [24]) do not allow us to build functions with such property. This initiated rather extensive research in this direction. More precisely, for a relatively low size of the input space (for $n \leq 13$) the minimum weight of CI functions has been determined and tabulated, apart from a few unknown values, see [16] and the subsequent work of Q. Wang and Y. Li [78]. For example, denoting the minimum weight of any d-th order CI function in n variables by $\omega_{n,d}$, the values of $\omega_{12,4}$, $\omega_{13,4}$ and $\omega_{13,5}$ have been determined in [78]. For the special case of 3-CI functions C. Carlet and X. Chen conjectured in [16] that $w_{n,3} = 8\lceil \frac{n}{4} \rceil$, for any integer $n \geq 3$, and it was shown by a construction that the conjecture is true for $n = 2^k$. Later

it was shown [76] that this conjecture is equivalent to the Hadamard conjecture, which claims that there exists a Hadamard matrix of order $4k$ for every positive integer k. Notice that the case when $n = 2^k$ then corresponds to Silvester-Hadamard matrices using this equivalence. We provide further evidence that the conjecture of C. Carlet and X. Chen is true through our generalization of their design method of CI functions from [16]. More precisely, it will be shown through the existence of 3-CI functions of minimum weight that the conjecture is true for any n of the form $n = 2^k - i$ and $n = 3 \cdot 2^k - i$, for $i = 0, 1, 2, 3$ and $k \geq 3$.

In a collection of open problems in the field of analysis of Boolean functions [52], R. O'Donnell stated a conjecture about the growth of the sum of linear Fourier coefficients, motivated by some problems in social choice. In [52], functions $f : \{-1, 1\}^n \to \{-1, 1\}$ were investigated, and hence in [52] the conjecture is stated as a conjecture about functions $f : \{-1, 1\}^n \to \{-1, 1\}$. In [77], Q. Wang translated O'Donnell's Conjecture to an equivalent conjecture about a class of resilient Boolean functions $f : \{0, 1\}^n \to \{0, 1\}$, thus giving an alternative interpretation of O'Donnell's Conjecture. In this form the conjecture states that if $g : \{0, 1\}^n \to \{0, 1\}$ is an $(n - d - 1)$-resilient Boolean function, then

$$\sum_{\substack{v \in \{0,1\}^n \\ \mathrm{wt}(v) = n-1}} W_g(v) \leq d \binom{d-1}{\lfloor \frac{d-1}{2} \rfloor} 2^{n+1-d},$$

where $W_g(v)$ is the Walsh coefficient of g at point $v \in \mathbb{F}_2^n$, given by

$$W_g(v) = \sum_{x \in \mathbb{F}_2^n} (-1)^{g(x)+v \cdot x}.$$

This alternative formulation was used by Q. Wang [77] to prove that the conjecture is true when $d = 1$ and $d = n - 1$, which gives a nontrivial relationship between the Walsh coefficients of weight $n - 1$ and the order of resilience of a Boolean function.

In Chapter 8, we will further employ Q. Wang's approach using the standard Boolean setting. Firstly, we will derive an interesting combinatorial property related to the conjecture which implies that, for a fixed d, the conjecture only depends on a finite number of integers n. More precisely, we show that if the conjecture is correct for all $n \leq 2^{2d-2}$, then it is true for all $n \in \mathbb{N}$. Then we will prove, again for a fixed d, that if the conjecture fails for some n_0, it is incorrect for every $n > n_0$. These two results will imply that, for a fixed d, if the conjecture is true for $n = 2^{2d-2}$, then it is true for every $n \in \mathbb{N}$. Therefore, an immediate consequence is that the conjecture is true for $d = 2$, since it can be easily checked exhaustively for $n = 4$. Nevertheless, a direct proof of this fact will be provided using a characterisation of $(n - 3)$-resilient functions given in [8]. Then, for $d = 3$, we will combine the results on characterisations of $(n-4)$-resilient functions given in [7] and [13], and show that it is enough to check the conjecture for $n = 6$, and in some special cases for $n = 7$. For the purpose of proving that the conjecture is true for $d = 3$, we will employ integer programming to verify the mentioned cases.

However, when $d = 4$, we will identify a 2-resilient Boolean function in 7 variables which violates the conjecture. This means that the conjecture is not true in general.

More specifically, the conjecture is not true whenever $n \geq 7$ implying that $(n-5)$-resilient Boolean functions do not necessarily satisfy the bound in the conjecture.

Finally, we will conclude the thesis by summarising the most important results presented in the thesis, and suggesting a couple of possible problems and directions for future research.

This PhD Thesis is based on the results obtained in the following articles:

- S. Kudin, E. Pasalic. A complete characterization of $\mathcal{D}_0 \cap \mathcal{M}^{\#}$ and a general framework for specifying bent functions in $\mathcal{C}$ outside $\mathcal{M}^{\#}$. *Designs, Codes and Cryptography*, vol. 90(8), pp. 1783–1796, (2022).

- S. Kudin, E. Pasalic, N. Cepak, F. Zhang. Permutations without linear structures inducing bent functions outside the completed Maiorana-McFarland class. *Cryptography and Communications*, vol. 14(1), pp. 101–116, (2022).

- E. Pasalic, S. Kudin, A. Polujan, A. Pott. Vectorial bent-negabent functions – their constructions and bounds. *IEEE Transactions on Information Theory*, doi: 10.1109/TIT.2022.3226571, (2022).

- E. Pasalic, F. Zhang, S. Kudin, Y. Wei. Vectorial bent functions weakly/strongly outside the completed Maiorana–McFarland class. *Discrete Applied Mathematics*, vol. 294, pp. 138–151, (2021).

- S. Kudin, E. Pasalic. Efficient design methods of low-weight correlation-immune functions and revisiting their basic characterization. *Discrete Applied Mathematics*, vol. 284, pp. 150–157, (2020).

- S. Kudin, E. Pasalic. Proving the conjecture of O'Donnell in certain cases and disproving its general validity. *Discrete Applied Mathematics*, vol. 289, pp. 345–353, (2021).

Chapter 2

Definitions, notation, and preliminary results

In this section, we introduce the concepts and results related to Boolean functions which will be used throughout the thesis. The goal is to make the thesis as self-contained as possible. However, if the reader finds that some details or explanations are missing, we refer to the following two excellent books on the subject by C. Carlet [12], and by T. Cusick and P. Stănică [20].

By $\mathbb{F}_2$ we denote the finite field with two elements, that is, the set $\{0, 1\}$ with the addition $+$ and the multiplication $\cdot$, such that 0 is the additive identity, 1 is the multiplicative identity, and $1 + 1 = 0$. We will also use the notation $+$ and $\cdot$ to represent operations in various other structures as well, but since it will always be clear from the context to which structure the elements belong, there will be no ambiguity. Throughout the thesis, we use the lowercase letters n, m and k to denote three (not necessarily distinct) natural numbers, usually such that $m = 2n$. The n-dimensional vector space over $\mathbb{F}_2$ is denoted by $\mathbb{F}_2^n$, that is, $\mathbb{F}_2^n$ is the set of all binary vectors of length n viewed as an $\mathbb{F}_2$-vectorspace. We denote the all-zero vector in $\mathbb{F}_2^n$ with 0_n, and by $\mathbb{F}_2^{n*}$ we denote the set $\mathbb{F}_2^n \setminus \{0_n\}$. We use $\mathbb{e}_i$ to denote the vector in $\mathbb{F}_2^n$ whose i-th coordinate is 1 and the rest are 0. By $\mathbb{F}_{2^n}$ we denote the finite field with 2^n elements. Once a basis for $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ is fixed, one can isomorphically identify $\mathbb{F}_2^n$ with $\mathbb{F}_{2^n}$.

Any function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ (or, equivalently from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$) is called *Boolean function* in n variables and the set of all Boolean functions in n variables is denoted by $\mathfrak{B}_n$. We can represent every Boolean function with its *truth table*, where in the first column we have all the possible vectors in $\mathbb{F}_2^n$, and in the second column we have the values of the Boolean function at the vectors in the same row of the first column. If we fix an ordering of $\mathbb{F}_2^n$ (and we do fix it to be the lexicographic ordering, if not stated otherwise), then we only need the second column of the truth table, assuming that the first one is ordered from the smallest to the largest element according to the ordering. Hence, we can identify an n-variable Boolean functions with an element of $\mathbb{F}_2^{2^n}$ in a unique way (when the ordering is fixed). From this, we deduce that there are 2^{2^n} Boolean functions in n variables. For example, the following (Table 2.1) are two Boolean functions in 4 variables with their truth tables.

x	$f(x)$
(0, 0, 0, 0)	0
(1, 0, 0, 0)	1
(0, 1, 0, 0)	0
(1, 1, 0, 0)	1
(0, 0, 1, 0)	0
(1, 0, 1, 0)	1
(0, 1, 1, 0)	0
(1, 1, 1, 0)	1
(0, 0, 0, 1)	0
(1, 0, 0, 1)	1
(0, 1, 0, 1)	0
(1, 1, 0, 1)	1
(0, 0, 1, 1)	0
(1, 0, 1, 1)	1
(0, 1, 1, 1)	0
(1, 1, 1, 1)	1

x	$g(x)$
(0, 0, 0, 0)	0
(1, 0, 0, 0)	0
(0, 1, 0, 0)	0
(1, 1, 0, 0)	1
(0, 0, 1, 0)	0
(1, 0, 1, 0)	0
(0, 1, 1, 0)	0
(1, 1, 1, 0)	1
(0, 0, 0, 1)	0
(1, 0, 0, 1)	0
(0, 1, 0, 1)	0
(1, 1, 0, 1)	1
(0, 0, 1, 1)	1
(1, 0, 1, 1)	1
(0, 1, 1, 1)	1
(1, 1, 1, 1)	0

Table 2.1: Truth tables of two Boolean functions in 4 variables.

When the ordering is understood, then we can write the truth tables of f and g (given in Table 2.1) simply as

$$f = (0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1);\ g = (0,0,0,1,0,0,0,1,0,0,0,1,1,1,1,0).$$

A *vectorial Boolean function* in n variables is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^k$. Throughout the thesis, we will use uppercase letters for vectorial Boolean functions, and lowercase letters for Boolean functions. From the definitions we see that every vectorial Boolean function $F : \mathbb{F}_2^n \to \mathbb{F}_2^k$ can be represented as

$$F(x) = (f_1(x), \ldots, f_k(x)), \text{ for all } x \in \mathbb{F}_2^n,$$

where $f_1, \ldots, f_k$ are Boolean functions in n variables. The functions $f_1, \ldots, f_k$ are called *coordinate functions* of F. Linear combinations (over $\mathbb{F}_2$) of the coordinate functions of F are called *component functions* of F. Similarly, like in the case of Boolean functions, we can represent vectorial Boolean functions via truth tables. For instance, the truth table of the vectorial Boolean function $F : \mathbb{F}_2^4 \to \mathbb{F}_2^2$ defined by $F = (f, g)$, where f and g are the Boolean functions defined in Table 2.1 is given in Table 2.2. The coordinate functions of F are f and g, and the component functions of F are 0 (the zero function from $\mathbb{F}_2^4$ to $\mathbb{F}_2$), f, g and

$$f + g = (0,1,0,0,0,1,0,0,0,1,0,0,1,0,1,1).$$

Truth tables, although probably the most intuitive, are not the only way to represent Boolean functions. Another way to represent an n-variable Boolean function f is to write it as an element of $\mathbb{F}_2[x_1, \ldots, x_n]/\langle x_1^2 + x_1, \ldots, x_n^2 + x_n \rangle$, and we call that representation the *algebraic normal form* (in brief the ANF) of f. More precisely,

x	$F(x)$
(0, 0, 0, 0)	$(0,0)$
(1, 0, 0, 0)	$(1,0)$
(0, 1, 0, 0)	$(0,0)$
(1, 1, 0, 0)	$(1,1)$
(0, 0, 1, 0)	$(0,0)$
(1, 0, 1, 0)	$(1,0)$
(0, 1, 1, 0)	$(0,0)$
(1, 1, 1, 0)	$(1,1)$
(0, 0, 0, 1)	$(0,0)$
(1, 0, 0, 1)	$(1,0)$
(0, 1, 0, 1)	$(0,0)$
(1, 1, 0, 1)	$(1,1)$
(0, 0, 1, 1)	$(0,1)$
(1, 0, 1, 1)	$(1,1)$
(0, 1, 1, 1)	$(0,1)$
(1, 1, 1, 1)	$(1,0)$

Table 2.2: Truth table of a vectorial Boolean function.

any Boolean function f in n variables can be uniquely represented in its algebraic normal form

$$f(x_1,\ldots,x_n) = \sum_{a=(a_1,\ldots,a_n)\in\mathbb{F}_2^n} \mu_a x_1^{a_1}\cdots x_n^{a_n}, \tag{2.1}$$

where $\mu_a \in \mathbb{F}_2$, for all $a=(a_1,\ldots,a_n)\in\mathbb{F}_2^n$. The coefficients μ_a are given by

$$\mu_a = \sum_{\substack{z\preceq a\\ z\in\mathbb{F}_2^n}} f(z), \tag{2.2}$$

where $\preceq$ is the partial order on $\mathbb{F}_2^n$ defined by: $z\preceq a$ if and only if $z_i\le a_i$ for all $i\in\{1,2,\ldots,n\}$; for every $a=(a_1,\ldots,a_n)$ and $z=(z_1,\ldots,z_n)$ in $\mathbb{F}_2^n$. For example, the algebraic normal forms of the functions f and g from Table 2.1 are

$$f(x_1,x_2,x_3,x_4)=x_1 \text{ and } g(x_1,x_2,x_3,x_4)=x_1x_2+x_3x_4.$$

For any binary vector $x\in\mathbb{F}_2^n$, the *Hamming weight* of x, denoted by $\mathrm{wt}(x)$, is defined as the number of nonzero entries of x, i.e. for $x=(x_1,\ldots,x_n)\in\mathbb{F}_2^n$ we have $\mathrm{wt}(x)=|\{i\in\{1,2,\ldots,n\}: x_i\neq 0\}|$. By abuse of notation, we sometimes write $\mathrm{wt}(d)$ for a positive integer d and mean that d is implicitly represented as a binary string. The *algebraic degree* of a Boolean function f in n variables with the algebraic normal form $f(x_1,\ldots,x_n)=\sum_{a=(a_1,\ldots,a_n)\in\mathbb{F}_2^n}\mu_a x_1^{a_1}\cdots x_n^{a_n}$, denoted by $\deg(f)$, is defined as $\deg(f)=\max_{a\in\mathbb{F}_2^n}\{\mathrm{wt}(a):\mu_a\neq 0\}$, that is, the maximum weight of those $a\in\mathbb{F}_2^n$ for which μ_a is nonzero. For example, the algebraic degrees of f and g from Table 2.1 are 1 and 2 respectively. A Boolean function is called *affine* if its algebraic degree is not larger than 1, *quadratic* if its degree is 2, and *cubic* if its degree is 3. The *algebraic degree of a vectorial Boolean function* F is the maximal algebraic degree of the coordinate functions of F.

The support of a Boolean function f in n variables, denoted by $supp(f)$, is defined as $supp(f) = \{x \in \mathbb{F}_2^n : f(x) \neq 0\}$. The *Hamming weight of a Boolean function* f, denoted by $\mathrm{wt}(f)$, is the number of elements in the support of the function. The *Hamming distance* between two Boolean functions f and g (in the same number of variables), is defined as $d(f,g) = \mathrm{wt}(f+g)$. For f and g given in Table 2.1, one can verify that $\mathrm{wt}(f) = 8$, $\mathrm{wt}(g) = 6$ and $d(f,g) = 6$.

The following theorem relates the Hamming distance with the algebraic degree of Boolean functions.

Theorem 2.0.1 *Any two distinct n-variable Boolean functions f and g of algebraic degree at most r have mutual distance at least 2^{n-r}.*

The theorem can be proved by a double induction over r and n using the equation (2.2). The theorem is stated as Theorem 7 in [12], where a detailed proof can be found (although in a slightly different, but equivalent form). For example, for f and g given in Table 2.1, since they are of algebraic degree at most 2, we have $d(f,g) = 6 \geq 2^{4-2} = 4$.

The standard scalar (dot) product of two vectors $u = (u_1, \ldots, u_n)$ and $x = (x_1, \ldots, x_n)$ from $\mathbb{F}_2^n$ is defined as $u \cdot x := \sum_{i=1}^{n} u_i x_i$. The finite field equivalent of the scalar product is the trace function. By $Tr_k^n(\cdot)$ we denote the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^k}$, where k divides n:

$$Tr_k^n(\beta) = \beta + \beta^{2^k} + \cdots + \beta^{2^{(n/k-1)k}}.$$

When $k = 1$, we denote $Tr_1^n(\cdot)$ simply by $Tr(\cdot)$ and call it the *absolute trace* on $\mathbb{F}_{2^n}$.

Every vectorial Boolean function in n variables, viewing them as functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$, has a unique representation as a polynomial over $\mathbb{F}_{2^n}$ of degree less than or equal to $2^n - 1$:

$$F(x) = \sum_{i=0}^{2^n-1} a_i x^i, \text{ for all } x \in \mathbb{F}_{2^n}. \tag{2.3}$$

We call this representation the (univariate) *polynomial form* of F. Since $\mathbb{F}_2$ is a subfield of $\mathbb{F}_{2^n}$, we deduce, as a special case, that every Boolean function has a unique representation as a polynomial over $\mathbb{F}_{2^n}$, and we also call this the polynomial form of a Boolean function.

Every Boolean function in n variables can be written in the form $f(x) = Tr(P(x))$ where P is a mapping from $\mathbb{F}_{2^n}$ into $\mathbb{F}_{2^n}$. For example, if we take $\lambda \in \mathbb{F}_{2^n}$ such that $Tr(\lambda) = 1$ and if Q is the polynomial form of f, then setting $P = \lambda Q$, we have that $f(x) = Tr(P(x))$, for all $x \in \mathbb{F}_{2^n}$. We call this representation the trace representation of f. Trace representation of a Boolean function in not necessarily unique.

One of the crucial tools used in the analysis of Boolean functions is the appropriate version of the discrete Fourier transform. *The Walsh transform* (or sometimes Walsh-Hadamard transform) of an n-variable Boolean function f is the mapping $W_f : \mathbb{F}_2^n \to \mathbb{Z}$, defined by:

$$W_f(w) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+x\cdot w}, \text{ for every } w \in \mathbb{F}_2^n. \tag{2.4}$$

The Fourier transform (or sometimes Fourier-Hadamard transform) of an n-variable Boolean function f is the mapping $\widehat{f} : \mathbb{F}_2^n \to \mathbb{Z}$, defined by:

$$\widehat{f}(w) = \sum_{x \in \mathbb{F}_2^n} f(x)(-1)^{x \cdot w}, \text{ for every } w \in \mathbb{F}_2^n. \tag{2.5}$$

In the definitions of the Walsh and Fourier transforms of Boolean functions, we need to be aware of a slight technicality, and that is, in the sums we look at $\mathbb{F}_2$ as if it is a subset of $\mathbb{Z}$ and use the addition in the set of integers, so in the end, the values of the sums are integers. Additionally, the Fourier transform can be defined more generally, with the same expression, for *pseudo-Boolean functions* – the functions from $\mathbb{F}_2^n$ into the set of real numbers $\mathbb{R}$. Consequently, we will sometimes use the Fourier transform of pseudo-Boolean functions without explicitly stating it. Therefore, we can think of the Walsh transform of a Boolean function f as if it is the Fourier transform of the pseudo-Boolean function $(-1)^{f(x)}$. That being the case, from the fact that $(-1)^{f(x)} = 1 - 2f(x)$, we deduce (using Proposition 2.0.2) the following relation between the two transforms:

$$W_f(w) = \begin{cases} -2\widehat{f}(w), & w \neq 0_n \\ 2^n - 2\widehat{f}(w), & w = 0_n. \end{cases} \tag{2.6}$$

For example, the transforms of the functions f and g given in Table 2.1 are:

w	$W_f(w)$	$\widehat{f}(w)$
(0, 0, 0, 0)	0	8
(1, 0, 0, 0)	16	-8
(0, 1, 0, 0)	0	0
(1, 1, 0, 0)	0	0
(0, 0, 1, 0)	0	0
(1, 0, 1, 0)	0	0
(0, 1, 1, 0)	0	0
(1, 1, 1, 0)	0	0
(0, 0, 0, 1)	0	0
(1, 0, 0, 1)	0	0
(0, 1, 0, 1)	0	0
(1, 1, 0, 1)	0	0
(0, 0, 1, 1)	0	0
(1, 0, 1, 1)	0	0
(0, 1, 1, 1)	0	0
(1, 1, 1, 1)	0	0

w	$W_g(w)$	$\widehat{g}(w)$
(0, 0, 0, 0)	4	6
(1, 0, 0, 0)	4	-2
(0, 1, 0, 0)	4	-2
(1, 1, 0, 0)	-4	2
(0, 0, 1, 0)	4	-2
(1, 0, 1, 0)	4	-2
(0, 1, 1, 0)	4	-2
(1, 1, 1, 0)	-4	2
(0, 0, 0, 1)	4	-2
(1, 0, 0, 1)	4	-2
(0, 1, 0, 1)	4	-2
(1, 1, 0, 1)	-4	2
(0, 0, 1, 1)	-4	2
(1, 0, 1, 1)	-4	2
(0, 1, 1, 1)	-4	2
(1, 1, 1, 1)	4	-2

Table 2.3: Walsh and Fourier transforms of f and g from Table 2.1

Notice that there is a degree of uniformity in the Walsh transforms of f and g. For f, we have only one nonzero Walsh coefficient, and that is because f is an affine function. We can deduce that from the following, slightly more general proposition (for example, stated as Proposition 10 in [12]) about the Fourier transforms of the

indicators of vector subspaces of $\mathbb{F}_2^n$. Before we state the proposition, we need some notation. Let S be a subset of $\mathbb{F}_2^n$. By $\mathbb{1}_S$ we denote *the indicator* of S, that is, the Boolean function such that $\mathbb{1}_S(x) = 1$ if $x \in S$ and $\mathbb{1}_S(x) = 0$ if $x \in \mathbb{F}_2^n \setminus S$. However, when $S = \{0_n\}$, we denote the indicator $\mathbb{1}_{\{0_n\}}$ by δ_0, and when $S = \mathbb{F}_2^n$, we denote $\mathbb{1}_{\mathbb{F}_2^n}$ simply by 1. By $S^\perp$ we denote *the orthogonal complement* of S, with respect to the standard scalar product on $\mathbb{F}_2^n$, that is, the set $S^\perp = \{x \in \mathbb{F}_2^n : x \cdot y = 0 \text{ for all } y \in S\}$.

Proposition 2.0.2 *Let E be any vector subspace of $\mathbb{F}_2^n$. Then:*

$$\widehat{\mathbb{1}_E} = |E|\mathbb{1}_{E^\perp}. \tag{2.7}$$

In particular, $\widehat{1} = 2^n\delta_0$.

On the other hand, the absolute value of the Walsh coefficients of g is constant (Table 2.3), and that is because g belongs to a class of Boolean functions called bent functions. We will define and say more about bent functions in the next section. However, in general, the Walsh transform of a Boolean function does not have to be so uniform. For example, the following (Table 2.4) is the Walsh transform of the Boolean function $h(x_1, x_2, x_3, x_4) = x_1x_2x_3x_4 + x_1x_4 + x_4$.

w	$W_h(w)$
(0, 0, 0, 0)	6
(1, 0, 0, 0)	-6
(0, 1, 0, 0)	2
(1, 1, 0, 0)	-2
(0, 0, 1, 0)	2
(1, 0, 1, 0)	-2
(0, 1, 1, 0)	-2
(1, 1, 1, 0)	2
(0, 0, 0, 1)	10
(1, 0, 0, 1)	6
(0, 1, 0, 1)	-2
(1, 1, 0, 1)	2
(0, 0, 1, 1)	-2
(1, 0, 1, 1)	2
(0, 1, 1, 1)	2
(1, 1, 1, 1)	-2

Table 2.4: Walsh transform of $h = x_1x_2x_3x_4 + x_1x_4 + x_4$.

Proposition 2.0.2, although simple looking, can be used to reveal some more subtle connections between the Fourier coefficients. The following, fairly general version of the *Poisson summation formula*, can be deduced from Proposition 2.0.2 and the fact that the Fourier transform of a pseudo-Boolean function of the form $f(x) = (-1)^{a\cdot x}\varphi(x + b)$, where φ is an arbitrary pseudo-Boolean function, is the function $\widehat{f}(w) = (-1)^{b\cdot(a+w)}\widehat{\varphi}(a + w)$.

Corollary 2.0.3 (Poisson summation formula) *For every pseudo-Boolean function φ on $\mathbb{F}_2^n$, for every vector subspace E of $\mathbb{F}_2^n$, and for every $a, b \in \mathbb{F}_2^n$, we have:*

$$\sum_{u \in a+E} (-1)^{b \cdot u} \widehat{\varphi}(u) = |E|(-1)^{a \cdot b} \sum_{x \in b+E^{\perp}} (-1)^{a \cdot x} \varphi(x). \tag{2.8}$$

From the Poisson summation formula, setting $a = 0_n$ and $E = \mathbb{F}_2^n$, we deduce the Fourier inversion formula for the Fourier transform of pseudo-Boolean functions.

Corollary 2.0.4 *For every pseudo-Boolean function φ on $\mathbb{F}_2^n$:*

$$\widehat{\widehat{\varphi}} = 2^n \varphi.$$

Proposition 2.0.2 can also be used to prove the following version of *Parseval's relation* for pseudo-Boolean functions.

Corollary 2.0.5 *For every pseudo-Boolean function φ on $\mathbb{F}_2^n$:*

$$\sum_{w \in \mathbb{F}_2^n} \widehat{\varphi}^2(w) = 2^n \sum_{x \in \mathbb{F}_2^n} \varphi^2(x).$$

In particular, for every Boolean function f on $\mathbb{F}_2^n$:

$$\sum_{w \in \mathbb{F}_2^n} W_f^2(w) = 2^{2n}.$$

To illustrate, for f and g in Table 2.1, we have $\sum_{w \in \mathbb{F}_2^n} W_f^2(w) = 16^2 = 256 = 2^{2 \cdot 4}$, and $\sum_{w \in \mathbb{F}_2^n} W_g^2(w) = 16 \cdot (\pm 4)^2 = 256$, and similarly for h in Table 2.4 we have $\sum_{w \in \mathbb{F}_2^n} W_h^2(w) = 12 \cdot (\pm 2)^2 + 3 \cdot (\pm 6)^2 + 10^2 = 48 + 108 + 100 = 256$.

2.1 Bent Functions

In this section, we state the definitions and results related to bent functions, which will be used throughout the thesis. For a much more detailed exposition we refer to [48].

There are various different, but equivalent, definitions of bent functions. We will start with the most intuitive definition, which is related to nonlinearity.

The *nonlinearity* of a Boolean function f (denoted by $nl(f)$) is the minimum Hamming distance between f and the set of affine functions (in the same number of variables). The nonlinearity of a function can be computed from the Walsh transform of the function. Let f be a Boolean function in n variables. For $a = (a_1, \ldots, a_n) \in \mathbb{F}_2^n$ denote by l_a the linear function $l_a(x) = a \cdot x = a_1 x_1 + \cdots + a_n x_n$, for all $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$. We have:

$$\begin{aligned} W_f(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+x \cdot a} &= |\{x \in \mathbb{F}_2^n : f(x) = l_a(x)\}| - |\{x \in \mathbb{F}_2^n : f(x) \neq l_a(x)\}| \\ &= 2^n - 2|\{x \in \mathbb{F}_2^n : f(x) \neq l_a(x)\}| = 2^n - 2d(f, l_a), \end{aligned}$$

hence $d(f, l_a) = 2^{n-1} - \frac{1}{2}W_f(a)$. Similarly, $d(f, l_a + 1) = 2^{n-1} + \frac{1}{2}W_f(a)$, so we conclude that the nonlinearity and the Walsh transform of a Boolean function in n variables are related as follows:

$$nl(f) = 2^{n-1} - \frac{1}{2}\max_{a\in\mathbb{F}_2^n}|W_f(a)|. \tag{2.9}$$

Parseval's relation (Corollary 2.0.5) states that for any Boolean function f in n variables $\sum_{w\in\mathbb{F}_2^n} W_f^2(w) = 2^{2n}$, therefore there has to be at least one $a \in \mathbb{F}_2^n$ such that $|W_f(a)| \geq 2^{\frac{n}{2}}$. Combining that with (2.9), we deduce the following bound for the nonlinearity of an n-variable Boolean function:

$$nl(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}. \tag{2.10}$$

A Boolean function f in n variables is called *bent* if its nonlinearity equals $nl(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$. In other words, bent functions are the Boolean functions which are as nonlinear as possible. As mentioned, from Parseval's relation, we know that there is at least one $a \in \mathbb{F}_2^n$ such that $|W_f(a)| \geq 2^{\frac{n}{2}}$, so combining that with the definition of bent functions and (2.9), we deduce the following: f is a bent function in n variables if and only $W_f(w) = \pm 2^{\frac{n}{2}}$ for all $w \in \mathbb{F}_2^n$.

From the definition of bent functions, we immediately deduce that there are no bent functions if the number of variables is odd, since in that case $2^{n-1} - 2^{\frac{n}{2}-1}$ is not an integer. On the other hand, for every even n, there are bent functions in n variables. We will discuss the existence of bent functions in more detail in the next section.

A different characterization of bent functions can be achieved via derivatives. The *derivative* of an n-variable Boolean function f at $a \in \mathbb{F}_2^n$ (or in the direction of a), denoted by $D_a f$, is the Boolean function defined by

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

and the k-th order derivative of f at $v_1, v_2, \ldots, v_k \in \mathbb{F}_2^n$, denoted $D_{v_1}D_{v_2}\ldots D_{v_k}f$, is the Boolean function defined recursively by

$$D_{v_1}D_{v_2}\ldots D_{v_k}f(x) = D_{v_1}(D_{v_2}\ldots D_{v_k}f)(x), \text{ for all } x \in \mathbb{F}_2^n.$$

For example, the explicit form of the second order derivative of f at $a, b \in \mathbb{F}_2^n$ is

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

To obtain a connection between the Walsh coefficients of a Boolean function and its derivatives, we square the Walsh coefficients to get

$$W_f(a)^2 = \left(\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+x\cdot a}\right)\left(\sum_{y\in\mathbb{F}_2^n}(-1)^{f(y)+y\cdot a}\right) = \sum_{x,y\in\mathbb{F}_2^n}(-1)^{f(x)+f(y)+(x+y)\cdot a}$$
$$= \sum_{x,v\in\mathbb{F}_2^n}(-1)^{f(x)+f(x+v)+v\cdot a} = \sum_{v\in\mathbb{F}_2^n}\left(\sum_{x\in\mathbb{F}_2^n}(-1)^{D_v f(x)}\right)(-1)^{v\cdot a}.$$

Denoting by s_f the pseudo-Boolean function in n variables defined by

$$s_f(v) = \sum_{x \in \mathbb{F}_2^n} (-1)^{D_v f(x)} \text{ for all } v \in \mathbb{F}_2^n,$$

it follows that

$$W_f(a)^2 = \sum_{v \in \mathbb{F}_2^n} s_f(v)(-1)^{v \cdot a} = \widehat{s_f}(a).$$

Combining Proposition 2.0.2 with the Fourier inversion formula, we deduce that when f is a bent function, since $W_f(a)^2$ is constant, then $\widehat{s_f}(a)$ is constant, therefore $s_f(v) = 0$ for all $v \neq 0_n$. Similarly, if $s_f(v) = 0$ for all $v \neq 0_n$, then $\widehat{s_f}(a)$, and hence $W_f(a)^2$ is constant, therefore f is bent. Moreover, $s_f(v) = \sum_{x \in \mathbb{F}_2^n} (-1)^{D_v f(x)} = 0$ if and only if $\mathrm{wt}(D_v f) = 2^{n-1}$. A Boolean function h in n variables is called *balanced* if $\mathrm{wt}(h) = 2^{n-1}$. Therefore, we obtain the following characterization of bent functions: f is bent if and only if $D_v f$ is balanced for all $v \in \mathbb{F}_2^n \setminus \{0_n\}$.

An important fact about derivatives, which we will use throughout the thesis, is the following lemma about the algebraic degrees of the second order derivatives of δ_0.

Lemma 2.1.1 *For any two distinct nonzero vectors $a, b \in \mathbb{F}_2^n$, the algebraic degree of $D_a D_b \delta_0$ is $n - 2$.*

Lemma 2.1.1 follows from Theorem 2.0.1, because the weight of $D_a D_b \delta_0$ is $4 = 2^2$, hence its algebraic degree is at least $n - 2$. But it is also at most $n - 2$, hence it is exactly $n - 2$. On the other hand, if $a = b$, or if one of them is the zero vector, then $D_a D_b \delta_0 = 0$.

Another important notion related to derivatives is the notion of a linear structure. A vector $a \in \mathbb{F}_2^n$ is a *linear structure* of a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ if there exists a constant $c \in \mathbb{F}_2$, such that $D_a f(x) = f(x + a) + f(x) = c$ for every $x \in \mathbb{F}_2^n$. The trivial case, $a = (0, 0, \ldots, 0)$, the zero vector in $\mathbb{F}_2^n$, is a linear structure of every Boolean function. It is easy to see that the set of linear structures of a Boolean function is always a vector subspace of $\mathbb{F}_2^n$.

For vectorial Boolean functions, we define their derivatives in the same way (with the same formulas) as in the Boolean case. A vectorial Boolean function $G : \mathbb{F}_2^n \to \mathbb{F}_2^k$ is called *balanced* if its output distribution is uniformly distributed (for $k \leq n$), that is, if it takes every value of $\mathbb{F}_2^k$ the same number of times (precisely, 2^{n-k} times). We can use the characterization of bent functions via derivatives to generalize the notion in the vectorial case.

A *vectorial* Boolean function $F : \mathbb{F}_2^n \to \mathbb{F}_2^k$ is called *bent* if $D_v F$ is balanced for all $v \in \mathbb{F}_2^n \setminus \{0_n\}$. Equivalently, F is bent if its component functions $v \cdot F$ are bent for all $v \in \mathbb{F}_2^k \setminus \{0_k\}$. The equivalence of the two definitions follows from the fact that a vectorial Boolean function $G : \mathbb{F}_2^n \to \mathbb{F}_2^k$ is balanced if and only if its component functions $v \cdot G$ are balanced for all $v \in \mathbb{F}_2^k \setminus \{0_k\}$ (for example, this is stated as Proposition 35 in [12]). Alternatively, we can also define bent functions using the generalized version of the Walsh transform for vectorial Boolean functions.

The *Walsh transform* (or sometimes Walsh-Hadamard transform) of a *vectorial* Boolean function $F : \mathbb{F}_2^n \to \mathbb{F}_2^k$ is the mapping $W_F : \mathbb{F}_2^n \times \mathbb{F}_2^k \to \mathbb{Z}$, defined by:

$$W_F(w, v) = \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot F(x) + x \cdot w}, \text{ for every } (w, v) \in \mathbb{F}_2^n \times \mathbb{F}_2^k. \tag{2.11}$$

Using this definition, we get that a vectorial Boolean function $F : \mathbb{F}_2^n \to \mathbb{F}_2^k$ is bent if and only is $W_F(w, v) = \pm 2^{\frac{n}{2}}$, for every $w \in \mathbb{F}_2^n$ and $v \in \mathbb{F}_2^k \setminus \{0_k\}$.

Using the Walsh coefficients of an arbitrary Boolean bent function, we can define another Boolean bent function, called its dual, in the following way. For a Boolean bent function f in n variables, *the dual function* of f, denoted by f^* (notation $\tilde{f}$ is also common) is the Boolean function in n variables defined by

$$W_f(w) = 2^{\frac{n}{2}} (-1)^{f^*(w)}, \text{ for all } w \in \mathbb{F}_2^n. \tag{2.12}$$

From the Fourier inversion formula (Corollary 2.0.4) we deduce that the dual f^* of any bent function f is also bent, and that its own dual is f itself, that is $(f^*)^* = f$.

Combining the Poisson summation formula (Corollary 2.0.3) for the pseudo-Boolean function $(-1)^{f(x)}$ and $a = b = 0_n$, with the notion of dual function, we get:

$$2^{\frac{n}{2}} \sum_{u \in E} (-1)^{f^*(u)} = |E| \sum_{x \in E^\perp} (-1)^{f(x)} \Rightarrow$$
$$\frac{2^{\frac{n}{2}}}{|E|} \sum_{u \in E} (-1)^{f^*(u)} = |E^\perp| - 2 \sum_{x \in E^\perp} f(x).$$

Now, in combination with the formula for the coefficients of the algebraic normal form of f (2.2), we get that the algebraic degree of an arbitrary bent function in n variables is always less than or equal to $\frac{n}{2}$. (When $\dim(E^\perp) = \frac{n}{2} + 1$, we use the fact that $\sum_{u \in E} (-1)^{f^*(u)}$ is even, which is deduced in the same manner as (2.9).)

We can use similar ideas with the Walsh transform of vectorial Boolean functions to prove that vectorial bent functions from $\mathbb{F}_2^n$ into $\mathbb{F}_2^k$ can exist only if $k \leq n/2$. This is known as *Nyberg's bound* [50]. We can prove it as follows. Assume that $F : \mathbb{F}_2^n \to \mathbb{F}_2^k$ is a vectorial bent function. Then, for every $v \in \mathbb{F}_2^k \setminus \{0_k\}$, we have $W_F(0_n, v) = \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot F(x)} = (-1)^{(v \cdot F)^*(0_n)} 2^{\frac{n}{2}}$, because every nonzero component of F is a bent function. Proposition 2.0.2 implies that

$$\sum_{x \in \mathbb{F}_2^n} \sum_{v \in \mathbb{F}_2^k} (-1)^{v \cdot F(x)} = 2^k |F^{-1}(0_k)|, \text{ and therefore}$$

$$2^k |F^{-1}(0_k)| = 2^n + 2^{\frac{n}{2}} \sum_{v \in \mathbb{F}_2^k \setminus \{0_k\}} (-1)^{(v \cdot F)^*(0_n)}.$$

The sum $\sum_{v \in \mathbb{F}_2^k \setminus \{0_k\}} (-1)^{(v \cdot F)^*(0_n)}$ is odd (since $|v \in \mathbb{F}_2^k \setminus \{0_k\}|$ is an odd integer), and because $2^{\frac{n}{2}} \sum_{v \in \mathbb{F}_2^k \setminus \{0_k\}} (-1)^{(v \cdot F)^*(0_n)}$ needs to be divisible by 2^k (assuming $k \leq n$, which we can assume without loss of generality just by discarding a sufficient number of coordinate functions of F), we conclude that $k \leq \frac{n}{2}$.

2.2 Classes of Bent functions

In this section, we introduce the classes of bent functions which we will use and study throughout the thesis. The concept of affine equivalence will be an important part of our investigation. Two Boolean functions in n variables, f and g, are said to be *affine equivalent* if there exist a linear isomorphism $L : \mathbb{F}_2^n \to \mathbb{F}_2^n$, a linear function $l : \mathbb{F}_2^n \to \mathbb{F}_2$, $a \in \mathbb{F}_2^n$, and $b \in \mathbb{F}_2$ such that $f(x) = g(L(x) + a) + l(x) + b$, for all $x \in \mathbb{F}_2^n$. A lot of the important cryptographic properties remain unchanged under the affine equivalence. For example, if f is bent and g is affine equivalent to f, then, since the distance from the set of all affine functions remains unchanged under the transformation, g is also bent.

A *class* of Boolean/bent functions is a set of Boolean/bent functions, usually sharing the the same defining property or form. A class of bent functions is *complete* if it is globally invariant under the affine equivalence. More precisely, a class of bent functions B is complete if for every $f \in B$ all the functions affine equivalent to f are also in B. The *completed class* of a class of bent functions B, denoted by $B^{\#}$, is the smallest complete class containing B.

Constructions of bent functions are split into two groups: primary constructions (constructions which do not require other bent functions in order to construct new ones), and secondary constructions (constructions utilising other bent functions to construct new ones).

One of the first primary constructions of bent functions was described in 1973 by J. A. Maiorana and R. L. McFarland (independently). The construction was actually a construction of a class of difference sets in certain non-cyclic groups, but it translates to an equivalent construction of bent functions, as described in [21].

The *Maiorana-McFarland class* $\mathcal{M}$ is the set of m-variable ($m = 2n$) Boolean functions of the form

$$f(x, y) = x \cdot \pi(y) + g(y), \text{ for all } x, y \in \mathbb{F}_2^n,$$

where π is a permutation of $\mathbb{F}_2^n$, and g is an arbitrary Boolean function on $\mathbb{F}_2^n$.

Alternatively, we can describe the Maiorana-McFarland class in terms of finite fields as the set of all functions of the form

$$f(x, y) = Tr(x\pi(y)) + g(y), \text{ for all } x, y \in \mathbb{F}_{2^n},$$

where π is a permutation of $\mathbb{F}_{2^n}$, and g is any function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$.

Proposition 2.0.2 can be used to show that every function in the Maiorana-McFarland class is bent, and that the dual of $f(x, y) = x \cdot \pi(y) + g(y)$ is $f^*(x, y) = y \cdot \pi^{-1}(x) + g(\pi^{-1}(x))$.

A useful indicator for the purpose of establishing whether a given bent function belongs to the completed Maiorana-McFarland class $\mathcal{M}^{\#}$ can be obtained using the second order derivatives of the function.

Lemma 2.2.1 *([21, p.102], [12, Proposition 54]) 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, for all $\alpha, \beta \in V$,*

$$D_\alpha D_\beta f(x) = f(x) + f(x + \alpha) + f(x + \beta) + f(x + \alpha + \beta) = 0, \text{ for all } x \in \mathbb{F}_2^m.$$

In [9], C. Carlet derived two new (secondary) classes of bent functions, called $\mathcal{C}$ and $\mathcal{D}$, from the Maiorana-McFarland class.
The *class* $\mathcal{C}$ is the set of all Boolean functions of the form

$$f(x,y) = x \cdot \pi(y) + \mathbb{1}_{L^\perp}(x), \tag{2.13}$$

where L is any linear subspace of $\mathbb{F}_2^n$, $\mathbb{1}_{L^\perp}$ is the indicator function of the space $L^\perp$, and π is any permutation of $\mathbb{F}_2^n$ such that:

$$(C) \quad \phi(a+L) \text{ is an affine subspace, for all } a \in \mathbb{F}_2^n, \text{ where } \phi := \pi^{-1}.$$

The permutation ϕ and the subspace L are then said to satisfy the (C) property, or for short (ϕ, L) *has property* (C).
The class $\mathcal{D}$, defined similarly as $\mathcal{C}$, is the set of all Boolean functions of the form

$$f(x,y) = x \cdot \pi(y) + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y), \tag{2.14}$$

where π is a permutation of $\mathbb{F}_2^n$ and E_1, E_2 two linear subspaces of $\mathbb{F}_2^n$ such that $\pi(E_2) = E_1^\perp$. The permutation π and the subspaces E_1, E_2 are then said to satisfy the (D) property, or for short (π, E_1, E_2) *has property* (D).

A special subclass of the classes $\mathcal{C}$ and $\mathcal{D}$ is the subclass $\mathcal{D}_0$. It contains all functions of the form

$$f(x,y) = x \cdot \pi(y) + \delta_0(x),$$

where $\delta_0(x) = \prod_{i=1}^n (x_i + 1)$ so that it corresponds to the case $E_1 \times E_2 = \{0_n\} \times \mathbb{F}_2^n$.

It is proved in [9], by analyzing the duals of the building functions from $\mathcal{M}$, that every function in the classes $\mathcal{C}$ and $\mathcal{D}$ is bent, and additionally, that there are functions in the class $\mathcal{D}_0$ which are not in the completed Maiorana-McFarland class.

In 1974 J. Dillon in his PhD thesis [21] introduced another primary class of bent functions called *Partial Spread class*, denoted by $\mathcal{PS}$. The construction uses the sums (modulo 2) of the indicators of an appropriate number of $n/2$-dimensional subspaces of $\mathbb{F}_2^n$ to define the functions in the class. According to the number of the subspaces used, the class $\mathcal{PS}$ is divided into two subclasses called $\mathcal{PS}^-$ and $\mathcal{PS}^+$. The class $\mathcal{PS}^-$ is the set of all the sums (modulo 2) of the indicators of $2^{n/2-1}$ pairwise "disjoint" $n/2$-dimensional subspaces of $\mathbb{F}_2^n$ ("disjoint" meaning that their intersection is only the zero vector 0_n). Similarly, the class $\mathcal{PS}^+$ is the set of all the sums (modulo 2) of the indicators of $2^{n/2-1}+1$ pairwise "disjoint" $n/2$-dimensional subspaces of $\mathbb{F}_2^n$.

Every function in the Partial Spread class is bent. The degree of any n-variable function f in $\mathcal{PS}^-$ is always equal to $n/2$, but this does not have to be the case for the functions in $\mathcal{PS}^+$ whose degree may be less than $n/2$. The characterization of the algebraic normal forms of the bent functions in the $\mathcal{PS}$ class appears to be hard, and is still an open problem.

In general, it is not an easy task to construct elements of the Partial Spread class practically, that is, it is not a simple matter to find the appropriate number of "disjoint" $n/2$-dimensional subspaces effectively. Nevertheless, J. Dillon in [21] exhibits one explicit subclass of the $\mathcal{PS}^-$ class, denoted by $\mathcal{PS}_{ap}$. The class $\mathcal{PS}_{ap}$ is the set of all Boolean functions $f : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \to \mathbb{F}_2$ of the form

$$f(x,y) = g(xy^{2^n-2}), \text{ for all } x, y \in \mathbb{F}_{2^n},$$

where $g : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is any balanced Boolean function such that $g(0) = 0$.

Using Lemma 2.2.1, J. Dillon in [21] proved that there are functions in the class $\mathcal{PS}_{ap}$ which do not belong to the completed Maiorana-McFarland class. On the other hand, C. Carlet in [9] proved that there are functions in the Maiorana-McFarland class and in the class $\mathcal{D}_0$ (hence in $\mathcal{C}$ and $\mathcal{D}$ as well), which do not belong to the completed Partial Spread class.

For vectorial bent functions, the question of class membership is a bit more vague. In order to make it more precise, in Chapter 6 we introduce the notion of vectorial bent functions *weakly* and *strongly* outside of a class of bent functions. For completeness, we state the definition here as well.

Definition 2.2.2 *A vectorial bent function $F : \mathbb{F}_2^{2n} \to \mathbb{F}_2^k$, with $k \leq n$, is* weakly outside *of a class of bent functions if there is at least one (nonzero) component function of F (linear combination of its coordinate functions) which does not belong to the considered class. If all component functions of F do not belong to a class of bent functions then F is* strongly outside *the considered class.*

2.3 Negabent functions

C. Riera and M. Parker in [61] introduced the class of negabent functions, motivated by applications to quantum computing. A Boolean function f in n variables, is called *negabent* if $|\mathcal{N}_f(u)| = 2^{n/2}$ for all $u \in \mathbb{F}_2^n$, where $\mathcal{N}_f$ is the complex-valued function $\mathcal{N}_f \colon \mathbb{F}_2^n \to \mathbb{C}$ defined by

$$\mathcal{N}_f(u) = \sum_{x \in \mathbb{F}_2^n} i^{wt(x)} (-1)^{f(x)+u\cdot x}, \text{ for all } u \in \mathbb{F}_2^n, \tag{2.15}$$

called the *nega-Hadamard transform* of f. As standard, in the equation (2.15) the symbol i denotes the imaginary unit, i.e., $i^2 = -1$.

With the following result, one can verify the negabent property of a given Boolean function f on $\mathbb{F}_2^n$ without the use of the nega-Hadamard transform.

Lemma 2.3.1 *[53] Let n be even and $f \colon \mathbb{F}_2^n \to \mathbb{F}_2$. Then, f is negabent if and only if $f + s_2$ is bent, where $s_2 \colon \mathbb{F}_2^n \to \mathbb{F}_2$ is the elementary symmetric quadratic Boolean function, i.e.,*

$$s_2(x) = \sum_{1 \leq i < j \leq n} x_i x_j, \quad \text{for } x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n.$$

For an even number of variables, a function is called *bent–negabent* if it is both bent and negabent.

An important notion, upon which most of our constructions of vectorial bent-negabent functions will be based, is the notion of complete mappings. A mapping $F \colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is called *complete* if both $x \mapsto F(x)$ and $x \mapsto F(x) + x$ permute $\mathbb{F}_{2^n}$.

2.4 Correlation immune and Resilient functions

Correlation immune functions (CI) were defined by T. Siegenthaler [67] in 1984, in order to investigate and improve resistance of stream ciphers against correlation attacks. An n-variable Boolean function f is called *correlation immune* of order d (in brief, d-CI) if the output distribution of f does not change when at most d input variables are fixed. However, throughout the thesis we will use a characterisation of correlation immunity (see [73]), which is slightly more intuitive and easier to use. In order to state the characterization, we need the concept of a subfunction. A *subfunction* of order d, $0 < d \leq n$, of a Boolean function f in variables $x_1, \ldots, x_n$ is a Boolean function in $n - d$ variables, denoted by $f_{i_1,\ldots,i_d}^{a_1,\ldots,a_d}$, obtained from f by fixing each variable x_{i_j} to be some value $a_{i_j} \in \{0, 1\}$, for $j = 1, \ldots, d$.

Proposition 2.4.1 *A function $f(x)$ in n variables is correlation immune of order d if and only if the Hamming weight of every subfunction of f of order d equals* $\mathrm{wt}(f)/2^d$.

A Boolean function f in n variables is called *resilient* of order d if it is d-CI and if it is balanced (i.e. $\mathrm{wt}(f) = 2^{n-1}$). G. Z. Xiao and J. L. Massey in [81] gave the following characterisation of correlation immune and resilient functions in terms of their Walsh-Hadamard transform:

Theorem 2.4.2 *[81] An n-variable Boolean function f is correlation immune (resp. resilient) of order d if and only if $W_f(w) = 0$ for every $w \in \mathbb{F}_2^n$ satisfying $1 \leq \mathrm{wt}(w) \leq d$; (resp. $0 \leq \mathrm{wt}(w) \leq d$).*

The bound of Siegenthaler states that the algebraic degree of any n-variable resilient function of order d is at most $n-d-1$, and that the algebraic degree of any n-variable correlation immune function of order d is at most $n - d$.

Chapter 3

Characterization of the intersection of the class $\mathcal{D}_0$ and the completed Maiorana-McFarland class

In the 1990s, C. Carlet (in [9]) provided two new secondary constructions of bent functions using bent functions from the Maiorana-McFarland class and adding indicators of appropriately chosen vector subspaces. The classes of bent functions obtained by the constructions are called $\mathcal{C}$ and $\mathcal{D}$. A particular subclass of both $\mathcal{C}$ and $\mathcal{D}$, called $\mathcal{D}_0$, is singled out in [9] because of a simpler form of the subspaces used and for the ease of construction. It is established in [9] that there are functions in the class $\mathcal{D}_0$ which are not affine equivalent to any function in the class $\mathcal{M}$, as well as that there are some functions in $\mathcal{D}_0$ which are not affine equivalent to any function in the class $\mathcal{PS}$.

