UNIVERZA NA PRIMORSKEM

FAKULTETA ZA MATEMATIKO, NARAVOSLOVJE IN INFORMACIJSKE TEHNOLOGIJE

DOKTORSKA DISERTACIJA

(DOCTORAL THESIS)

KONSTRUKCIJE NOVIH SUPERRAZREDOV UKRIVLJENIH FUNKCIJ IN NADALJNJE KONSTRUKCIJE KRIPTOGRAFSKO POMEMBNIH PRESLIKAV IZVEN $\mathcal{M}^{\#}$

(CONSTRUCTING NEW SUPERCLASSES OF BENT FUNCTIONS AND FURTHER CONSTRUCTIONS OF CRYPTOGRAPHICALLY SIGNIFICANT MAPPINGS OUTSIDE $\mathcal{M}^{\#}$)

AMAR BAPIĆ

KOPER, 2022

UNIVERZA NA PRIMORSKEM

FAKULTETA ZA MATEMATIKO, NARAVOSLOVJE IN INFORMACIJSKE TEHNOLOGIJE

DOKTORSKA DISERTACIJA

(DOCTORAL THESIS)

KONSTRUKCIJE NOVIH SUPERRAZREDOV UKRIVLJENIH FUNKCIJ IN NADALJNJE KONSTRUKCIJE KRIPTOGRAFSKO POMEMBNIH PRESLIKAV IZVEN $\mathcal{M}^{\#}$

(CONSTRUCTING NEW SUPERCLASSES OF BENT FUNCTIONS AND FURTHER CONSTRUCTIONS OF CRYPTOGRAPHICALLY SIGNIFICANT MAPPINGS OUTSIDE $\mathcal{M}^{\#}$)

AMAR BAPIĆ

KOPER, 2022

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

Mojoj porodici

Acknowledgements

I would like to express my gratitude to my mentor Prof. Enes Pasalic for his guidance and support throughout this journey. To the UP Crypto Group - Samir, Nastja, Rene and Sadmir, thank you for your continuous help and guidance. I am equally grateful to the Department of Mathematics, administrative units and colleagues at UP IAM/FAMNIT, especially our dean Dr. Ademir Hujdurović and rector Prof. Klavdija Kutnar.

Posebnu zahvalnost osjećam prema svojoj majci i sestri, Hati i Ilmi, čija je ljubav i podrška neizmjerljiva. Mom rahmetli babi Ibrahimu, koji je bio veliki oslonac i, vjerujem, oduvijek znao da ću doći do ovog cilja. Mojoj rahmetli profesorici Senki, zbog koje sam se zaljubio u matematiku.

Na kraju, moram izraziti zahvalnost svim nevjerovatnim prijateljima, koje sam stekao tokom decenije studiranja.

Hvala Sanji i Tanji na svakodnevnom druženju, smijehu i pomoći tokom radnog dana.

Mojim dajcikama Amri B., Amri S., Merjem i Dženani u Tuzli, te lemurima Boki, Kreši, Niniju, Đukici i Ingici u Kopru. Hvala vam za sve što ste učinili za mene. Hvala vam što ste mi bili motivacija i podrška, kada mi je ona bila potrebna.

Amar Bapić

Abstract

CONSTRUCTING NEW SUPERCLASSES OF BENT FUNCTIONS AND FURTHER CONSTRUCTIONS OF CRYPTOGRAPHICALLY SIGNIFICANT MAPPINGS OUTSIDE $\mathcal{M}^{\#}$

This thesis introduces results which lead to new secondary constructions of (vectorial) bent functions outside the completed Maiorana-McFarland class $\mathcal{M}^{\#}$. It consists of roughly three parts.

The first part considers a new construction method for vectorial bent functions via the so-called (P_U) property, which is obtained as a generalization of the construction methods provided by Tang *et al.* [82] and Zheng *et al.* [90]. We extend the number of infinite families of vectorial bent functions and provide a modification of the mentioned construction to obtain instances of vectorial Boolean functions with maximal number of bent components. The same method was further extended to the p-ary case to obtain instances of p-ary weakly regular bent and plateaued (n, m)-functions, where p is an odd prime. We also showed that the (P_U) property can be characterized via second-order derivatives, as it was done in [90] for the binary case.

The second part addresses the construction of two new superclasses of bent functions $\mathcal{SC}$ (superclass of $\mathcal{C}$ and $\mathcal{D}_0$) and $\mathcal{CD}$ (superclass of $\mathcal{C}$ and $\mathcal{D}$), and their applications in the design of related combinatorial objects. We provide sufficient conditions for which these functions are outside $\mathcal{M}^{\#}$. Furthermore, we obtain new instances of bent (n, k)-functions weakly/almost strongly/strongly outside $\mathcal{M}^{\#}$. Unfortunately the output dimension is not maximal ($k < n/2$), however our instances provide the largest known output dimensions in the literature. We also used the notion of these classes to characterize (n, m)-functions with maximal number of bent components outside $\mathcal{M}^{\#}$, where $m > n/2$, and for $n = 6$ we give a complete characterization. We also obtained new instances of bent 4-decompositions via the $\mathcal{SC}$ and $\mathcal{CD}$ classes.

The third part addresses some known secondary constructions of bent functionsc, like the direct and indirect sum as well as 4-decompositions.

We provide conditions for which these construction methods yield bent functions outside $\mathcal{M}^{\#}$. We also construct several classes of (homogeneous) cubic bent functions (without affine derivatives) outside $\mathcal{M}^{\#}$ and show that one of the obtained classes is non-decomposable (inseperable).

Math. Subj. Class. (2020): 94A60, 06E30, 11T71

Keywords: (vecotorial) bent functions, class inclusion, complete Maiorana-McFaralnd class, MNBC functions, secondary constructions, weakly/almost strongly/strongly outside $\mathcal{M}^{\#}$, 4-decomposition, (P_U) property, $\mathcal{SC}$ and $\mathcal{CD}$ class, direct and indirect sum

Povzetek

KONSTRUKCIJE NOVIH SUPERRAZREDOV UKRIVLJENIH FUNKCIJ IN NADALJNJE KONSTRUKCIJE KRIPTOGRAFSKO POMEMBNIH PRESLIKAV IZVEN $\mathcal{M}^{\#}$

Doktorska disertacija predstavlja rezultate, ki vodijo do novih sekundarnih konstrukcij (vektorskih) ukrivljenih funkcij izven poplnega Maiorana-McFarland razreda $\mathcal{M}^{\#}$. Sestavljena je iz okvirno treh delov.

V prvem delu doktorske disertacije obravnavamo novo metodo konstrukcije vektorskih ukrivljenih funkcij z uporabo tako imenovane (P_U) lastnosti, ki je pridobljena kot posplošitev konstrukcijskih metod, ki sta jih uvedla Tang *et al.* [82] in Zheng *et al.* [90]. V tem delu razširimo množico neskončnih družin vektorskih ukrivljenih funkcij in modificiramo omenjeno konstrukcijo, da dobimo primere vektorskih Boolovih funkcij z največjim številom ukrivljenih komponent. Isto metodo razširimo na problem p-arnih funkcij (p je liho praštevilo), kjer dobimo primere p-arnih šibko regularnih ukrivljenih in platojskih (n, m)-funkcij. Pokažemo tudi, da je mogoče (P_U) lastnost karakterizirati z odvodi drugega reda, podobno kot je bilo za binarni primer storjeno v [90].

V drugem delu doktorske disertacije obravnavamo konstrukcijo dveh novih superrazredov ukrivljenih funkcij $\mathcal{SC}$ (superrazred razredov $\mathcal{C}$ in $\mathcal{D}_0$) in $\mathcal{CD}$ (superrazred razredov $\mathcal{C}$ in $\mathcal{D}$) ter njune uporabe pri načrtovanju njima sorodnih kombinatoričnih objektov. Zagotovimo tudi zadostne pogoje, pod katerimi ležijo te funkcije izven razreda $\mathcal{M}^{\#}$. Poleg tega predstavimo nove primere ukrivljenih (n, k)-funkcij šibko/skoraj močno/močno izven $\mathcal{M}^{\#}$. Žal izhodna dimenzija ni največja ($k < n/2$), vendar naši primeri zagotavljajo največje znane izhodne dimenzije v literaturi. Pojem teh razredov uporabimo tudi za karakterizacijo (n, m)-funkcij z največjim številom ukrivljenih komponent izven razreda $\mathcal{M}^{\#}$, kjer je $m > n/2$. V posebnem primeru, kjer je $n = 6$, podamo tudi popolno karakterizacijo. Preko razredov $\mathcal{SC}$ in $\mathcal{CD}$ pridobimo tudi nove primere ukrivljenih 4-dekompozicij.

Tretji del doktorske disertacije je obravnava določenih znanih sekun-

darnih konstrukcij ukrivljenih funkcij, kot sta neposredna in posredna vsota ter 4-dekompozicije. V tem delu podamo pogoje, pri katerih te konstrukcije generirajo ukrivljene funkcije izven razreda $\mathcal{M}^{\#}$. Konstruiramo tudi več razredov (homogenih) kubičnih ukrivljenih funkcij (brez afinih odvodov) izven $\mathcal{M}^{\#}$ in pokažemo, da je en izmed pridobljenih razredov nerazgradljiv (neločljiv).

Math. Subj. Class. (2020): 94A60, 06E30, 11T71

Ključne besede: (vektorske) ukrivljene funkcije, vključitev razreda, popoln Maiorana-McFaralnd razred, MNBC funkcije, sekundarne konstrukcije, šibko/skoraj močno/močno izven $\mathcal{M}^{\#}$, 4-dekompozicija, (P_U) lastnost, razreda $\mathcal{SC}$ in $\mathcal{CD}$, neposredna in posredna vsota

Contents

List of Figures **xv**

List of Tables **xvii**

1 Introduction **1**

2 Preliminary concepts **9**
2.1 Boolean functions 10
2.2 Bent functions 12
2.2.1 Classes of bent functions 14
2.3 Vectorial Boolean (bent) functions 17
2.4 p-ary functions 20

3 Secondary constructions of vectorial bent functions via the (P_U) property **22**
3.1 Generic construction of vectorial bent functions 23
3.2 New infinite families of vectorial bent functions 27
3.3 New families of (n, n)-functions with maximal number of bent components 32

4 Secondary constructions of vectorial p-ary weakly regular bent functions via the (P_U) property **34**
4.1 Generic construction of vectorial p-ary bent functions . . 34
4.2 New infinite families of vectorial p-ary weakly regular bent functions 38
4.2.1 Observations on monomial p-ary weakly regular bent functions 38
4.2.2 New infinite families of vectorial p-ary weakly regular bent functions from the p-ary Maiorana-McFarland class 40

5 Two new superclasses of bent functions $\mathcal{SC}$ and $\mathcal{CD}$ **43**
5.1 Bentness of Boolean functions in the class $\mathcal{SC}$ 43
5.1.1 On EA-equivalence between $\mathcal{D}_0$ and $\mathcal{SC}$ class . . . 48
5.2 Bentness of Boolean functions in the class $\mathcal{SD}$ 49
5.3 Bentness of Boolean functions in the class $\mathcal{CD}$ 51

5.3.1 Sufficient conditions for functions in $\mathcal{CD}$ to be outside $\mathcal{M}^{\#}$ 54
5.3.2 Addressing the normality of functions in $\mathcal{CD}$ . . . 60
5.4 Bent duals of functions in $\mathcal{C}, \mathcal{D}, \mathcal{SC}$ and $\mathcal{CD}$ 62
5.4.1 Bent duals of certain functions in $\mathcal{C}$ and $\mathcal{D}$ 62
5.4.2 Duals of bent functions in $\mathcal{SC}$ and $\mathcal{CD}$ 67

6 Applications of the classes $\mathcal{SC}$ and $\mathcal{CD}$ for the construction of other cryptographically significant mappings 69
6.1 Vectorial bent functions weakly/almost strongly/strongly outside $\mathcal{M}^{\#}$ 69
6.1.1 New families of (vectorial) bent functions weakly/almost strongly outside $\mathcal{M}^{\#}$ 69
6.1.2 New families of vectorial bent functions strongly outside $\mathcal{M}^{\#}$ 78
6.2 Vectorial Boolean functions with the maximum number of bent components outside $\mathcal{M}^{\#}$ 82
6.2.1 Complete classification of MNBC functions in six variables 83
6.2.2 MNBC functions from the $\mathcal{PS}_{ap}$ class 87
6.2.3 MNBC functions from secondary constructions of Boolean bent functions 88
6.2.4 A family of t-step extension MNBC functions . . 93

7 Explicit infinite families of 4-decompositions outside $\mathcal{M}^{\#}$ 98
7.1 Preliminary results on the spectral design 98
7.1.1 Specifying 5-valued spectra functions through duals 98
7.1.2 Decomposition of bent functions 99
7.2 Decomposing bent functions - design methods 101
7.2.1 An algorithm for determining whether $f \in \mathcal{M}^{\#}$. 101
7.2.2 Defining suitable bent 4-decompositions 102
7.2.3 Constructing bent 4-decompositions using $\mathcal{SC}$ and $\mathcal{CD}$ 105
7.2.4 Semi-bent case of 4-decomposition 108
7.2.5 Four bent decomposition in terms of 5-valued spectra functions 114
7.3 5-valued spectra functions from the generalized $\mathcal{M}$ class 119

8 Applications of the indirect sum in the design of several special classes of bent functions outside $\mathcal{M}^{\#}$ 123
8.1 Direct and indirect sum methods 123
8.1.1 Specifying sufficient conditions for the direct sum method 124
8.1.2 Indirect sum method giving rise to bent functions outside $\mathcal{M}^{\#}$ 127
8.2 Design methods for homogenous bent functions 134
8.2.1 Homogenous bent functions using the indirect sum 134

8.2.2 Non-decomposability of our bent functions 138
8.2.3 Another method of specifying (non-decomposable) cubic bent functions 141
8.3 Vectorial bent functions strongly outside $\mathcal{M}^{\#}$ 143
8.3.1 A generic construction using companion matrices 145

9 Conclusions **147**

Bibliography **149**

Index **157**

Appendix **158**

Povzetek v slovenskem jeziku **168**

List of Figures

1.1 Scheme of a classic cryptosystem 2
1.2 Example of a block cipher 2
1.3 Example of a stream cipher 2

6.1 The structure of CCZ-equivalence classes of $(6, m)$-MNBC functions. If an equivalence class i is extendable to an equivalence class j, we put a directed edge between them. The equivalence classes denoted by gray are inside $\mathcal{M}^{\#}$ and by red are outside $\mathcal{M}^{\#}$. 86

9.1 Shema klasičnega kriptosistema 168
9.2 Primer bločne šifre 169
9.3 Primer tokovne šifre 169

List of Tables

5.1 Class inclusion in $\mathcal{M}^{\#}$ of the Boolean function f defined by (5.15) 58

6.1 Behaviour of the function ψ_λ for $\lambda \in \mathbb{F}_{2^3}^*$ 81

8.1 Comparison of bounds for the dimension n obtained in [71] with our results. The entry denoted 18^* is the correct value instead of 16 stated in [71]. 143

Chapter 1

Introduction

People's desire of wanting to keep some information confidential in physical form marks the beginning of *cryptography* - the discipline that by today's definition enables two parties to securely communicate via an insecure channel. Naturally, wanting to keep something secret will not work for everyone, who would like to know what lies behind this secrecy. This resulted in the development of *cryptanalysis* - the science of breaking ciphers and revealing the original message. Together, cryptography and cryptanalysis form the field of *cryptology*, whose study and importance has grown exponentially with the development of modern science as we know it today.

At first, before the modern era, the main purpose of cryptography was to ensure secrecy in communications related to war and diplomatic affairs, whilst in recent decades the field has expanded beyond confidentiality to the concerns of checking message integrity, sender/receiver identity authentication, digital signatures, interactive proofs, and secure computation, among others. The information we want to send has to travel through insecure channels via some servers over which we have no control, but despite that, we want the information to remain private.

A key objective of cryptography is to enable two parties, usually referred to as Alice (sender) and Bob (reciever) to communicate safely over an insecure channel. This means that no third party, known as the *adversary*, usually referred to as Eve, is not able to derive any information about the plaintext from the observed ciphertext. The message they want to exchange is called *plaintext* and the message they send through the channel is called *ciphertext*. Alice *encrypts* the plaintext m and obtains the ciphertext c via some encryption key K_E. The ciphertext is then transmitted to Bob, who uses a decryption process together with the ciphertext and decryption key K_D to obtain the original message. A classic example of such a cryptosystem is depicted in Figure 1.1. If both the encryption and decryption key are the same ($K_E = K_D$), we are talking about *symmetric-key crpytography*. On the other hand, if the encryption key is public, in other words, if everyone is able to send Bob a ciphered message which only he can decipher using his secret decryption

key, we are talking about *public-key cryptography*. The main advantage of symmetric-key cryptography over public-key cryptography is that it is fast and efficient for large amounts of data. On the other hand, public-key cryptography can be used not only for safe communication but also for authentication with digital signatures.

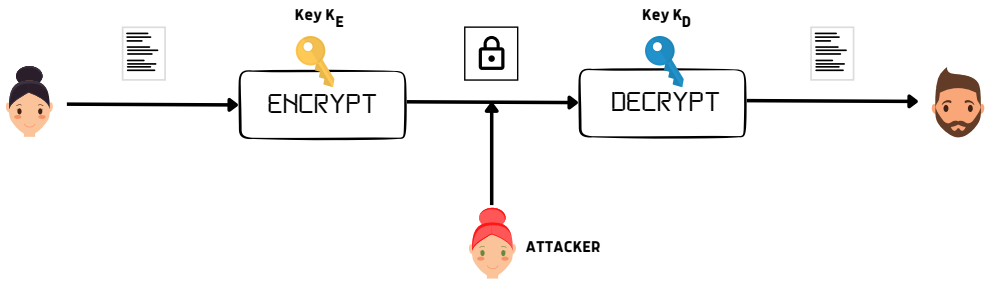

Figure 1.1: Scheme of a classic cryptosystem

When simulating attacks on cryptosystems, it is assumed that Eve knows both encryption and decryption algorithms. That is, the security of a cryptographic system should not rely on the secrecy of the algorithms and methods but only on the secrecy of the keys. These principles were stated by A. Kerckhoffs in [42].

We will focus mainly on symmetric cryptography, as the topics in the thesis adress properties of cryptographic primitives related to it. Symmetric-key cryptography contains two large families of cryptographic primitives, namely, *block ciphers* (Figure 1.2) and *stream ciphers* (Figure 1.3).

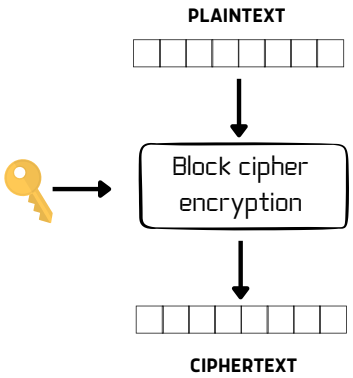

Figure 1.2: Example of a block cipher

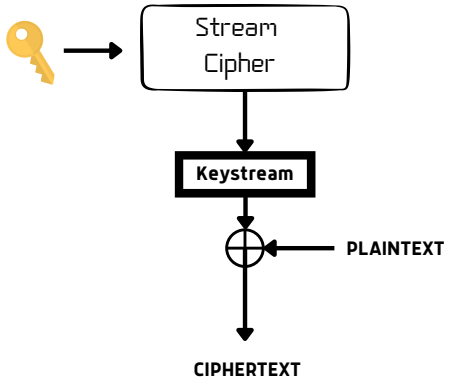

Figure 1.3: Example of a stream cipher

Stream ciphers generate a pseudorandom sequence (appears to be statistically random, despite having been produced by a completely deter-

ministic and repeatable process) of bits, called *keystream*, that is usually XOR-ed (added modulo two) to the plaintext to obtain the ciphertext. Some of the well-known encryption algorithms that belong to the family of stream ciphers include SEAL [76], SNOW [34], ISAAC [40], Trivium [26], and Grain [35].

On the other hand, the general idea in the design of block ciphers is to divide the plaintext into *blocks* (of length 2^k, usually it equals 64, 128 or 256) and encrypt each block individually, thus obtaining a cipher comprised of ciphertext blocks. Two popular structures used within the design block are *Feistel-based* or alternatively a *substitution-permutation network*. Modern designs of block cipher employ an iterative application of several identical rounds to produce a cipher text block. A key aspect is that these rounds implement the concept of *confusion* and *diffusion*, which were introduced by C. E. Shannon in his classified report [80]. The role of confusion is that each bit of the ciphertext should depend on the plaintext and secret key in a very complicated manner. On the other hand, diffusion can be roughly interpreted as the property that the ciphertext bits, after applying one encryption round, depend on many input bits. In other words, the change of one single bit in the plaintext should result in the change of roughly half of the bits in the ciphertext.

In the substitution-permutation network (SPN) we note two notions: S-box and P-box. The *substitution box* (S-box) employs Shannon's principle of confusion and substitutes a small block of input bits by another block of bits. In general it is a mapping that maps n bits to m bits, where n is not necessarily the same as m. For example, the S-box used in DES (see below) mapped 6-bit inputs to 4-bit outputs. Another component in the SPN is the so-called *permutation box* (P-box), which takes the outputs of all S-boxes and permutes them. In principle, the P-box employs Shannon's principle of diffusion.

One of the first block cipher is considered to be Lucifer, developed at IBM in the 1970s based on work done by Horst Feistel. Later, a revised version of Lucifer was adapted as a US government FIPS (Federal Information Processing Standard) standard, which was called the Data Encryption Standard (DES, which was publicly released in 1976 and has been widely used by both governmental and private organisations.

As soon as the specifications of DES were made public, the cipher became the subject of controversy. Doubts about the security of DES arose from the fact that Lucifer's original 128-bit secret key had been reduced to 56 bits, and also that the design principles of its substitution and permutation tables were never made public.

In 1992, Matsui introduced the concept of linear cryptanalysis [54] and applied it to DES. A few years later, the DESCHALL project publicly broke a DES enciphered message. It became clear that due to the small keylength of DES, it was susceptible to brute force attacks and hence, a new encryption standard had to be chosen. DES has been superseded as a United States Federal Standard by the *Advanced Encryption Stan-*

dard (AES), adopted by National Institute of Standards and Technology (NIST) in 2001 after a 5-year public competition. It was developed by Joan Daemen and Vincent Rijmen, and submitted to the competition under the name *Rijndael* [25]. Some other well-known block ciphers are for instance IDEA [47], Blowfish [78], RC5 [75], PRESENT [9], to name a few.

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

- ⋆ In the weakest *ciphertext-only* scenario, the attacker only has access to several ciphertext that were generated by a targeted block cipher using the unknown secret symmetric key. Their goal is then either to recover parts (or entire) plaintexts or alternatively to recover (a portion of) the secret key. This type of scenario is the most practical, but on the other hand the cryptanalysis is hardest to perform.
- ⋆ In the case of *known-plaintext* scenario, the attacker has at his disposal many plaintext/ciphertext pairs and his goal is to deduce (a portion of) the secret key.
- ⋆ The *chosen-plaintext* scenario is similar to the known-plaintext attack with the difference that the attacker has the access to the encryption device and can encrypt any messages (plaintexts) of his choice. The goal is, again, to recover the secret key or a portion of it.
- ⋆ The *chosen-ciphertext* scenario is similar to the latter scenario though the attacker decrypts the ciphertexts of his choice thus obtaining the corresponding plaintexts.

In order to ensure high security, the functions in block ciphers have to satisfy various conditions/properties. In what follows we will mainly address the security of S-boxes, which can be viewed as a collection of mappings from $\mathbb{F}_2^n \to \mathbb{F}_2$, known as *Boolean functions*. Here, with $\mathbb{F}_2^n$, we denote the n-dimensional vector space over $\mathbb{F}_2 = \{0, 1\}$. As mentioned earlier, Matsui developed the notion of linear cryptanalysis which breaks the full 16-round DES cipher with 2^{47} plaintext/ciphertext pairs.

To ensure high enough protection against these types of attacks the notion of *nonlinearity* was introduced (cf. Chapter 2). Boolean functions which are at the maximal possible distance to the set of all affine functions (mappings $l_a : \mathbb{F}_2^n \to \mathbb{F}_2$ defined by $l_a(x) = a \cdot x \oplus b$, $a \in \mathbb{F}_2^n$, $b \in \mathbb{F}_2$) have the highest nonlinearity and are called *bent functions*, a term introduced by O. Rothaus in 1976 [77]. Aside from high nonlinearity, other cryptographically important properties of a Boolean functions are connected with the notion of balancedness, strict avalanche criterion and propagation criterion, algebraic degree, correlation immunity, to name a few. For more details on these properties we refer the reader to the books [19, 24]. Throughout the thesis, the notion of nonlinearity and

bent functions will be of main interest for us.

In the last fifty years, a lot of research was done on bent functions and their applications. In coding theory, the task of determining the so-called covering radius for the Reed-Muller code $RM(r, n)$ of order 1 is equivalent to the task of finding certain bent functions [41, 50]. Some special instances of quadratic bent functions can be used to construct Kerdock codes [43] that are optimal and have large code distances, which grow with the code lengths [27, 81]. The problem of constructing *Hadamard matrices* is a well-known combinatorial problem, which remains unsolved since 1893. If the matrix size is $N = 2^n$ (n is even), then this problem can be transformed (with some restrictions) to the task of constructing bent functions in n variables [77]. Bent functions can also be characterized via *strongly regular graphs* with parameters (v, k, λ, μ). This means that the graph contains v vertices each of degree k and for any vertices a and b the number of vertices incident to a and b simultaneously is equal to λ or μ, which depends on the presence or absence of the edge between a and b, respectively. In [8] it was shown that a Boolean function f is bent if and only if its Cayley graph G_f is strongly regular and $\lambda = \mu$. Bent functions have also been studies because of their connection with difference sets. Let $(G, +)$ be an Abelian group of order v. A subset $D \subseteq G$ of size k is called a *difference set* with parameters (v, k, λ) if every nonzero $g \in G$ can be represented as $g = b - d$ in exactly λ ways, where $b, d \in D$. In [28] it was proved that a Boolean function f in n variables is bent if and only if the set $D = \{(x, f(x)) : x \in \mathbb{F}_2^n\}$ is a difference set with parameters $(2^{n+1}, 2^n, 2^{n-1})$ in the additive group $\mathbb{Z}_2^{n+1}$. Although they seem like a perfect choice for secure cryptographical mappings, their main cryptographic drawback is that they are not balanced. However, even though they cannot be used directly, bent functions can be modified to obtain new functions which still have high nonlinearity and are applicable in the construction of block and stream ciphers. For example, the ciphers CAST [1] and Grain [35] as well as the hash function HAVAL [93] use certain modifications of bent functions in their construction. For more details on bent functions we refer to the books of Carlet, Sihem and Tokareva [19, 59, 83] and to the paper of Zhang and Pasalic [87].

Although a lot of research in the field of bent function has been done, there are still a lot of open problems. Among those, we note the problem of determining the number of bent functions for a fixed number of variables, their design and characterization. The construction methods of vectorial bent functions can be divided into two classes: *primary* and *secondary*, referring respectively to the designs that build these functions form scratch and alternatively using the known ones, respectively.

When considering classes of bent functions, there are two primary classes referred to as partial spread ($\mathcal{PS}$) class due to Dillon [29] and the Maiorana-McFarland ($\mathcal{M}$) class [55]. The term primary refers to the design that does not employ known bent functions to generate new ones (giving rise to the so-called secondary methods), it rather uses a suitable

set of affine functions (typical for the Maiorana-McFarland method [55]) or a collection of disjoint $n/2$-dimensional subspaces to construct a bent function on $\mathbb{F}_2^n$ (typical for the partial spread class introduced by Dillon [29]). Another generic class, denoted by $\mathcal{N}$, was proposed by Dobbertin [30] and it includes both $\mathcal{M}$ and a subclass of $\mathcal{PS}$ commonly denoted $\mathcal{PS}_{ap}$. A non-exhaustive list of various secondary constructions can be found in the following works [17, 18, 22, 37, 57, 92]. In 1993, Carlet [17], motivated by the results of Dillon, introduced two secondary classes of bent functions, which will be of great interest throughout the thesis, denoted by $\mathcal{C}$ and $\mathcal{D}$, which are derived through a suitable modification of bent functions in the $\mathcal{M}$ class. The main problem with the secondary constructions is the difficulty to answer the question about the classification of such generated bent functions. More precisely, it may happen that some of these secondary constructions simply generate bent functions which belong to the known primary classes of bent functions in which case only their explicit representation is of importance. Nevertheless, showing the non-inclusion into the completed primary classes (for the definition of a completed class see Definition 2.2.3) is usually a hard task, especially in the case of the so-called $\mathcal{PS}$ class due to the lack of efficient indicators. Essentially, the problem can be reduced to identifying cliques in a graph, which is known to be NP-hard [88]. In the case of the completed $\mathcal{M}$ class such an indicator exists (cf. Lemma 2.2.4), however it becomes computationally inefficient for $n \geq 14$ (cf. Section 7.2.1).

An explicit subclass of $\mathcal{D}$, named $\mathcal{D}_0$, was introduced by Carlet in [17] and its cardinality is of approximately the same size as of $\mathcal{M}$. It was shown that this subclass contains bent functions that do not belong to the completed classes $\mathcal{M}^\#$ or $\mathcal{PS}^\#$. A complete characterization of the $\mathcal{D}_0$ class with respect to its intersection with $\mathcal{M}$, extending a partial characterization of Carlet, has recently been given in [44]. This does not substantially help in achieving a complete classification of bent functions, as the two primary classes stand only for a portion of $\approx 2^{76}$ of bent functions on $\mathbb{F}_2^8$, whereas their totality is around 2^{106} [48]. In recent articles [89, 88, 45], the analysis of these two secondary classes has been taken further towards specifying a sufficient set of conditions so that the resulting bent functions are also provably outside $\mathcal{M}^\#$, where the superscript "#" in general denotes a completed version of the considered class (cf. Definition 2.2.3). Due to the hardness of overall conditions, ensuring that at the same time the specified bent functions are indeed in $\mathcal{C}$ or $\mathcal{D}$ and additionally outside $\mathcal{M}^\#$ (possibly also outside $\mathcal{PS}^\#$) is a rather difficult task. One of the main objectives of this thesis is to further extend the number of bent functions lying outside the $\mathcal{M}^\#$ class.