The main purpose of this chapter is to provide a more accurate description (in terms of the class membership) of the secondary class $\mathcal{D}_0$. Carlet in [9, Proposition 2] provided a sufficient condition for bent functions in the class $\mathcal{D}_0$ (which are of the form $f(x, y) = x \cdot \pi(y) + \delta_0(x)$, where $x, y \in \mathbb{F}_2^n$, π is a permutation of $\mathbb{F}_2^n$ and $\delta_0(x)$ is the indicator of the subspace $\{0_n\} \times \mathbb{F}_2^n$), to be outside $\mathcal{M}^\#$. Namely, if the permutation π is not affine on any linear hyperplane of $\mathbb{F}_2^n$ (i.e. $(n-1)$-dimensional subspace of $\mathbb{F}_2^n$), then f is outside $\mathcal{M}^\#$. We prove that when the degree of a permutation π is greater than 2 the Boolean function $f(x, y) = x \cdot \pi(y) + \delta_0(x)$, with $f : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2$, is always outside $\mathcal{M}^\#$ class (regardless of the fact whether π is affine on some hyperplane or not). On the other hand, we prove that the sufficient condition of Carlet is also necessary when $\deg(\pi) = 2$. Lastly, when the algebraic degree of the permutation π is equal to 1, the function f is obviously in the completed Maiorana-McFarland class. This means that we will cover all the possible cases, and hence completely characterize $\mathcal{D}_0 \cap \mathcal{M}^\#$.

The chapter is divided into two sections, depending on the algebraic degree of the permutation π used to define the bent function $f(x, y) = x \cdot \pi(y) + \delta_0(x)$.

3.1 Permutations with the algebraic degree greater than two

In order to achieve the characterization of $\mathcal{D}_0 \cap \mathcal{M}^{\#}$, we first need to study some properties of the second order derivatives of f. The following lemma provides a connection between the vanishing property of second order derivatives and the algebraic degree of the function.

Lemma 3.1.1 *Let g be a Boolean function in n variables. If there exists an $(n-k)$ dimensional subspace H of $\mathbb{F}_2^n$, such that $D_aD_bg = 0$ for all $a, b \in H$, then the algebraic degree of g is at most $k+1$.*

Proof. First note that, without loss of generality, we can assume that $H = \{0_k\} \times \mathbb{F}_2^{n-k}$. Otherwise, we can consider the function $h = g \circ A$, where A is a linear permutation of $\mathbb{F}_2^n$ that maps $\{0_k\} \times \mathbb{F}_2^{n-k}$ to H. Then, h has the same degree as g and $D_aD_bh = 0$, for all $a, b \in \{0_k\} \times \mathbb{F}_2^{n-k}$. Hence, for the rest of the proof we assume that $H = \{0_k\} \times \mathbb{F}_2^{n-k}$.

Using the algebraic normal form of g, we can write g in the following form:

$$g(x) = \sum_{u \in \mathbb{F}_2^k} g_u(x_{k+1}, \ldots, x_n) x_1^{u_1} \cdots x_k^{u_k}, \ \ \forall x \in \mathbb{F}_2^n,$$

where g_u's are functions depending only on $x_{k+1}, \ldots, x_n$. If a and b are two vectors from $\{0_k\} \times \mathbb{F}_2^{n-k}$, then from $D_aD_bg = 0$, we have:

$$D_aD_bg(x) = \sum_{u \in \mathbb{F}_2^k} (D_aD_bg_u(x_{k+1}, \ldots, x_n)) x_1^{u_1} \cdots x_k^{u_k} = 0, \ \ \forall x \in \mathbb{F}_2^n.$$

Then, fixing an arbitrary $v \in \mathbb{F}_2^k$ and denoting by $\bar{x}, \bar{a}, \bar{b}$ the restriction to the last $(n-k)$ coordinates of x, a and b respectively, we have:

$$D_aD_bg(v_1 \ldots, v_k, x_{k+1}, \ldots, x_n) = \sum_{u \in \mathbb{F}_2^k} (D_{\bar{a}}D_{\bar{b}}g_u(\bar{x})) v_1^{u_1} \cdots v_k^{u_k} = \sum_{u \preceq v} D_{\bar{a}}D_{\bar{b}}g_u(\bar{x}) = 0,$$

for all $\bar{x} = (x_{k+1}, \ldots, x_n) \in \mathbb{F}_2^{n-k}$. Here, for $u, v \in \mathbb{F}_2^k$, the notation $u \preceq v$ means that $u_i \leq v_i$, for all $i = 1, \ldots, k$. Since v is arbitrary, using mathematical induction on the weight of v, we deduce that

$$D_{\bar{a}}D_{\bar{b}}g_u(\bar{x}) = g_u(\bar{x}) + g_u(\bar{x} + \bar{a}) + g_u(\bar{x} + \bar{b}) + g_u(\bar{x} + \bar{a} + \bar{b}) = 0, \ \ \forall \bar{x} \in \mathbb{F}_2^{n-k},$$

for all $u \in \mathbb{F}_2^k$. Setting $\bar{x} = 0_{n-k}$, we have

$$g_u(\bar{a} + \bar{b}) = g_u(\bar{a}) + g_u(\bar{b}) + g_u(0_{n-k}),$$

for all $\bar{a}, \bar{b} \in \mathbb{F}_2^{n-k}$. Hence, g_u is affine for all $u \in \mathbb{F}_2^k$, but then $\deg(g_u) \leq 1$, and so the algebraic degree of g is at most $k+1$. ∎

As an immediate corollary of Lemma 3.1.1, applying it to the coordinate functions of a vectorial Boolean function, we deduce the following vectorial version of it.

Corollary 3.1.2 *Let $G : \mathbb{F}_2^n \to \mathbb{F}_2^t$ be a vectorial Boolean function. If there exists an $(n-k)$-dimensional subspace H of $\mathbb{F}_2^n$ such that $D_aD_bG = 0$ for all $a, b \in H$, then the algebraic degree of G is at most $k+1$.*

Combining Corollary 3.1.2 and Lemma 2.2.1, we can prove that when the algebraic degree of a permutation π is greater than 2, then the function $x \cdot \pi(y) + \delta_0(x)$ from the class $\mathcal{D}_0$ is outside $\mathcal{M}^{\#}$.

Theorem 3.1.3 *Let n be an integer, $n \geq 4$. Let π be a permutation of $\mathbb{F}_2^n$ with the algebraic degree $\deg(\pi) \geq 3$. Then, the function $f : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2$ defined by $f(x, y) = x \cdot \pi(y) + \delta_0(x) \in \mathcal{D}_0$ is a bent function outside $\mathcal{M}^{\#}$.*

Proof. Assume that f is in the class $\mathcal{M}^{\#}$. Then, there exists an n-dimensional vector subspace V of $\mathbb{F}_2^n \times \mathbb{F}_2^n$ such that $D_aD_bf = 0$, for all $a, b \in V$. By Lemma 2.1.1, the degree of $D_aD_b\delta_0(x)$ is either $n-2$ or alternatively $D_aD_b\delta_0(x) = 0$. If the degree of $D_aD_b\delta_0(x)$ is $n-2 \geq 4-2 = 2$, then since $D_aD_b(x \cdot \pi(y))$ is at most linear with respect to x, we have $D_aD_bf \neq 0$. Since $D_aD_bf = 0$ for all $a, b \in V$, this implies that $D_aD_b\delta_0(x) = 0$, for all $a, b \in V$.

Now, denote by a_1 and b_1 the restriction of a and b to the first n coordinates, respectively. Again, by Lemma 2.1.1, if there exist $a, b \in V$ such that $a_1, b_1 \neq 0_n$ are nonzero and $a_1 \neq b_1$, then $D_aD_b\delta_0(x) = D_{a_1}D_{b_1}\delta_0(x) \neq 0$, which is a contradiction. This means that there is at most one nonzero $r \in \mathbb{F}_2^n$ such that $a_1 = r$ for some $a \in V$. Hence, there is at least an $(n-1)$-dimensional vector subspace V' of V such that it is also a subspace of $\{0_n\} \times \mathbb{F}_2^n$, i.e. there is an $(n-1)$-dimensional subspace H of $\mathbb{F}_2^n$ such that $V' = \{0_n\} \times H$. Since for all $a', b' \in V' = \{0_n\} \times H$, we have $D_{a'}D_{b'}x \cdot \pi(y) = x \cdot D_{a'}D_{b'}\pi(y) = 0$, we conclude that for all $v, w \in H$ we have $D_vD_w\pi(y) = 0$. From Corollary 3.1.2, we deduce that the algebraic degree of π is at most 2. ∎

3.2 Permutations with the algebraic degree equal to two

From Theorem 3.1.3, it follows that, in order to characterize $\mathcal{D}_0 \cap \mathcal{M}^{\#}$, we only have to characterize quadratic permutations π such that $x \cdot \pi(y) + \delta_0(x)$ is in the $\mathcal{M}^{\#}$ class. In order to provide such a characterization, we will use the following lemma.

Lemma 3.2.1 *Let $\pi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a permutation such that there is a linear hyperplane V of $\mathbb{F}_2^n$, on which π is affine. Let $l(x)$ be the linear Boolean function that defines V, that is, $l(x) = 0$ if and only if $x \in V$. Then, $l(x)$ or $l(x) + 1$ is a component function of π.*

Proof. Let A be a linear permutation of $\mathbb{F}_2^n$ that maps the subspace $\mathbb{F}_2^{n-1} \times \{0\}$ to V. Then, $l(Ax) = x_n$ for all $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$, and hence $\rho = \pi \circ A$ is affine on the hyperplane defined by $x_n = 0$ (that is $\mathbb{F}_2^{n-1} \times \{0\}$). From this, we deduce that we can write ρ in the form:

$$\rho(x) = L(x_1, \ldots, x_{n-1}) + x_nT(x_1, \ldots, x_{n-1}), \quad \forall x = (x, \ldots, x_n) \in \mathbb{F}_2^n,$$

where L and T are functions from $\mathbb{F}_2^{n-1}$ to $\mathbb{F}_2^n$, and L is affine.

Our goal now is to prove that ρ has x_n or $x_n + 1$ as a component function. Without loss of generality, we can assume that L is linear. Otherwise, we can consider $\rho(x) + \rho(0_n)$ since x_n or $x_n + 1$ is a component function of $\rho(x)$ if and only if x_n or $x_n + 1$ is a component function of $\rho(x) + \rho(0_n)$. Let us express L and T as

$$L(x_1, \ldots, x_{n-1}) = \begin{bmatrix} l_1(x_1, \ldots, x_{n-1}) \\ \vdots \\ l_n(x_1, \ldots, x_{n-1}) \end{bmatrix}, \text{ and } T(x_1, \ldots, x_{n-1}) = \begin{bmatrix} t_1(x_1, \ldots, x_{n-1}) \\ \vdots \\ t_n(x_1, \ldots, x_{n-1}) \end{bmatrix}.$$

The set $\{l_1(x_1, \ldots, x_{n-1}), \ldots, l_n(x_1, \ldots, x_{n-1})\}$ is a set of n linear Boolean functions in $(n-1)$ variables, hence it is linearly dependent. This means that there is a linear combination of them, i.e. a component function of L which is the constant 0 function. Without loss of generality, we can assume that $l_n(x_1, \ldots, x_{n-1}) = 0$, for all $(x_1, \ldots, x_{n-1}) \in \mathbb{F}_2^{n-1}$, otherwise we can consider $B \circ \rho$ for some linear permutation B of $\mathbb{F}_2^n$, because $B \circ \rho$ and ρ have the same component functions. Since π is a permutation, L is injective, and since $l_n = 0$, L maps $\mathbb{F}_2^{n-1}$ onto $\mathbb{F}_2^{n-1} \times \{0\}$.

Assume now that $t_n(a_1, \ldots, a_{n-1}) = 0$, for some $(a_1, \ldots, a_{n-1}) \in \mathbb{F}_2^{n-1}$. Then,

$$\rho(a_1, \ldots, a_{n-1}, 1) = L(a_1, \ldots, a_{n-1}) + T(a_1, \ldots, a_{n-1})$$

is in $\mathbb{F}_2^{n-1} \times \{0\}$. Because L maps $\mathbb{F}_2^{n-1}$ onto $\mathbb{F}_2^{n-1} \times \{0\}$, there is some $(b_1, \ldots, b_{n-1}) \in \mathbb{F}_2^{n-1}$ such that $L(b_1, \ldots, b_{n-1}) = L(a_1, \ldots, a_{n-1}) + T(a_1, \ldots, a_{n-1})$, but this would imply that $\rho(b_1, \ldots, b_{n-1}, 0) = \rho(a_1, \ldots, a_{n-1}, 1)$, and this is a contradiction, since ρ is a permutation. Hence, $t_n(x_1, \ldots, x_{n-1}) = 1$ for all $(x_1, \ldots, x_{n-1}) \in \mathbb{F}_2^{n-1}$, and so we have that $\rho_n(x_1, \ldots, x_{n-1}, x_n) = x_n$, for all $(x_1, \ldots, x_{n-1}, x_n) \in \mathbb{F}_2^n$. That is, x_n is a component function of $\rho = (\rho_1, \ldots, \rho_n)$. We conclude that $\rho_n \circ A^{-1}(x) = l(x)$ is a component function of $\rho \circ A^{-1} = \pi$. ∎

Using Lemma 3.2.1 we can now provide a characterization of the quadratic permutations π for which $x \cdot \pi(y) + \delta_0(x)$ is in the $\mathcal{M}^\#$ class.

Theorem 3.2.2 *Let π be a quadratic permutation of $\mathbb{F}_2^n$, $n \geq 4$. The function $f : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2$, defined by $f(x, y) = x \cdot \pi(y) + \delta_0(x)$, is in the class $\mathcal{M}^\#$ if and only if there is a linear hyperplane of $\mathbb{F}_2^n$ on which π is affine.*

Proof. First assume that f is in the $\mathcal{M}^\#$ class. Then, there is a subspace V of $\mathbb{F}_2^{2n}$, with $\dim(V) = n$, such that $D_a D_b f = 0$ for all $a, b \in V$. Similarly as in the proof of Theorem 3.1.3, we can deduce that there is an $(n-1)$-dimensional subspace H of V that is also a subspace of $\{0_n\} \times \mathbb{F}_2^n$. Let A be an invertible $n \times n$ matrix such that the $2n \times 2n$ matrix $M = \begin{bmatrix} I & 0 \\ 0 & A \end{bmatrix}$ maps $\{0_n\} \times \mathbb{F}_2^{n-1} \times \{0\}$ to H. Hence, M^{-1} maps the space V to an n-dimensional space V' so that $\{0_n\} \times \mathbb{F}_2^{n-1} \times \{0\}$ is a subspace of V'. Let v be the nonzero vector in V' such that $v_{n+1} = \ldots = v_{2n-1} = 0$. Then $V' = \langle v, e_{n+1}, \ldots, e_{2n-1} \rangle$. Set $\phi = \pi \circ A$. The function $f' = f \circ M$ is a bent function, also in $\mathcal{M}^\#$, such that for all $a, b \in V'$ we have $D_a D_b f' = 0$. Moreover, as in the proof of Theorem 3.1.3, we have that $D_a D_b (x \cdot \phi(y)) = 0$, for all $x, y \in \mathbb{F}_2^n$ and

all $a, b \in V'$. From this, we can deduce, similarly as in the proof of Lemma 3.1.1, that $\phi(y)$ is of the form:

$$\phi(y) = L(y_1, \ldots, y_{n-1}) + y_n T(y_1, \ldots, y_{n-1}), \ \ \forall y = (y_1, \ldots, y_n) \in \mathbb{F}_2^n,$$

where L and T are affine function from $\mathbb{F}_2^{n-1}$ to $\mathbb{F}_2^n$. From this, we deduce that ϕ is affine on the subspace $y_n = 0$, and hence π is also affine on a linear hyperplane of $\mathbb{F}_2^n$.

Now, assume that $\pi(y)$ is affine on a linear hyperplane of $\mathbb{F}_2^n$. After possibly adding a vector to π (which does not change the class membership of f to $\mathcal{M}^{\#}$), by Lemma 3.2.1, we have that $\pi(y)$ has a linear component function $l(y)$ such that the restriction of π to the hyperplane $l(y) = 0$ is affine. Without loss of generality, after possibly a linear transformation of variables, we can assume that the component function is $l(y) = y_n$. Similarly as in Lemma 3.1.1, using the fact that π is affine on $y_n = 0$ and that π is quadratic, we can write π in the form

$$\pi(y) = \begin{bmatrix} \pi_1(y_1, \ldots, y_{n-1}) + \pi_1'(y_1, \ldots, y_{n-1}) y_n \\ \vdots \\ \pi_n(y_1, \ldots, y_{n-1}) + \pi_n'(y_1, \ldots, y_{n-1}) y_n \end{bmatrix}$$

where π_i and π_i' are affine functions for all $i \in \{1, 2, \ldots, n\}$.

Since y_n is a component function of π, there is a subset S of $\{1, \ldots, n\}$ such that $\sum_{i \in S} (\pi_i(y_1, \ldots, y_{n-1}) + \pi_i'(y_1, \ldots, y_{n-1}) y_n) = y_n$. Define the vector $v \in \mathbb{F}_2^{2n}$ as the linear combination $v = \sum_{i \in S} \mathbb{e}_i$ and set $V = \langle v, \mathbb{e}_{n+1}, \ldots, \mathbb{e}_{2n-1} \rangle \subset \mathbb{F}_2^{2n}$. If $a, b \in \langle \mathbb{e}_{n+1}, \ldots, \mathbb{e}_{2n-1} \rangle$, we have

$$D_a D_b f(x, y) = \sum_{i=1}^{n} x_i (D_a D_b \pi_i(y_1, \ldots, y_{n-1}) + y_n D_a D_b \pi_i'(y_1, \ldots, y_{n-1})) = 0,$$

since π_i and π_i' are affine. On the other hand,

$$D_v(x \cdot \pi(y)) = \sum_{i=1}^{n} v_i (\pi_i(y_1, \ldots, y_{n-1}) + y_n \pi_i'(y_1, \ldots, y_{n-1})) = y_n,$$

by the definition of v, and so $D_a D_v f = 0$, for all $a \in V$. Consequently, we conclude that $D_a D_b f = 0$ for all $a, b \in V$, hence f belongs to $\mathcal{M}^{\#}$. ∎

As already mentioned, C. Carlet [9, Proposition 2] provided a sufficient condition for $f(x, y) = x \cdot \pi(y) + \delta_0(x)$ to be outside the $\mathcal{M}^{\#}$ class. More precisely, if there is no linear hyperplane on which π is affine, then $f \notin \mathcal{M}^{\#}$. In the case of quadratic permutation, this actually proves Theorem 3.2.2 in one direction. But Theorem 3.2.2 shows that in the case of quadratic permutations, the condition of Carlet is not only sufficient, but also necessary for f to be outside $\mathcal{M}^{\#}$. On the other hand, if π is not quadratic, from Theorem 3.1.3, we can deduce that the condition in [9, Proposition 2] is not necessary for f to be outside $\mathcal{M}^{\#}$.

Corollary 3.2.3 *Let L be an arbitrary affine permutation of $\mathbb{F}_2^{n-1}$, and let P be an arbitrary permutation of $\mathbb{F}_2^{n-1}$ with $\deg(P) \geq 2$. Let π be a permutation of $\mathbb{F}_2^n$ defined by*

$$\pi(y_1, \ldots, y_n) = (L(y_1, \ldots, y_{n-1}), 0) + y_n(P(y_1, \ldots, y_{n-1}) + L(y_1, \ldots, y_{n-1}), 1),$$

for all $(y_1, \ldots, y_n) \in \mathbb{F}_2^n$. Then, the function $f : \mathbb{F}_2^{2n} \to \mathbb{F}_2$ defined by $f(x, y) = x \cdot \pi(y) + \delta_0(x)$ is a bent function outside the class $\mathcal{M}^{\#}$. Furthermore, the restriction of π to the hyperplane $y_n = 0$ is affine.

Proof. The restriction of π to $y_n = 0$ is $(L(y_1, \ldots, y_{n-1}), 0)$, hence it is affine because L is affine. On the other hand, because $\deg(P) \geq 2$, then $\deg(\pi) \geq 3$, and so it follows from Theorem 3.1.3 that f is outside $\mathcal{M}^{\#}$. ∎

The following is an example of an explicit bent function in the $\mathcal{D}_0$ class for which we can use Corollary 3.2.3 to deduce that it is outside the $\mathcal{M}^{\#}$ class, but for which we are not able to use [9, Proposition 2] to conclude the same.

Example 1 *Let $n = 4$. We represent $\mathbb{F}_{2^3}$ as $\mathbb{F}_2(a)$, where $a^3 + a + 1 = 0$. Let $B = \{1, a, a^2\}$ be a basis of $\mathbb{F}_{2^3}$ over $\mathbb{F}_2$. We identify $\mathbb{F}_{2^3}$ and $\mathbb{F}_2^3$ via the isomorphism sending 1 in $\mathbb{F}_{2^3}$ to $(1, 0, 0)$ in $\mathbb{F}_2^3$, a to $(0, 1, 0)$, and a^2 to $(0, 0, 1)$. Set $L(t) = t$, and $P(t) = t^3$, for all $t \in \mathbb{F}_{2^3}$, in Corollary 3.2.3. Then, we get that the permutation π has the following form:*

$$\pi(y_1, y_2, y_3, y_4) = \begin{bmatrix} y_1 + y_2y_3y_4 + y_2y_4 + y_3y_4 \\ y_2 + y_1y_2y_4 + y_1y_3y_4 \\ y_3 + y_1y_2y_4 \\ y_4 \end{bmatrix},$$

for all $(y_1, y_2, y_3, y_4) \in \mathbb{F}_2^4$. The algebraic normal form of $f : \mathbb{F}_2^8 \to \mathbb{F}_2$ defined by $f(x, y) = x \cdot \pi(y) + \delta_0(x)$ is

$$f(x_0, \ldots, x_7) = x_0x_1x_2x_3 + x_0x_1x_2 + x_0x_1x_3 + x_0x_1 + x_0x_2x_3 + x_0x_2 + x_0x_3 + x_0x_4 + x_0x_5x_6x_7 + x_0x_5x_7 + x_0x_6x_7 + x_0 + x_1x_2x_3 + x_1x_2 + x_1x_3 + x_1x_4x_5x_7 + x_1x_4x_6x_7 + x_1x_5 + x_1 + x_2x_3 + x_2x_4x_5x_7 + x_2x_6 + x_2 + x_3x_7 + x_3 + 1.$$

Using Corollary 3.2.3, we deduce that f is outside the $\mathcal{M}^{\#}$ class. This has been additionally verified using the second order derivatives criterion of J. Dillon [21] (see also Lemma 2.2.1), implemented in Sage. *On the other hand, note that the restriction of π to the linear hyperplane $y_4 = 0$ is linear, hence we cannot deduce that f is outside $\mathcal{M}^{\#}$ from [9, Proposition 2].*

Chapter 4

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

This chapter focuses on the class membership problem for the secondary class of bent functions $\mathcal{C}$. Predominantly, we consider the problem of specifying bent functions in $\mathcal{C}$ outside the completed Maiorana-McFarland class $\mathcal{M}^{\#}$. In [83], a set of sufficient conditions for functions in $\mathcal{C}$ to be outside $\mathcal{M}^{\#}$ was specified. The result is stated in this chapter as Theorem 4.1.1. For a bent function $f \in \mathcal{C}$ of the form $f(x, y) = x \cdot \pi(y) + \mathbb{1}_{L^{\perp}}(x)$, where $x, y \in \mathbb{F}_2^n$, π is a permutation of $\mathbb{F}_2^n$ and L is a suitably chosen subspace of $\mathbb{F}_2^n$, the sufficient conditions in Theorem 4.1.1 mainly focus on properties of the permutation π. For example, one important requirement is that the component functions of π do not admit linear structures. However, although sufficient and very useful when specifying bent functions in $\mathcal{C}$ and $\mathcal{D}$ outside $\mathcal{M}^{\#}$, the conditions from [83] are not necessary, see e.g. [84]. In particular, certain modifications of the identity permutation (swapping two output values) were shown to provide bent functions which are provably outside $\mathcal{M}^{\#}$, even though the component functions of those permutations admit linear structures. In this context, for bent functions in $\mathcal{C}$, in Section 4.2 we show a stronger result which enables modifications of the identity permutation on arbitrary subsets of suitably selected subspaces (for the purpose of defining π), while at the same time the resulting bent functions will provably be in $\mathcal{C} \setminus \mathcal{M}^{\#}$. The component functions of such permutations π still admit linear structures which again indicate that there is a possibility of relaxing the set of sufficient conditions in [83]. Notice that the possibility of selecting arbitrary subsets of a linear subspace for the modification of the identity permutation will give us many infinite classes of bent functions in $\mathcal{C}$ which are provably outside $\mathcal{M}^{\#}$.

Using ranks of bent functions, in Section 4.3 we investigate the intersection of the class $\mathcal{C}$ and the partial spread class $\mathcal{PS}_{ap}$. In particular, we show that the probability that an n-variable function in $\mathcal{PS}_{ap}$ is also in $\mathcal{C}$ approaches zero as n increases.

We also pursue the opposite direction compared to the one in Section 4.2, that is, we will construct a class of permutations suitable for specifying bent functions in $\mathcal{C}$, and rely on the set of sufficient conditions from [83] to prove that the functions are outside $\mathcal{M}^{\#}$. To illustrate the hardness of the underlying problem, we first show in Section 4.4 that coset-based permutations are not suitable for our purpose since the members of this family of permutations inevitably have component functions that admit linear structures. Instead, in Section 4.5, we employ a certain method

of non-trivial decomposition of the vector space $\mathbb{F}_2^n$ into disjoint affine subspaces, originally considered by L.E. Baum and L.P. Neuwirth in [2]. The permutations are constructed using the decomposition and suitable permutations in a smaller number of variables. The possibility of selecting different subspaces in the decomposition and different permutations in a smaller number of variables provides us with a large family of bent functions in the $\mathcal{C}$ class which are outside $\mathcal{M}^{\#}$. This approach requires that the dimension of the subspace L is less than $n/2$. In contrast with this result, in Section 4.6, we prove that when the dimension of the subspace L is relatively large and the component functions of π do not admit linear structures, the pair (π^{-1}, L) cannot satisfy the property (C). Recall that (π^{-1}, L) satisfies the property (C) if $\pi^{-1}(a + L)$ is an affine subspace for all $a \in \mathbb{F}_2^n$, and that the property (C) is the defining property of the class $\mathcal{C}$. This result gives a further insight into what is likely a trade-off of using the sufficient (but not necessary) conditions in [83] for distinguishing bent functions in $\mathcal{C}$ which are outside $\mathcal{M}^{\#}$.

4.1 Some known relations between $\mathcal{C}$ and $\mathcal{M}^{\#}$

In [83], the authors provided sufficient conditions for bent functions in the classes $\mathcal{C}$ and $\mathcal{D}$ to be outside $\mathcal{M}^{\#}$, based on the properties of linear structures of the permutations used in the construction. The following result is the slightly corrected version of [83, Theorem 1] stated in [84], providing a sufficient conditions for functions in the class $\mathcal{C}$ to be outside $\mathcal{M}^{\#}$.

Theorem 4.1.1 *[84, Theorem 3] Let $m = 2n \geq 8$ be an even integer and let $f(x, y) = x \cdot \pi(y) + \mathbb{1}_{L^{\perp}}(x)$, where L is any linear subspace of $\mathbb{F}_2^n$ and π is a permutation on $\mathbb{F}_2^n$ such that (π^{-1}, L) has the property (C). If (π, L) satisfies:*

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

2) $u \cdot \pi$ has no nonzero linear structure for all $u \in \mathbb{F}_2^{n*}$,

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

We would like to point out that Theorem 4.1.1 is the result proved in [83], but the statement in [83] is slightly imprecise. Here, appropriate corrections were made. More precisely, (π, L) has the property (C) in [83] is replaced by (π^{-1}, L) has the property (C). Moreover, the condition that π has no linear structures in [83] is changed to $u \cdot \pi$ has no linear structures for all $u \in \mathbb{F}_2^n \backslash \{0_n\}$, which is the property actually used in the proof of the theorem in [83].

A similar result, namely [83, Theorem 2], provides sufficient conditions for bent functions in the $\mathcal{D}$ class to be outside $\mathcal{M}^{\#}$. Subsequently, in some recent papers (for example [84]) several constructions of permutations satisfying the sufficient conditions are presented, hence giving rise to some subclasses of the classes $\mathcal{C}$ and $\mathcal{D}$, provably outside $\mathcal{M}^{\#}$. In contrast to these results, our goal in Section 4.2 is to specify some permutations which fail to satisfy the sufficient conditions in Theorem 4.1.1, but which will nevertheless, together with an appropriately chosen subspace, produce functions in the class $\mathcal{C}$ outside $\mathcal{M}^{\#}$.

On the other hand, bent functions in $\mathcal{C}$ and $\mathcal{D}$ can easily lie in $\mathcal{M}^{\#}$. This is already discussed in [84], where the following theorem is proved, providing some sufficient conditions for functions in the class $\mathcal{C}$ to also be in $\mathcal{M}^{\#}$.

Theorem 4.1.2 *[84] Let $m = 2n \geq 8$ be an even integer and let $f(x, y) = x \cdot \pi(y) + \mathbb{1}_{L^{\perp}}(x)$, where L is any linear subspace of $\mathbb{F}_2^n$ and π is a permutation of $\mathbb{F}_2^n$ such that (π^{-1}, L) has property (C). Let S be a linear subspace of $\mathbb{F}_2^n$. If*

1) $S \subseteq L^{\perp}$;

2) For any $u \in S$, there exists a linear subspace K_0 of $\mathbb{F}_2^n$ such that $D_v(u \cdot \pi(y)) = 0$ for any $v \in K_0$;

3) $D_u D_v \pi(y) = 0$ for $u, v \in K_0$;

4) $\dim(S \times K_0) \geq n$,

then f belongs to $\mathcal{M}^{\#}$.

As an example of application of Theorem 4.1.2 the following result is proved in [84], utilizing a particular class of involutions over $\mathbb{F}_2^n$, for the purpose of identifying some bent functions that belong to both $\mathcal{C}$ and $\mathcal{M}^{\#}$.

Theorem 4.1.3 *[84] Let $n \geq 3$ be an integer, and let $a, b \in \mathbb{F}_2^n$. Let $\sigma_{a,b}$ be an involution that exchanges elements a and b and fixes all other elements, defined as*

$$\sigma_{a,b}(y) = \begin{cases} y, & y \in \mathbb{F}_2^n \setminus \{a, b\} \\ a, & y = b \\ b, & y = a. \end{cases} \tag{4.1}$$

Let $f(x, y) = x \cdot \sigma_{a,b}(y) + \mathbb{1}_{L^{\perp}}(x)$, where $L = \{0_n, a, b, a+b\}$. Then f belongs to both $\mathcal{C}$ and $\mathcal{M}^{\#}$.

However, in Section 4.2 we will show that, if the subspace L is chosen in a different way and if the dimension of L is large enough, we can still use involutions $\sigma_{a,b}$ to construct functions in $\mathcal{C}$ outside $\mathcal{M}^{\#}$.

4.2 A new class of $\mathcal{C}$ bent functions outside $\mathcal{M}^{\#}$

As mentioned in Section 4.1, our goal in this section is to find permutations with linear structures, which will, in contrast to Theorem 4.1.1, give us bent functions in the class $\mathcal{C}$ outside $\mathcal{M}^{\#}$. Theorem 4.2.1 is a rather general result which achieves that. Before we state the theorem, a few remarks are in order.
We define the permutation $\sigma_{\mathbb{e}_l, \mathbb{e}_t}$ as

$$\sigma_{\mathbb{e}_l, \mathbb{e}_t}(y) = \begin{cases} y, & y \notin \{\mathbb{e}_l, \mathbb{e}_t\}; \\ \mathbb{e}_l, & y = \mathbb{e}_t; \\ \mathbb{e}_t, & y = \mathbb{e}_l, \end{cases} \tag{4.2}$$

for all $y \in \mathbb{F}_2^n$, where $l, t \in \{1, 2, \ldots, n\}$ with $l \neq t$, and furthermore $\mathbb{e}_l, \mathbb{e}_t \in \mathbb{F}_2^n$ denote elements in the canonical basis of $\mathbb{F}_2^n$. It is an example of a permutation with components admitting linear structures, but it nevertheless can be efficiently used (as will be demonstrated by Corollary 4.2.2) for the purpose of generating bent functions in $\mathcal{C}$ outside $\mathcal{M}^{\#}$. Note that we can write $\sigma_{\mathbb{e}_1,\mathbb{e}_2}$ in the form

$$\sigma_{\mathbb{e}_1,\mathbb{e}_2}(y) = y + \left(\prod_{i=1}^{n}(y_i + (\mathbb{e}_1)_i + 1) + \prod_{i=1}^{n}(y_i + (\mathbb{e}_2)_i + 1)\right)(\mathbb{e}_1 + \mathbb{e}_2),$$

and so, not only does $\sigma_{\mathbb{e}_1,\mathbb{e}_2}$ have components with linear structures but when $n > 2$ it has linear coordinate functions. The cardinality of this family of permutations swapping only two elements of the identity permutation is quite small and therefore the derived family of bent functions in $\mathcal{C}$ outside $\mathcal{M}^{\#}$ is consequently also small. Nevertheless, the same approach that employs $\sigma_{\mathbb{e}_1,\mathbb{e}_2}$ can be generalized to modifications of the identity permutation performed on more than two elements. Especially, we address the case when S is chosen to be a linear (affine) subspace of certain dimension which also implies less tedious computations concerning second order derivatives of bent functions that use this kind of permutations. We notice that in general the modification of $\pi(y) = y$ on a subset S of $\mathbb{F}_2^n$ can be compactly written in the form

$$\sigma_S(y) = y + \mathbb{1}_S(y)(y + g(y)), \tag{4.3}$$

where g must permute S in order to ensure the bijectivity of σ_S.

In the special case that S is a subspace of $\mathbb{F}_2^n$, its algebraic normal form can be given in terms of the basis of its associated orthogonal complement. Namely, if $S^{\perp} = \{y \in \mathbb{F}_2^n : y \cdot s = 0, \text{ for all } s \in S\}$ then $\mathbb{1}_{S^{\perp}}(y) = \prod_{i=1}^{k}(a_i \cdot y + 1)$ if $\{a_1, \ldots, a_k\}$ constitutes a basis of the k-dimensional subspace S. Using a similar argument (S being the orthogonal complement of $S^{\perp}$) we have $\mathbb{1}_S(y) = \prod_{i=1}^{n-k}(b_i \cdot y + 1)$, where $\{b_1, \ldots, b_{n-k}\}$ is a basis of $S^{\perp}$.

In what follows, we show that the modification of the identity permutation on an arbitrary subset S of a suitably chosen subspace of an appropriate dimension, still leads to bent functions outside $\mathcal{M}^{\#}$.

Theorem 4.2.1 *Let n, k and t be three integers such that and $n \geq k \geq t+3 \geq 4$. Let S be an arbitrary subset of $E_t = \langle \mathbb{e}_1, \mathbb{e}_2, \ldots, \mathbb{e}_t \rangle \subset \mathbb{F}_2^n$. Let $\sigma_S(y)$ be an arbitrary non-identity permutation of $\mathbb{F}_2^n$ which fixes elements in $\mathbb{F}_2^n \setminus S$, (hence $|S| \geq 2$). Define $f(x, y) = x \cdot \sigma_S(y) + \mathbb{1}_{E_k^{\perp}}(x)$, with $x, y \in \mathbb{F}_2^n$, where $E_k = \langle \mathbb{e}_1, \mathbb{e}_2, \ldots, \mathbb{e}_k \rangle \subseteq \mathbb{F}_2^n$. Then, f is a bent function in the class $\mathcal{C}$ outside $\mathcal{M}^{\#}$.*

Proof. First, note that $S \subseteq E_t \subset E_k$ and therefore $\sigma_S(a + E_k) = a + E_k$, for every $a \in \mathbb{F}_2^n$. Hence, f is a bent function in the class $\mathcal{C}$.

When $S \subseteq E_t$, the permutations of $\mathbb{F}_2^n$ which fix elements in $\mathbb{F}_2^n \setminus S$ are special cases of permutations of $\mathbb{F}_2^n$ which fix elements in $\mathbb{F}_2^n \setminus E_t$, so it is enough to prove the theorem for the case $S = E_t$. Hence, for the rest of the proof we assume that $S = E_t$.

Since σ_{E_t} fixes elements of $\mathbb{F}_2^n \setminus E_t$, we can represent σ_{E_t} in the form

$$\sigma_{E_t}(y) = y + \mathbb{1}_{E_t}(y)g(y_1, \ldots, y_t), \text{ for all } y \in \mathbb{F}_2^n,$$

where g is a function from $\mathbb{F}_2^t$ to $\mathbb{F}_2^n$ of the form $g(y_1,\ldots,y_t)=(g'(y_1,\ldots,y_t),0_{n-t})$, and g' is a function from $\mathbb{F}_2^t$ to $\mathbb{F}_2^t$. Note that g is not the zero function, because σ_{E_t} is not the identity permutation of $\mathbb{F}_2^n$. Using this, along with the fact that $\mathbb{1}_{E_t}(y)=\prod_{i=t+1}^{n}(y_i+1)$ and $\mathbb{1}_{E_k^{\perp}}(x)=\prod_{i=1}^{k}(x_i+1)$, we get the following representation of f:

$$f(x,y)=x\cdot y+\prod_{i=t+1}^{n}(y_i+1)(x\cdot g(y_1,\ldots,y_t))+\prod_{i=1}^{k}(x_i+1),\ \text{for all } x,y\in\mathbb{F}_2^n.$$

Let V be an arbitrary n-dimensional subspace of $\mathbb{F}_2^{2n}$. To show that f is not in $\mathcal{M}^{\#}$, we will find $v',v''\in V$ such that $D_{v'}D_{v''}f\neq 0$. Denote by W the subspace $\langle \mathbb{e}_{t+1},\mathbb{e}_2,\ldots,\mathbb{e}_n\rangle\subset\mathbb{F}_2^n$ and by $U\subset\mathbb{F}_2^{2n}$ the subspace $(E_k\times\{0_n\})\oplus(\{0_n\}\times W)$, thus a direct sum of two disjoint subspaces (intersecting at $(0_n,0_n)$). Since V and U are subspaces of $\mathbb{F}_2^{2n}$, we have

$$\dim(V\cap U)=\dim V+\dim U-\dim(V+U),$$

where $V+U$ is the subspace $V+U=\{v+u\in\mathbb{F}_2^{2n}:v\in V,u\in U\}$. We know that $\dim V=n$, $\dim U=k+n-t$ and $\dim(V+U)\leq 2n$, so $\dim(V\cap U)\geq n+n+k-t-2n=k-t\geq 3$, since $k\geq t+3$. Every $v\in V\cap U$ can be represented in a unique way as $(e,0_n)+(0_n,w)$, for some $e\in E_k$ and $w\in W$, and so we can define a mapping $L:V\cap U\to E_k$ by $L(v)=L((e,0_n)+(0_n,w))=e$. Then, L is a well-defined linear mapping from $V\cap U$ to E_k. Hence, by the rank-nullity theorem, we have $\dim(Im(L))+\dim(Ker(L))=\dim(V\cap U)\geq 3$.

If $\dim(Im(L))\geq 2$, then there are two nonzero $e',e''\in E_k$, $e'\neq e''$, and some $w',w''\in W$ such that $v':=(e',0_n)+(0_n,w')$ and $v'':=(e'',0_n)+(0_n,w'')$ are in V. Moreover, we have

$$\begin{aligned}D_{v'}D_{v''}f(x,y)&=c+D_{v'}D_{v''}\left(\textstyle\prod_{i=t+1}^{n}(y_i+1)(x\cdot g(y_1,\ldots,y_t))+\prod_{i=1}^{k}(x_i+1)\right)\\&=c+D_{v'}D_{v''}\left(\textstyle\prod_{i=t+1}^{n}(y_i+1)(x\cdot g(y_1,\ldots,y_t))\right)+D_{e'}D_{e''}\left(\prod_{i=1}^{k}(x_i+1)\right),\end{aligned}$$

where $c\in\mathbb{F}_2$ is a constant. By Lemma 2.1.1, $D_{e'}D_{e''}\left(\prod_{i=1}^{k}(x_i+1)\right)$ is a function of degree $k-2\geq 2$, and since $\prod_{i=t+1}^{n}(y_i+1)(x\cdot g(y_1,\ldots,y_t))$ is of degree at most 1 in x, we can conclude that $D_{v'}D_{v''}f\neq 0$.

If $\dim(Im(L))\leq 1$, then $\dim(Ker(L))\geq 2$. Thus, there are two nonzero $w',w''\in W$, with $w'\neq w''$, such that $v':=(0_n,w')$ and $v'':=(0_n,w'')$ are in V. Then, we have

$$D_{v'}D_{v''}f(x,y)=c+(x\cdot g(y_1,\ldots,y_t))D_{w'}D_{w''}\left(\prod_{i=t+1}^{n}(y_i+1)\right)+0,$$

since $x\cdot g(y_1,\ldots,y_t)$ and $\prod_{i=1}^{k}(x_i+1)$ do not depend on $y_{t+1},\ldots,y_n$. Again, by Lemma 2.1.1, $D_{w'}D_{w''}\left(\prod_{i=t+1}^{n}(y_i+1)\right)$ is of degree at least $n-t-2\geq 1$, and hence we can deduce that $D_{v'}D_{v''}f\neq 0$ in this case as well.

We conclude that in any case, there are some v', v'' in V such that $D_{v'}D_{v''}f \neq 0$. Since V is an arbitrary n-dimensional subspace of $\mathbb{F}_2^{2n}$, we can conclude that f is outside $\mathcal{M}^{\#}$. ∎

As an immediate corollary of Theorem 4.2.1, we show that, in contrast to Theorem 4.1.3, we can still modify the identity permutation at exactly two positions and get bent functions outside $\mathcal{M}^{\#}$. We just have to be careful about the dimension of the subspace L.

Corollary 4.2.2 *Let n and k be two integers such that $n \geq k \geq 5$. Let $\sigma_{\mathbb{e}_1,\mathbb{e}_2}(y)$ be the permutation of $\mathbb{F}_2^n$ given by (4.2). Define $f(x,y) = x \cdot \sigma_{\mathbb{e}_1,\mathbb{e}_2}(y) + \mathbb{1}_{E_k^{\perp}}(x)$, with $x, y \in \mathbb{F}_2^n$, where $E_k = \langle \mathbb{e}_1, \mathbb{e}_2, \ldots, \mathbb{e}_k \rangle \subseteq \mathbb{F}_2^n$. Then, f is a bent function outside $\mathcal{M}^{\#}$.*

Proof. The result follows directly from Theorem 4.2.1 by setting $t = 2$ and $S = E_2 = \langle \mathbb{e}_1, \mathbb{e}_2 \rangle \subset \mathbb{F}_2^n$. ∎

4.3 Ranks of bent functions in the $\mathcal{C}$ class

In this section, we will consider ranks of bent functions in the class $\mathcal{C}$. More precisely, we will give an upper bound for the rank of bent functions in the class $\mathcal{C}$. Then, we will compare this bound with ranks of $\mathcal{PS}_{ap}$ functions and use that to prove that almost all bent functions in the class $\mathcal{PS}_{ap}$ are outside the class $\mathcal{C}$.

We recall here some basic definitions about ranks of Boolean functions, and for a more detailed study we refer to [80]. Let $f : \mathbb{F}_2^k \to \mathbb{F}_2$ be a Boolean function and let A^f be the $2^k \times 2^k$ matrix, with rows and columns indexed by elements of $\mathbb{F}_2^k$, whose (x,y)-th entry is $A^f(x,y) = f(x+y)$, for $x, y \in \mathbb{F}_2^k$. The rank of a Boolean function f, denoted by $\mathrm{rank}(f)$, is defined to be the rank of the matrix A^f over the field $\mathbb{F}_2$.

Proposition 4.3.1 *Let E be a vector subspace of $\mathbb{F}_2^n$, and let $f : \mathbb{F}_2^{2n} \to \mathbb{F}_2$ be a bent function in the class $\mathcal{C}$ given by $f(x,y) = x \cdot \pi(y) + \mathbb{1}_E(x)$, $x, y \in \mathbb{F}_2^n$, for some permutation π of $\mathbb{F}_2^n$. Then* $\mathrm{rank}(f) \leq 3 \cdot 2^n$.

Proof. The idea for the proof is similar to the one used in [80], when showing a similar bound for bent functions in the class $\mathcal{M}^{\#}$. For $(x,y), (a,b) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$ we have

$$A^f((x,y),(a,b)) = f((x,y)+(a,b)) = (x+a) \cdot \pi(y+b) + \mathbb{1}_E(x+a).$$

To cancel the $\mathbb{1}_E(x+a)$ term, we add the row indexed by $(x, 0_n)$ to the row indexed by (x,y) when $y \neq 0_n$. Thus, the $((x,y),(a,b))$ entry of A^f becomes

$$(x+a) \cdot (\pi(y+b) + \pi(b)).$$

Now, adding the column indexed by $(0_n, b)$ to the column (a,b) when $a \neq 0_n$, we get that the entry $((x,y),(a,b))$, with $y, a \neq 0_n$, evaluates to $(a \cdot (\pi(y+b)+\pi(b))$. Notice that this expression does not depend on x, so we can use this to get a lot of zeroes

in A^f in the following way. Add the row indexed by $(0_n, y)$ to the row indexed by (x, y), for all $x \neq 0_n$ and $y \neq 0_n$. Then, we get that the entry $((x, y), (a, b))$, with $a \neq 0_n$, $x \neq 0_n$, and $y \neq 0_n$ equals $(a \cdot (\pi(y + b) + \pi(b)) + (a \cdot (\pi(y + b) + \pi(b)) = 0$. Hence, by possibly rearranging rows of the matrix and using elementary row and column operations, we can transform the matrix A^f to a matrix of the form

$$\begin{pmatrix} A & A' \\ B & B' \\ C & \mathbf{0} \end{pmatrix}$$

where A, B are $2^n \times 2^n$ matrices, A', B' are $2^n \times (2^{2n} - 2^n)$ matrices, C is a $(2^{2n} - 2^{n+1}) \times 2^n$ matrix, and $\mathbf{0}$ is $(2^{2n} - 2^{n+1}) \times (2^{2n} - 2^n)$ matrix. From this, we have

$$\operatorname{rank}(f) \leq \operatorname{rank}\begin{pmatrix} A & A' \end{pmatrix} + \operatorname{rank}\begin{pmatrix} B & B' \end{pmatrix} + \operatorname{rank}\begin{pmatrix} C & \mathbf{0} \end{pmatrix} \leq 2^n + 2^n + 2^n = 3 \cdot 2^n.$$

■

Theorem 5.11 in [80] and remarks after it, state that for any given integer c, the probability that a bent function in $\mathcal{PS}_{ap}$ has rank less than $c \cdot 2^n$ approaches zero as n increases. Combining this result with Proposition 4.3.1, we get the following result.

Corollary 4.3.2 *The probability that a $2n$-variable bent function from the class $\mathcal{PS}_{ap}$ is also in the class $\mathcal{C}$ approaches zero as n increases.*

Proof. From Proposition 4.3.1, we have that when $f : \mathbb{F}_2^{2n} \to \mathbb{F}_2$ is in the $\mathcal{C}$ class, then $\operatorname{rank}(f) \leq 3 \cdot 2^n$. The corollary then follows from the result in [80], which states that, for any given integer c, the probability that a bent function in $\mathcal{PS}_{ap}$ has rank less than $c \cdot 2^n$ approaches zero as n increases. ■

4.4 Coset-based permutations and permutations without linear structures

In this section, we consider the problem of using Theorem 4.1.1 to construct bent functions in the $\mathcal{C}$ class, which are outside the completed Maiorana-McFarland class. From Theorem 4.1.1, we deduce that, in order to construct functions in $\mathcal{C}$ outside $\mathcal{M}^{\#}$, it is enough to construct permutations of $\mathbb{F}_2^n$ such that (π^{-1}, L) has property (C) for some subspace L of $\mathbb{F}_2^n$ with $\dim(L) \geq 2$, and such that $u \cdot \pi$ has no nonzero linear structures for all $u \in \mathbb{F}_2^n \backslash \{0_n\}$. In other words, non-trivial component functions of π should have no nonzero linear structures. Because of that, for the rest of this chapter, we will focus on the construction of permutations over $\mathbb{F}_2^n$ satisfying the mentioned properties.

To satisfy the (C) property, we note that the main condition that $\pi^{-1}(a + L)$ is a flat (affine subspace), for a k-dimensional subspace L, can be easily achieved by decomposing the space $\mathbb{F}_2^n$ into a set of disjoint cosets (flats) of some fixed k-dimensional subspace L' of $\mathbb{F}_2^n$. Indeed, let $\mathcal{A}$ denote a set of coset representatives

so that $\mathbb{F}_2^n = \cup_{a\in\mathcal{A}}(a+L)$, where clearly $|\mathcal{A}| = 2^{n-k}$. Let us denote $[a] := a + L$. Then, for any fixed k-dimensional subspaces L and L' we can define a mapping

$$a + L \overset{\phi}{\mapsto} a' + L'; \qquad a \in \mathcal{A}, a' \in \mathcal{A}', \tag{4.4}$$

where $\mathcal{A}$ and $\mathcal{A}'$ are the sets of coset representatives with respect to L and L', respectively. The necessary and sufficient condition that ϕ can be extended to a permutation on $\mathbb{F}_2^n$ is that $\phi : \mathcal{A} \to \mathcal{A}'$ is one-to-one. Then, we can extend it by deciding which elements of the coset $a + L$ maps to which elements of the coset $\phi(a + L)$. More formally, given a permutation ϕ on cosets we can take some bijection $\Phi_{[a]}$ from $a + L$ to $\phi(a + L)$, and then define our permutation Φ' on $\mathbb{F}_2^n$ to be $\Phi'(x) = \Phi_{[a]}(x)$, where $x \in [a]$, for every $x \in \mathbb{F}_2^n$.

Remark 1 *Denoting by P_k the number of k-dimensional subspaces of $\mathbb{F}_2^n$, one can show that the number of permutations obtained in this way is at least $P_k(2^{n-k})!(2^k)!$.*

We will show that every permutation obtained in this way has at least one component function with nonzero linear structure. Before we state and prove the result, we need to add a few remarks about coordinate and component functions.

We have defined coordinate and component functions in a way which is standard in the literature, for example in [12] or [20]. In the proof of the next theorem, we will use a slight generalization of the definition which we explain now. Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a vectorial Boolean function. The Boolean functions $f_1, \ldots, f_n$ defined, at every $x \in \mathbb{F}_2^n$, by $F(x) = (f_1(x), \ldots, f_n(x))$, are called the *coordinate functions* of F, and linear combinations (over $\mathbb{F}_2$) of the coordinate functions of F are called the *component functions* of F. If we denote the standard basis vectors of $\mathbb{F}_2^n$ by $\mathbb{e}_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ for $i = 1, \ldots, n$ (the i-th coordinate is 1 and the rest are 0), then, for every $x \in \mathbb{F}_2^n$ we can write

$$F(x) = (f_1(x), \ldots, f_n(x)) = f_1(x)\mathbb{e}_1 + \ldots + f_n(x)\mathbb{e}_n.$$

The product $f_i(x)\mathbb{e}_i$ is well defined when $x \in \mathbb{F}_2^n$ is fixed, since it is a product of a vector, $\mathbb{e}_i \in \mathbb{F}_2^n$, and a scalar, $f_i(x) \in \mathbb{F}_2$.

If $B = \{b_1, b_2, \ldots, b_n\}$ is any (ordered) basis for $\mathbb{F}_2^n$, we can use the same idea as for the standard basis and define the *coordinate functions of F with respect to the basis B* as the Boolean functions $f'_1, \ldots, f'_n$, which are defined, at every $x \in \mathbb{F}_2^n$, by

$$F(x) = f'_1(x)b_1 + f'_2(x)b_2 + \ldots + f'_n(x)b_n.$$

As in the standard basis case, the product $f'_i(x)b_i$ is well defined when $x \in \mathbb{F}_2^n$ is fixed, as a product of a vector $b_i \in \mathbb{F}_2^n$ and a scalar $f'(x) \in \mathbb{F}_2$. Furthermore, we know that $f'_1, \ldots, f'_n$ exist and are well defined, because B is a basis for $\mathbb{F}_2^n$. Linear combinations (over $\mathbb{F}_2$) of $f'_1, \ldots, f'_n$ are called the *component functions of F with respect to the basis B*.

Let $A = \{a_1, \ldots a_n\}$ and $B = \{b_1, \ldots b_n\}$ be two bases of $\mathbb{F}_2^n$. The set of coordinate functions $f_1^A, \ldots, f_n^A$ of F with respect to the basis A might be different from the set of coordinate functions $f_1^B, \ldots, f_n^B$ of F with respect to B, but the set of all

component functions of F with respect to either A or B is the same. To see this, represent every a_i, for $i \in \{1, \ldots, n\}$, as $a_i = \sum_{j=1}^{n} \alpha_j^{(i)} b_j$, where $\alpha_j^{(i)} \in \mathbb{F}_2$. Then from

$$F(x) = \sum_{i=1}^{n} f_i^A(x) a_i = \sum_{i=1}^{n} f_i^A(x) \left(\sum_{j=1}^{n} \alpha_j^{(i)} b_j \right) = \sum_{j=1}^{n} \left(\sum_{i=1}^{n} \alpha_j^{(i)} f_i^A(x) \right) b_j,$$

we conclude that $f_j^B = \left(\sum_{i=1}^{n} \alpha_j^{(i)} f_i^A \right)$ for every $j \in \{1, 2, \ldots n\}$. Thus, the set of all component functions of F with respect to the basis B is a subset of the set of all component functions of F with respect to the basis A, and reversing the roles of A and B, we get the equality. This means that we can just say the set of component functions of F without having to refer to a specific basis.

We are now ready to prove the following result, which asserts that the construction of permutations described at the beginning of this section generates permutations whose component functions admit nonzero linear structures. This shows that the simple idea of taking two (not necessarily different) subspaces of $\mathbb{F}_2^n$, and mapping their cosets in some bijective way to construct a permutation with the (C) property, will necessarily produce a permutation with components admitting non-trivial linear structures, hence we will not be able to use Theorem 4.1.1 to show that the constructed bent function in the $\mathcal{C}$ class is outside $\mathcal{M}^{\#}$.

Proposition 4.4.1 *Let L and P be two k-dimensional subspaces of $\mathbb{F}_2^n$, and let $\pi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a permutation such that π maps cosets of L to cosets of P, i.e. $\pi(a + L) = \pi(a) + P$, for every $a \in \mathbb{F}_2^n$. Then, π has at least $2^{(n-\dim(L))}$ component functions such that their space of linear structures contains L.*

Proof. Assume that $d := \dim(L) \neq 0, n$, (if $L = \{0_n\}$, or $L = \mathbb{F}_2^n$, the result is trivially true). Let P' be a subspace of $\mathbb{F}_2^n$ such that $P \cap P' = \{0_n\}$ and $P \oplus P' = \mathbb{F}_2^n$. Let $B_1 = \{p_1, p_2, \ldots, p_d\}$ be a basis for P and $B_2 = \{p'_1, p'_2, \ldots, p'_{n-d}\}$ be a basis for P'. Then, $B = B_1 \cup B_2$ is a basis of $\mathbb{F}_2^n$. Denote by $\pi_i : \mathbb{F}_2^n \to \mathbb{F}_2$, $i \in \{1, 2, \ldots n\}$, the coordinate functions of π with respect to the basis B, i.e. $\pi_1, \ldots, \pi_n$ are Boolean functions such that, for every (fixed) $x \in \mathbb{F}_2^n$,

$$\pi(x) = \pi_1(x)p_1 + \ldots + \pi_d(x)p_d + \pi_{d+1}(x)p'_1 + \ldots + \pi_n(x)p'_{n-d}.$$

Now, select an arbitrary $v \in L$ and $x \in \mathbb{F}_2^n$ and fix these values. Since x and $x + v$ are in the same coset of L, we have that $\pi(x)$ and $\pi(x + v)$ are in the same coset of P. This means that there exists $q \in P$ such that $\pi(x + v) = \pi(x) + q$. Rewriting this, we have

$$\pi(x + v) + \pi(x) = q,$$

and since $q \in P$ we have that $\pi_{d+i}(x+v)+\pi_{d+i}(x) = 0$, for every $i \in \{1, 2, \ldots, n-d\}$. Since $x \in \mathbb{F}_2^n$ and $v \in L$ were arbitrary, this implies that every component function of the form $\sum_{i=1}^{n-d} \alpha_i \pi_{d+i}(x)$, $\alpha_i \in \mathbb{F}_2$, has L as a subspace of its linear structure space. So, there are at least 2^{n-d} component functions of π such that their linear structure space contains L. ∎

Note that when the dimension of L is in $\{1, 2, \ldots, n-1\}$, (which are the dimensions we are actually interested in) this result implies that for a permutation constructed as described at the beginning of this section, there will always be at least one non-trivial component function with a nonzero linear structure.

4.5 Permutations via non-trivial decompositions of $\mathbb{F}_2^n$

In this section, we describe a different (compared to the one in Section 4.4), non-trivial decomposition of $\mathbb{F}_2^n$ into affine subspaces, presented in [2], which is more suitable for constructing functions in $\mathcal{C}$ outside $\mathcal{M}^{\#}$. Essentially, this decomposition is a collection of nonparallel affine subspaces which means that the disjoint subspaces are not cosets of the same affine subspace of certain dimension. This is the main reason why such a decomposition is suitable for finding the permutations whose components do not admit linear structures.

We start by taking an arbitrary subspace of $\mathbb{F}_2^n$, let us denote it by E, with $1 \leq d := \dim(E) \leq (n-1)/2$. Then, we take another subspace V of $\mathbb{F}_2^n$ such that $\mathbb{F}_2^n$ is the direct sum of E and V, i.e. $E \cap V = \{0_n\}$, and $E \oplus V = \mathbb{F}_2^n$. Moreover, we will need $d+1$ permutations $I_V, \sigma_1, \ldots, \sigma_d$ on V, (here I_V is the identity permutation on V) such that any non-trivial linear combination of them is again a permutation of V. To achieve this, we interpret V as the finite field $\mathbb{F}_{2^{n-d}}$ in the following way. We define a mapping $\mathcal{L}$ between the vector subspace V and the finite field $\mathbb{F}_{2^{n-d}}$. Let $u_1, \ldots, u_{n-d}$ be the basis of the subspace V and let α be a primitive element of the finite field $\mathbb{F}_{2^{n-d}}$. Then, we define $\mathcal{L} : u_i \mapsto \alpha^{i-1}$ whereas the remaining elements are mapped in such a way as to preserve isomorphism between additive structures. That is,

$$\mathcal{L}\left(\sum_{i=1}^{n-d} \beta_i u_i\right) = \sum_{i=1}^{n-d} \beta_i \alpha^{i-1}, \tag{4.5}$$

where $\beta_i \in \mathbb{F}_2$. Using such a mapping we can induce a multiplication operation on elements of the subspace V by defining

$$v_i \star v_j = \mathcal{L}^{-1}(\mathcal{L}(v_i)\mathcal{L}(v_j)), \text{ for any } v_i, v_j \in V. \tag{4.6}$$

With "$\star$" defined in this way $(V, +, \star)$ has the structure of a finite field. Moreover, $\mathcal{L}$ becomes a field isomorphism between V and $\mathbb{F}_{2^{n-d}}$.

Now we take $d+1$ linearly independent vectors $w_0 = 1_V, w_1, \ldots, w_d \in V$, where $d \leq n-d-1$, and define σ_i by $\sigma_i(v) = w_i \star v$ as a permutation of V. Here, 1_V denotes the multiplicative identity in $(V, +, \star)$, which by (4.5) and (4.6) corresponds to $u_1 \in V$. Constructed like this, $I_V, \sigma_1, \ldots, \sigma_d$ have the desired property that any non-trivial linear combination of them is again a permutation of V because $1_V, w_1, \ldots, w_d$ are linearly independent.

Let $e_1, \ldots, e_d$ be a basis for E, and let $V = \{v_1, v_2, \ldots, v_{2^{n-d}}\}$. For every $i \in \{1, 2, \ldots, 2^{n-d}\}$, we define the following set

$$A_i := \left\{ v_i + \sum_{k \in S} (\sigma_k(v_i) + e_k) \mid S \subseteq \{1, 2, \ldots, d\} \right\}.$$

Then, according to Theorem 2 in [2], A_i are pairwise disjoint affine subspaces of dimension d and they cover the whole $\mathbb{F}_2^n$. Moreover, the subspaces $A_i^* := v_i + A_i$ are also pairwise disjoint (i.e. have only 0_n in common).

We can use this decomposition to construct permutations with the (C) property in the following way. Take an arbitrary d-dimensional subspace of $\mathbb{F}_2^n$, for simplicity we can take E, and map each A_i to some coset of E in a one-to-one way. Therefore, we are free to select which A_i maps to which coset of E, and then we can specify which element of A_i maps to which element of the corresponding coset of E, also in a one-to-one way. Having specified this, we get a mapping, denote it by ϕ, from $\mathbb{F}_2^n$ to itself. Since A_i are pairwise disjoint, ϕ is a permutation of $\mathbb{F}_2^n$. Also, it follows from the construction that the pair (ϕ^{-1}, E) satisfies the property (C).

To ensure that ϕ does not have any component functions admitting linear structures, we need to further specify the mappings that we use in the construction.

Let $\varphi(v) = \mathcal{L}^{-1}(\mathcal{L}(v)^m) = \underbrace{v \star v \star \ldots \star v}_{m\text{-times}} = v^m$ be a monomial permutation of V whose component functions are without linear structures. From [19], we know that m needs to be such that $\gcd(2^{n-d} - 1, m) = 1$, and $wt_2(m) \geq 3$. Also, let ψ be an arbitrary permutation of E with no component functions admitting linear structures. (For example, we can again use results from [19], and take ψ to be a monomial permutation of E with no component functions admitting linear structures, using the same approach we used for V and φ.) Having specified φ and ψ, we can now define a function ϕ on $\mathbb{F}_2^n$ in the following way:

- For $x = v + e \in \mathbb{F}_2^n$, $v \in V$ and $e \in E$, where $v \neq 0_n$, represent e as $e = \sum_{k \in S_e} e_k$, $S_e \subseteq \{1, 2, \ldots d\}$. We know that $I_V + \sum_{k \in S_e} \sigma_k$ is a linear permutation of V, (since it depends on e, we can denote it by P_e) and so for each $v \in V$ there exists $w \in V$ such that $v = \left(I_V + \sum_{k \in S_e} \sigma_k\right)(w) = P_e(w)$. Define
$$\phi(v + e) = \varphi(w) + e. \tag{4.7}$$
Since $v = P_e(w)$, we can write it as $\phi(v + e) = \varphi(P_e^{-1}(v)) + e$.

- For $x = v + e \in E \subset \mathbb{F}_2^n$, thus having $v = 0_n$, we define:
$$\phi(x) = \psi(x). \tag{4.8}$$

Note that we can now express $A_i = \{P_e(v_i) + e \mid e \in E\}$. It follows that ϕ maps A_i exactly to $\varphi(v_i) + E$ and is a permutation of $\mathbb{F}_2^n$. Therefore, (ϕ^{-1}, E) has the property (C). Since $\varphi(P_e^{-1}(0_n)) = 0_n$, for every e in E, we can write (4.7) and (4.8) as one equation in the following way:

$$\phi(x) = \phi(v + e) = \varphi\left(P_e^{-1}(v)\right) + e + \delta_0(v)\left(e + \psi(e)\right), \text{ for all } x \in \mathbb{F}_2^n. \tag{4.9}$$

Here, we write x as $x = v + e$ for some $v \in V$, $e \in E$. Also, $\delta_0(v)$ denotes the Dirac function, namely $\delta_0 : V \to \mathbb{F}_2$ equals 1 when $v = 0_n \in V$ and 0 otherwise.

The following result shows that the component functions of ϕ do not admit linear structures. In the theorem below, we will treat V interchangeably as a subspace $(V, +)$ of $\mathbb{F}_2^n$, and as a finite field $(V, +, \star)$, where the addition is again inherited from $\mathbb{F}_2^n$ and multiplication $\star$ is defined by (4.6). Moreover, 1_V will denote the multiplicative identity in $(V, +, \star)$.

Theorem 4.5.1 *Let E and V be two subspaces of $\mathbb{F}_2^n$ such that $E \cap V = \{0_n\}$, $E \oplus V = \mathbb{F}_2^n$, and $1 \leq d := \dim(E) \leq (n-1)/2$. Let $1_V, w_1, \ldots, w_d \in V$ be linearly independent vectors and σ_i be the permutation of V defined by $\sigma_i(v) = w_i \star v$. Let m be such that $\gcd(2^{n-d}-1, m) = 1$, $wt_2(m) \geq 3$, and let $\varphi(v) = \underbrace{v \star v \star \ldots \star v}_{m\text{-times}} = v^m$, for all $v \in V$. Let ψ be a permutation of E whose component functions do not admit linear structures. Then, the function $\phi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ defined by (4.7) and (4.8) is a permutation of $\mathbb{F}_2^n$ whose (non-trivial) component functions do not admit (nonzero) linear structures.*

Proof. By the discussion preceding the Theorem, we know that ϕ is well defined and that it is a permutation of $\mathbb{F}_2^n$, so we just need to prove that ϕ has no component functions with linear structures.

Let $B = \{u_1, u_2, \ldots, u_{n-d}, e_1, e_2, \ldots, e_d\}$ be a basis for $\mathbb{F}_2^n$, such that $u_i \in V$ and $e_j \in E$. Let $\{\phi_1^V, \ldots, \phi_{n-d}^V, \phi_1^E, \ldots, \phi_d^E\}$ be the coordinate functions of ϕ with respect to the basis B, i.e. $\phi_i^V, \phi_j^E : \mathbb{F}_2^n \to \mathbb{F}_2$ are such that

$$\phi(x) \;=\; \sum_{i=1}^{n-d} \phi_i^V(x) u_i + \sum_{j=1}^{d} \phi_j^E(x) e_j, \quad \forall x \in \mathbb{F}_2^n. \tag{4.10}$$

Take an arbitrary $a \in \mathbb{F}_2^{n*}$, represent it as $a = v' + e'$, where $v' \in V$ and $e' \in E$, and fix it. Also, represent the variable x as $x = v + e$ with $v \in V$ and $e \in E$. Further, denote $I_V + \sum_{k \in S_e} \sigma_k$ by P_e, where S_e is the set of indices such that $e = \sum_{k \in S_e} e_k$. From (4.9), we deduce that the sum $\phi(x+a) + \phi(x) = \phi(v + e + v' + e') + \phi(v + e)$ is equal to

$$\varphi\left(P_{e+e'}^{-1}(v+v')\right) + \varphi\left(P_e^{-1}(v)\right) + e' + \delta_0(v+v')\left(e + e' + \psi(e+e')\right) + \delta_0(v)\left(e + \psi(e)\right).$$

The coordinate functions of $\phi(x+a) + \phi(x)$ corresponding to the basis elements in V are the coordinate functions of $\varphi\left(P_{e+e'}^{-1}(v+v')\right) + \varphi\left(P_e^{-1}(v)\right)$, and similarly the coordinate functions corresponding to the basis of E are the coordinate functions of $e' + \delta_0(v+v')\left(e + e' + \psi(e+e')\right) + \delta_0(v)\left(e + \psi(e)\right)$. According to this, we will split the proof into three cases.

Case I: The component functions of the form $\sum_{i=1}^{n-d} c_i \phi_i^V(x)$.

In this part of the proof, we will show that the coordinate functions ϕ_i^V from (4.10) (corresponding to the basis elements in V), and their (non-trivial) linear combinations, do not admit linear structures. This will be done by proving that the component functions of $\varphi\left(P_{e+e'}^{-1}(v+v')\right) + \varphi\left(P_e^{-1}(v)\right)$ are non-constant for every nonzero element $v' + e'$.

- If $e' = 0_n$, implying that $v' \neq 0_n$, set $r = 1_V + \sum_{k \in S_e} w_k \in V$. Then $\varphi\left(P_e^{-1}(v+v')\right) + \varphi\left(P_e^{-1}(v)\right)$ is equal to

  $$\varphi\left((v+v') \star r^{-1}\right) + \varphi\left(v \star r^{-1}\right) = r^{-m} \star (v^m + (v+v')^m),$$

  where $r^{-1} \in V$ satisfies $r \star r^{-1} = 1_V$. We know that φ has no component functions with linear structures since $wt_2(m) > 2$ (this is a direct consequence

of [19], Theorem 5), therefore $(v^m + (v+v')^m)$ has no constant component functions and it only depends on the variable v. This term is multiplied (using the operation $\star$) with the nonzero $r^{-m} = \left(1_V + \sum_{k\in S_e} w_k\right)^{-m} \in V$, which only depends on e. This product cannot be constant.

- If $e' \neq 0_n$, then set $e = 0_n$. Let S' be the set for which $e' = \sum_{k\in S'} e_k$, and let $b = (1_V + \sum_{k\in S'} w_k)^{-1} \in V$. Then $P_{e'}^{-1}(v) = b \star v$, for all $v \in V$. We know that $b \neq 0, 1_V$; since $1_V, w_1, \ldots, w_d$ are linearly independent and $S' \neq \emptyset$. Then, $\varphi\left(P_{e'}^{-1}(v+v')\right) + \varphi\left(P_{0_n}^{-1}(v)\right)$ is equal to

$$(b\star(v+v'))^m + v^m = (b\star(v+v'))^m + (b\star v)^m + (1_V + b^m)\star v^m.$$

  All component functions of $(b\star(v+v'))^m + (b\star v)^m$ are of degree strictly less than $wt_2(m)$, while all component functions of $(1_V + b^m)\star v^m$ are of degree exactly $wt_2(m)$. We conclude that the component functions of $(b\star(v+v'))^m + (b\star v)^m + (1_V + b^m)\star v^m$ are of degree $wt_2(m)$, and hence not constant.

Case II: The component functions of the form $\sum_{i=1}^{d} c_i\phi_i^E(x)$.

In this part, we show that the component functions derived from the coordinate functions of $\phi(x+a) + \phi(x)$ corresponding to the basis elements in E, that is the component functions of $e' + \delta_0(v+v')\,(e + e' + \psi(e+e')) + \delta_0(v)\,(e+\psi(e))$, are non-constant.

Let $v = v_1u_1 + \ldots + v_{n-d}u_{n-d}$, and $v' = v'_1u_1 + \ldots + v'_{n-d}u_{n-d}$, where $v_i, v'_i \in \mathbb{F}_2$. Then, we can write $e' + \delta_0(v+v')\,(e+e'+\psi(e+e')) + \delta_0(v)\,(e+\psi(e))$ as

$$\left(\prod_{i=1}^{n-d} v_i\right)\left(e' + \psi(e+e') + \psi(e)\right) + f_{v'}(v)\left(e + e' + \psi(e+e')\right) + g(v)\,(e+\psi(e)) + e',$$

where $f_{v'}(v)$ and $g(v)$ are Boolean functions with the algebraic degrees strictly less than $n-d$.

- Let $e' \neq 0_n$. Since ψ has no component function with linear structure, the component functions of $(e' + \psi(e+e') + \psi(e))$ are non-constant, and we conclude that component functions of $e' + \delta_0(v+v')\,(e+e'+\psi(e+e')) + \delta_0(v)\,(e+\psi(e))$ are non-constant as well, since the algebraic degrees of $f_{v'}(v)$ and $g(v)$ are strictly less than $n-d$.

- If $e' = 0_n$, then fix $v = 0_n (\neq v')$. We have

$$e' + \delta_0(v+v')\left(e + e' + \psi(e+e')\right) + \delta_0(v)\,(e+\psi(e)) = e + \psi(e),$$

  and component functions of $e + \psi(e)$ are non-constant since ψ has no affine component functions.

Case III: The component functions of the form $\sum_{i=1}^{n-d} c_i\phi_i^V(x) + \sum_{j=1}^{d} c'_j\phi_j^E(x)$, such that there exist i_0, j_0 such that $c_{i_0} = c'_{j_0} = 1$.

- If $e' \neq 0_n$, the degree of the part $\sum_{i=1}^{n-d} c_i(\phi_i^V(v+v'+e+e') + \phi_i^V(v+e))$, with respect to the variable v, is $wt_2(m) \leq n-d-1$ as shown in Case I, and the

degree of the part $\sum_{j=1}^{d} c'_j(\phi_j^E(v+v'+e+e')+\phi_j^E(v+e))$ with respect to the variable v is $n-d$ (from Case II). Therefore we conclude that the component function $\sum_{i=1}^{n-d} c_i\phi_i^V(x)+\sum_{j=1}^{d} c'_j\phi_j^E(x)$ has no linear structures in this case.

- If $e'=0_n$, set $e=0_n$ and fix it. As shown in Case I, $\sum_{i=1}^{n-d} c_i(\phi_i^V(v+v')+\phi_i^V(v))$ is a component function of $\varphi(v+v')+\varphi(v)$, and so, it is non-constant. Since it has degree strictly less than $wt_2(m)\leq n-d-1$, we can choose two vectors in V different from 0_n and v', such that it is equal to 0 for one of the vectors, and 1 for the other one (follows from Theorem 2.0.1). On the other hand, $\sum_{i=1}^{d} c'_i(\phi_i^E(v+v')+\phi_i^E(v))$ is a component function of $(\delta_0(v+v')+\delta_0(v))\psi(0)$, and so it is 0, when $v\neq 0_n, v'$. This proves that the component function $\sum_{i=1}^{n-d} c_i\phi_i^V(x)+\sum_{j=1}^{d} c'_j\phi_j^E(x)$ has no linear structures in this case as well. ■

Combining Theorem 4.1.1 and Theorem 4.5.1, we have the following corollary.

Corollary 4.5.2 *Let ϕ be as in Theorem 4.5.1. Then the function $f\colon \mathbb{F}_2^{2n}\to\mathbb{F}_2$ defined by $f(x,y)=x\cdot\phi(y)+1_{E^\perp}(x)$ is a function in the class $\mathcal{C}$ outside $\mathcal{M}^\#$.*

Note that when $\dim(E)\geq 4$, one possible choice for permutations φ and ψ is the inverse function, i.e. $\varphi(v)=v^{-1}$ and $\psi(e)=e^{-1}$, since they will not have component functions with linear structures (see [19]). This proves the following corollary.

Corollary 4.5.3 *Let n be an integer, and let E be a subspace of $\mathbb{F}_2^n$ such that $4\leq\dim(E)\leq(n-1)/2$. Then there is a permutation ϕ of $\mathbb{F}_2^n$ with no non-trivial component functions with nonzero linear structures, such that ϕ^{-1} maps cosets of E to affine subspaces.*

The example below describes in detail the use of Theorem 4.5.1 for the purpose of constructing permutations that satisfy the property (C), whose component functions at the same time do not admit linear structures.

Example 2 *For $n=9$, let E be the subspace of $\mathbb{F}_2^9$ generated by:*

$$\begin{bmatrix} e_1\\ e_2\\ e_3\\ e_4\end{bmatrix}=\begin{bmatrix}(1,\,0,\,0,\,0,\,0,\,0,\,0,\,0,\,0)\\ (0,\,1,\,0,\,1,\,0,\,1,\,1,\,1,\,1)\\ (0,\,0,\,1,\,0,\,0,\,0,\,1,\,1,\,1)\\ (0,\,0,\,0,\,0,\,1,\,1,\,0,\,0,\,1)\end{bmatrix}.$$

Then $\dim(E)=4$. Now we need to take a subspace V of $\mathbb{F}_2^9$ such that $E\cap V=\{0_9\}$ and $E\oplus V=\mathbb{F}_2^9$. For example, we can set V to be the subspace generated by vectors $\{u_1,u_2,u_3,u_4,u_5\}$, where:

$$\begin{bmatrix} u_1\\ u_2\\ u_3\\ u_4\\ u_5\end{bmatrix}=\begin{bmatrix}(0,\,1,\,0,\,0,\,0,\,0,\,0,\,0,\,0)\\ (0,\,0,\,1,\,0,\,0,\,0,\,0,\,0,\,0)\\ (0,\,0,\,0,\,1,\,0,\,0,\,0,\,0,\,0)\\ (0,\,0,\,0,\,0,\,1,\,0,\,0,\,0,\,0)\\ (0,\,0,\,0,\,0,\,0,\,0,\,1,\,0,\,0)\end{bmatrix}.$$

We can now identify V with the finite field $\mathbb{F}_{2^5}$ in the following way. Let α be a root of $p(x) = x^5 + x^2 + 1$. The polynomial $p(x)$ is irreducible over $\mathbb{F}_2$, so $\{1, \alpha, \alpha^2, \alpha^3, \alpha^4\}$ generate $\mathbb{F}_{2^5}$ over $\mathbb{F}_2$. Let $\mathcal{L}(u_i) = \alpha^{i-1}$, and extend this mapping to V so it remains linear, as described in the beginning of the section. Define multiplication on V, so that $\mathcal{L}$ remains an isomorphism of the fields, i.e. set $v_i \star v_j = \mathcal{L}^{-1}(\mathcal{L}(v_i)\mathcal{L}(v_j))$. Set $\sigma_k(v) = u_{k+1} \star v$ for $k \in \{1, 2, 3, 4\}$. Furthermore, set $\varphi(v) = v^{-1} = v^{30}$ for every $v \in V$. Because $wt_2(30) > 2$, we know that φ has no component functions with linear structure.

In a similar way, we can relate the subspace E to the finite field $\mathbb{F}_{2^4}$ in order to define the mapping ψ. We use a root γ of the polynomial $x^4 + x + 1$. We can then set $\psi(e) = e^{-1} = e^{14}$, for every $e \in E$. Since $wt_2(14) > 2$, we conclude that ψ has no linear structure. Finally, we use equations (4.7) and (4.8) to get the permutation ϕ of $\mathbb{F}_2^9$. Constructed in this way, ϕ is equal to $\phi = (\phi_1, \phi_2, \ldots, \phi_9)$, where the coordinate functions, in their hexadecimal form, are given by:

$\phi_1 =$ `00000c0000000030000000000000000fffffffffffffffffffdffffbfffffff`
`ffdfffffff7fffffffffffffffffffff00000000000000000000000000000000`

$\phi_2 =$ `a80c9bf1fc26401967ad21f58ae56f47cab4546e11637ae5376df06206d38a3c`
`43250f29af3158c36fb8b916def5a8618629ee636751ca4b85c0c5dfcf9207ac`

$\phi_3 =$ `8f1ac93597315caf981928df582a0be74c71759e72c2b59ecafb4a2c5ca3046d`
`939368c1f1c680e537eb5b2518e368d9ba927101456e8fb1f492df9cb5233638`

$\phi_4 =$ `af792b805dca3dd8b54799c312620f99fc5ae1295a0cab771f41266f013b3958`
`01e862c62fbc9f85fc9a2d5d590c49bb64b856f012dac36a3a97c1f8d5afdc40`

$\phi_5 =$ `90fc8634fc09d072f6d64a4d549f8e9edbe986c5a41853ae01d9336c577336f0`
`df4103c64ac46303425e98af497efae5939d942b4ac617e5090f5b7ccc90f1ea`

$\phi_6 =$ `aaaaaeaa55555565aaaaaaaa55555555aaaaaaaa55555555aaa8aaaa55555555`
`55655555a6aaaaaa55555555aaaaaaaa55555555aaaaaaaa55559555aaaaaaaa`

$\phi_7 =$ `8c2213a784cd16f4d1ecd6460bbbad64da4a73445d64e20d52be8bd37eb638e1`
`d938b4cd2c548c2e52a4fb48d5b91ee31efd6d9b7c7b254638210d8988d3ae70`

$\phi_8 =$ `fffff3fffffffffffffffffffffffff00000000000000000002000040000000`
`ffffffffffffffffffffffffffffffff00000000000000000000000000000000`

$\phi_9 =$ `555555555555554555555555555555aaaaaaaaaaaaaaaaaaaabaaaa2aaaaaaa`
`557555555555555555555555555555aaaaaaaaaaaaaaaaaaaa6aaaaaaaaaa`

To get the truth table of ϕ_1, for example, we need to reverse its hexadecimal string (due to the implementation in the mathematical software Sage) and to convert every hexadecimal number to its binary representation, `0` *to* 0000, `1` *to* 1000, *...,* `f` *to* 1111. *This finally gives a binary string of length* 512 *which is the truth table of our function ϕ_1 written in the lexicographic order, i.e. in the form*

$$\phi_1(0,0,\ldots,0), \phi_1(1,0,\ldots,0), \phi_1(0,1,\ldots,0), \ldots, \phi_1(1,1,\ldots,1).$$

Corollary 4.5.2 implies that the 18*-variable function $f(x, y) = x \cdot \phi(y) + 1_{E^\perp}(x)$ constructed in this way is a bent function in $\mathcal{C}$ outside $\mathcal{M}^{\#}$.*

4.6 A trade-off between the (C) property and linear structures

In this section, we will prove that for a permutation π of $\mathbb{F}_2^n$ there is a trade-off between the property that no component functions of π admit linear structures, and the requirement that π^{-1} satisfies the (C) property for some subspace E. The dimension of E will play an essential role in this trade-off. Note that Corollary 4.5.3 states that for $4 \leq \dim(E) \leq (n-1)/2$ there is a permutation whose components do not have linear structures and such that (π^{-1}, E) satisfies the (C) property. In contrast, Theorem 4.6.2 below claims that when the dimension of E is relatively large and (π^{-1}, E) has the (C) property, the permutation π will necessarily have some component functions with nonzero linear structures.

In order to prove our result, we will use the following result from [2].

Theorem 4.6.1 *[[2], Theorem 3] If $n > 2^d(d-1)+1$, then every cover of $\mathbb{F}_2^n$ by affine subspaces of dimension $n-d$ is a cross product with at least one trivial factor of dimension at least $n - 2^d(d-1) - 1$.*

Let us give a quick overview of the notation used in [2] in the statement of Theorem 4.6.1. The term cover is used to denote a family $\{A_i\}_{i=1}^t$ of affine subspaces of $\mathbb{F}_2^n$ such that $A_i \cap A_j = \emptyset$ when $i \neq j$, and such that $\mathbb{F}_2^n = \cup_{i=1}^t A_i$. Also, a cover $\{A_i\}_{i=1}^t$ of $\mathbb{F}_2^n$ is a cross product if it is of the form $\{B_j \times C_k\}_{(j,k)=(1,1)}^{(t_0,t_1)}$ where $\{B_j\}_{j=1}^{t_0}$ is a cover of $\mathbb{F}_2^r$, $\{C_k\}_{k=1}^{t_1}$ is a cover of $\mathbb{F}_2^{n-r}$, and $\times$ is the standard Cartesian product. The cover $\{\mathbb{F}_2^n\}$ is called the trivial cover of $\mathbb{F}_2^n$.

We will now combine Theorem 4.6.1 with a method similar to the one used in Section 4.4, to prove the result mentioned at the beginning of this section.

Theorem 4.6.2 *Let n and d be two integers such that $d \geq 1$ and $n > 2^d(d-1)+1$. Let $\pi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a permutation. If there exists a linear subspace E with dimension $\dim(E) = n-d$, such that $\left(\pi^{-1}, E\right)$ has the (C) property, i.e. $\pi^{-1}(a+E)$ is an affine subspace for every $a \in \mathbb{F}_2^n$, then π has at least one (non-trivial) component function that admits (nonzero) linear structures.*

Proof. For any given permutation π on $\mathbb{F}_2^n$, assume there exists a subspace E so that $\left(\pi^{-1}, E\right)$ satisfies the (C) property. Let $\{a_i\}_{i=1}^{2^d}$ be a set of coset representatives of E, and let $A_i = \pi^{-1}(a_i + E)$. Since π is a permutation and $\left(\pi^{-1}, E\right)$ has the (C) property, $\{\pi^{-1}(a_i+E)\}_{i=1}^{2^d} = \{A_i\}_{i=1}^{2^d}$ is a cover of $\mathbb{F}_2^n$ by $(n-d)$-dimensional affine subspaces. Now we apply Theorem 4.6.1 to the cover $\{A_i\}_{i=1}^{2^d}$, which implies that there exist a subspace $W \subset \mathbb{F}_2^n$ of dimension at least $n - 2^d(d-1) - 1 \geq 1$ and affine subspaces $B_i \subset \mathbb{F}_2^n$, $i \in \{1, 2, \ldots 2^d\}$, of dimension $n - d - \dim(W)$, such that $W + B_i = A_i$.

Take a basis $Q = \{e_1, e_2, \ldots e_{n-d}, r_1, \ldots, r_d\}$ of $\mathbb{F}_2^n$ such that $\{e_1, e_2, \ldots, e_{n-d}\}$ is a basis of E. Let $\{\pi_1, \pi_2, \ldots, \pi_n\}$ be the set of coordinate functions of π with respect to the basis Q, i.e. $\pi_i : \mathbb{F}_2^n \to \mathbb{F}_2$, for $i \in \{1, 2, \ldots, n\}$, are such that

$$\pi(x) = \pi_1(x)e_1 + \ldots + \pi_{n-d}(x)e_{n-d} + \pi_{n-d+1}(x)r_1 + \ldots + \pi_n(x)r_d, \text{ for all } x \in \mathbb{F}_2^n.$$

Take a nonzero element from W, and denote it by w. Take an arbitrary $x \in \mathbb{F}_2^n$, and fix it. Let $i_0 \in \{1, 2, \dots 2^d\}$ be such that $x \in A_{i_0} = W + B_{i_0}$. Then $x + w$ is in $W + B_{i_0}$ as well, since $w \in W$. This means that $\pi(x)$ and $\pi(x + w)$ are in the same coset of E, i.e. they are both in $a_{i_0} + E$, and so the sum $\pi(x+w)+\pi(x)$ is in E. But $\pi(x + w) + \pi(x) \in E$ implies $\pi_i(x + w) + \pi_i(x) = 0$ for $i \in \{n - d + 1, \dots, n\}$. Since x was an arbitrary element of $\mathbb{F}_2^n$, we conclude that w is a nonzero linear structure of π_i when $i \in \{n - d + 1, \dots, n\}$. ∎

Note that from the proof of Theorem 4.6.2, we can actually deduce that there exist at least 2^d component functions whose linear structure spaces have dimension at least $n - 2^d(d - 1) - 1$.

Chapter 5

Vectorial bent-negabent functions – their constructions and bounds

Recall that the *nega-Hadamard transform* of a Boolean function f in n variables, is defined by

$$\mathcal{N}_f(u) = \sum_{x \in \mathbb{F}_2^n} i^{wt(x)} (-1)^{f(x)+u \cdot x}, \text{ for all } u \in \mathbb{F}_2^n$$

where i is the imaginary unit, i.e. $i^2 = -1$. The Boolean bent functions whose nega-Hadamard transform is flat (i.e. $|\mathcal{N}_f(u)| = 2^{n/2}$ for all $u \in \mathbb{F}_2^n$), are called bent-negabent functions. They were introduced by C. Riera and M. Parker in [61], motivated by applications to quantum computing. The problem of constructing Boolean functions, which are simultaneously bent and negabent, was considered in [53, 65, 69, 71, 82]. There are several design methods of bent-negabent functions given in e.g. [65, 71, 82]. In [71], a set of necessary and sufficient conditions for a Boolean function to be negabent (regardless of the parity of the number of variables) was derived, which also allowed the design of a broader class of n-variable bent-negabent functions (n even) of algebraic degree ranging from 2 to $n/2$. M. Parker and A. Pott in [53] considered the problem of determining the number of quadratic bent-negabent functions in n variables. It was consequently resolved by A. Pott *et al.* [59], who used a characterization of bent-negabent Boolean functions, given by M. Parker and A. Pott in [53] (see Lemma 2.3.1). Bent-negabent functions have recently got a renewed attention due to the work in [70], where the connection between bent-negabent functions and Kerdock codes was established, and additionally recently in [40], where the (non-)existence of these objects within the Maiorana-McFarland class of bent functions was investigated.

Whenever a class of single-output Boolean functions had desirable algebraic or combinatorial properties, it was of a general interest to consider vectorial, i.e., multi-output versions of these functions (e.g. planar functions from p-ary bent functions and vectorial bent functions from Boolean bent functions [58]). So far, the bent-negabent property was only considered in the Boolean case and the possibility of building vector spaces of bent-negabent functions has not been addressed in the

literature. In this chapter, we introduce the notion of *vectorial bent-negabent* functions and show that in general for a vectorial bent-negabent function $F\colon \mathbb{F}_2^{2n} \to \mathbb{F}_2^k$ we necessarily have that $k \leq n-1$. We specify a class of vectorial bent-negabent functions with the maximal output dimension $n-1$ by using a set of linear complete mappings of cardinality $n-1$. We then show that the so-called b-complete mappings on $\mathbb{F}_{2^n}$ considered in e.g. [18], which are permutations $x + bF(x)$ for many $b \in \mathbb{F}_{2^n}$ can be used for the purpose of designing non-quadratic vectorial bent-negabent functions. Finally, in a similar fashion as it was done for the vectorial functions with the maximum number of bent components [60, 86], we derive an upper bound on the maximum number of bent-negabent components for mappings $F\colon \mathbb{F}_2^{2n} \to \mathbb{F}_2^k$, where $n \leq k \leq 2n$, and identify some families of these functions reaching this upper bound.

5.1 Vectorial bent-negabent functions

Let $m = 2n \geq 4$ and $\nu : \mathbb{F}_2^m \to \mathbb{F}_2$ be the (canonical) quadratic bent function defined as

$$\nu(x) = \sum_{i=1}^{n} x_i x_{n+i},$$

for all $x = (x_1, \ldots, x_m) \in \mathbb{F}_2^m$. It is well-known that the elementary symmetric quadratic Boolean function $s_2 : \mathbb{F}_2^m \to \mathbb{F}_2$, defined by

$$s_2(x) = \sum_{1 \leq i < j \leq m} x_i x_j, \quad \text{for all } x = (x_1, \ldots, x_m) \in \mathbb{F}_2^n,$$

is bent and that it is equivalent to the quadratic bent function ν, see [44]. More precisely, there exist $A \in GL(m, \mathbb{F}_2), b, u \in \mathbb{F}_2^m$, and $\epsilon \in \mathbb{F}_2$ such that

$$s_2(x) = \nu(xA + b) + u \cdot x + \epsilon. \tag{5.1}$$

Remark 2 *Since the bent-negabent property is, in general, not invariant under the action of $GL(m, \mathbb{F}_2)$, it is important to specify precisely the transformation of the input $x \mapsto xA + b$, which maps the dot-product bent function $\nu : \mathbb{F}_2^m \to \mathbb{F}_2$ to the bent-negabent function $s_2 : \mathbb{F}_2^m \to \mathbb{F}_2$, up to the addition of an affine function. Let $m = 2n$ and let $x = (x_1, \ldots, x_m)$. Now, starting with*

$$s_2(x) = \sum_{1 \leq i < j \leq m} x_i x_j = (x_1 + \sum_{\substack{1 \leq i \leq m \\ i \neq 1, n+1}} x_i)(x_{n+1} + \sum_{\substack{1 \leq i \leq m \\ i \neq 1, n+1}} x_i) + \sum_{\substack{1 \leq i \leq m \\ i \neq 1, n+1}} x_i + \sum_{\substack{1 \leq i < j \leq m \\ i, j \neq 1, n+1}} x_i x_j,$$

setting $x'_1 = (x_1 + \sum_{\substack{1 \leq i \leq m \\ i \neq 1, n+1}} x_i)$, $x'_{n+1} = (x_{n+1} + \sum_{\substack{1 \leq i \leq m \\ i \neq 1, n+1}} x_i)$, and repeating this process recursively, one gets $\nu(x') + L(x')$, where $L\colon \mathbb{F}_2^m \to \mathbb{F}_2$ is a linear function. In this way, without loss of generality, one can specify $b \in \mathbb{F}_2^m$ and $A \in GL(m, \mathbb{F}_2)$ in (5.1) *as follows. From the described above procedure, the matrix $A \in GL(m, \mathbb{F}_2)$ has the following block-form*

$$A = \left(\begin{array}{c|c} A_n^{\leq} & A_n^{<} \\ \hline A_n^{<} & A_n^{\leq} \end{array} \right), \tag{5.2}$$

where $A_n^{\leq} = (a_{i,j})_{i,j=1,\ldots,n}$ *with* $a_{i,j} = 1$ *if* $j \leq i$ *and* $a_{i,j} = 0$ *otherwise; similarly, we define* $A_n^{<} = (a_{i,j})_{i,j=1,\ldots,n}$ *with* $a_{i,j} = 1$ *if* $j < i$ *and* $a_{i,j} = 0$ *if* $j \geq i$. *Setting* $b = 0_m$, *we observe that* $\nu(xA) = s_2(x)$, *up to some linear terms.*

Finally, one can also observe that $AA = I_m$, *where* I_m *is the identity matrix of order* m. *In this way, the transformation* $x \mapsto xA$ *is an involution, and, hence* $s_2(xA) = \nu(x)$, *up to some linear terms. A concrete example of such transformation will be considered in more detail in Example 3.*

A construction of Boolean bent-negabent functions, based on the use of complete permutations, was addressed in [69].

Lemma 5.1.1 *[69] Let* $m = 2n$ *and* $s_2(x) = \nu(xA + b) + u \cdot x + \epsilon$ *for all* $x \in \mathbb{F}_2^m$, *where* $A \in GL(m, \mathbb{F}_2)$, $b, u \in \mathbb{F}_2^m$, $\epsilon \in \mathbb{F}_2$. *Suppose that* $f : \mathbb{F}_2^m \to \mathbb{F}_2$ *is a bent function such that* $f + \nu$ *is also a bent function. Then the function* $g : \mathbb{F}_2^m \to \mathbb{F}_2$ *defined by* $g(x) = f(xA + b)$ *is a bent-negabent function.*

The above condition, the requirement that $f + \nu$ is also bent, can be satisfied if one considers a special class of bent functions in the Maiorana-McFarland class, which uses a complete mapping in its definition, as shown in [69, Theorem 22]. A mapping $F\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is called *complete* if both $x \mapsto F(x)$ and $x \mapsto F(x) + x$ permute $\mathbb{F}_{2^n}$.

Proposition 5.1.2 *[69] Let* $m = 2n$ *and* π_F *denote the (complete) permutation on* $\mathbb{F}_2^n$ *induced by a complete mapping* $F(X) \in \mathbb{F}_{2^n}[X]$. *Let* $f_F : \mathbb{F}_2^m \to \mathbb{F}_2$ *be defined by*

$$f_F(x) = \pi_F(x_1, \ldots, x_n) \cdot (x_{n+1}, \ldots, x_n),$$

for all $x \in \mathbb{F}_2^m$. *Then the function* $f_F + \nu$ *on* $\mathbb{F}_2^m$ *is a Maiorana-McFarland bent function and the function* $g : \mathbb{F}_2^m \to \mathbb{F}_2$ *defined by* $g(x) = f_F(xA+b)$ *is bent-negabent, for some* $A \in GL(m, \mathbb{F}_2)$, $b \in \mathbb{F}_2^m$.

In addition, the use of complete mappings was also considered in [82] for the purpose of constructing bent-negabent functions outside the completed Maiorana-McFarland class.

Now we introduce the following formal definition of vectorial bent-negabent functions.

Definition 5.1.3 *For even* $m = 2n$, *a function* $F\colon \mathbb{F}_2^m \to \mathbb{F}_2^k$ *is called vectorial bent-negabent if its component functions* $\lambda \cdot F$ *are bent-negabent for all* $\lambda \in \mathbb{F}_2^k \setminus \{0_k\}$.

Notice that the upper bound on the output dimension $k \leq n$ comes from Nyberg's bound [50], since the nonzero component functions are bent. However, using the negabent condition, which involves the elementary symmetric quadratic bent function s_2, it is possible to deduce a sharper bound.

Proposition 5.1.4 *Let* $m = 2n$. *If* $F\colon \mathbb{F}_2^m \to \mathbb{F}_2^k$ *is a vectorial bent-negabent function, then* $k \leq n - 1$.

Proof. Since F is vectorial bent then $k \leq n$. On the other hand, assuming that $k = n$, the property of being negabent implies that for any $\lambda \in \mathbb{F}_2^k$, the Boolean functions defined by $x \in \mathbb{F}_2^m \mapsto \lambda \cdot F(x) + s_2(x)$ are also bent. This would imply the possibility of defining a vectorial bent function $G\colon \mathbb{F}_2^m \to \mathbb{F}_2^{n+1}$ with coordinate functions $G(x) = (f_1(x), \ldots, f_n(x), s_2(x))$, which then violates the Nyberg's bound. Hence, we have that $k \leq n - 1$. ∎

5.2 Vectorial bent-negabent functions of maximal output dimension

As already mentioned, in [69], the authors used complete mappings to specify bent-negabent functions. We now show that a set of linear complete mappings can be used for constructing vectorial bent-negabent functions with the maximal output dimension. On the other hand, these functions are in the Maiorana-McFarland class and their component functions are always quadratic. However, similarly to adding arbitrary $\rho(y)$ in the definition of $f(x,y) = \pi(y)\cdot x + \rho(y)$, the degree and cardinality of this class can be extended significantly.

Theorem 5.2.1 *Let $m = 2n$ and let $\pi_1, \ldots, \pi_k$ be linearly independent permutations of $\mathbb{F}_2^n$ such that any nonzero $\pi \in \langle \pi_1, \ldots, \pi_k \rangle$ is a complete permutation of $\mathbb{F}_2^n$. Let also $\rho_1, \ldots, \rho_k$ be arbitrary Boolean functions on $\mathbb{F}_2^n$. Define the vectorial bent function $F\colon \mathbb{F}_2^m \to \mathbb{F}_2^k$ in the following way*

$$F(x) = F(x_1, \ldots, x_m) = \begin{bmatrix} (x_1, \ldots, x_n) \cdot \pi_1(x_{n+1}, \ldots, x_m) + \rho_1(x_{n+1}, \ldots, x_m) \\ \vdots \\ (x_1, \ldots, x_n) \cdot \pi_k(x_{n+1}, \ldots, x_m) + \rho_k(x_{n+1}, \ldots, x_m) \end{bmatrix}.$$

Suppose that $s_2(x) = \nu(xA + b) + u \cdot x + \epsilon$ for all $x \in \mathbb{F}_2^m$, where $A \in GL(m, \mathbb{F}_2)$, $b, u \in \mathbb{F}_2^m$, $\epsilon \in \mathbb{F}_2$. Then, the function $G\colon \mathbb{F}_2^m \to \mathbb{F}_2^k$ defined by

$$G(x) = F(xA + b)$$

is a vectorial bent-negabent function.

Proof. It is enough to show that any nonzero component function of G is negabent, since the transformation $x \mapsto xA + b$ preserves bentness. Let f be a nonzero component function of F, i.e.,

$$f(x_1, \ldots, x_m) = (x_1, \ldots, x_n) \cdot \pi(x_{n+1}, \ldots, x_m) + \rho(x_{n+1}, \ldots, x_m),$$

where for any nonzero $(\alpha_1, \ldots, \alpha_k) \in \mathbb{F}_2^k$ the mapping $\pi := \sum_{i=1}^k \alpha_i \pi_i$ is a complete permutation of $\mathbb{F}_2^n$ and $\rho := \sum_{i=1}^k \alpha_i \rho_i$ is a Boolean function on $\mathbb{F}_2^n$. Clearly, the function g on $\mathbb{F}_2^m$ defined by $g(x) := f(xA + b)$ is a component function of G.

Consider now the Boolean function f' on $\mathbb{F}_2^n \times \mathbb{F}_2^n$ defined by

$$f'(x_1, \ldots, x_m) = (x_1, \ldots, x_n) \cdot \pi'(x_{n+1}, \ldots, x_m) + \rho(x_{n+1}, \ldots, x_m) = f(x) + \nu(x),$$

where $\pi'(v) = \pi(v) + v$, for all $v \in \mathbb{F}_2^n$. We know that π' is a permutation, since π is complete, and hence f' is bent. Applying the transformation $x \mapsto xA + b$ to the input of f', we get

$$f'(xA + b) = f(xA + b) + \nu(xA + b) = g(x) + s_2(x) + u \cdot x + \epsilon.$$

By Lemma 2.3.1, we get that g is bent-negabent, since $g(x) + s_2(x) = f'(xA + b) + u \cdot x + \epsilon$ is a bent function. Since an arbitrary nonzero component function g of G is bent-negabent, we conclude that G is a vectorial bent-negabent function. ∎

Remark 3 *To preserve the negabent property of the component functions one can use different subgroups of the general linear group $GL(m, \mathbb{F}_2)$. For instance, the use of the subgroup of orthogonal matrices $O(m, \mathbb{F}_2)$ was first proposed in [65] and recently a subgroup of $GL(m, \mathbb{F}_2)$ of the so-called weight preserving transformations was identified in [70].*

In the following theorem, we consider linear permutations π_i in order to obtain vectorial bent-negabent functions whose output dimension is maximal.