The bentness property has been extended to general (n, m)-functions, i.e. mappings from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ (cf. Section 2.3). As shown by Nyberg [64], these functions exist only for $m \leq n/2$. The construction methods of vectorial bent functions can also be divided into two classes: *primary* and *secondary*. For some known constructions (primary and

secondary) of both Boolean and vectorial bent functions, we refer to [21, 31, 58, 61, 62, 63, 68, 86]. Another goal of this thesis is to additionally address the design of vectorial bent functions that are weakly/strongly or almost strongly outside $\mathcal{M}^{\#}$ (cf. Definition 2.3.5), a notion which was introduced in [67]. Most of the constructions are based on a generlized construction inspired by the works in [82, 90] via the so-called (P_τ) property (we will refer it as the (P_U) property, cf. Lemma 3.1.5). Similarly to the Boolean case, these vectorial objects may provide better understanding related to more complete classification of these structures.

The rest of the thesis is organized in the following way. In Chapter 2 we give basic notations, definitions and some well-known results used throughout the thesis. However, certain notions will be introduced throughout the thesis when deemed appropriate and needed.

Chapters 3 and 4 introduce a new method for the secondary construction of bent (n, m)-functions and p-ary weakly regular bent (n, m)-functions (for definition see Section 2.4) via the so-called (P_U) property. This construction will be of great importance for obtaining functions weakly, strongly or almost strongly outside $\mathcal{M}^{\#}$.

Chapter 5 addresses the construction of two new superclasses $\mathcal{SC}$ (superclass of $\mathcal{C}$ and $\mathcal{D}_0$) and $\mathcal{CD}$ (superclass of $\mathcal{C}$ and $\mathcal{D}$) as well as providing sufficient conditions for which these functions are outside $\mathcal{M}^{\#}$. In the end of the chapter, we provide explicit definitions of the duals of certain functions in $\mathcal{SC}$ and $\mathcal{CD}$.

In Chapter 6, we give an overview of the applications of the newly constructed classes $\mathcal{SC}$ and $\mathcal{CD}$ for the construction of vectorial bent functions weakly/strongly/almost strongly outside $\mathcal{M}^{\#}$ as well as so-called vectorial MNBC functions (cf. Definition 3.3.1) weakly/strongly outside $\mathcal{M}^{\#}$.

Chapter 7 further extends the number of bent functions outside the $\mathcal{M}^{\#}$ class viewed as so-called 4-decompositions. We also obtain instances of so-called bent 4-decompositions outside $\mathcal{M}^{\#}$ via the $\mathcal{SC}$ and $\mathcal{CD}$ classes.

Chapter 8 considers two well-known secondary constructions - direct and indirect sum, and we provide conditions for which these functions lie outside $\mathcal{M}^{\#}$. We also give instances of (homogeneous) cubic bent functions (without affine derivatives) and greatly increase the bounds of [71] for the dimensions in which they exist. We also show that one of the constructed classes is non-decomposable (inseperable) and we also provide vectorial bent functions strongly outside $\mathcal{M}^{\#}$ of relatively large output dimension.

At the end of the thesis we provide some concluding remarks. The results of this PhD Thesis are published in the following articles:

- ⋆ A. Bapić and E. Pasalic. A new method for secondary constructions of vectorial bent functions. *Designs, Codes and Cryptography*, volume 89(11), pages 2463–2475, 2021.
- ⋆ A. Bapić and E. Pasalic. Constructions of (vectorial) bent functions outside the completed Maiorana–McFarland class. *Discrete Applied Mathematics*, volume 314, pages 197–212, 2022.
- ⋆ A. Bapić, E. Pasalic, F. Zhang, and S. Hodžić. Constructing new superclasses of bent functions from known ones. *Cryptography and Communications*, SI Boolean Functions and Their Applications VI, pages 1–28, 2022.
- ⋆ A. Bapić, E. Pasalic, A. Polujan, and A. Pott. Vectorial boolean functions with the maximum number of bent components outside the $\mathcal{M}^{\#}$ class. *Submitted manuscript.* Available at: `https://www.wcc2022.uni-rostock.de/storages/uni-rostock/Tagungen/WCC2022/Papers/WCC_2022_paper_9.pdf`
- ⋆ A. Bapić. Secondary constructions of vectorial p-ary weakly regular bent functions. *Submitted manuscript.* Available at: `https://arxiv.org/submit/4600103/view`
- ⋆ E. Pasalic, A. Bapić, F. Zhang, and Y. Wei. Explicit infinite families of bent functions outside the completed Mairona-McFarland. *Submitted manuscript.* Available at: `https://eprint.iacr.org/2022/1126`
- ⋆ F. Zhang, E. Pasalic, A. Bapić and B. Wang. Applications of the indirect sum in the design of several special classes of bent functions outside the completed $\mathcal{M}$ class. *Submitted manuscript.* Available at: `https://eprint.iacr.org/2022/8697`

Chapter 2

Preliminary concepts

In this chapter, we give most of the definitions and concepts related to (vectorial) Boolean functions that will be used throughout the thesis. Some specific concepts will be also introduced in the corresponding sections when deemed appropriate due to simplicity and overall structure of the thesis.

Let $\mathbb{F}_{p^n}$ denote the Galois field of order p^n, where p is a prime number. Its cyclic group $\mathbb{F}_{p^n}^*$ is a multiplicative group with $p^n - 1$ elements, containing all the elements of the finite field $\mathbb{F}_{p^n}$ except the zero element. It is generated by a primitive element $\alpha \in \mathbb{F}_{p^n}$ and once such an element is fixed, we can use it to express the basis of the finite field as $\{\alpha^0, \alpha^1, \ldots, \alpha^{n-1}\}$. Consequently, any element ω in $\mathbb{F}_{p^n}$ can be expressed as

$$\omega = v_0\alpha^0 + v_1\alpha^1 + \cdots + v_{n-1}\alpha^{n-1},$$

where $v_0, \ldots, v_{n-1} \in \mathbb{F}_p$. From this, we note a natural isomorphism τ between the finite field $\mathbb{F}_{p^n}$ and the vector space $\mathbb{F}_p^n$ of p-ary n-tuples such that

$$v_0\alpha^0 + v_1\alpha^1 + \cdots + v_{n-1}\alpha^{n-1} \in \mathbb{F}_{p^n} \mapsto (v_0, \ldots, v_{n-1}) \in \mathbb{F}_p^n.$$

Because of this, we will often use both the notion of finite fields as well as vector spaces. With "$\oplus$" we will denote the summation when working with vector spaces and "$+$" when considering finite field notation.

Apart from Chapter 4, we will be considering the binary case, i.e. $p = 2$, throughout the thesis. The *Hamming weight* of a vector $x = (x_0, x_1, \ldots, x_{n-1}) \in \mathbb{F}_2^n$, denoted by $\mathrm{wt}(x)$, is defined as

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

The *Hamming distance* d between two vectors $x, y \in \mathbb{F}_2^n$ is the number of positions in which their coordinates differ. That is $d(x, y) = |\{i : x_i \neq y_i\}|$. For $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in \mathbb{F}_2^n$ the usual *scalar (dot) product* over $\mathbb{F}_2$ is defined as

$$x \cdot y = x_1y_1 \oplus \cdots \oplus x_ny_n,$$

wheras in the finite field notations it is characterized via the *trace function* $Tr_m^n : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$, $m|n$, defined with

$$Tr_m^n(x) = x + x^{2^m} + x^{2^{2m}} + \cdots + x^{2^{(n/m-1)m}}, \ x \in \mathbb{F}_{2^n}.$$

If $m = 1$, this function is called the *absolute trace* function. For $x, y \in \mathbb{F}_{2^n}$, their scalar product (using a suitable basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$) the following connection can be established (see [19]) as

$$x \cdot y = Tr_1^n(xy).$$

2.1 Boolean functions

Any mapping from $\mathbb{F}_2^n$ (or $\mathbb{F}_{2^n}$) to $\mathbb{F}_2$ is called an n-variable *Boolean function* and the set of all such functions will be denoted with $\mathcal{B}_n$. The *support* of the function is defined as $S_f = \{x \in \mathbb{F}_2^n \colon f(x) = 1\}$. The *distance* between two Boolean function f and g on the same number of variables n is measured as the number of places in which their truth tables differ, i.e. $d(f, g) = |\{x \in \mathbb{F}_2^n \colon f(x) \neq g(x)\}|$. A function on n variables is said to be *balanced* if exactly half of its output bits are zero and half are one; that is if $|S_f| = 2^{n-1}$. There are many ways on how to represent a Boolean function $f \in \mathcal{B}_n$:

- *truth table.* The $(0, 1)$-sequence defined by

  $$T_f = (f(v_0), f(v_1), \ldots, f(v_{2^n-1}))$$

  is called the truth table of f, where $v_0 = (0, \ldots, 0, 0)$, $v_1 = (0, \ldots, 0, 1), \ldots, \ v_{2^n-1} = (1, \ldots, 1, 1)$ are ordered by lexicographical order ($\{e_0, \ldots, e_{2^{n-s}-1}\} \subset \mathbb{F}_2^n$ is ordered lexicographically if $|e_i| < |e_{i+1}|$ for any $i \in [0, 2^{n-s} - 2]$, where $|e_i| = \sum_{j=0}^{n-1} e_{i,n-1-j} 2^j$ denotes the integer representation of $e_i \in \mathbb{F}_2^n$). For higher values of n such sequences are very long and they are often presented in hexadecimal or `base32` form (cf. bent functions in the Appendix).

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

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

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

  The following theorem gives us an explicit formula on how to compute the values a_u in the ANF (2.1).

Theorem 2.1.1. *[19] Let f be a Boolean function defined on $\mathbb{F}_2^n$. Then the algebraic normal form of f is unique. Moreover, the coefficients of the ANF and the values of f satisfy the following*

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

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

An important notion that we have to mention here is the so-called algebraic degree of a Boolean function. Let f be a Boolean function in algebraic normal form (2.1). The *algebraic degree* of f is defined as

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

- *trace representation.* The trace representation of f is *not* unique unlike the previous two representations. Every Boolean function can be presented as

$$x \mapsto Tr_1^n \left(\sum_{i=0}^{2^n-1} \delta_i x^i \right),$$

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

Throughout the thesis, especially when considering the inclusion/exclusion in the $\mathcal{M}^{\#}$ class (cf. Lemma 2.2.4), the notion of derivatives of Boolean functions will be of great importance.

Definition 2.1.2. The *derivative* of $f \in \mathcal{B}_n$ in the direction of $a \in \mathbb{F}_2^n$, denoted by $D_a f$, is again a Boolean function in $\mathcal{B}_n$ defined by

$$D_a(f) = f(x \oplus a) \oplus f(x),\ x \in \mathbb{F}_2^n.$$

For any $k > 1$ we can define the *k-th order derivative* of a Boolean function at $a_1, a_2, \ldots, a_k \in \mathbb{F}_2^n$ with

$$D_{a_1,a_2,\ldots,a_k} f = D_{a_1} D_{a_2} \ldots D_{a_k} f.$$

Specially, with $\mathcal{A}_n$, we will denote the class of all affine Boolean functions, i.e. functions of the form $x \mapsto a \cdot x \oplus \varepsilon$, for $a \in \mathbb{F}_2^n, \varepsilon \in \mathbb{F}_2$. For a Boolean function $f \in \mathcal{B}_n$ we define its *nonlinearity* $\mathcal{N}_f$ as the minimal Hamming distance of f from the set of all affine functions, that is,

$$\mathcal{N}_f = \min\{d(f, g) : g \in \mathcal{A}_n\}.$$

Aside from nonlinearity, another imporant tool we will need to introduce bent functions and describe important cryptographic properties of Boolean functions is called the Walsh-Hadamard transform, which is defined as follows.

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

$$W_f(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus x \cdot u}, \ u \in \mathbb{F}_2^n, \tag{2.2}$$

where $x \cdot u = x_0 u_0 \oplus \ldots \oplus x_{n-1} u_{n-1}$. The sequence of the 2^n *Walsh coefficients* given by (2.2) as u varies is called the *Walsh spectrum* of f. Similarly, we define the *inverse Walsh-Hadamard transform* (inverse WHT) at a point $u \in \mathbb{F}_2^n$ with

$$(-1)^{f(u)} = 2^{-n} \sum_{x \in \mathbb{F}_2^n} W_f(x)(-1)^{x \cdot u}. \tag{2.3}$$

In terms of the Walsh-Hadamard transform, the nonlinearity of f can be defined as

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

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

Definition 2.1.3. For two Boolean functions f and g defined on $\mathbb{F}_2^n$ we say that they are *extended affine equivalent (EA equivalent)* if there is a nonsingular $n \times n$ matrix A over the field $\mathbb{F}_2$, vectors b and c in $\mathbb{F}_2^n$, and a constant $\lambda \in \mathbb{F}_2$ such that, for every $x \in \mathbb{F}_2^n$,

$$g(x) = f(Ax \oplus b) \oplus c \cdot x \oplus \lambda.$$

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

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

In the following section we introduce the notion of bent functions as well as some primary and secondary classes of bent functions which will be the core topic of the thesis.

2.2 Bent functions

The term "bent function" was introduced by Rothaus in 1976 [77]. These functions have a wide range of applications in cryptography, coding theory, maximum length sequences, theory of difference sets, and many more. For more details on bent functions and their applications we refer to [19, 24, 59, 83].

One of the many important cryptographic properties a Boolean functions has to have is high nonlinearity to provide resistance against so-called linear cryptanalysis [54]. The functions that have maximal nonlinearity are exactly bent functions, i.e., they are at maximal Hamming distance from the set of affine functions. There are many characterizations of bent functions. To summarize, we state just a few that will be of interest to us.

For a function $f \in \mathcal{B}_n$ the following statements are equivalent:

- f is bent.
- $W_f(u) = \pm 2^{n/2}$ for all $u \in \mathbb{F}_2^n$.
- $D_a f$ is balanced for all $a \in \mathbb{F}_2^{n^*}$.
- $x \mapsto f(x) \oplus a \cdot x$ is bent for any $a \in \mathbb{F}_2^n$.
- $\mathcal{N}_f = 2^{n-1} - 2^{n/2-1}$.

When a Boolean function f is bent, the Boolean function $f^* \in \mathcal{B}_n$ such that

$$W_f(u) = 2^{\frac{n}{2}}(-1)^{f^*(u)},$$

for any $u \in \mathbb{F}_2^n$, is also bent and is called the *dual* of f (see [19]). Aside from bent functions, we will be also interested in so called s-plateaued and 5-valued spectra Boolean functions.

A function $f \in \mathcal{B}_n$ is called *s-plateaued* if its Walsh spectra only takes three values 0 and $\pm 2^{\frac{n+s}{2}}$ (the value $2^{\frac{n+s}{2}}$ is called the *amplitude*), where $s \geq 1$ if n is odd and $s \geq 2$ if n is even (s and n always have the same parity).

A class of 1-plateaued functions for n odd, or 2-plateaued for n even, corresponds to so-called *semi-bent* functions.

The Walsh support of an s-plateaued function has cardinality $\#S_f = 2^{n-s}$ [14, Proposition 4]. A *dual* function f^* of an s-plateaued $f \in \mathcal{B}_n$ is defined through $W_f(\omega) = 2^{\frac{n+s}{2}}(-1)^{f^*(\omega)}$, for $\omega \in S_f$. To specify the dual function as $f^* : \mathbb{F}_2^{n-s} \to \mathbb{F}_2$ we use the concept of lexicographic ordering, which was introduced in Section 2.1.

Since S_f is not ordered in general, *we will always represent it* as $S_f = v \oplus E$, where E is lexicographically ordered for some fixed $v \in S_f$ and $e_0 = \mathbf{0}_n$. A direct correspondence between $\mathbb{F}_2^{n-s}$ and $S_f = \{\omega_0, \ldots, \omega_{2^{n-s}-1}\}$ is achieved through E so that for the lexicographically ordered $\mathbb{F}_2^{n-s} = \{x_0, x_1, \ldots, x_{2^{n-s}-1}\}$ we have

$$\overline{f}^*(x_i) = f^*(v \oplus e_i) = f^*(\omega_i), \tag{2.4}$$

where $x_i \in \mathbb{F}_2^{n-s},\ e_i \in E,\ i \in [0, 2^{n-s} - 1]$.

Remark 2.2.1. Throughout the thesis, the dual of an s-plateaued function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ will be denoted by f^* and is considered as a function on S_f (that is $f^* : S_f \to \mathbb{F}_2$). However, as specified in (2.4), the notation $\overline{f}^*$ associates this dual to a function defined on $\mathbb{F}_2^{n-s}$, that is $\overline{f}^* : \mathbb{F}_2^{n-s} \to \mathbb{F}_2$.

Throughout the thesis, several special forms of bent functions will be of interest for us, which is why we summarize their notion in the following section.

2.2.1 Classes of bent functions

Till today, the number of bent functions in n variables is only known for $n \leq 8$. For $n \geq 10$ this remains an open problem. In $n = 2, 4$ and 6 bent functions have been completely classified under the action of the general linear group.

For $n = 8$ there are approximately 2^{106} [48] bent functions. If we were to imagine all these bent functions as an enormous garden, the bent functions classified for $n = 8$ could fit on a single flower(whose cardinality is c.a. 2^{76}). Thus, it is natural to ask, what are the remaining "flowers". The solution is to study constructions of bent functions. One approach of designing "new" bent functions, on the same or on a larger variable space, uses already known bent functions. these methods are commonly referred to as secondary constructions. These are called *secondary constructions*. The two known *primary constructions* are direct in the sense that they do not use bent functions as building blocks, and most likely there do not exist other primary methods. Therefore, to classify and enumerate bent functions, the secondary construction methods are of great importance. In what follows we present the two main primary classes $\mathcal{M}$ and $\mathcal{PS}$, as well as two secondary classes $\mathcal{C}$ and $\mathcal{D}$, which will be of great interest throughout the thesis.

Bent functions in $\mathcal{M}$ and $\mathcal{PS}$

When considering classes of bent functions, there are two primary classes referred to as partial spread ($\mathcal{PS}$) class due to Dillon [29] and the Maiorana-McFarland ($\mathcal{M}$) class [55]. The term primary refers to the design that does not employ known bent functions to generate new ones (giving rise to the so-called secondary methods), it rather uses a suitable set of affine functions (typical for the Maiorana-McFarland method [55]) or a collection of disjoint $n/2$-dimensional subspaces to construct a bent function on $\mathbb{F}_{2^n}$ (typical for the partial spread class introduced by Dillon [29]).

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

$$(\mathcal{M}) : f(x, y) = x \cdot \pi(y) \oplus g(y), \quad x, y \in \mathbb{F}_2^m$$

where π is a permutation on $\mathbb{F}_2^m$, and g is an arbitrary Boolean function on $\mathbb{F}_2^m$. This is one of the few classes where the explicit construction of the duals is known. For $f \in \mathcal{M}$, we have that its associated dual bent function $f^* \in M$ (see also Remark 7.2.1 for the fact that f^* is in M) is given by

$$f^*(x, y) = y \cdot \pi^{-1}(x) \oplus g(\pi^{-1}(x)),\ x, y \in \mathbb{F}_2^m,$$

where π^{-1} denotes the inverse permutation of π. Quite often we will describe these functions using finite field notation:

$$f(x, y) = Tr_1^m(x\pi(y)) + g(y),\ x, y \in \mathbb{F}_{2^m},$$

where Tr_1^m denotes the absolute trace.

In order to introduce the partial spread construction of bent functions functions, we first give a definition of a partial spread.

Definition 2.2.2. A *partial spread* of order s in $\mathbb{F}_2^n$ with $n = 2k$ is a set of s vector subspaces $U_1, \ldots, U_s$ of $\mathbb{F}_2^n$ of dimension k each, such that $U_i \cap U_j = \{0\}$ for all $i \neq j$. The partial spread of order $s = 2^k + 1$ in $\mathbb{F}_2^n$ with $n = 2k$ is called a spread.

In the following, we denote by $\mathbb{1}_U : \mathbb{F}_2^n \to \mathbb{F}_2$ the *indicator function* of $U \subseteq \mathbb{F}_2^n$, i.e., $\mathbb{1}_U(x) = 1$ if $x \in U$, and 0 otherwise. Using the notion of a partial spread, Dillon [29] introduced a partial spread construction of bent functions, which splits the $\mathcal{PS}$ class into the following two subclasses:

- The $\mathcal{PS}^+$ *class* is the set of Boolean bent functions of the form

$$(\mathcal{PS}^+) : f(x) = \sum_{i=1}^{2^{k-1}+1} \mathbb{1}_{U_i}(x),\ x \in \mathbb{F}_2^n$$

  where the vector spaces $U_1, \ldots, U_{2^{k-1}+1}$ of $\mathbb{F}_2^n$ form a partial spread in $\mathbb{F}_2^n$.

- The $\mathcal{PS}^-$ *class* is the set of Boolean bent functions of the form

$$(\mathcal{PS}^-) : f(x) = \sum_{i=1}^{2^{k-1}} \mathbb{1}_{U_i^*}(x),\ x \in \mathbb{F}_2^n$$

  where the vector spaces $U_1, \ldots, U_{2^{k-1}}$ of $\mathbb{F}_2^n$ form a partial spread in $\mathbb{F}_2^n$ and $U_i^* := U_i \setminus \{0\}$.

The *Desarguesian partial spread* class $\mathcal{PS}_{ap} \subset \mathcal{PS}^-$ is the set of Boolean bent functions f on $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ of the form

$$(\mathcal{PS}_{ap}) : f\colon (x, y) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \mapsto h\left(x/y\right),$$

where $x/y = 0$ if $y = 0$ for $x, y \in \mathbb{F}_{2^k}$ and $h\colon \mathbb{F}_{2^k} \to \mathbb{F}_2$ is a balanced Boolean function with $h(0) = 0$.

Bent functions in $\mathcal{C}$ and $\mathcal{D}$

In 1993, Carlet [17] introduced two additional secondary classes of bent functions, denoted by $\mathcal{C}$ and $\mathcal{D}$, which are derived through a suitable modification of bent functions in the $\mathcal{M}$ class. One explicit class derived by Carlet, containing instances that do not belong to $\mathcal{M}$ or $\mathcal{PS}$, is named $\mathcal{D}_0$ and its cardinality is of approximately the same size as of $\mathcal{M}$. This does not substantially help in achieving a complete classification of bent functions, as the two primary classes stand only for a portion of $\approx 2^{76}$ of bent functions on $\mathbb{F}_2^8$, whereas their totality is around 2^{106} [48].

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

$$(\mathcal{C}) : f(x, y) = x \cdot \pi(y) \oplus \mathbb{1}_{L^\perp}(x), \tag{2.5}$$

where L is any linear subspace of $\mathbb{F}_2^m$, $\mathbb{1}_{L^\perp}$ is the indicator function of the space $L^\perp = \{x \in \mathbb{F}_2^m : x \cdot y = 0,\ \forall y \in L\}$, and π is any permutation on $\mathbb{F}_2^m$ such that:

$$(C) \quad \pi^{-1}(a \oplus L) \text{ is a flat (affine subspace), for all } a \in \mathbb{F}_2^m.$$

The permutation π^{-1} and the subspace L are then said to satisfy the (C) property, or for short (π^{-1}, L) *has property* (C).

Another class introduced by Carlet [17], called $\mathcal{D}$, is defined similarly as

$$(\mathcal{D}) : f(x, y) = x \cdot \pi(y) \oplus \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y), \tag{2.6}$$

where π is a permutation on $\mathbb{F}_2^m$ and E_1, E_2 two linear subspaces of $\mathbb{F}_2^m$ such that $\pi(E_2) = E_1^\perp$.

Class inclusion of bent functions

As we want to have non-equivalent bent functions, we note the following definition in connection with the EA-equivalence (cf. Definition 2.1.3)

Definition 2.2.3. Let $\mathcal{F} \subset \mathcal{B}_n$ be any class of bent functions. Its *completed class* $\mathcal{F}^\# \subset \mathcal{B}_n$ is defined as follows:

$$\mathcal{F}^\# = \{f(Ax \oplus b) \oplus c \cdot x \oplus \varepsilon : f \in \mathcal{F},\ A \in GL(n, \mathbb{F}_2),\ b, c \in \mathbb{F}_2^n, \varepsilon \in \mathbb{F}_2\},$$

i.e., it contains the primary class and all the other bent functions that can be derived from the primary class using some affine transformations.

Showing the non-inclusion into the completed primary classes is usually a hard task. For $\mathcal{M}^\#$ there exist an inclusion indicator due to Dillon (1974) (cf. Lemma 2.2.4), but it becomes computationally inefficient for $n \geq 14$. For $\mathcal{PS}^\#$, there are no such inclusion indicators and consequently proving that a function is outside $\mathcal{PS}^\#$ becomes an extremely difficult task.

Lemma 2.2.4. *[29] A bent function f in n variables belongs to $\mathcal{M}^\#$ if and only if there exists an $\frac{n}{2}$-dimensional linear subspace V of $\mathbb{F}_2^n$ such*

that the second order derivatives

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

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

In recent articles [89, 88, 45], the analysis of the $\mathcal{C}$ and $\mathcal{D}$ classes has been taken further towards specifying a sufficient set of conditions so that the resulting bent functions are also provably outside $\mathcal{M}^\#$. Due to the hardness of overall conditions, ensuring that at the same time the specified bent functions are indeed in $\mathcal{C}$ or $\mathcal{D}$ and additionally outside $\mathcal{M}^\#$ (possibly also outside $\mathcal{PS}^\#$) is a rather difficult task. These conditions involve the concept of linear structures which is defined below.

Definition 2.2.5. An n-variable Boolean function f is said to have a linear structure if there exists a nonzero $a \in \mathbb{F}_2^n$ such that $f(x \oplus a) \oplus f(x)$ is a constant function.

We note the following useful results for confirming if a function is in $\mathcal{C}$ and $\mathcal{D}$ outside $\mathcal{M}^\#$.

Theorem 2.2.6. *[88, Theorem 1] Let $n = 2m \geq 8$ be an even integer and let $f(x, y) = \pi(y) \cdot x \oplus \mathbb{1}_{L^\perp}(x)$, where L is any linear subspace of $\mathbb{F}_2^m$ and π is a permutation on $\mathbb{F}_2^m$ such that (π^{-1}, L) has property (C). If (π^{-1}, L) satisfies:*

$(C1)$ $\dim(L) \geq 2$*;*

$(C2)$ $u \cdot \pi$ *has no nonzero linear structure for all* $u \in \mathbb{F}_2^{m^*}$*,*

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

Theorem 2.2.7. *[88, Theorem 2] Let $n = 2m \geq 8$ be an even integer and let $f(x, y) = \pi(y) \cdot x \oplus \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y)$, where π is a permutation on $\mathbb{F}_2^m$, and E_1, E_2 are two linear subspaces of $\mathbb{F}_2^m$ such that $\pi(E_2) = E_1^\perp$. If (π, E_1, E_2) satisfies:*

$(D1)$ $\dim(E_1) \geq 2$ *and* $\dim(E_2) \geq 2$*;*

$(D2)$ $u \cdot \pi$ *has no nonzero linear structure for all* $u \in \mathbb{F}_2^{m^*}$*;*

$(D3)$ $\deg(\pi) \leq m - \dim(E_2)$,

then f is a bent function in $\mathcal{D}$ outside $\mathcal{M}^\#$.

2.3 Vectorial Boolean (bent) functions

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

S-boxes. Clearly, any vectorial Boolean function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ can be presented in the form

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

where $f_i : \mathbb{F}_2^n \to \mathbb{F}_2$, $i = 0, \ldots, m-1$, are called the *coordinate functions* of the function F. Properties of an (n, m)-function F may be characterised by the $2^m - 1$ non-zero linear combinations of its coordinate functions, called *component functions.*

Definition 2.3.1. Let F be an (n, m) function. The functions $x \in \mathbb{F}_2^n \mapsto v \cdot F(x), 0 \neq v \in \mathbb{F}_2^m$ are called the *component functions* of F. Equivalently, in the finite field representation, let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$. The component functions of F are the functions $Tr_1^m(bF(x)), \ b \in \mathbb{F}_{2^m}^*$.

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

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

is called the *(extended) Walsh-Hadamard transform of the function* F and the *Walsh support* of F is the set of those $(u, v) \in \mathbb{F}_2^n \times \mathbb{F}_2^{m^*}$ such that $W_F(u, v) \neq 0$, denoted by $\mathcal{W}_F$. The *algebraic degree* of an (n, m)-function F is defined by

$$\deg F = \max\{\deg(v \cdot F) : v \in \mathbb{F}_2^{m^*}\}.$$

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

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

Similarly as in the Boolean case we can define bent (n, m)-functions as follows.

Definition 2.3.2. An (n, m)-function is said to be *bent* if all of its component functions are bent, i.e., $|W_{v \cdot F}(u)| = 2^{\frac{n}{2}}$, for all $u \in \mathbb{F}_2^n, v \in \mathbb{F}_2^{m^*}$.

As it was shown by Nyberg [64], these functions exist only for $m \leq n/2$. When talking about equivalent vectorial Boolean functions, we note the following equivalences.

Definition 2.3.3. [13] Two (n, m)-functions F and F' are called:

- *affine equivalent* if $F' = A_1 \circ F \circ A_2$, where the mappings A_1 and A_2 are affine permutations of $\mathbb{F}_{2^m}$ and $\mathbb{F}_{2^n}$, respectively;
- *extended affine equivalent (EA-equivalent)* if $F' = A_1 \circ F \circ A_2 + A$, where the mappings $A : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}, \ A_1 : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}, \ A_2 : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are affine, and where A_1 and A_2 are permutations;

- *Carlet-Charpin-Zinoviev equivalent (CCZ-equivalent)* if for some affine permutation $\mathcal{L}$ of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$ the image of the graph of F is the graph of F', that is, $\mathcal{L}(\Gamma_F) = \Gamma_{F'}$, where $\Gamma_F = \{(x, F(x)) : x \in \mathbb{F}_{2^n}\}$ and $\Gamma_{F'} = \{(x, F'(x)) : x \in \mathbb{F}_{2^n}\}$.

Although different, these equivalent relations have a connection. Obviously, every affine equivalence is a particular case of EA-equivalence. In [20] it has been shown that EA-equivalence is a particular case of CCZ-equivalence and every permutation is CCZ-equivalent to its inverse.

Remark 2.3.4. In [12] it has been shown that when considering bent (n, m)-functions, CCZ- and EA-equivalence coincide.

Similarly as for the Boolean case, we distinguish primary and secondary classes of vectorial bent Boolean functions.

Let us define $F : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ with $F(x, y) = x\pi(y) + g(y)$, where $\pi : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ is a permutation and $g : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ is an arbitrary function. A function defined in such a way belongs to the class of vectorial bent Maiorana-McFarland functions. Similarly to the Boolean case, the *Desarguesian partial spread* class $\mathcal{PS}_{ap}$ of bent (n, m)-functions with $m = n/2$ is defined as the set of (n, m)-functions F on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ of the form $F\colon (x, y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \mapsto H\,(x/y)$, where $x/y = 0$ if $y = 0$ for $x, y \in \mathbb{F}_{2^m}$ and H is a permutation on $\mathbb{F}_{2^m}$ such that $H(0) = 0$.