Theorem 5.2.2 *Let $\alpha_1, \alpha_2, \ldots, \alpha_{n-1}$ be a set of linearly independent elements in $\mathbb{F}_{2^n}$ (over $\mathbb{F}_2$), whose span does not contain the element $1 \in \mathbb{F}_{2^n}$. Let π_i be the permutations of $\mathbb{F}_{2^n}$ for $i = 1, \ldots, n-1$ defined by $\pi_i \colon y \in \mathbb{F}_{2^n} \mapsto \alpha_i y$. Define the coordinate functions $f_i \colon \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2$ as $f_i(x, y) = x \cdot \pi_i(y) + \rho_i(y)$, where $\rho_i : \mathbb{F}_2^n \to \mathbb{F}_2$ are arbitrary. Then, the function $F = (f_1, \ldots, f_{n-1})$ is affine equivalent to a vectorial bent-negabent function whose output dimension is maximal.*

Proof. The proof follows immediately from Theorem 5.2.1, since the nonzero binary linear combinations of $\pi_i(y)$ are complete mappings. ∎

Example 3 *Let $m = 2n$ and $n = 4$. The polynomial $x^4 + x + 1$ is irreducible over $\mathbb{F}_2$, hence we can represent $\mathbb{F}_{2^4}$ as $\mathbb{F}_2(a)$ where $a^4 + a + 1 = 0$. Then, the set $B = \{1, a, a^2, a^3\}$ is a basis for $\mathbb{F}_{2^4}$ over $\mathbb{F}_2$, and consequently, the span of $\{a, a^2, a^3\}$ does not contain 1. Set $\alpha_1 = a$, $\alpha_2 = a^2$ and $\alpha_3 = a^3$ in Theorem 5.2.2 and, for simplicity, let $\rho_1(y) = \rho_2(y) = \rho_3(y) = 0$, for all $y \in \mathbb{F}_{2^4}$. From Theorem 5.2.2, we deduce that the function $F = (f_1, f_2, f_3)$ (using the same notation as in Theorem 5.2.2), is a function affine equivalent to a vectorial bent-negabent function whose output dimension is maximal. Identifying $\mathbb{F}_{2^4}$ and $\mathbb{F}_2^4$ via the isomorphism (of vector spaces) sending 1 in $\mathbb{F}_{2^4}$ to $(1,0,0,0)$ in $\mathbb{F}_2^4$, a to $(0,1,0,0)$, a^2 to $(0,0,1,0)$, and a^3 to $(0,0,0,1)$, we get the following algebraic normal form of F:*

$$F(x_1, \ldots, x_8) = \begin{bmatrix} x_1x_8 + x_2x_5 + x_2x_8 + x_3x_6 + x_4x_7 \\ x_1x_7 + x_2x_7 + x_2x_8 + x_3x_5 + x_3x_8 + x_4x_6 \\ x_1x_6 + x_2x_6 + x_2x_7 + x_3x_7 + x_3x_8 + x_4x_5 + x_4x_8 \end{bmatrix},$$

for all $(x_1, \ldots, x_8) \in \mathbb{F}_2^8$. More precisely, we get that $G \colon \mathbb{F}_2^8 \to \mathbb{F}_2^3$, defined by

$$G(x_1, \ldots, x_8) = \begin{bmatrix} g_1(x_1, \ldots, x_8) \\ g_2(x_1, \ldots, x_8) \\ g_3(x_1, \ldots, x_8) \end{bmatrix} = F((x_1, \ldots, x_8)A)$$

for all $(x_1, \ldots, x_8) \in \mathbb{F}_2^8$, where $A \in GL(8, \mathbb{F}_2)$ is defined as in Remark 2, is a vectorial bent-negabent function whose output dimension is maximal. The algebraic normal forms of the functions g_1, g_2 and g_3 are given as follows:

$$\begin{aligned} g_1(x_1, \ldots, x_8) &= x_1x_8 + x_2x_5 + x_2x_6 + x_2 + x_3x_5 + x_3x_7 + x_4x_5 + x_4x_8 + x_4 + x_5x_7 \\ &\quad + x_5x_8 + x_6x_7 + x_6x_8 + x_7x_8 + x_7, \\ g_2(x_1, \ldots, x_8) &= x_1x_4 + x_1x_7 + x_1x_8 + x_2x_3 + x_2x_4 + x_3x_4 + x_3x_5 + x_3x_6 + x_3x_7 \\ &\quad + x_3 + x_4x_5 + x_4x_6 + x_4x_8 + x_5x_8 + x_6x_7 + x_8, \\ g_3(x_1, \ldots, x_8) &= x_1x_3 + x_1x_4 + x_1x_6 + x_1x_7 + x_1x_8 + x_2x_7 + x_2x_8 + x_3x_4 + x_3x_6 \\ &\quad + x_3x_8 + x_4x_5 + x_4x_8 + x_4 + x_6x_7 + x_6x_8 + x_6 + x_7x_8 + x_7 + x_8. \end{aligned}$$

5.3 Complete mappings from linear translators

Several methods of constructing permutations using the notion of linear translators were considered in the literature, e.g. in [18, 36], whereas a nice survey on this framework is given by Hou in [29]. This concept was further generalized by Akbary, Ghioca and Wang who unified the Kyureghyan's construction [36] 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 [49, Theorem 8.1.39].

For our purpose, we consider the so-called b-complete mappings whose definition is as follows.

Definition 5.3.1 *[18] A mapping $h\colon \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}$ is called complete with respect to $b \in \mathbb{F}_{p^k}$, or b-complete, when both $x \mapsto h(x)$ and $x \mapsto x + bh(x)$ permute $\mathbb{F}_{p^k}$.*

In [74, Theorem 4], a class of permutation trinomials, which are 1-complete mappings over $\mathbb{F}_{2^{3r}}$, was proposed. Below we give a slightly reformulated version of [74, Theorem 4].

Theorem 5.3.2 *[74] For any $\beta \in \mathbb{F}_{2^r} \setminus \{0, 1\}$, the trinomial*

$$h(x) = x^{2^{2r}+1} + x^{2^r+1} + \beta x$$

is complete over $\mathbb{F}_{2^{3r}}$ with respect to any $b \in \mathbb{F}_{2^r} \setminus \{0, \beta^{-1}\}$. Thus, both $x \mapsto h(x)$ and $x \mapsto x + bh(x)$ are permutations for $b \in \mathbb{F}_{2^r} \setminus \{0, \beta^{-1}\}$.

Now we can use Theorem 5.3.2 to construct vectorial bent-negabent functions. Note that permutations in Theorem 5.3.2 are quadratic, hence the following result is an improvement over Theorem 5.2.2, where the used permutations are linear.

Theorem 5.3.3 *Let $m = 2n$ and let n, r be positive integers such that $n = 3r$. Let β be an element of $\mathbb{F}_{2^r} \setminus \{0, 1\}$. Let $b_1, \ldots, b_{r-1} \in \mathbb{F}_{2^r}$ be such that $\{\beta^{-1}, b_1, \ldots, b_{r-1}\}$ is a set of linearly independent elements in $\mathbb{F}_{2^r}$ over $\mathbb{F}_2$. Let $h(y) = y^{2^{2r}+1} + y^{2^r+1} + \beta y$, for all $y \in \mathbb{F}_{2^n}$ and let also $\rho_1, \ldots, \rho_{r-1}$ be arbitrary Boolean functions on $\mathbb{F}_{2^n}$. Then the function $F\colon \mathbb{F}_2^n \times \mathbb{F}_{2^n} \to \mathbb{F}_2^{r-1}$ defined by*

$$F(x, y) = \begin{bmatrix} x \cdot b_1 h(y) + \rho_1(y) \\ \vdots \\ x \cdot b_{r-1} h(y) + \rho_{r-1}(y) \end{bmatrix},$$

for all $x \in \mathbb{F}_2^n$, $y \in \mathbb{F}_{2^n}$, is affine equivalent to a vectorial bent-negabent function.

Proof. Let S be a non-empty subset of $\{1, 2, \ldots, r-1\}$. Since $\{\beta^{-1}, b_1, \ldots, b_{r-1}\}$ is a set of linearly independent elements, $\sum_{i \in S} b_i \neq 0$, and since from Theorem 5.3.2 we know that $y \mapsto h(y)$ is a permutation, we can conclude that $y \mapsto (\sum_{i \in S} b_i) h(y)$ is a permutation of $\mathbb{F}_{2^n}$ and so the function $(x, y) \mapsto \sum_{i \in S} (x \cdot b_i h(y) + \rho_i(y))$ is a bent function on $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ in the $\mathcal{M}$ class. We conclude that F is a vectorial bent function.

To prove that F is affine equivalent to a negabent function, we will prove that the Boolean function $(x, y) \mapsto \sum_{i \in S} (x \cdot b_i h(y) + \rho_i(y)) + x \cdot y$ on $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ is also bent. First, we notice that $\sum_{i \in S} (x \cdot b_i h(y) + \rho_i(y)) + x \cdot y = x \cdot ((\sum_{i \in S} b_i) h(y) + y) + \sum_{i \in S} \rho_i(y)$. Since $\{\beta^{-1}, b_1, \ldots, b_{r-1}\}$ is a set of linearly independent elements, we have that $\sum_{i \in S} b_i \in \mathbb{F}_{2^r} \setminus \{0, \beta^{-1}\}$, and from Theorem 5.3.2 we deduce that the mapping $y \mapsto (\sum_{i \in S} b_i) h(y) + y$ is a permutation of $\mathbb{F}_{2^n}$. Hence, $(x, y) \mapsto \sum_{i \in S} (x \cdot b_i h(y) + \rho_i(y)) + x \cdot y$ is a bent function on $\mathbb{F}_2^n \times \mathbb{F}_2^n$ inside the $\mathcal{M}$ class. Denote by g the quadratic Boolean bent function $(x, y) \mapsto x \cdot y$ on $\mathbb{F}_2^m$, which we identify with $\mathbb{F}_2^n \times \mathbb{F}_2^n$. Since all quadratic bent functions are affine equivalent, there exist an invertible $m \times m$ matrix A, a vector $w \in \mathbb{F}_2^m$ and an affine Boolean function $L \colon \mathbb{F}_2^m \to \mathbb{F}_2$, such that $s_2(x, y) = g((x, y)A + w) + L(x, y)$. Since addition of affine functions does not affect bent-negabentness, we conclude that $F((x, y)A + w)$ is a vectorial bent-negabent function. ∎

Example 4 *Set $r = 3$ and $n = 3r = 9$. The polynomial $x^9 + x^4 + 1$ is irreducible over $\mathbb{F}_2$, hence we can represent $\mathbb{F}_{2^9}$ as $\mathbb{F}_2(a)$, where $a^9 + a^4 + 1 = 0$. The set $B = \{1, a, \ldots, a^8\}$ is a basis of $\mathbb{F}_{2^9}$ over $\mathbb{F}_2$. Set $b_1 = 1$, $b_2 = a^4 + a^3 + a^2$ and $b_3 = \beta^{-1} = a^8 + a^6 + a^3 + a^2 + 1$. Because $b_i^{2^3} - b_i = 0$, for $i \in \{1, 2, 3\}$, and because b_1, b_2, and b_3 are linearly independent over $\mathbb{F}_2$ we deduce that $\mathbb{F}_{2^3}$ is given by $\langle b_1, b_2, b_3 \rangle$. We compute $\beta = b_3^{-1} = a^8 + a^6 + a^4$. Set $\rho_1(y) = \rho_2(y) = 0$ and $h(y) = y^{65} + y^9 + \left(a^8 + a^6 + a^4\right) y$, for all $y \in \mathbb{F}_{2^9}$. Then, from Theorem 5.3.3, we deduce that the function defined as*

$$F(x, y) = \begin{bmatrix} x \cdot b_1 h(y) \\ x \cdot b_2 h(y) \end{bmatrix},$$

for all $(x, y) \in \mathbb{F}_2^{18}$, is a function affine equivalent to a bent-negabent function. More precisely, we get that $G \colon \mathbb{F}_2^{18} \to \mathbb{F}_2^2$, defined by $G(x_1, \ldots, x_{18}) = F((x_1, \ldots, x_{18})A)$, for all $(x_1, \ldots, x_{18}) \in \mathbb{F}_2^{18}$, where $A \in GL(18, \mathbb{F}_2)$ is defined as in Remark 2, is a bent-negabent function.

All component functions of vectorial bent-negabent functions $F \colon \mathbb{F}_2^{3r} \times \mathbb{F}_{2^{3r}} \to \mathbb{F}_2^{r-1}$ constructed in Theorem 5.3.3 belong to the $\mathcal{M}^\#$ class. Moreover, the dimension of the output space of these vectorial bent-negabent functions, being equal to $r - 1$, is quite small compared to the maximal dimension, which is $3r - 1$ according to Proposition 5.1.4.

5.4 Maximum number of bent-negabent components

The problem of specifying functions $F \colon \mathbb{F}_2^m \to \mathbb{F}_2^m$, for even $m = 2n$, which contain the maximum number of bent components (MNBC functions) was originally considered in [60]. It was shown that this number equals to $2^m - 2^n$ and this result was later generalized to mappings $F \colon \mathbb{F}_2^m \to \mathbb{F}_2^k$ with $n + 1 \leq k \leq 2n$, whose maximal number of bent components is then $2^k - 2^{k-n}$, see [86]. Nevertheless, for vectorial functions with the maximum number of bent-negabent components the situation is slightly different. First, we recall the following result used in deriving the upper bound on the maximum number of bent components of functions $F \colon \mathbb{F}_2^m \to \mathbb{F}_2^m$.

Lemma 5.4.1 *[60, Corollary 1] A set S of elements in $\mathbb{F}_2^m \setminus \{0_m\}$ meeting all $(m+1-k)$-dimensional subspaces of $\mathbb{F}_2^m$ has at least 2^k-1 elements with equality if and only if $S \cup \{0_m\}$ is a k-dimensional subspace of $\mathbb{F}_2^m$.*

The correspondence to bent-negabent functions is as follows.

Theorem 5.4.2 *Let $m = 2n$, $k \geq n-1$ and let $F\colon \mathbb{F}_2^m \to \mathbb{F}_2^k$ be arbitrary. Define*

$$S := \{\lambda \in \mathbb{F}_2^k\colon F_\lambda = \lambda \cdot F \text{ is not bent-negabent}\}.$$

Then, $|S| \geq 2^{k-n+1}$ with equality if and only if S is a linear subspace of dimension $k-n+1$.

Proof. The case $k = n-1$ is trivial, since $0_k \in S$. Now, we assume that $k > n-1$. If $|S| < 2^{k-n+1}$, then there are at most $2^{k-n+1}-2$ nonzero elements $\lambda \in \mathbb{F}_2^k$ for which F_λ is not bent-negabent. Due to Lemma 5.4.1, this set cannot meet all subspaces of dimension $k+1-(k-n+1) = n$. In this way, there must be at least one subspace T of dimension n disjoint from $S \setminus \{0_k\}$. This shows that there is an n-dimensional subspace $T \subseteq \{\lambda \in \mathbb{F}_2^k\colon F_\lambda \text{ is bent-negabent}\} \cup \{0_k\}$, that is, there is a vectorial bent-negabent function from $\mathbb{F}_2^m$ to $\mathbb{F}_2^n$, which is impossible due to the bound in Proposition 5.1.4. ∎

Similarly to the MNBC case, there exists a trivial construction of vectorial Boolean functions with the maximum number of bent-negabent components due to the invariance of negabent property under addition of affine functions. In the following theorem and in the sequel, we consider $F\colon \mathbb{F}_2^m \to \mathbb{F}_2^k$, where $m = 2n$ and $k > n-1$, since the case $k \leq n-1$ corresponds to vectorial bent-negabent functions.

Theorem 5.4.3 *Let $m = 2n$, $k > n-1$ and $\mathbb{F}_2^k = \mathbb{F}_2^{n-1} \times \mathbb{F}_2^{k-n+1}$. Let $F\colon \mathbb{F}_2^m \to \mathbb{F}_2^k$ be a function defined by $F(x,y) = (B(x,y), A(x,y))$, where $x, y \in \mathbb{F}_2^n$ and $A\colon \mathbb{F}_2^m \to \mathbb{F}_2^{k-n+1}$ is an affine function. If B is vectorial bent-negabent, then the component function defined by $(x,y) \mapsto u \cdot B(x,y) + v \cdot A(x,y)$ is bent-negabent function for all $u \in \mathbb{F}_2^{n-1} \setminus \{0_{n-1}\}, v \in \mathbb{F}_2^{k-n+1}$. Hence, F has $2^k - 2^{k-n+1}$ component functions which are bent-negabent.*

Proof. For any nonzero $u \in \mathbb{F}_2^{n-1}$ and any $v \in \mathbb{F}_2^{k-n+1}$, the component function defined by $(x,y) \mapsto u \cdot B(x,y) + v \cdot A(x,y)$ is bent-negabent since B is vectorial bent-negabent, and for a Boolean bent-negabent function f on $\mathbb{F}_2^m$ the function $f+l$ is again bent-negabent for any affine function $l : \mathbb{F}_2^m \to \mathbb{F}_2$, see [53, Lemma 2]. Thus, there are $(2^{n-1}-1)\cdot 2^{k-n+1} = 2^k - 2^{k-n+1}$ bent-negabent component functions of F. ∎

Theorem 5.4.4 *Let $m = 2n$ and $k > n-1$. Let $\alpha_1, \alpha_2, \ldots, \alpha_{n-1}$ be a set of linearly independent elements in $\mathbb{F}_{2^n}$ (over $\mathbb{F}_2$), whose span does not contain the element $1 \in \mathbb{F}_{2^n}$. Let $\pi_i(y) = \alpha_i y$ be permutations of $\mathbb{F}_{2^n}$ for $i = 1, \ldots, n-1$. Let*

$F\colon \mathbb{F}_2^m \to \mathbb{F}_2^k$ be a vectorial function defined by

$$F(x,y) = \begin{bmatrix} f_1(x,y) \\ \vdots \\ f_{n-1}(x,y) \\ f_n(x,y) \\ \vdots \\ f_k(x,y) \end{bmatrix} = \begin{bmatrix} x \cdot \pi_1(y) + \rho_1(y) \\ \vdots \\ x \cdot \pi_{n-1}(y) + \rho_{n-1}(y) \\ \rho_n(y) \\ \vdots \\ \rho_k(y) \end{bmatrix}, \tag{5.3}$$

where functions $\rho_i\colon \mathbb{F}_2^n \to \mathbb{F}_2$ for $i = 1, \ldots, k$ are arbitrary. Then the function $F\colon \mathbb{F}_2^m \to \mathbb{F}_2^k$ is affine equivalent to a vectorial function with the maximum number of bent-negabent components.

Proof. By Theorem 5.2.2, the function $F'\colon \mathbb{F}_2^m \to \mathbb{F}_2^{n-1}$ given by $F' = (f_1, \ldots, f_{n-1})$ is equivalent to a vectorial bent-negabent function with the maximum output dimension, because all nonzero binary linear combinations of $\pi_i(y)$ are complete mappings. Since any nonzero function $f \in \langle f_1, \ldots, f_{n-1} \rangle$ is a Maiorana-McFarland bent function, which is equivalent to a bent-negabent function, we get that any function from the coset $f + \langle \rho_n, \ldots, \rho_k \rangle$ is again a Maiorana-McFarland bent function, equivalent to a bent-negabent function using the same transformation $x \mapsto xA + b$ as in Theorem 5.2.1. In total, we have $2^k - 2^{k-n+1}$ bent-negabent components, which is the maximum number. ∎

Remark 4 *Recently, based on the classification of vectorial bent functions in six variables [57], all MNBC functions in $m = 6$ variables have been classified in [3] as well. Since all MNBC functions $F\colon \mathbb{F}_2^6 \to \mathbb{F}_2^6$ are equivalent to the Maiorana-McFarland construction [3, Proposition 1], and vectorial functions $F\colon \mathbb{F}_2^6 \to \mathbb{F}_2^5$ with the maximum number of bent-negabent components are affine equivalent to MNBC functions with at least one quadratic coordinate function, we deduce that all functions $F\colon \mathbb{F}_2^6 \to \mathbb{F}_2^5$ with the maximum number of bent-negabent components are described up to equivalence, by construction* (5.3) *in Theorem 5.4.4.*

Chapter 6

Vectorial bent functions weakly/strongly outside $\mathcal{M}^{\#}$

In order to describe the properties of vectorial bent functions (related to the class inclusion/exclusion problem) more precisely, in this chapter we introduce the concept of *weakly* and *strongly* outside a given class of bent functions (which is fixed to be $\mathcal{M}^{\#}$ in this chapter). The main reason for establishing this concept is to emphasize the difference between the standard $\mathcal{M}$ class whose vectorial bent functions have the property that all nonzero linear combinations (components) of its coordinate functions are bent functions in $\mathcal{M}$ (the same applies to vectorial bent functions in $\mathcal{PS}_{ap}$). This is, in general, not true for vectorial functions having its coordinates in $\mathcal{C}$ or $\mathcal{D}$ since most of the methods presented in this chapter provide component bent functions that do not stem from a single bent class. Another reason for being interested in the property of being weakly or strongly outside $\mathcal{M}^{\#}$ relates to the fact that in the previous chapters (also in [84]) certain infinite classes of bent functions in $\mathcal{C}$ and $\mathcal{D}$, but provably outside $\mathcal{M}^{\#}$, have been specified. Then, employing such functions as initial bent functions gives vectorial bent spaces whose certain components are in the primary class $\mathcal{M}$, whereas the remaining ones belong to $\mathcal{C}$ or $\mathcal{D}$ and are provably outside the $\mathcal{M}^{\#}$ class.

First, in Section 6.1.1 we show that the subclass $\mathcal{D}_0$ can be extended to its vectorial counterpart, to get vectorial bent functions with the maximal output dimension weakly outside the $\mathcal{M}^{\#}$ class. Then, in Section 6.1.2 we show that similar extension related to another explicit subclass of $\mathcal{D}$, called $\mathcal{D}_2^{\star}$, becomes harder unless an additional structure on the permutations and corresponding subspaces is imposed. More precisely, one can specify $f_1(x,y) = \pi_1^{\star}(y) \cdot x + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y)$ for $x, y \in \mathbb{F}_2^n$, for a suitable permutation $\pi_1^{\star}$ on $\mathbb{F}_2^n$ and a certain 2-dimensional subspace E_1 of $\mathbb{F}_2^n$ such that $\pi_1^{\star}(E_2) = E_1^{\perp}$. This defines a bent function $f_1 \in \mathcal{D}_2^{\star}$ which is provably outside $\mathcal{M}^{\#}$. Then, defining another bent function in this class, say $f_2(x,y) = \pi_2^{\star}(y) \cdot x + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y)$, we must ensure that $\pi_2^{\star}(E_2) = E_1^{\perp}$ as well (which is the (D) property) and furthermore $\pi_1^{\star} + \pi_2^{\star}$ must be a permutation so that $f_1 + f_2$ is bent. These conditions become hard and therefore we restrict ourselves to consider a special relationship between the permutations π_i so that all of them are of the form $\alpha_i \pi$, for suitably chosen $\alpha_i \in \mathbb{F}_{2^n}$ and a permutation π on $\mathbb{F}_2^n$. This

will ensure that the linear combinations $\sum_i \alpha_i \pi_i$ are permutations as well, and more importantly the condition that $(\sum_i \alpha_i \pi_i)(E_2) = E_1^{\perp}$ is then more easily handled.

Whereas in Section 6.1 we provide design methods which do not intrinsically ensure the weakly/strongly outside property (though in certain cases this may be achieved), similar approaches are used in a more refined manner in Section 6.2, to specify vectorial bent functions weakly outside $\mathcal{M}^{\#}$ again stemming from class $\mathcal{D}$. To achieve this, we propose the use of a class of complete mappings and demonstrate how vectorial bent functions weakly outside $\mathcal{M}^{\#}$ can be built assuming the existence of such permutations (at least when the output bent dimension is small). Alternatively, an explicit class of trinomial permutations given in [27] is utilized for the same purpose of defining bent functions weakly outside $\mathcal{M}^{\#}$. We emphasize that possibly many other classes of permutations are suitable to be used in the design (those whose component functions do not admit linear structures and permute a desired subfield) but we do not investigate this issue further.

In Section 6.3 we combine the notion of weakly outside the $\mathcal{M}^{\#}$ class and the notion of vectorial bent-negabent functions introduced in Chapter 5. Namely, using a suitable decomposition of the vector space (alternatively identifying suitable subfields) we provide a generic method of specifying vector spaces of complete mappings which are then efficiently used to specify vectorial bent-negabent functions weakly outside the $\mathcal{M}^{\#}$ class (having approximately half of the component functions outside the completed $\mathcal{M}$ class) .

The problem of specifying vectorial functions which are strictly outside the completed class $\mathcal{M}^{\#}$ is quite delicate, along with the question whether these functions can be extended to the maximal output bent dimension (being n for the input space of size $2n$). In this direction, in Section 6.4, we provide a construction of vectorial bent functions $F : \mathbb{F}_2^{2n} \to \mathbb{F}_2^d$, derived from the $\mathcal{C}$ class, which are strongly outside $\mathcal{M}^{\#}$, for some output dimensions d (though not for the the maximal one).

6.1 Vectorial bent functions derived from the class $\mathcal{D}$

The notion of vectorial bent functions $F : \mathbb{F}_2^{2n} \to \mathbb{F}_2^k$ refers to a collection of $k \leq n$ Boolean bent functions $f_1, \ldots, f_k : \mathbb{F}_2^{2n} \to \mathbb{F}_2$ with the property that each nonzero linear combination (over $\mathbb{F}_2$) of these functions is bent. We introduce the concept of vectorial bent functions which are *weakly* or *strongly* outside a given class of bent functions as follows.

Definition 2.2.2 *A vectorial bent function $F : \mathbb{F}_2^{2n} \to \mathbb{F}_2^k$, with $k \leq n$, is* weakly outside *of a class of bent functions if there is at least one (nonzero) component function of F (linear combination of its coordinate functions) which does not belong to the considered class. If all component functions of F do not belong to a class of bent functions then F is* strongly outside *the considered class.*

Notice that the primary class of Boolean bent functions $\mathcal{M}$ is easily extendable to its vectorial counterpart having maximum output dimension. Thus, instead of considering the Boolean case $f(x, y) = \pi(y) \cdot x + g(y)$, where $x, y \in \mathbb{F}_2^n$, one can easily show that $F(x, y) = \pi(y)x + G(y)$, considered as a mapping from $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_{2^k}$,

is a vectorial bent function. The same reasoning applies to the $\mathcal{PS}_{ap}$ class, see for instance [12].

In what follows, we show the existence of vectorial bent functions in $\mathcal{D}$ which are weakly outside $\mathcal{M}^{\#}$. The property of being weakly outside is essentially achieved by selecting a suitable bent function which is outside $\mathcal{M}^{\#}$ and specifying other coordinate bent functions so that the components are all bent (but not necessarily outside $\mathcal{M}^{\#}$).

6.1.1 Vectorial bent functions of maximal dimension from $\mathcal{D}_0$

We now investigate the existence of vectorial bent functions $F : \mathbb{F}_2^{2n} \to \mathbb{F}_2^n$ of maximal output dimension stemming from the $\mathcal{D}_0$ class. One should remark however that the problem of extending the secondary classes $\mathcal{C}$ and $\mathcal{D}$ to a vectorial case is difficult in general. A straightforward approach, as in the case of the $\mathcal{M}$ class cannot always be applied. In particular, when extension to a full output dimension is possible then commonly the resulting vectorial bent function contains component functions which do not belong to the same class.

Theorem 6.1.1 *Let $f_0(x, y) = \pi(y) \cdot x + \prod_{j=1}^{n}(x_j + 1)$, with $x, y \in \mathbb{F}_2^n$, be a bent function in $\mathcal{D}_0$ outside $\mathcal{M}^{\#}$ (or $\mathcal{PS}^{\#}$), and let $\{\alpha_0, \ldots, \alpha_{n-1}\}$ be a set of linearly independent elements in $\mathbb{F}_{2^n}$ (over $\mathbb{F}_2$), with $\alpha_0 = 1$. Define n permutations of $\mathbb{F}_{2^n}$ as $\pi_i(y) = \alpha_i\pi(y)$ for $i = 0, \ldots, n-1$. Then, $F = (f_0, \ldots, f_{n-1})$, where $f_i(x, y) = \alpha_i\pi(y) \cdot x + \prod_{j=1}^{n}(x_j + 1)$, is a vectorial bent function weakly outside $\mathcal{M}^{\#}$ (or $\mathcal{PS}^{\#}$).*

Proof. Clearly, each function f_i is in $\mathcal{D}_0$. Their linear combinations $f_a = a_0 f_0 + \cdots + a_{n-1} f_{n-1}$, with $a_i \in \mathbb{F}_2$, are of the form

$$f_a(x, y) = (\sum_{i=0}^{n-1} a_i\alpha_i)\pi(y) \cdot x + (\sum_{i=0}^{n-1} a_i) \prod_{j=1}^{n}(x_j + 1).$$

Thus, when the Hamming weight of $a = (a_0, \ldots, a_{n-1})$ is odd, the function f_a is a bent function in $\mathcal{D}_0$ since the term $\prod_{j=1}^{n}(x_j + 1)$ is not cancelled. Otherwise, if the weight of $(a_0, \ldots, a_{n-1})$ is even f_a is in $\mathcal{M}$. Consequently, since f_0 is a bent function outside $\mathcal{M}^{\#}$ (or $\mathcal{PS}^{\#}$), the function $F = (f_0, \ldots, f_{n-1})$ is a vectorial bent function weakly outside $\mathcal{M}^{\#}$ (or $\mathcal{PS}^{\#}$). ∎

For the details of switching between the vector space and finite field representation, especially when $\alpha\pi(y)$ is considered, we refer to Example 5. More precisely, one can use the trace representation and define coordinate functions $f_i : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \to \mathbb{F}_2$ (components as well) as $f_i(x, y) = Tr_1^n(\alpha_i\pi(y)x) + Tr_1^n(\gamma(x^{2^n-1}+1))$, where $\gamma \in \mathbb{F}_{2^n}$ is such that $Tr_1^n(\gamma) = 1$, hence the last term describes the delta function $\prod_{i=1}^{n}(x_i+1)$.

To provide classes of vectorial bent functions which are weakly or strongly outside $\mathcal{M}^{\#}$, which is treated in Sections 6.2 and 6.4, we will rely on the following set of sufficient conditions derived in [83].

Theorem 6.1.2 *[83] Let $m = 2n > 6$ be an even integer and let $f(x, y) = \pi(y) \cdot x + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y)$, where π is a permutation of $\mathbb{F}_2^n$, and E_1, E_2 are two linear subspaces of $\mathbb{F}_2^n$ such that $\pi(E_2) = E_1^{\perp}$. If (E_1, E_2, π) satisfies:*

1. $\dim(E_1) \geq 2$ *and* $\dim(E_2) \geq 2$;

2. $u \cdot \pi$ *has no nonzero linear structure for all* $u \in \mathbb{F}_2^n \backslash \{0_n\}$;

3. $\deg(\pi) \leq n - \dim(E_2)$,

then f *is a bent function in* $\mathcal{D}$ *and it does not belong to* $\mathcal{M}^{\#}$.

Notice that the above conditions are not necessary which is justified by noting that the class $\mathcal{D}_0$ contains functions provably outside $\mathcal{M}^{\#}$.

6.1.2 Vectorial bent functions from the $\mathcal{D}$ class different from $\mathcal{D}_0$

Whereas vectorial bent functions of maximal dimension stemming from $\mathcal{D}_0$ class were relatively easy to deduce, the problem becomes substantially harder in the case $E_1 \times E_2 \neq \{0_n\} \times \mathbb{F}_2^n$. In the recent article [84], a simple modification of the identity permutation was considered, specified as

$$\pi^{\star}(y) = \begin{cases} y, & y \notin \{\mathbb{e}_l, \mathbb{e}_t\}; \\ \mathbb{e}_l, & y = \mathbb{e}_t; \\ \mathbb{e}_t, & y = \mathbb{e}_l, \end{cases} \tag{6.1}$$

where $l, t \in \{1, 2, \ldots, n\}$ with $l \neq t$, and furthermore $\mathbb{e}_l, \mathbb{e}_t \in \mathbb{F}_2^n$ denote elements in the canonical basis of $\mathbb{F}_2^n$. More precisely, $(\mathbb{e}_l)_i = 1$ if $i = l$, otherwise $(\mathbb{e}_l)_i = 0$. Based on this, the following result characterizes the properties of bent functions in the so-called class $\mathcal{D}_2^{\star}$ (defined as the subclass of $\mathcal{D}$ that employs the 2-dimensional subspaces $E_1 = \langle \mathbb{e}_l, \mathbb{e}_t \rangle$). According to the definition of the $\mathcal{D}_2^{\star}$ class of bent functions, it is obvious that $f(x, y) = \pi^{\star}(y) \cdot x + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y)$ is a bent function whenever we select $E_2 = E_1^{\perp}$ since then $\pi^{\star}(E_2) = E_1^{\perp}$.

Theorem 6.1.3 *[84] Let* $n \geq 5$ *be a positive integer and let* l, t *be two positive integers such that* $1 \leq l < t \leq n$. *Let* $\pi^{\star}$ *be the permutation of* $\mathbb{F}_2^n$ *defined by* (6.1). *Let* l, t *be two integers such that* $1 \leq l < t \leq n$. *Define the function* $f : \mathbb{F}_2^n \to \mathbb{F}_2$ *by* $f(x, y) = \pi^{\star}(y) \cdot x + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y)$, *with* $x, y \in \mathbb{F}_2^n$, *where* $E_1 = \langle \mathbb{e}_l, \mathbb{e}_t \rangle$ *and* $E_2 = E_1^{\perp}$ *(implying that* $\dim(E_2) = n - 2$*). Then* f *is a bent function outside* $\mathcal{M}^{\#}$.

A straightforward extension of the bent functions in the $\mathcal{D}_2^{\star}$ class to their vectorial counterparts with the maximal output dimension appears to be difficult. The main reason is that having $\dim(E_2) < n$ implies certain restrictions due to the condition $\pi(E_2) = E_1^{\perp}$. To define a vectorial bent function stemming from $\mathcal{D}_2^{\star}$, using a similar approach as for the $\mathcal{D}_0$ class, we need to ensure that the permutations $\pi_i^{\star}(y) = \alpha_i \pi^{\star}(y)$, for $i = 1, \ldots, k$, where $k \leq n$, preserve the property that $\pi_i^{\star}(E_2) = E_1^{\perp}$. Notice that, assuming the linear independence of $\alpha_1, \ldots, \alpha_k$, for any such $\alpha_i \pi^{\star}(y)$ one can associate different 2-dimensional subspaces $E_1^{(k)} = \langle \mathbb{e}_{i_k}, \mathbb{e}_{l_k} \rangle$ and the corresponding subspaces $E_2^{(k)}$ but then the indicators of $\sum_k E_1^{(k)}$ do not (in general) correspond to linear subspaces.

Theorem 6.1.4 *Let $f_0^\star(x,y) = \pi^\star(y)\cdot x + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y)$, with $x,y \in \mathbb{F}_2^n$, be a bent function in $\mathcal{D}_2^\star$, where $\pi^\star$ is defined by (6.1) and $E_1 = \langle \mathbb{e}_l, \mathbb{e}_t\rangle \subset \mathbb{F}_2^n$, $E_2 = E_1^\perp$. Assume $\{\alpha_0, \alpha_1, \ldots, \alpha_{k-1}\}$, with $\alpha_0 = 1$ and $k \le n$, is a set of linearly independent elements in $\mathbb{F}_{2^n}$ (over $\mathbb{F}_2$), such that*

$$\pi_a^\star(y) := \left(\sum_{i=0}^{k-1} a_i\alpha_i\right)\pi^\star(y) \text{ satisfies } \pi_a^\star(E_2) = E_1^\perp,$$

for any $a = (a_0,\ldots,a_{k-1}) \in \mathbb{F}_2^k \setminus \{0_k\}$. Then, $F = (f_0,\ldots,f_{k-1})$, where $f_i(x,y) = \alpha_i\pi^\star(y)\cdot x + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y)$, is a vectorial bent function weakly outside $\mathcal{M}^{\#}$.

Proof. Clearly, by definition, $f_0^\star$ is a bent function in $\mathcal{D}_2^\star$ and it is outside $\mathcal{M}^{\#}$ by Theorem 6.1.3. Also, $\pi_a^\star(y) = \left(\sum_{i=0}^{k-1} a_i\alpha_i\right)\pi^\star(y)$ is a permutation for any $a = (a_0,\ldots,a_{k-1}) \in \mathbb{F}_2^k \setminus \{0_k\}$ and by assumption it preserves the property that $\pi_a^\star(E_2) = E_1^\perp = E_2$. Any component function $a_0f_0 + \cdots + a_{k-1}f_{k-1}$ is either of the form $\pi_a^\star(y)\cdot x$ (when $(a_0,\ldots,a_{k-1})$ is of even weight), or alternatively of the form $\pi_a^\star(y)\cdot x + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y)$ when the weight of a is odd. The former case gives bent functions in the $\mathcal{M}$ class and the latter bent functions in the $\mathcal{D}$ class. Thus, F is a vectorial bent function weakly outside $\mathcal{M}^{\#}$. ∎

The following example illustrates the whole approach and also indicates design difficulties when no further structure on the subspace E_2 is imposed.

Example 5 *Let $\pi^\star$ over $\mathbb{F}_2^3$ be defined by (6.1), where $l = 1, t = 2$ so that $E_1 = \langle(1,0,0),(0,1,0)\rangle$ and $E_2 = \langle(0,0,1)\rangle$. Then $\pi^\star(E_2) = E_1^\perp$. Indeed, we have*

y	$\pi^\star(y)$
$(0,0,0)$	$(0,0,0)$
$(0,0,1)$	$(0,0,1)$
$\mathbf{(0,1,0)}$	$\mathbf{(1,0,0)}$
$(0,1,1)$	$(0,1,1)$
$\mathbf{(1,0,0)}$	$\mathbf{(0,1,0)}$
$(1,0,1)$	$(1,0,1)$
$(1,1,0)$	$(1,1,0)$
$(1,1,1)$	$(1,1,1)$

To define the permutations $\alpha_i\pi^\star(y)$ over $\mathbb{F}_{2^3}$, for $i = 0,1$ we can use the elements of a polynomial basis $\{1,\beta,\beta^2\}$ of $\mathbb{F}_{2^3}$ where β is a root of the primitive polynomial $p(x) = x^3 + x + 1$ over $\mathbb{F}_2$. These elements are clearly independent and we can define $f_1^\star(x,y) = \beta\pi^\star(y)\cdot x + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y)$. However, the permutation $\beta\pi^\star(y)$ is defined over $\mathbb{F}_{2^3}$ so we need to give its isomorphic representation over $\mathbb{F}_2^3$. Using the isomorphism $(a_0,a_1,a_2) \in \mathbb{F}_2^3 \mapsto a_0 + a_1\beta + a_2\beta^2 \in \mathbb{F}_{2^3}$ we can use $\pi^\star(y) = (\pi_0^\star(y),\pi_1^\star(y),\pi_2^\star(y))$ and write $\pi^\star(y) = \pi_0^\star(y) + \beta\pi_1^\star(y) + \beta^2\pi_1^\star(y)$, where the latter $\pi^\star(y)$ representation refers to $\mathbb{F}_{2^3}$. Then, the multiplication by β in the field $\mathbb{F}_{2^3}$ is well defined and we obtain:

$$\beta(\pi_0^\star(y) + \beta\pi_1^\star(y) + \beta^2\pi_2^\star(y)) = \pi_2^\star(y) + \beta(\pi_0^\star(y) + \pi_2^\star(y)) + \beta^2\pi_1^\star(y).$$

Therefore, the permutation $\alpha\pi^\star(y)$ (using $\alpha = \beta$) is given as:

y	$\alpha\pi^\star(y)$
$(0,0,0)$	$(0,0,0)$
$(0,0,1)$	$(1,1,0)$
$(0,1,0)$	$(0,1,0)$
$(0,1,1)$	$(1,1,1)$
$(1,0,0)$	$(0,0,1)$
$(1,0,1)$	$(1,0,0)$
$(1,1,0)$	$(0,1,1)$
$(1,1,1)$	$(1,0,1)$

Then, for the permutation $\alpha\pi^\star(y)$ we have $\alpha\pi^\star(E_2) \neq E_2$ and then the function $\alpha\pi^\star(y) \cdot x + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y)$ is not necessarily bent.

The above example indicates that this design approach requires a careful selection of the permutation $\pi(y)$ and the corresponding subspaces E_1 and E_2 in order to construct vectorial bent functions stemming from the $\mathcal{D}$ class.

Remark 5 *Notice that specifying a vectorial bent function $F = (f_0, \ldots, f_{n-1})$ of the maximal dimension, when $\dim(E_2) < n$ and $f_i(x,y) = \alpha_i\pi(y) + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y)$ is not possible if $\pi(E_2) = E_2$. This is due to the fact that $\alpha_0, \ldots, \alpha_{n-1}$ must be linearly independent over $\mathbb{F}_2$ to ensure that $(\sum_{i=0}^{n-1} a_i\alpha_i)\pi(y)$ is a permutation for any nonzero $(a_0, \ldots, a_{n-1}) \in \mathbb{F}_2^n$ which cannot be satisfied simultaneously with $(\sum_{i=0}^{n-1} a_i\alpha_i)\pi(E_2) = E_2$ because $\dim(E_2) < n$.*

A natural solution to the problem discussed in Example 5 is to ensure that the elements of E_2 form a subfield, say $\mathbb{F}_{2^k} < \mathbb{F}_{2^n}$, with $k \mid n$. Then, by selecting a set of linearly independent elements $\alpha_0, \ldots, \alpha_{k-1} \in \mathbb{F}_{2^k}$ one can easily ensure that $(\sum_{i=0}^{n-1} a_i\alpha_i)\pi(E_2) = E_2$ provided that $\pi(E_2) = E_2$. This however, excludes (for $n > 4$) the use of the permutation $\pi^\star$ and E_1 in the setup of Theorem 6.1.4, since there $\dim(E_1) = 2$, so $\dim(E_2) = n - 2$, and hence it cannot be a subfield of $\mathbb{F}_{2^n}$.

Theorem 6.1.5 *Let π be a permutation of $\mathbb{F}_2^n$ and let E_2 be a k-dimensional subspace of $\mathbb{F}_2^n$ corresponding to the subfield $\mathbb{F}_{2^k}$ of $\mathbb{F}_{2^n}$, where $k \mid n$ and $1 < k \leq n/2$. If π satisfies that $\pi(E_2) = E_1^\perp = E_2$, then $F = (f_0, \ldots, f_{k-1})$, where $f_i(x,y) = \alpha_i\pi(y) \cdot x + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y)$ and $\alpha_0, \ldots, \alpha_{k-1}$ form a basis of $\mathbb{F}_{2^k}$, is a vectorial bent function with components in $\mathcal{M}$ and $\mathcal{D}$.*

Proof. The proof follows the same reasoning as the proofs of Theorem 6.1.4 or Theorem 6.1.1 and the details are omitted. The fact that $(\sum_{i=0}^{k-1} a_i\alpha_i)\pi(E_2) = E_2$, for any nonzero $(a_0, \ldots, a_{k-1}) \in \mathbb{F}_2^k$, follows from the fact that $E_2 = \mathbb{F}_{2^k}$ and $\alpha_i \in \mathbb{F}_{2^k}$ along with the assumption that $\pi(E_2) = E_1^\perp = E_2$. ∎

For example, one can set $E_2 = \mathbb{F}_{2^k}$ and $\pi(x) = x^{-1}$ if $x \in E_2 = \mathbb{F}_{2^k}$, otherwise $\pi(x) = x$. Such a permutation $\pi(x)$ satisfies the condition of Theorem 6.1.5 when $\alpha_0, \ldots, \alpha_{k-1}$ are selected as a basis of $E_2 = \mathbb{F}_{2^k}$. More precisely, $(\sum_i a_i\alpha_i)\pi(y) := \pi_a(y)$ is a permutation and furthermore $\pi_a(E_2) = E_2$ for all

nonzero $a = (a_0, \ldots, a_{k-1}) \in \mathbb{F}_2^k$. In general, when $\phi(x)$ is a permutation of E_2, we can set $\pi(x) = \phi(x)$ if $x \in E_2$, otherwise $\pi(x) = x$. Then, such $\pi(x)$ satisfies the condition of Theorem 6.1.5 if $\alpha_0, \ldots, \alpha_{k-1}$ form a basis of $E = \mathbb{F}_{2^k}$ (since $\pi_a(x) \in E_2$ when $x \in E_2$).

The case of special interest, allowing an easier treatment of the condition that $\pi(E_2) = E_1^{\perp} = E_2$, arises when n is even and $\dim(E_1) = \dim(E_2) = n/2$ which is treated in the next section. This also allows us to specify many permutations such that $\pi_a(E_2) = E_2$, where $(\sum_i a_i\alpha_i)\pi(y) := \pi_a(y)$ as before, though not in an explicit univariate form.

6.1.3 Some explicit classes of vectorial bent functions from $\mathcal{D}$

As already discussed, the main problem of providing generic methods for constructing functions $F : \mathbb{F}_2^{2n} \to \mathbb{F}_2^k$, derived from the $\mathcal{D}$ class using the ideas from Section 6.1.2, is related to the property that any permutation $\pi_a(y) = (\sum_{i=0}^{k-1} a_i\alpha_i)\pi(y)$ over $\mathbb{F}_{2^n}$ needs to have the property that $\pi(E_2) = E_2$.

Based on the works of G. Kyureghyan [36] and A. Akbary *et al.* [1], the authors in [18] proposed several explicit classes of permutations using the notion of linear translators. For our purpose we recall the following results which can be found in [18].

Theorem 6.1.6 *[18] Let $n = 2k$ and $\pi : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$ with $\pi(x) = x + (x + x^{2^k} + \delta)^s$, where $\delta \in \mathbb{F}_{2^n}$ and s is any integer in the range $[0, 2^n - 2]$. Then π is a permutation over $\mathbb{F}_{2^n}$ if and only if the function*

$$y \mapsto y + (y + \delta)^s + (y + \delta)^{2^k s} \quad \text{from } \mathbb{F}_{2^k} \text{ to } \mathbb{F}_{2^k}$$

is bijective. In particular, if s satisfies $2^k s \equiv s \pmod{2^n - 1}$ then π is a permutation.

As a corollary of this general result an explicit class of permutations was deduced.

Corollary 6.1.7 *[18] Using the same notation as in Theorem 6.1.6, if $\delta \in \mathbb{F}_{2^k}$ then $\pi(x) = x + (x + x^{2^k} + \delta)^s$ is a permutation for any $s \in [0, 2^k - 2]$.*

The result of Corollary 6.1.7 is important for two reasons. Firstly, this result is generic and compared to Theorem 6.1.6 it does not impose any conditions on the choice of s. Secondly, the assumption that $\delta \in \mathbb{F}_{2^k}$ ensures that π permutes the subfield $\mathbb{F}_{2^k}$, which is important for keeping the subspace $E_2 = \mathbb{F}_{2^k}$ fixed so that $\pi(\mathbb{F}_{2^k}) = \mathbb{F}_{2^k}$. Indeed, for any element $x \in \mathbb{F}_{2^k}$ we obviously have that $x + x^{2^k} + \delta \in \mathbb{F}_{2^k}$ since $\delta \in \mathbb{F}_{2^k}$, and therefore π permutes the subfield $\mathbb{F}_{2^k}$. Notice that the selection of exponent s is directly related to the degree of such permutations. This immediately leads us to a result similar to that of Theorem 6.2.1.

Theorem 6.1.8 *Let $n = 2k$ and $\pi(y) = y + (y + y^{2^k} + \delta)^s$ be a permutation over $\mathbb{F}_{2^n}$, where $\delta \in \mathbb{F}_{2^k}$ and $s \in [0, 2^k - 2]$. Let E_2 be a k-dimensional subspace of $\mathbb{F}_2^n$ such that it can be regarded as the subfield $\mathbb{F}_{2^k}$ of $\mathbb{F}_{2^n}$. Then, π satisfies $\pi(E_2) = E_1^{\perp} = E_2$, and $F = (f_0, \ldots, f_{k-1})$, where $f_i(x, y) = \alpha_i\pi(y) \cdot x + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y)$ for $x, y \in \mathbb{F}_2^n$, and $\alpha_0, \ldots, \alpha_{k-1}$ form a basis of $\mathbb{F}_{2^k}$, is a vectorial bent function.*

Notice that we do not claim the property of being weakly outside $\mathcal{M}^{\#}$ since the permutation $\pi(y) = y + (y + y^{2^k} + \delta)^s$ over $\mathbb{F}_{2^n}$ does not satisfy the sufficient conditions given in Theorem 6.1.2, as we explain now. The requirement $\deg(\pi) \leq n - \dim E_2 = k$ is automatically achieved for any $s \in [0, 2^k - 2]$ since its Hamming weight, which is essentially the degree of π, is always less or equal than k. The main problem is therefore to ensure that $Tr_1^n(u\pi(y)) = Tr_1^n(u(y + (y + y^{2^k} + \delta)^s)$ has no linear structures for any nonzero $u \in \mathbb{F}_{2^n}$, see Theorem 6.1.2. To investigate the existence of linear structures of $\pi(y) = y + (y + y^{2^k} + \delta)^s$ it is enough to consider $\pi'(y) = (y + y^{2^k} + \delta)^s$. However, regardless of the choice of s the permutation π' admits linear structures. More precisely, any $a \in \mathbb{F}_{2^k}$ is a linear structure of π' since $\pi'(y) + \pi'(y + a) = (y + y^{2^k} + \delta)^s + (y + a + (y + a)^{2^k} + \delta)^s = 0$, using that $a^{2^k} = a$. Therefore, we cannot use the sufficient conditions of Theorem 6.1.2 and it might be the case that F defined in Theorem 6.1.8 (possibly all its component functions) belongs to $\mathcal{M}$.

6.2 Vectorial bent functions from $\mathcal{D}$ weakly outside $\mathcal{M}^{\#}$

So far, apart from employing $\mathcal{D}_0$ to obtain vectorial bent functions (weakly) outside $\mathcal{M}^{\#}$, the explicit methods given in Section 6.1 only ensure that the component functions of the vectorial bent functions come from different classes. To derive vectorial bent functions, from $\mathcal{D}$, that are provably (at least) weakly outside $\mathcal{M}^{\#}$ one needs to ensure, based on the sufficient conditions given in Theorem 6.1.2, that the permutation π does not admit linear structures.

A class of Boolean bent functions for even n, satisfying the conditions in Theorem 6.1.2, was specified in [84, Proposition 2] using a monomial permutation $\pi(y) = y^d$ (with $wt(d) \geq 3$) which satisfies $\pi(E_2) = E_2 = E_1^{\perp}$ for the 2-dimensional vector subspace (subfield isomorphic to $\mathbb{F}_{2^2}$) $E_2 = \langle \zeta^{\frac{2^n-1}{3}}, \zeta^{\frac{2(2^n-1)}{3}} \rangle$, where ζ is a primitive element of $\mathbb{F}_{2^n}$. Then, specifying $f(x, y) = \pi(y) \cdot x + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y)$ gives a bent function in $\mathcal{D}$ and outside $\mathcal{M}^{\#}$. The extension to the vectorial case using a basis $\{\alpha_0, \ldots, \alpha_{k-1}\}$ of the subfield $\mathbb{F}_{2^k} < \mathbb{F}_{2^n}$ is again possible. From this, we can immediately deduce the following theorem.

Theorem 6.2.1 *Let $\pi(y) = y^d$, where $3 \leq wt(d) \leq n - 2$, be a permutation of $\mathbb{F}_2^n$. Let E_2 be a k-dimensional subspace of $\mathbb{F}_2^n$, where $k|n$, corresponding to the subfield $\mathbb{F}_{2^k}$ of $\mathbb{F}_{2^n}$ and $1 < k \leq n/2$. Then, π satisfies $\pi(E_2) = E_2 = E_1^{\perp}$, and $F = (f_0, \ldots, f_{k-1})$, where $f_i(x, y) = \alpha_i\pi(y) \cdot x + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y)$, and $\alpha_0, \ldots, \alpha_{k-1} \in \mathbb{F}_{2^k}$ are linearly independent over $\mathbb{F}_2$, is a vectorial bent function weakly outside $\mathcal{M}^{\#}$.*

6.2.1 Vectorial bent functions from complete mappings

To obtain a greater design variety and to possibly specify functions affine inequivalent to those derived using a set of permutations which are affine equivalent (thus related through $\pi_i(y) = \alpha_i\pi(y)$), one may employ a class of complete mappings. We recall that a permutation $\pi(y)$ over $\mathbb{F}_{2^n}$ is called complete if $\pi(y) + y$ is also a permutation. More generally, like in Chapter 5, one can consider a set of permutations $\{\pi(y) + \alpha_i y\}$ for a set of linearly independent elements $\alpha_i \in \mathbb{F}_{2^n}$ over $\mathbb{F}_2$. For

instance, for the special case when $\dim(E_2) = 2$, we may use a bent function of the form $f(x,y) = \pi(y) \cdot x + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y)$, where $\pi(y) = y^d$ (like in Theorem 6.2.1), and specify another bent function using $\pi(y) + \alpha y$, assuming that the latter is a permutation.

Proposition 6.2.2 *Assume that $\pi(y) = y^d$, with $3 \leq wt(d) \leq n-2$, as well as that $\pi(y) + \alpha y$ is a permutation over $\mathbb{F}_{2^n}$, for some $\alpha \in \mathbb{F}_{2^n}$ and even n. Let $f_0(x,y) = \pi(y) \cdot x + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y)$, $x, y \in \mathbb{F}_2^n$, be a bent function for $E_2 = \langle \zeta^{\frac{2^n-1}{3}}, \zeta^{\frac{2(2^n-1)}{3}} \rangle$ and $E_1 = E_2^{\perp}$, where ζ is a primitive element of $\mathbb{F}_{2^n}$ so that $\pi(E_2) = E_2$. Define $f_1(x,y) = (\alpha y + a) \cdot x$ to be a bent function in the $\mathcal{M}$ class, where $a \in E_2$. If $\alpha \in E_2$, then*

$$f(x,y) = (f_0 + f_1)(x,y) = (\pi(y) + \alpha y + a) \cdot x + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y)$$

is again a bent function, which lies outside the $\mathcal{M}^{\#}$ class.