For some known constructions (primary and secondary) of both Boolean and vectorial bent functions, we refer to [21, 31, 58, 61, 62, 63, 68, 86]. Similarly as for the Boolean case, the (partial) exclusion of a given (n, m) bent function from a considered completed class is a difficult task. Since, in contrast to $\mathcal{M}^{\#}$, there are no class inclusion criteria for the $\mathcal{PS}^{\#}$ class (similar to Lemma 2.2.4 of Dillon), throughout this thesis we will consider (partial) exclusion from the $\mathcal{M}^{\#}$ class. With respect to this, we note the notion of functions weakly and strongly outside given completed version of some primary class introduced in [67] as well as a new notion of functions almost strongly outside a completed class.

Definition 2.3.5. Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ be any bent (n, m)-function, $m \leq n/2$, and let $\mathcal{F}$ denote some primary class of bent functions.

- F is **weakly** outside $\mathcal{F}^{\#} \Leftrightarrow (\exists u \in \mathbb{F}_2^{m^*})\ u \cdot F \notin \mathcal{F}^{\#}$.
- F is **strongly** outside $\mathcal{F}^{\#} \Leftrightarrow (\forall u \in \mathbb{F}_2^{m^*})\ u \cdot F \notin \mathcal{F}^{\#}$.
- F is **almost strongly** outside $\mathcal{F}^{\#} \Leftrightarrow (\exists! u \in \mathbb{F}_2^{m^*})\ u \cdot F \in \mathcal{F}^{\#}$.

More details on vectorial bent functions and their class inclusion will be introduced in Chapter 6. In the following section we give a brief overview of p-ary functions which will be discussed in Chapter 4.

2.4 p-ary functions

A function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ is called a *p-ary function* and the set of all such functions is denoted by $\mathcal{B}_n^p$. Any p-ary function $f \in \mathcal{B}_n^p$ can be uniquely expressed as a polynomial in $\mathbb{F}_p[x_0, \ldots, x_{n-1}] \setminus \langle x_0^p - x, \ldots, x_{n-1}^p - x \rangle$ as

$$f(x_0, \ldots, x_{n-1}) = \sum_{a \in \mathbb{F}_p^n} \lambda_a \prod_{i=0}^{n-1} x_i^{a_i},$$

where $\lambda_a \in \mathbb{F}_p$. The algebraic degree of f is defined as

$$\deg(f) = \max\{wt(a) : \lambda_a \neq 0\},$$

where $wt(a) = |\{i : a_i \neq 0, 0 \leq i \leq n-1\}|$ is the weight of $a \in \mathbb{F}_p^n$. The generalized Walsh-Hadamard transform (GWHT) and its inverse of a p-ary function $f \in \mathcal{B}_n^p$ at a point $a \in \mathbb{F}_p^n$ are defined by

$$\mathcal{H}_f(a) = \sum_{x \in \mathbb{F}_p^n} \xi_p^{f(x) - \langle a, x \rangle},$$

and

$$\xi^{f(a)} = p^{-n} \sum_{x \in \mathbb{F}_p^n} \mathcal{H}_f(x) \xi_p^{\langle a, x \rangle},$$

respectively, where $\xi_p = e^{\frac{2\pi i}{p}}$ denotes the complex primitive p-th root of unity and $\langle a, b \rangle$ denotes an inner product on $\mathbb{F}_p^n$. For convenience, if we are considering functions in vector space notation, we will define $\langle x, y \rangle = \sum_{i=1}^n x_i y_i$, and if are considering finite field notation, we will define $\langle \alpha, \beta \rangle = tr_n(\alpha\beta)$, where

$$tr_m^n(\alpha) := \alpha + \alpha^{p^m} + \alpha^{p^{2m}} + \cdots + \alpha^{p^{m(n/m-1)}}$$

denotes the trace function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$, $m|n$. For simplicity we will use the notation $tr_n := tr_1^n$.

A function $f \in \mathcal{B}_n^p$ is said to be *bent* if $|\mathcal{H}_f(a)|^2 = p^n$ for all $a \in \mathbb{F}_p^n$. Furthermore, f is said to be *regular bent* if for every $b \in \mathbb{F}_p^n$, $p^{-n/2}\mathcal{H}_f(b) = \xi_p^{f^*(b)}$ for some mapping $f^* \in \mathcal{B}_n^p$, which is then called the *dual* of f. The bent function f is said to be *weakly regular* if there exists a complex number z with $|z| = 1$, such that $zp^{-n/2}\mathcal{H}_f(b) = \xi_p^{f^*(b)}$ for all $b \in \mathbb{F}_p^n$. As noted in [59], regular bent functions can only be found for even n and for odd n with $p \mod 4 = 1$. Moreover, for a weakly regular bent function, the constant z (defined above) can only be equal to ± 1 or $\pm i$. Weakly regular bent functions always come in pairs, since the dual is bent as well. Moreover, it holds that $f^{**}(x) = f(-x)$, $f^{***}(x) = f^*(-x)$, $f^{****}(x) =$

$f(x)$ (see [59]). For a p-ary function $f \in \mathcal{B}_n^p$, we define its derivative $D_a f \in \mathcal{B}_n^p$ at a point $a \in \mathbb{F}_{p^n}$ as

$$D_a f(x) = f(x+a) - f(x),\ x \in \mathbb{F}_{p^n}.$$

Similarly, the k-th order derivative of f with respect to $a_1, \ldots, a_k \in \mathbb{F}_{p^n}$ is defined by $D_{a_1,\ldots,a_k} f(x) = D_{a_1} D_{a_2} \ldots D_{a_k} f(x)$, for all $x \in \mathbb{F}_{p^n}$.

Any mapping F from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ is called a vectorial p-ary function (or a p-ary (n,m)-function). We say that F is (weakly regular) bent if for every $u \in \mathbb{F}_{p^m}^*$, its component function $F_u \in \mathcal{B}_n^p$ defined as $F_u(x) = tr_m(uF(x)),\ x \in \mathbb{F}_{p^n}$, is p-ary (weakly regular) bent. Unlike the binary case, p-ary bent (n,m)-functions exist for all $m \leq n$ [23].

Another important class of vectorial p-ary bent functions are the so-called plateaued p-ary (n,m)-functions. Namely, we say that a p-ary (n,m)-function F is plateaued if $\mathcal{H}^2_{F_\lambda}(x) \in \{0, p^{n+s}\}$ for all $x \in \mathbb{F}_{p^n}$ and all $\lambda \in \mathbb{F}_{p^m}^*$, for some $s \in \mathbb{N}_0$ (which is called the amplitude). Specially, if $s = 0$ we are talking about bent functions, and if $s = 1$, then such functions are called near-bent. If all the components have the same amplitude s, then these functions are called s-plateaued p-ary (n,m)-functions.

Chapter 3

Secondary constructions of vectorial bent functions via the (P_U) property

In 2017, Tang *et al.* [82] proposed a secondary construction of bent functions of the form

$$f(x) = g(x) + h(Tr_1^n(u_1x), \ldots, Tr_1^n(u_tx)),$$

where $n = 2m$, g is any known bent function in n variables satisfying some conditions, $h(X_1, \ldots, X_t)$ is an arbitrary polynomial in $\mathbb{F}_2[X_1, \ldots, X_t]$, t is a positive integer such that $1 \leq t \leq m$, and $u_1, \ldots, u_t$ are suitably selected (distinct) nonzero elements in $\mathbb{F}_{2^n}$. Using this construction, several new infinite families of bent functions from specific instances of bent functions (derived from Kasami, Niho and Gold-like monomials; or taken from the Maiorana-McFarland class) were obtained.

This result has been recently extended by Zheng *et al.* [90] for the purpose of specifying vectorial bent functions. Let $n = 2m$ and k be its positive divisor such that $k \leq m$. The authors of [90] proposed a method of constructing bent (n, k)-functions of the form

$$F(x) = G(x) + h(x),$$

where G is a bent (n, k)-function satisfying certain properties and h is a Boolean function. Using this approach the authors in [90] constructed three new infinite families of bent (n, k)-functions, as well as new infinite families of vectorial plateaued $(n, k + t)$-functions $(t \geq 0)$ having maximal number of bent components.

In this chapter, we extend the result of Zheng *et al.* [90] by proposing a new construction method of bent (n, m)-functions, $n = 2m$ and $t|m$, of the form

$$F(x) = G(x) + \mathbf{H}(x), \tag{3.1}$$

where G is a suitable bent (n, m)-function and $\mathbf{H}$ is an (n, t)-function (in difference to the use of Boolean $h(x)$). More precisely, the assumption on G is that the duals of its components $G_\lambda(x) = Tr_1^m(\lambda F(x))$

satisfy certain forms of linearity, so that for some nonzero elements $u_1, u_2, \ldots, u_t \in \mathbb{F}_{2^m}$ it holds that

$$G^*_\lambda\left(x + \sum_{i=1}^{t} u_i w_i\right) = G^*_\lambda(x) + \sum_{i=1}^{t} w_i g_i(x) \tag{3.2}$$

for all $x \in \mathbb{F}_{2^n}$ and $(w_1, \ldots, w_t) \in \mathbb{F}_2^t$, where G^*_λ denotes the dual of G_λ.

Remark 3.0.1. In this case, we will say that $(G^*_\lambda)_{\lambda \in \mathbb{F}^*_{2^m}}$ satisfies the (P_U) *property* (with the *defining set* $U = \{u_1, \ldots, u_t\}$).

Most notably, specifying $\mathbf{H}(x) = \mathbf{h}(Tr^n_1(u_1x), \ldots, Tr^n_1(u_tx))$, the function $\mathbf{h} : \mathbb{F}_2^t \to \mathbb{F}_{2^t}$ can be chosen arbitrarily which gives a relatively large class of different functions for a fixed function G. It is also proved that the vectorial bentness of $F(x) = G(x) + \mathbf{H}(x)$ implies that $\mathbf{H}$ cannot be bent. We identify several suitable classes of vectorial bent functions G (satisfying the above mentioned property), which then give rise to infinite families of vectorial bent functions for any fixed G. The rest of the chapter is organised as follows. In Section 3.1 we give our main construction of vectorial bent functions, along with an analysis on EA-equivalence. Some new infinite families of vectorial bent functions are derived in Section 3.2. In Section 3.3, we propose a new method of specifying infinite classes of vectorial (n, n)-functions having maximum number of bent components.

3.1 Generic construction of vectorial bent functions

Motivated by the results given in [82] and [90], we provide the following construction of vectorial Boolean functions.

Construction 3.1.1. Let $\{u_1, \ldots, u_t\} = U \subseteq \mathbb{F}^*_{2^n}$ be linearly independent elements over $\mathbb{F}_2$, where $n = 2m$ and $t|m$. Let $G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ be any vectorial bent function such that $(G^*_\lambda)_{\lambda \in \mathbb{F}^*_{2^m}}$ satisfies the (P_U) property (3.2). Let $\mathbf{h}(X_1, \ldots, X_t)$ be any vectorial Boolean Function from $\mathbb{F}_2^t$ to $\mathbb{F}_{2^t}$. Define $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$, using G and $\mathbf{h}$, as

$$F(x) = G(x) + \mathbf{H}(x), \tag{3.3}$$

where $\mathbf{H} : \mathbb{F}_{2^n} \to \mathbb{F}_{2^t}$ is defined by $\mathbf{H}(x) = \mathbf{h}(Tr^n_1(u_1x), \ldots, Tr^n_1(u_tx))$. Equivalently, if $\mathbf{h}$ is defined using the finite field notation so that $\mathbf{h} : \mathbb{F}_{2^t} \to \mathbb{F}_{2^t}$, then define

$$\begin{aligned} F(x) &= G(x) + \mathbf{H}(x) \\ &= G(x) + \mathbf{h}(Tr^n_1(u_1x) + \alpha Tr^n_1(u_2x) + \cdots + \alpha^{t-1} Tr^n_1(u_tx)), \end{aligned} \tag{3.4}$$

where α is a primitive element of $\mathbb{F}_{2^t}$.

Example 3.1.2. Let us consider the Kasami function $G : \mathbb{F}_{2^8} \to \mathbb{F}_{2^4}$ defined by $G(x) = x^{2^4+1}$. It is well-known that the components of G are bent whose duals G^*_λ satisfy (3.2) [57, 82]. We note that $(2^8-1)/(2^4-1) = 17$ and thus $\mathbb{F}^*_{2^4} = \langle \alpha^{17} \rangle$, where α is a root of the primitive polynomial $p(x) = x^8 + x^4 + x^3 + x^2 + 1 \in \mathbb{F}_{2^8}[x]$. As suggested in [90], let us define $S = \{x \in \mathbb{F}_{2^8} : x \cdot x^{2^4} = 1\}$ and assume that $\{\tau_1, \ldots, \tau_4\}$ is a basis of $\mathbb{F}_{2^4}$. The so-called defining set, introduced in [90] and required in (3.2), is $U = \{\tau_1 v, \ldots, \tau_4 v\}$, where $v \in S, v \neq 1$. For example, we can take

$$\begin{aligned} U &= \{u_1, \ldots, u_4\} \\ &= \{\alpha^5 + \alpha^2 + \alpha, \alpha^7 + \alpha^4 + \alpha^3 + \alpha^2 + 1, \alpha^7 + \alpha^3 + \alpha^2, \alpha^6 + \alpha^5 + 1\}. \end{aligned}$$

Let $\mathbf{h} : \mathbb{F}_{2^4} \to \mathbb{F}_{2^4}$ be defined as $\mathbf{h}(x) = x^3$. Then

$$\begin{aligned} F(x) &= G(x) + \mathbf{H}(x) \\ &= x^{17} + (Tr_1^8(u_1 x) + \beta Tr_1^8(u_2 x) + \cdots + \beta^2 Tr_1^8(u_3 x) + \beta^3 Tr_1^8(u_4 x))^3, \end{aligned}$$

where $\beta = \alpha^{17}$. Using the mathematical software Sage and MAGMA, we confirm that F is a bent $(8, 4)$-function and it is CCZ-inequivalent to G and $\mathbf{H}$.

In connection to Construction 3.1.1 and Example 3.1.2, we state the following theorem.

Theorem 3.1.3. *The function F generated by Construction 3.1.1 is a bent (n, m)-function.*

Proof. Let $\lambda \in \mathbb{F}^*_{2^m}$ be arbitrary. Let us consider the component G_λ and let $\mathbf{h}_\lambda : \mathbb{F}_2^t \to \mathbb{F}_2$ be defined as $\mathbf{h}_\lambda = Tr_1^m(\lambda \mathbf{h})$. From the inverse Walsh-Hadamard transform, we have that

$$(-1)^{\mathbf{h}_\lambda(X_1, \ldots, X_t)} = \sum_{(w_1, \ldots, w_t) \in \mathbb{F}_2^t} W_{\mathbf{h}_\lambda}(w_1, \ldots, w_t)(-1)^{\sum_{i=1}^t w_i X_i}.$$

For any $x \in \mathbb{F}_{2^n}$ and $1 \leq i \leq t \leq m$, taking $X_i = Tr_1^n(u_i x)$, we obtain

$$(-1)^{\mathbf{h}_\lambda(Tr_1^n(u_1 x), \ldots, Tr_1^n(u_t x))} = \sum_{(w_1, \ldots, w_t) \in \mathbb{F}_2^t} W_{\mathbf{h}_\lambda}(w_1, \ldots, w_t)(-1)^{Tr_1^n\left(\left(\sum_{i=1}^t w_i u_i\right)x\right)}. \tag{3.5}$$

Multiplying both sides of (3.5) by $(-1)^{G_\lambda(x) + Tr_1^n(\beta x)}$, we have

$$\begin{aligned} &(-1)^{G_\lambda(x) + \mathbf{H}_\lambda(x) + Tr_1^n(\beta x)} \\ &= \sum_{(w_1, \ldots, w_t) \in \mathbb{F}_2^t} W_{\mathbf{h}_\lambda}(w_1, \ldots, w_t)(-1)^{G_\lambda(x) + Tr_1^n\left(\left(\beta + \sum_{i=1}^t w_i u_i\right)x\right)}. \end{aligned}$$

By summing the previous expression on both sides over all $x \in \mathbb{F}_{2^n}$ and using the fact that G is vectorial bent, we obtain that

$$\begin{aligned} W_{F_\lambda}(\beta) &= \sum_{(w_1,\ldots,w_t)\in\mathbb{F}_2^t} W_{\mathbf{h}_\lambda}(w_1,\ldots,w_t) W_{G_\lambda}(\beta + \sum_{i=1}^{t} u_i w_i) \\ &= 2^m \sum_{(w_1,\ldots,w_t)\in\mathbb{F}_2^t} W_{\mathbf{h}_\lambda}(w_1,\ldots,w_t)(-1)^{G_\lambda^*(\beta+\sum_{i=1}^t u_i w_i)}. \end{aligned} \tag{3.6}$$

It follows from (3.2) and (3.6) that

$$W_{F_\lambda}(\beta) = 2^m(-1)^{G_\lambda^*(\beta)} \sum_{(w_1,\ldots,w_t)\in\mathbb{F}_2^t} W_{\mathbf{h}_\lambda}(w_1,\ldots,w_t)(-1)^{\sum_{i=1}^t w_i g_i(\beta)}.$$

The sum on the right-hand side corresponds to the inverse Walsh-Hadamard transform of $\mathbf{h}_\lambda$ at the point $(g_1(\beta),\ldots,g_t(\beta))$ and thus we have

$$W_{F_\lambda}(\beta) = 2^m(-1)^{G_\lambda^*(\beta)+\mathbf{h}_\lambda(g_1(\beta),g_2(\beta),\ldots,g_t(\beta))}.$$

Since $\beta \in \mathbb{F}_{2^n}$ is arbitrary, we have that F_λ is bent for all $\lambda \in \mathbb{F}_{2^m}^*$. In other words, F is a bent (n,m)-function. □

Remark 3.1.4. If we have a function $f : X \to Y$, then the number of possible functions f equals to $\#Y^{\#X}$. Thus, since $\mathbf{h}$ is a (t,t)-function, there are 2^{t2^t} possible choices for $\mathbf{h}$. Hence, we can construct at most 2^{t2^t} bent (n,m)-functions F from a fixed bent function G and an arbitrary function $\mathbf{h}$. In the case when $n = 8$ and $m = t = 4$, we have 2^{64} possibilities.

We note that in [90] the authors characterized the (P_U) property via second-order derivatives as follows.

Lemma 3.1.5. *[90] Let $g \in \mathcal{B}_n$ be any bent function. Then the following statements are equivalent.*

(i) There exist $u_1,\ldots,u_t \in \mathbb{F}_{2^n}$ and $g_1,\ldots,g_t \in \mathcal{B}_n$ such that

$$g\left(x + \sum_{i=1}^{t} w_i u_i\right) = g(x) + \sum_{i=1}^{t} w_i g_i(x), \tag{3.7}$$

for all $w = (w_1,\ldots,w_t) \in \mathbb{F}_{2^t}$.

(ii) $D_{u_i}D_{u_j}g \equiv 0$ for all $1 \le i,j \le t$.

For convenience and simplicity we will sometimes consider the (P_U) property via second order derivatives as seen in Lemma 3.1.5.

The following lemma is a straightforward consequence of linearity of the mapping $L : \mathbb{F}_{2^n} \to \mathbb{F}_2^t$, where $L(x) = (Tr_1^n(u_1x),\ldots,Tr_1^n(u_tx))$ and $u_1,\ldots,u_t \in \mathbb{F}_{2^t}$ are linearly independent over $\mathbb{F}_2$.

Lemma 3.1.6. *Let $u_1, \ldots, u_t \in \mathbb{F}_{2^t}^*$ be linearly independent elements over $\mathbb{F}_2$, $n = 2m, t|m$. Then the multiset*

$$V = \{(Tr_1^n(u_1x), \ldots, Tr_1^n(u_tx)) : x \in \mathbb{F}_{2^n}\} = \underbrace{\mathbb{F}_2^t \cup \mathbb{F}_2^t \ldots \cup \mathbb{F}_2^t}_{2^{n-t} \text{ sets}}, \quad (3.8)$$

contains exactly 2^{n-t} copies of every element of $\mathbb{F}_2^t$.

It is interesting to notice that $\mathbf{H} : \mathbb{F}_{2^n} \to \mathbb{F}_{2^t}$ in Construction 3.1.1 cannot be vectorial bent, as shown below.

Proposition 3.1.7. *Let $u_1, \ldots, u_m \in \mathbb{F}_{2^n}^*$ be linearly independent elements over $\mathbb{F}_2$, where $n = 2m$. The function $\mathbf{H} : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ defined by*

$$\mathbf{H}(x) = \mathbf{h}(Tr_1^n(u_1x), \ldots, Tr_1^n(u_mx)),$$

where $\mathbf{h} : \mathbb{F}_2^m \to \mathbb{F}_{2^m}$ is arbitrary, cannot be bent.

Proof. Let $\lambda \in \mathbb{F}_{2^m}^*$ be arbitrary. Let us consider the value of $W_{\mathbf{H}_\lambda}(0)$.

$$W_{\mathbf{H}_\lambda}(0) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathbf{H}_\lambda(x)} = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathbf{h}_\lambda(Tr_1^n(u_1x), \ldots, Tr_1^m(u_mx))}$$
$$\stackrel{(3.8)}{=} 2^{n-m} \sum_{X \in \mathbb{F}_2^m} (-1)^{\mathbf{h}_\lambda(X)} = 2^m \cdot W_{\mathbf{h}_\lambda}(0)$$

Since $W_{\mathbf{h}_\lambda}(0) \neq \pm 1$, it follows that $W_{\mathbf{H}_\lambda}(0) \neq \pm 2^m$. Hence, $\mathbf{H}_\lambda$ cannot be bent. Thus, no components of $\mathbf{H}$ are bent Boolean functions.

□

Remark 3.1.8. From [82, Lemma 2.1] we know that if $u_1, \ldots, u_t \in \mathbb{F}_{2^n}^*$ are linearly independent over $\mathbb{F}_2$ and $f \in \mathbb{F}_2[X_1, \ldots, X_t]$ is a reduced polynomial of algebraic degree d, then $f(Tr_1^n(u_1x), \ldots, Tr_1^n(u_tx))$ is also of algebraic degree d. Hence, the algebraic degree of $\mathbf{H}$ is

$$\deg(\mathbf{H}) = \max_{\lambda \in \mathbb{F}_{2^t}^*} \deg(\mathbf{H}_\lambda)$$

Remark 3.1.9. (CCZ-equivalence) From [12, Theorem 1], the CCZ-equivalence between bent (n, m)-functions coincides with EA-equivalence. Therefore, since $\mathbf{H}$ is not vectorial bent it follows that the functions G and $\mathbf{H}$ used in Construction 3.1.1 are always EA-inequivalent. Moreover, it is interesting to note that the vectorial bent function F is obtained by adding a nonlinear non-bent vectorial function $\mathbf{H}$ to a bent function G.

Example 3.1.10. Let us consider the bent $(8, 4)$-function

$$G(x) = \sum_{i=1}^{2^r-1} x^{(i2^{m-r}+1)(2^m-1)+1}$$

with $m = 4, r = 3$. $(G^*_\lambda)_{\lambda \in \mathbb{F}^*_{2^m}}$ satisfies the (P_U) property (3.2) with the defining set $U = \{u_1, \ldots, u_4\}$, where U forms a basis of $\mathbb{F}_{2^4}$ over $\mathbb{F}_2$. We note that $\deg(G) = 4$. Let us consider the functions $\mathbf{h}_1, \mathbf{h}_2, \mathbf{h}_3 : \mathbb{F}_{2^4} \to \mathbb{F}_{2^4}$ defined by

$$\begin{aligned}\mathbf{h}_1(X) &= X^3;\\ \mathbf{h}_2(X) &= X^3 + X^{13};\\ \mathbf{h}_3(X) &= X^3 + X^{13} + X^{15},\end{aligned}$$

where $\deg(\mathbf{h}_i) = i + 1$, for $i = 1, 2, 3$. Let F_i be the bent $(8, 4)$-function obtained from Construction 3.1.1 via G and $\mathbf{h}_i$. Using Sage and MAGMA we confirm that $\deg(F_i) = 4$. Furthermore, when considering the EA-equivalence between the functions we observe that F_i and G are EA-inequivalent, for $i = 1, 2, 3$. Moreover, the functions F_1 and F_3, F_2 and F_3 are EA-inequivalent, whereas F_1 and F_2 are EA-equivalent.

The following result is a direct consequence of the fact that the algebraic degree is an EA-invariant.

Proposition 3.1.11. *Using the same notation as in Construction 3.1.1, let F be a bent (n, m)-function constructed from G and $\mathbf{H}$. If $\deg(\mathbf{H}) > \deg(G)$, then F and G are EA-inequivalent.*

Proof. The result follows directly from

$$\deg(F) = \max\{\deg(\mathbf{H}), \deg(G)\} = \deg(\mathbf{H}) > \deg(G)$$

and the fact that the algebraic degree is invariant under EA-equivalence. □

We conclude the section with the following two questions.

Question 3.1.12. *What can we say about EA-equivalence between F and G, if F and G have the same algebraic degree?*

Question 3.1.13. *Let F_i be bent (n, m)-functions obtained from Construction 3.1.1 via G_i and $\mathbf{H}_i$, for $i = 1, 2$. Assuming that $\deg(F_1) = \deg(F_2)$, what can we say about the EA-equivalence between F_1 and F_2?*

From Example 3.1.10, we have observed that among the functions F_1, F_2 and F_3, the functions F_1 and F_2 were EA-equivalent, whilst the other pairings were EA-inequivalent. Thus, it is natural to ask, what choice of G or $\mathbf{H}$ affects this EA-equivalence.

3.2 New infinite families of vectorial bent functions

In [90], the authors constructed several infinite families of vectorial bent functions using certain vectorial bent functions G that satisfy the

property (3.2). The very same functions can be used to construct new families of vectorial bent functions via Construction 3.1.1. In addition, we consider vectorial bent functions from the Maiorana-McFarland class which were not considered in [90], but were considered by Tang *et al.*[82] in the construction of bent Boolean functions.

We summarise some useful results from [90] in the following theorem.

Theorem 3.2.1. *Let G be one of the following bent (n,m)-functions:*

(i) $G(x) = x^{2^m+1},\ n = 2m;$

(ii) $G(x) = \sum_{i=1}^{2^r-1} x^{(i2^{m-r}+1)(2^m-1)+1},\ n = 2m,\ \gcd(r,m) = 1;$

(iii) $G(x) = Tr_m^n(\omega x^{2^m+1}),\ n = 4m,\ m \geq 2$ *and* ω *is a generator of the cyclic group* $U = \{x \in \mathbb{F}_{2^{2m}} : x^{2^m+1} = 1\}$.

Then $(G_\lambda^*)_{\lambda\in\mathbb{F}_{2^m}^*}$ satisfies the (P_U) property (3.2) with the defining set

(i) $\{u_1,\ldots,u_m\} \subset \mathbb{F}_{2^n}^*$ *such that* $u_i u_j^{2^m} \in \mathbb{F}_{2^m}^*$ *for all* $1 \leq i < j \leq m;$

(ii) $\{u_1,\ldots,u_m\}$ *is a basis of* $\mathbb{F}_{2^m}$ *over* $\mathbb{F}_2;$

(iii) $\{u_1,\ldots,u_m\} \subset \mathbb{F}_{2^n}^*$ *such that* $u_i u_j^{2^m} \in \mathbb{F}_{2^m}^*$ *for all* $1 \leq i < j \leq m,$

respectively.

Theorem 3.2.2. *Let $G(x)$ be one of the three bent (n,m)-functions in Theorem 3.2.1, $\{u_1,\ldots,u_t\}$ the corresponding defining set for property (3.2) for $(G_\lambda^*)_{\lambda\in\mathbb{F}_{2^m}^*}$ and let t be a positive divisor of m. Let $\mathbf{h}(X_1,\ldots,X_t)$ be any vectorial Boolean function from $\mathbb{F}_2^t$ to $\mathbb{F}_{2^t}$. Then the function $F(x) = G(x) + \mathbf{H}(x)$, generated by Construction 3.1.1, is a bent (n,m)-function.*

Proof. The result is an immediate consequence of Construction 3.1.1, Theorem 3.1.3 and Theorem 3.2.1. □

Let us define $F : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ with $F(x,y) = x\pi(y) + g(y)$, where $\pi : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ is a permutation and $g : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ is an arbitrary function. A function defined in such a way belongs to the class of vectorial bent Maiorana-McFarland functions. Let $\lambda \in \mathbb{F}_{2^m}^*$ be arbitrary, we then have the component $F_\lambda(x,y) = Tr_1^m(\lambda x\pi(y) + \lambda g(y))$. Its corresponding dual is defined with (see [96]):

$$F_\lambda^*(x,y) = Tr_1^m\left(y\pi^{-1}(x/\lambda) + \lambda g(\pi^{-1}(x/\lambda)\right),$$

where π^{-1} is the inverse permutation of π. Motivated by [82, Section E], we will consider two subclasses of the vectorial Maiorana-McFarland class which satisfy the (P_U) property (3.2).

Following the methodology in [82], we note that (3.2) can be written in bivariate form as follows:

$$G_\lambda^*\left(x+\sum_{i=1}^{t}\alpha_i w_i, y+\sum_{i=1}^{t}\beta_i w_i\right) = G_\lambda^*(x,y)+\sum_{i=1}^{t} w_i g_i(\alpha_i,\beta_i)$$

for all $(x,y) \in \mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$ and $(w_1,\ldots,w_t)\in\mathbb{F}_2^t$, where $0 \neq u_i = (\alpha_i,\beta_i)\in\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$ and g_i is a Boolean function from $\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$ to $\mathbb{F}_2$, $1\le i\le t$.