Proof. We first show that f is a bent function. The mapping $\phi(y) = \pi(y) + \alpha y + a$ is clearly a permutation. Furthermore, since $a, \alpha \in E_2$ and E_2 is a subfield of $\mathbb{F}_{2^n}$ it still holds that $\phi(E_2) = E_2 = E_1^{\perp}$. Therefore, f belongs to the $\mathcal{D}$ class and is bent. Also, since $wt(d) \geq 3$, ϕ has no linear structures [19]. It follows, by Theorem 6.1.2, that f lies outside the $\mathcal{M}^{\#}$ class. ∎

Remark 6 *The existence of vectorial bent functions weakly outside the $\mathcal{M}^{\#}$ class generated by Proposition 6.2.2 relies on the existence of permutations $\pi(y) = y^d$ such that $\pi(y) + \alpha y$ is also a permutation for some $\alpha \in E_2$. This class of permutations was analyzed in [17] and the main result is that for sufficiently large q, assuming $d \mid q-1$, there exists at least one $u \in \mathbb{F}_q$ such that $y^{d+1} + uy$ is a permutation over $\mathbb{F}_q$. For instance, when $n = 6$ the mappings $\pi(y) = y^{10}$ and $\pi(y) + \zeta^i y$ on $\mathbb{F}_{2^6}$, for a primitive element $\zeta \in \mathbb{F}_{2^6}$, are both permutations for $i = 3, 6, 12, 15, 21, 24, 30, 33, 39, 42, 48, 51, 57, 60$ (for a primitive polynomial $p(x) = x^6 + x + 1$).*

The above approach can be easily extended provided the existence of complete mappings such that $\pi(y) + \alpha_i y$ is a permutation for some linearly independent $\alpha_1, \ldots, \alpha_k \in \mathbb{F}_2^n$ over $\mathbb{F}_2$, additionally satisfying the image preservation of E_2.

Since $f_1 \in \mathcal{M}$ whereas $f_0 \notin \mathcal{M}^{\#}$ in Proposition 6.2.2, it is clear that these bent functions cannot lie in the same affine equivalence class. Nevertheless, the question of possible affine inequivalence of bent functions derived from complete mappings is quite interesting. More precisely, comparing the function $f_0(x,y) = \pi(y) \cdot x + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y)$ in Proposition 6.2.2, when $\pi(y) = y^d$ (which is not necessary), to the function $f'(x,y) = (\pi(y) + \alpha y) \cdot x + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y)$ for $\alpha \in E_2$ we remark that

$$f_0(x,y) + f'(x,y) = \alpha y \cdot x; \quad x, y \in \mathbb{F}_2^n, \tag{6.2}$$

which is again bent and belongs to $\mathcal{M}$. Now if f_0 and f' given above are affine equivalent, having (6.2) necessarily satisfied, then there exists an invertible binary matrix A of size $2n \times 2n$, an element $(a,b) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$, and an affine $l : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2$, so that expressing $f'(x,y) = f_0((x,y)A + (a,b)) + l(x,y)$ we have

$$f_0(x,y) + f'(x,y) = f_0(x,y) + f_0((x,y)A + (a,b)) + l(x,y) = \alpha y \cdot x.$$

Nevertheless, even in the simple case of $\pi(y) = y^d$ so that $f_0(x,y) = y^d \cdot x + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y)$ this analysis becomes difficult.

An alternative approach to this problem of establishing affine (in)equivalence between f_0 and f', is to consider the weight distribution of the second order derivatives. More precisely, one can collect the Hamming weights of $D_aD_bf_0(x,y)$ and $D_aD_bf'(x,y)$ for all $(a,b) \in \mathbb{F}_2^{n*} \times \mathbb{F}_2^{n*}$ (with $a \neq b$) and compare their distributions. It was shown by J. Dillon [22] that f_0 and f' are affine inequivalent if these weight distributions differ form each other.

6.2.2 Vectorial bent functions from subfield permutations

In difference to the subfield permutations used in Section 6.1.3, there are other explicit classes of permutation polynomials that permute subfields but do not admit linear structures. Notice that any permutation polynomial $\pi(y) = \sum_{i=0}^{2^n-1} a_i y^i$ over $\mathbb{F}_{2^n}$ has the desired property that $\pi(\mathbb{F}_{2^k}) = \mathbb{F}_{2^k}$ whenever the coefficients $a_i \in \mathbb{F}_{2^k}$, for a subfield $\mathbb{F}_{2^k}$ of $\mathbb{F}_{2^n}$. In a recent article [27], the authors proposed four different classes of permutation trinomials over $\mathbb{F}_{2^n}$ with binary coefficients, for n even.

Theorem 6.2.3 *[27] The polynomial $f_1(x) = x^4 + x^{2^k+3} + x^{3\cdot 2^k+1} \in \mathbb{F}_{2^{2k}}[x]$ is a permutation polynomial over $\mathbb{F}_{2^{2k}}$ if and only if* $\gcd(k,3) = 1$.

As a corollary of this result, a permutation polynomial of the form $\pi(y) = y + y^{2^k} + y^{2^{2k-1}-2^{k-1}+1}$ (with $\gcd(k,3) = 1$) can be deduced, originally found in [39]. This permutation polynomial can be employed for deriving vectorial bent functions weakly outside $\mathcal{M}^{\#}$.

Theorem 6.2.4 *Let $n = 2k$ and $\pi(y) = y + y^{2^k} + y^{2^{2k-1}-2^{k-1}+1}$, with* $\gcd(k,3) = 1$, *be a permutation over $\mathbb{F}_{2^n}$. Let E_2 be a k-dimensional subspace of $\mathbb{F}_2^n$ regarded as the subfield $\mathbb{F}_{2^k}$ of $\mathbb{F}_{2^n}$. Then, π satisfies $\pi(E_2) = E_2 = E_1^{\perp}$ and $F = (f_0, \ldots, f_{k-1})$, where $f_i(x,y) = \alpha_i\pi(y) \cdot x + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y)$ for linearly independent $\alpha_i \in \mathbb{F}_{2^k}$ over $\mathbb{F}_2$, is a vectorial bent function weakly outside $\mathcal{M}^{\#}$.*

Proof. We notice that $\pi(\mathbb{F}_{2^k}) = \mathbb{F}_{2^k}$ since the coefficients of π are binary (the same would be true for the coefficients from $\mathbb{F}_{2^k}$), due to the closedness of $\mathbb{F}_{2^k}$. It can be easily verified that $wt(2^{2k-1} - 2^{k-1} + 1) \geq 3$ for any $k \geq 2$ hence the term $g(y) = y^{2^{2k-1}-2^{k-1}+1}$ does not admit linear structures (see [19, Theorem 5]). Then, as the remaining two terms $y + y^{2^k}$ are linear and do not affect derivatives we conclude that $\pi(y)$ satisfies the conditions of Theorem 6.1.2. Therefore, F is a vectorial bent function weakly outside $\mathcal{M}^{\#}$ with components in $\mathcal{D}$ and $\mathcal{M}$. ∎

The particular instances of permutations mentioned above all belong to a broader class of permutation polynomials of the form $x^r h(x^s)$ which contains many explicit classes specified in the literature. We believe that most of these permutations eventually satisfy the condition related to the absence of linear structures and can be used in Theorem 6.2.4, but we do not investigate this issue further.

6.3 Vectorial bent-negabent functions weakly outside the $\mathcal{M}^{\#}$ class

In this section we combine the notion of vectorial bent-negabent functions introduced in Chapter 5 and the notion of vectorial bent functions weakly outside $\mathcal{M}^{\#}$ introduced in this chapter. We propose several different methods of constructing vectorial bent-negabent functions provably weakly outside the completed $\mathcal{M}$ class. For this purpose, we first consider a class of complete mappings over $\mathbb{F}_{2^n}$ of the form $x \mapsto F(x) + ax$, which remain permutations for "many" values $a \in \mathbb{F}_{2^n}$ and combine it with bent functions in the $\mathcal{D}_0$ class to construct vectorial bent-negabent functions weakly outside $\mathcal{M}$. Then, we propose a generic method of constructing complete mappings from a suitable vector space decomposition. The complete mappings are then utilised to construct vectorial bent-negabent functions (whose dimension is not maximal) with approximately half of the component functions in $\mathcal{C} \setminus \mathcal{M}^{\#}$.

6.3.1 Vectorial bent-negabent functions from the $\mathcal{D}_0$ class

Firstly we focus on constructions of vectorial bent-negabent functions outside $\mathcal{M}^{\#}$, using bent functions from $\mathcal{D}_0$ class together with some known results about complete monomial permutations.

Consider the following characterization of the permutation binomials of the form $F(x) = x^{\frac{2^n-1}{2^k-1}+1} + ax$ on $\mathbb{F}_{2^n}$, where $n = 2^r k$, which we will use to construct Boolean and vectorial bent-negabent functions outside $\mathcal{M}^{\#}$.

Theorem 6.3.1 *[5] Let r, k be positive integers with k odd and $n = 2^r k$. Then the polynomial $F(x) = x^{\frac{2^n-1}{2^k-1}+1} + ax$, $a \in \mathbb{F}_{2^n}^*$ is a permutation polynomial of $\mathbb{F}_{2^n}$ if and only if (i) $r = 1, 2$ and (ii) $a \in \omega\mathbb{F}_{2^k}^* \cup \omega^2\mathbb{F}_{2^k}^*$, where $\omega \in \mathbb{F}_{2^2}$ is a root of the equation $\omega^2 + \omega + 1 = 0$.*

Using this result, we now show that $\mathcal{D}_0$ class contains members, which are not only equivalent to bent-negabent functions, but also do not belong to the completed Maiorana-McFarland class $\mathcal{M}^{\#}$.

Theorem 6.3.2 *Let $m = 2n = 4t$, where $t \geq 3$ is an odd positive integer. Let $\pi \colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a permutation defined by $\pi(y) = y^{2^t+2}$, for $y \in \mathbb{F}_{2^n}$. Then, the function $f(x, y) = x \cdot \pi(y) + \delta_0(x)$, where $x, y \in \mathbb{F}_2^n$, is a bent function outside $\mathcal{M}^{\#}$ and it is affine equivalent to a negabent function.*

Proof. Notice that since all components of π are quadratic, using results from Chapter 3, we can immediately deduce that f is a bent function outside $\mathcal{M}^{\#}$. However, for completeness, we present another proof here, based on [9, Proposition 2]. To prove that f is outside $\mathcal{M}^{\#}$, it is enough to show that the restriction of π to any linear hyperplane is not affine, see [9, Proposition 2]. Similarly to the proof of [9, Corollary 2], since $\pi(by) = b^{2^t+2}\pi(y)$ for $b \in \mathbb{F}_{2^n}$, the restriction of π to the linear hyperplane $H_b = \{y \in \mathbb{F}_{2^n} \mid Tr(by) = 0\}$ is affine if and only if the restriction of π to the linear hyperplane $H_0 = \{y \in \mathbb{F}_{2^n} \mid Tr(y) = 0\}$ is affine. Since H_0 is the image of the linear mapping $y \mapsto y^2 + y$, if the mapping π restricted to H_0 is

affine, then $\pi(y^2+y) = (y^2+y)^{2^t+2}$ would also be affine, but it is a polynomial of degree $2^{t+1}+4$ defined on $\mathbb{F}_{2^{2t}}$, and so it is not affine. Hence, the restriction of π to any linear hyperplane is not affine, and we conclude that f is a bent function in $\mathcal{D}_0$ outside $\mathcal{M}^{\#}$.

Now, let $a \in \omega\mathbb{F}_{2^t}^* \cup \omega^2\mathbb{F}_{2^t}^*$, where $\omega \in \mathbb{F}_{2^2}$ is a root of the equation $\omega^2+\omega+1=0$. From Theorem 6.3.1, we have that $y \mapsto \pi(y)+ay$ is again a permutation, and hence the Boolean function $(x,y) \mapsto f(x,y) + x \cdot (ay)$ is a bent function in the $\mathcal{D}_0$ class, where ay is the product of a and y in $\mathbb{F}_{2^{2t}}$. Denote by g the quadratic Boolean bent function $(x,y) \mapsto x \cdot (ay)$ on $\mathbb{F}_2^m$, which we identify with $\mathbb{F}_2^n \times \mathbb{F}_2^n$. Since g is a quadratic bent function on $\mathbb{F}_2^m$, there exists an invertible $m \times m$ matrix M, a vector $v \in \mathbb{F}_2^m$ and an affine Boolean function $l : \mathbb{F}_2^m \to \mathbb{F}_2$, such that $s_2(x,y) = g((x,y)M+v)+l(x,y)$. Since addition of affine functions does not affect bent-negabentness, we conclude that $f((x,y)M+v)$ is a negabent function. In this way, we conclude that $f((x,y)M+v)$ is a bent-negabent function outside the $\mathcal{M}^{\#}$ class. ∎

Using Theorem 6.3.1 and Theorem 6.3.2, we derive the following construction of vectorial bent-negabent functions weakly outside the $\mathcal{M}^{\#}$ class.

Theorem 6.3.3 *Let $m = 2n = 4t$, where $t \geq 3$ is an odd positive integer. Let $\pi\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a permutation defined by $\pi(y) = y^{2^t+2}$, for $y \in \mathbb{F}_{2^n}$, and let $f\colon \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \to \mathbb{F}_2$ be defined by $f(x,y) = x \cdot \pi(y) + \delta_0(x)$ for $x, y \in \mathbb{F}_{2^n}$. Let $\{a_1, \ldots, a_t\}$ be a basis of $\omega\mathbb{F}_{2^t}$ over $\mathbb{F}_2$, where $\omega \in \mathbb{F}_{2^2}$ is a root of the equation $\omega^2+\omega+1=0$. Then, the function $F\colon \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \to \mathbb{F}_2^t$ defined by*

$$F(x,y) = \begin{bmatrix} f(x,y) \\ x \cdot a_1 y \\ \vdots \\ x \cdot a_{t-1} y \end{bmatrix}$$

is affine equivalent to a vectorial bent-negabent function and is weakly outside the $\mathcal{M}^{\#}$ class.

Proof. From Theorem 6.3.2, we know that f is a bent function outside the $\mathcal{M}^{\#}$ class. Let S be a non-empty subset of $\{1, \ldots, t-1\}$. Then, by Theorem 6.3.1, the function $(x,y) \mapsto f(x,y) + x \cdot (\sum_{i \in S} a_i)y$ is bent and belongs to the $\mathcal{D}_0$ class. The function $(x,y) \mapsto x \cdot (\sum_{i \in S} a_i)y$ is also bent and is in $\mathcal{M}^{\#}$. Hence, F is a vectorial bent function.

Since the function $g(x,y) = x \cdot (a_t y)$ is a quadratic bent function on $\mathbb{F}_2^m$, which is identified with $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$, there exists an invertible $m \times m$ binary matrix M, a vector $v \in \mathbb{F}_2^m$ and an affine Boolean function $l\colon \mathbb{F}_2^m \to \mathbb{F}_2$, such that $s_2(x,y) = g((x,y)M+v) + l(x,y)$. Now, $f(x,y) + x \cdot (\sum_{i \in S} a_i)y + x \cdot a_t y$ is a bent function by Theorem 6.3.1, and $x \cdot (\sum_{i \in S} a_i)y + x \cdot a_t y$ is a bent function in $\mathcal{M}^{\#}$. Hence, we conclude that $F((x,y)M+v)$ is a vectorial bent-negabent function weakly outside $\mathcal{M}^{\#}$. ∎

6.3.2 Vectorial bent-negabent functions from the $\mathcal{C}$ class

Apart from the permutations specified in [5], one can identify other classes of permutations which can be viewed as vector spaces of complete mappings in the sense discussed above. In the sequel, we propose a generic method of constructing such mappings.

6.3.2.1 A generic construction method of vector spaces of nonlinear complete mappings

L.E. Baum and L.P. Neuwirth [2] introduced a method of decomposing vector spaces in a non-trivial manner. This method was used in Chapter 4 for the purpose of specifying permutations without linear structures, and another approach to generate this type of vector space decomposition was suggested in [38]. In the following theorem, instead of using suitable permutations $x \mapsto F(x)$ such that $x \mapsto F(x) + bx$ remains a permutation for many b's (alternatively using b-complete permutations), one can provide a generic method of building such mappings using a suitable vector space decomposition. The benefits of such an approach are: a larger variation of the constructed objects and a higher algebraic degree of such mappings.

Lemma 6.3.4 *Let E be a subspace of $\mathbb{F}_2^n$, and let $\phi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a function such that ϕ is constant on cosets of E (i.e., $\phi(a) = \phi(a + e)$, $\forall a \in \mathbb{F}_2^n$, and $\forall e \in E$), and such that it has values in only one additive coset of E (i.e., $\phi(a) + \phi(b) \in E$, $\forall a, b \in \mathbb{F}_2^n$). Then, the mapping $x \in \mathbb{F}_2^n \mapsto L \circ \phi(x) + x$ is a permutation for every invertible linear mapping $L \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ such that $L(E) = E$.*

Proof. For every invertible linear mapping L, the function F defined by $F(x) = L \circ \phi(x) + x$ is a permutation if and only if the function $G = L^{-1} \circ F = \phi + L^{-1}$ is a permutation. Hence, in order to prove that $L \circ \phi(x) + x$ is a permutation for every invertible linear mapping $L \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ such that $L(E) = E$, we will prove the equivalent statement that $\phi + L$ is a permutation of $\mathbb{F}_2^n$ for every invertible linear mapping $L \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ such that $L(E) = E$ (note that $L(E) = E$ is equivalent to $L^{-1}(E) = E$, and consequently the statement is true for every L^{-1} if and only if it is true for every L).

Let $L \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ be an invertible linear mapping such that $L(E) = E$. Assume that for some $v, w \in \mathbb{F}_2^n$ we have $\phi(v) + L(v) = \phi(w) + L(w)$. Then $\phi(v) + \phi(w) = L(v) + L(w) = L(v + w)$, and since $\phi(v) + \phi(w) \in E$ and $L(E) = E$, we have $v + w \in E$. Thus, v and w are in the same coset of E. But since v and w are in the same coset of E, we have $\phi(v) = \phi(w)$, so $L(v + w) = 0$, and hence $v = w$. We conclude that $\phi + L$ is a permutation of $\mathbb{F}_2^n$. ∎

We can now use similar ideas as in Section 6.3.1 and combine these with Lemma 6.3.4 to construct vectorial bent-negabent functions. In order to find vector spaces of linear permutations that fix E, we will set E to be a subfield of $\mathbb{F}_{2^n}$ and use the multiplication in $\mathbb{F}_{2^n}$ with elements from E. By doing this, we will be able to get higher degree of the permutations compared to the construction in Section 6.3.1. However, since now ϕ itself is not a permutation (it is constant on cosets of E),

we have to reduce the dimension of the vectorial function by one, compared to the functions in Theorem 6.3.3.

Theorem 6.3.5 *Let $m = 2n$. Let $\mathbb{F}_{2^t}$ be a subfield of $\mathbb{F}_{2^n}$, and let $\{a_1, \ldots, a_t\}$ be a basis of $\mathbb{F}_{2^t}$ over $\mathbb{F}_2$. Let $L_i \colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be the linear functions defined by $L_i(y) = a_i y$, and let $\pi_i \colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be the mapping defined by $\pi_i(y) = L_i(y) + \mathbb{1}_{\mathbb{F}_{2^t}}(y)$, for $i = 1, \ldots, t-1$. Let also $\rho_1, \ldots, \rho_{t-1}$ be arbitrary Boolean functions on $\mathbb{F}_{2^n}$. Then, the function $F \colon \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \to \mathbb{F}_2^{t-1}$ defined by*

$$F(x,y) = \begin{bmatrix} Tr(x\pi_1(y)) + \rho_1(y) \\ \vdots \\ Tr(x\pi_{t-1}(y)) + \rho_{t-1}(y) \end{bmatrix}$$

is affine equivalent to a vectorial bent-negabent function.

Proof. Choose an arbitrary non-empty subset S of $\{1, \ldots, t-1\}$ and fix it. First, we will show that the component function

$$\sum_{i \in S} (Tr(x\pi_i(y)) + \rho_i(y)) = Tr(x \sum_{i \in S} \pi_i(y)) + \sum_{i \in S} \rho_i(y)$$

is a bent function. From the definition of π_i's, we have $\sum_{i \in S} \pi_i(y) = \sum_{i \in S} (a_i y + \mathbb{1}_{\mathbb{F}_{2^t}}(y))$.

If the number of elements in S is even, then $\sum_{i \in S} \pi_i(y) = (\sum_{i \in S} a_i)y$, and since a_i's are linearly independent $\sum_{i \in S} a_i \neq 0$, so $\sum_{i \in S} \pi_i(y)$ is a permutation. In this way, the component function $\sum_{i \in S} Tr(x\pi_i(y)) + \sum_{i \in S} \rho_i(y)$ is a bent function inside the $\mathcal{M}$ class.

On the other hand, if the number of elements in S is odd, then $\sum_{i \in S} \pi_i(y) = (\sum_{i \in S} a_i)y + \mathbb{1}_{\mathbb{F}_{2^t}}(y)$. Since $b := \sum_{i \in S} a_i$ is a nonzero element of $\mathbb{F}_{2^t}$, the linear mapping $L(y) = by$ is invertible, and maps $\mathbb{F}_{2^t}$ to $\mathbb{F}_{2^t}$. The mapping $\mathbb{1}_{\mathbb{F}_{2^t}}(y)$ is constant on cosets of $\mathbb{F}_{2^t}$, and it obviously has values only in $\mathbb{F}_{2^t}$. Hence, from Lemma 6.3.4, we deduce that $\sum_{i \in S} \pi_i(y) = (\sum_{i \in S} a_i)y + \mathbb{1}_{\mathbb{F}_{2^t}}(y)$ is again a permutation, and therefore $\sum_{i \in S} Tr(x\pi_i(y)) + \sum_{i \in S} \rho_i(y)$ is a bent function in $\mathcal{M}$.

Since the function $g'(x,y) = Tr(x(a_t y))$ is a quadratic bent function on $\mathbb{F}_2^m$, which is identified with $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$, and all quadratic bent functions are affine equivalent, there is an invertible $m \times m$ binary matrix M, a vector $r \in \mathbb{F}_2^m$, and an affine Boolean function $l \colon \mathbb{F}_2^m \to \mathbb{F}_2$, such that $s_2(x,y) = g'((x,y)M + r) + l(x,y)$. Similarly to the paragraph above, the function $\sum_{i \in S} \pi_i(y) + a_t y$ is a permutation, and so $\sum_{i \in S} Tr(x\pi_i(y)) + \sum_{i \in S} \rho_i(y) + Tr(x(a_t y))$ is a bent function in the $\mathcal{M}$ class. Hence, we conclude that the function $F((x,y)M + r)$ is a vectorial bent-negabent function (ignoring the linear terms and constants, since they do not affect the bent-negabent property). ∎

Remark 7 *Notice that the algebraic degree of the permutations $\pi_i(y) = L_i(y) + \mathbb{1}_{\mathbb{F}_{2^t}}(y)$ in Theorem 6.3.5 is $n - t$, since we can view $\mathbb{1}_{\mathbb{F}_{2^t}}(y)$ as an indicator of a t-dimensional subspace of $\mathbb{F}_2^n$, and hence its algebraic degree is $n - t$. This is an improvement over the degree of the permutations used in Theorem 6.3.2 and Theorem 6.3.3, which are quadratic. Also, notice that the parameter t in Theorem 6.3.5 is not required to be odd, which is another improvement over Theorem 6.3.3.*

Example 6 *Let $m = 2n = 4t$ and $t = 3$. The polynomial $x^6 + x^4 + x^3 + x + 1$ is irreducible over $\mathbb{F}_2$, hence we can represent $\mathbb{F}_{2^6}$ as $\mathbb{F}_2(\alpha)$, where $\alpha^6+\alpha^4+\alpha^3+\alpha+1 = 0$. The set $B = \{1, \alpha, \ldots, \alpha^5\}$ is a basis of $\mathbb{F}_{2^6}$ over $\mathbb{F}_2$. Let $a_1 = \alpha + \alpha^5$, $a_2 = \alpha+\alpha^4+\alpha^5$, and $a_3 = 1$. Because $a_i^{2^3} - a_i = 0$, for $i \in \{1, 2, 3\}$, and because a_1, a_2, and a_3 are linearly independent over $\mathbb{F}_2$ we deduce that $\mathbb{F}_{2^3}$ is given by $\langle a_1, a_2, a_3\rangle$. Then, the indicator of $\mathbb{F}_{2^3}$ is given by $\mathbb{1}_{\mathbb{F}_{2^3}}(y) = y^{56}+y^{49}+y^{42}+y^{35}+y^{28}+y^{21}+y^{14}+y^7+1$, for all $y \in \mathbb{F}_{2^6}$, and its algebraic degree is $n-t = 3$. Define $\pi_i(y) = a_i y + \mathbb{1}_{\mathbb{F}_{2^3}}(y)$, for $i = 1, 2$. We write $x = x_1+x_2\alpha+\cdots+x_6\alpha^5 \in \mathbb{F}_{2^6}$ and also $y = x_7+x_8\alpha+\cdots+x_{12}\alpha^5 \in \mathbb{F}_{2^6}$. Define the function $F\colon \mathbb{F}_2^{12} \to \mathbb{F}_2^2$ by*

$$F(x, y) = F(x_1, \ldots, x_{12}) = \begin{bmatrix} f_1(x_1, \ldots, x_{12}) \\ f_2(x_1, \ldots, x_{12}) \end{bmatrix} = \begin{bmatrix} (x_1, \ldots, x_6) \cdot \pi_1(x_7, \ldots, x_{12}) \\ (x_1, \ldots, x_6) \cdot \pi_2(x_7, \ldots, x_{12}) \end{bmatrix},$$

where the dot product is used instead of trace in Theorem 6.3.5. With the identification of $\mathbb{F}_2^6$ and $\mathbb{F}_{2^6}$ above, we can specify algebraic normal forms of the coordinate functions f_1 and f_2 of the function $F\colon \mathbb{F}_2^{12} \to \mathbb{F}_2^2$ in the following way:

$$\begin{aligned} f_1(x_1, \ldots, x_{12}) = {} & x_1x_8x_9x_{10} + x_1x_8x_9 + x_1x_8x_{10}x_{11} + x_1x_8x_{10} + x_1x_8x_{11} + \\ & x_1x_9x_{10}x_{11}+x_1x_9x_{10}x_{12}+x_1x_9x_{10}+x_1x_9x_{11}+x_1x_9x_{12}+x_1x_9+x_1x_{10}x_{11}x_{12}+ \\ & x_1x_{10}x_{11} + x_1x_{10}x_{12} + x_1x_{11}x_{12} + x_1x_{12} + x_1 + x_2x_7 + x_2x_8 + x_2x_9 + x_2x_{10} + \\ & x_2x_{12} + x_3x_8 + x_3x_9 + x_3x_{10} + x_3x_{11} + x_4x_8 + x_4x_9 + x_4x_{12} + x_5x_8 + x_5x_9 + \\ & x_5x_{11} + x_6x_7 + x_6x_9 + x_6x_{10} + x_6x_{12}, \end{aligned}$$

$$\begin{aligned} f_2(x_1, \ldots, x_{12}) = {} & x_1x_8x_9x_{10} + x_1x_8x_9 + x_1x_8x_{10}x_{11} + x_1x_8x_{10} + x_1x_8x_{11} + \\ & x_1x_9x_{10}x_{11} + x_1x_9x_{10}x_{12} + x_1x_9x_{10} + x_1x_9x_{11} + x_1x_9x_{12} + x_1x_{10}x_{11}x_{12} + \\ & x_1x_{10}x_{11} + x_1x_{10}x_{12} + x_1x_{11}x_{12} + x_1x_{12} + x_1 + x_2x_8 + x_2x_{12} + x_3x_7 + x_3x_9 + \\ & x_4x_9 + x_4x_{11} + x_5x_7 + x_5x_8 + x_5x_9 + x_5x_{11} + x_5x_{12} + x_6x_7 + x_6x_8 + x_6x_9 + \\ & x_6x_{10} + x_6x_{12}. \end{aligned}$$

Define the matrix $A \in GL(12, \mathbb{F}_2)$, as in Remark 2 (Chapter 5), i.e.,

$$A = \left(\begin{array}{cccccc|cccccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{array}\right).$$

Then, we get that $\nu((x_1, \ldots, x_{12})A) = s_2(x_1, \ldots, x_{12})$, up to some linear terms (Remark 2). Again, ignoring the linear terms, since they do not affect the bent-negabent property, we conclude that $F((x_1, \ldots, x_{12})A)$ is a vectorial bent-negabent function.

6.3.2.2 Vectorial bent-negabent functions outside the $\mathcal{M}^{\#}$ class from vector spaces of complete mappings

By a slight modification of the construction in Theorem 6.3.5, using functions in the $\mathcal{C}$ class instead, we can also construct vectorial bent-negabent functions which are weakly outside the $\mathcal{M}^{\#}$ class.

In the rest of this subsection, we will continue to use dot product instead of trace in a finite field, but at the same time we will also use the multiplication in the finite field. The symbol "$\cdot$" will represent the dot product in $\mathbb{F}_2^n$ between two elements, even when we have two field elements $x, y \in \mathbb{F}_{2^n}$; it is possible, since the finite field $\mathbb{F}_{2^n}$ is a vector space over $\mathbb{F}_2$, and hence it is isomorphic to the vector space $\mathbb{F}_2^n$. For simplicity, we will write $x \cdot y$ for the dot product between x and y instead of the formally correct $L(x) \cdot L(y)$, where L is an isomorphism between $\mathbb{F}_{2^n}$ and $\mathbb{F}_2^n$, and we will write xy for the product in the finite field. Furthermore, when we deal with a tower of finite fields such that $\mathbb{F}_{2^t}$ is a subfield of $\mathbb{F}_{2^k}$, and $\mathbb{F}_{2^k}$ is a subfield of $\mathbb{F}_{2^n}$, we will use a basis for $\mathbb{F}_{2^n}$ of the form $\{1, v_1, \ldots, v_{n-1}\}$, such that $\{1, v_1, \ldots, v_{t-1}\}$ is a basis for $\mathbb{F}_{2^t}$, and $\{1, v_1, \ldots, v_{k-1}\}$ is a basis for $\mathbb{F}_{2^k}$. Note that it is always possible to find such a basis, because, we can start with any basis for $\mathbb{F}_{2^t}$ over $\mathbb{F}_2$ of the form $B_1 = \{1, v_1, \ldots, v_{t-1}\}$, and since $\mathbb{F}_{2^t}$ is a subfield of $\mathbb{F}_{2^k}$ (hence also a subspace) we can extend B_1 to a basis $B_2 = \{1, v_1, \ldots, v_{k-1}\}$ for $\mathbb{F}_{2^k}$ over $\mathbb{F}_2$, and similarly, we can extend B_2 to a basis $B_3 = \{1, v_1, \ldots, v_{n-1}\}$ for $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, and B_3 is a basis of the desired form. In order to identify $\mathbb{F}_{2^n}$ with $\mathbb{F}_2^n$, we will use the isomorphism, which maps the basis $\{1, v_1, \ldots, v_{n-1}\}$ to the standard basis $\{\mathbb{e}_1, \mathbb{e}_2, \ldots, \mathbb{e}_n\}$ of $\mathbb{F}_2^n$, where $\mathbb{e}_i \in \mathbb{F}_2^n$ is the i-th unit vector.

In the following theorem, using bent functions from the $\mathcal{C}$ class, we derive another construction of Boolean bent-negabent functions weakly outside the $\mathcal{M}^{\#}$ class.

Theorem 6.3.6 *Let $E = \mathbb{F}_{2^k}$ be a subfield of $\mathbb{F}_{2^n}$, $k \geq 6$, $W = \mathbb{F}_{2^t}$ be a proper subfield of $\mathbb{F}_{2^k}$, and let $a \in \mathbb{F}_{2^t} \setminus \{0\}$. Then the function f defined by $f(x, y) = x \cdot (ay + \mathbb{1}_W(y)) + \mathbb{1}_{E^\perp}(x)$, for all $x, y \in \mathbb{F}_{2^n}$, is a bent function outside the $\mathcal{M}^{\#}$ class.*

Proof. Since a is a nonzero element of $\mathbb{F}_{2^t}$, the linear mapping $L(y) = ay$ is a permutation of $\mathbb{F}_{2^n}$, and it maps $\mathbb{F}_{2^t}$ to $\mathbb{F}_{2^t}$. The mapping $\mathbb{1}_{\mathbb{F}_{2^t}}(y)$ is constant on the cosets of $\mathbb{F}_{2^t}$, and it obviously has values in $\mathbb{F}_{2^t}$ only. Hence, from Lemma 6.3.4, we deduce that $y \in \mathbb{F}_{2^n} \mapsto ay + \mathbb{1}_{\mathbb{F}_{2^t}}(y)$ is a permutation, and since $\mathbb{F}_{2^t}$ is a subfield of $\mathbb{F}_{2^k}$, it maps cosets of $\mathbb{F}_{2^k}$ to cosets of $\mathbb{F}_{2^k}$, and so f is a bent function in the $\mathcal{C}$ class.

In order to prove that f is outside of the $\mathcal{M}^{\#}$ class we could use results from Chapter 4 (namely Theorem 4.2.1). However, for the sake of completeness and clarity, we present an explicit proof here.

To show that f is outside the $\mathcal{M}^{\#}$ class, we need to show that there exists no n-dimensional subspace V of $\mathbb{F}_2^{2n}$ such that $D_v D_w f = 0$, for all $v, w \in V$, see Lemma 2.2.1. Since the function $(x, y) \mapsto D_v D_w(x \cdot ay)$ is constant for all $v, w \in V$, it is enough to show that $(x, y) \mapsto D_v D_w(x \cdot \mathbb{1}_W(y)) + D_v D_w \mathbb{1}_{E^\perp}(x)$ is non-constant, for some elements in $v, w \in V$. In order to prove this, we consider the algebraic normal form of $(x, y) \mapsto D_v D_w(x \cdot \mathbb{1}_W(y)) + D_v D_w \mathbb{1}_{E^\perp}(x)$, which is given

by

$$D_v D_w(x_1(\prod_{i=t+1}^{n}(y_i+1)) + D_v D_w \prod_{i=1}^{k}(x_i+1). \tag{6.3}$$

For any two vectors $v, w \in \mathbb{F}_2^{2n}$, the second-order derivative $D_v D_w \prod_{i=1}^{k}(x_i+1)$ is of degree $k-2$ if the restrictions of v and w to the first k "x"-coordinates are two different nonzero vectors; otherwise, it is 0 (follows from Lemma 2.1.1). Similarly for $D_v D_w \prod_{i=t+1}^{n}(y_i+1)$, it is of degree $n-t-2$ if the restrictions of v and w to the last $n-t$ "y"-coordinates are two different nonzero vectors. Hence, in order to show that there are two vectors $v, w \in V$ such that $D_v D_w f$ is non-constant, from (6.3), we deduce that it is enough to show that there are two vectors $v, w \in V$ such that their restrictions to the first k "x"-coordinates are two different nonzero vectors, or such that their restrictions to the last $n-t$ "y"-coordinates are two different nonzero vectors.

Consider the following subspaces $K, T \subset \mathbb{F}_2^n$ and $S \subset \mathbb{F}_2^{2n}$, which are given by $K = \langle e_1, e_2, \ldots, e_k \rangle$, $T = \langle e_{t+1}, e_{t+2}, \ldots, e_n \rangle$ and $S = (K \times \{0_n\}) \oplus (\{0_n\} \times T)$. Denote by U the subspace $V \cap S$.

Assume that there are three linearly independent vectors in U. Denote them by u_1, u_2 and u_3. If the restriction of u_1, u_2 and u_3 to the the first k "x"-coordinates is the zero vector, then from the definition of S we have that their restriction to the last $n-t$ "y"-coordinates are three different nonzero vectors, since they are linearly independent. Assume now that in the restrictions of u_1, u_2 and u_3 to the the first k "x"-coordinates there is only one nonzero vector. Without loss of generality, we can assume that the restriction of u_1 to the first k "x"-coordinates is nonzero. By possibly adding u_1 to u_2 or u_3, we can assume that the restriction of u_2 and u_3 to the first k "x"-coordinates is the zero vector. Then, because u_2 and u_3 are linearly independent, from the definition of S, we deduce that the restrictions of u_2 and u_3 to the last $n-t$ "y"-coordinates are two different nonzero vectors. Hence, we conclude that, in order to show that there are two vectors in V such that their restrictions to the first k "x"-coordinates are two different nonzero vectors, or such that their restrictions to the last $n-t$ "y"-coordinates are two different nonzero vectors, it is enough to prove that $\dim U \geq 3$.

Because V and S are subspaces of $\mathbb{F}_2^{2n}$, we have

$$\dim U = \dim(V \cap S) = \dim V + \dim S - \dim(V + S).$$

We know that $\dim V = n$, $\dim S = k+n-t$ and $\dim(V+S) \leq 2n$, so $\dim(V \cap S) \geq n+n+k-t-2n = k-t \geq k/2 \geq 3$, since $k \geq 6$. Thus, we conclude that there are two vectors $v, w \in V$ such that $D_v D_w f$ is non-constant. In this way, since V was an arbitrary n-dimensional subspace of $\mathbb{F}_2^{2n}$, f is a bent function outside $\mathcal{M}^{\#}$. ∎

We can use Theorem 6.3.6 along with the ideas used in the proof of Theorem 6.3.5 to construct vectorial bent-negabent functions weakly outside $\mathcal{M}^{\#}$.

Theorem 6.3.7 *Let $E = \mathbb{F}_{2^k}$ be a subfield of $\mathbb{F}_{2^n}$, $n \geq 6$, and let $\mathbb{F}_{2^t}$ be a proper subfield of $\mathbb{F}_{2^k}$. Set $a_1 = 1$, and let $a_1, \ldots, a_t$ be a basis for $\mathbb{F}_{2^t}$ over $\mathbb{F}_2$. Denote by $L_i \colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ the permutation defined by $L_i(y) = a_i y$, and denote by $\pi_i \colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$*

the function defined by $\pi_i(y) = L_i(y) + \mathbb{1}_{\mathbb{F}_{2^t}}(y)$. *Then, the function* $F : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \to \mathbb{F}_2^{t-1}$ *defined by*

$$F(x,y) = \begin{bmatrix} x \cdot \pi_1(y) + \mathbb{1}_{E^\perp}(x) \\ \vdots \\ x \cdot \pi_{t-1}(y) + \mathbb{1}_{E^\perp}(x) \end{bmatrix}$$

is affine equivalent to a vectorial bent-negabent function, and it is weakly outside $\mathcal{M}^{\#}$ *with* 2^{t-2} *bent components in* $\mathcal{C} \setminus \mathcal{M}^{\#}$.

Proof. Choose an arbitrary non-empty subset S of $\{1, \ldots, t-1\}$ and fix it. First, we will show that the component function given by $(x,y) \mapsto \sum_{i \in S}(x \cdot \pi_i(y) + \mathbb{1}_{E^\perp}(x)) = x \cdot \sum_{i \in S} \pi_i(y) + \sum_{i \in S} \mathbb{1}_{E^\perp}(x)$ is a bent function. From the definition of π_i's, we have $\sum_{i \in S} \pi_i(y) = \sum_{i \in S}(a_i y + \mathbb{1}_{\mathbb{F}_{2^t}}(y))$.

If the number of elements in S is even, then (similarly to Theorem 6.3.5) we have that $(x,y) \mapsto \sum_{i \in S} x \cdot \pi_i(y)$ is a bent function in $\mathcal{M}$. On the other hand, if the cardinality of S is odd, then $\sum_{i \in S} \pi_i(y) = (\sum_{i \in S} a_i)y + \mathbb{1}_{\mathbb{F}_{2^t}}(y)$. Since $b := \sum_{i \in S} a_i$ is a nonzero element of $\mathbb{F}_{2^t}$, we deduce from Theorem 6.3.6 that $(x,y) \mapsto \sum_{i \in S} x \cdot \pi_i(y) + \mathbb{1}_{E^\perp}(x)$ is a bent function in the $\mathcal{C}$ class outside $\mathcal{M}^{\#}$. In this way, F is a vectorial bent function, weakly outside the $\mathcal{M}^{\#}$ class. Similarly to the proof of Theorem 6.3.5, we get that F is affine equivalent to a vectorial bent-negabent function. ∎

Open problem 6.3.1 *None of the vectorial bent-negabent functions specified in Section 6.3 reaches the maximum dimension of the output space given in Theorem 5.2.2, unless the algebraic degree of the permutations used is equal to one (for example, setting* $t = n$ *in Theorem 6.3.5). Is there a vector space of complete permutations of* $\mathbb{F}_2^n$*, some of which have the algebraic degree greater than one, whose dimension is equal to* $n-1$*? In other words, provide new constructions of non-quadratic vectorial bent-negabent functions with maximum output dimension.*

In this context, we recall that it was conjectured by R.J. Evans et al. *[25] that if* $F(x) + cx$ *is a permutation over* $\mathbb{F}_q$ *for at least* $q/2$ *different values* $c \in \mathbb{F}_q$*, then* F *is necessarily a linearized polynomial over* $\mathbb{F}_q$.

6.4 Vectorial bent functions from the $\mathcal{C}$ class strongly outside $\mathcal{M}^{\#}$

In this section, we will present an approach to construct vectorial bent functions $F : \mathbb{F}_2^{2n} \to \mathbb{F}_2^k$, which are strongly outside the $\mathcal{M}^{\#}$ class, for some dimensions k. Again, we identify the finite field $\mathbb{F}_{2^n}$ with the vector space $\mathbb{F}_2^n$ via the natural isomorphism. However, since the connection between the finite field and the vector space representation will be a bit more delicate in this section, in order to avoid any confusion, when $x \in \mathbb{F}_{2^n}$, we will denote by $\overline{x}$ the corresponding vector in $\mathbb{F}_2^n$. Nevertheless, "$\cdot$" will always denote the dot product on $\mathbb{F}_2^n$. The following theorem specifies some monomial permutations $\phi(x) = x^d$ which are later employed in our construction.

Theorem 6.4.1 *[41, Theorem 5.8] Suppose $\phi(x) = x^{2^r+1}$, for all $x \in \mathbb{F}_{2^n}$, where $\gcd(r,n) = e$ and n/e is odd (which implies $\gcd(2^n-1, 2^r+1) = 1$).*

(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) 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.

We will now specify a set of 2-dimensional subspaces L_i of $\mathbb{F}_2^n$ such that any function $f_i(x,y) = \overline{\pi_i(y)} \cdot x + \mathbb{1}_{L_i^{\perp}}(x)$ is in $\mathcal{C}$ but outside $\mathcal{M}^{\#}$. Let $\{1, \alpha_1, \ldots, \alpha_{e-1}\}$ be a set of elements in $\mathbb{F}_{2^e} < \mathbb{F}_{2^n}$ such that $\{\overline{1}, \overline{\alpha_1}, \ldots, \overline{\alpha_{e-1}}\}$ is a set of linearly independent vectors in $\mathbb{F}_2^n$. Consider a permutation $\phi : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ defined by $\phi(y) = y^{2^r+1}$, where $\gcd(r,n) = e$, n/e is odd and $e \geq 3$. Furthermore, we can specify $\pi(y) = \phi(y)^{-1} = y^d$, and set $\pi_i(y) = \alpha_i y^d$, for $i \in \{1, 2, \ldots, e-1\}$. Set $L_i = \langle \overline{1}, \overline{\alpha_i}\rangle \subset \mathbb{F}_2^n$. This is in accordance with Theorem 6.4.1 (taking $u = 1$). Since L_i are 2-dimensional subspaces, then $\dim(L_i^{\perp}) = n-2$. Furthermore, we have:

$$\mathbb{1}_{L_i^{\perp}}(x) = (\overline{1} \cdot x + 1)(\overline{\alpha_i} \cdot x + 1).$$

Define $f_i(x,y) = \overline{\pi_i(y)} \cdot x + \mathbb{1}_{L_i^{\perp}}(x)$, for all $x \in \mathbb{F}_2^n$, $y \in \mathbb{F}_{2^n}$. The inverse permutation of π_i is given by $\pi_i^{-1}(y) = c_i y^{2^r+1} = c_i\phi(y)$, where $c_i = \alpha_i^{-(2^r+1)}$. From Theorem 6.4.1, we deduce that ϕ maps cosets of L_i to affine subspaces, and so, $\pi_i^{-1} = c_i\phi$ maps cosets of L_i to affine subspaces as well. This means that f_i are bent functions in the $\mathcal{C}$ class. The next result describes how to use functions f_i to define vectorial bent functions strongly outside $\mathcal{M}^{\#}$.

Theorem 6.4.2 *Let n and r be integers satisfying $n \geq 5$, $r < n$, $\gcd(n,r) = e$, where $e \geq 3$ and n/e is odd. Define a permutation $\phi(y) = y^{2^r+1}$ over $\mathbb{F}_{2^n}$ and its inverse $\pi(y) = \phi(y)^{-1} = y^d$. Let $\{1, \alpha_1, \ldots, \alpha_{e-1}\} \subset \mathbb{F}_{2^e} < \mathbb{F}_{2^n}$ be a set of linearly independent elements (over $\mathbb{F}_2$). Set $L_i = \langle \overline{1}, \overline{\alpha_i}\rangle \subset \mathbb{F}_2^n$, $\pi_i = \alpha_i\pi$, and $f_i(x,y) = \overline{\pi_i(y)} \cdot x + \mathbb{1}_{L_i^{\perp}}(x)$, for $i \in \{1, \ldots, e-1\}$. Then, $F : \mathbb{F}_2^{2n} \to \mathbb{F}_2^{e-1}$ defined by*

$$F = (f_1, f_2, \ldots, f_{e-1})$$

is a vectorial bent function in $\mathcal{C}$ strongly outside $\mathcal{M}^{\#}$.

Proof. We need to show that for every non-empty subset $S \subseteq \{1, 2, \ldots, e-1\}$ the linear combination $\sum_{i \in S} f_i$ is a bent function outside the $\mathcal{M}^{\#}$ class. Let $S \subseteq \{1, 2, \ldots, e-1\}$ be arbitrary and non-empty. From the discussion preceding the theorem, we know that $f_i(x,y) = \overline{\alpha_i\pi(y)} \cdot x + (\overline{1} \cdot x + 1)(\overline{\alpha_i} \cdot x + 1)$, and so

$$\sum_{i \in S} f_i(x,y) = \overline{\left(\left(\sum_{i \in S} \alpha_i\right)\pi(y)\right)} \cdot x + \left(\overline{1} \cdot x + 1\right)\left(\left(\sum_{i \in S} \overline{\alpha_i}\right) \cdot x + \sum_{i \in S} 1\right).$$

Since $\{\overline{1}, \overline{\alpha_1}, \ldots, \overline{\alpha_{e-1}}\}$ is a set of linearly independent vectors, $c_S := \sum_{i \in S} \alpha_i$ is a nonzero element of $\mathbb{F}_{2^e} < \mathbb{F}_{2^n}$ different from 1 and the above equation can be rewritten as

$$\begin{aligned} \textstyle\sum_{i \in S} f_i(x,y) &= \overline{c_S \pi(y)} \cdot x + (\overline{1} \cdot x + 1)(\overline{c_S} \cdot x + \textstyle\sum_{i \in S} 1) \\ &= \overline{c_S \pi(y)} \cdot x + (\overline{1} \cdot x + 1)(\overline{c_S} \cdot x + 1) + (\overline{1} \cdot x + 1)(1 + \textstyle\sum_{i \in S} 1). \end{aligned}$$

Because $(\overline{1} \cdot x + 1)(1 + \sum_{i \in S} 1)$ is an affine function, it is enough to show that $\overline{c_s \pi(y)} \cdot x + (\overline{1} \cdot x + 1)(\overline{c_S} \cdot x + 1)$ is a bent function in the $\mathcal{C}$ class outside $\mathcal{M}^{\#}$. We denote $(c_S \pi)^{-1} := b_S \phi$, where $b_S = c_S^{-(2^r+1)}$, and denote by E_S the two dimensional subspace $\langle \overline{1}, \overline{c_S} \rangle$ of $\mathbb{F}_2^n$. From Theorem 6.4.1 we deduce that ϕ maps cosets of E_S to affine subspaces, and so, $b_S \phi$ maps cosets of E_S to affine subspaces as well. This means that $\overline{c_s \pi(y)} \cdot x + (\overline{1} \cdot x + 1)(\overline{c_s} \cdot x + 1)$ is a bent function in the $\mathcal{C}$ class.

Since $n \geq 5$, we know that $wt(d) \geq 3$, see Lemma 10 in [84]. We deduce from results in [19] that $\pi(y) = y^d$ has no (non-trivial) component functions with nonzero linear structures, and so the same is true for $c_S \pi$ as well. From Theorem 4.1.1, we deduce that $\overline{c_S \pi(y)} \cdot x + (\overline{1} \cdot x + 1)(\overline{c_s} \cdot x + 1) = \overline{c_S \pi(y)} \cdot x + 1_{E_S^{\perp}}(x)$ is a bent function in the $\mathcal{C}$ class outside $\mathcal{M}^{\#}$, and so, $\sum_{i \in S} f_i$ is a bent function outside the $\mathcal{M}^{\#}$ class. Since S was an arbitrary non-empty subset of $\{1, 2, \ldots, e-1\}$, the statement is proved. ■

Chapter 7

Correlation immune functions with low Hamming weight

For cryptographic applications, the notion of correlation immunity (CI) is commonly related to the so-called nonlinear combiner model as a representative of certain family of stream ciphers [46]. This property is crucial for this model in order to withstand correlation attacks [30, 31, 45, 68]. Most often, a closely related notion of resiliency is used as a cryptographic criterion which, apart from a certain order of correlation immunity of the combining Boolean function, also requires its balancedness. Apart from this application, a subclass of minimum weight CI functions has received a lot of attention recently due to their use as masking primitives for the purpose of hardware protection of certain cipher families [4], see also [16]. In addition, CI functions are closely related to secret-sharing schemes and error-correcting codes [6, 23, 26].

A tight bound for the achievable algebraic degree of correlation immune functions was given by T. Siegenthaler [67]. G.Z. Xiao and J.L. Massey [81] showed that a Boolean function is kth-order correlation immune if and only if its Walsh-Hadamard transform values are equal to zero for all the vectors whose Hamming weight is in the range $\{1, \ldots, k\}$. In addition to the Walsh-Hadamard spectral characterization, CI Boolean functions can be characterized using orthogonal arrays [6], and in terms of Fourier spectra [79]. The proof of Xiao and Massey [81], regarding the spectral characterization of CI functions, was later simplified by P. Sarkar [63] and it then became a standard proof used in the textbooks, see e.g. [20]. Yet another approach in this direction was taken by C. Carlet [12], where the so-called numerical normal form (NNF) was used for the purpose of providing the most elegant and concise proof (though addressing the resiliency).

In the first part of this chapter, in Section 7.1, we show that using certain weight divisibility results related to restrictions of CI functions (taken from [73], see Proposition 2.4.1), an elegant and compact proof of Siegenthaler's bound on the algebraic degree can be deduced. In addition, we specify precisely the weight of k-th order CI functions having (all) terms of degree $n - k$ in its algebraic normal form, cf. Theorem 7.1.2. Using the same divisibility results, we also exactly determine the Walsh spectral values at vectors of weight $k + 1$ for k-th order correlation immune Boolean functions.

In the second part of this chapter, in Section 7.2, we present two efficient constructions of CI functions which are well-suited for designing a subclass of these functions having low Hamming weight. Such functions have an immediate applications as masking schemes for protecting ciphers against side-channel cryptanalysis [16]. As remarked in [15], for an efficient hardware implementation CI functions need to have as low weight as possible. Nevertheless, most of the known constructions (such as for instance the primary Maiorana-McFarland construction and secondary constructions like the indirect sum, see for example [12], [24]) do not allow to build functions with such property, which initiated rather extensive research in this direction. More precisely, for a relatively low size of the input space (for $n \leq 13$) the minimum weight of CI functions has been determined and tabulated in [16] apart from a few unknown values and some of the remaining cases were handled the subsequent work of Q. Wang and Y. Li [78]. Following the notation introduced by C. Carlet and X. Chen in [16], thus denoting the minimum weight of any n-variable k-th order CI function by $\omega_{n,k}$, the values of $\omega_{12,4}$, $\omega_{13,4}$ and $\omega_{13,5}$ have been determined in [78]. For the special case of 3-CI functions Carlet and Chen conjectured that $w_{n,3} = 8\lceil \frac{n}{4} \rceil$, for any integer $n \geq 3$, and it was shown by construction that the conjecture is true for $n = 2^r$, for all $r \geq 3$. Later, it was shown [76] that this conjecture is equivalent to the famous conjecture of J. Hadamard which claims that there exists a Hadamard matrix of order $4t$ for every positive integer t. Notice that the case when $n = 2^r$ then corresponds to Silvester-Hadamard matrices using this equivalency. We provide the further evidence that the conjecture of Carlet and Chen is true through a generalized design method of CI-functions. More precisely, it is shown through the existence of 3-CI functions of minimum weight that the conjecture is true for any n of the form $n = 2^r - i$ and $n = 3 \cdot 2^r - i$, for $i = 0, 1, 2, 3$ and $r \geq 3$.

7.1 On the algebraic degree of correlation immune functions

In [67], T. Siegenthaler defined the notion of correlation immunity of Boolean functions and provided a necessary condition to satisfy this property in terms of their maximum achievable algebraic degree, known as Siegenthaler's bound. G.Z. Xiao and J.L. Massey [81] provided a spectral characterization of CI functions and they slightly extended the result of Siegenthaler by showing certain regularities in the algebraic normal forms of this class of functions. These proofs were somewhat complicated and in his note [63] P. Sarkar gave simplified proofs of these results which then became standard versions used in books (see for example [20]). In this section, using the weight divisibility results from [73], we will further simplify these proofs and at the same time derive some new results related to the characterization of CI functions.

The following result considers an alternative method of proving Siegenthaler's bound.

Theorem 7.1.1 *Let f be an n-variable k-th order correlation immune function. Then, the algebraic degree of f is at most $n - k$.*

PROOF. We use the algebraic normal form of f, which is given by:

$$f(x) = \sum_{w=(w_1,\ldots,w_n)\in\mathbb{F}_2^n} (\sum_{\substack{t\preceq w\\ t\in\mathbb{F}_2^n}} f(t)) x_1^{w_1} x_2^{w_2} \cdots x_n^{w_n}.$$

It is enough to prove that $\sum_{t\preceq w} f(t) = 0 \bmod 2$, for $\mathrm{wt}(w) > n-k$. Fix $w \in \mathbb{F}_2^n$, with $\mathrm{wt}(w) = n-i > n-k$. Let $1 \le d_1 < d_2 \cdots < d_i \le n$ be the integers for which $w_{d_j} = 0$, $j = 1, \ldots, i$. Then

$$\sum_{t\preceq w} f(t) = \mathrm{wt}(f^{0,0,\ldots,0}_{d_1,d_2,\ldots,d_i}) = \mathrm{wt}(f)/2^i,$$

because f is also an i-CI function for $i < k$. Since f is a k-CI function, $\mathrm{wt}(f)$ is divisible by 2^k, so $\mathrm{wt}(f)/2^i = 0 \bmod 2$, for $i < k$. We conclude that $\sum_{t\preceq w} f(t) = 0 \bmod 2$. ∎

Now we will give a simpler proof of the result of G.Z. Xiao and J.L. Massey from [81], which is the first part of the next theorem. The second part is the extension of their result and to the best of our knowledge is new.

Theorem 7.1.2 *Let f be an n-variable, k-CI function. Then, either f has all terms of degree $n-k$, or no terms of degree $n-k$ at all. Furthermore, f has all terms of degree $n-k$ if and only if $\mathrm{wt}(f) = 2^k m$, where m is odd.*

PROOF. Let $w \in \mathbb{F}_2^n$ such that $\mathrm{wt}(w) = n-k$, and let $d_1, \ldots, d_k$ be the integers such that $w_{d_j} = 0$, $j = 1, \ldots, k$. As in the proof of Theorem 7.1.1, we have that

$$\sum_{t\preceq w} f(t) = \mathrm{wt}(f^{0,0,\ldots,0}_{d_1,d_2,\ldots,d_k}) = \mathrm{wt}(f)/2^k.$$

So, the sum $\sum_{t\preceq w} f(t)$ does not really depend on the choice of w with weight $n-k$, hence we have that either f has all terms of degree $n-k$, or no terms of degree $n-k$ at all. Furthermore, $\mathrm{wt}(f)/2^k = 1 \bmod 2$ if and only if $\mathrm{wt}(f) = 2^k m$, where m is odd, so f has all terms of degree $n-k$ if and only if $\mathrm{wt}(f) = 2^k m$, where m is odd. ∎

As a corollary, we get Siegenthaler's bound for resilient functions.

Corollary 7.1.3 *If f is an n-variable balanced k-CI Boolean function (thus k-resilient) with $k < n-1$, then the degree of f is at most $n-k-1$.*

PROOF. Follows from Theorem 7.1.1 and 7.1.2 and the fact that $\mathrm{wt}(f) = 2^{n-1}$ as f is balanced. ∎

The following result specifies the Walsh-Hadamard coefficients at vectors of weight $k+1$ for a given k-CI Boolean function.

Theorem 7.1.4 *Let f ba an n-variable, k-CI function, $k < n$, and let $w \in \mathbb{F}_2^n$ such that $\mathrm{wt}(w) = k+1$. Let $\{i_1, \ldots, i_k, i_{k+1}\} \subset \{1, 2, \ldots, n\}$ be the set of nonzero coordinates of w. Then*

$$W_f(w) = 2^{k+1}\left(\mathrm{wt}(f)/2^k - 2\mathrm{wt}(f^{0,\ldots,0,0}_{i_1,\ldots,i_k,i_{k+1}})\right).$$

PROOF. Without loss of generality, to avoid complicated notation, we assume that $w = (1, \ldots, 1, 0, \ldots, 0)$, so that $\{i_1, \ldots, i_k, i_{k+1}\} = \{1, \ldots, k, k+1\}$. The Walsh-Hadamard coefficient of f at the point w is computed as:

$$W_f(w) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+x\cdot w} = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+x\cdot(1,1,\ldots,1,0,\ldots,0)} = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+x_1+x_2+\cdots+x_{k+1}}.$$

Rewriting the sum, in order to focus on the first k coordinates, we have:

$$\sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+x_1+\cdots+x_{k+1}} = \sum_{v \in \mathbb{F}_2^k} \Big(\sum_{x \in S_0(v)} (-1)^{f(x)} - \sum_{x \in S_1(v)} (-1)^{f(x)} \Big) (-1)^{v_1+\cdots+v_k},$$

where $S_0(v) = \{x \in \mathbb{F}_2^n : (x_1, \ldots, x_k) = v \text{ and } x_{k+1} = 0\}$, and $S_1(v) = \{x \in \mathbb{F}_2^n : (x_1, \ldots, x_k) = v \text{ and } x_{k+1} = 1\}$, for all $v \in \mathbb{F}_2^k$. Notice that

$$\sum_{x \in S_0(v)} (-1)^{f(x)} = 2^{n-k-1} - 2\mathrm{wt}(f^{v_1,\ldots,v_k,0}_{1,\ldots,k,k+1}), \text{ and}$$
$$\sum_{x \in S_1(v)} (-1)^{f(x)} = 2^{n-k-1} - 2\mathrm{wt}(f^{v_1,\ldots,v_k,1}_{1,\ldots,k,k+1}),$$

so we have

$$W_f(w) = 2 \sum_{v \in \mathbb{F}_2^k} (\mathrm{wt}(f^{v_1,\ldots,v_k,1}_{1,\ldots,k,k+1}) - \mathrm{wt}(f^{v_1,\ldots,v_k,0}_{1,\ldots,k,k+1}))(-1)^{v_1+\cdots+v_k}. \tag{7.1}$$

Now, select and fix an arbitrary value of $d \in \{1, 2, \ldots, k\}$. Since f is k-th order correlation immune, we have

$$\mathrm{wt}(f^{v_1,\ldots,v_d,\ldots,v_k,0}_{1,\ldots,d,\ldots,k,k+1}) + \mathrm{wt}(f^{v_1,\ldots,v_d,\ldots,v_k,1}_{1,\ldots,d,\ldots,k,k+1}) = \mathrm{wt}(f^{v_1,\ldots,v_k}_{1,\ldots,k}) = \mathrm{wt}(f)/2^k, \text{ and similarly}$$

$$\mathrm{wt}(f^{v_1,\ldots,v_d\oplus 1,\ldots,v_k,1}_{1,\ldots,d,\ldots,k,k+1}) + \mathrm{wt}(f^{v_1,\ldots,v_d,\ldots,v_k,1}_{1,\ldots,d,\ldots,k,k+1}) = \mathrm{wt}(f)/2^k.$$

Subtracting the second equation from the first, we get:

$$\mathrm{wt}(f^{v_1,\ldots,v_d,\ldots,v_k,0}_{1,\ldots,d,\ldots,k,k+1}) = \mathrm{wt}(f^{v_1,\ldots,v_d\oplus 1,\ldots,v_k,1}_{1,\ldots,d,\ldots,k,k+1}).$$

Similarly

$$\mathrm{wt}(f^{v_1,\ldots,v_d,\ldots,v_k,1}_{1,\ldots,d,\ldots,k,k+1}) = \mathrm{wt}(f^{v_1,\ldots,v_d\oplus 1,\ldots,v_k,0}_{1,\ldots,d,\ldots,k,k+1}).$$

Hence

$$\mathrm{wt}(f^{v_1,\ldots,v_d,\ldots,v_k,1}_{1,\ldots,d,\ldots,k,k+1}) - \mathrm{wt}(f^{v_1,\ldots,v_d,\ldots,v_k,0}_{1,\ldots,d,\ldots,k,k+1}) = - \left(\mathrm{wt}(f^{v_1,\ldots,v_d\oplus 1,\ldots,v_k,1}_{1,\ldots,k,k+1}) - \mathrm{wt}(f^{v_1,\ldots,v_d\oplus 1,\ldots,v_k,0}_{1,\ldots,k,k+1})\right).$$

Combining this equality with the equation (7.1), since d was arbitrary, we have:

$$W_f(w) = 2^{k+1} \left(\mathrm{wt}(f^{0,\ldots,0,1}_{1,\ldots,k,k+1}) - \mathrm{wt}(f^{0,\ldots,0,0}_{1,\ldots,k,k+1})\right).$$

Since f is k-CI, then

$$W_f(w) = 2^{k+1}(\mathrm{wt}(f)/2^k - 2\mathrm{wt}(f^{0,\ldots,0,0}_{1,\ldots,k,k+1})).$$

■

As a corollary, we obtain the same spectral characterization of CI functions as originally derived by G.Z. Xiao and J.L. Massey in [81].

Corollary 7.1.5 *[81] A Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is k-CI if and only if $W_f(w) = 0$, for all $w \in \mathbb{F}_2^n$ with $1 \leq \mathrm{wt}(w) \leq k$.*

Proof. If f is k-CI, then f is also $(d+1)$-CI for all $d < k$. Thus, $\mathrm{wt}(f^{0,0,\ldots,0}_{i_1,i_2,\ldots,i_{d+1}}) = \mathrm{wt}(f)/2^{d+1}$. Theorem 7.1.4 then implies that $W_f(w) = 0$, for all $w \in \mathbb{F}_2^n$ with $1 \leq \mathrm{wt}(w) \leq k$.

Conversely, if f is not k-CI, let d be the largest number such that f is d-CI. Then, there are indices $\{i_1, i_2, \ldots, i_{d+1}\}$ such that $\mathrm{wt}(f^{0,0,\ldots,0}_{i_1,i_2,\ldots,i_{d+1}}) \neq \mathrm{wt}(f)/2^{d+1}$. Consequently $W_f(w) \neq 0$, for $w \in \mathbb{F}_2^n$ defined by $w_j = 1 \Leftrightarrow j \in \{i_1, \ldots, i_{d+1}\}$. ■

As another corollary we have a result about the Walsh-Hadamard coefficients of correlation immune functions with the maximal algebraic degree.

Corollary 7.1.6 *Let f be an n-variable k-CI function and assume that $\mathrm{wt}(f) = 2^k m$, where m is an odd number. Then, $W_f(w) \neq 0$ for all $w \in \mathbb{F}_2^n$ of weight $k+1$.*

Proof. Follows from Theorem 7.1.4 and the fact that $\mathrm{wt}(f)/2^k = m$ is an odd number, while $2\mathrm{wt}(f^{0,0,\ldots,0}_{i_1,i_2,\ldots,i_{k+1}})$ is an even number. ■

7.2 Construction methods for low–weight correlation immune functions

In this section, we give some general construction methods for correlation immune functions, which are quite efficient in the design of their low-weight subclass. One of the most important construction of such functions was given by C. Carlet and X. Chen in [16] and is based on the multiplication of suitable functions on smaller variable spaces. Recall that, following the terminology in [16], $\mathcal{D}_{n,d}$ denotes the set of all d-CI Boolean functions in n-variables whereas $\omega_{n,d}$ stands for the minimal Hamming weight of n-variable d-CI functions.

Theorem 7.2.1 *[16, Corollary 3.2] Let n, d, k be positive integers satisfying $d \leq n$ and $k \geq 2$. Assume that $f_1 \in \mathcal{D}_{n,d}$ and $f_j \in \mathcal{D}_{n,\lfloor \frac{d}{2} \rfloor}$ for any $2 \leq j \leq k$. Define*

$$h\left(x^{(1)}, \ldots, x^{(k)}\right) = f_1\left(x^{(1)}\right) \prod_{i=2}^{k} f_i\left(x^{(i)} + x^{(1)}\right), \quad x^{(1)}, \ldots, x^{(k)} \in \mathbb{F}_2^n.$$

Then, h belongs to $\mathcal{D}_{nk,d}$ and has the Hamming weight $\mathrm{wt}(h) = \prod_{i=1}^{k} \mathrm{wt}(f_i)$.

A generalization which gives a larger class of low-weight CI functions, with greater flexibility with respect to the dimension of subfunctions, is given below.

Theorem 7.2.2 *Let n, d, k be positive integers satisfying $d \leq n$ and $k \geq 2$. Assume that $f_1 \in \mathcal{D}_{n,d}$ and $f_i \in \mathcal{D}_{n_i,\lfloor \frac{d}{2} \rfloor}$, where $n_i \leq n$ for $i = 2, \ldots, k$. For every $2 \leq i \leq k$, let π_i be an injection from $\{1, \ldots, n_i\}$ to $\{1, \ldots, n\}$. Then,*

$$g\left(x^{(1)}, \ldots, x^{(k)}\right) = f_1\left(x^{(1)}\right) \prod_{i=2}^{k} f_i\left(x^{(i)} + \Phi_i(x^{(1)})\right), \quad x^{(1)} \in \mathbb{F}_2^n, x^{(i)} \in \mathbb{F}_2^{n_i}$$

is a d-CI function, where $\Phi_i(x^{(1)})$ denotes the vector $\left(x^{(1)}_{\pi_i(1)}, \ldots, x^{(1)}_{\pi_i(n_i)}\right) \in \mathbb{F}_2^{n_i}$. Furthermore, $\mathrm{wt}(g) = \prod_{i=1}^{k} \mathrm{wt}(f_i)$.

Proof. First, note that $\mathrm{wt}(g) = \prod_{i=1}^{k} \mathrm{wt}(f_i)$. Let us fix d variables $i_1, \ldots, i_d$ in $(x^{(1)}, \ldots, x^{(k)})$ to be $a_{i_1}, \ldots, a_{i_d}$. If in each $x^{(i)}$, for $i = 2, \ldots, k$, we have fixed at most $\lfloor \frac{d}{2} \rfloor$ variables then we have

$$\mathrm{wt}(g^{a_{i_1},\ldots,a_{i_d}}_{i_1,\ldots,i_d}) = \prod_{l=1}^{k} \mathrm{wt}\left((f_l)^{a_{i_1^{(l)}},\ldots,a_{i_{r_l}^{(l)}}}_{i_1^{(l)},\ldots,i_{r_l}^{(l)}}\right) = \frac{1}{2^{r_1}}\mathrm{wt}(f_1) \cdots \frac{1}{2^{r_k}}\mathrm{wt}(f_k) = \frac{1}{2^d} \prod_{i=1}^{k} \mathrm{wt}(f_i),$$

because each f_i is $\lfloor \frac{d}{2} \rfloor$-CI function. Here, $r_i \leq \lfloor \frac{d}{2} \rfloor$ denotes the number of fixed variables in $x^{(i)}$.

Now, assume that for some j we have more than $\lfloor d/2 \rfloor$ variables fixed in $x^{(j)}$. Note that it can only happen for one j, because $2(\lfloor d/2 \rfloor + 1) > d$. Without loss of generality, we can assume that $j = 2$. Suppose that we have fixed $\lfloor d/2 \rfloor + m$ variables in $x^{(2)}$, which w.l.o.g. are taken to be the first $\lfloor d/2 \rfloor + m$ variables. Consequently, we have at least m variables in $x^{(1)}$ among $x^{(1)}_{\pi_2^{-1}(1)}, \ldots, x^{(1)}_{\pi_2^{-1}(\lfloor d/2 \rfloor + m)}$ that are not fixed. Again, we can w.l.o.g. assume that these m variables are $x^{(1)}_{\pi_2^{-1}(1)}, \ldots, x^{(1)}_{\pi_2^{-1}(m)}$.

Let now $b = (b_1, \ldots, b_m) \in \mathbb{F}_2^m$ be arbitrary and fixed. In addition to the already fixed variables, we also fix the variables $(x^{(1)}_{\pi_2^{-1}(1)}, \ldots, x^{(1)}_{\pi_2^{-1}(m)})$ to be $(b_1, \ldots, b_m)$. Because f_1 is d-CI, the weight of the function g with these variables fixed is:

$$\frac{1}{2^{r_1+m}}\mathrm{wt}(f_1)\mathrm{wt}\left((f_2)^{a_1 \oplus b_1,\ldots,a_m \oplus b_m,\ldots,a_{r_2}}_{1^{(2)},\ldots,m^{(2)},\ldots,r_2^{(2)}}\right) \frac{1}{2^{r_3}}\mathrm{wt}(f_3) \cdots \frac{1}{2^{r_k}}\mathrm{wt}(f_k).$$

Obviously, the same is true for every $b \in \mathbb{F}_2^m$. Summing over $b \in \mathbb{F}_2^m$, we get

$$\mathrm{wt}(g^{a_{i_1},\ldots,a_{i_d}}_{i_1,\ldots,i_d}) = \sum_{b \in \mathbb{F}_2^m} \frac{1}{2^{r_1+m}}\mathrm{wt}(f_1)\mathrm{wt}\left((f_2)^{a_1 \oplus b_1,\ldots,a_m \oplus b_m,\ldots a_{r_2}}_{1^{(2)},\ldots,m^{(2)},\ldots,r_2^{(2)}}\right) \frac{1}{2^{r_3}}\mathrm{wt}(f_3) \cdots \frac{1}{2^{r_k}}\mathrm{wt}(f_k).$$

On the other hand, we have that

$$\sum_{b \in \mathbb{F}_2^m} \mathrm{wt}\left((f_2)^{a_1 \oplus b_1,\ldots,a_m \oplus b_m,\ldots,a_{r_2}}_{1^{(2)},\ldots,m^{(2)},\ldots,r_2^{(2)}}\right) = \mathrm{wt}\left((f_2)^{a_{m+1},\ldots,a_{r_2}}_{m+1^{(2)},\ldots,r_2^{(2)}}\right) = \frac{1}{2^{\lfloor d/2 \rfloor}}\mathrm{wt}(f_2),$$

because f_2 is a $\lfloor d/2 \rfloor$-CI function. Finally, we deduce that

$$\mathrm{wt}(g_{i_1,\ldots,i_d}^{a_{i_1},\ldots,a_{i_d}}) = \frac{1}{2^{r_1+m}}\mathrm{wt}(f_1)\frac{1}{2^{\lfloor d/2 \rfloor}}\mathrm{wt}(f_2)\frac{1}{2^{r_3}}\mathrm{wt}(f_3)\cdots\frac{1}{2^{r_k}}\mathrm{wt}(f_k) = \frac{1}{2^d}\prod_{i=1}^{k}\mathrm{wt}(f_i),$$

and since $\mathrm{wt}(g) = \prod_{i=1}^{k}\mathrm{wt}(f_i)$, we conclude that g is a d-CI function. ∎

Example 7 *This example demonstrates how to use Theorem 7.2.2 to construct CI-functions with low Hamming weight from CI-functions in a smaller number of variables. For the sake of simplicity, we will keep the number of variables low. Using the same notation as in Theorem 7.2.2, set* $n = 3$, $d = 2$ *and* $k = 3$. *Let* $n_2 = n_3 = 2$, *and* $\pi_2, \pi_3 \colon \{1,2\} \to \{1,2,3\}$, *be defined by* $\pi_2(1) = 1$; $\pi_2(2) = 2$, *and* $\pi_3(1) = 2$; $\pi_3(2) = 3$. *In order to apply Theorem 7.2.2 in this setting, we need to find one* 2*-CI function* f_1 *in* 3 *variables, and two* 1*-CI functions* f_2, f_3 *in* 2 *variables. Let*

$$f_1(x_1,x_2,x_3) = x_1+x_2+x_3, \quad f_2(x_4,x_5) = x_4+x_5+1, \text{ and } f_3(x_6,x_7) = x_6+x_7.$$

From the characterization of CI-functions via their Walsh transform (Theorem 2.4.2), it is easy to see that f_1 *is a* 2*-CI function and that* f_2 *and* f_3 *are* 1*-CI functions. Now, from Theorem 7.2.2, we get that the function* $g : \mathbb{F}_2^7 \to \mathbb{F}_2$ *defined by*

$$g(x_1,\ldots,x_7) = f_1(x_1,x_2,x_3)f_2(x_4+x_1,x_5+x_2)f_3(x_6+x_2,x_7+x_3), \tag{7.2}$$

is a 2*-CI function, and that its Hamming weight is* $\mathrm{wt}(g) = \prod_{i=1}^{3}\mathrm{wt}(f_i) = 4\times2\times2 = 16$. *From* (7.2), *we get the algebraic normal form of* g*:*

$$\begin{aligned} g(x_1,\ldots,x_7) \;=\; & x_1x_2x_3 + x_1x_2x_4 + x_1x_2x_5 + x_1x_3x_4 + x_1x_3x_5 + x_1x_3x_6 + \\ & x_1x_3x_7 + x_1x_3 + x_1x_4x_6 + x_1x_4x_7 + x_1x_5x_6 + x_1x_5x_7 + x_2x_3x_6 + x_2x_3x_7 + \\ & x_2x_3 + x_2x_4x_6 + x_2x_4x_7 + x_2x_4 + x_2x_5x_6 + x_2x_5x_7 + x_2x_5 + x_3x_4x_6 + x_3x_4x_7 + \\ & x_3x_4 + x_3x_5x_6 + x_3x_5x_7 + x_3x_5 + x_3x_6 + x_3x_7 + x_3. \end{aligned}$$

The truth table and the Walsh transform of g *(from which we can check that* g *is indeed a* 2*-CI function with* $\mathrm{wt}(g) = 16$*), can be found in Table 7.1 and Table 7.2 at the end of the chapter.*

The following corollary is a special case of Theorem 7.2.2, assuming that all f_i are CI-functions with the minimal Hamming weight. Furthermore, we select π_i in Theorem 7.2.2 to be identity for all $i \in \{2,\ldots k\}$, i.e. $\pi_i(t) = t$, for all $t \in \{1,\ldots,n_i\}$.

Corollary 7.2.3 *Let* $t, d, n_1, n_2, \ldots, n_t$ *be positive integers satisfying* $n_1 \geq n_i$ *for all* $i = 2,3,\ldots,t$, *and* $d \leq n_1$. *Then,*

$$\omega_{(n_1+n_2+\cdots+n_t),d} \leq \omega_{n_1,d}\omega_{n_2,\lfloor d/2 \rfloor}\cdots\omega_{n_t,\lfloor d/2 \rfloor}.$$

Corollary 7.2.3 is a generalization of [16, Corollary 3.4], which is a special case of the result for $n_1 = n_2 = \cdots = n_t$.

In [16], C. Carlet and X. Chen conjectured that the minimum Hamming weight of 3-CI nonzero Boolean functions in n variables equals $8\lceil \frac{n}{4} \rceil$, i.e. $\omega_{n,3} = 8\lceil \frac{n}{4} \rceil$. Using

the constructions given in [16], the authors were able to show that, for $n = 2^k$, where $k \geq 3$, there exists a 3-CI function f such that $wt(f) = 8\lceil \frac{n}{4} \rceil$.
To indicate that the construction in Theorem 7.2.2 is indeed more general then the one given in [16, Corollary 3.2], and at the same time to give another example for Theorem 7.2.2 we prove the following corollary.

Corollary 7.2.4 *There exists a 3-CI function f such that $\mathrm{wt}(f) = 8\lceil \frac{n}{4} \rceil$, for every n of the form $2^k - i$ and $3 \cdot 2^k - i$, for $i = 0, 1, 2, 3$ and $k \geq 3$.*

Proof. Set $n_1 = n_2 = \cdots = n_{t-1} = m$ and $n_t = m - i$, in Corollary 7.2.3 for $m > 4$. Using the fact that $\omega_{m,1} = 2$, we get $\omega_{tm-i,3} \leq 2^{t-1}\omega_{m,3}$. Setting $t = 2$, we get $\omega_{2m-i,3} \leq 2\omega_{m,3}$. The result then follows by induction, using the fact that $\omega_{4,3} = 8$ for the base case, when n is of the form $2^k - i$, and that $\omega_{12,3} = 24$, when n is of the form $3 \cdot 2^k - i$ (see Table II in [16]). ∎

Using similar arguments one can show, assuming existence of a $4z$-variable 3-CI function with the Hamming weight $8\lceil \frac{4z}{4} \rceil = 8z$, that there exists a 3-CI function f such that $\mathrm{wt}(f) = 8\lceil \frac{n}{4} \rceil$, when $n = z \cdot 2^k - i$, and $i = 0, 1, 2, 3$, for all $k \geq 3$.

The design rationale given in Theorem 7.2.2 can be utilised to derive more constructions of correlation immune functions of similar type. For instance, the following result addresses a particular case of 2-CI functions.

Proposition 7.2.5 *Let f_1 be an n-variable 2-CI function, and f_2 an $(n+1)$-variable 1-CI function. Let π be a permutation of $n+1$ elements. For every $v \in \mathbb{F}_2^{n+1}$, denote by $\Phi(v)$ the vector $(v_{\pi(1)}, \ldots, v_{\pi(n+1)}) \in \mathbb{F}_2^{n+1}$. Then*

$$g\left(x^{(1)}, x^{(2)}\right) = f_1\left(x^{(1)}\right) f_2\left(x^{(2)} + \Phi((x^{(1)}, 0))\right)$$

and

$$h\left(x^{(1)}, x^{(2)}\right) = f_1\left(x^{(1)}\right) f_2\left(x^{(2)} + \Phi((x^{(1)}, 1))\right),$$

are 2-correlation immune functions in $(2n+1)$ variables, where $x^{(1)} \in \mathbb{F}_2^n$ and $x^{(2)} \in \mathbb{F}_2^{n+1}$.

Proof. Again, note that $\mathrm{wt}(g) = \mathrm{wt}(f_1)\mathrm{wt}(f_2)$. Without loss of generality, we can assume that π is the identity permutation. If we fix two variables at positions i_1, i_2 in $x^{(1)}$ to be a_1, a_2, then because f_1 is 2-CI we have $\mathrm{wt}(g_{i_1,i_2}^{a_1,a_2}) = \frac{1}{4}\mathrm{wt}(f_1)\mathrm{wt}(f_2) = \frac{1}{4}\mathrm{wt}(g)$. Similarly, by fixing one variable in both $x^{(1)}$ and $x^{(2)}$ and noticing that f_1 and f_2 are 1-CI functions, we get $\mathrm{wt}(g_{i_1,i_2}^{a_1,a_2}) = \frac{1}{2}\mathrm{wt}(f_1)\frac{1}{2}\mathrm{wt}(f_2) = \frac{1}{4}\mathrm{wt}(g)$. Finally, by fixing two variables in $x^{(2)}$, say $x_{i_1}^{(2)}$ and $x_{i_2}^{(2)}$, we obtain

$$\begin{aligned}
\mathrm{wt}\left(g_{i_1^{(2)},i_2^{(2)}}^{a_1,a_2}\right) &= \mathrm{wt}\left((f_1)_{i_1^{(1)}}^{0}\right)\mathrm{wt}\left((f_2)_{i_1^{(2)},i_2^{(2)}}^{a_1,a_2}\right) + \mathrm{wt}\left((f_1)_{i_1^{(1)}}^{1}\right)\mathrm{wt}\left((f_2)_{i_1^{(2)},i_2^{(2)}}^{a_1\oplus 1,a_2}\right) \\
&= \frac{1}{2}\mathrm{wt}(f_1)\mathrm{wt}\left((f_2)_{i_2^{(2)}}^{a_2}\right) = \frac{1}{2}\mathrm{wt}(f_1)\frac{1}{2}\mathrm{wt}(f_2) = \frac{1}{4}\mathrm{wt}(g).
\end{aligned}$$

So, we conclude that g is indeed 2-CI. The proof for h is identical, thus omitted. ∎

7.2.1 A nonlinearity analysis

The primary goal of the design methods given above concerns the possibility of constructing CI function with the minimal (generally low) Hamming weight. Therefore, this class of CI functions generally does not achieve high nonlinearity (even when the input functions are not chosen to be with the minimal Hamming weight). This is the consequence of the fact that both Theorem 7.2.2 and Proposition 7.2.5 define a function g as a product of the initial functions f_i, which generally gives a lower nonlinearity than the highest known, obtained by the methods in [54] and [72].

Nevertheless, we provide an exact specification of the Fourier coefficients of g in Theorem 7.2.2, similar to the one given by C. Carlet and X. Chen in [16], which can be used to compute the nonlinearity of the constructed functions. Let the notation of Theorem 7.2.2 hold. Let $n + n_2 + \cdots + n_k = m$, and choose arbitrary but fixed $v \in \mathbb{F}_2^m$. For simplicity, we will assume that $\pi_i(t) = t$, for all $t \in \{1, \ldots, n_i\}$, and $i \in \{2, \ldots k\}$. To compute $\widehat{g}(v)$, we represent v as $(v^{(1)}, \ldots, v^{(k)})$ with $v^{(i)} \in \mathbb{F}_2^{n_i}$, for $i \in \{2, 3, \ldots, k\}$, and $v^{(1)} \in \mathbb{F}_2^n$. We have,

$$\begin{aligned}
\widehat{g}(v) &= \sum_{x \in \mathbb{F}_2^m} \left(f_1(x^{(1)}) \prod_{i=2}^{k} f_i\left(x^{(i)} + \Phi_i(x^{(1)})\right) (-1)^{v \cdot x} \right) \\
&= \sum_{x^{(1)} \in \mathbb{F}_2^n} f_1(x^{(1)}) (-1)^{v^{(1)} \cdot x^{(1)}} \left(\prod_{i=2}^{k} \left(\sum_{x^{(i)} \in \mathbb{F}_2^{n_i}} f_i\left(x^{(i)} + \Phi_i(x^{(1)})\right) (-1)^{v^{(i)} \cdot x^{(i)}} \right) \right) \\
&= \sum_{x^{(1)} \in \mathbb{F}_2^n} f_1(x^{(1)}) (-1)^{v^{(1)} \cdot x^{(1)}} \times \\
&\times \left(\prod_{i=2}^{k} \left(\sum_{x^{(i)} \in \mathbb{F}_2^{n_i}} f_i\left(x^{(i)} + \Phi_i(x^{(1)})\right) (-1)^{v^{(i)} \cdot \left(x^{(i)} + \Phi_i(x^{(1)})\right)} (-1)^{v^{(i)} \cdot \Phi_i(x^{(1)})} \right) \right) \\
&= \prod_{i=2}^{k} \widehat{f}_i(v^{(i)}) \left(\sum_{x^{(1)} \in \mathbb{F}_2^n} f_1(x^{(1)}) (-1)^{v^{(1)} \cdot x^{(1)} + \sum_{l=2}^{k} v^{(l)} \cdot \Phi(x^{(1)})} \right).
\end{aligned}$$

Now, $v^{(l)} \cdot \Phi(x^{(1)}) = v_1^{(l)} x_1 + \cdots + v_{n_i}^{(l)} x_{n_i}$. If, for every $l \in \{2, \ldots, k\}$, we denote by ${}^0v^{(l)} \in \mathbb{F}_2^n$ the vector $(v_1^{(l)}, v_2^{(l)}, \ldots v_{n_i}^{(l)}, 0, \ldots, 0)$, then

$$v^{(l)} \cdot \Phi(x^{(1)}) = v_1^{(l)} x_1 + \cdots + v_{n_l}^{(l)} x_{n_i} = {}^0v^{(l)} \cdot x^{(1)}.$$

Using this, we get:

$$\begin{aligned}
\widehat{g}(v) &= \prod_{i=2}^{k} \widehat{f}_i(v^{(i)}) \left(\sum_{x^{(1)} \in \mathbb{F}_2^n} f_1(x^{(1)}) (-1)^{v^{(1)} \cdot x^{(1)} + \sum_{l=2}^{k} v^{(l)} \cdot \Phi(x^{(1)})} \right) \\
&= \prod_{i=2}^{k} \widehat{f}_i(v^{(i)}) \left(\sum_{x^{(1)} \in \mathbb{F}_2^n} \left(f_1(x^{(1)}) \right) (-1)^{v^{(1)} \cdot x^{(1)} + \sum_{l=2}^{k} {}^0v^{(l)} \cdot x^{(1)}} \right).
\end{aligned}$$

For convenience, let ${}^0v^{(1)}$ denote the vector $v^{(1)}$. Then,

$$\begin{aligned}\widehat{g}(v) &= \prod_{i=2}^{k} \widehat{f}_i(v^{(i)}) \left(\sum_{x^{(1)} \in \mathbb{F}_2^n} (f_1(x^{(1)})(-1)^{\sum_{l=1}^{k} {}^0v^{(l)} \cdot x^{(1)}} \right) \\ &= \widehat{f}_1 \left(\sum_{i=1}^{k} {}^0v^{(l)} \right) \prod_{l=2}^{k} \widehat{f}_i \left(v^{(i)} \right).\end{aligned}$$

To conclude, from the computations in this section, we get that the Fourier coefficients of the function g from Theorem 7.2.2 are

$$\widehat{g}(v) = \widehat{f}_1 \left(\sum_{i=1}^{k} {}^0v^{(l)} \right) \prod_{l=2}^{k} \widehat{f}_i \left(v^{(i)} \right),$$

for all $v = (v^{(1)}, \ldots, v^{(k)}) \in \mathbb{F}_2^{n+n_2+\cdots+n_k}$.

x	$g(x)$	x	$g(x)$	x	$g(x)$
(0, 0, 0, 0, 0, 0, 0)	0	(1, 1, 0, 1, 0, 1, 0)	0	(0, 1, 1, 0, 1, 0, 1)	0
(1, 0, 0, 0, 0, 0, 0)	0	(0, 0, 1, 1, 0, 1, 0)	0	(1, 1, 1, 0, 1, 0, 1)	0
(0, 1, 0, 0, 0, 0, 0)	0	(1, 0, 1, 1, 0, 1, 0)	0	(0, 0, 0, 1, 1, 0, 1)	0
(1, 1, 0, 0, 0, 0, 0)	0	(0, 1, 1, 1, 0, 1, 0)	0	(1, 0, 0, 1, 1, 0, 1)	0
(0, 0, 1, 0, 0, 0, 0)	1	(1, 1, 1, 1, 0, 1, 0)	0	(0, 1, 0, 1, 1, 0, 1)	0
(1, 0, 1, 0, 0, 0, 0)	0	(0, 0, 0, 0, 1, 1, 0)	0	(1, 1, 0, 1, 1, 0, 1)	0
(0, 1, 1, 0, 0, 0, 0)	0	(1, 0, 0, 0, 1, 1, 0)	1	(0, 0, 1, 1, 1, 0, 1)	0
(1, 1, 1, 0, 0, 0, 0)	0	(0, 1, 0, 0, 1, 1, 0)	0	(1, 0, 1, 1, 1, 0, 1)	0
(0, 0, 0, 1, 0, 0, 0)	0	(1, 1, 0, 0, 1, 1, 0)	0	(0, 1, 1, 1, 1, 0, 1)	0
(1, 0, 0, 1, 0, 0, 0)	0	(0, 0, 1, 0, 1, 1, 0)	0	(1, 1, 1, 1, 1, 0, 1)	1
(0, 1, 0, 1, 0, 0, 0)	1	(1, 0, 1, 0, 1, 1, 0)	0	(0, 0, 0, 0, 0, 1, 1)	0
(1, 1, 0, 1, 0, 0, 0)	0	(0, 1, 1, 0, 1, 1, 0)	0	(1, 0, 0, 0, 0, 1, 1)	0
(0, 0, 1, 1, 0, 0, 0)	0	(1, 1, 1, 0, 1, 1, 0)	0	(0, 1, 0, 0, 0, 1, 1)	0
(1, 0, 1, 1, 0, 0, 0)	0	(0, 0, 0, 1, 1, 1, 0)	0	(1, 1, 0, 0, 0, 1, 1)	0
(0, 1, 1, 1, 0, 0, 0)	0	(1, 0, 0, 1, 1, 1, 0)	0	(0, 0, 1, 0, 0, 1, 1)	1
(1, 1, 1, 1, 0, 0, 0)	0	(0, 1, 0, 1, 1, 1, 0)	0	(1, 0, 1, 0, 0, 1, 1)	0
(0, 0, 0, 0, 1, 0, 0)	0	(1, 1, 0, 1, 1, 1, 0)	0	(0, 1, 1, 0, 0, 1, 1)	0
(1, 0, 0, 0, 1, 0, 0)	0	(0, 0, 1, 1, 1, 1, 0)	0	(1, 1, 1, 0, 0, 1, 1)	0
(0, 1, 0, 0, 1, 0, 0)	1	(1, 0, 1, 1, 1, 1, 0)	0	(0, 0, 0, 1, 0, 1, 1)	0
(1, 1, 0, 0, 1, 0, 0)	0	(0, 1, 1, 1, 1, 1, 0)	0	(1, 0, 0, 1, 0, 1, 1)	0
(0, 0, 1, 0, 1, 0, 0)	0	(1, 1, 1, 1, 1, 1, 0)	1	(0, 1, 0, 1, 0, 1, 1)	1
(1, 0, 1, 0, 1, 0, 0)	0	(0, 0, 0, 0, 0, 0, 1)	0	(1, 1, 0, 1, 0, 1, 1)	0
(0, 1, 1, 0, 1, 0, 0)	0	(1, 0, 0, 0, 0, 0, 1)	0	(0, 0, 1, 1, 0, 1, 1)	0
(1, 1, 1, 0, 1, 0, 0)	0	(0, 1, 0, 0, 0, 0, 1)	0	(1, 0, 1, 1, 0, 1, 1)	0
(0, 0, 0, 1, 1, 0, 0)	0	(1, 1, 0, 0, 0, 0, 1)	0	(0, 1, 1, 1, 0, 1, 1)	0
(1, 0, 0, 1, 1, 0, 0)	0	(0, 0, 1, 0, 0, 0, 1)	0	(1, 1, 1, 1, 0, 1, 1)	0
(0, 1, 0, 1, 1, 0, 0)	0	(1, 0, 1, 0, 0, 0, 1)	0	(0, 0, 0, 0, 1, 1, 1)	0
(1, 1, 0, 1, 1, 0, 0)	0	(0, 1, 1, 0, 0, 0, 1)	0	(1, 0, 0, 0, 1, 1, 1)	0
(0, 0, 1, 1, 1, 0, 0)	1	(1, 1, 1, 0, 0, 0, 1)	1	(0, 1, 0, 0, 1, 1, 1)	1
(1, 0, 1, 1, 1, 0, 0)	0	(0, 0, 0, 1, 0, 0, 1)	0	(1, 1, 0, 0, 1, 1, 1)	0
(0, 1, 1, 1, 1, 0, 0)	0	(1, 0, 0, 1, 0, 0, 1)	1	(0, 0, 1, 0, 1, 1, 1)	0
(1, 1, 1, 1, 1, 0, 0)	0	(0, 1, 0, 1, 0, 0, 1)	0	(1, 0, 1, 0, 1, 1, 1)	0
(0, 0, 0, 0, 0, 1, 0)	0	(1, 1, 0, 1, 0, 0, 1)	0	(0, 1, 1, 0, 1, 1, 1)	0
(1, 0, 0, 0, 0, 1, 0)	0	(0, 0, 1, 1, 0, 0, 1)	0	(1, 1, 1, 0, 1, 1, 1)	0
(0, 1, 0, 0, 0, 1, 0)	0	(1, 0, 1, 1, 0, 0, 1)	0	(0, 0, 0, 1, 1, 1, 1)	0
(1, 1, 0, 0, 0, 1, 0)	0	(0, 1, 1, 1, 0, 0, 1)	0	(1, 0, 0, 1, 1, 1, 1)	0
(0, 0, 1, 0, 0, 1, 0)	0	(1, 1, 1, 1, 0, 0, 1)	0	(0, 1, 0, 1, 1, 1, 1)	0
(1, 0, 1, 0, 0, 1, 0)	0	(0, 0, 0, 0, 1, 0, 1)	0	(1, 1, 0, 1, 1, 1, 1)	0
(0, 1, 1, 0, 0, 1, 0)	0	(1, 0, 0, 0, 1, 0, 1)	1	(0, 0, 1, 1, 1, 1, 1)	1
(1, 1, 1, 0, 0, 1, 0)	1	(0, 1, 0, 0, 1, 0, 1)	0	(1, 0, 1, 1, 1, 1, 1)	0
(0, 0, 0, 1, 0, 1, 0)	0	(1, 1, 0, 0, 1, 0, 1)	0	(0, 1, 1, 1, 1, 1, 1)	0
(1, 0, 0, 1, 0, 1, 0)	1	(0, 0, 1, 0, 1, 0, 1)	0	(1, 1, 1, 1, 1, 1, 1)	0
(0, 1, 0, 1, 0, 1, 0)	0	(1, 0, 1, 0, 1, 0, 1)	0		

Table 7.1: Truth table of g from Example 7.

x	$W_g(x)$	x	$W_g(x)$	x	$W_g(x)$
(0, 0, 0, 0, 0, 0, 0)	96	(1, 1, 0, 1, 0, 1, 0)	0	(0, 1, 1, 0, 1, 0, 1)	0
(1, 0, 0, 0, 0, 0, 0)	0	(0, 0, 1, 1, 0, 1, 0)	0	(1, 1, 1, 0, 1, 0, 1)	0
(0, 1, 0, 0, 0, 0, 0)	0	(1, 0, 1, 1, 0, 1, 0)	0	(0, 0, 0, 1, 1, 0, 1)	0
(1, 1, 0, 0, 0, 0, 0)	0	(0, 1, 1, 1, 0, 1, 0)	0	(1, 0, 0, 1, 1, 0, 1)	0
(0, 0, 1, 0, 0, 0, 0)	0	(1, 1, 1, 1, 0, 1, 0)	0	(0, 1, 0, 1, 1, 0, 1)	0
(1, 0, 1, 0, 0, 0, 0)	0	(0, 0, 0, 0, 1, 1, 0)	0	(1, 1, 0, 1, 1, 0, 1)	0
(0, 1, 1, 0, 0, 0, 0)	0	(1, 0, 0, 0, 1, 1, 0)	0	(0, 0, 1, 1, 1, 0, 1)	0
(1, 1, 1, 0, 0, 0, 0)	32	(0, 1, 0, 0, 1, 1, 0)	0	(1, 0, 1, 1, 1, 0, 1)	0
(0, 0, 0, 1, 0, 0, 0)	0	(1, 1, 0, 0, 1, 1, 0)	0	(0, 1, 1, 1, 1, 0, 1)	0
(1, 0, 0, 1, 0, 0, 0)	0	(0, 0, 1, 0, 1, 1, 0)	0	(1, 1, 1, 1, 1, 0, 1)	0
(0, 1, 0, 1, 0, 0, 0)	0	(1, 0, 1, 0, 1, 1, 0)	0	(0, 0, 0, 0, 0, 1, 1)	0
(1, 1, 0, 1, 0, 0, 0)	0	(0, 1, 1, 0, 1, 1, 0)	0	(1, 0, 0, 0, 0, 1, 1)	-32
(0, 0, 1, 1, 0, 0, 0)	0	(1, 1, 1, 0, 1, 1, 0)	0	(0, 1, 0, 0, 0, 1, 1)	0
(1, 0, 1, 1, 0, 0, 0)	0	(0, 0, 0, 1, 1, 1, 0)	0	(1, 1, 0, 0, 0, 1, 1)	0
(0, 1, 1, 1, 0, 0, 0)	0	(1, 0, 0, 1, 1, 1, 0)	0	(0, 0, 1, 0, 0, 1, 1)	0
(1, 1, 1, 1, 0, 0, 0)	0	(0, 1, 0, 1, 1, 1, 0)	0	(1, 0, 1, 0, 0, 1, 1)	0
(0, 0, 0, 0, 1, 0, 0)	0	(1, 1, 0, 1, 1, 1, 0)	0	(0, 1, 1, 0, 0, 1, 1)	32
(1, 0, 0, 0, 1, 0, 0)	0	(0, 0, 1, 1, 1, 1, 0)	0	(1, 1, 1, 0, 0, 1, 1)	0
(0, 1, 0, 0, 1, 0, 0)	0	(1, 0, 1, 1, 1, 1, 0)	0	(0, 0, 0, 1, 0, 1, 1)	0
(1, 1, 0, 0, 1, 0, 0)	0	(0, 1, 1, 1, 1, 1, 0)	0	(1, 0, 0, 1, 0, 1, 1)	0
(0, 0, 1, 0, 1, 0, 0)	0	(1, 1, 1, 1, 1, 1, 0)	0	(0, 1, 0, 1, 0, 1, 1)	0
(1, 0, 1, 0, 1, 0, 0)	0	(0, 0, 0, 0, 0, 0, 1)	0	(1, 1, 0, 1, 0, 1, 1)	0
(0, 1, 1, 0, 1, 0, 0)	0	(1, 0, 0, 0, 0, 0, 1)	0	(0, 0, 1, 1, 0, 1, 1)	0
(1, 1, 1, 0, 1, 0, 0)	0	(0, 1, 0, 0, 0, 0, 1)	0	(1, 0, 1, 1, 0, 1, 1)	0
(0, 0, 0, 1, 1, 0, 0)	0	(1, 1, 0, 0, 0, 0, 1)	0	(0, 1, 1, 1, 0, 1, 1)	0
(1, 0, 0, 1, 1, 0, 0)	0	(0, 0, 1, 0, 0, 0, 1)	0	(1, 1, 1, 1, 0, 1, 1)	0
(0, 1, 0, 1, 1, 0, 0)	0	(1, 0, 1, 0, 0, 0, 1)	0	(0, 0, 0, 0, 1, 1, 1)	0
(1, 1, 0, 1, 1, 0, 0)	-32	(0, 1, 1, 0, 0, 0, 1)	0	(1, 0, 0, 0, 1, 1, 1)	0
(0, 0, 1, 1, 1, 0, 0)	32	(1, 1, 1, 0, 0, 0, 1)	0	(0, 1, 0, 0, 1, 1, 1)	0
(1, 0, 1, 1, 1, 0, 0)	0	(0, 0, 0, 1, 0, 0, 1)	0	(1, 1, 0, 0, 1, 1, 1)	0
(0, 1, 1, 1, 1, 0, 0)	0	(1, 0, 0, 1, 0, 0, 1)	0	(0, 0, 1, 0, 1, 1, 1)	0
(1, 1, 1, 1, 1, 0, 0)	0	(0, 1, 0, 1, 0, 0, 1)	0	(1, 0, 1, 0, 1, 1, 1)	0
(0, 0, 0, 0, 0, 1, 0)	0	(1, 1, 0, 1, 0, 0, 1)	0	(0, 1, 1, 0, 1, 1, 1)	0
(1, 0, 0, 0, 0, 1, 0)	0	(0, 0, 1, 1, 0, 0, 1)	0	(1, 1, 1, 0, 1, 1, 1)	0
(0, 1, 0, 0, 0, 1, 0)	0	(1, 0, 1, 1, 0, 0, 1)	0	(0, 0, 0, 1, 1, 1, 1)	0
(1, 1, 0, 0, 0, 1, 0)	0	(0, 1, 1, 1, 0, 0, 1)	0	(1, 0, 0, 1, 1, 1, 1)	0
(0, 0, 1, 0, 0, 1, 0)	0	(1, 1, 1, 1, 0, 0, 1)	0	(0, 1, 0, 1, 1, 1, 1)	-32
(1, 0, 1, 0, 0, 1, 0)	0	(0, 0, 0, 0, 1, 0, 1)	0	(1, 1, 0, 1, 1, 1, 1)	0
(0, 1, 1, 0, 0, 1, 0)	0	(1, 0, 0, 0, 1, 0, 1)	0	(0, 0, 1, 1, 1, 1, 1)	0
(1, 1, 1, 0, 0, 1, 0)	0	(0, 1, 0, 0, 1, 0, 1)	0	(1, 0, 1, 1, 1, 1, 1)	32
(0, 0, 0, 1, 0, 1, 0)	0	(1, 1, 0, 0, 1, 0, 1)	0	(0, 1, 1, 1, 1, 1, 1)	0
(1, 0, 0, 1, 0, 1, 0)	0	(0, 0, 1, 0, 1, 0, 1)	0	(1, 1, 1, 1, 1, 1, 1)	0
(0, 1, 0, 1, 0, 1, 0)	0	(1, 0, 1, 0, 1, 0, 1)	0		

Table 7.2: Walsh transform of g from Example 7.

Chapter 8

Resilient functions and sums of their Walsh coefficients

In order to motivate and explain the problems we will consider in this chapter, we have to change our setting from Boolean functions defined on $\mathbb{F}_2^n$ mapping to $\mathbb{F}_2$, and consider instead functions from $\{-1,1\}^n$ to $\{-1,1\}$. Once we do that, we will translate the problems back to the standard setting of Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ and investigate them there.