Since each linear function from $\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$ to $\mathbb{F}_2$ can be written as $Tr_1^m(ux+vy)$, where $(u,v)\in\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$, the vectorial Boolean function in (4.2) by Construction 3.1.1 can be rewritten as:

$$F(x,y) = G(x,y)+\mathbf{h}\left(Tr_1^m(\alpha_i x+\beta_i y),\ldots,Tr_1^m(\alpha_t x+\beta_t y)\right).$$

Lemma 3.2.3. *Let $u_i=(\alpha_i,\beta_i)\in\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$ be linearly independent elements over $\mathbb{F}_2$, where $1\le t\le m$. Let $G(x,y)=y\pi(x)$, where π is a linear permutation over $\mathbb{F}_{2^m}$. If $Tr_1^m\left(\beta_i\pi^{-1}\left(\frac{\alpha_j}{\lambda}\right)+\beta_j\pi^{-1}\left(\frac{\alpha_i}{\lambda}\right)\right)=0$ for each $1\le i<j\le t$ and $\lambda\in\mathbb{F}_{2^m}^*$, then the dual component G_λ^* satisfies (3.2) with*

$$g_i(x,y) = Tr_1^m\left(y\pi^{-1}\left(\frac{\alpha_i}{\lambda}\right)+\beta_i\pi^{-1}\left(\frac{x}{\lambda}\right)+\beta_i\pi\left(\frac{\alpha_i}{\lambda}\right)\right). \tag{3.9}$$

Proof. Let $X = x+\sum_{i=1}^t w_i\alpha_i$ and $Y = y+\sum_{i=1}^t w_i\beta_i$. It follows from (3.2) and the fact that π is linear that

$$\begin{aligned}
G_\lambda^*(X,Y) &= Tr_1^m\left(\left(y+\sum_{i=1}^t w_i\beta_i\right)\pi^{-1}\left(\frac{x}{\lambda}+\sum_{i=1}^t w_i\frac{\alpha_i}{\lambda}\right)\right)\\
&= G_\lambda^*(x,y)+\sum_{i=1}^t w_i Tr_1^m\left(y\pi^{-1}\left(\frac{\alpha_i}{\lambda}\right)+\beta_i\pi^{-1}\left(\frac{x}{\lambda}\right)\right)+\\
&+\sum_{i=1}^t Tr_1^m\left(w_i^2\beta_i\pi\left(\frac{\alpha_i}{\lambda}\right)\right)+\sum_{1\le i<j\le t} w_i w_j Tr_1^m\left(\beta_i\pi^{-1}\left(\frac{\alpha_j}{\lambda}\right)+\beta_j\pi^{-1}\left(\frac{\alpha_i}{\lambda}\right)\right)\\
&= G_\lambda^*(x,y)+\sum_{i=1}^t w_i Tr_1^m\left(y\pi^{-1}\left(\frac{\alpha_i}{\lambda}\right)+\beta_i\pi^{-1}\left(\frac{x}{\lambda}\right)+\beta_i\pi\left(\frac{\alpha_i}{\lambda}\right)\right)+\\
&+\sum_{1\le i<j\le t} w_i w_j Tr_1^m\left(\beta_i\pi^{-1}\left(\frac{\alpha_j}{\lambda}\right)+\beta_j\pi^{-1}\left(\frac{\alpha_i}{\lambda}\right)\right)\\
&= G_\lambda^*(x,y)+\sum_{i=1}^t w_i g_i(x,y)+\sum_{1\le i<j\le t} w_i w_j Tr_1^m\left(\beta_i\pi^{-1}\left(\frac{\alpha_j}{\lambda}\right)+\beta_j\pi^{-1}\left(\frac{\alpha_i}{\lambda}\right)\right),
\end{aligned}$$

where g_i is defined by (3.9). The conclusion follows from the assumption that

$$Tr_1^m\left(\beta_i\pi^{-1}\left(\frac{\alpha_j}{\lambda}\right)+\beta_j\pi^{-1}\left(\frac{\alpha_i}{\lambda}\right)\right)=0,$$

for each $1 \leq i < j \leq t$ and $\lambda \in \mathbb{F}_{2^m}^*$. □

The following result is an immediate consequence of Lemma 3.2.3.

Corollary 3.2.4. *Let $\alpha_1, \ldots, \alpha_t \in \mathbb{F}_{2^m}^*$ be linearly independent elements over $\mathbb{F}_2$, $1 \leq t \leq m$. Denote $u_i = (\alpha_i, 0)$ and let $G(x, y) = y\pi(x)$, where π is a linear permutation over $\mathbb{F}_{2^m}$. Then, the dual component G_λ^* satisfies* (3.2) *with*

$$g_i(x, y) = Tr_1^m\left(y\pi^{-1}\left(\frac{\alpha_i}{\lambda}\right)\right),$$

for any $\lambda \in \mathbb{F}_{2^m}^*$.

The use of non-quadratic vectorial bent functions in the Maiorana-McFarland class in Construction 3.1.1 is given below.

Proposition 3.2.5. *Let s be a positive divisor of m such that m/s is odd. Let $u_i = (\alpha_i, \beta_i) \in \mathbb{F}_{2^s} \times \mathbb{F}_{2^s}$ be linearly independent elements over $\mathbb{F}_2$, where $1 \leq t \leq m$. Let $G(x, y) = x\pi(y)$, where $\pi(y) = ay^d$ for a positive integer d such that $d(2^s + 1) \equiv 1 \pmod{2^m - 1}$ and $a \in \mathbb{F}_{2^m}^*$. If $\alpha_i\beta_j + \alpha_j\beta_i = 0$ and $Tr_1^m(\beta_i\alpha_j^2 + \beta_j\alpha_i^2) = 0$ for any $1 \leq i < j \leq t$ and $\lambda \in \mathbb{F}_{2^m}^*$, then the dual component G_λ^* satisfies* (3.2) *with*

$$g_i(x, y) = Tr_1^m\left(\frac{y}{(a\lambda)^{2^s+1}}\left(\alpha_i^2 + \alpha_i x + \alpha_i x^{2^s}\right) + \frac{1}{(a\lambda)^{2^s+1}}\left(\beta_i\alpha_i x + \beta_i\alpha_i x^{2^s} + \beta_i\alpha_i^2\right)\right). \tag{3.10}$$

Proof. Since $\pi^{-1}(x) = x^{2^s+1}$, we have that $G_\lambda^*(x, y) = Tr_1^m\left(y\left(\frac{x}{\lambda}\right)^{2^s+1}\right)$. Let $X = x + \sum_{i=1}^t w_i\alpha_i$ and $Y = y + \sum_{i=1}^t w_i\beta_i$. It follows from (3.2) and the fact that $\alpha_i^{2^s} = \alpha_i, \beta_i^{2^s} = \beta_i$, that

$$\begin{aligned}
G_\lambda^*(X, Y) &= Tr_1^m\left(\left(y + \sum_{i=1}^t w_i\beta_i\right)\left(\frac{x}{a\lambda} + \sum_{i=1}^t w_i\frac{\alpha_i}{a\lambda}\right)^{2^s+1}\right) \\
&= Tr_1^m\left(\left(y + \sum_{i=1}^t w_i\beta_i\right)\left(\frac{x}{a\lambda} + \sum_{i=1}^t w_i\frac{\alpha_i}{a\lambda}\right)^{2^s}\left(\frac{x}{a\lambda} + \sum_{i=1}^t w_i\frac{\alpha_i}{a\lambda}\right)\right) \\
&= Tr_1^m\left(y\left(\frac{x}{a\lambda}\right)^{2^s+1} + y\frac{x}{a\lambda}\sum_{i=1}^t w_i\left(\frac{\alpha_i}{a\lambda}\right)^{2^s} + y\left(\frac{x}{a\lambda}\right)^{2^s}\sum_{i=1}^t w_i\frac{\alpha_i}{a\lambda} + y\sum_{i=1}^t w_i\left(\frac{\alpha_i}{a\lambda}\right)^{2^s+1}\right. \\
&\quad + \sum_{i=1}^t w_i\beta_i\left(\frac{x}{a\lambda}\right)^{2^s+1} + \sum_{i=1}^t w_i\beta_i\frac{x}{a\lambda}\sum_{j=1}^t w_j\left(\frac{\alpha_j}{a\lambda}\right)^{2^s} + \sum_{i=1}^t w_i\beta_i\left(\frac{x}{a\lambda}\right)^{2^s}\sum_{j=1}^t w_j\frac{\alpha_j}{a\lambda} \\
&\quad \left. + \sum_{i=1}^t w_i\beta_i\left(\frac{\alpha_i}{a\lambda}\right)^{2^s+1}\right) = G_\lambda^*(x, y) + \sum_{i=1}^t w_i Tr_1^m\left(\frac{y}{(a\lambda)^{2^s+1}}\left(\alpha_i^2 + \alpha_i x + \alpha_i x^{2^s}\right)\right) + \\
&\quad + \sum_{i=1}^t\sum_{j=1}^t w_i w_j Tr_1^m\left(\frac{1}{(a\lambda)^{2^s+1}}\left(\beta_i\alpha_j x + \beta_i\alpha_j x^{2^s} + \beta_i\alpha_j^2\right)\right)
\end{aligned}$$

$$
\begin{aligned}
&= G^*_\lambda(x,y) + \sum_{i=1}^{t} w_i Tr_1^m\left(\frac{y}{(a\lambda)^{2^s+1}}\left(\alpha_i^2 + \alpha_i x + \alpha_i x^{2^s}\right)\right) + \\
&+ \sum_{i=1}^{t} w_i Tr_1^m\left(\frac{1}{(a\lambda)^{2^s+1}}\left(\beta_i\alpha_i x + \beta_i\alpha_i x^{2^s} + \beta_i\alpha_i^2\right)\right) \\
&+ \sum_{1\le i<j\le t} Tr_1^m\left((x^{2^s}+x)(\beta_i\alpha_j + \beta_j\alpha_i) + \beta_i\alpha_j^2 + \beta_j\alpha_i^2\right) \\
&= G^*_\lambda(x,y) + \sum_{i=1}^{t} w_i g_i(x,y) + \sum_{1\le i<j\le t} Tr_1^m\left((x^{2^s}+x)(\beta_i\alpha_j + \beta_j\alpha_i) + \beta_i\alpha_j^2 + \beta_j\alpha_i^2\right),
\end{aligned}
$$

where g_i is defined by (3.10). The conclusion follows immediately from the assumption that $\alpha_i\beta_j + \alpha_j\beta_i = 0$ and $Tr_1^m(\beta_i\alpha_j^2 + \beta_j\alpha_i^2) = 0$. □

Corollary 3.2.6. *Let s be a positive divisor of m such that m/s is odd. Let $\alpha_1, \ldots, \alpha_t \in \mathbb{F}_{2^s}^*$ be linearly independent elements over $\mathbb{F}_2$, $1 \le t \le m$, and define $u_i = (\alpha_i, 0)$. Let $G(x,y) = x\pi(y)$, where $\pi(y) = ay^d$ for a positive integer d such that $d(2^s+1) \equiv 1 \pmod{2^m-1}$ and $a \in \mathbb{F}_{2^m}^*$. Then, the dual component G^*_λ satisfies (3.2) with*

$$
g_i(x,y) = Tr_1^m\left(\frac{y}{(a\lambda)^{2^s+1}}\left(\alpha_i^2 + \alpha_i x + \alpha_i x^{2^s}\right)\right),
$$

for any $\lambda \in \mathbb{F}_{2^m}^*$.

Theorem 3.2.7. *Let $\alpha_1, \ldots, \alpha_t \in \mathbb{F}_{2^m}^*$ be linearly independent elements over $\mathbb{F}_2$, $t|m$. Let $G(x,y) = y\pi(x)$, where π is a linear permutation over $\mathbb{F}_{2^m}$, and let $\mathbf{h}$ be any vectorial Boolean function from $\mathbb{F}_2^t$ to $\mathbb{F}_{2^t}$. Then, the function $F : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ given by*

$$
F(x,y) = y\pi(x) + \mathbf{h}(Tr_1^m(\alpha_1 x), \ldots, Tr_1^m(\alpha_t x)),
$$

generated by Construction 3.1.1, is a bent (n,m)-function.

Proof. The result follows immediately from Theorem 3.1.3 and Corollary 3.2.4. □

Example 3.2.8. Let $G : \mathbb{F}_{2^4} \times \mathbb{F}_{2^4} \to \mathbb{F}_{2^4}$ be defined with $G(x,y) = xy$. Let $U = \{1, \beta, \beta^2, \beta^3\}$, where $\beta = \alpha^{17}$, and α be a root of the primitive polynomial $p(x) = x^8 + x^4 + x^3 + x^2 + 1 \in \mathbb{F}_{2^8}[x]$. Let $\mathbf{h} : \mathbb{F}_{2^4} \to \mathbb{F}_{2^4}$ be defined with $\mathbf{h}(X) = X^3$. From Theorem 3.2.7, the function

$$
F(x,y) = xy + \left(Tr_1^m(x) + \beta Tr_1^m(\beta x) + \beta^2 Tr_1^m(\beta^2 x) + \beta^3 Tr_1^m(\beta^3 x)\right)^3
$$

is a quadratic bent $(8,4)$-function EA-inequivalent to G.

Theorem 3.2.9. *Let s be a positive divisor of m such that m/s is odd. Let $\alpha_1, \ldots, \alpha_t \in \mathbb{F}_{2^s}^*$ be linearly independent elements over $\mathbb{F}_2$, $t|m$. Let $G(x,y) = x\pi(y)$, where $\pi(y) = ay^d$ for a positive integer d such that*

$d(2^s+1) \equiv 1 \pmod{2^m-1}$ and $a \in \mathbb{F}_{2^m}^*$, and let $\mathbf{h}$ be any vectorial Boolean function from $\mathbb{F}_2^t$ to $\mathbb{F}_{2^t}$. Then, the function $F : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ given by

$$F(x,y) = axy^d + \mathbf{h}(Tr_1^m(\alpha_1 x), \ldots, Tr_1^m(\alpha_t x)),$$

generated by Construction 3.1.1, is a bent (n,m)-function.

Proof. The result follows immediately from Theorem 3.1.3 and Corollary 3.2.6. □

3.3 New families of (n,n)-functions with maximal number of bent components

In 2018 Pott *et al.* [73] proved that an (n,n)-function, $n = 2m$, can have at most $2^n - 2^m$ bent components. Furthermore, by studying these objects, they have found a new infinite class of bent (n,m)-functions of the form

$$F_\alpha^i(x) = Tr_m^n(\alpha x^{2^i}(x + x^{2^k})),$$

where $\alpha \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$. Later, Mesnager *et al.* [60] presented a class of (n,n)-functions with maximal number of bent components CCZ-inequivalent to F_α^i and this topic was also treated by Zheng et al. [90].

A generic method of generating new vectorial plateaued $(n, m+t)$-functions with maximal number of bent components, where $n = 2m$ and $t > 1$, was given in [90]. More precisely, given a bent (n,m)-function G, under certain conditions, the $(n, m+t)$-function

$$T_1(x) = (G(x), f_1(x), \ldots, f_t(x))$$

is vectorial plateaued if and only if the (n,t)-function $(f_1(x), \ldots, f_t(x))$ is vectorial plateaued. For certain choices of the vectorial bent function G, it was shown that T_1 has the maximal number of bent components. In the same article, the authors also showed that the (n,n)-functions

$$T_2 = \left(G(x), Tr_1^n(u_1 x), Tr_1^n(u_1 x) Tr_1^n(u_2 x), \ldots, \prod_{i=1}^{m} Tr_1^n(u_i x) \right),$$

under additional conditions and certain choices of the bent (n,m)-function G, also have the maximal number of bent components.

Definition 3.3.1. F is said to be an (n,m)-MNBC, $m \geq n/2$ function if it has $2^m - 2^{m-n/2}$ bent components.

In the rest of this section, we present a new method to construct (n,n)-functions with maximal number of bent components. We note that the functions T_1 and T_2 above are constructed by extending a bent (n,m)-function G through addition of suitably chosen coordinates, whereas in our method we are summing a bent (n,m)-function G and some (n,n)-function $\mathbf{H}'$.

Construction 3.3.2. Let $u_1, \ldots, u_t \in \mathbb{F}_{2^n}^*$ be linearly independent elements over $\mathbb{F}_2$, where $n = 2m$ and $t|m$. Let G be a bent (n, m)-function such that $(G_\lambda^*)_{\lambda \in \mathbb{F}_{2^m}^*}$ satisfies the (P_U) property (3.2). Let $\mathbf{h}(X_1, \ldots, X_t)$ be any vectorial Boolean Function from $\mathbb{F}_2^t$ to $\mathbb{F}_{2^t}$. Construct an (n, n)-function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ via G and $\mathbf{h}$ as follows:

$$F(x) = G(x) + \mathbf{H}'(x),$$

where $\mathbf{H}' \colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is defined by

$$\mathbf{H}'(x) = \gamma \mathbf{h}(Tr_1^n(u_1 x), \ldots, Tr_1^n(u_t x))$$

and $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$. Equivalently, if $\mathbf{h}$ is defined using the finite field notation, then F can be written as

$$\begin{aligned} F(x) &= G(x) + \mathbf{H}'(x) \\ &= G(x) + \gamma \mathbf{h}(Tr_1^n(u_1 x) + \alpha Tr_1^n(u_2 x) + \cdots + \alpha^{t-1} Tr_1^n(u_t x)), \end{aligned}$$

where α is a primitive element of $\mathbb{F}_{2^t}$.

Theorem 3.3.3. *Let F be an (n, n)-function, $n = 2m$, generated by Construction 2. Then, F has $2^n - 2^m$ bent components.*

Proof. Let $G(x) = (f_1(x), \ldots, f_m(x))$, where $f_1, \ldots, f_m : \mathbb{F}_{2^n} \to \mathbb{F}_2$ are the coordinates of G. Without loss of generality, we can extend G to an (n, n)-function with $G(x) = (f_1, \ldots, f_m, 0, \ldots, 0)$. For $\lambda \in \mathbb{F}_{2^n}^*$, we have that G_λ is not bent if and only if $Tr_1^n(\lambda G(x)) = 0$, or equivalently, if $\lambda \in \mathbb{F}_{2^m}^*$. Hence, the number of bent components is $2^n - 1 - (2^m - 1) = 2^n - 2^m$. Let $\lambda \in \mathbb{F}_{2^n}$ such that G_λ is bent. We have that

$$F_\lambda(x) = G_\lambda(x) + Tr_1^n(\lambda \mathbf{H}'(x))$$

is also bent, by the result of Tang *et al.* [82] and the fact that $Tr_1^n(\lambda \mathbf{H}')$ is a Boolean function. The number of bent components of F equals to the number of bent components of G, which is $2^n - 2^m$. Hence F is an (n, n)-function with maximal number of bent components. □

Theorem 3.3.4. *Let $G(x)$ be one of the bent (n, m)-functions in Theorem 3.1.3, 3.2.7 or 3.2.9 and let $\{u_1, \ldots, u_t\}$ (with $t|m$) be its corresponding defining set for the property (3.2). Let $\mathbf{h}(X_1, \ldots, X_t)$ be any vectorial Boolean function from $\mathbb{F}_2^t$ to $\mathbb{F}_{2^t}$. Then the function $F(x) = G(x) + \mathbf{H}'(x)$, generated by Construction 2, is an (n, n)-function with maximal number of bent components.*

Proof. The result follows immediately from Theorem 3.3.3 and Construction 2. □

Chapter 4

Secondary constructions of vectorial p-ary weakly regular bent functions via the (P_U) property

In [74], the results of Tang et al. introduced in Chapter 3, were generalized for the construction of several infinite families of p-ary weakly regular bent functions. In this chapter, we further generalize these results to obtain a secondary construction of vectorial p-ary weakly regular bent and plateaued functions of the form

$$F(x) = G(x) + \mathbf{H}(x),$$

where G is a suitable p-ary weakly regular bent (n, m)-function and $\mathbf{H}$ is a p-ary (n, t)-function. Furthermore, we give a characterization of the (P_U) property for the p-ary case via second-order derivatives, as it was done for the Boolean case in [90]. The rest of the chapter is organized as follows. In Section 4.1 we give our main construction of vectorial p-ary weakly regular bent and plateaued functions. Some new infinite families of vectorial p-ary weakly regular bent functions via the p-ary Maiorana-McFarland class are presented in Section 4.2. We also show that certain monomial p-ary weakly regular bent (n, m)-functions cannot be used for this construction, as it was the case for $p = 2$ in [4, 82, 90].

4.1 Generic construction of vectorial p-ary bent functions

Similarly as in the binary case, with G_λ^* we denote the dual of the p-ary bent component G_λ, $\lambda \in \mathbb{F}_{p^m}^*$, of a vectorial p-ary bent function $G : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$, $m|n$.

Construction 4.1.1. Let $u_1, \ldots, u_t \in \mathbb{F}_{p^n}^*$ be linearly independent elements over $\mathbb{F}_p$, where $m|n$ and $t|m$. Let $G : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ be any p-ary

weakly regular bent function whose components $G_\lambda(x) = tr_m(\lambda G(x))$, with $\lambda \in \mathbb{F}_{p^m}^*$, satisfy

$$G_\lambda^*\left(x + \sum_{i=1}^{t} u_i w_i\right) = G_\lambda^*(x) + \sum_{i=1}^{t} w_i g_i(x) \tag{4.1}$$

for all $x \in \mathbb{F}_{p^n}$ and $(w_1, \ldots, w_t) \in \mathbb{F}_p^t$, where $g_i(x)$ is a p-ary function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$, $1 \leq i \leq t$.

Let $\mathbf{h}(X_1, \ldots, X_t)$ be any vectorial p-ary function from $\mathbb{F}_p^t$ to $\mathbb{F}_{p^t}$. Define $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$, using G and $\mathbf{h}$, as

$$F(x) = G(x) + \mathbf{H}(x), \tag{4.2}$$

where $\mathbf{H} : \mathbb{F}_{p^n} \to \mathbb{F}_{p^t}$ is defined by $\mathbf{H}(x) = \mathbf{h}(tr_n(u_1 x), \ldots, tr_n(u_t x))$. Equivalently, if $\mathbf{h}$ is defined using the finite field notation so that $\mathbf{h} : \mathbb{F}_{p^t} \to \mathbb{F}_{p^t}$, then define

$$\begin{aligned} F(x) &= G(x) + \mathbf{H}(x) \\ &= G(x) + \mathbf{h}(tr_n(u_1 x) + \alpha tr_n(u_2 x) + \cdots + \alpha^{t-1} tr_n(u_t x)), \end{aligned}$$

where α is a primitive element of $\mathbb{F}_{p^t}$.

Remark 4.1.2. Similarly as for the binary case, we will say that $(G_\lambda^*)_{\lambda \in \mathbb{F}_{p^{m^*}}}$ satisfies the (P_U) *property* (with the *defining set* $U = \{u_1, \ldots, u_t\}$).

Remark 4.1.3. We note that in this case $\mathbf{h}$ can be a function in $\mathcal{B}_p^n$. This cooresponds to the p-ary case of [90, Theorem 3.3].

Using this construction, we prove the following result which is the p-ary equivalent of Theorem 3.1.3.

Theorem 4.1.4. *The function F generated by Construction 4.1.1 is a p-ary weakly regular bent (n, m)-function.*

Proof. Let $\lambda \in \mathbb{F}_{p^m}^*$ be arbitrary. Let us consider the component G_λ and let $\mathbf{h}_\lambda : \mathbb{F}_p^t \to \mathbb{F}_{p^t}$ be defined as $\mathbf{h}_\lambda = tr_m(\lambda \mathbf{h})$. From the inverse GWHT, we have that

$$\xi_p^{\mathbf{h}_\lambda(X_1, \ldots, X_t)} = p^{-t} \sum_{(w_1, \ldots, w_t) \in \mathbb{F}_p^t} \mathcal{H}_{\mathbf{h}_\lambda}(w_1, \ldots, w_t)(-1)^{\sum_{i=1}^{t} w_i X_i}.$$

For any $x \in \mathbb{F}_{p^n}$ and $1 \leq i \leq t \leq m$, taking $X_i = tr_n(u_i x)$, we obtain

$$\xi_p^{\mathbf{h}_\lambda(tr_n(u_1 x), \ldots, tr_n(u_t x))} = p^{-t} \sum_{(w_1, \ldots, w_t) \in \mathbb{F}_p^t} \mathcal{H}_{\mathbf{h}_\lambda}(w_1, \ldots, w_t) \xi_p^{tr_n\left(\left(\sum_{i=1}^{t} w_i u_i\right) x\right)}. \tag{4.3}$$

Multiplying both sides of (4.3) by $\xi^{G_\lambda(x)+tr_n(\beta x)}$, we have

$$\xi^{G_\lambda(x)+\mathbf{H}_\lambda(x)+tr_n(\beta x)} = p^{-t} \sum_{(w_1,\ldots,w_t)\in\mathbb{F}_p^t} \mathcal{H}_{\mathbf{h}_\lambda}(w_1,\ldots,w_t)\xi_p^{G_\lambda(x)+tr_n\left(\left(\beta+\sum_{i=1}^t w_iu_i\right)x\right)}.$$

By summing the previous expression on both sides over all $x \in \mathbb{F}_{p^n}$ and using the fact that G is p-ary weakly regular bent, we obtain that

$$\begin{aligned}\mathcal{H}_{F_\lambda}(\beta) &= p^{-t} \sum_{(w_1,\ldots,w_t)\in\mathbb{F}_p^t} \mathcal{H}_{\mathbf{h}_\lambda}(w_1,\ldots,w_t)\mathcal{H}_{G_\lambda}(\beta+\sum_{i=1}^t u_iw_i) \\ &= p^{-t+n/2}z \sum_{(w_1,\ldots,w_t)\in\mathbb{F}_p^t} \mathcal{H}_{\mathbf{h}_\lambda}(w_1,\ldots,w_t)\xi_p^{G_\lambda^*(\beta+\sum_{i=1}^t u_iw_i)}, \qquad (4.4)\end{aligned}$$

where $z \in \mathcal{C}$ such that $|z| = 1$. It follows from (4.1) and (4.4) that

$$\mathcal{H}_{F_\lambda}(\beta) = p^{-t+n/2}z\xi^{G_\lambda^*(\beta)} \sum_{(w_1,\ldots,w_t)\in\mathbb{F}_p^t} \mathcal{H}_{\mathbf{h}_\lambda}(w_1,\ldots,w_t)\xi_p^{\sum_{i=1}^t w_ig_i(\beta)}.$$

The sum on the right-hand side corresponds to the inverse GWHT of $\mathbf{h}_\lambda$ at the point $(g_1(\beta),\ldots,g_t(\beta))$ and thus we have

$$\mathcal{H}_{F_\lambda}(\beta) = p^{n/2}z\xi_p^{G_\lambda^*(\beta)+\mathbf{h}_\lambda(g_1(\beta),g_2(\beta),\ldots,g_t(\beta))}.$$

Since $\beta \in \mathbb{F}_{p^n}$ is arbitrary, we have that F_λ is p-ary weakly regular bent for all $\lambda \in \mathbb{F}_{p^m}^*$. In other words, F is a p-ary weakly regular bent (n,m)-function. □

Remark 4.1.5. If we have a function $f : X \to Y$, then the number of possible functions f equals to $\#Y^{\#X}$. Thus, since $\mathbf{h}$ is a p-ary (t,t)-function, there are p^{tp^t} possible choices for $\mathbf{h}$. Hence, we can construct at most p^{tp^t} p-ary bent (n,m)-functions F from a fixed bent function G and an arbitrary function $\mathbf{h}$. In the case when $p = 3, n = 4$ and $m = t = 2$, we have 3^{18} possibilities.

Similarly, as noted in [90] for the Boolean case, we can use Construction 4.1.1 to obtain new instances of plateaued p-ary (n,m)-functions.

Corollary 4.1.6. *With the same conditions as in Theorem 4.1.4, let l be any positive integer. Let $\mathbf{h}_i$ be any reduced polynomial in $\mathbb{F}_p[X_1,\ldots,X_n]$, for $i = 1,\ldots,l$. Then*

$$F(x) = (G(x), \mathbf{h}_1(tr_n(u_1x),\ldots,tr_n(u_2x)),\ldots,\mathbf{h}_l(tr_n(u_1x),\ldots,tr_n(u_2x)))$$

is a plateaued p-ary $(n, m+l)$-function if and only if the p-ary (n,l)-function

$$x \mapsto (\mathbf{h}_1(tr_n(u_1x),\ldots,tr_n(u_2x)),\ldots,\mathbf{h}_l(tr_n(u_1x),\ldots,tr_n(u_2x))),$$

$x \in \mathbb{F}_{p^n}$, is plateaued.

Proof. For any $v \in \mathbb{F}_p^t$ the function $\langle v, (\mathbf{h}_1, \ldots, \mathbf{h}_l)\rangle$ is again a reduced polynomial, and thus by Theorem 1, the p-ary function $\langle(\lambda, v), F\rangle$ is bent for all $\lambda \in \mathbb{F}_{p^m}^*$. Hence, F is plateaued if and only if all the components $\langle(0, v), (\mathbf{h}_1, \ldots, \mathbf{h}_l)\rangle$ are plateaued for $v \neq 0$, or equivalently, if $x \mapsto (\mathbf{h}_1, \ldots, \mathbf{h}_l)$, $x \in \mathbb{F}_{p^n}$, is a plateaued p-ary (n, l)-function. □

Before providing instances of new vectorial p-ary weakly regular bent functions, we will provide another characterisation of the (P_U) property via second-order derivatives, as it was done by Zheng et. al for the binary case in [90].

Lemma 4.1.7. *Let $g \in \mathcal{B}_p^n$ be any p-ary weakly regular bent function. Then the following statements are equivalent.*

(i) There exist $u_1, \ldots, u_t \in \mathbb{F}_{p^n}$ and $g_1, \ldots, g_t \in \mathcal{B}_p^n$ such that

$$g\left(x + \sum_{i=1}^{t} w_i u_i\right) = g(x) + \sum_{i=1}^{t} w_i g_i(x), \tag{4.5}$$

for all $w = (w_1, \ldots, w_t) \in \mathbb{F}_{p^t}$.

(ii) $D_{u_i} D_{u_j} g \equiv 0$ for all $1 \leq i, j \leq t$.

Proof. $(i \Rightarrow ii)$ As w is arbitrary, let us take $w = e_i$, where $e_i = (e_0, \ldots, e_t)$ with $e_k = 1$ for $k = i$, and $e_k = 0$, otherwise, for $1 \leq k \leq t$. Then (4.5) becomes $g(x + u_i) = g(x) + g_i(x)$, or equivalently,

$$g_i(x) = g(x + u_i) - g(x) = D_{u_i} g(x).$$

Similarly, for any $1 \leq i, j \leq t$, we deduce that

$$\begin{aligned} g(x + u_i + u_j) &= g(x) + g_i(x) + g_j(x) \\ &= -g(x) + (g(x + u_i) + g(x + u_j)) \\ \Rightarrow & D_{u_i} D_{u_j} g(x) = 0, \text{ for any } x \in \mathbb{F}_{p^n}. \end{aligned}$$

$(ii \Rightarrow i)$ Let us define $g_i := D_{u_i} g$, for $i = 1, \ldots, t$. Let $q \in \mathbb{F}_p$ and $1 \leq i \leq t$ be arbitrary. We will show that that $g(x + qu_i) = g(x) + qD_{u_i} g(x)$, for all $x \in \mathbb{F}_{p^n}$. From the assumption that $D_{u_i} D_{u_j} g \equiv 0$ and taking $i = j$, we have that

$$\begin{aligned} & g(x + 2u_i) - 2g(x + u_i) + g(x) = 0 \\ \Rightarrow\ & g(x + 2u_i) = -g(x) + 2g(x + u_i) = g(x) + 2D_{u_i} g(x). \end{aligned} \tag{4.6}$$

If we change x with $x + u_i$ in (4.6), then:

$$g(x + 3u_i) - 2g(x + 2u_i) + g(x + u_i) = 0. \tag{4.7}$$

Furthermore, from (4.6) and (4.7), we also note that

$$\begin{aligned} g(x+3u_i) &= 2(g(x)+2D_{u_i}g(x)) - g(x+u_i) \\ &= g(x) + 4D_{u_i}g(x) - D_{u_i}g(x) \\ &= g(x) + 3D_{u_i}g(x) \end{aligned} \tag{4.8}$$

If we continue inductively, we observe that $g(x+qu_i) = g(x)+3D_{u_1}g(x)$ holds indeed for all $x \in \mathbb{F}_{p^n}$ and all $q \in \mathbb{F}_p$. Assume now that $1 \leq i, j \leq t$ and $w_i, w_j \in \mathbb{F}_p$ are arbitrary. Since $g(x+qu_i) = g(x) + qD_{u_i}g(x)$ holds for all $q \in \mathbb{F}_p$ and $1 \leq i \leq t$, we have that

$$\begin{aligned} g(x+w_iu_i+w_ju_j) &= g((x+w_iu_i)+w_ju_j) \\ &= g(x+w_iu_i) + w_jD_{u_j}g(x+w_iu_i) \\ &= g(x) + w_iD_{u_i}g(x) + w_j(g(x+w_iu_i+u_j) \\ &- g(x+w_iu_i)) \\ &= g(x) + w_iD_{u_i}g(x) + w_j\left(g(x+u_j) + w_iD_{u_i}g(x+u_j)\right) \\ &-g(x) - w_iD_{u_i}g(x)) \\ &= g(x) + w_iD_{u_i}g(x) + w_j\left(D_{u_j}g(x) + w_iD_{u_j}D_{u_i}g(x)\right) \\ &= g(x) + w_iD_{u_i}g(x) + w_jD_{u_j}g(x) \end{aligned}$$

Using mathematical induction, it is easy to show that (4.5) holds for all $(w_1, \ldots, w_t) \in \mathbb{F}_{p^t}$ and all $x \in \mathbb{F}_{p^n}$. □

Remark 4.1.8. We note that the functions g_i in (4.5) are exactly the derivatives $D_{u_i}g$, $i = 1, \ldots, t$.

4.2 New infinite families of vectorial p-ary weakly regular bent functions

Using similar methods as in [4, 74, 82, 90], we will present certain classes of p-ary vectorial weakly regular bent functions whose components satisfy the (P_U) property and thus may be used for the construction of new p-ary weakly regular bent and plateaued functions via Construction 4.1.1. We note that the proofs are analogous to the proofs in binary case as seen in Chapter 3. Before that, we present some observations on certain monomial weakly regular bent functions and their connection to the (P_U) property.

4.2.1 Observations on monomial p-ary weakly regular bent functions

Let $n = 2m$. Since functions of the form $x \mapsto tr_m(\lambda x^{p^m+1})$, $x \in \mathbb{F}_{p^n}$ are p-ary weakly regular bent for $\lambda \in \mathbb{F}^*_{p^m}$ (see e.g. [49]), the function F defined

by $G(x) = x^{p^m+1}$ is a vectorial p-ary weakly regular bent function. From [36], we know that the dual of G_λ is defined as $G^*_\lambda(x) = -tr_m\left(\frac{x^{p^m+1}}{\lambda^{p^m}+\lambda}\right)$. From [74, Theorem 3.4], the component G^*_λ satisfies the property (P_U) if

$$tr_m\left(\frac{u_i^{p^m}u_j + u_i u_j^{p^m}}{\lambda^{p^m}+\lambda}\right) = 0,$$

for all $u_i, u_j \in U \subseteq \mathbb{F}_{p^n}$ with $|U| = t|m$. Thus, for $i = j$, we must have that $tr_m(2(\lambda^{p^m}+\lambda)^{-1}u_i^{p^m+1}) = 0$ for all $1 \leq i \leq t$. If we want to construct a vectorial p-ary bent function F from G via Construction 4.1.1, then the above equality has to hold for all $\lambda \in \mathbb{F}^*_{p^m}$. Thus, we must have that $u_i^{p^m+1} = 0$ and consequently $u_i = 0$ for all $1 \leq i \leq t$. Hence, one cannot construct a vectorial p-ary weakly regular bent (n, m)-function via the Kasami function G.

Similarly, let us we consider the function $G(x) = x^2$ on $\mathbb{F}_{p^n}$. The duals of its components $G_\lambda(x) = tr_n(\lambda x^2)$ are defined by $G^*_\lambda(x) = -tr(\frac{x^2}{4\lambda})$, for $\lambda \in \mathbb{F}^*_{p^n}$. Suppose $U \subset \mathbb{F}_{p^n}$ denotes the set from Construction 4.1.1. From Lemma 4.1.7, we must have $D_u D_v G^*_\lambda \equiv 0$, for all $u, v \in U$, and consequently, for all $\lambda \in \mathbb{F}^*_{p^n}$. Let $u, v \in U$ be arbitrary, then

$$\begin{aligned} D_u D_v G^*_\lambda g(x) &= -tr_n\left(\frac{x^2 - (x+u)^2 - (x+u)^2 + (x+2u)^2}{4\lambda}\right) \\ &= -tr\left(\frac{2uv}{4\lambda}\right) = -tr\left(\frac{uv}{2\lambda}\right). \end{aligned}$$

Thus, we must have that $tr\left(\frac{uv}{2\lambda}\right) = 0$ for all $u, v \in U$ and all $\lambda \in \mathbb{F}^*_{p^n}$. Specially, if $u = v$, then we have that $tr\left(\frac{u^2}{2\lambda}\right) = 0$. However, this is only possible if $u = 0$. In other words, we cannot construct vectorial p-ary bent functions via G and Construction 4.1.1. Consequently, we have the following remark.

Remark 4.2.1. If G is a vectorial p-ary weakly regular bent function defined as $G(x) = x^{p^m} + 1$ or $G(x) = x^2$, for $x \in \mathbb{F}_{p^n}$, then one cannot construct new vectorial p-ary weakly regular bent functions via Construction 4.1.1.

Based on this observation, we have the following interesting open problem.

Question 4.2.2. *Can we find an exponent d such that $G(x) = x^d$ is a monomial p-ary weakly regular bent function and all of its components satisfy the (P_U) property?*

4.2.2 New infinite families of vectorial p-ary weakly regular bent functions from the p-ary Maiorana-McFarland class

Let $n = 2m$ and let us identify $\mathbb{F}_{p^n}$ with $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$. The well known Maiorana-McFarland class of vectorial p-ary bent functions can be defined as

$$F(x, y) = x\pi(y) + g(y),\ x, y \in \mathbb{F}_{p^m},$$

where $\pi : \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ is a permutation and $g \in \mathcal{B}_p^n$ is an arbitrary p-ary function. Let $\lambda \in \mathbb{F}_{p^m}^*$ be arbitrary, then $F_\lambda(x, y) = tr_m(\lambda x\pi(y) + \lambda g(y))$. Its corresponding dual is defined with (see [96]):

$$F_\lambda^*(x, y) = tr_m\left(-y\pi^{-1}(x/\lambda) + \lambda g(\pi^{-1}(x/\lambda))\right),$$

where π^{-1} is the inverse permutation of π. Following the methodology in [74], we note that for $\alpha = (a_1, a_2), \beta = (b_1, b_2) \in \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$, the scalar product $tr_m(\alpha\beta)$ can be defined as $tr_m(a_1b_1 + a_2b_2)$.

In [74] the authors considered the p-ary case for linearized polynomials. In the following results, we extend this notion to the vectorial p-ary case and obtain new instances of vectorial p-ary weakly regular bent and plateaued functions. The vectorial p-ary function (4.2) in Construction 4.1.1 can be rewritten in bivariate form as:

$$F(x, y) = G(x, y) + \mathbf{h}\left(tr_m(\alpha_i x + \beta_i y), \ldots, tr_m(\alpha_t x + \beta_t y)\right),$$

where the elements $u_i \in U$ correspond to $u_i = (\alpha_i, \beta_i) \in \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$.

Lemma 4.2.3. *Let $n = 2m$ and $u_1, \ldots, u_t \in \mathbb{F}_{p^n}^*$ be linearly independent elements over $\mathbb{F}_p$, where $1 \leq t | m$. Denote $u_i = (\alpha_i, \beta_i) \in \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$. Let $G(x, y) = y\pi(x)$, where π is a linear permutation over $\mathbb{F}_{p^m}$. If $tr_m\left(\beta_i\pi^{-1}\left(\frac{\alpha_j}{\lambda}\right) + \beta_j\pi^{-1}\left(\frac{\alpha_i}{\lambda}\right)\right) = 0$ for each $1 \leq i, j \leq t$ and $\lambda \in \mathbb{F}_{p^m}^*$, then the dual component G_λ^* satisfies (4.1) with*

$$g_i(x, y) = -tr_m\left(y\pi^{-1}\left(\frac{\alpha_i}{\lambda}\right) + \beta_i\pi^{-1}\left(\frac{x}{\lambda}\right)\right). \tag{4.9}$$

Proof. Let $X = x + \sum_{i=1}^t w_i\alpha_i$ and $Y = y + \sum_{i=1}^t w_i\beta_i$. It follows from (4.1) and the fact that π is linear that

$$\begin{aligned} G_\lambda^*(X, Y) &= tr_m\left(-\left(y + \sum_{i=1}^t w_i\beta_i\right)\pi^{-1}\left(\frac{x}{\lambda} + \sum_{i=1}^t w_i\frac{\alpha_i}{\lambda}\right)\right) \\ &= G_\lambda^*(x, y) - \sum_{i=1}^t w_i tr_m\left(y\pi^{-1}\left(\frac{\alpha_i}{\lambda}\right) + \beta_i\pi^{-1}\left(\frac{x}{\lambda}\right)\right) \\ &\quad - \sum_{i=1}^t w_i^2 tr_k\left(\beta_i\pi^{-1}\left(\frac{\alpha_i}{\lambda}\right)\right) \end{aligned}$$

$$
\begin{aligned}
&- \sum_{1\le i<j\le t} w_i w_j tr_m\left(\beta_i \pi^{-1}\left(\frac{\alpha_j}{\lambda}\right) + \beta_j \pi^{-1}\left(\frac{\alpha_i}{\lambda}\right)\right) \\
&= G^*_\lambda(x,y) + \sum_{i=1}^{t} w_i g_i(x,y) - \sum_{i=1}^{t} w_i^2 tr_m\left(\beta_i \pi^{-1}\left(\frac{\alpha_i}{\lambda}\right)\right) - \\
&\sum_{1\le i<j\le t} w_i w_j tr_m\left(\beta_i \pi^{-1}\left(\frac{\alpha_j}{\lambda}\right) + \beta_j \pi^{-1}\left(\frac{\alpha_i}{\lambda}\right)\right),
\end{aligned}
$$

where g_i is defined by (3.9). The conclusion follows from the assumption that

$$tr_m\left(\beta_i \pi^{-1}\left(\frac{\alpha_j}{\lambda}\right) + \beta_j \pi^{-1}\left(\frac{\alpha_i}{\lambda}\right)\right) = 0,$$

for each $1 \le i, j \le t$ and $\lambda \in \mathbb{F}_{p^m}^*$. □

The following result is an immediate consequence of Lemma 4.2.3.

Corollary 4.2.4. *Let $\alpha_1, \ldots, \alpha_t \in \mathbb{F}_{p^m}^*$ be linearly independent elements over $\mathbb{F}_p$, $1 \le t \le k$. Denote $u_i = (\alpha_i, 0)$ and let $G(x,y) = y\pi(x)$, $x, y \in \mathbb{F}_{p^m}$, where π is a linear permutation over $\mathbb{F}_{p^m}$. Then, the dual component G^*_λ satisfies (4.1) with*

$$g_i(x,y) = tr_m\left(y\pi^{-1}\left(\frac{\alpha_i}{\lambda}\right)\right),$$

for any $\lambda \in \mathbb{F}_{p^m}^*$.

Thus, as an immediate result of Theorem 4.1.4 (Corrolary 4.1.6) and Corollary 4.2.4, we have the following infinite family of vectorial p-ary weakly regular bent (plateaued) $(2m, m)$-functions.

Theorem 4.2.5. *Let $\alpha_1, \ldots, \alpha_t \in \mathbb{F}_{p^m}^*$ be linearly independent elements over $\mathbb{F}_p$, $t|m$. Let $G(x,y) = y\pi(x)$, where π is a linear permutation over $\mathbb{F}_{p^m}$, and let $\mathbf{h}$ be any vectorial function from $\mathbb{F}_p^t$ to $\mathbb{F}_{p^t}$. Then, the function $F : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ given by*

$$F(x,y) = y\pi(x) + \mathbf{h}(tr_m(\alpha_1 x), \ldots, tr_m(\alpha_t x)),$$

generated by Construction 4.1.1, is a vectorial p-ary weakly regular bent (n,m)-function.

Theorem 4.2.6. *Let $\alpha_1, \ldots, \alpha_t \in \mathbb{F}_{p^m}^*$ be linearly independent elements over $\mathbb{F}_p$, $t|m$. Let $G(x,y) = y\pi(x)$, where π is a linear permutation over $\mathbb{F}_{p^m}$, and let $\mathbf{h}_i$ be any reduced polynomial in $\mathbb{F}_p[X_1, \ldots, X_t]$, for $1 \le i \le l$, such that the function*

$$x \mapsto \mathbf{H}(x) = (\mathbf{h}_1(tr_m(\alpha_1 x), \ldots, tr_m(\alpha_t x)), \ldots, \mathbf{h}_1(tr_m(\alpha_1 x), \ldots, tr_m(\alpha_t x))),$$

with $x \in \mathbb{F}_{p^m}$, is a plateaued p-ary (m,l)-function. Then, the function $F : \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \to \mathbb{F}_p^{m+l}$ defined by

$$F(x,y) = (y\pi(x), \mathbf{H}(x))$$

is a plateaued p-ary $(n, m+l)$-function.

Example 4.2.7. Let $G : \mathbb{F}_{3^4} \times \mathbb{F}_{3^4} \to \mathbb{F}_{3^4}$ be defined with $G(x, y) = xy$. Let $U = \{1, \beta, \beta^3, \beta^9\}$, where $\beta = \alpha^{82}$, and α be a root of the primitive polynomial $p(x) = x^8+2x^5+x^4+2x^2+2x+2 \in \mathbb{F}_{3^8}[x]$. Let $\mathbf{h} : \mathbb{F}_{3^4} \to \mathbb{F}_{3^4}$ be defined with $\mathbf{h}(X) = X^{13}$. From Theorem 4.2.5, the function

$$F(x, y) = xy + \big(tr_4(x) + \beta tr_4(\beta x) + \beta^2 tr_4(\beta^2 x) + \beta^3 tr_4(\beta^3 x)\big)^{13}$$

is a ternary weakly regular bent $(8, 4)$-function.

Chapter 5

Two new superclasses of bent functions $\mathcal{SC}$ and $\mathcal{CD}$

In this chapter, we show that under certain conditions it is possible to construct two superclasses of bent functions that stem from $\mathcal{D}_0$, $\mathcal{D}$ and $\mathcal{C}$, which will be denoted as the $\mathcal{SC}$ and $\mathcal{CD}$ class. These classes of functions use the addition of indicators typical to $\mathcal{D}_0$ and $\mathcal{C}$, and $\mathcal{D}$ and $\mathcal{C}$, respectively. Therefore their overall effect is a modification of a bent function on a suitable subset instead on a subspace. We also show that the adding indicators of $\mathcal{D}_0$ and $\mathcal{D}$ cannot give bent functions.

We give sufficient conditions which ensure that bent functions in $\mathcal{CD}$ and $\mathcal{SC}$ lie outside $\mathcal{M}^{\#}$ and provide several generic methods for specifying these objects. We also partially address the normality of these functions and in this context we further refine the constraints on functions in $\mathcal{CD}$ to be outside the completed $\mathcal{PS}^{+}$ class. This problem of finding non(weakly)-normal bent functions is intrinsically difficult and it remains open to show whether there are instances of bent functions in $\mathcal{CD}$ which are non(weakly)-normal.

At the end of the chapter we explicitly characterize the duals of certain instances of bent functions in $\mathcal{C}, \mathcal{D}, \mathcal{SC}$ and $\mathcal{CD}$ which will be of interest for the construction of bent 4-concatenations (cf. Section 7.2.3).

5.1 Bentness of Boolean functions in the class $\mathcal{SC}$

Let $g : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$, defined by $g(x, y) = Tr_1^m(x\pi(y))$, be a bent Boolean function, where π is a permutation on $\mathbb{F}_{2^m}$. Obviously, $g \in \mathcal{M}^{\#}$. If we define $\delta_0(x) = x^{2^m-1} + 1$ to be the Dirac symbol, that is $\delta_0(x) = 1$, if $x = 0$, and equals 0 otherwise, the function $g(x, y) + \delta_0(x)$ is a function in the class $\mathcal{D}_0$[17]. If L is a linear subspace of $\mathbb{F}_{2^m}$, then

$$\mathbb{1}_{L^{\perp}}(x) = \prod_{\omega \in \mathbf{b}(L)} (Tr_1^m(\omega x) + 1),$$

where $\mathbf{b}(L)$ denotes the basis of L, is the indicator function of $L^\perp$ in finite field notation. We note that if (π^{-1}, L) satisfies the (C) property, then $g(x,y) + \mathbb{1}_{L^\perp}(x)$ is in the $\mathcal{C}$ class. Furthermore, let $r = \dim(L^\perp)$.

We will show that functions of the form

$$f(x,y) = g(x,y) + \mathbb{1}_{L^\perp}(x) + \delta_0(x),\ x, y \in \mathbb{F}_{2^m}$$

are bent and outside $\mathcal{M}^\#$ under certain conditions. This is the first time where the truth table of a bent function from the Maiorana-McFarland class was modified in $2^m(2^r-1) = 2^{m+r} - 2^m$ places, that is, it is not a power of 2 nor corresponds to an indicator of a subspace.

Theorem 5.1.1. *Let π be a permutation on $\mathbb{F}_{2^m}$ and $L \subset \mathbb{F}_{2^m}$ be a linear subspace of $\mathbb{F}_{2^m}$ such that (π^{-1}, L) satisfies the (C) property. Then the function $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ defined by*

$$f(x,y) = Tr_1^m(x\pi(y)) + \mathbb{1}_{L^\perp}(x) + \delta_0(x) \tag{5.1}$$

is bent.

Proof. Let $(a,b) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}^*$ be arbitrary. Let us consider the Walsh coefficient $W_f(a,b)$.

$$\begin{aligned} W_f(a,b) &= \sum_{x,y \in \mathbb{F}_{2^m}} (-1)^{f(x,y)+Tr_1^m(ax+by)} \\ &= \sum_{x,y \in \mathbb{F}_{2^m}} (-1)^{Tr_1^m(x\pi(y))+\mathbb{1}_{L^\perp}(x)+\delta_0(x)+Tr_1^m(ax+by)}. \end{aligned}$$

Since $\delta_0(x) = 1$ only if $x = 0$, and equals 0 otherwise, we have that

$$\begin{aligned} W_f(a,b) &= \sum_{x \in \mathbb{F}_{2^m}^*} \sum_{y \in \mathbb{F}_{2^m}} (-1)^{Tr_1^m(x\pi(y))+\mathbb{1}_{L^\perp}(x)+Tr_1^m(ax+by)} \\ &+ \sum_{y \in \mathbb{F}_{2^m}} (-1)^{0+1+1+Tr_1^m(0+by)} \\ &= \sum_{x \in \mathbb{F}_{2^m}^*} \sum_{y \in \mathbb{F}_{2^m}} (-1)^{Tr_1^m(x\pi(y))+\mathbb{1}_{L^\perp}(x)+Tr_1^m(ax+by)} + \sum_{y \in \mathbb{F}_{2^m}} (-1)^{Tr_1^m(by)} \\ &= \sum_{x \in \mathbb{F}_{2^m}^*} \sum_{y \in \mathbb{F}_{2^m}} (-1)^{Tr_1^m(x\pi(y))+\mathbb{1}_{L^\perp}(x)+Tr_1^m(ax+by)} + 0 \\ &= \sum_{x \in \mathbb{F}_{2^m}^*} \sum_{y \in \mathbb{F}_{2^m}} (-1)^{Tr_1^m(x\pi(y))+\mathbb{1}_{L^\perp}(x)+Tr_1^m(ax+by)} \end{aligned} \tag{5.2}$$

Furthermore, if we denote with $g(x,y) = Tr_1^m(x\pi(y)) + \mathbb{1}_{L^\perp}(x)$, we note that

$$\sum_{y \in \mathbb{F}_{2^m}} (-1)^{g(0,y)+Tr_1^m(yb)} = \sum_{y \in \mathbb{F}_{2^m}} (-1)^{1+Tr_1^m(yb)} = 0.$$

Thus, we may add this sum to (5.2) and obtain that

$$W_f(a,b) = \sum_{x\in\mathbb{F}_{2^m}} \sum_{y\in\mathbb{F}_{2^m}} (-1)^{Tr_1^m(x\pi(y))+\mathbb{1}_{L^\perp}(x)+Tr_1^m(ax+by)} = W_g(a,b).$$

If $b = 0$, we have that

$$\begin{aligned} W_f(a,0) &= \sum_{x\in\mathbb{F}_{2^m}^*} \sum_{y\in\mathbb{F}_{2^m}} (-1)^{Tr_1^m(x\pi(y))+\mathbb{1}_{L^\perp}(x)+Tr_1^m(ax)} + 2^m \\ &= \sum_{x,y\in\mathbb{F}_{2^m}} (-1)^{Tr_1^m(x\pi(y))+\mathbb{1}_{L^\perp}(x)+Tr_1^m(ax)} \\ &\quad - \sum_{y\in\mathbb{F}_{2^m}} (-1)^{g(0,y)+Tr_1^m(0)} + 2^m \\ &= \sum_{x,y\in\mathbb{F}_{2^m}} (-1)^{Tr_1^m(x\pi(y))+\mathbb{1}_{L^\perp}(x)+Tr_1^m(ax)} + 2^{m+1} \\ &= W_g(a,0) + 2^{m+1} \end{aligned} \tag{5.3}$$

From the well-known Parseval's equation, it holds that

$$\sum_{a,b\in\mathbb{F}_{2^m}} W_f^2(a,b) = \sum_{a,b\in\mathbb{F}_{2^m}} W_g^2(a,b) = 2^{4m}.$$

Let us express W_f^2 in terms of W_g^2 as follows.

$$\begin{aligned} 2^{4m} &= \sum_{a,b\in\mathbb{F}_{2^m}} W_f^2(a,b) = \sum_{a\in\mathbb{F}_{2^m}} W_f^2(a,0) + \sum_{b\neq 0,a\in\mathbb{F}_{2^m}} W_f^2(a,b) \\ &= \sum_{a\in\mathbb{F}_{2^m}} (W_g(a,0) + 2^{m+1})^2 + \sum_{b\neq 0,a\in\mathbb{F}_{2^m}} W_g^2(a,b) \\ &= \sum_{a\in\mathbb{F}_{2^m}} (W_g^2(a,0) + 2^{m+2}W_g(a,0) + 2^{2m+2}) \\ &\quad + \sum_{b\neq 0,a\in\mathbb{F}_{2^m}} W_g^2(a,b) \\ &= \sum_{a,b\in\mathbb{F}_{2^m}} W_g^2(a,b) + 2^{m+2} \sum_{a\in\mathbb{F}_{2^m}} W_g(a,0) + 2^{3m+2} \\ 2^{4m} &= 2^{4m} + 2^{m+2} \sum_{a\in\mathbb{F}_{2^m}} W_g(a,0) + 2^{3m+2} \end{aligned}$$

$$\sum_{a\in\mathbb{F}_{2^m}} W_g(a,0) = -2^{2m} \tag{5.4}$$

Since g is a bent function (it is in the $\mathcal{C}$ class), it follows that $W_g(a,b) = \pm 2^m$ for all $a, b \in \mathbb{F}_{2^m}$. Thus, from (5.4) it follows that

$$\sum_{a\in\mathbb{F}_{2^m}} W_g(a,0) = \alpha\cdot 2^m + \beta\cdot(-2^m) = -2^{2m},\ \alpha,\beta\in\mathbb{Z},\ 0\le\alpha,\beta\le 2^m$$

$$\Rightarrow \alpha = 0, \beta = 2^m,$$

that is, $W_g(a,0) = -2^m$ for all $a \in \mathbb{F}_{2^m}$. Hence, from (5.3) we have that $W_f(a,0) = 2^m$ for all $a \in \mathbb{F}_{2^m}$. In other words, $W_f(a,b) = \pm 2^m$ for all $(a,b) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, i.e., the function f is indeed bent. □

The above result motivates the following definition.

Definition 5.1.2. Let π be a permutation on $\mathbb{F}_{2^m}$ and let $L \subset \mathbb{F}_{2^m}$ be a linear subspace of $\mathbb{F}_{2^m}$ such that (π^{-1}, L) satisfies the (C) property. Then the class of bent functions $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ containing all functions of the form

$$(\mathcal{SC}) : f(x,y) = Tr_1^m(x\pi(y)) + a_0\mathbb{1}_{L^\perp}(x) + a_1\delta_0(x),\ a_i \in \mathbb{F}_2, \qquad (5.5)$$

is called $\mathcal{SC}$ and is a superclass of $\mathcal{D}_0$ and $\mathcal{C}$.

Remark 5.1.3. Notice that for $f(x,y) = Tr_1^m(x\pi(y)) + a_0\mathbb{1}_{L^\perp}(x) + a_1\delta_0(x)$, the indicator $\mathbb{1}_S(x) = \mathbb{1}_{L^\perp}(x) + \delta_0(x)$ (taking $a_0 = a_1 = 1$) is the characteristic function of the set $S := L^\perp \setminus \{0\}$. Setting $a_0 = 1, a_1 = 0$ we recover the class $\mathcal{D}_0$, whereas the case $a_0 = 0, a_1 = 1$ specifies the class $\mathcal{C}$. Is is interesting to observe that these functions can also be viewed either as further modifications performed on the members of $\mathcal{D}_0$ (addition of $\mathbb{1}_{L^\perp}(x)$) or alternatively a modification of the members in $\mathcal{C}$ (through addition of $\delta_0(x)$).

With the following result, we show that the newly constructed class of bent functions is indeed outside $\mathcal{M}^\#$ under certain conditions.

Theorem 5.1.4. *With the same notation as in Theorem 5.1.1, the function $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ defined by*

$$f(x,y) = Tr_1^m(x\pi(y)) + \mathbb{1}_S(x),\ x,y\in\mathbb{F}_{2^m},$$

where $\mathbb{1}_S(x) = \mathbb{1}_{L^\perp}(x) + \delta_0(x)$, $2 \le \dim(L) < m$ and $Tr_1^m(\mu\pi)$ has no non-zero linear structures for all $\mu \in \mathbb{F}_{2^m}^*$, is a bent function in the class $\mathcal{SC}$ outside $\mathcal{M}^\#$.

Proof. From Lemma 2.2.4, it suffices to show that there is no subspace K of $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ on which the second-order derivative D_aD_bf vanishes, for some $a, b \in K$.

Let $K = K_1 \times K_2$, $K_1, K_2 \neq \{0\}$, be an m-dimensional subspace of $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, and let $a = (a_1, a_2), b = (b_1, b_2) \in K$ be arbitrary nonzero elements with $a \neq b$. Then, we have that

$$D_aD_bf(x,y) = D_aD_bg(x,y) + D_{a_1}D_{b_1}\delta_0(x) = 0$$

$$\Leftrightarrow D_a D_b g(x,y) = D_{a_1} D_{b_1} \delta_0(x),$$

for all $x, y \in \mathbb{F}_{2^m}$, where $g(x,y) = Tr_1^m(x\pi(y)) + \mathbb{1}_{L^\perp}(x)$.The degree of $g(x,y)$ relative to x equals $\deg(\mathbb{1}_{L^\perp}) = \dim(L) < m$. Thus, $\deg(D_a D_b g) \leq m - 1 - 2 = m - 3$. On the other hand, $\deg(\delta_0) = m$, and thus $\deg(D_{a_1} D_{b_1} \delta_0) = m - 2$. Since the degrees of the functions $D_a D_b g$ and $D_{a_1} D_{b_1} \delta_0$ relative to x differ, it follows that $D_a D_b f \neq 0$. If $K = \mathbb{F}_{2^m} \times \{0\}$, with the same conclusion as before, $D_a D_b f \neq 0$ for $0 \neq a, b \in K,\ a \neq b$. Suppose $K = \{0\} \times \mathbb{F}_{2^m}$ and let $a = (0, a_2), b = (0, b_2) \in K$ be arbitrary and distinct. Then

$$D_a D_b \delta_0(x,y) = D_0 D_0 \delta_0(x,y) = 0,$$

for all $x, y \in \mathbb{F}_{2^m}$. Since g is in $\mathcal{C}$ outside $\mathcal{M}^\#$ (all conditions of Theorem 2.2.6 are satisfied), we have that $D_a D_b g \neq 0$. Hence, it follows that $D_a D_b f \neq 0$ for $0 \neq a, b \in K$ distinct. Thus, there is no m-dimensional subspace of $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ on which the second-order derivatives $D_a D_b f$ vanish, i.e. the function f is outside $\mathcal{M}^\#$. □

Especially, we can specify the following explicit family of bent functions outside $\mathcal{M}^\#$. But first, we note the following useful result.

Proposition 5.1.5. *[88] Let $\pi(x) = x^d$ be a monomial permutation over $\mathbb{F}_{2^n}$. Then none of the component functions of $\pi(x)$ will admit a linear structure if and only if* $\mathrm{wt}(d) \geq 3$.

Corollary 5.1.6. *Let $n = 2m$ and $s \geq 2$ be a positive divisor of m such that m/s is odd. Let $\pi(y) = y^d$ be a permutation on $\mathbb{F}_{2^m}$ such that $d(2^s + 1) \equiv 1 \pmod{2^m - 1}$ and* $\mathrm{wt}(d) \geq 3$. *Let $U = \{1, \alpha, \ldots, \alpha^{s-1}\}$, where α is a primitive element of $\mathbb{F}_{2^s}$. If $L = \langle K \rangle$, where $K \subseteq U$, then the Boolean function $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ defined by*

$$f(x,y) = Tr_1^m(xy^d) + \mathbb{1}_{L^\perp}(x) + \delta_0(x),\ x, y \in \mathbb{F}_{2^m},$$

is a bent function in $\mathcal{SC}$ outside $\mathcal{M}^\#$.