When f is a function from $\{-1,1\}^n$ to $\{-1,1\}$, similarly like in the $\mathbb{F}_2$ case, f can be written as

$$f(x) = \sum_{S \subseteq [n]} \widehat{f}(S) \prod_{i \in S} x_i,$$

where $[n] = \{1, 2, \ldots, n\}$ and $\widehat{f}(S)$ are the Fourier coefficients[1] of f given by

$$\widehat{f}(S) = \frac{1}{2^n} \sum_{x \in \{-1,1\}^n} f(x) \prod_{i \in S} x_i. \tag{8.1}$$

The total degree of f (or simply the degree of f), denoted by $\deg(f)$, is defined by $\deg(f) = max\{|S| : \widehat{f}(S) \neq 0\}$. We use $\widehat{f}(i)$ instead of $\widehat{f}(\{i\})$ for a natural number $i \leq n$, and refer to them as linear (weight one) coefficients.

In a collection of open problems in field of the analysis of Boolean functions [52], R. O'Donnell attributed the following conjecture to P. Gopalan and R. Servedio (ca. 2009): If f is a function from $\{-1,1\}^n$ to $\{-1,1\}$, and $\deg(f) = d$, then

$$\sum_{i=1}^{n} \widehat{f}(i) \leq \sqrt{d}.$$

In the same paper [52], O'Donnell stated that one could propose the following, stronger conjecture.

[1] Notice that we use the same notation for the Fourier coefficients of the Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, but since it will always be clear whether we are in the $\mathbb{F}_2$ or $\{-1,1\}$ setting, this will cause no confusion.

Conjecture 8.0.1 *[52] Let $f : \{-1,1\}^n \to \{-1,1\}$ and let d be the degree of f. Then*

$$\sum_{i=1}^{n} \widehat{f}(i) \leq d\binom{d-1}{\lfloor \frac{d-1}{2} \rfloor} 2^{1-d}.$$

Motivation for studying growth of the sum of linear Fourier coefficients of f, $\sum_{i=1}^{n} \widehat{f}(i)$, comes from social choice. If we consider a function $f : \{-1,1\}^n \to \{-1,1\}$ as a voting rule for a 2-candidate election, then the expected number of votes that agree with the outcome of the election is equal to $\frac{n}{2} + \frac{1}{2}\sum_{i=1}^{n} \widehat{f}(i)$, see [51, Chapter 2] for details. It is generally assumed that the larger the expected number of votes that agree with the outcome of the election, the better. So, it is natural to ask how big that number can be, and which functions are the maximizers. To answer that, one approach is to study $\sum_{i=1}^{n} \widehat{f}(i)$ and try to derive some efficient upper bounds. If we do not impose any restrictions on the degree of a function, the answer is known. The unique maximizers of $\sum_{i=1}^{n} \widehat{f}(i)$ among all $f : \{-1,1\}^n \to \{-1,1\}$ are the majority functions, see Section 8.1 for more details.

Since the statement of the conjecture, there had not been a lot of progress towards its validity until recently. In [77], Q. Wang translated O'Donnell's conjecture (Conjecture 8.0.1) to an equivalent conjecture about a class of resilient Boolean functions $g : \mathbb{F}_2^n \to \mathbb{F}_2$, thus giving alternative aspects of O'Donnell's conjecture. The notions used here about Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ are defined precisely in the preliminaries, Section 2.4.

Conjecture 8.0.2 *[77] Let $g : \mathbb{F}_2^n \to \mathbb{F}_2$ be an $(n-d-1)$-resilient Boolean function, where $1 \leq d \leq n-1$. Then*

$$\sum_{\substack{v \in \mathbb{F}_2^n \\ \mathrm{wt}(v)=n-1}} W_g(v) \leq d\binom{d-1}{\lfloor \frac{d-1}{2} \rfloor} 2^{n+1-d},$$

where $W_g(v)$ is the Walsh coefficient of g at point $v \in \mathbb{F}_2^n$.

This alternative formulation was used by Q. Wang [77] to prove that the conjecture is true when $d = 1$ and $d = n-1$.

In this chapter, we further employ Wang's approach using the standard Boolean setting. Firstly, in Section 8.1, we show an interesting combinatorial property related to Conjecture 8.0.2 which implies that (for a fixed d) the upper bound only depends on a finite number of integers n. More precisely, we show that if Conjecture 8.0.2 is correct for all $n \leq 2^{2d-2}$, then it is true for all $n \in \mathbb{N}$. Then we prove, again for a fixed d, that if the conjecture fails for some n_0, then it is incorrect for every $n > n_0$. These two results imply that, for a fixed d, if the conjecture is true for $n = 2^{2d-2}$ then it is correct for every $n \in \mathbb{N}$. Therefore, an immediate consequence is that the conjecture is true for $d = 2$, since it can be easily checked exhaustively for $n = 4$. Nevertheless, in Section 8.3 a direct proof of this fact is provided using a characterisation of $(n-3)$-resilient functions given in [8]. Then, for $d = 3$, we combine the results on characterisations of $(n-4)$-resilient functions given in [7] and [13], and show that it is enough to check the conjecture for $n = 6$, and in some

special cases for $n = 7$. For the purpose of proving that the conjecture is true for $d = 3$, we employ integer programming to deal with the mentioned cases.

However, despite the positive results, in Section 8.4, for $d = 4$, we have identified a 2-resilient Boolean function in 7 variables which violates Conjecture 8.0.1. This means that Conjecture 8.0.1 is not true in general. More specifically, the conjecture is not true whenever $n \geq 7$, implying that the Walsh coefficients of an $(n-5)$-resilient Boolean function do not necessarily satisfy the conjectured bound.

8.1 Maximizers of the sum of linear Fourier coefficients

For n odd, the majority function $\mathrm{Maj}_n : \{-1,1\}^n \to \{-1,1\}$ is defined by $\mathrm{Maj}_n(x) = \mathrm{sgn}(x_1 + x_2 + \cdots + x_n)$, and when n is even we say that f is a majority function if $f(x)$ equals the sign of $x_1 + \cdots + x_n$ whenever this number is nonzero, and 1 otherwise. Notice that in the Boolean case, as a mapping from $\{0,1\}^n$ to $\{0,1\}$, the exact formula for computing the output of the majority function is given by $\lfloor \frac{1}{2} + \frac{(\sum_{i=1}^n x_i) - 1/2}{n} \rfloor$.

As already mentioned, the majority function is a maximizer of the sum $\sum_{i=1}^n \widehat{f}(i)$. This fact can be demonstrated as follows.

$$\sum_{i=1}^{n} \widehat{f}(i) = \frac{1}{2^n} \sum_{x \in \{-1,1\}^n} f(x)(x_1 + \cdots + x_n) \leq \frac{1}{2^n} \sum_{x \in \{-1,1\}^n} |x_1 + \cdots + x_n| = \sum_{i=1}^{n} \widehat{Maj}_n(i)$$

and equality holds if and only if $f(x) = \mathrm{sgn}(x_1 + \cdots + x_n)$ whenever $x_1 + \cdots + x_n \neq 0$. Furthermore,

$$\sum_{x \in \{-1,1\}^n} |x_1 + \cdots + x_n| = \sum_{k=0}^{n} \binom{n}{k} |n - 2k| = 2 \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{k} (n - 2k) = \cdots = 2n \binom{n-1}{\lfloor \frac{n-1}{2} \rfloor}. \tag{8.2}$$

From this, we can conclude that Conjecture 8.0.1 is true for $d = n$. Equation (8.2) is also where the motivation for the bound in Conjecture 8.0.1 comes from. More precisely, because the majority functions are maximizers for $d = n$, it is tempting to assume that, even when $d < n$, the maximizers are again going to be majority functions, just this time the majority functions on d bits. And indeed, the bound in Conjecture 8.0.1 is equal to the sum of linear Fourier coefficients of an n-variable majority function on d bits (replacing n by d in (8.2) and comparing to Conjecture 8.0.1).

8.2 General results related to O'Donnell's conjecture

In [77], Conjecture 8.0.1 is shown to be equivalent to Conjecture 8.0.2. For completeness, we will give here a different and more straightforward way of showing this equivalence. It is a more or less standard procedure for translating a question about $\{-1,1\}$ functions into the $\{0,1\}$ Boolean domain.

Let f be a function from $\{-1,1\}^n$ to $\{-1,1\}$. To each set $S \subseteq [n]$ we can associate a vector $v_S \in \{0,1\}^n$ by setting $(v_S)_i = 1$ if $i \in S$, and $(v_S)_i = 0$ if

$i \in [n] \setminus S$. Furthermore, we can also associate to each vector $x \in \{-1,1\}^n$ a vector $y_x \in \{0,1\}^n$ by setting $(y_x)_i = 1$ if $x_i = -1$, and $(y_x)_i = 0$ if $x_i = 1$. Then we have:

$$\prod_{i \in S} x_i = \prod_{i \in S} (-1)^{(y_x)_i} = (-1)^{\sum_{i \in S} (y_x)_i} = (-1)^{y_x \cdot v_S}.$$

Finally, to each function $f : \{-1,1\}^n \to \{-1,1\}$ we can associate a function $g_f : \{0,1\}^n \to \{0,1\}$ by defining $g_f(y_x) = 0$ if $f(x) = 1$, and $g_f(y_x) = 1$ if $f(x) = -1$. Then, $f(x) = (-1)^{g_f(y_x)}$. It is easy to see that all three mappings are bijections, so everything is well-defined, and we have:

$$\widehat{f}(S) = \frac{1}{2^n} \sum_{x \in \{-1,1\}^n} f(x) \prod_{i \in S} x_i = \frac{1}{2^n} \sum_{y \in \{0,1\}^n} (-1)^{g_f(y) + y \cdot v_S} = \frac{1}{2^n} W_{g_f}(v_S). \quad (8.3)$$

Note that from the relation (8.3) we have that $f : \{-1,1\}^n \to \{-1,1\}$ has degree at most d if and only if $W_{g_f}(v) = 0$ for every $v \in \{0,1\}^n$ such that $\mathrm{wt}(v) \geq d+1$. This means that Conjecture 8.0.1 is equivalent to the following conjecture:

Conjecture 8.2.1 *Let $g : \mathbb{F}_2^n \to \mathbb{F}_2$ be a function such that $W_g(v) = 0$ for every $v \in \mathbb{F}_2^n$ with $\mathrm{wt}(v) \geq d+1$. Then:*

$$\sum_{\substack{v \in \mathbb{F}_2^n \\ \mathrm{wt}(v) = 1}} W_g(v) \leq d \binom{d-1}{\lfloor \frac{d-1}{2} \rfloor} 2^{n+1-d}.$$

If we set $g'(x) = g(x) + x_1 + x_2 + \cdots + x_n$, we have the following relation between the Walsh coefficients: $W_{g'}(v) = W_g(v + \overline{1})$ (here $\overline{1}$ is the vector with every coordinate equal to 1). Using this relation and Proposition 2.4.2, we can conclude that Conjecture 8.0.2 and 8.2.1 are equivalent and consequently Conjecture 8.0.1 and 8.0.2 are equivalent as well. We notice that the research on resilient functions has been quite extensive during the last few decades [8, 16, 54, 73, 75, 76, 78]. Apart from their use in certain encryption schemes (e.g. nonlinear combiners), correlation immune Boolean functions have applications in secret-sharing schemes and error-correcting codes [6, 23, 26].

Now, using certain well-known (divisibility) results about resilient Boolean functions, we deduce some interesting facts related to Conjecture 8.0.2.

Proposition 8.2.2 *For every natural number $d \in \mathbb{N}$, there exists a number N_d depending only on d, such that, if Conjecture 8.0.2 is true for all $n \leq N_d$, then it is true for all $n \in \mathbb{N}$. Moreover, we can take $N_d = 2^{2d-2}$.*

Proof. Select and fix a $d \in \mathbb{N}$, and let $n \geq d+2$. We already know that the conjecture is true for $d = n-1$ and $d = n$. Now, let g be an $(n-d-1)$-resilient function in n variables. Then, expressing the sum in Conjecture 8.0.2 in terms of

similar sums but in a smaller dimension, we have:

$$\begin{aligned}\sum_{\substack{v\in\mathbb{F}_2^n\\ \mathrm{wt}(v)=n-1}} W_g(v) &= \sum_{\substack{v\in\mathbb{F}_2^n\\ \mathrm{wt}(v)=n-1}} \sum_{z\in\mathbb{F}_2^n} (-1)^{g(z)+z\cdot v}\\ &= \sum_{\substack{v\in\mathbb{F}_2^n\\ \mathrm{wt}(v)=n-1}} \left(\sum_{x\in\mathbb{F}_2^{n-1}} (-1)^{g(x,1)+(x,1)\cdot v} + \sum_{x\in\mathbb{F}_2^{n-1}} (-1)^{g(x,0)+(x,0)\cdot v} \right)\\ &= \sum_{\substack{u\in\mathbb{F}_2^{n-1}\\ \mathrm{wt}(u)=n-2}} \sum_{x\in\mathbb{F}_2^{n-1}} (-1)^{g(x,1)+x\cdot u+1} + \sum_{\substack{u\in\mathbb{F}_2^{n-1}\\ \mathrm{wt}(u)=n-2}} \sum_{x\in\mathbb{F}_2^{n-1}} (-1)^{g(x,0)+x\cdot u}\\ &\quad + \sum_{x\in\mathbb{F}_2^n} (-1)^{g(x)+x\cdot(\overline{1},0)}\end{aligned}$$

Define functions $g_0, g_1 : \mathbb{F}_2^{n-1} \to \mathbb{F}_2$ by $g_0(x) = g(x,0)$ and $g_1(x) = g(x,1)+1$, for all $x \in \mathbb{F}_2^{n-1}$. Then, we get:

$$\sum_{\substack{v\in\mathbb{F}_2^n\\ \mathrm{wt}(v)=n-1}} W_g(v) = \sum_{\substack{u\in\mathbb{F}_2^{n-1}\\ \mathrm{wt}(u)=n-2}} W_{g_1}(u) + \sum_{\substack{u\in\mathbb{F}_2^{n-1}\\ \mathrm{wt}(u)=n-2}} W_{g_0}(u) + W_g(\overline{1},0).$$

Note that the $(n-1)$-variable functions g_0 and g_1 are $n-d-1-1 = (n-1)-d-1$ resilient, hence if the conjecture is true for $n-1$ we have:

$$\begin{aligned}\sum_{\substack{v\in\mathbb{F}_2^n\\ \mathrm{wt}(v)=n-1}} W_g(v) &\le d\binom{d-1}{\lfloor\frac{d-1}{2}\rfloor}2^{n-d} + d\binom{d-1}{\lfloor\frac{d-1}{2}\rfloor}2^{n-d} + W_g(\overline{1},0)\\ &= d\binom{d-1}{\lfloor\frac{d-1}{2}\rfloor}2^{n+1-d} + W_g(\overline{1},0).\end{aligned}$$

Essentially, the same reasoning applies to arbitrary $v \in \mathbb{F}_2^n$ with $\mathrm{wt}(v) = n-1$, not just $(\overline{1},0)$. Thus, it is sufficient to show that for large enough n there exists at least one $v \in \mathbb{F}_2^n$ with $\mathrm{wt}(v) = n-1$ satisfying $W_g(v) \le 0$.

As g is $(n-d-1)$-resilient, we know from Sarkar-Maitra's divisibility bound [64] (improved later by C. Carlet [10, 12]), that its Walsh coefficients are divisible by $2^{n-d-1+2} = 2^{n-d+1}$. Using Parseval's equality, we have:

$$2^{2n} = \sum_{v\in\mathbb{F}_2^n} W_g(v)^2 = K2^{2n-2d+2},$$

for some natural number $K \in \mathbb{N}$. Therefore, $K \le 2^{2d-2}$. The number of nonzero Walsh coefficients of g is less than or equal to K. Consequently, if $n > K$, then we can find at least one $v \in \mathbb{F}_2^n$ with $\mathrm{wt}(v) = n-1$ such that $W_g(v) = 0$. So we can set $N_d = 2^{2d-2}$, and the result will follow by induction on n. ∎

Remark 8 *In the proof of Proposition 8.2.2, it was enough to find one $v \in \mathbb{F}_2^n$ with $\mathrm{wt}(v) = n-1$ such that $W_g(v) \leq 0$, rather than $W_g(v) = 0$. Thus, it is possible to get a slightly better bound for N_d with the same approach, but the improvement is not going to be better than one half of the current bound. It would be interesting to see whether the bound for N_d can be improved more substantially.*

By Proposition 8.2.2, for $d = 2$, Conjecture 8.0.2 needs to be checked for all $n \leq 4$ which can be easily done exhaustively. Its correctness has been confirmed for $n \leq 4$ and therefore it is true for all $n \in \mathbb{N}$. Nevertheless, we will later provide a direct proof of this fact using a characterization of $(n-3)$-resilient functions. A similar characterization of $(n-4)$-resilient functions is then helpful in proving the conjecture for $d = 3$, since in this case the values $n \leq N_d = 16$ cannot be checked exhaustively. Nevertheless, using the characterization, later we will show that for $d = 3$ it is sufficient check the conjecture exhaustively for $n \leq 7$.

For a fixed d, the next result asserts that if the conjecture fails for some n_0 then it fails for every $n \geq n_0$.

Proposition 8.2.3 *Let $d \in \mathbb{N}$ and $g : \mathbb{F}_2^n \to \mathbb{F}_2$ be an $(n-d-1)$-resilient function for which Conjecture 8.0.2 fails. Then, for every $m \geq n$ there is an $(m-d-1)$-resilient function in m variables for which the conjecture fails.*

Proof. Let g be an $(n-d-1)$-resilient function in n variables for which Conjecture 8.0.2 fails, and let $m > n$. Define a Boolean function $h : \mathbb{F}_2^m \to \mathbb{F}_2$ by

$$h(x, x_{n+1}, \ldots, x_m) = g(x) + x_{n+1} + \cdots + x_m,$$

for all $x \in \mathbb{F}_2^n$ and $(x_{n+1}, \ldots, x_m) \in \mathbb{F}_2^{m-n}$. The Walsh coefficients of h are given by

$$W_h(a,b) = W_g(a) W_{x_{n+1}+\cdots+x_m}(b). \tag{8.4}$$

From Proposition 2.4.2 and (8.4), we conclude that h is $(n-d-1)+(m-n-1)+1 = (m-d-1)$ resilient, and

$$\begin{aligned}\sum_{\substack{w \in \mathbb{F}_2^m \\ \mathrm{wt}(w)=m-1}} W_h(w) &= \sum_{\substack{v \in \mathbb{F}_2^n \\ \mathrm{wt}(v)=n-1}} W_g(v) 2^{m-n} > d\binom{d-1}{\lfloor \frac{d-1}{2} \rfloor} 2^{n+1-d} 2^{m-n} \\ &= d\binom{d-1}{\lfloor \frac{d-1}{2} \rfloor} 2^{m+1-d}.\end{aligned}$$

So, h is an $(m-d-1)$-resilient function in m variables for which Conjecture 8.0.2 fails. ∎

8.3 Proving O'Donnell's conjecture for $d \in \{2,3\}$

As noted in the previous section, it is possible to prove the conjecture for $d = 2$, for every $n \in \mathbb{N}$, by checking exhaustively that it is true for $n = 4$. But, using the characterisation of quadratic $(n-3)$-resilient functions from [8], it is possible to give a direct proof.

Proposition 8.3.1 *Let g be an $(n-3)$-resilient function in n variables. Then,*

$$\sum_{\substack{v\in\mathbb{F}_2^n\\ wt(v)=n-1}} W_g(v) \le 2^n.$$

Proof. For an arbitrary Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, using the Poisson summation formula (Corollary 2.0.3) for the 1-dimensional subspace $\{0_n, \mathbb{e}_i\}$ we have:

$$W_f(0_n) + W_f(\mathbb{e}_i) = 2\sum_{\substack{x\in\mathbb{F}_2^n\\ x_i=0}} (-1)^{f(x)},$$

where $\mathbb{e}_i$ is the vector with all coordinates 0 except the i-th, which is 1. Summing over all $1 \le i \le n$ we obtain:

$$\begin{aligned}\sum_{i=1}^{n} W_f(\mathbb{e}_i) &= -nW_f(0_n) + 2\sum_{i=1}^{n}\sum_{\substack{x\in\mathbb{F}_2^n\\ x_i=0}} (-1)^{f(x)}\\ &= -nW_f(0_n) + 2\sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)}\,(n-\mathrm{wt}(x)) = 2\sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)}(\frac{n}{2}-\mathrm{wt}(x)).\end{aligned} \tag{8.5}$$

Now, let g be an arbitrary $(n-3)$-resilient function in n variables. If the algebraic degree of g is one, then the theorem is obviously true, so we assume that g is quadratic. We use the characterization of quadratic $(n-3)$-resilient functions in n variables given in [8]. According to [8, Theorem 4.1] there are 4 types of polynomial forms of $(n-3)$-resilient functions in n variables. We will prove the proposition for the functions of the first type, since the proof for the remaining types is analogous. The first type are the functions of the form

$$g(x) = x_ix_j + \sum_{t\in[n]\setminus\{i,j\}} x_t + a_ix_i + a_jx_j + a, \text{ where } a_i, a_j, a \in \mathbb{F}_2.$$

Adding the function $\sum_{i\in[n]} x_i$ to g we will verify Conjecture 8.2.1, for functions $g'(x) = x_ix_j + a_ix_i + a_jx_j + a$, where $a_i, a_j, a \in \mathbb{F}_2$. By looking at the four cases $(x_i, x_j) = (0,0)$, $(x_i, x_j) = (1,0)$, $(x_i, x_j) = (0,1)$, $(x_i, x_j) = (1,1)$, and using the formula $\sum_{t=1}^{k} t\binom{k}{t} = k2^{k-1}$, we have:

$$\sum_{\substack{x\in\mathbb{F}_2^n\\ x_i,x_j=0}} \Big(\frac{n}{2}-\mathrm{wt}(x)\Big) = \frac{n}{2}2^{n-2} - \sum_{t=0}^{n-2}\binom{n-2}{t}t = n2^{n-3} - (n-2)2^{n-3} = 2^{n-2},$$

$$\begin{aligned}\sum_{\substack{x\in\mathbb{F}_2^n\\ x_i=0,x_j=1}} \Big(\frac{n}{2}-\mathrm{wt}(x)\Big) = \sum_{\substack{x\in\mathbb{F}_2^n\\ x_i=1,x_j=0}} \Big(\frac{n}{2}-\mathrm{wt}(x)\Big) &= \frac{n}{2}2^{n-2} - \sum_{t=0}^{n-2}\binom{n-2}{t}(t+1) =\\ &= n2^{n-3} - \big((n-2)2^{n-3} + 2^{n-2}\big) = 0,\end{aligned}$$

$$\sum_{\substack{x\in\mathbb{F}_2^n \\ x_i,x_j=1}} \Big(\frac{n}{2} - \mathrm{wt}(x)\Big) = \frac{n}{2}2^{n-2} - \sum_{t=0}^{n-2} \binom{n-2}{t}(t+2) = 2^{n-2} - 2^{n-1} = -2^{n-2}.$$

Combining these equations with (8.5) (for $f = g'$), we get:

$$\sum_{i=1}^{n} W_{g'}(\mathbb{e}_i) = 2\sum_{x\in\mathbb{F}_2^n} (-1)^{g'(x)}(\frac{n}{2} - \mathrm{wt}(x)) \leq 2(2^{n-2} + 0 + 0 + 2^{n-2}) = 2^n.$$

Since 2^n is the upper bound in Conjecture 8.2.1 for $d = 2$, we can conclude that the proposition is true in this case. The proof for the remaining types is analogous, and therefore omitted. ∎

Since Conjecture 8.0.1 and 8.0.2 are equivalent, an immediate consequence is the following:

Theorem 8.3.2 *When $d = 2$, Conjecture 8.0.1 and Conjecture 8.0.2 are true for every $n \in \mathbb{N}$.*

8.3.1 Proving the conjecture for $d = 3$

To apply Proposition 8.2.2, when $d = 3$, would imply checking that the conjecture is true for all $n \leq 16$ which is not possible. By Siegenthaler's bound, the algebraic degree of an n-variable $(n-4)$-resilient function is at most 3, so we will look at three different cases, depending on the algebraic degree of the function.

In the case of linear functions, Conjecture 8.0.2 is obviously true. To deal with quadratic and cubic functions, we need the following divisibility result of C. Carlet (see [12, Proposition 120] or [10]) which states that for any n-variable m-resilient function f (where $m \leq n-2$), with algebraic degree t, its Walsh coefficients are divisible by $2^{m+2+\lfloor\frac{n-m-2}{t}\rfloor}$. Assume now that g is a quadratic n-variable $(n-4)$-resilient function. By the mentioned divisibility result, its Walsh coefficients are divisible by $2^{n-4+2+\lfloor\frac{n-(n-4)-2}{2}\rfloor} = 2^{n-1}$. Parseval's identity implies that

$$2^{2n} = \sum_{v\in\mathbb{F}_2^n} W_g(v)^2 = 4\cdot 2^{2n-2},$$

which implies that the number of nonzero Walsh coefficients of g is less then or equal to 4. In the same way as in the proof of Proposition 8.2.2, (since for the induction step there, we only need to know that there is at least one vector v_i with weight $n-1$ such that $W_g(v_i) = 0$), we have that, in this case, if Conjecture 8.0.2 is true for $n = 4$, then it is true for every $n \in \mathbb{N}$. But we already know that Conjecture 8.0.2 is true for $d = 3$ and $n = 4$, since this is the already proved case $d = n-1$ mentioned in the introduction. So, we can conclude that Conjecture 8.0.2 is true in this case as well.

Let us now consider the third case. Assume that g is a cubic n-variable $(n-4)$-resilient function. In [7] and [13], the authors classified cubic $(n-4)$-resilient

functions in n-variables with respect to certain properties of their Walsh spectra. To explain the classification we need the following notion of rank of a subset of $\mathbb{F}_2^n$. For a subset E of $\mathbb{F}_2^n$ the rank of E is the dimension of the subspace of $\mathbb{F}_2^n$ generated by E, and the affine rank of E is the dimension of the smallest affine subspace containing E. The classification divides $(n-4)$-resilient functions in n-variables into four types. In particular, it was proved in [7] that the functions of the first three types have the affine rank of the support of their Walsh spectrum which is less than or equal to five. Similarly, the functions of the fourth type have the affine rank of the support of their Walsh spectrum which is less than or equal to six.

The affine rank of the set $\{v \in \mathbb{F}_2^n : \mathrm{wt}(v) = n-1\}$ is equal to $n-1$. In our case, this means that for $n \geq 8$ there has to be at least one $v_i \in \mathbb{F}_2^n$ with weight $n-1$ such that $W_g(v_i) = 0$, otherwise, we would have a cubic n-variable $(n-4)$-resilient function with the affine rank of the support of its Walsh spectrum strictly larger than 6. Nevertheless, from the preceding discussion we know this is impossible. Moreover, if g is not of the fourth type, then for $n \geq 7$ there has to be at least one $v_i \in \mathbb{F}_2^n$ with the Hamming weight $n-1$ such that $W_g(v_i) = 0$, since the affine rank of the support of its Walsh spectrum is ≤ 5. This means that, in the same way as in the proof of Proposition 8.2.2, (again, for the induction step there, we only need to know that there is at least one vector v_i with the Hamming weight $n-1$ such that $W_g(v_i) = 0$), we have that if Conjecture 8.0.2 is true for $n = 6$, for all cubic 6-variable 2-resilient functions, and if the conjecture is true for $n = 7$, for all cubic 7-variable 3-resilient functions of the fourth type, then the conjecture is true for all $n \in \mathbb{N}$ when $d = 3$.

From the above discussion, it follows that to finish the proof for $d = 3$ we only need to check two things:

(a) Is there a (cubic) 6-variable 2-resilient function violating Conjecture 8.0.2. More precisely, is there a 6-variable function $g : \mathbb{F}_2^6 \to \mathbb{F}_2$ satisfying the following conditions:

- $\widehat{g}(0_6) = 32$;
- $\widehat{g}(v) = 0$, for all $v \in \mathbb{F}_2^6$ with $1 \leq wt(v) \leq 2$;
- $$\sum_{\substack{v \in \mathbb{F}_2^6 \\ \mathrm{wt}(v)=5}} \widehat{g}(v) < -3\binom{3-1}{\lfloor \frac{3-1}{2} \rfloor} 2^{6-3} = -48.$$

(Here $\widehat{g}$ is the standard Fourier transform of a Boolean function from $\mathbb{F}_2^6$ to $\mathbb{F}_2$ introduced in the preliminaries. We used the relationship (2.6) between the Walsh and Fourier coefficients, to get this equivalent (and easier to implement on a computer) formulation of the problem.)

(b) Is there a (cubic) 7-variable 3-resilient function of the fourth type violating Conjecture 8.0.2. In general, the Walsh spectrum of an $(n-4)$-resilient cubic function g belongs to the set: $\{0, \pm 2^{n-2}\}$ (see [7], [13]), hence g is plateaued. The bound in Conjecture 8.0.2, related to the Walsh coefficients, for $n = 7$ and $d = 3$ is: $3\binom{3-1}{\lfloor \frac{3-1}{2} \rfloor} 2^{7+1-3} = 6 \cdot 32$. This essentially implies that the only

situation in which a function g in 7 variables of the fourth type can violate Conjecture 8.0.2 arises when $W_g(v) = 32$ for all 7 vectors $v \in \mathbb{F}_2^7$ with $\mathrm{wt}(v) = 6$. Thus, the correctness of Conjecture 8.0.2 in this case corresponds to answering the question whether there is a 7-variable function $g : \mathbb{F}_2^7 \to \mathbb{F}_2$ satisfying the following conditions:

- $\widehat{g}(0_7) = 64$;
- $\widehat{g}(v) = 0$, for all $v \in \mathbb{F}_2^7$ with $1 \leq \mathrm{wt}(v) \leq 3$;
- $\widehat{g}(v) = -\frac{32}{2} = -16$, for all $v \in \mathbb{F}_2^7$ with $\mathrm{wt}(v) = 6$.

We can formulate the two questions as a binary linear programming problems in 64, and in 128 variables, respectively. More precisely, in (a) we represent a function g via its truth table in the form $g := (g_0, g_1, \ldots, g_{63})$ and treat $g_0, g_1, \ldots, g_{63} \in \{0, 1\}$ as unknowns, whereas in (b) we consider $g := (g_0, g_1, \ldots, g_{127})$ and treat $g_0, g_1, \ldots, g_{127} \in \{0, 1\}$ as unknowns. Then our conditions become linear equations (plus one linear inequality in (a)), and it is exactly the kind of problem suitable for linear programming solvers.

To solve the above problem instances, we used a free mixed integer linear programming solver lp_ solve, version 5.5.2.5, on a standard desktop PC (Intel Core i5-8265U processor, with clock frequency 1.60 GHz, 6 MB cache and with 8 GB RAM). The results are as follows: there does not exist a function satisfying the conditions in (a), and there does not exist a function satisfying the conditions in (b). The results were obtained in less than 0.1 seconds in both cases.

With this, we can now conclude that Conjecture 8.0.2 is true for cubic n-variable $(n-4)$-resilient functions for every $n \in \mathbb{N}$, and since we already know that it is true in the quadratic and in the linear case, this completes the proof of Conjecture 8.0.2 when $d = 3$.

Theorem 8.3.3 *For $d = 3$, Conjecture 8.0.1 and Conjecture 8.0.2 are true for every $n \in \mathbb{N}$. More precisely, for any $(n-4)$-resilient function $g : \mathbb{F}_2^n \to \mathbb{F}_2$ we have*

$$\sum_{\substack{v \in \mathbb{F}_2^n \\ \mathrm{wt}(v) = n-1}} W_g(v) \leq 6 \cdot 2^{n-2}.$$

8.4 O'Donnell's conjecture is not true when $d = 4$

With a similar approach to the one we used in the preceding section to prove Conjecture 8.0.2 when $d = 3$, we managed to find a counterexample to the conjecture when $d = 4$. The idea was to check in the same way if the conjecture is true for all the cases that we are able to get an answer with a computer within a reasonable time limit. We got a counterexample for $n = 7$ and $d = 4$, in which case the question related to the Fourier-Hadamard coefficients becomes: Is there a 7-variable 2-resilient function violating Conjecture 8.0.2. More precisely, is there a function $g : \mathbb{F}_2^7 \to \mathbb{F}_2$ satisfying the following conditions:

- $\widehat{g}(0_7) = 64$;

- $\widehat{g}(v) = 0$, for all $v \in \mathbb{F}_2^7$ with $1 \leq \mathrm{wt}(v) \leq 2$;
- $$\sum_{\substack{v \in \mathbb{F}_2^7 \\ \mathrm{wt}(v)=6}} \widehat{g}(v) < -4\binom{4-1}{\lfloor \frac{4-1}{2} \rfloor} 2^{7-4} = -96.$$

The first step is to represent a function in the form $g = (g_0, g_1, \ldots, g_{127})$, and to treat $g_0, g_1, \ldots, g_{127} \in \{0, 1\}$ as unknowns. Then the conditions become a system of linear equations and inequalities in 128 variables. Again, like in the previous section, we used lp_ solve to check if there is a solution to the system, but this time we got a positive answer. Furthermore, with lp_ solve we were able to get that for any 2-resilient function in 7 variables we have the following,

$$\sum_{\substack{v \in \{0,1\}^7 \\ \mathrm{wt}(v)=6}} \widehat{g}(v) \geq -112.$$

Moreover, we could retrieve such a 2-resilient function $g : \mathbb{F}_2^7 \to \mathbb{F}_2$, being a counterexample to Conjecture 8.0.2, achieving this minimum value:

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

where the truth table of g is represented as

$$g = (g(0,0,\ldots,0), g(1,0,\ldots,0), g(0,1,\ldots,0), \ldots, g(1,1,\ldots,1)).$$

The algebraic normal form of g is

$$\begin{aligned} g(x_0,\ldots,x_6) = {} & x_0x_1x_2x_3 + x_0x_1x_2x_6 + x_0x_1x_2 + x_0x_1x_3x_4 + x_0x_1x_3 + x_0x_1x_4 + \\ & x_0x_1x_6 + x_0x_1 + x_0x_2x_3 + x_0x_2x_4x_6 + x_0x_2x_4 + x_0x_2x_6 + x_0x_2 + x_0x_3x_4x_6 + \\ & x_0x_3x_5x_6 + x_0x_3x_5 + x_0x_3 + x_0x_4 + x_0x_5x_6 + x_0x_5 + x_0x_6 + x_1x_2x_3 + x_1x_2x_4x_5 + \\ & x_1x_2x_4x_6 + x_1x_2x_5 + x_1x_2 + x_1x_3x_4x_6 + x_1x_3x_4 + x_1x_3x_6 + x_1x_3 + x_1x_4x_5 + \\ & x_1x_4 + x_1x_5 + x_1x_6 + x_2x_3 + x_2x_4x_5x_6 + x_2x_4x_5 + x_2x_4x_6 + x_2x_4 + x_2x_5x_6 + \\ & x_2x_5 + x_2x_6 + x_3x_4x_5x_6 + x_3x_4x_5 + x_3x_4x_6 + x_3x_4 + x_3x_5x_6 + x_3x_5 + x_3x_6 + \\ & x_4x_5x_6 + x_4x_5 + x_4x_6 + x_5x_6 + 1. \end{aligned}$$

In order to be completely precise, the truth table of g is given in Table 8.1 at the end of the chapter. The Walsh transform of g is given in Table 8.2. From the Walsh transform of g one can verify that g is in fact 2-resilient and furthermore $W_g(v) = 32$, for any v of weight $n - 1 = 6$. From this we conclude that

$$\sum_{\substack{v \in \mathbb{F}_2^7 \\ \mathrm{wt}(v)=6}} W_g(v) = 7 \cdot 32 = 224,$$

whereas the bound in Conjecture 8.0.2 for $n = 7$ and $d = 4$ is 192. Thus, g is indeed a counterexample to Conjecture 8.0.2. Consequently, we conclude that Conjecture 8.0.1 and Conjecture 8.0.2 are not true in general.

x	$g(x)$	x	$g(x)$	x	$g(x)$
(0, 0, 0, 0, 0, 0, 0)	1	(1, 1, 0, 1, 0, 1, 0)	1	(0, 1, 1, 0, 1, 0, 1)	1
(1, 0, 0, 0, 0, 0, 0)	1	(0, 0, 1, 1, 0, 1, 0)	0	(1, 1, 1, 0, 1, 0, 1)	0
(0, 1, 0, 0, 0, 0, 0)	1	(1, 0, 1, 1, 0, 1, 0)	1	(0, 0, 0, 1, 1, 0, 1)	1
(1, 1, 0, 0, 0, 0, 0)	0	(0, 1, 1, 1, 0, 1, 0)	1	(1, 0, 0, 1, 1, 0, 1)	1
(0, 0, 1, 0, 0, 0, 0)	1	(1, 1, 1, 1, 0, 1, 0)	0	(0, 1, 0, 1, 1, 0, 1)	1
(1, 0, 1, 0, 0, 0, 0)	0	(0, 0, 0, 0, 1, 1, 0)	0	(1, 1, 0, 1, 1, 0, 1)	0
(0, 1, 1, 0, 0, 0, 0)	0	(1, 0, 0, 0, 1, 1, 0)	0	(0, 0, 1, 1, 1, 0, 1)	1
(1, 1, 1, 0, 0, 0, 0)	1	(0, 1, 0, 0, 1, 1, 0)	1	(1, 0, 1, 1, 1, 0, 1)	0
(0, 0, 0, 1, 0, 0, 0)	1	(1, 1, 0, 0, 1, 1, 0)	1	(0, 1, 1, 1, 1, 0, 1)	0
(1, 0, 0, 1, 0, 0, 0)	0	(0, 0, 1, 0, 1, 1, 0)	1	(1, 1, 1, 1, 1, 0, 1)	1
(0, 1, 0, 1, 0, 0, 0)	0	(1, 0, 1, 0, 1, 1, 0)	1	(0, 0, 0, 0, 0, 1, 1)	0
(1, 1, 0, 1, 0, 0, 0)	1	(0, 1, 1, 0, 1, 1, 0)	1	(1, 0, 0, 0, 0, 1, 1)	1
(0, 0, 1, 1, 0, 0, 0)	0	(1, 1, 1, 0, 1, 1, 0)	0	(0, 1, 0, 0, 0, 1, 1)	0
(1, 0, 1, 1, 0, 0, 0)	1	(0, 0, 0, 1, 1, 1, 0)	1	(1, 1, 0, 0, 0, 1, 1)	1
(0, 1, 1, 1, 0, 0, 0)	1	(1, 0, 0, 1, 1, 1, 0)	1	(0, 0, 1, 0, 0, 1, 1)	1
(1, 1, 1, 1, 0, 0, 0)	0	(0, 1, 0, 1, 1, 1, 0)	0	(1, 0, 1, 0, 0, 1, 1)	0
(0, 0, 0, 0, 1, 0, 0)	1	(1, 1, 0, 1, 1, 1, 0)	0	(0, 1, 1, 0, 0, 1, 1)	1
(1, 0, 0, 0, 1, 0, 0)	0	(0, 0, 1, 1, 1, 1, 0)	1	(1, 1, 1, 0, 0, 1, 1)	0
(0, 1, 0, 0, 1, 0, 0)	0	(1, 0, 1, 1, 1, 1, 0)	0	(0, 0, 0, 1, 0, 1, 1)	1
(1, 1, 0, 0, 1, 0, 0)	1	(0, 1, 1, 1, 1, 1, 0)	0	(1, 0, 0, 1, 0, 1, 1)	1
(0, 0, 1, 0, 1, 0, 0)	0	(1, 1, 1, 1, 1, 1, 0)	1	(0, 1, 0, 1, 0, 1, 1)	1
(1, 0, 1, 0, 1, 0, 0)	1	(0, 0, 0, 0, 0, 0, 1)	1	(1, 1, 0, 1, 0, 1, 1)	0
(0, 1, 1, 0, 1, 0, 0)	0	(1, 0, 0, 0, 0, 0, 1)	0	(0, 0, 1, 1, 0, 1, 1)	1
(1, 1, 1, 0, 1, 0, 0)	0	(0, 1, 0, 0, 0, 0, 1)	0	(1, 0, 1, 1, 0, 1, 1)	0
(0, 0, 0, 1, 1, 0, 0)	0	(1, 1, 0, 0, 0, 0, 1)	1	(0, 1, 1, 1, 0, 1, 1)	0
(1, 0, 0, 1, 1, 0, 0)	0	(0, 0, 1, 0, 0, 0, 1)	0	(1, 1, 1, 1, 0, 1, 1)	1
(0, 1, 0, 1, 1, 0, 0)	1	(1, 0, 1, 0, 0, 0, 1)	1	(0, 0, 0, 0, 1, 1, 1)	1
(1, 1, 0, 1, 1, 0, 0)	1	(0, 1, 1, 0, 0, 0, 1)	0	(1, 0, 0, 0, 1, 1, 1)	1
(0, 0, 1, 1, 1, 0, 0)	0	(1, 1, 1, 0, 0, 0, 1)	1	(0, 1, 0, 0, 1, 1, 1)	1
(1, 0, 1, 1, 1, 0, 0)	1	(0, 0, 0, 1, 0, 0, 1)	0	(1, 1, 0, 0, 1, 1, 1)	0
(0, 1, 1, 1, 1, 0, 0)	1	(1, 0, 0, 1, 0, 0, 1)	0	(0, 0, 1, 0, 1, 1, 1)	0
(1, 1, 1, 1, 1, 0, 0)	0	(0, 1, 0, 1, 0, 0, 1)	1	(1, 0, 1, 0, 1, 1, 1)	0
(0, 0, 0, 0, 0, 1, 0)	1	(1, 1, 0, 1, 0, 0, 1)	0	(0, 1, 1, 0, 1, 1, 1)	0
(1, 0, 0, 0, 0, 1, 0)	0	(0, 0, 1, 1, 0, 0, 1)	0	(1, 1, 1, 0, 1, 1, 1)	1
(0, 1, 0, 0, 0, 1, 0)	0	(1, 0, 1, 1, 0, 0, 1)	1	(0, 0, 0, 1, 1, 1, 1)	0
(1, 1, 0, 0, 0, 1, 0)	0	(0, 1, 1, 1, 0, 0, 1)	1	(1, 0, 0, 1, 1, 1, 1)	0
(0, 0, 1, 0, 0, 1, 0)	0	(1, 1, 1, 1, 0, 0, 1)	0	(0, 1, 0, 1, 1, 1, 1)	0
(1, 0, 1, 0, 0, 1, 0)	0	(0, 0, 0, 0, 1, 0, 1)	0	(1, 1, 0, 1, 1, 1, 1)	1
(0, 1, 1, 0, 0, 1, 0)	1	(1, 0, 0, 0, 1, 0, 1)	0	(0, 0, 1, 1, 1, 1, 1)	0
(1, 1, 1, 0, 0, 1, 0)	1	(0, 1, 0, 0, 1, 0, 1)	0	(1, 0, 1, 1, 1, 1, 1)	1
(0, 0, 0, 1, 0, 1, 0)	0	(1, 1, 0, 0, 1, 0, 1)	1	(0, 1, 1, 1, 1, 1, 1)	1
(1, 0, 0, 1, 0, 1, 0)	1	(0, 0, 1, 0, 1, 0, 1)	1	(1, 1, 1, 1, 1, 1, 1)	0
(0, 1, 0, 1, 0, 1, 0)	0	(1, 0, 1, 0, 1, 0, 1)	1		

Table 8.1: Truth table of g (Conjecture 8.0.2 counterexample).

x	$W_g(x)$	x	$W_g(x)$	x	$W_g(x)$
(0, 0, 0, 0, 0, 0, 0)	0	(1, 1, 0, 1, 0, 1, 0)	-16	(0, 1, 1, 0, 1, 0, 1)	-16
(1, 0, 0, 0, 0, 0, 0)	0	(0, 0, 1, 1, 0, 1, 0)	0	(1, 1, 1, 0, 1, 0, 1)	0
(0, 1, 0, 0, 0, 0, 0)	0	(1, 0, 1, 1, 0, 1, 0)	0	(0, 0, 0, 1, 1, 0, 1)	0
(1, 1, 0, 0, 0, 0, 0)	0	(0, 1, 1, 1, 0, 1, 0)	0	(1, 0, 0, 1, 1, 0, 1)	-16
(0, 0, 1, 0, 0, 0, 0)	0	(1, 1, 1, 1, 0, 1, 0)	0	(0, 1, 0, 1, 1, 0, 1)	0
(1, 0, 1, 0, 0, 0, 0)	0	(0, 0, 0, 0, 1, 1, 0)	0	(1, 1, 0, 1, 1, 0, 1)	0
(0, 1, 1, 0, 0, 0, 0)	0	(1, 0, 0, 0, 1, 1, 0)	0	(0, 0, 1, 1, 1, 0, 1)	0
(1, 1, 1, 0, 0, 0, 0)	-16	(0, 1, 0, 0, 1, 1, 0)	0	(1, 0, 1, 1, 1, 0, 1)	-16
(0, 0, 0, 1, 0, 0, 0)	0	(1, 1, 0, 0, 1, 1, 0)	0	(0, 1, 1, 1, 1, 0, 1)	-16
(1, 0, 0, 1, 0, 0, 0)	0	(0, 0, 1, 0, 1, 1, 0)	0	(1, 1, 1, 1, 1, 0, 1)	32
(0, 1, 0, 1, 0, 0, 0)	0	(1, 0, 1, 0, 1, 1, 0)	-16	(0, 0, 0, 0, 0, 1, 1)	0
(1, 1, 0, 1, 0, 0, 0)	-16	(0, 1, 1, 0, 1, 1, 0)	0	(1, 0, 0, 0, 0, 1, 1)	0
(0, 0, 1, 1, 0, 0, 0)	0	(1, 1, 1, 0, 1, 1, 0)	0	(0, 1, 0, 0, 0, 1, 1)	0
(1, 0, 1, 1, 0, 0, 0)	0	(0, 0, 0, 1, 1, 1, 0)	-16	(1, 1, 0, 0, 0, 1, 1)	0
(0, 1, 1, 1, 0, 0, 0)	0	(1, 0, 0, 1, 1, 1, 0)	0	(0, 0, 1, 0, 0, 1, 1)	-16
(1, 1, 1, 1, 0, 0, 0)	0	(0, 1, 0, 1, 1, 1, 0)	0	(1, 0, 1, 0, 0, 1, 1)	0
(0, 0, 0, 0, 1, 0, 0)	0	(1, 1, 0, 1, 1, 1, 0)	0	(0, 1, 1, 0, 0, 1, 1)	0
(1, 0, 0, 0, 1, 0, 0)	0	(0, 0, 1, 1, 1, 1, 0)	-16	(1, 1, 1, 0, 0, 1, 1)	0
(0, 1, 0, 0, 1, 0, 0)	0	(1, 0, 1, 1, 1, 1, 0)	-16	(0, 0, 0, 1, 0, 1, 1)	0
(1, 1, 0, 0, 1, 0, 0)	0	(0, 1, 1, 1, 1, 1, 0)	0	(1, 0, 0, 1, 0, 1, 1)	0
(0, 0, 1, 0, 1, 0, 0)	0	(1, 1, 1, 1, 1, 1, 0)	32	(0, 1, 0, 1, 0, 1, 1)	-16
(1, 0, 1, 0, 1, 0, 0)	0	(0, 0, 0, 0, 0, 0, 1)	0	(1, 1, 0, 1, 0, 1, 1)	0
(0, 1, 1, 0, 1, 0, 0)	-16	(1, 0, 0, 0, 0, 0, 1)	0	(0, 0, 1, 1, 0, 1, 1)	-16
(1, 1, 1, 0, 1, 0, 0)	0	(0, 1, 0, 0, 0, 0, 1)	0	(1, 0, 1, 1, 0, 1, 1)	0
(0, 0, 0, 1, 1, 0, 0)	0	(1, 1, 0, 0, 0, 0, 1)	0	(0, 1, 1, 1, 0, 1, 1)	-16
(1, 0, 0, 1, 1, 0, 0)	0	(0, 0, 1, 0, 0, 0, 1)	0	(1, 1, 1, 1, 0, 1, 1)	32
(0, 1, 0, 1, 1, 0, 0)	0	(1, 0, 1, 0, 0, 0, 1)	0	(0, 0, 0, 0, 1, 1, 1)	-16
(1, 1, 0, 1, 1, 0, 0)	-16	(0, 1, 1, 0, 0, 0, 1)	0	(1, 0, 0, 0, 1, 1, 1)	-16
(0, 0, 1, 1, 1, 0, 0)	0	(1, 1, 1, 0, 0, 0, 1)	-16	(0, 1, 0, 0, 1, 1, 1)	-16
(1, 0, 1, 1, 1, 0, 0)	0	(0, 0, 0, 1, 0, 0, 1)	0	(1, 1, 0, 0, 1, 1, 1)	-16
(0, 1, 1, 1, 1, 0, 0)	-16	(1, 0, 0, 1, 0, 0, 1)	-16	(0, 0, 1, 0, 1, 1, 1)	0
(1, 1, 1, 1, 1, 0, 0)	16	(0, 1, 0, 1, 0, 0, 1)	0	(1, 0, 1, 0, 1, 1, 1)	16
(0, 0, 0, 0, 0, 1, 0)	0	(1, 1, 0, 1, 0, 0, 1)	0	(0, 1, 1, 0, 1, 1, 1)	0
(1, 0, 0, 0, 0, 1, 0)	0	(0, 0, 1, 1, 0, 0, 1)	0	(1, 1, 1, 0, 1, 1, 1)	32
(0, 1, 0, 0, 0, 1, 0)	0	(1, 0, 1, 1, 0, 0, 1)	-16	(0, 0, 0, 1, 1, 1, 1)	0
(1, 1, 0, 0, 0, 1, 0)	0	(0, 1, 1, 1, 0, 0, 1)	0	(1, 0, 0, 1, 1, 1, 1)	0
(0, 0, 1, 0, 0, 1, 0)	0	(1, 1, 1, 1, 0, 0, 1)	16	(0, 1, 0, 1, 1, 1, 1)	16
(1, 0, 1, 0, 0, 1, 0)	-16	(0, 0, 0, 0, 1, 0, 1)	0	(1, 1, 0, 1, 1, 1, 1)	32
(0, 1, 1, 0, 0, 1, 0)	16	(1, 0, 0, 0, 1, 0, 1)	0	(0, 0, 1, 1, 1, 1, 1)	16
(1, 1, 1, 0, 0, 1, 0)	-16	(0, 1, 0, 0, 1, 0, 1)	0	(1, 0, 1, 1, 1, 1, 1)	32
(0, 0, 0, 1, 0, 1, 0)	0	(1, 1, 0, 0, 1, 0, 1)	0	(0, 1, 1, 1, 1, 1, 1)	32
(1, 0, 0, 1, 0, 1, 0)	16	(0, 0, 1, 0, 1, 0, 1)	0	(1, 1, 1, 1, 1, 1, 1)	-16
(0, 1, 0, 1, 0, 1, 0)	-16	(1, 0, 1, 0, 1, 0, 1)	0		

Table 8.2: Walsh transform g (Conjecture 8.0.2 counterexample).

Chapter 9

Conclusions

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.