Proof. Since $\gcd(m, s) = s$ and m/s is odd, from [88, Theorem 9] we know that (π^{-1}, L) satisfies the (C) property. Furthermore, $\mathrm{wt}(d) \geq 3$, which implies that $Tr_1^m(\mu\pi)$ has no nonzero linear structures (cf. Proposition 5.1.5), for all $\mu \in \mathbb{F}_{2^m}^*$, and $2 \leq \dim(L) \leq s < m$. Thus, from Theorem 5.1.4 it follows that f is a bent function in $\mathcal{SC}$ outside $\mathcal{M}^\#$. □

Remark 5.1.7. Notice that our modification is performed on sets which however possess a lot of structure (a union of two subspaces). A similar modification of bent functions performed on random sets of the same cardinality as our union of two subspaces, thus considering $(x, y) \mapsto Tr_1^m(x\pi(y)) + \mathbb{1}_S(x)$, can hardly preserve the bentness. For this purpose we considered 20000 randomly selected sets $S \subset \mathbb{F}_{2^{12}}$ of cardinality $2^6 \times (2^4 - 1)$ which is of the same size as for $\delta_0(x) + 1_{L^\perp}(x)$ when $\dim(L) = 2$),

see also Example 5.1.8. It could be checked that for **none** of the 20000 randomly chosen sets S the function $(x, y) \mapsto Tr_1^6(xy^{38}) + \mathbb{1}_S(x)$ was bent. In addition, other choices of permutation $\pi(y)$, different from $\pi(y) = y^{38}$ gave the same result. Hence, considering modifications of bent functions on randomly selected sets S seems not to be an efficient method for deriving new bent functions.

5.1.1 On EA-equivalence between $\mathcal{D}_0$ and $\mathcal{SC}$ class

One indicator for the EA-equivalence of bent functions is the weight distribution of the second-order derivatives, originally considered by Dillon [29]. That is, two bent functions $f, g \in \mathscr{B}_n$ are EA-equivalent if and only if the multisets $\{* \text{ wt}(D_aD_bf) : a, b \in \mathbb{F}_{2^n}^* *\}$ and $\{* \text{ wt}(D_aD_bg) : a, b \in \mathbb{F}_{2^n}^* *\}$ are equal. This criterion can be applied to bent functions in $\mathcal{SC}$ and $\mathcal{D}_0$ for proving their EA-inequivalence. That is, let π be a permutation on $\mathbb{F}_{2^m}$ and let $L \subset \mathbb{F}_{2^m}$ be a linear subspace of $\mathbb{F}_{2^m}$ such that (π^{-1}, L) satisfies the (C) property. Then, the function $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ defined by

$$f(x, y) = Tr_1^m(x\pi(y)) + \mathbb{1}_{L^\perp}(x) + \delta_0(x)$$

is a function in $\mathcal{SC}$. One can rewrite f as $f(x, y) = g(x, y) + \mathbb{1}_{L^\perp}(x)$, where $g(x, y) = Tr_1^m(x\pi(y)) + \delta_0(x) \in \mathcal{D}_0$. Let us consider the second-order derivatives of f. For $0 \neq a = (a_1, a_2), b = (b_1, b_2) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, we have that

$$D_aD_bf(x, y) = D_aD_bg(x, y) + D_{a_1}D_{b_1}\mathbb{1}_{L^\perp}(x).$$

For simplicity, we assume that $\dim(L) = 2$ (see also Example 5.1.8 below), then $\dim(L^\perp) = m - 2$. Since $\deg(\mathbb{1}_{L^\perp}) = 2$, it is easy to verify that

$$D_{a_1}D_{b_1}\mathbb{1}_{L^\perp} \equiv \begin{cases} 1, & \langle a_1, b_1\rangle^* \nsubseteq L^\perp \\ 0, & \text{otherwise,} \end{cases}$$

where $\langle a_1, b_1\rangle^* = \{a_1, b_1, a_1 + b_1\}$. In other words,

$$D_aD_bf \equiv \begin{cases} D_aD_bg + 1, & \langle a_1, b_1\rangle^* \nsubseteq L^\perp \\ D_aD_bg, & \text{otherwise.} \end{cases}.$$

Hence, assuming that D_aD_bg is not balanced for all $\langle a_1, b_1\rangle^* \nsubseteq L^\perp$ then the weight distributions of D_aD_bf and D_aD_bg differ and thus f and g are EA-inequivalent. Thus, functions in $\mathcal{SC}$ can be EA-inequivalent to functions in the class $\mathcal{D}_0$. A similar argument can be applied when $\dim(L) > 2$ in which case the difference between D_aD_bg and D_aD_bf is a function of degree $\dim(L) - 2$ and in general the weight distributions of the second order derivatives are different.

We give also the following computational observation confirming the above discussion regarding EA-equivalence.

Example 5.1.8. Let $f : \mathbb{F}_{2^6} \times \mathbb{F}_{2^6} \to \mathbb{F}_2$ be defined by $f(x, y) = g(x, y) + \mathbb{1}_{L^\perp}(x)$, where $g(x, y) = Tr_1^6(xy^{38}) + \delta_0(x)$ and $L = \langle 1, \alpha^{(2^6-1)/3} \rangle$, α is a primitive element of $\mathbb{F}_{2^6}$. Then, the functions f and g are bent functions in $\mathcal{SC}$ and $\mathcal{D}_0$, respectively. Let us consider the weight distributions of their second-order derivatives. For simplicity, we denote with $[u, v]$ the weight u which appears v times as a weight of D_aD_bg or D_aD_bf.
The weight distribution $\{* \ \mathrm{wt}(D_aD_bg) : 0 \neq a, b \in \mathbb{F}_{2^6} \times \mathbb{F}_{2^6} \ *\}$ is given by:

$$\begin{array}{ccc} [256, 1953] & [1024, 567] & [1152, 17577] \\ [1536, 2268] & [1600, 70308] & [1664, 189] \\ [1792, 61425] & [1824, 60480] & [1856, 82782] \\ [1888, 117936] & [1920, 577836] & [1952, 396144] \\ [1984, 470484] & [2016, 982800] & [2048, 2682666] \\ [2080, 970704] & [2112, 447930] & [2144, 423360] \\ [2176, 554715] & [2208, 120960] & [2240, 70308] \\ [2272, 60480] & [2304, 81585] & [2496, 117180] \\ [2560, 3780] & [2944, 5859] & [3072, 189] \end{array}$$

On the other hand, the weight distribution $\{* \ \mathrm{wt}(D_aD_bf) : 0 \neq a, b \in \mathbb{F}_{2^6} \times \mathbb{F}_{2^6} \ *\}$ is:

$$\begin{array}{cccc} [256, 1185] & [1024, 567] & [1152, 12969] & [1536, 2268] \\ [1600, 88740] & [1664, 117] & [1792, 68145] & [1824, 59040] \\ [1856, 75870] & [1888, 116784] & [1920, 560196] & [1952, 403920] \\ [1984, 457620] & [2016, 974160] & [2048, 2682666] & [2080, 979344] \\ [2112, 460794] & [2144, 415584] & [2176, 572355] & [2208, 122112] \\ [2240, 77220] & [2272, 61920] & [2304, 74865] & [2432, 72] \\ [2496, 98748] & [2560, 3780] & [2944, 10467] & [3072, 189] \\ [3840, 768] & & & \end{array}$$

The above weight distributions are clearly different. Moreover, in the weight distribution of D_aD_bf we have two additional values, which do not appear in the weight distribution of D_aD_bg. Notice that the weight distributions remain different for suitably chosen subspaces L with $\dim(L) > 2$.

Motivated by this construction, we will consider the existence of other superclasses: $\mathcal{SD}$ (superclass of $\mathcal{D}$ and $\mathcal{D}_0$), $\mathcal{CD}$ (superclass of $\mathcal{C}$ and $\mathcal{D}$) and $\mathcal{SCD}$ (superclass of $\mathcal{C}$, $\mathcal{D}$ and $\mathcal{D}_0$). It turns out that only the class $\mathcal{CD}$ contains bent functions, whereas the other classes do not.

5.2 Bentness of Boolean functions in the class $\mathcal{SD}$

As before, we consider $g : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ defined as $g(x, y) = Tr_1^m(x\pi(y))$, where π is a permutation on $\mathbb{F}_{2^m}$, which is a bent func-

tion in $\mathcal{M}$. We now show that if $E_1, E_2 \neq \{0\}$ are two linear subspaces of $\mathbb{F}_{2^m}$ such that $\pi(E_2) = E_1^{\perp}$ (we do not consider the possibilities $E_1 \times E_2 = \{0\} \times \mathbb{F}_{2^m}$ or $\mathbb{F}_{2^m} \times \{0\}$), then Boolean functions of the form, constituting the $\mathcal{SD}$ class,

$$(\mathcal{SD}) : f(x,y) = g(x,y) + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y) + \delta_0(x),\ x,y \in \mathbb{F}_{2^m}, \tag{5.6}$$

cannot be bent.

Theorem 5.2.1. *Let π be a permutation on $\mathbb{F}_{2^m}$ and $E_1, E_2 \subset \mathbb{F}_{2^m}$ be two linear subspace of $\mathbb{F}_{2^m}$ such that $\pi(E_2) = E_1^{\perp}$. Then, the function $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ defined by*

$$f(x,y) = Tr_1^m(x\pi(y)) + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y) + \delta_0(x)$$

is not bent.

Proof. Let us first compute $W_f(0,0)$ as:

$$\begin{aligned}
W_f(0,0) &= \sum_{x \in \mathbb{F}_{2^m}^*} \sum_{y \in \mathbb{F}_{2^m}} (-1)^{Tr_1^m(x\pi(y)) + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y)} + \sum_{y \in \mathbb{F}_{2^m}} (-1)^{\mathbb{1}_{E_2}(y)+1} \\
&= \sum_{x \in \mathbb{F}_{2^m}^*} \sum_{y \in \mathbb{F}_{2^m}} (-1)^{Tr_1^m(x\pi(y)) + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y)} - \sum_{y \in \mathbb{F}_{2^m}} (-1)^{\mathbb{1}_{E_2}(y)} \\
&= \sum_{x \in \mathbb{F}_{2^m}} \sum_{y \in \mathbb{F}_{2^m}} (-1)^{Tr_1^m(x\pi(y)) + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y)} - 2 \sum_{y \in \mathbb{F}_{2^m}} (-1)^{\mathbb{1}_{E_2}(y)} \\
&= W_g(0,0) - 2 \cdot (2^m - |E_2|).
\end{aligned}$$

Since $g(x,y) = Tr_1^m(x\pi(y)) + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y)$ is a bent function in $\mathcal{D}$, we have that either $W_g(0,0) = 2^m$ or -2^m.

Assuming that $W_g(0,0) = 2^m$, then

$$W_f(0,0) = 2^m - 2 \cdot 2^m + 2|E_2| = -2^m + 2|E_2|.$$

The requirement that $W_f(0,0) = \pm 2^m$ implies that $|E_2| = 0$ or 2^m. However, $E_2 \neq \emptyset$ and obviously $\dim E_2 < m$, thus this case is not possible.

On the other hand, if $W_g(0,0) = -2^m$ then we necessarily have

$$W_f(0,0) = -2^m - 2 \cdot 2^m + 2|E_2| = -3 \cdot 2^m + 2|E_2|.$$

Requiring that $W_f(0,0) = \pm 2^m$, implies that $|E_2| = 2^{m+1}$ or 2^m, both of which are again not possible. Hence, $W_f(0,0) \neq \pm 2^m$, that is, f is not a bent function. □

Remark 5.2.2. Similarly, using the ideas as in the proof of Theorem 5.2.1, one can show that functions of the form (constituting the $\mathcal{SCD}$ class)

$$(\mathcal{SCD}) : f(x,y) = g(x,y) + \mathbb{1}_{L^{\perp}}(x) + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y) + \delta_0(x),$$

cannot be bent.

5.3 Bentness of Boolean functions in the class $\mathcal{CD}$

In this section, we consider the remaining case which corresponds to the mixture of indicators stemming from $\mathcal{C}$ and $\mathcal{D}$. Let $g : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$, defined by $g(x, y) = Tr_1^m(x\pi(y)) \in \mathcal{M}$, be a bent Boolean function, where π is a permutation on $\mathbb{F}_{2^m}$. Let $L \subset \mathbb{F}_{2^m}$ be a linear subspace of $\mathbb{F}_{2^m}$ such that (π^{-1}, L) satisfies the (C) property, and let $E_1, E_2 \neq \{0\}$ be two linear subspaces of $\mathbb{F}_{2^m}$ such that $\pi(E_2) = E_1^{\perp}$. We consider the bentness of Boolean functions f in $2m$ variables, being members of the class $\mathcal{CD}$ (cf. Definition 5.3.3), of the form

$$f(x, y) = g(x, y) + \mathbb{1}_{L^{\perp}}(x) + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y),\ x, y \in \mathbb{F}_{2^m}. \tag{5.7}$$

The primary task is to find conditions which ensure that the function f given by (5.7) is bent. Let us consider the Walsh coefficient $W_f(a, b)$ for arbitrary but fixed $(a, b) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$. Furthermore, let us denote with $C(x, y) := Tr_1^m(x\pi(y)) + \mathbb{1}_{L^{\perp}}(x)$ and $M(a, b) = C(x, y) + Tr_1^m(ax + by)$. Then,

$$\begin{aligned}
W_f(a,b) &= \sum_{x,y\in\mathbb{F}_{2^m}} (-1)^{M(a,b)+\mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y)} \\
&= \sum_{x\in E_1}\sum_{y\in\mathbb{F}_{2^m}} (-1)^{M(a,b)+\mathbb{1}_{E_2}(y)} + \sum_{x\notin E_1}\sum_{y\in\mathbb{F}_{2^m}} (-1)^{M(a,b)} \\
&= -\sum_{x\in E_1}\sum_{y\in E_2}(-1)^{M(a,b)} + \sum_{x\in E_1}\sum_{y\notin E_2}(-1)^{M(a,b)} \\
&+ \sum_{x\notin E_1}\sum_{y\in\mathbb{F}_{2^m}} (-1)^{M(a,b)} \\
&= -2\sum_{x\in E_1}\sum_{y\in E_2}(-1)^{M(a,b)} + \sum_{x\in E_1}\sum_{y\in\mathbb{F}_{2^m}} (-1)^{M(a,b)} \\
&+ \sum_{x\notin E_1}\sum_{y\in\mathbb{F}_{2^m}} (-1)^{M(a,b)} \\
&= \sum_{x,y\in\mathbb{F}_{2^m}} (-1)^{M(a,b)} - 2\sum_{x\in E_1}\sum_{y\in E_2}(-1)^{M(a,b)} \\
&= W_C(a,b) - 2\sum_{x\in E_1}\sum_{y\in E_2}(-1)^{M(a,b)} \\
&= W_C(a,b) - 2\sum_{x\in E_1}\sum_{y\in E_2}(-1)^{Tr_1^m(x\pi(y))+\mathbb{1}_{L^{\perp}}(x)+Tr_1^m(ax+by)}.
\end{aligned}$$

Since $E_1^{\perp} = \pi(E_2)$, we have that $Tr_1^m(x\pi(y)) = 0$ for $(x, y) \in E_1 \times E_2$.

It follows now that

$$W_f(a,b) = W_C(a,b) - 2 \cdot \left(\sum_{x \in E_1} \sum_{y \in E_2} (-1)^{Tr_1^m(ax+by)} \right.$$
$$\left. -2 \sum_{x \in E_1 \cap L^\perp} \sum_{y \in E_2} (-1)^{Tr(ax+by)} \right). \tag{5.8}$$

Furthermore, if we denote $K = E_1 \cap L^\perp$, it is easy to see that

$$\sum_{x \in E_1} \sum_{y \in E_2} (-1)^{Tr_1^m(ax+by)} = \begin{cases} 2^{\varepsilon_1+\varepsilon_2}, & (a,b) \in E_1^\perp \times E_2^\perp \\ 0, & \text{otherwise} \end{cases}, \tag{5.9}$$

$$\sum_{x \in K} \sum_{y \in E_2} (-1)^{Tr_1^m(ax+by)} = \begin{cases} 2^{\kappa+\varepsilon_2}, & (a,b) \in K^\perp \times E_2^\perp \\ 0, & \text{otherwise} \end{cases}, \tag{5.10}$$

where $\varepsilon_i = \dim(E_i)$ and $\kappa = \dim(K)$. Since $K \subset E_1$, it follows that $E_1^\perp \subset K^\perp$, and therefore $E_1^\perp \times E_2^\perp \subset K^\perp \times E_2^\perp$. Obviously, when $(a,b) \notin K^\perp \times E_2^\perp$, we have that $W_f(a,b) = W_C(a,b)$. Let us now consider the following cases:

Case 1: Suppose that $(a,b) \in E_1^\perp \times E_2^\perp$. Since we want that f is a bent function, we have the following situations:

(I) If $W_f(a,b) = W_C(a,b)$, then

$$\begin{aligned} & W_C(a,b) = W_C(a,b) - 2^{\varepsilon_1+\varepsilon_2+1} + 2^{\kappa+\varepsilon_2+2} \\ \Leftrightarrow & 2^{\varepsilon_1+\varepsilon_2+1} = 2^{\kappa+\varepsilon_2+2} \\ \Leftrightarrow & \kappa = \varepsilon_1 - 1. \end{aligned}$$

(II) If $W_f(a,b) = -W_C(a,b)$, then $-2W_C(a,b) = -2^{m+1} + 2^{\kappa+\varepsilon_2+2}$. Since $W_C(a,b) = \pm 2^m$, we have

$$-2^{m+1} = -2^{m+1} + 2^{\kappa+\varepsilon_2+2} \text{ or } 2^{m+1} = -2^{m+1} + 2^{\kappa+\varepsilon_2+2}.$$

The first case is not possible since a power of two is strictly larger than zero, and the second one leads to $\kappa = \varepsilon_1$.

Case 2: Suppose that $(a,b) \in (K^\perp \setminus E_1^\perp) \times E_2^\perp$. Again, requiring that f is bent leads to the following cases:

(I) If $W_f(a,b) = W_C(a,b)$, then

$$W_C(a,b) = W_C(a,b) + 2^{\kappa+\varepsilon_2+2} \Leftrightarrow 2^{\kappa+\varepsilon_2+2} = 0,$$

which is not possible.

(II) If $W_f(a,b) = -W_C(a,b)$, then $-2W_C(a,b) = 2^{\kappa+\varepsilon_2+2}$. Since the right-hand side of the equality is positive, so must be the left-hand side. Thus, we must have that $W_C(a,b) = -2^m$ and in this case $\kappa = \varepsilon - 1$.

From **Case** 1 and 2, we obtain bent Walsh coefficients only when $\kappa = \varepsilon_1$ or $\kappa = \varepsilon_1 - 1$. These observations are summarized below, where Theorem 5.3.1 corresponds to the case $\kappa = \varepsilon_1 - 1$ and Theorem 5.3.2 refers to the case $\kappa = \varepsilon_1$.

Theorem 5.3.1. *Let π be a permutation on $\mathbb{F}_{2^m}$, $L \subset \mathbb{F}_{2^m}$ be a linear subspace of $\mathbb{F}_{2^m}$ such that (π^{-1}, L) satisfies the (C) property, and let $E_1, E_2 \neq \{0\}$ be two linear subspaces of $\mathbb{F}_{2^m}$ such that $\pi(E_2) = E_1^\perp$ and $\dim(E_1 \cap L^\perp) = \dim(E_1) - 1$. Then, the function $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ defined by*

$$f(x,y) = C(x,y) + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y),$$

where $C(x,y) = Tr_1^m(x\pi(y)) + \mathbb{1}_{L^\perp}(x)$, is bent. Moreover, it holds that

$$W_f(a,b) = \begin{cases} -W_C(a,b), & (a,b) \in ((E_1 \cap L)^\perp \setminus E_1^\perp) \times E_2^\perp \\ W_C(a,b), & \text{otherwise} \end{cases}.$$

Proof. Suppose that $(a,b) \notin (E_1 \cap L)^\perp \times E_2^\perp$. From (5.8)-(5.10), it is easy to see that $W_f(a,b) = W_C(a,b)$. Suppose that $(a,b) \in E_1^\perp \times E_2^\perp$. Again, (5.8)-(5.10) implies that

$$W_f(a,b) = W_C(a,b) - 2 \cdot (2^{\varepsilon_1+\varepsilon_2} - 2 \cdot 2^{\varepsilon_1-1+\varepsilon_2}) = W_C(a,b).$$

Lastly, if $(a,b) \in ((E_1 \cap L)^\perp \setminus E_1^\perp) \times E_2^\perp$, the sum (5.9) is equal to zero, and thus from (5.8) and (5.10) it follows that

$$W_f(a,b) = W_C(a,b) - 2 \cdot 2^{\varepsilon_1+\varepsilon_2} = W_C(a,b) - 2^{m+1}.$$

Using Parseval's equation, it is straightforward to show that $W_C(a,b) = 2^m$, for all $(a,b) \in (E_1 \cap L)^\perp \times E_2^\perp$. Thus,

$$W_f(a,b) = 2^m - 2^{m+1} = -2^m = -W_C(a,b).$$

In other words, the function f is bent. □

Theorem 5.3.2. *Let π be a permutation on $\mathbb{F}_{2^m}$, $E_1, E_2 \neq \{0\}$ be two linear subspaces of $\mathbb{F}_{2^m}$ such that $\pi(E_2) = E_1^\perp$ and $(\pi^{-1}, E_1^\perp)$ satisfies the (C) property. Then the function $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ defined by*

$$f(x,y) = C(x,y) + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y),$$

where $C(x,y) = Tr_1^m(x\pi(y)) + \mathbb{1}_{E_1}(x)$, is bent. Moreover, it holds that

$$W_f(a,b) = \begin{cases} -W_C(a,b), & (a,b) \in E_1^\perp \times E_2^\perp \\ W_C(a,b), & \text{otherwise} \end{cases}.$$

Proof. We note that (5.8) becomes

$$W_f(a,b) = W_C(a,b) + 2\sum_{x\in E_1}\sum_{y\in E_2}(-1)^{Tr_1^m(ax+by)} = \begin{cases} W_C(a,b) + 2^{m+1}, & (a,b) \in E_1^\perp \times E_2^\perp \\ W_C(a,b), & \text{otherwise} \end{cases}.$$

Using Parseval's equation, it is straightforward to show that $W_C(a,b) = -2^m$ for all $(a,b) \in E_1^\perp \times E_2^\perp$. Thus,

$$W_f(a,b) = -2^m + 2^{m+1} = 2^m = -W_C(a,b).$$

In other words, the function f is bent. □

Definition 5.3.3. Let π be a permutation on $\mathbb{F}_{2^m}$, $L \subset \mathbb{F}_{2^m}$ be a linear subspace of $\mathbb{F}_{2^m}$ such that (π^{-1}, L) satisfies the (C) property, and let $E_1, E_2 \neq \{0\}$ be two linear subspaces of $\mathbb{F}_{2^m}$ such that $\pi(E_2) = E_1^\perp$. If $\dim(E_1 \cap L^\perp) = \dim(E_1) - 1$ or $E_1 = L^\perp$, then the class of bent functions $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ containing all functions of the form

$$(\mathcal{CD}) : f(x,y) = Tr_1^m(x\pi(y)) + a_0\mathbb{1}_{L^\perp}(x) + a_1\mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y), \;\; a_i \in \mathbb{F}_2, \tag{5.11}$$

is called $\mathcal{CD}$ and is a superclass of $\mathcal{C}$ and $\mathcal{D}$.

Remark 5.3.4. Let us consider the sum of the indicators $\mathbb{1}_{L^\perp}(x) + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y)$ defined above. We note that

$$\begin{aligned} &\mathbb{1}_{L^\perp}(x) + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y) = 1 \\ \Leftrightarrow &(x,y) \in (L^\perp \times \mathbb{F}_{2^m}) \setminus (E_1 \times E_2) \;\vee\; (x,y) \in (E_1 \times E_2) \setminus (L^\perp \times \mathbb{F}_{2^m}) \\ \Leftrightarrow &(x,y) \in (L^\perp \times \mathbb{F}_{2^m}) \triangle (E_1 \times E_2) := S, \end{aligned}$$

where Δ denotes the symmetric difference of sets. Moreover, the cardinality of S is equal to

$$|S| = 2^{m+\lambda} + 2^{\epsilon_1+\epsilon_2} - 2^{\epsilon_2+1} \cdot |L^\perp \cap E_1|, \tag{5.12}$$

where $\dim(L^\perp) = \lambda$ and $\dim(E_i) = \epsilon_i$, $i = 1, 2$. It is easy to verify that S is neither a linear nor an affine subspace of $\mathbb{F}_{2^n}$, rather a set of elements in $\mathbb{F}_{2^n}$.

5.3.1 Sufficient conditions for functions in $\mathcal{CD}$ to be outside $\mathcal{M}^\#$

Similarly as for functions in $\mathcal{SC}$, we present sufficient conditions for functions in the $\mathcal{CD}$ class to be provably outside $\mathcal{M}^\#$. We also partially address the normality of these functions and the main conclusion is that the choice of indicators must be further refined in order to possibly identify

instances within $\mathcal{CD}$ class which are weakly non-normal. Consequently, this would imply that such functions lie outside the completed $\mathcal{PS}^+$ class.

The following proposition is proved to be useful for our main result.

Proposition 5.3.5. *Let V be a subspace of $\mathbb{F}_2^n$. Then, we have*

$$\deg(D_aD_b(\mathbb{1}_V(x))) = \begin{cases} n-\dim(V)-2, & if\ a,b,a\oplus b \notin V \\ 0, & otherwise \end{cases}.$$

Proof. We know that $\deg(\mathbb{1}_V(x)) = n-\dim(V)$. Further, if $a, b, a\oplus b \notin V$, then

$$\begin{aligned} D_aD_b(\mathbb{1}_V(x))) = {} & \mathbb{1}_V(x) \oplus \mathbb{1}_V(x\oplus a) \\ & \oplus \mathbb{1}_V(x\oplus b) \oplus \mathbb{1}_V(x\oplus a\oplus b) \\ = {} & \mathbb{1}_{V\cup(V\oplus a)\cup(V\oplus b)\cup(V\oplus a\oplus b)}(x), \end{aligned}$$

that is, $\deg(D_aD_b(\mathbb{1}_V(x))) = n-\dim(V)-2$. If either $a\in V$, $b\in V$, or $a\oplus b\in V$ then

$$D_aD_b(\mathbb{1}_V(x))) = 0.$$

□

We are now able to prove that, under certain conditions, functions in $\mathcal{CD}$ are provably outside $\mathcal{M}^\#$.

Theorem 5.3.6. *Let π be a permutation on $\mathbb{F}_2^m$, $L\subset\mathbb{F}_2^m$ be a linear subspace of $\mathbb{F}_2^m$ such that (π^{-1}, L) satisfies the (C) property, and let $E_1, E_2 \neq \{\mathbf{0}_m\}$ be two linear subspaces of $\mathbb{F}_2^m$ such that $\pi(E_2) = E_1^\perp$. Furthermore, we assume that either $\dim(E_1\cap L^\perp) = \dim(E_1)-1$ or $E_1 = L^\perp$. Let $f:\mathbb{F}_2^m\times\mathbb{F}_2^m\to\mathbb{F}_2$ be defined by*

$$f(x,y) = x\cdot\pi(y)\oplus\mathbb{1}_{L^\perp}(x)\oplus\mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y).$$

If (π^{-1}, L) and (π, E_1, E_2) satisfy the properties $(C1)$ and $(D1)-(D3)$, respectively (cf. Theorems 2.2.6 and 2.2.7), then f is a bent function in $\mathcal{CD}$ outside $\mathcal{M}^\#$.

Proof. From Theorems 5.3.1-5.3.2, it follows that f is bent. From Lemma 2.2.4, it suffices to show that there is no m-dimensional subspace V of $\mathbb{F}_2^m\times\mathbb{F}_2^m := \mathbb{F}_2^n$ on which the second-order derivative $D_aD_b(f)$ vanishes, for any nonzero $a, b\in V$.

The second-order derivative of f with respect to $a=(a_1,a_2)$ and $b=(b_1,b_2)$ in $V\subset\mathbb{F}_2^m\times\mathbb{F}_2^m$, can be written as

$$\begin{aligned} D_aD_bf(x,y) = {} & x\cdot(D_{a_2}D_{b_2}\pi(y)) \oplus a_1\cdot D_{b_2}\pi(y\oplus a_2) \\ & \oplus b_1\cdot D_{a_2}\pi(y\oplus b_2) \oplus D_{a_1}D_{b_1}\mathbb{1}_{L^\perp}(x) \oplus D_aD_b\mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y). \end{aligned} \tag{5.13}$$

We know that $E_1\times E_2$ is a subspace of $\mathbb{F}_2^n$ and therefore $\mathbb{F}_2^n = \bigcup_{u_i\in U}(E_1\times E_2)\oplus u_i$, where U is a set of (disjoint) coset representatives w.r.t. $E_1\times E_2$

and consequently $(u_i \oplus (E_1 \times E_2)) \cap (u_j \oplus (E_1 \times E_2)) = \emptyset$ for any $u_i \neq u_j \in U$. Any $a \in \mathbb{F}_2^n$ can then be written as $a = a^{[1]} \oplus a^{[2]}$, where $a^{[1]} \in E_1 \times E_2$ and $a^{[2]} \in U$. Thus, we have

$$D_a D_b \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y) = D_{a^{[2]}} D_{b^{[2]}} \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y). \tag{5.14}$$

If $|\{a^{[2]} \in U : (a^{[1]} \oplus a^{[2]}) \in V\}| > 2$, then we select two nonzero vectors $a, b \in V$ such that $a^{[2]}, b^{[2]} \in U$, where $a = a^{[1]} \oplus a^{[2]}$ and $b = b^{[1]} \oplus b^{[2]}$. Thus, we have $a^{[2]} \oplus b^{[2]} \in U$, that is, $a^{[2]} \oplus b^{[2]} \notin E_1 \times E_2$. From Proposition 5.3.5 and (5.14), we have that

$$\deg\left(D_a D_b \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y)\right) = m - 2.$$

Since the properties $(D1)$ and $(D3)$ are satisfied, we have that $\deg\left(D_a D_b(\pi(y) \cdot x)\right) < m - 2$ and $\deg\left(D_{a_1} D_{b_1} \mathbb{1}_{L^\perp}(x)\right) \leq \dim(L) - 2 < m - 2$. From (5.13), it follows that

$$D_a D_b f \not\equiv 0.$$

If $|\{a^{[2]} \in U : (a^{[1]} \oplus a^{[2]}) \in V\}| \leq 2$, then $|V \cap (E_1 \times E_2)| \geq 2^{m-1}$ (since $|V| = 2^m$). From property $(D1)$ and $\pi(E_2) = E_1^\perp$, we have

$$|V \cap (E_1 \times E_2)| \geq 2^{m-1} > |E_1| \quad \text{and} \quad |V \cap (E_1 \times E_2)| \geq 2^{m-1} > |E_2|.$$

Moreover, we have that

$$|V \cap (E_1 \times \mathbf{0}_m)| \geq 2 \quad \text{and} \quad |V \cap (\mathbf{0}_m \times E_2)| \geq 2,$$

which can be justified as follows. For instance, assuming that $|V \cap (E_1 \times \mathbf{0}_m)| < 2$ then $|V \cap (E_1 \times E_2)| \leq |E_2|$, which is in contradiction with $|V \cap (E_1 \times E_2)| \geq 2^{m-1} > |E_2|$. Hence, we can select two nonzero vectors $a, b \in V \cap (E_1 \times E_2)$ such that $a = (a_1, \mathbf{0}_m), b = (\mathbf{0}_m, b_2)$.

From (5.13), we have that

$$\begin{aligned} D_a D_b f(x, y) &= a_1 \cdot D_{b_2}\pi(y) \oplus D_a D_b \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y) \\ &= a_1 \cdot D_{b_2}\pi(y), \end{aligned}$$

since $a, b \in V \cap (E_1 \times E_2)$ and therefore $D_a D_b \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2} \equiv 0$. As the property $(D2)$ is satisfied, it holds that $a_1 \cdot D_{b_2}\pi \not\equiv const$. Thus, for any m-dimensional subspace V of $\mathbb{F}_2^m \times \mathbb{F}_2^m$ we can find nonzero $a, b \in V$ such that $D_a D_b f \not\equiv 0$. □

As an immediate consequence of the previous result, we present the following explicit family of bent functions in $\mathcal{CD}$ outside $\mathcal{M}^\#$. We will define it using a finite field notation.

Proposition 5.3.7. *Let $n = 2m$, m even, and s be a positive divisor of m such that m/s is odd. Let $\pi(y) = y^d$ be a permutation on $\mathbb{F}_{2^m}$ such that $d(2^s+1) \equiv 1 \pmod{2^m-1}$ and $wt(d) \geq 3$. Let $L = \langle 1, \alpha, \ldots, \alpha^{s-1} \rangle$, where α is a primitive element of $\mathbb{F}_{2^s}$, $E_2 = \langle \alpha^{\frac{2^s-1}{3}}, \alpha^{\frac{2(2^s-1)}{3}} \rangle$ and $E_1 = E_2^{\perp}$. Then, the function $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ defined by*

$$f(x,y) = Tr_1^m(xy^d) + \mathbb{1}_{L^{\perp}}(x) + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y),\ x, y \in \mathbb{F}_{2^m},$$

is a bent function in $\mathcal{CD}$ outside $\mathcal{M}^{\#}$.

Proof. From [88, Theorem 9] we know that (π^{-1}, L) satisfies the (C) property. Since m is even and m/s is odd, we must have that s is even. Thus, $2^2 - 1 = 3 | 2^s - 1$ and furthermore E_2 is not only a vector space but also corresponds to a subfield $\{0, 1, \alpha^{\frac{2^s-1}{3}}, \alpha^{\frac{2(2^s-1)}{3}}\}$ of $\mathbb{F}_{2^s}$. Since π is a monomial permutation, it must map every subfield to itself, thus $\pi(E_2) = E_2 = E_1^{\perp}$. Since $\mathrm{wt}(d) \geq 3$, from [88, Proposition 5], we have that $Tr_1^m(u\pi(y))$ admits no linear structures, for any $u \in \mathbb{F}_{2^m}^*$. Since $\dim(E_2) = 2$, we have that $\dim(E_1) = m - 2$. Hence, the conditions $(C1)$ and $(D1) - (D3)$ of Theorems 2.2.6 and 2.2.7, respectively, are satisfied. From Theorem 5.3.6, it follows that f is a bent function in $\mathcal{CD}$ outside $\mathcal{M}^{\#}$. □

Example 5.3.8. Let $m = 6$, $s = 2$ and $d = 38$. One can easily verify that $d(2^s + 1) \equiv 1 \pmod{2^m - 1}$. With respect to the notation in Proposition 5.3.7, we have that for $E_2 = \mathbb{F}_{2^2}$ and $E_1 = E_2^{\perp}$ the function $f : \mathbb{F}_{2^6} \times \mathbb{F}_{2^6} \to \mathbb{F}_2$ defined by

$$f(x,y) = Tr_1^6(xy^{38}) + \mathbb{1}_{E_1}(x)(1 + \mathbb{1}_{E_2}(y)),\ x, y \in \mathbb{F}_{2^6},$$

is a bent function in $\mathcal{CD}$ and is outside $\mathcal{M}^{\#}$.

Remark 5.3.9. Especially, for $m = 6$, we inspected all possible choices for L, E_1 and E_2 such that either $\dim(L) = \dim(E_2) = 2$ or 3, (π^{-1}, L) satisfies the (C) property and $\pi(E_2) = E_1^{\perp}$, where $\pi(y) = y^{38}$ is a fixed permutation on $\mathbb{F}_{2^6}$. Using the mathematical software Sage, we were able to construct 500 functions $f \in \mathcal{CD}$ of the form (5.11) for the fixed permutation π given above. Furthermore, all of them are outside $\mathcal{M}^{\#}$. With the same notation as in the example above, we could also confirm that the function f is pairwise EA-inequivalent to the functions $f_1(x,y) = Tr_1^6(xy^{38}) + \mathbb{1}_{E_1}(x) \in \mathcal{C}$ and $f_2(x,y) = Tr_1^6(xy^{38}) + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2} \in \mathcal{D}$. The question whether (some of) these functions induce distinct EA-equivalent classes is left open.

We now provide one more example of bent functions in $\mathcal{CD}$ outside $\mathcal{M}^{\#}$, for larger n.

Example 5.3.10. Let $m = 9$ and $d = 284$. We note that $d(2^3 + 1) \bmod (2^9 - 1) = 1$, $\mathrm{wt}(d) = 4$ and $d \bmod (2^3 - 1) = 4$. Let $L =$

$\langle 1, \alpha, \alpha^2 \rangle$ and $E_2 = \langle \alpha, \alpha^2 \rangle$, where α is a primitive element of $\mathbb{F}_{2^3}$ such that $\alpha^3 + \alpha + 1 = 0$. From [88, Theorem 9], we know that (π^{-1}, L) satisfies the (C) property. We further observe that E_2 is a 2-dimensional subspace of $\mathbb{F}_{2^6}$. Let us show that $\pi(E_2) = E_2$. From $\alpha^3 = \alpha + 1$ we have that $\alpha^4 = \alpha + \alpha^2$. Because α is an element in the small field $\mathbb{F}_{2^3}$, we consider its exponent modulo $2^3 - 1$. Thus, we have that:

$$\begin{aligned} 0^d &= 0, \\ \alpha^d &= \alpha^4 = \alpha + \alpha^2, \\ (\alpha^2)^d &= (\alpha^2)^4 = \alpha^8 = \alpha, \\ (\alpha + \alpha^2)^d &= (\alpha^4)^d = \alpha^{16} = (\alpha^8)^2 = \alpha^2. \end{aligned}$$

In other words, $\pi(E_2) = E_2 = E_1^{\perp}$. Since $\mathrm{wt}(d) \geq 3$, from [88, Proposition 5], we have that $Tr_1^m(u\pi)$ does not admit linear structures, for any $u \in \mathbb{F}_{2^m}^*$. Since $\dim(E_2) = 2$, we have that $\dim(E_1) = m - 2$. Hence the conditions $(C1)$ and $(D1) - (D3)$ of Theorems 2.2.6 and 2.2.7, respectively, are satisfied. From Theorem 5.3.6, it follows that the function $f : \mathbb{F}_{2^9} \times \mathbb{F}_{2^9} \to \mathbb{F}_2$ defined by

$$f(x, y) = Tr_1^9(xy^d) + \mathbb{1}_S(x, y), \ x, y \in \mathbb{F}_{2^9},$$

is a bent function in $\mathcal{CD}$ outside $\mathcal{M}^{\#}$, where $\mathbb{1}_S(x, y) = 1$ if and only if $(x, y) \in S$ and $S = (L^{\perp} \times \mathbb{F}_{2^m}) \triangle (E_1 \times E_2)$ (see Remark 5.3.4), and equals 0 otherwise. From (5.12), it is clear that $\mathbb{1}_S$ modifies the truth table of $g(x, y)$ at $2^{9+6} = 2^{15}$ positions. Furthermore, S is neither a linear nor an affine subspace.

With the same notation as in Example 5.3.10, Table 5.1 illustrates the bentness and algebraic degree of the Boolean function $f : \mathbb{F}_{2^9} \times \mathbb{F}_{2^9} \to \mathbb{F}_2$ defined as

$$f(x, y) = Tr_1^9(xy^d) + a_0 \mathbb{1}_{L^{\perp}}(x) + a_1 \mathbb{1}_{E_1}(x) \mathbb{1}_{E_2}(y) + a_2 \delta_0(x), \qquad (5.15)$$

for all possible values $a_0, a_1, a_2 \in \mathbb{F}_2$.

$(a_0, a_1, a_2) \in \mathbb{F}_2^3$	Algebraic degree	Bent	Class
$(0, 0, 0)$	5	yes	$\mathcal{M}$
$(0, 0, 1)$	9	yes	$\mathcal{D}_0 \setminus \mathcal{M}^{\#}$
$(0, 1, 0)$	9	yes	$\mathcal{D} \setminus \mathcal{M}^{\#}$
$(0, 1, 1)$	9	no	-
$(1, 0, 0)$	5	yes	$\mathcal{C} \setminus \mathcal{M}^{\#}$
$(1, 0, 1)$	9	yes	$\mathcal{SC} \setminus \mathcal{M}^{\#}$
$(1, 1, 0)$	9	yes	$\mathcal{CD} \setminus \mathcal{M}^{\#}$
$(1, 1, 1)$	9	no	-

Table 5.1: Class inclusion in $\mathcal{M}^{\#}$ of the Boolean function f defined by (5.15)

As a generalization of Example 5.3.10, we give the following result which regards the case $n = 2m$ where m is odd.

Proposition 5.3.11. *Let $n = 2m$, $m = 3l$ is odd and r be a positive integer such that $\gcd(r, 3l) = 3$ and $d(2^r + 1) \equiv 1 \mod 2^m - 1$ with $\mathrm{wt}(d) \geq 3$. Let $L = \langle 1, \alpha, \alpha^2 \rangle$ and $E_2 = \langle \alpha, \alpha^2 \rangle$ and $E_1 = E_2^{\perp}$, where α is a primitive element of $\mathbb{F}_{2^3}$ such that $\alpha^3 + \alpha + 1 = 0$. Then the function $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ defined by*

$$f(x, y) = Tr_1^m(xy^d) + \mathbb{1}_{L^{\perp}}(x) + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y), \ x, y \in \mathbb{F}_{2^m},$$

is a bent function in $\mathcal{CD}$ outside $\mathcal{M}^{\#}$.

Proof. Because $\gcd(r, 3l) = 3$ and $m/3 = l$ is odd, by [88, Theorem 9], we have that (ϕ, L) satisfies the (C) property, where $\phi(x) = x^{2^r+1}$ is a permutation of $\mathbb{F}_{2^m}$ and $L = \langle 1, \alpha, \alpha^2 \rangle$. Furthermore, since $\pi(x) = x^d$ is the inverse of ϕ and $\mathrm{wt}(d) \geq 3$, we know that $Tr_1^m(u\pi)$ has no nonzero linear structures for any $u \in \mathbb{F}_{2^m}^*$. Now, we prove that $d \mod (2^3 - 1) = 4$. It is well-known that $\gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a,b)} - 1$. Thus, $\gcd(2^{3l} - 1, 2^3 - 1) = 2^3 - 1$. Furthermore, if $a \equiv b \mod N$ and $M|N$, then $a \equiv b \mod M$. Hence, we have that $d(2^r + 1) \equiv 1 \mod 2^3 - 1$. Since $(2^3 - 1)|(2^r - 1) = (2^r + 1 - 2)$, we have that $2^r + 1 \equiv 2 \mod 2^3 - 1$. From the last two congruences, we conclude that $2d \equiv 1 \mod 7$ and it is easy to compute that $d \equiv 4 \mod 7$. From $\alpha^3 = \alpha + 1$ we have that $\alpha^4 = \alpha + \alpha^2$. Because α is an element in the small field $\mathbb{F}_{2^3}$, we consider its exponent modulo $2^3 - 1$. Thus, we have that:

$$\begin{aligned} 0^d &= 0, \\ \alpha^d &= \alpha^4 = \alpha + \alpha^2, \\ (\alpha^2)^d &= (\alpha^2)^4 = \alpha^8 = \alpha, \\ (\alpha + \alpha^2)^d &= (\alpha^4)^d = \alpha^{16} = (\alpha^8)^2 = \alpha^2. \end{aligned}$$

In other words, $\pi(E_2) = E_2 = E_1^{\perp}$. Since $\dim(E_2) = 2$, we have that $\dim(E_1) = m - 2$. Hence, the conditions $(C1)$ and $(D1) - (D3)$ of Theorems 2.2.6 and 2.2.7, respectively, are satisfied. From Theorem 5.3.6, it follows that the function $f : \mathbb{F}_{2^9} \times \mathbb{F}_{2^9} \to \mathbb{F}_2$ defined by

$$f(x, y) = Tr_1^m(xy^d) + \mathbb{1}_{L^{\perp}}(x) + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y), \ x, y \in \mathbb{F}_{2^m},$$

is a bent function in $\mathcal{CD}$ outside $\mathcal{M}^{\#}$. □

Using the software `Wolfram Mathematica`, we could confirm this result, and additionally some suitable values of r and d for different m are listed below.

m	r	d
9	3	284
9	6	228
15	3	18204
15	6	18652
15	9	14116
15	12	14564
21	3	1165084
21	6	935652
21	9	1197788
21	12	899364
21	15	1161500
21	18	932068

5.3.2 Addressing the normality of functions in $\mathcal{CD}$

In [15], it has been shown that if a Boolean function f in $2m$ variables is in the completed $\mathcal{PS}^+$ class, then it is weakly normal. In other words, if a function is weakly non-normal then it lies outside the completed $\mathcal{PS}^+$ class. Recall that a function $f : \mathbb{F}_2^{2m} \to \mathbb{F}_2$ is called *normal* (*weakly normal*) if there exists a flat of dimension m in $\mathbb{F}_2^{2m}$ such that f is constant (affine) on this flat. In this section, we discuss the weak normality of the functions in $\mathcal{CD}$ and propose an interesting research problem regarding them.

Remark 5.3.12. Depending on the choice of L, E_1 and E_2, the functions in $\mathcal{CD}$ are weakly normal in the majority of cases when $\pi(E_2) = E_2 = E_1^{\perp}$.

If $\dim(E_1 \cap L^{\perp}) = \dim(E_1) - 1$ or $E_1 = L^{\perp}$, we can have four possible situations $E_1 = L^{\perp}, L^{\perp} \subset E_1, E_1 \subset L^{\perp}$ and $\dim(E_1) = \dim(L^{\perp}) \wedge \dim(E_1 \cap L^{\perp}) = \dim(E_1) - 1$. We will consider these cases depending if $\pi(E_2) = E_2$ or $\pi(E_2) \neq E_2$.

1. Suppose that $\pi(E_2) = E_2 = E_1^{\perp}$.

   (a) $L^{\perp} = E_1$. If we consider an m-dimensional subspace $E_1 \times E_2$ of $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, we have that $1 + \mathbb{1}_{E_2}(y) = 0$ for all $y \in E_2$. Thus, $\mathbb{1}_{E_1}(x)(1 + \mathbb{1}_{E_2}(y))$ is always equal to 0. On the other hand, because of the choice of E_1 and E_2, we have that $Tr_1^m(x\pi(y)) = 0$ because $x \in E_1$ and $\pi(E_2) = E_1^{\perp}$. Thus, $f|_{E_1 \times E_2} \equiv 0$.

   (b) $L^{\perp} \subset E_1$. If we take $\alpha \in \mathbb{F}_{2^m} \setminus E_1$, we have that $\mathbb{1}_{L^{\perp}}(x) = \mathbb{1}_{E_1}(x) = 0$ for all $x \in \alpha + E_1$. Thus, $\mathbb{1}_{L^{\perp}}(x) + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y)$ vanishes on the m-dimensional flat $(\alpha + E_1) \times E_2$. Furthermore,

for $(x, y) \in (\alpha + E_1) \times E_2$ (w.l.o.g. say $x = \alpha + e_1$) we have:

$$Tr_1^m(x\pi(y)) = Tr_1^m((\alpha + e_1)\pi(y)) = Tr_1^m(\alpha\pi(y)) + \underbrace{Tr_1^m(e_1\pi(y))}_{=0 \text{ (same as in 1.)}}$$

$$= Tr_1^m(\alpha\pi(y)).$$

Since $\pi(E_2) = E_2$ we have that $\{Tr_1^m(\alpha\pi(y)) : y \in E_2\} = \{Tr_1^m(\alpha y) : y \in E_2\}$, which is obviously the truth table of an affine function. Thus, $f|_{(\alpha+E_1)\times E_2}$ is affine.

(c) $E_1 \subset L^\perp$. If we take $\lambda \in L^\perp \setminus E_1$, we have that $\mathbb{1}_{L^\perp}(x) = 1$ and $\mathbb{1}_{E_1}(x) = 0$ for all $x \in \lambda + E_1$. Thus, $\mathbb{1}_{L^\perp}(x) + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y) = 1$ on the m-dimensional flat $(\lambda + E_1) \times E_2$. Similarly as in 2., $Tr_1^m(x\pi(y))$ is affine on this flat. Thus, $f|_{(\lambda+E_1)\times E_2}$ is affine.

(d) $\dim(E_1) = \dim(L^\perp) = m - \mu$, $\dim(E_1 \cap L^\perp) = m - \mu - 1$. Let $U = E_1 + L^\perp$ be the direct sum of E_1 and $L^\perp$. It holds that $\dim(U) = \dim(E_1) + \dim(L^\perp) - \dim(E_1 \cap L^\perp) = m - \mu + 1$. On the other hand, $\dim(E_2) = \mu$.

i. If $\mu = 2$ (all of the known constructions of functions in $\mathcal{D}$ outside $\mathcal{M}^\#$ have $\dim(E_2) = 2$), then $\dim(U) = m - 1$. Let $\alpha \in \mathbb{F}_{2^m} \setminus U$. If we consider the flat $A = (\alpha + U) \times \{0, \beta\}$, where $\beta \in E_2$, we have that $\mathbb{1}_{L^\perp}(x) + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y) = 0$ and $Tr_1^m(x\pi(y))$ is affine for all $(x, y) \in A$. Thus, $f|_A$ is affine.

ii. Suppose $\mu > 2$. Again, we have that $\dim(U) = m - \mu + 1$ and $\dim(E_2) = \mu$. Let W be any $(\mu - 1)$-dimensional subspace of E_2. Then, $\mathbb{1}_{L^\perp}(x) + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y)$ vanishes on $A = (\alpha, 0) + (U \times W)$, where $\alpha \notin U$. Let us consider the function $Tr_1^m(x\pi(y))$. If $x \in \alpha + U$, then w.l.o.g. $x = \alpha + x_u$ for some $x_u \in U$. We have that:

$$Tr_1^m((\alpha + x_u)\pi(y))) = Tr_1^m(\alpha\pi(y)) + Tr_1^m(x_u\pi(y)).$$

We note that if $x_u \in U \setminus E_1$, then $Tr_1^m(x_u\pi(y))$ is not necessarily an affine function and thus we cannot be certain if f is affine on A.

To summarize, we have that f is weakly normal for the situations (a)-(d-i). In the case (d-ii), the question whether f is weakly normal remains open.

The case when $\pi(E_2) \neq E_2$, seems to be more difficult to analyse which leads to the following open problem.

Question 5.3.13. *With the same notation as in Definition 5.3.3, suppose that either $\pi(E_2) \neq E_2$ or $\pi(E_2) = E_2$ with $\dim(E_1) = \dim(L^\perp) = m - \mu$, $\mu > 2$. Is the function f defined by (5.11) weakly normal?*

Remark 5.3.14. Apart from the exclusion from the $\mathcal{PS}$ class, it would be of interest to investigate whether bent functions in $\mathcal{CD}$ may also lie outside the completed classes $\mathcal{C}^{\#}$ and $\mathcal{D}^{\#}$. Apparently, by the definition of $\mathcal{CD}$, the members of $\mathcal{CD}$ cannot lie in $\mathcal{C}$ or $\mathcal{D}$ but due to the lack of indicators for the membership in their completed versions there is no rigorous conclusion concerning this question. Most likely, only certain instances of functions in $\mathcal{CD}$ are outside $\mathcal{C}^{\#}$ and $\mathcal{D}^{\#}$. This however remains to be shown and appears to be a difficult task.

5.4 Bent duals of functions in $\mathcal{C}, \mathcal{D}, \mathcal{SC}$ and $\mathcal{CD}$

In 1993, Carlet determined the bent duals of functions in $\mathcal{D}_0$ [17, Corollary 1] and $\mathcal{D}$ [17, Proposition 1]. In this section, we determine explicitly the bent duals of certain instances of functions in $\mathcal{C}$ not covered by Carlet's result. We also present another approach to determine the duals of certain functions in $\mathcal{D}$ and show that these can be constructed from the $\mathcal{C}$ and $\mathcal{M}$ class. The duals of certain functions in $\mathcal{SC}$ and $\mathcal{CD}$ are also specified and it is shown that these can be used to construct bent functions in $\mathcal{B}_{n+2}$ by concatenating four suitable bent functions in $\mathcal{B}_n$ that stem from these classes. Moreover, we show that the resulting bent functions are outside the $\mathcal{M}^{\#}$ class.

We recall that, by [17, Corollary 1], the following result gives us the bent duals of functions in $\mathcal{D}_0$.

Proposition 5.4.1. *[17] Let $n = 2m$ and π be a permutation on $\mathbb{F}_{2^m}$. Let $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ be a bent function in the $\mathcal{D}_0$ class defined by*

$$f(x, y) = x\pi(y) + \delta_0(x), \ x, y \in \mathbb{F}_{2^m}. \tag{5.16}$$

Then, its dual f^* is also a bent function in $2m$ variables defined by $f^*(x, y) = y\pi^{-1}(x) + \delta_0(y)$.

Throughout this section we will be using the notion of (P_U) property as seen in Lemma 3.1.5.

5.4.1 Bent duals of certain functions in $\mathcal{C}$ and $\mathcal{D}$

In what follows, we determine the bent duals of certain instances of bent functions in $\mathcal{C}$ and $\mathcal{D}$.

Proposition 5.4.2. *($\mathcal{C}$ instance) Let $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ be a bent function defined by*

$$f(x, y) = Tr_1^m(xy^d) + \prod_{i \in I}(Tr_1^m(\alpha^i x) + 1), \ x, y \in \mathbb{F}_{2^m}, \tag{5.17}$$

where α is a primitive element of $\mathbb{F}_{2^s}$, $I \subset \{0, \ldots, s-1\}$, s is a positive divisor of m such that m/s is odd, $d(2^s+1) \equiv 1 \pmod{2^m-1}$ and $wt(d) \geq 3$. Then, the dual $f^* : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ of f is defined by

$$f^*(x,y) = Tr_1^m(x^{2^s+1}y) + \prod_{i \in I}(Tr_1^m(y(\alpha^i x + \alpha^i x^{2^s} + \alpha^{2i})) + 1),\ x, y \in \mathbb{F}_{2^m}.$$

Proof. By [82, Lemma 4.15], it holds that the function $(x,y) \mapsto Tr_1^m(x^{2^s+1}y)$ satisfies the (P_U) property with the defining set $U = \{(\alpha^i, 0) : i = 0, \ldots, s-1\}$ (we note that the general condition is that for all $(u_1,u_2),(v_1,v_2) \in U \subset \mathbb{F}_{2^s} \times \mathbb{F}_{2^s}$ it holds that $u_1v_2 + u_2v_1 = 0$ and $Tr_1^m(u_1^2v_2 + v_1^2u_2) = 0$). Thus, by [82, Theorem 4.17], its dual is defined by

$$f^*(x,y) = Tr_1^m(x^{2^s+1}y) + \prod_{i \in I}(Tr_1^m(y(\alpha^i x + \alpha^i x^{2^s} + \alpha^{2i})) + 1),\ x, y \in \mathbb{F}_{2^m}.$$

□

Notice that $\prod_{i \in I}(Tr_1^m(\alpha^i x) + 1)$ corresponds to the indicator function $\mathbb{F}_{2^m} \ni x \mapsto \mathbb{1}_{L^\perp}(x)$ where $L = \langle \alpha^i : i \in I \rangle$. Furthermore, by [52, Theorem 5.8-(ii)], we can take $L = \langle c_1, \ldots, c_l \rangle$ where $c_i \in \mathbb{F}_{2^s}^*$ for $i = 1, \ldots, l$, so that (π^{-1}, L) satisfies the (C) property, where π is defined as above.

To determine the duals of functions in the $\mathcal{D}$ class, we will use a secondary construction of bent functions in bivariate form introduced in [82]:

Construction 5.4.3. Let $U = \{\mathbf{u}_i = (u_{1,i}, u_{2,i}) : 1 \leq i \leq t\} \subseteq \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, where $1 \leq t \leq m$. Let $g : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ be any bent function function whose dual g^* satisfies the (P_U) property with the defining set U. Let $F(X_1, \ldots, X_t)$ be any reduced polynomial in $\mathbb{F}_2[X_1, \ldots, X_t]$. Then the function $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ defined by

$$f(x,y) = g(x,y) + F(Tr_1^m(u_{1,1}x + u_{1,2}y), \ldots, Tr_1^m(u_{t,1}x + u_{t,2}y))$$

is bent and its dual (by [90, Theorem 2.3]) is defined by

$$f^*(x,y) = g^*(x,y) + F(D_{\mathbf{u}_1}g^*(x,y), \ldots, D_{\mathbf{u}_t}g^*(x,y)). \tag{5.18}$$

Let $\pi(y) = y^d$ and E_2 be a vector subspace corresponding to a subfield in $\mathbb{F}_{2^s}$, where s is a positive divisor of m such that m/s is odd, $d(2^s+1) \equiv 1 \pmod{2^m-1}$ and $\mathrm{wt}(d) \geq 3$. The following lemma shows that the duals g^* of bent functions g in $2m$ variables, defined by $g(x,y) = Tr_1^m(xy^d) + \mathbb{1}_{E_2}(y)$, $x, y \in \mathbb{F}_{2^m}$, satisfy the (P_U) property with the defining set $U = \{0\} \times \mathbf{b}(E_2)$, where $\mathbf{b}(E_2)$ is a basis of E_2.

Lemma 5.4.4. *Let E_2 be a vector space in $\mathbb{F}_{2^m}$ which corresponds to a subfield in $\mathbb{F}_{2^s}$, where s is a positive divisor of m such that m/s is odd, $d(2^s+1) \equiv 1 \pmod{2^m-1}$ and $wt(d) \geq 3$. Let $g : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ be a bent function defined by*

$$g(x,y) = Tr_1^m(xy^d) + \mathbb{1}_{E_2}(y),\ x,y \in \mathbb{F}_{2^m}.$$

Then, its dual is defined by

$$g^*(x,y) = Tr_1^m(x^{2^s+1}y) + \mathbb{1}_{E_2}(x^{2^s+1}),$$

and furthermore $D_aD_bg^* \equiv 0$ for all $a,b \in U = \{0\} \times \mathbf{b}(E_2)$ or $\mathbf{b}(E_2) \times \{0\}$.

Proof. Obviously, the function g is a Maiorana-McFarland function of the form $g(x,y) = Tr_1^m(x\pi(y)) + h(y)$ with $\pi(y) = y^d$ and $h(y) = \mathbb{1}_{E_2}(y)$. Thus, its dual is of the form

$$g^*(x,y) = Tr_1^m(y\pi^{-1}(x)) + h(\pi^{-1}(x)) = Tr_1^m(x^{2^s+1}y) + \mathbb{1}_{E_2}(x^{2^s+1}),\ x,y \in \mathbb{F}_{2^m}.$$

Let $a,b \in U$ and $x,y \in \mathbb{F}_{2^m}$ be arbitrary. Clearly,

$$D_aD_bg^*(x,y) = D_aD_bTr_1^m(yx^{2^s+1}) + D_aD_b\mathbb{1}_{E_2}(x^{2^s+1}).$$

By [82, Lemma 4.15], it holds that $D_aD_bTr_1^m(yx^{2^s+1}) = 0$. On the other hand, because $\mathbb{1}_{E_2}(x^{2^s+1})$ depends only on x, it is easy to note that $D_aD_b\mathbb{1}_{E_2}(x^{2^s+1}) = 0$ for all $x \in \mathbb{F}_{2^m}$ if $a,b \in \{0\} \times E_2$. Hence, g^* satisfies the (P_U) property with the defining set $U = \{0\} \times \mathbf{b}(E_2)$. On the other hand, if $U = \mathbf{b}(E_2) \times \{0\}$, then

$$\begin{aligned} D_aD_b\mathbb{1}_{E_2}(x^{2^s+1}) = {} & \mathbb{1}_{E_2}(x^{2^s+1}) + \mathbb{1}_{E_2}((x+a)^{2^s+1}) + \mathbb{1}_{E_2}((x+b)^{2^s+1}) \\ & + \mathbb{1}_{E_2}((x+a+b)^{2^s+1}). \end{aligned}$$

Now if $x \in E_2$, then $x^{2^s+1}, (x+a)^{2^s+1}, (x+b)^{2^s+1}, (x+a+b)^{2^s+1} \in E_2$ for all $a,b \in \mathbf{b}(E_2)$ and thus $D_aD_b\mathbb{1}_{E_2}(x^{2^s+1}) = 0$. If $x \notin E_2$, as E_2 is a field and $x \mapsto x^{2^s+1}$ is a monomial permutation, the elements of E_2 are mapped to itself and thus $x^{2^s+1} \notin E_2$. Furthermore, since $a \in \mathbf{b}(E_2)$, it must hold that $x+a \notin E_2$ and similarly as before $(x+a)^{2^s+1} \notin E_2$. The same argument holds for $(x+b)^{2^s+1}$ and $(x+a+b)^{2^s+1}$. Thus, $D_aD_b\mathbb{1}_{E_2}(x^{2^s+1}) = 0$ for all $x \in \mathbb{F}_{2^m}$. □

Now, as a direct consequence of Construction 3.1.1 and Lemma 5.4.4, we have the following result which is used to provide the dual of certain instances of bent functions in $\mathcal{D}$, namely in Theorem 5.4.7.