We have provided a complete characterization of bent functions in $\mathcal{D}_0 \setminus \mathcal{M}^{\#}$ in Chapter 3, which further refines a sufficient condition of Carlet [9, Proposition 2]. Furthermore, in Chapter 4, we have shown that the sufficient conditions in [83] (related to the absence of linear structures in the component functions of a permutation) are not necessary in a quite general framework of specifying bent functions in $\mathcal{C}$ which are outside $\mathcal{M}^{\#}$, by providing a construction of permutations that do not satisfy the sufficient condition, but still produce bent functions in $\mathcal{C}$ outside $\mathcal{M}^{\#}$. On the other hand, in Chapter 4, the problem of specifying suitable permutations satisfying the sufficient conditions in [83] for generating bent functions which are outside the $\mathcal{M}^{\#}$ class is also addressed, and a class of permutation satisfying the conditions in provided, assuming that the dimension of the subspace L is not too large. The impossibility of finding such permutations for relatively large dimensions of the subspace L may again indicate that the sufficient conditions in [83] are too restrictive. It might be of interest to investigate whether some weaker conditions can be deduced or alternatively combined with the indicator based on the second order derivatives for the purpose of proving the exclusion from the class $\mathcal{M}^{\#}$. Even more importantly, a hard problem of showing whether the derived families are also outside $\mathcal{PS}^{\#}$ remains open. Nevertheless, we prove that asymptotically, bent functions in $\mathcal{PS}_{ap}$ are nonintersecting with the class $\mathcal{C}$. This is probably true when the completed $\mathcal{PS}$ class is considered, but it remains to be proved.

In Chapter 5, we have introduced a class of vectorial bent-negabent functions and specified a tight upper bound for the dimension of their output space, which can be reached using a set of linear complete mappings. The same goal becomes harder to achieve when nonlinear mappings are employed, but nevertheless three different methods, one of which is generic, are provided (some of them in Chapter 6) for specifying vectorial bent-negabent functions of varying output dimensions. Most notably, due to a specific choice of underlying permutations, these functions have a large number of components which are outside $\mathcal{M}^{\#}$. Similarly to the case of bent components, we derived the maximal number of bent-negabent components for mappings $F\colon \mathbb{F}_2^{2m} \to \mathbb{F}_2^k$, where $k \geq m$, and provided two constructions of such functions.

In Chapter 6, in order to describe the properties of vectorial bent functions (related to the class inclusion/exclusion problem) more precisely, we introduced the concept of weakly and strongly outside of a given class of bent functions. In this context, some questions related to vectorial bent functions that stem from the classes $\mathcal{C}$ and $\mathcal{D}$ have been addressed. In certain cases, such as the explicit subclass $\mathcal{D}_0$, vectorial bent functions with the maximal bent output dimension could be derived, though being only weakly outside $\mathcal{M}^{\#}$. In other words, due to the cancellation of the subspace indicators the component bent functions corresponding to linear combinations of even weight necessarily remain in the class $\mathcal{M}$. Using a suitable structure of the considered ambient space, mainly subfields of suitable order, we have also demonstrated the possibility of building vectorial bent functions from the classes $\mathcal{C}$ and $\mathcal{D}$, weakly outside $\mathcal{M}^{\#}$, whose output dimension is not maximal. We also exhibit vectorial bent functions $F : \mathbb{F}_2^{2n} \to \mathbb{F}_2^k$, derived from the class $\mathcal{C}$, which are strictly outside $\mathcal{M}^{\#}$, for some output dimensions k. The extendibility issue for the vectorial classes derived from $\mathcal{C}$ and $\mathcal{D}$, thus the possibility of extending these functions to the maximal output dimensions, remains open and appears to be very difficult.

In Chapter 7, we have provided compact proofs regarding some basic properties of correlation immune (CI) functions. In addition, more precision regarding the algebraic normal forms and the Walsh coefficients of k-CI functions has been obtained. Two construction methods of correlation immune functions are presented. They provide an efficient framework for the design of low weight CI functions and allow us to extend the range of the known 3-CI functions having the minimum Hamming weight. It is of interest to further refine these methods to possibly cover other values of $n = 4k$, which may give an efficient and alternative design of Hadamard matrices of the same size.

In Chapter 8, we have shown that O'Donnell's conjecture (Conjecture 8.0.1) is correct for $d \in \{2, 3\}$, apart from the previously confirmed cases $d \in \{1, n - 1, n\}$. The established cases $d \in \{2, 3\}$ give some interesting combinatorial properties related to the Walsh coefficients of weight $n - 1$ for $(n - 4)$ and $(n - 3)$-resilient functions. However, we show that the conjecture is not true in general, and more precisely, that it cannot be applied to $(n - 5)$-resilient functions. We remark that the weaker variant of this conjecture, due to P. Gopalan and R. Servedio, remains open.

Bibliography

[1] A. Akbary, D. Ghioca, Q. Wang. On constructing permutations of finite fields. *Finite Fields Appl.* 17, pp. 51–67, (2011).

[2] L.E. Baum, L.P. Neuwirth. Decompositions of vector spaces over GF(2) into disjoint equidimensional affine spaces. *Journal of Combinatorial Theory*, Series A, 18(1), pp. 88–100, (1975).

[3] A. Bapić, E. Pasalic, A. Polujan, A. Pott. Vectorial Boolean functions with the maximum number of bent components outside the $\mathcal{M}^{\#}$ class. *Proceedings of the Twelfth International Workshop on Coding and Cryptography*, (2022).

[4] S. Bhasin, C Carlet, S. Guilley. Theory of masking with codewords in hardware: low weight d-th order correlation-immune functions. *IACR ePrint Archive*, available at https://eprint.iacr.org/2013/303.pdf2013, (2014).

[5] S. Bhattacharya, S. Sarkar. On some permutation binomials and trinomials over $\mathbb{F}_{2^n}$. *Designs, Codes and Cryptography*, vol. 82(1-2), pp. 149–160, (2017).

[6] J. Bierbrauer, K. Gopalakrishnan, D. R. Stinson. Orthogonal arrays, resilient functions, error-correcting codes, and linear programming bounds. *SIAM Journal on Discrete Mathematics* 9(3), pp. 424–452, (1996).

[7] A. Braeken, Y. Borissov, S. Nikova, B. Preneel. Classification of cubic $(n-4)$-resilient Boolean functions. *IEEE Trans. on Inform. Theory* 52(4), pp. 1670–1676, (2006).

[8] P. Camion, C. Carlet, P. Charpin, N. Sendrier. On correlation-immune functions. *Annual International Cryptology Conference*, pp. 86–100, (1991).

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

[10] C. Carlet. On the coset weight divisibility and nonlinearity of resilient and correlation-immune functions. *Proceedings of SETA'01 (Sequences and their Applications 2001), Discrete Mathematics and Theoretical Computer Science*, pp. 131–144, (2001).

[11] C. Carlet. On the secondary constructions of resilient and bent functions. *In Proc. Coding, Cryptograph. Combinat.*, published by Birkhäuser Verlag, vol. 23, pp. 3–28, (2004).

[12] C. Carlet. Boolean Functions for Cryptography and Coding Theory. *Cambridge University Press*, (2020).

[13] C. Carlet, P. Charpin. Cubic Boolean functions with highest resiliency. *IEEE Trans. on Inform. Theory* 51(2), pp. 562–571, (2005).

[14] C. Carlet, F. Zhang, Y. Hu. Secondary constructions of bent functions and their enforcement. *Adv. Math. Commun.*, vol. 6, pp. 305–314, (2012).

[15] C. Carlet, S. Guilley. Side-channel indistinguishability. *Proceedings of HASP '13, 2nd International Workshop on Hardware and Architectural Support for Security and Privacy*, pp. 9:1-9:8. Tel Aviv, Israel, June 2013. ACM, New York, (2013).

[16] C. Carlet, X. Chen. Constructing low-weight dth-order correlation-immune Boolean functions through the Fourier-Hadamard transform. *IEEE Trans. on Inform. Theory*, 64(4), pp. 2969–2978, (2018).

[17] L. Carlitz, C. Wells. The number of solutions of a special system of equations in a finite field. *Acts. Arith.* vol. 12, pp. 77–84, (1966).

[18] N. Cepak, P. Charpin, E. Pasalic. Permutations via linear translators. *Finite Fields and Their Applications*, vol. 45, pp. 19–42, (2017).

[19] P. Charpin, G. Kyureghyan. Monomial functions with linear structure and permutation polynomials. *Finite Fields: Theory and Applications FQ9*, vol. 518, pp. 99–111, (2010).

[20] T. W. Cusick, P. Stănică. Cryptographic Boolean functions and applications. *Elsevier–Academic Press*, (2009).

[21] J. F. Dillon. Elementary Hadamard difference sets. *In proceedings of 6th S. E. Conference of Combinatorics, Graph Theory, and Computing*, Utility Mathematics, Winnipeg, pp. 237–249, (1975).

[22] J. F. Dillon. Elementary Hadamard difference sets, Ph.D. dissertation. *University of Maryland, College Park, Md, USA*, (1974).

[23] C. Ding, G. Xiao, W. Shan. The stability theory of stream ciphers. *Springer Science & Business Media*, (1991).

[24] J. Du, L. Qu, C. Li, X. Liao. Constructing 1-resilient rotation symmetric functions over $\mathbb{F}_p$ with q variables through special orthogonal arrays *Advances in Mathematics of Communications*, (2019).

[25] R. J. Evans, J. Greene, H. Niederreiter. Linearized polynomials and permutation polynomials of finite fields. *Michigan Mathematical Journal*, vol. 39, pp. 405–413, (1992).

[26] K. Gopalakrishnan, D. R. Stinson. Applications of designs to cryptography. *The CRC Handbook of Combinatorial Designs* pp. 549–557, (1996).

[27] R. Gupta, R.K. Sharma. Some new classes of permutation trinomials over finite fields with even characteristic. *Finite Fields Appl.*, vol. 41(C), pp. 89–96, (2016).

[28] S. Hodžić, E. Pasalic, Y. Wei. A general framework for secondary constructions of bent and plateaued functions. *Des. Codes Cryptogr.*, vol. 88(10), pp. 2007–2035, (2020).

[29] X. Hou. Permutation polynomials over finite fields — A survey of recent advances. *Finite Fields and Their Applications*, vol. 32, pp. 82–119, (2015).

[30] T. Johansson, F. Jönsson. Improved fast correlation attacks on stream ciphers via convolutional codes. In *Advances in Cryptology—EUROCRYPT'99*, volume LNCS 1592, pp. 347–362, Springer-Verlag, (1999).

[31] T. Johansson, F. Jönsson. Fast correlation attacks based on turbo code techniques. In *Advances in Cryptology—CRYPTO'99*, LNCS, vol. 1666, pp. 181–197, Springer-Verlag, (1999).

[32] S. Kudin, E. Pasalic. Efficient design methods of low-weight correlation-immune functions and revisiting their basic characterization. *Discrete Applied Mathematics*, vol. 284, pp. 150–157, (2020).

[33] S. Kudin, E. Pasalic. Proving the conjecture of O'Donnell in certain cases and disproving its general validity. *Discrete Applied Mathematics*, vol. 289, pp. 345–353, (2021).

[34] S. Kudin, E. Pasalic. A complete characterization of $\mathcal{D}_0 \cap \mathcal{M}^{\#}$ and a general framework for specifying bent functions in $\mathcal{C}$ outside $\mathcal{M}^{\#}$. *Designs, Codes and Cryptography*, vol. 90(8), pp. 1783–1796, (2022).

[35] S. Kudin, E. Pasalic, N. Cepak, F. Zhang. Permutations without linear structures inducing bent functions outside the completed Maiorana-McFarland class. *Cryptography and Communications*, vol. 14(1), pp. 101–116, (2022).

[36] G. M. Kyureghyan. Constructing permutations of finite fields via linear translators. *J. Combinatorial Theory, Ser. A*, Vol. 118, pp. 1052–1061, (2011).

[37] P. Langevin, G. Leander. Counting all bent functions in dimension eight 99270589265934370305785861242880. *Designs, Codes and Cryptography*, vol. 59, pp. 193—205, (2011).

[38] S. Li, W. Meidl, A. Polujan, A. Pott, C. Riera, P. Stănică. Vanishing Flats: A Combinatorial Viewpoint on the Planarity of Functions and Their Application. *IEEE Transactions on Information Theory*, vol. 66(11), pp. 7101–7112, (2020).

[39] K. Li, L. Qu, X. Chen. New classes of permutation binomials and permutation trinomials over finite fields. *Finite Fields Appl.*, vol. 43, pp. 69–85, (2017).

[40] B. Mandal, S. Maitra, P. Stănică. On the existence and non-existence of some classes of bent–negabent functions. *Appl. Algebra Eng. Commun. Comput.* (2020).

[41] B. Mandal, P. Stanica, S. Gangopadhyay, E. Pasalic. An analysis of $\mathcal{C}$ class of bent functions. *Fundamenta Informaticae*, vol. 147 (3), pp. 271–292, (2016).

[42] J.L. Massey, R.A. Rueppel. Linear Ciphers and Random Sequence Generators with Multiple Clocks. *In: Beth, T., Cot, N., Ingemarsson, I. (eds) Advances in Cryptology. EUROCRYPT 1984. Lecture Notes in Computer Science*, vol. 209, pp. 74–87, (1985).

[43] R. L. McFarland. A family of noncyclic difference sets. *J. Combinatorial Theory, Ser. A*, Vol. 15, pp. 1–10, (1973).

[44] F. J. McWilliams, N. J. A Sloane. The theory of error-correcting codes. Parts I and II. *North-Holland Publishing Company*, Amsterdam, (1977).

[45] W. Meier, O. Staffelbach. Fast correlation attacks on certain stream ciphers. *Journal of Cryptology*, Vol. 1, pp. 159–176, (1989).

[46] A. J. Menezes, S. A. Vanstone, P. C. Van Oorschot. Handbook of Applied Cryptography. 1st ed., *CRC Press, Inc.*, Boca Raton, FL, USA, (1996).

[47] S. Mesnager. Several new infinite families of bent functions and their duals. *IEEE Trans. on Inform. Theory*, vol. 60, no. 7, pp. 4397–4407, (2014).

[48] S. Mesnager. Bent functions - Fundamentals and Results. *Springer*, (2016).

[49] G. L. Mullen, Q. Wang. Permutation polynomials. Chapter 8 in *Handbook of Finite Fields*, Chapman and Hall/CRC, Boca Raton, FL, pp. 215–230, (2013).

[50] K. Nyberg. Perfect nonlinear S-Boxes. *Advances in Cryptology - EUROCRYPT '91, Lecture Notes in Computer Science*, vol. 547, (1991).

[51] R. O'Donnell. Analysis of boolean functions. *Cambridge University Press*, (2014).

[52] R. O'Donnell. Open problems in analysis of Boolean functions. *arXiv preprint*, arXiv:1204.6447, (2012).

[53] M. G. Parker, A. Pott. On Boolean functions which are bent and negabent. In *Sequences, Subsequences, Consequences, Lecture Notes in Computer Science, Springer*, Berlin, vol. 4893, pp. 9–23, (2007).

[54] E. Pasalic, T. Johansson, S. Maitra, P. Sarkar. New constructions of resilient and correlation immune Boolean functions achieving upper bound on nonlinearity. *Electronic Notes in Discrete Mathematics* vol. 6, pp. 158–167, (2001).

[55] E. Pasalic, F. Zhang, S. Kudin, Y. Wei. Vectorial bent functions weakly/strongly outside the completed Maiorana–McFarland class. *Discrete Applied Mathematics*, vol. 294, pp. 138–151, (2021).

[56] E. Pasalic, S. Kudin, A. Polujan, A. Pott. Vectorial bent-negabent functions - their constructions and bounds. *IEEE Trans. on Inform. Theory*, doi: 10.1109/TIT.2022.3226571, (2022).

[57] A. Polujan, A. Pott. On design-theoretic aspects of Boolean and vectorial bent functions. *IEEE Trans. on Inform. Theory*, vol. 67(2), pp. 1027–1037, (2021).

[58] A. Pott. Almost perfect and planar functions. *Designs, Codes and Cryptography*, vol. 78(1), pp. 141–195, (2016).

[59] A. Pott, K-U. Schmidt, Y. Zhou. Pairs of quadratic forms over finite fields. *Electron. J. Comb.* 23(2), P. 2.8, (2016)

[60] A. Pott, E. Pasalic, A. Muratović-Ribić, S. Bajrić. On the maximum number of bent components of vectorial functions. *IEEE Trans. on Inform. Theory*, vol. 64(1), pp. 403–411, (2018).

[61] C. Riera, M. G. Parker. Generalized bent criteria for Boolean functions. *IEEE Trans. on Inform. Theory*, 52(9), pp. 4142–4159, (2006).

[62] O. S. Rothaus. On Bent Functions. *J. Combinatorial Theory, Ser. A*, vol. 20, pp. 300–305, (1976).

[63] P. Sarkar. A note on the spectral characterisation of correlation immune Boolean functions. *Information Processing Letters*, vol. 74(5-6), pp. 191–195, (2000).

[64] P. Sarkar, S. Maitra. Nonlinearity Bounds and Constructions of Resilient Boolean Functions. *Proceedings of CRYPTO 2000, Lecture Notes in Computer Science 1880*, pp. 515–532, (2000).

[65] K.-U. Schmidt, M. G. Parker, A. Pott. Negabent functions in Maiorana–McFarland class. In: *SETA, LNCS* vol. 5203, pp. 390–402, (2008).

[66] C. E. Shannon. A mathematical theory of communication, *Bell System Technical Journal, vol. 27:379423 (Part I) and 623656 (Part II)*, (1948).

[67] T. Siegenthaler. Correlation-immunity of nonlinear combining functions for cryptographic applications. *IEEE Trans. on Inform. Theory*, vol. 30(5), pp. 776–780, (1984).

[68] T. Siegenthaler. Decrypting a class of stream ciphers using ciphertext only. *IEEE Trans. on Computers*, C-34, pp. 81–85, (1985).

[69] P. Stănică, S. Gangopadhyay, A. Chaturvedi, A. K. Gangopadhyay, S. Maitra. Investigations on bent and negabent functions via the nega-Hadamard transform. *IEEE Trans. on Inform. Theory*, 58(6), pp. 4064–4072, (2012).

[70] P. Stănică, B. Mandal, S. Maitra. The connection between quadratic bent–negabent functions and the Kerdock code. *Appl. Algebra Eng. Commun. Comput.*, vol. 30(5), pp. 387–401, (2019).

[71] W. Su, A. Pott, X. Tang. Characterization of negabent functions and construction of bent–negabent functions with maximum algebraic degree. *IEEE Trans. Inf. Theory*, vol. 59(6), pp. 3387–3395, (2013).

[72] Y. Tarannikov. On resilient Boolean functions with maximal possible nonlinearity. *Proceeding of INDOCRYPT 2000, Lecture Notes in Computer Science 1977*, pp. 19–30, (2000).

[73] N. Tokareva. Bent functions: results and application to cryptography. *Academic Press*, (2015).

[74] Z. Tu, X. Zeng, L. Hu. Several classes of complete permutation polynomials. *Finite Fields and Their Applications*, vol. 25, pp. 182–193, (2014).

[75] L. Wang, B. Wu, Z. Liu, D. Lin. Three new infinite families of bent functions. *Sci. China Inf. Sci.*, vol. 61, 032104, (2018).

[76] Q. Wang. Hadamard matrices, d-linearly independent sets and correlation-immune Boolean functions with minimum Hamming weights. *Designs Codes and Cryptography*, vol. 87, pp. 2321–2333, (2019).

[77] Q. Wang. On a Conjecture of O'Donnell. *IACR Cryptology ePrint Archive*, `https://eprint.iacr.org/2020/002`, (2020).

[78] Q. Wang, Y. Li. A note on minimum Hamming weights of correlation-immune Boolean functions. *IEEE Trans. Fundamentals* vol. E102-A (2), pp. 464–466, (2019).

[79] Z. Wang, G. Gong. Discrete Fourier transform of Boolean functions over the complex field and its applications. *IEEE Trans. on Inform. Theory*, vol. 64(4), pp. 3000–3009, (2018).

[80] G. Weng, R. Feng, W. Qiu. On the ranks of bent functions. *Finite Fields and Their Applications* 13(4), pp. 1096–1116, (2007).

[81] G.Z. Xiao, J. L. Massey. A spectral characterization of correlation-immune combining functions. *IEEE Trans. on Inform. Theory*, vol. 34(3), pp. 569–571, (1988).

[82] F. Zhang, Y. Wei, E. Pasalic. Constructions of bent-negabent functions and their relation to the completed Maiorana–McFarland class. *IEEE Trans. on Inform. Theory*, vol. 61(3), pp. 1496–1506, (2015)

[83] F. Zhang, E. Pasalic, N. Cepak, Y. Wei. Bent functions in $\mathcal{C}$ and $\mathcal{D}$ outside the completed Maiorana-McFarland class. *Codes, Cryptology and Information Security*, C2SI, LNCS 10194, Springer-Verlag, pp. 298–313, (2017).

[84] F. Zhang, N. Cepak, E. Pasalic, Y. Wei. Further analysis of bent functions from $\mathcal{C}$ and $\mathcal{D}$ which are provably outside or inside $\mathcal{MM}^{\#}$. *Discret. Appl. Math.* vol. 285, pp. 458–472, (2020).

[85] L. Zheng, J. Peng, H. Kan, Y. Li. Several new infinite families of bent functions via second order derivatives. *Cryptogr. Commun.*, vol. 12, pp. 1143–1160, (2020).

[86] L. Zheng, J. Peng, H. Kan, Y. Li, Y. Luo. On constructions and properties of (n, m)-functions with maximal number of bent components. *Designs, Codes and Cryptography*, vol. 88, pp. 2171–2186, (2020).

Index

Povzetek v slovenskem jeziku

Glavni predmet študija doktorske disertacije so kriptografsko pomembne lastnosti Boolovih funkcij. Neformalno so Boolove funkcije funkcije, ki kot vhodne parametre sprejmejo nize ničel in enic (fiksne dolžine) in kot izhodni podatek vrnejo ničlo ali enico, ali v bolj splošnem primeru vektorskih Boolovih funkcij, izpišejo tudi nize ničel in enic. Ta intuitivni pojem formaliziramo tako, da rečemo, da so Boolove funkcije funkcije, ki slikajo iz $\{0,1\}^n$ (kjer je n naravno število) v $\{0,1\}$, ali v vektorskem primeru v $\{0,1\}^k$ (kjer je k tudi neko naravno število, morda drugačno od n).

Z razvojem in porastom zanimanja za sodobno računalništvo, ki se je začelo v prvi polovici 20. stoletja, je vzporedno naraščalo zanimanje znanstvene skupnosti za različne lastnosti Boolovih funkcij, ki so postale ena temeljnih predmetov študija teoretičnega računalništva. Kmalu je postal pomen varne zasebne komunikacije očiten in leta 1945 (objavljeno leta 1949 v [66]) je Claude Shannon opredelil dve lastnosti, zmedo in razpršenost, ki ju mora imeti vsaka varna šifra, da bi preprečila statistične napade in druge metode kriptoanalize. Po drugi strani pa nam zmeda in razpršenost pomagata ugotoviti, katere lastnosti Boolovih funkcij, uporabljenih v varni šifri, so zaželene in katere nezaželene. Te lastnosti imenujemo kriptografsko pomembne lastnosti Boolovih funkcij.

Ena od kriptografsko pomembnih lastnosti Boolovih funkcij je nelinearnost. Da bi se izognili linearnim napadom, v splošnem želimo, da so funkcije, ki se uporabljajo v šifri, čim bolj nelinearne, seveda ob upoštevanju drugih zaželenih kriptografskih lastnosti. Motiviran s tem je v šestdesetih letih prejšnjega stoletja (objavljeno leta 1976 v [62]) O. Rothaus uvedel razred Boolovih funkcij, imenovanih ukrivljene funkcije, in jih opredelil kot Boolove funkcije, ki so čim bolj oddaljene od linearnih in afinih funkcij (razdalja med dvema funkcijama je Hammingova razdalja, torej število vektorjev, v katerih se funkciji razlikujeta).

Pomemben del raziskav ukrivljenih funkcij se ukvarja z njihovimi konstrukcijami, torej z iskanjem različnih načinov za konstruiranje ukrivljenih funkcij. Konstrukcije ukrivljenih funkcij so razdeljene v dve skupini: primarne konstrukcije (konstrukcije, ki ne uporabljajo drugih ukrivljenih funkcij za konstruiranje novih) in sekundarne konstrukcije (konstrukcije, ki uporabljajo druge ukrivljene funkcije za konstruiranje novih). Za podrobno raziskavo o ukrivljenih funkcijah se sklicujemo na knjigo S. Mesnager [48], medtem ko je izčrpno raziskavo o kriptografskih (vektorskih) Boolovih funkcijah mogoče najti v [12]. Dva najbolje raziskana primarna razreda ukrivljenih funkcij sta razreda Maiorana-McFarland ($\mathcal{M}$) in razred delni pokritij (Partial Spread) ($\mathcal{PS}$), ki sta bila predstavljena v sedemdesetih letih prejšnjega stoletja v [43] oziroma [21,22]. Ker je v praksi zahtevno sestaviti elemente razreda $\mathcal{PS}$,

je naveden eksplicitni podrazred razreda $\mathcal{PS}$, označen z $\mathcal{PS}_{ap}$ v [21] zaradi enostavnejše konstrukcije. Delni seznam različnih sekundarnih konstrukcij je na voljo v sledečih delih [11, 14, 28, 47, 75, 85]. (Popoln Maiorana-McFarland razred je množica vseh Boolovih funkcij na $2n$ spremenljivkah oblike

$$f(x, y) = x \cdot \pi(y) + \rho(y), \text{ za vse } x, y \in \mathbb{F}_2^n,$$

kjer je ρ poljubna Boolova funkcija nad prostorom $\mathbb{F}_2^n$, π pa je permutacija prostora $\mathbb{F}_2^n$.)

V devetdesetih letih prejšnjega stoletja je Carlet ([9]) predstavil dve novi sekundarni konstrukciji ukrivljenih funkcij z uporabo ukrivljenih funkcij iz razreda $\mathcal{M}$ in dodal indikatorje ustrezno izbranega vektorskega podprostora. Razreda ukrivljenih funkcij, ki jih dobimo s to konstrukcija, se imenujeta razred $\mathcal{C}$ in $\mathcal{D}$. Določen podrazred razreda $\mathcal{C}$ in $\mathcal{D}$, imenovan razred $\mathcal{D}_0$, je v [9] izpostavljen zaradi enostavnejše oblike uporabljenih podprostorov in zaradi enostavne konstrukcije. V [9] je ugotovljeno, da v razredu $\mathcal{D}_0$ obstajajo funkcije, ki niso afino ekvivalentne nobeni funkciji v razredu $\mathcal{M}$, kot tudi, da obstajajo nekatere funkcije v razredu $\mathcal{D}_0$, ki niso afino ekvivalentne nobeni funkciji v razredu $\mathcal{PS}$.

V Poglavju 3 se bomo osredotočil na natančnejši opis (glede na pripadnost razredu) sekundarnega razreda ukrivljenih funkcij $\mathcal{D}_0$. Carlet je v [9, Predlogi 2] zagotovil zadosten pogoj, da leži ukrivljena funkcija v razredu $\mathcal{D}_0$ oblike $f(x, y) = x \cdot \pi(y) + \delta_0(x)$ nad $\mathbb{F}_2^{2n}$, kjer je $x, y \in \mathbb{F}_2^n$, π permutacija $\mathbb{F}_2^n$ in $\delta_0(x)$ indikator (karakteristična funkcija) podprostora $\{0_n\} \times \mathbb{F}_2^n$, zunaj razreda $\mathcal{M}^\#$ na podlagi lastnosti permutacije π. ($\mathcal{M}^\#$ označuje popoln razred $\mathcal{M}$, ki je razred vseh ukrivljenih funkcij, ki so afino ekvivalentne funkcijam v razredu $\mathcal{M}$.) Namreč, če permutacija π ni afina na nobeni hiperravnini prostora $\mathbb{F}_2^n$, potem funkcija f leži zunaj razreda $\mathcal{M}^\#$. Pokazali bomo, da, ko je stopnja permutacije π večja od 2, Boolova funkcija $f(x, y) = x \cdot \pi(y) + \delta_0(x)$, z $f : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2$, vedno leži zunaj razreda $\mathcal{M}^\#$ (ne glede na to, ali je permutacija π afina na neki hiperravnini ali ne). Po drugi strani pa bomo dokazali, da je zadosten pogoj Carleta nujen tudi pri $\deg(\pi) = 2$. Posledično, podajamo popoln opis razmerja med razredoma $\mathcal{D}_0$ in $\mathcal{M}^\#$.

V Poglavju 4 bomo obravnavali problem pripadnosti za sekundarni razred ukrivljenih funkcij $\mathcal{C}$. Ogledali si bomo problem določanja ukrivljenih funkcij v razredu $\mathcal{C}$, ki so oblike $f(x, y) = x \cdot \pi(y) + \mathbb{1}_{L^\perp}(x)$, kjer je $x, y \in \mathbb{F}_2^n$, za ustrezno izbran podprostor $L \subseteq \mathbb{F}_2^n$, ki so dokazljivo zunaj $\mathcal{M}^\#$. Nabor zadostnih pogojev je bil prvotno določen v [83] in ti se v glavnem nanašajo na določene lastnosti permutacije π, ki vključujejo zahtevo, da komponentne funkcije permutacije π ne vsebujejo linearnih struktur. Ti zadostni pogoji so zelo uporabni pri določanju ukrivljenih funkcij v $\mathcal{C} \backslash \mathcal{M}^\#$, vendar je bilo dokazano, da niso potrebni, glej npr. [84]. Zlasti se je pokazalo, da nekatere modifikacije identične permutacije π (zamenjava dveh izhodnih vrednosti) zagotavljajo ukrivljene funkcije v razredu $\mathcal{D}$, ki dokazljivo ležijo zunaj $\mathcal{M}^\#$, čeprav komponentne funkcije permutacije π dopuščajo linearne strukture. V tem kontekstu, povezanem z ukrivljenimi funkcijami v razredu $\mathcal{C}$, bomo pokazali močnejši rezultat, ki omogoča modifikacije permutacije identitete na poljubnih podmnožicah ustrezno izbranih podprostorov (za namen definiranja permutacije π), hkrati pa bomo opisali ukrivljene funkcije, ki dokazljivo ležijo v $\mathcal{C} \backslash \mathcal{M}^\#$. Komponentne funkcije takšnih permutacij π še vedno dopuščajo linearne strukture, ki ponovno kažejo, da

obstaja možnost sprostitve niza zadostnih pogojev v [85]. Upoštevajmo, da nam bo možnost izbire poljubne podmnožice linearnega podprostora za modifikacijo permutacije identitete dala veliko neskončnih razredov ukrivljenih funkcij v $\mathcal{C}$, ki so dokazljivo zunaj $\mathcal{M}^{\#}$.

V Poglavju 4 bomo tudi raziskavi, ki se ukvarja z obratnim problemom. Torej, zgradili bomo razred permutacij, primernih za določanje ukrivljenih funkcij razreda $\mathcal{C}$, ki so dokazljivo zunaj dokončanega $\mathcal{M}^{\#}$ razreda z zadostnimi rezultati, dokazanimi v [83]. Da bi ponazorili kompleksnost osnovnega problema, bomo najprej pokazali, da permutacije, ki temeljijo na odsekih, niso primerne za naš namen, saj imajo člani te družine permutacij neizogibno komponentne funkcije, ki dopuščajo linearne strukture. Namesto tega uporabljamo določeno metodo netrivialne razdelitve vektorskega prostora $\mathbb{F}_2^n$ v disjunktne afine podprostore, ki sta jo prvotno obravnavala L.E. Baum in L.P. Neuwirth v [2]. Permutacije so konstruirane z uporabo dekompozicije in ustreznih permutacij v manjšem številu spremenljivk. Možnost izbire različnih podprostorov pri razgradnji in različnih permutacij v manjšem številu spremenljivk nam omogoča konstrukcijo družine ukrivljenih funkcij v razredu $\mathcal{C}$, ki so zunaj $\mathcal{M}^{\#}$. Ta pristop zahteva, da je dimenzija podprostora L manjša od $n/2$. V nasprotju s tem rezultatom dokazujemo, da, ko je dimenzija podprostora L relativno velika in komponente permutacije ne dopuščajo linearnih struktur, par (π^{-1}, L) ne more izpolnjevati lastnosti (C). (Pravimo da (π^{-1}, L) izpolnjujeta lastnost (C), če je $\pi^{-1}(a + L)$ afin podprostor za vse $a \in \mathbb{F}_2^n$.) Ta rezultat daje nadaljnji vpogled v to, kar je verjetno kompromis v uporabi zadostnih (vendar ne potrebnih) pogojev v [83] za razlikovanje ukrivljenih funkcij v $\mathcal{C}$, ki so zunaj $\mathcal{M}^{\#}$.

S pomočjo ranga ukrivljenih funkcij bomo v Poglavju 4 raziskali tudi presečišče razreda $\mathcal{C}$ in razreda delnega pokritja $\mathcal{PS}_{ap}$ ter pokazali, da se verjetnost, da je funkcija n spremenljivk, ki je v razredu $\mathcal{PS}_{ap}$, tudi v $\mathcal{C}$, približuje nič, ko se n povečuje.

V drugem delu disertacije se bomo osredotočili na vektorske Boolove funkcije in raziskali različne lastnosti, povezane z nelinearnostjo vektorskih Boolovih funkcij. Ukrivljena lastnost Boolovih funkcij je bila razširjena na vektorske Boolove funkcije z zahtevo, da so vse neničelne linearne kombinacije njihovih koordinatnih funkcij ukrivljene funkcije. Takšne vektorske funkcije se imenujejo vektorske ukrivljene funkcije. V literaturi so metode za konstruiranje novih vektorskih ukrivljenih funkcij ponovno razdeljene v dva razreda: konstrukcije brez začetnih ukrivljenih funkcije se imenujejo primarne; tiste, ki uporabljajo znane vektorske ukrivljene funkcije, se imenujejo sekundarne. Za primarne konstrukcije je K. Nyberg najprej predstavila konstrukcije vektorskih ukrivljenih funkcij, ki temeljijo na nekaterih posebnih razredih ukrivljenih funkcij, kot sta razred Maiorana-McFarland in Dillonov razred delnega pokritja.

V Poglavju 5 bomo definirali in raziskali razred ukrivljenih-negaukrivljenih vektorskih Boolovih funkcij. C. Riera in M. Parker v [61] sta predstavila razred negaukrivljenih funkcij motivirana z aplikacijami za kvantno računalništvo. Za funkcijo rečemo, da je negaukrivljena, če je njen absolutni nega-Hadamardov spekter plosk (ali ekvivalentno, f je negaukrivljena, če je $f + s_2$ ukrivljena, kjer s_2 označuje elementarno simetrično kvadratno Boolovo funkcijo, tj. $s_2(x) = \sum_{1 \le i < j \le n} x_i x_j$, za $x =$

$(x_1, \ldots, x_n) \in \mathbb{F}_2^n$). Za sodo število spremenljivk se funkcija imenuje ukrivljena-negaukrivljena, če je hkrati ukrivljena in negaukrivljena. Problem konstruiranja Boolovih funkcij, ki so hkrati ukrivljene in negaukrivljene, je bil obravnavan v [53, 65, 69, 71, 82]. M. Parker in A. Pott [53] sta obravnavala problem določanja števila kvadratnih ukrivljenih-negaukrivljenih funkcije v n spremenljivkah. Rešil so ga A. Pott *et al.* v [59], ki so uporabil karakterizacijo kvadratnih ukrivljenih-negaukrivljenih Boolovih funkcij, ki sta jo navedla M. Parker in A. Pott [53].

Obstaja več metod načrtovanja ukrivljenih-negaukrivljenih funkcij, ki so podane v npr. [65, 71, 82]. V [71] je bil izpeljan nabor potrebnih in zadostnih pogojev, da je Boolova funkcija negaukrivljena (ne glede na pariteto števila spremenljivk), kar je omogočilo tudi načrtovanje širšega razreda negaukrivljenih funkcij v n-spremenljivkah (n sodo) z algebraično stopnjo v razponu od 2 do $n/2$. Te funkcije pa so vsebovane v popolnem razredu Maiorana-McFarland ($\mathcal{M}$). Za razliko od standardne uporabe razreda Maiorana-McFarland, je bilo v [82] prikazano, da je mogoče ukrivljene-negaukrivljene funkcije zunaj popolnega razreda $\mathcal{M}$ konstruirati z uporabo metode posredne vsote in ustreznih popolnih preslikav.

Naj omenimo, da so o uporabi popolnih preslikav sprva razmišljali Stănică *et al.* [69], pozneje pa so te preslikave uporabili (v okviru tako imenovane posredne vsote) za konstruiranje ukrivljenih-negaukrivljenih funkcij zunaj popolnega razreda $\mathcal{M}$ [82]. Ukrivljene-negaukrivljene funkcije so bile v zadnjem času deležne nove pozornosti zaradi dela v [70], kjer je bila vzpostavljena povezava med ukrivljenimi-negaukrivljenimi funkcijami in Kerdock kodami, ter pred kratkim v [40], kjer je bil raziskan (ne)obstoj teh objektov v razredu ukrivljenih funkcij Maiorana-McFarland.

Kljub temu so vse doslej znane metode obravnavale le primer Boolovih funkcij in možnost konstrukcije vektorskih prostorov ukrivljenih negaukrivljenih funkcij v literaturi ni bila obravnavana. Uvedli bomo pojem *vektorske ukrivljene-negaukrivljene* funkcije in pokazali, da mora za ukrivljeno-negaukrivljeno funkcijo $F\colon \mathbb{F}_2^{2n} \to \mathbb{F}_2^k$ nujno veljati $k \leq n-1$. Določimo razred vektorskih ukrivljenih-negaukrivljenih funkcij z največjo izhodno dimenzijo $n-1$ z uporabo množice linearnih popolnih preslikav kardinalnosti $n-1$. Vendar pa zaradi linearnosti teh preslikav ta pristop generira samo funkcije, katerih komponente so vsebovane v razredu $\mathcal{M}$. Potem bomo pokazali, da so tako imenovane b-popolne preslikave na $\mathbb{F}_{2^n}$, obravnavane v npr. [18], torej permutacije $x + bF(x)$ za mnogo elementov $b \in \mathbb{F}_{2^n}$, lahko uporabljene za načrtovanje nekvadratnih vektorskih ukrivljenih-negaukrivljenih funkcij. Na podoben način, kot je bilo to storjeno za vektorske ukrivljene funkcije [60, 85], izpeljemo zgornjo mejo za največje število ukrivljenih-negaukrivljenih komponent za preslikave $F : \mathbb{F}_2^{2n} \to \mathbb{F}_2^k$, kjer je $2 \leq k \leq 2n$, in identificiramo nekatere družine teh funkcij, ki dosežejo zgornjo mejo.

Da bi natančneje opisali lastnosti teh vektorskih ukrivljenih funkcij, v Poglavju 6 uvedemo koncept *šibke izločenosti* in *močne izločenosti* zunaj dokončanega vnaprej določenega primarnega razreda. Glavni razlog za to je, da je za razred Maiorana-McFarland enostavno sklepati, da imajo njegove vektorske ukrivljene funkcije lastnost, da so vse linearne kombinacije (komponente), ki niso ničelne, ukrivljene funkcije v $\mathcal{M}$. To v splošnem ne velja za vektorske funkcije, ki imajo koordinate v $\mathcal{C}$ ali $\mathcal{D}$, saj večina metod, predstavljenih v disertaciji, zagotavlja komponentne ukrivljene funkcije, ki ne tvorijo enega samega razreda. Na primer, definicija vektorske ukrivl-

jene funkcije $F = (f_1, \ldots, f_n)$, kjer je $F : \mathbb{F}_2^{2n} \to \mathbb{F}_2^n$ in vsak $f_i \in \mathcal{D}_0$, implicira, da vsaka linearna kombinacija f_i enake teže daje ukrivljeno funkcijo v $\mathcal{M}$. Glavni interes našega koncepta, da smo *šibko* ali *močno* zunaj $\mathcal{M}^\#$, izhaja iz dejstva, da bodo v prvem delu disertacije predstavljeni določeni neskončni razredi ukrivljenih funkcij v $\mathcal{C}$ in $\mathcal{D}$, ki dokazljivo ležijo zunaj $\mathcal{M}^\#$. Nato z uporabo takšnih funkcij, kot so začetne ukrivljene funkcije, dobimo vektorske ukrivljene prostore, katerih določene komponente so v primarnem razredu $\mathcal{M}$. Preostale pripadajo razredoma $\mathcal{C}$ ali $\mathcal{D}$ in so dokazljivo zunaj $\mathcal{M}^\#$. To pomeni, da prvič nudimo dokaze o neskončnih razredih vektorskih ukrivljenih funkcij, ki imajo tako posebno lastnost. V tem kontekstu je problem določanja vektorskih funkcij, ki so strogo izven znanih primarnih razredov, precej delikaten, kot tudi vprašanje, ali je te funkcije mogoče razširiti na največjo izhodno ukrivljeno dimenzijo (ki ima vrednost n za vhodni prostor velikosti $2n$). V tej smeri nudimo način za konstruiranje vektorskih upognjenih funkcij, ki so močno zunaj $\mathcal{M}^\#$, za različne izhodne dimenzije.

V Poglavju 6 bomo tudi združili pojem šibko zunaj razreda $\mathcal{M}^\#$ in pojem vektorskih ukrivljenih-negaukrivljenih funkcij, predstavljenih v Poglavju 5. Da bi zagotovili več družin vektorskih ukrivljenih-negaukrivljenih funkcij, ki imajo komponente zunaj $\mathcal{M}$, uporabimo vektorske prostore popolnih preslikav oblike $F(x) = x^d + b_1 a_1 x + \cdots + b_1 a_t x$, kjer je F permutacija nad $\mathbb{F}_{2^n}$ za množico linearno neodvisnih elementov $a_1, \ldots, a_t \in \mathbb{F}_2^n$ in za poljubno izbiro binarnih koeficientov $b_i \in \mathbb{F}_2$. Upoštevajmo, da, ko je $1 \in \langle a_1, \ldots, a_t \rangle$, je F tudi standardna popolna preslikava, saj sta tako $F(x)$ kot $F(x)+x$ permutaciji nad $\mathbb{F}_{2^n}$. Kljub temu ni nujno, da je funkcija F permutacija in ta primer je obravnavan ločeno. Namreč, z uporabo primerne dekompozicije vektorskega prostora (in alternativne identificiranje ustreznih podpolj) nudimo splošno metodo določanja vektorskih prostorov popolnih preslikav, ki se nato učinkovito uporabijo za določanje vektorskih ukrivljenih negaukrivljenih funkcij (katerih dimenzija ni maksimalna), kjer približno polovica komponentnih funkcij leži zunaj popolnega razreda $\mathcal{M}$.

V Poglavju 7 bomo raziskali še eno kriptografsko pomembno lastnost Boolovih funkcij, imenovano korelacijsko imunost. Boolova funkcija na n-spremenljivkah f se imenuje korelacijsko imuna reda d (na kratko, d-CI), če se izhodna porazdelitev funkcije f ne spremeni, ko fiksiramo največ d vhodnih spremenljivk. Za kriptografske aplikacije je pojem korelacijske imunosti običajno povezan s tako imenovanim modelom nelinearnega združevalnika (linear combiner) kot predstavnikom določene družine pretočnih šifer [46]. Ta lastnost je ključnega pomena, da lahko model prenese korelacijske napade [30, 31, 45, 68]. Najpogosteje se kot kriptografsko merilo uporablja tesno povezan pojem odpornosti (resiliency), ki poleg določenega vrstnega reda CI kombinirane Boolove funkcije zahteva tudi njeno uravnoteženost. Poleg tega je podrazred funkcij CI z minimalno težo je v zadnjem času prejel veliko pozornosti tudi zaradi njihove uporabe kot maskirnih primitivov za namen zaščite strojne opreme nekaterih šifrirnih družin [4], glej tudi [16]. Poleg tega so funkcije CI tesno povezane s shemami delitve skrivnosti in kodami za odpravljanje napak [6, 23, 26].

Prvo karakterizacijo funkcij CI v smislu njihove še možne algebraične stopnje je podal T. Siegenthaler [67]. Pokazali bomo, da je z uporabo določenih rezultatov, vezanih na deljivosti uteži, povezanih z omejitvami funkcij CI (prevzetih iz [73]),

mogoče izpeljati kompakten dokaz Siegenthalerjeve meje algebraične stopnje. Poleg tega natančno določimo težo CI funkcij d-tega reda, kjer so (vsi) členi stopnje $n-d$ v svoji algebraični normalni obliki. Z uporabo istih rezultatov deljivosti bomo tudi natančno določili Walsheve spektralne vrednosti vektorjev teže $d+1$ za CI Boolove funkcije d-tega reda.

Predstavljeni bosta dve učinkoviti konstrukciji funkcij CI, ki sta primerni za načrtovanje podrazreda z minimalno težo. Takšne funkcije imajo takojšnjo uporabo kot maskirne sheme za zaščito šifer pred kriptanalizo stranskih kanalov [16]. Kot je navedeno v [15], morajo za učinkovito strojno implementacijo CI funkcije imeti čim manjšo težo in večina poznanih konstrukcij (primarne konstrukcije, kot je konstrukcija Maiorana-McFarland, in sekundarne konstrukcije, kot je posredna vsota itd., glejte na primer [12], [24]) ne dovoljujejo gradnje funkcij s tako lastnostjo. To je sprožilo precej obsežne raziskave v tej smeri. Natančneje, za razmeroma nizko velikost vhodnega prostora (za $n \leq 13$) je bila določena minimalna teža CI funkcij in z nekaj pomanjkljivostmi podrobno opisana, glej [16] in nadaljnje delo Q. Wang in Y. Li [78]. Po notaciji, ki sta ga uvedla C. Carlet in X. Chen, označujemo najmanjšo težo katere koli funkcije CI d-tega reda z $\omega_{n,d}$. Vrednosti $\omega_{12,4}$, $\omega_{13,4}$ in $\omega_{13,5}$ so bila določene v [78]. Za poseben primer funkcij 3-CI sta C. Carlet in X. Chen domnevala, da je $w_{n,3} = 8\lceil \frac{n}{4} \rceil$ za katero koli celo število $n \geq 3$. S konstrukcijo je bilo pokazano, da domneva velja za $n = 2^k$. Kasneje se je pokazalo [76], da je ta domneva enakovredna Hadamardovi domnevi, ki trdi, da obstaja Hadamardova matrika reda $4k$ za vsako pozitivno celo število k. Upoštevajmo, da primer, ko je $n = 2^k$, potem ustreza Silvester-Hadamardovim matrikam, ki uporabljajo to enakovrednost. Predložimo dodatne dokaze, da je domneva C. Carleta in X. Chena resnična s posplošeno metodo načrtovanja CI-funkcij. Natančneje, skozi obstoj 3-CI funkcij minimalne teže se bo pokazalo, da domneva velja za kateri koli n oblike $n = 2^k - i$ ali $n = 3 \cdot 2^k - i$, za $i = 0, 1, 2, 3$ in $k \geq 3$.

R. O'Donnell je v zbirki odprtih problemov na področju analize Boolovih funkcij [52] navedel domnevo o rasti vsote linearnih Fourierovih koeficientov, ki jo motivirajo nekateri problemi pri družbeni izbiri. V delu [52] so bile raziskane funkcije $f : \{-1,1\}^n \to \{-1,1\}$, zato je v [52] domneva navedena kot domneva o funkcijah $f : \{-1,1\}^n \to \{-1,1\}$. V [77] je Q. Wang prevedel O'Donnellovo domnevo v enakovredno domnevo o razredu odpornih Boolovih funkcij $f : \{0,1\}^n \to \{0,1\}$ in tako podal alternativni vidik O'Donnellove domneve. V tej obliki domneva navaja, da, če je $g : \{0,1\}^n \to \{0,1\}$ $(n-d-1)$-odporna Boolova funkcija, potem

$$\sum_{\substack{v \in \{0,1\}^n \\ \mathrm{wt}(v) = n-1}} W_g(v) \leq d \binom{d-1}{\lfloor \frac{d-1}{2} \rfloor} 2^{n+1-d},$$

kjer je $W_g(v)$ Walshev koeficient g v točki $v \in \mathbb{F}_2^n$, ki je podan kot

$$W_g(v) = \sum_{x \in \mathbb{F}_2^n} (-1)^{g(x)+v \cdot x}.$$

To alternativno formulacijo je uporabil Q. Wang [77], v dokazu, da je domneva resnična, ko je $d = 1$ in $d = n-1$.

V Poglavju 8 bomo uporabili Wangov pristop z uporabo standardnega Boolovega okolja. Najprej bomo pokazali zanimivo kombinatorično lastnost, povezano z domnevo, ki pomeni, da je (za fiksen d) zgornja meja odvisna le od končno mnogo celih števil n. Natančneje, pokažemo, da, če je domneva pravilna za vse $n \leq 2^{2d-2}$, potem velja za vse $n \in \mathbb{N}$. Nato bomo dokazali, ponovno za fiksen d, da, če domneva ne velja za nekatere n_0, potem je napačna za vsak $n > n_0$. Ta dva rezultata pomenita, da za fiksen d, če je domneva resnična za $n = 2^{2d-2}$, potem je pravilna za vsak $n \in \mathbb{N}$. Zato je takojšnja posledica, da domneva velja za $d = 2$, saj jo je mogoče enostavno izčrpno preveriti za $n = 4$. Kljub temu bo neposreden dokaz tega dejstva zagotovljen z uporabo karakterizacije $(n-3)$-odpornih funkcij, podanih v [8]. Nato bomo za $d = 3$ združili rezultate o karakterizacijah $(n-4)$-odpornih funkcij, podanih v [13] in [7], in pokazali, da je dovolj, da preverimo domnevo za $n = 6$ in v nekaterih posebnih primerih za $n = 7$. Da bi dokazali, da je domneva resnična za $d = 3$, bomo pri obravnavanju omenjenih primerov uporabili celoštevilsko programiranje.

Ko pa je $d = 4$, bomo identificirali 2-odporno Boolovo funkcijo na 7 spremenljivkah, ki krši domnevo. To pomeni, da domneva v splošnem ne drži. Natančneje, domneva ni resnična, ko je $n \geq 7$, kar pomeni, da $(n-5)$-odporne Boolove funkcije ne izpolnjujejo nujno omejitve v domnevi.

Na koncu bomo diplomsko nalogo zaključili s povzetkom najpomembnejših rezultatov, predstavljenih v diplomski nalogi, ter nakazali nekaj možnih problemov in usmeritev za prihodnje raziskave.

Rezultati doktorske disertacije so objavljeni v sledečih člankih:

- S. Kudin, E. Pasalic. A complete characterization of $\mathcal{D}_0 \cap \mathcal{M}^{\#}$ and a general framework for specifying bent functions in $\mathcal{C}$ outside $\mathcal{M}^{\#}$. *Designs, Codes and Cryptography*, vol. 90(8), pp. 1783–1796, (2022).

- S. Kudin, E. Pasalic, N. Cepak, F. Zhang. Permutations without linear structures inducing bent functions outside the completed Maiorana-McFarland class. *Cryptography and Communications*, vol. 14(1), pp. 101–116, (2022).

- E. Pasalic, S. Kudin, A. Polujan, A. Pott. Vectorial bent-negabent functions – their constructions and bounds. *IEEE Transactions on Information Theory*, doi: 10.1109/TIT.2022.3226571, (2022).

- E. Pasalic, F. Zhang, S. Kudin, Y. Wei. Vectorial bent functions weakly/strongly outside the completed Maiorana–McFarland class. *Discrete Applied Mathematics*, vol. 294, pp. 138–151, (2021).

- S. Kudin, E. Pasalic. Efficient design methods of low-weight correlation-immune functions and revisiting their basic characterization. *Discrete Applied Mathematics*, vol. 284, pp. 150–157, (2020).

- S. Kudin, E. Pasalic. Proving the conjecture of O'Donnell in certain cases and disproving its general validity. *Discrete Applied Mathematics*, vol. 289, pp. 345–353, (2021).

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.

Sadmir Kudin