Proposition 5.4.5. *With the same notation as in Lemma 5.4.4, let $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ be defined by*

$$f(x,y) = g(x,y) + \mathbb{1}_{E_1}(x),\ x,y \in \mathbb{F}_{2^m},$$

where $g(x,y) = Tr_1^m(xy^d) + \mathbb{1}_{E_2}(y)$ and $E_1 = E_2^{\perp}$. Then, f is bent and its dual is defined by

$$f^*(x,y) = g^*(x,y) + \prod_{\omega \in \mathbf{b}(E_2)} (Tr_1^m(y(\omega x^{2^s} + \omega x + \omega^2)) + 1),\ x,y \in \mathbb{F}_{2^m}.$$

Proof. By Lemma 5.4.4, g^* satisfies the property (P_U) with the defining set $\mathbf{b}(E_2) \times \{0\}$. Thus, by Construction 3.1.1, the function f defined by

$$f(x,y) = g(x,y) + \prod_{\omega \in \mathbf{b}(E_2)} (Tr_1^m(\omega x) + 1) = g(x,y) + \mathbb{1}_{E_1}(x)$$

is bent. Let us compute the first order derivative of g^* in $(\omega, 0)$ for $\omega \in \mathbf{b}(E_2)$.

$$\begin{aligned} D_{(\omega,0)}g^*(x,y) &= g^*(x,y) + g^*(x+\omega,y) \\ &= Tr_1^m(x^{2^s+1}y) + \mathbb{1}_{E_2}(x^{2^s+1}) + Tr_1^m((x+\omega)^{2^s+1}y) \\ &\quad + \mathbb{1}_{E_2}((x+\omega)^{2^s+1}) \\ &= Tr_1^m(y(\omega x^{2^s} + \omega x + \omega^2). \end{aligned}$$

Thus, by Construction 3.1.1, the dual f^* of f is defined by

$$f^*(x,y) = g^*(x,y) + \prod_{\omega \in \mathbf{b}(E_2)} (Tr_1^m(y(\omega x^{2^s} + \omega x + \omega^2)) + 1),\ x,y \in \mathbb{F}_{2^m}.$$

□

In [57] the author determines the duals for functions obtained by the following secondary construction of bent functions.

Theorem 5.4.6. *[57, Theorem 4] Let n be any positive even integer. Let f_1, f_2 and f_3 be three bent functions on $\mathbb{F}_2^n$. Denote by f_4 the function $f_1 + f_2 + f_3$ and by σ the function $f_1f_2 + f_1f_3 + f_2f_3$. Now, if f_4 is bent and if $f_4^* = f_1^* + f_2^* + f_3^*$, then σ is bent and $\sigma^* = f_1^*f_2^* + f_1^*f_3^* + f_2^*f_3^*$.*

We will now prove that certain functions in $\mathcal{D}$ can be expressed in terms of Theorem 5.4.6 and as a direct consequence we will be able to determine the duals of the corresponding functions in $\mathcal{SC}$ and $\mathcal{CD}$.

Theorem 5.4.7. *($\mathcal{D}$ instances) With the same notation as in Theorem 5.4.6, let $n = 2m$, s be a positive divisor of m such that m/s is odd, and d a positive integer such that $d(2^s+1) \equiv 1\ (mod\ 2^m - 1)$ and $wt(d) \geq 3$.*

Let E_2 be a subfield of $\mathbb{F}_{2^s}$ and $E_1 = E_2^{\perp}$. Let $f_i : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$, $i = 1, 2, 3, 4$, be defined by:

$$\begin{aligned} f_1(x,y) &= Tr_1^m(xy^d), \\ f_2(x,y) &= Tr_1^m(xy^d) + \mathbb{1}_{E_1}(x), \\ f_3(x,y) &= Tr_1^m(xy^d) + \mathbb{1}_{E_2}(y), \\ f_4(x,y) &= f_1(x,y) + f_2(x,y) + f_3(x,y). \end{aligned}$$

Then, using $\sigma = f_1 f_2 + f_1 f_3 + f_2 f_3$, the function $\sigma(x,y) = Tr_1^m(xy^d) + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y)$ is bent and its dual is defined by

$$\begin{aligned} \sigma^*(x,y) &= Tr_1^m(x^{2^s+1}y) \\ &\quad + \prod_{\omega \in \mathbf{b}(E_2)} (Tr_1^m(\omega x^{2^s+1}) + 1)(Tr_1^m(y(\omega x + \omega x^{2^s} + \omega^2)) + 1). \end{aligned} \tag{5.19}$$

Proof. Firstly, by Proposition 5.4.5, we have that f_4 is bent and its dual f_4^* is defined by

$$\begin{aligned} f_4^*(x,y) = Tr_1^m(x^{2^s+1}y) + \underbrace{\prod_{\omega \in \mathbf{b}(E_2)} (Tr_1^m(\omega x^{2^s+1}) + 1)}_{\psi_1(x)} + \\ \underbrace{\prod_{\omega \in \mathbf{b}(E_2)} (Tr_1^m(y(\omega x + \omega x^{2^s} + \omega^2)) + 1)}_{\psi_2(x,y)}. \end{aligned} \tag{5.20}$$

From Proposition 5.4.2 and Lemma 5.4.4, it is easy to compute that $f_1^* + f_2^* + f_3^* = f_4^*$. Thus, by Theorem 5.4.6, the function σ is bent. Furthermore,

$$\begin{aligned} \sigma(x,y) &= f_1(x,y)f_2(x,y) + f_1(x,y)f_3(x,y) + f_2(x,y)f_3(x,y) \\ &= Tr_1^m(xy^d) + Tr_1^m(xy^d)\mathbb{1}_{E_1}(x) + Tr_1^m(xy^d) + Tr_1^m(xy^d)\mathbb{1}_{E_2}(y) + \\ &+ Tr_1^m(xy^d) + Tr_1^m(xy^d)\mathbb{1}_{E_2}(y) + Tr_1^m(xy^d)\mathbb{1}_{E_1}(x) + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y) \\ &= Tr_1^m(xy^d) + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y), \end{aligned}$$

that is $\sigma \in \mathcal{D}$, and its dual is defined by:

$$\begin{aligned} \sigma^*(x,y) &= f_1^*(x,y)f_2^*(x,y) + f_1^*(x,y)f_3^*(x,y) + f_2^*f_3^*(x,y) \\ &= Tr_1^m(x^{2^s+1}y) + \psi_1(x)\psi_2(x,y) \\ &= Tr_1^m(x^{2^s+1}y) \\ &\quad + \prod_{\omega \in \mathbf{b}(E_2)} (Tr_1^m(\omega x^{2^s+1}) + 1)(Tr_1^m(y(\omega x + \omega x^{2^s} + \omega^2)) + 1). \end{aligned}$$

□

The above results are used in the next section for specifying the duals of bent functions in $\mathcal{SC}$ and $\mathcal{CD}$.

5.4.2 Duals of bent functions in $\mathcal{SC}$ and $\mathcal{CD}$

Using a similar approach as in Proposition 5.4.5, we will show that certain functions ("parts" of functions in $\mathcal{SC}$ and $\mathcal{CD}$) satisfy the (P_U) property with some defining set, and consequently we will be able to determine the duals of the corresponding functions in $\mathcal{SC}$ and $\mathcal{CD}$.

Proposition 5.4.8. *($\mathcal{SC}$ case) Let $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ be a bent function defined by*

$$f(x,y) = Tr_1^m(xy^d) + \prod_{i \in I} \left(Tr_1^m(\alpha^i x) + 1\right) + \delta_0(x), \ x, y \in \mathbb{F}_{2^m}, \quad (5.21)$$

where α is a primitive element of $\mathbb{F}_{2^s}$, $I \subset \{0, 1, \ldots, s-1\}$, s is a positive divisor of m such that m/s is odd, $d(2^s+1) \equiv 1 \pmod{2^m - 1}$ and $wt(d) \geq 3$. Then, the dual $f^* : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ of f is defined by

$$f^*(x,y) = Tr_1^m(x^{2^s+1}y) + \prod_{i \in I} \left(Tr_1^m(y(\alpha^i x + \alpha^i x^{2^s} + \alpha^{2i})) + 1\right) + \delta_0(y),$$

for $x, y \in \mathbb{F}_{2^m}$.

Proof. Let $g(x,y) = Tr_1^m(xy^d) + \delta_0(x)$. Then, by Proposition 5.4.1, we have that $g^*(x,y) = Tr_1^m(yx^{2^s+1}) + \delta_0(y)$. We will prove that g^* satisfies the (P_U) property with the defining set $U = \{\alpha^i : i \in I\} \times \{0\}$. Let $a, b \in U$ and $x, y \in \mathbb{F}_{2^m}$ be arbitrary. Then,

$$D_a D_b g^*(x,y) = D_a D_b(Tr_1^m(x^{2^s+1}y)) + D_a D_b(\delta_0(y)) = 0,$$

because the first summand is equal to zero by [82, Lemma 4.15] and the second summand is equal to zero since the y-coordinate of a and b is equal to zero. Thus, by [82, Theorem 4.17], the function f is indeed bent and its dual is defined by

$$f^*(x,y) = Tr_1^m(x^{2^s+1}y) + \prod_{i \in I} \left(Tr_1^m(y(\alpha^i x + \alpha^i x^{2^s} + \alpha^{2i})) + 1\right) + \delta_0(y),$$

for $x, y \in \mathbb{F}_{2^m}$. □

Using a similar method, we determine the duals of bent functions in $\mathcal{CD}$.

Theorem 5.4.9. *($\mathcal{CD}$ case) With the same notation as in Theorem 5.4.7, let $\sigma : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ be defined by $\sigma(x,y) = Tr_1^m(xy^d) +$*

$\mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y)$, $x, y \in \mathbb{F}_{2^m}$. *Let* $L \subset E_2$ *be any subspace of* $\mathbb{F}_{2^m}$ *of dimension at least* 2. *Then, the function* $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ *defined by*

$$f(x,y) = \sigma(x,y) + \prod_{\omega \in \mathbf{b}(L)} (Tr_1^m(\omega x) + 1),\ x, y \in \mathbb{F}_{2^m},$$

is bent and its dual is defined by

$$f^*(x,y) = \sigma^*(x,y) + \prod_{\omega \in \mathbf{b}(L)} (Tr_1^m(y(\omega x + \omega x^{2^s} + \omega^2)) + 1),\ x, y \in \mathbb{F}_{2^m}, \tag{5.22}$$

where $\mathbf{b}(L)$ *is the basis of* L.

Proof. Let $a, b \in \mathbf{b}(L) \times \{0\}$ and $x, y \in \mathbb{F}_{2^m}$ be arbitrary. From Theorem 5.4.7, we have that $D_a D_b \sigma^*(x,y) = D_a D_b Tr_1^m(x^{2^s+1}y) + D_a D_b \psi_1(x)\psi_2(x,y)$, where ψ_1, ψ_2 are defined by (5.20). By [82, Lemma 4.15], we have that $D_a D_b Tr_1^m(x^{2^s+1}y) = 0$. Let $\lambda \in \mathbf{b}(L) \subset E_2$ be arbitrary. Then,

$$\psi_2(x+\lambda, y) = \prod_{\omega \in \mathbf{b}(E_2)} (Tr1^m(y(\omega x^{2^s} + \omega\lambda + \omega x + \omega\lambda + \omega^2)) + 1) = \psi_2(x,y)$$

and thus $\psi_2(x) = \psi_2(x+a) = \psi_2(x+b) = \psi_2(x+a+b)$. Hence,

$$\begin{aligned}
&D_a D_b \psi_1(x)\psi_2(x,y) = \psi_1(x)\psi_2(x,y) + \psi_1(x+a)\psi_2(x+a,y) \\
&+ \psi_1(x+b)\psi_2(x+b,y) + \psi_1(x+a+b)\psi_2(x+a+b,y)) \\
&= \psi_2(x,y)(\psi_1(x) + \psi_1(x+a) + \psi_1(x+b) + \psi_1(x+a+b) \\
&= \psi_2(x,y)(\mathbb{1}_{E_2}(x^{2^s+1}) + \mathbb{1}_{E_2}((x+a)^{2^s+1}) + \\
&\quad \mathbb{1}_{E_2}((x+b)^{2^s+1}) + \mathbb{1}_{E_2}((x+a+b)^{2^s+1})).
\end{aligned}$$

Because $x \mapsto x^{2^s+1}$ is a monomial permutation and E_2 is a field, it holds that $(x+\lambda)^{2^s+1} \in E_2$ if and only if $x + \lambda \in E_2$, and for $\lambda \in E_2$, it is equivalent to the fact that $x \in E_2$. Thus, as $a, b \in \mathbf{b}(L) \subset E_2$, we have that

$$\begin{aligned}
D_a D_b \psi_1(x)\psi_2(x,y) = \psi_2(x,y)(&\mathbb{1}_{E_2}(x^{2^s+1}) + \mathbb{1}_{E_2}(x^{2^s+1}) \\
&+ \mathbb{1}_{E_2}(x^{2^s+1}) + \mathbb{1}_{E_2}(x^{2^s+1})) = 0,
\end{aligned}$$

for all $x, y \in \mathbb{F}_{2^m}$. Hence, σ^* satisfies the (P_U) property with the defining set $\mathbf{b}(L) \times \{0\}$. Consequently, by Construction 3.1.1, the function f is bent and its dual is defined by (5.22). □

Chapter 6

Applications of the classes $\mathcal{SC}$ and $\mathcal{CD}$ for the construction of other cryptographically significant mappings

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

One of the goals of this chapter is to address the design of vectorial bent functions (with coordinates in $\mathcal{C}$ or $\mathcal{D}$) weakly/strongly outside $\mathcal{M}^{\#}$ introduced in [88]. Similarly to the Boolean case, these vectorial objects may provide better understanding related to more complete classification of these structures.

6.1.1 New families of (vectorial) bent functions weakly/almost strongly outside $\mathcal{M}^{\#}$

In this section we construct several infinite families of bent functions lying weakly and almost strongly outside the class $\mathcal{M}^{\#}$. We use the construction method presented in [4] and show that with some additional constraints, we are able to give an univariate definition of vectorial bent functions whose (certain) components are outside $\mathcal{M}^{\#}$. In this section, we address the case when only some components are outside the class $\mathcal{M}^{\#}$, whilst in the next section we consider the design of functions strongly outside $\mathcal{M}^{\#}$.

Let us define $F : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ with $F(x, y) = x\pi(y) + g(y)$, where $\pi : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ is a permutation and $g : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ is an arbitrary function. Let $\lambda \in \mathbb{F}_{2^m}^*$ be arbitrary, we then have the component $F_\lambda(x, y) = Tr_1^m(\lambda x\pi(y) + \lambda g(y))$. Its corresponding dual is defined as

(see [96]):

$$F_\lambda^*(x,y) = Tr_1^m\left(y\pi^{-1}(x/\lambda) + \lambda g(\pi^{-1}(x/\lambda))\right),$$

where π^{-1} is the inverse permutation of π. As a generalization of the results in [4], we give the following result.

Lemma 6.1.1. *Let $\alpha_1,\ldots,\alpha_t$ be any t linearly independent elements in $\mathbb{F}_{2^m}^*$, where $1 \le t \le m$. Let $G(x,y) = x\pi(y)$, where π is any permutation over $\mathbb{F}_{2^m}$. Then the dual component G_λ^* satisfies (3.2) with*

$$g_i(x,y) = Tr_1^m\left(\alpha_i\pi^{-1}\left(\frac{x}{\lambda}\right)\right). \tag{6.1}$$

Proof. Let $\lambda, x, y \in \mathbb{F}_{2^m}^*$ and $(w_1,\ldots,w_t),(s_1,\ldots,s_t) \in \mathbb{F}_2^t$ be arbitrary. Let us consider (3.2).

$$\begin{aligned} G_\lambda^*\left(x+\sum_{i=1}^t u_{i,1}w_i, y+\sum_{i=1}^t u_{i,2}s_i\right) &= G_\lambda^*\left(x, y+\sum_{i=1}^t \alpha_i s_i\right) = Tr_1^m\left(\left(y+\sum_{i=1}^t \alpha_i s_i\right)\pi^{-1}\left(\frac{x}{\lambda}\right)\right) \\ &= Tr_1^m\left(y\pi^{-1}\left(\frac{x}{\lambda}\right)\right) + \sum_{i=1}^t s_i Tr_1^m\left(\alpha_i\pi^{-1}\left(\frac{x}{\lambda}\right)\right) \\ &= G_\lambda^*(x,y) + \sum_{i=1}^t s_i g_i(x,y), \end{aligned}$$

where g_i, $i = 1,\ldots,t$, is defined by (6.1). □

As a direct consequence of Theorem 3.1.3 and Lemma 6.1.1, we have the following result.

Theorem 6.1.2. *Let $\alpha_1,\ldots,\alpha_t$ be any t linearly independent elements in $\mathbb{F}_{2^m}^*$, $t|m$. Let $G(x,y) = x\pi(y)$, where π is any permutation over $\mathbb{F}_{2^m}$, and let $\mathbf{h}$ be any vectorial Boolean function from $\mathbb{F}_2^t$ to $\mathbb{F}_{2^t}$. Then the function*

$$F(x,y) = x\pi(y) + \mathbf{h}(Tr_1^m(\alpha_1 y),\ldots,Tr_1^m(\alpha_t y)),$$

generated by Construction 1, is a bent vectorial (n,t)-function.

Remark 6.1.3. We note that specifying $F(x,y) = G(x,y) + \mathbf{H}(x,y) = G(x,y) + \mathbf{H}_1(y)$ with $\mathbf{H}_1(y) = \mathbf{h}(Tr_1^m(\alpha_1 y),\ldots,Tr_1^m(\alpha_t y))$ gives bent functions in $\mathcal{M}$. Hence, we need to identify suitable sets $U = \{u_1,\ldots,u_t\}$ such that $\mathbf{H}$ depends on (x,y) with $x \neq 0$.

In connection with the class $\mathcal{D}_0$, we obtain the following result which holds in general for any permutation π for which the function is in $\mathcal{D}_0 \setminus \mathcal{M}^{\#}$.

Proposition 6.1.4. *Let $G(x,y) = x\pi(y)$ be a bent $(2m,m)$-function, where π is a permutation on $\mathbb{F}_{2^m}$ such that $x \mapsto Tr_1^m(x\lambda\pi(y)) + \delta_0(x) \in \mathcal{D}_0\setminus\mathcal{M}^{\#}$ for $\lambda \in \mathbb{F}_{2^m}^*$ such that $Tr_1^m(\lambda) = 1$. Then, the function $F(x,y) = G(x,y) + \delta_0(x)$ is a bent (n,m)-function weakly outside $\mathcal{M}^{\#}$.*

Proof. For $\lambda \in \mathbb{F}_{2^m}^*$ we have that

$$G_\lambda(x) = Tr_1^m(\lambda x \pi(y)) + \delta_0(x) Tr_1^m(\lambda) = \begin{cases} Tr_1^m(\lambda x \pi(y)) + \delta_0(x), & Tr_1^m(\lambda) = 1 \\ Tr_1^m(\lambda x \pi(y)), & Tr_1^m(\lambda) = 0 \end{cases}$$

In other words, the component G_λ is in $\mathcal{D}_0$ if $Tr_1^m(\lambda) = 1$ and in $\mathcal{M}^\#$ if $Tr_1^m(\lambda) = 0$. This implies that the function F is weakly outside the class $\mathcal{M}^\#$. □

Suppose G satisfies property (3.2) with the defining set $\{u_1, \ldots, u_m\}$, $u_i = (\alpha_i, 0)$, $\alpha_i \in \mathbb{F}_{2^m}^*$. Let $X = (Tr_1^m(u_1 x), \ldots, Tr_1^m(u_m x))$ and let $\mathbf{h}(X) = \delta_0(X)$, i.e. $\mathbf{h}(X) = 1$ if $X = \mathbf{0}_m$, and 0 otherwise. Since

$$\delta_0(X) = 1 \Leftrightarrow X = \mathbf{0}_m \Leftrightarrow Tr_1^m(u_1 x) = \ldots = Tr_1^m(u_m x) = 0 \Leftrightarrow x = 0 \Leftrightarrow \delta_0(x) = 1$$

we conclude that

$$G(x, y) + \mathbf{h}(Tr_1^m(\alpha_1 x), \ldots, Tr_1^m(\alpha_m x)) \Leftrightarrow G(x, y) + \delta_0(x).$$

In other words, the function F in Proposition 6.1.4 may be obtained using Construction 3.1.1.

Remark 6.1.5. In [67], the authors give an example of a vectorial bent function weakly outside $\mathcal{M}^\#$, constructed from the class $\mathcal{D}_0$. It is defined as follows: $F' = (f_1, \ldots, f_m)$, where $f_i : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ is defined by $f_i(x, y) = Tr_1^m(\alpha_i \pi(y) x) + x^{2^m - 1} + 1$, $1 \leq i \leq m$ and $(\alpha_1, \alpha_2, \ldots, \alpha_m) = (1, \gamma, \gamma^2, \ldots, \gamma^{2^{m-1}}) \in \mathcal{D}_0 \setminus \mathcal{M}^\#$, where γ is a primitive element of $\mathbb{F}_{2^m}$ and π is a permutation on $\mathbb{F}_{2^m}$. We note that the function constructed in Proposition 6.1.4 is the same as the one constructed in [67], but written in univariate form.

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

For a bent $(2m, m)$-function $G(x, y) = x\pi(y)$, let

$$G_\lambda(x, y) = Tr_1^m(\lambda x \pi(y)) = Tr_1^m(x \pi_\lambda(y))$$

denote its components, $\pi_\lambda = \lambda\pi$, $\lambda \in \mathbb{F}_{2^m}^*$. Suppose that for the permutation π there exists a subfield $L = \mathbb{F}_{2^t}$, $t|m$, of $\mathbb{F}_{2^m}$ (which corresponds to a linear subspace in $\mathbb{F}_2^m$) such that (π^{-1}, L) satisfies the (C) property. It is natural to ask, does this imply that (π_λ^{-1}, L) satisfies the (C) property. Depending on these results we can possibly define criteria for which the components of a certain vectorial bent function are in $\mathcal{C}$ (or $\mathcal{D}$) outside $\mathcal{M}^\#$ and give methods for their construction such that they are weakly/strongly outside $\mathcal{M}^\#$. Motivated by these questions, we give the following results.

Proposition 6.1.6. *Let π be a permutation of $\mathbb{F}_{2^m}$ and $L = \mathbb{F}_{2^t}$ be a subfield of $\mathbb{F}_{2^m}$ such that (π^{-1}, L) satisfies the (C) property. Then, for any $\lambda \in \mathbb{F}_{2^m}^*$, the pair $(\pi_\lambda^{-1}, \lambda L)$ satisfies the (C) property.*

Proof. Let $\lambda \in \mathbb{F}_{2^m}^*$ be arbitrary. For the permutation $\pi_\lambda(y) = \lambda\pi(y)$, its inverse is defined by $\pi_\lambda^{-1}(y) = \pi^{-1}\left(\frac{y}{\lambda}\right)$. Let $a \in \mathbb{F}_{2^m}$ be arbitrary. Then

$$\pi_\lambda^{-1}(a + \lambda L) = \pi^{-1}\left(\frac{a + \lambda L}{\lambda}\right) = \pi^{-1}\left(\frac{a}{\lambda} + L\right).$$

Since $a \in \mathbb{F}_{2^m}$ is arbitrary, so is $a/\lambda \in \mathbb{F}_{2^m}$. Thus, it follows that $(\pi_\lambda^{-1}, \lambda L)$ satisfies the (C) property. □

Corollary 6.1.7. *Let π be a permutation of $\mathbb{F}_{2^m}$ and $L = \mathbb{F}_{2^t}$ a subfield of $\mathbb{F}_{2^m}$ such that (π^{-1}, L) satisfies the (C) property. Then, for any $\lambda \in L \subset \mathbb{F}_{2^m}^*$, the pair (π_λ^{-1}, L) satisfies the (C) property.*

Given the behaviour of the components regarding (C) property, we give the following result which gives us an infinite family of bent $(2m, m)$-functions weakly outside $\mathcal{M}^{\#}$.

Proposition 6.1.8. *Let s be a positive divisor of m such that m/s is odd. Let $U = \{1, \alpha, \ldots, \alpha^{t-1}\}$ be t linearly independent elements in $\mathbb{F}_{2^s}^*$, α is a primitive element in $\mathbb{F}_{2^s}$ and $t|m$. Let $G(x, y) = x\pi(y)$, where $\pi(y) = y^d$ is a permutation on $\mathbb{F}_{2^m}$ for a positive integer d such that $\mathrm{wt}(d) \geq 3$ and $d(2^s + 1) \equiv 1 \pmod{2^m - 1}$. Then (π^{-1}, L), $L = \langle U \rangle$, satisfies the (C) property and the function*

$$F(x, y) = xy^d + \mathbf{h}(Tr_1^m(x), Tr_1^m(\alpha x), \ldots, Tr_1^m(\alpha^{t-1}x)),$$

where $\mathbf{h} : \mathbb{F}_2^t \to \mathbb{F}_2$ is defined by $\mathbf{h}(X_1, \ldots, X_t) = \prod_{i=1}^t (X_i + 1)$, with $X_i = Tr_1^m(\alpha^{i-1}x)$, is a bent $(2m, m)$-function weakly outside $\mathcal{M}^{\#}$.

Proof. From Theorem 3.2.9 we know that F is a bent (n, m)-function. Let $\lambda \in \mathbb{F}_{2^m}^*$ be arbitrary. Then,

$$F_\lambda(x) = Tr_1^m(\lambda xy^d) + \mathbf{H}(x)Tr_1^m(\lambda) = \begin{cases} Tr_1^m(\lambda xy^d) + \mathbf{H}(x), & Tr_1^m(\lambda) = 1 \\ Tr_1^m(\lambda xy^d), & Tr_1^m(\lambda) = 0. \end{cases}$$

If $Tr_1^m(\lambda) = 0$, then the component F_λ is obviously in $\mathcal{M}^{\#}$. If $Tr_1^m(\lambda) = 1$, then from Corollary 6.1.7 and Theorem 2.2.6 we have that F_λ is in $\mathcal{C}$ outside $\mathcal{M}^{\#}$ (we again point out that the function $\mathbf{h}$ can be chosen arbitrarily thanks to Theorem 3.1.3, and in this case it represents the indicator of the space $L^\perp$ in finite field notation, which ultimately led to the components being in $\mathcal{C}$ outside $\mathcal{M}^{\#}$, thanks to Theorem 2.2.6). □

Similarly, we can construct another infinite family of bent $(2m, m)$-functions weakly outside $\mathcal{M}^{\#}$ using the $\mathcal{SC}$ class.

Proposition 6.1.9. *Let s be a positive divisor of m such that m/s is odd. Let $U = \{1, \alpha, \ldots, \alpha^{t-1}\}$ be t linearly independent elements in $\mathbb{F}_{2^s}^*$, α is a primitive element in $\mathbb{F}_{2^s}$ and $t|m$. Let $G(x, y) = x\pi(y)$, where $\pi(y) = y^d$ is a permutation on $\mathbb{F}_{2^m}$ for a positive integer d such that $\mathrm{wt}(d) \geq 3$ and $d(2^s + 1) \equiv 1 \pmod{2^m - 1}$. Then (π^{-1}, L), $L = \langle U \rangle$, satisfies the (C) property and the function*

$$F(x, y) = xy^d + \mathbf{h}(Tr_1^m(x), Tr_1^m(\alpha x), \ldots, Tr_1^m(\alpha^{t-1}x)) + \delta_0(x),$$

where $\mathbf{h} : \mathbb{F}_2^t \to \mathbb{F}_2$ is defined by $\mathbf{h}(X_1, \ldots, X_t) = \prod_{i=1}^{t}(X_i + 1)$, with $X_i = Tr_1^m(\alpha^{i-1}x)$, is a bent $(2m, m)$-function weakly outside $\mathcal{M}^\#$.

Proof. Let $\lambda \in \mathbb{F}_{2^m}^*$ be arbitrary. Then,

$$\begin{aligned} F_\lambda(x) &= Tr_1^m(\lambda x y^d) + (\mathbf{H}(x) + \delta_0(x))Tr_1^m(\lambda) \\ &= \begin{cases} Tr_1^m(\lambda x y^d) + \mathbf{H}(x) + \delta_0(x), & Tr_1^m(\lambda) = 1 \\ Tr_1^m(\lambda x y^d), & Tr_1^m(\lambda) = 0. \end{cases} \end{aligned}$$

If $Tr_1^m(\lambda) = 0$, then the component F_λ is obviously in $\mathcal{M}^\#$. If $Tr_1^m(\lambda) = 1$, then from Corollary 5.1.6 we have that F_λ is in $\mathcal{SC}$ outside $\mathcal{M}^\#$. □

Example 6.1.10. Let $m = 6$ and $\lambda = \alpha^{\frac{2^m-1}{3}}$, where α is a primitive element of $\mathbb{F}_{2^m}$. If we choose $L = \langle 1, \lambda \rangle$ and $\pi(y) = y^{38}$, then (π^{-1}, L) satisfies the (C) property (see [88, Example 1]) and $\mathrm{wt}(38) = 3$, that is, π admits no linear structures. Hence, the function

$$F(x, y) = xy^{38} + (Tr_1^m(x) + 1)(Tr_1^m(\lambda x) + 1)$$

is a bent $(12, 6)$-function weakly outside $\mathcal{M}^\#$. Notice that the expression $(Tr_1^m(x) + 1)(Tr_1^m(\lambda x) + 1)$ specifies the indicator function in finite field notation.

The previous result can be extended to a more general case as follows.

Theorem 6.1.11. *Let $n = 2m > 8$ be an even integer and let $G(x, y) = Tr_t^m(x\pi(y))$ be a bent (n, t)-function, π is a permutation of $\mathbb{F}_{2^m}$, such that $(G_\lambda^*)_{\lambda \in \mathbb{F}_{2^t}^*}$ satisfies the property (3.2) with $U = \{u_1, \ldots, u_t\}$, $u_i = (\alpha^{i-1}, 0)$, α is a primitive element of $\mathbb{F}_{2^t}$, $t|m$. If $(\pi^{-1}, \mathbb{F}_{2^t})$ satisfies the (C) property, $\dim(\mathbb{F}_{2^t}) \geq 2$ and $Tr_1^m(\mu\pi)$ has no nonzero linear structures for $\mu \in \mathbb{F}_{2^m}^*$, then the function*

$$F(x, y) = Tr_t^m(x\pi(y)) + \mathbf{H}(x)$$

with

$$\mathbf{H}(x) = \mathbf{h}(Tr_1^m(x), Tr_1^m(\alpha x), \ldots, Tr_1^m(\alpha^{t-1}x)) = \prod_{i=1}^{t}(Tr_1^m(\alpha^{i-1}x) + 1),$$

is a bent (n, t)-function weakly outside $\mathcal{M}^\#$.

The proof is similar to the proof of Proposition 6.1.8.

Some remarks on functions in $\mathcal{C}$ and the (C) property

In reference to the results given in Proposition 6.1.6 and Corollary 6.1.7, the following question is quite natural: If (π^{-1}, L) satisfies the (C) property and $\lambda \notin L$, does this imply that (π_λ^{-1}, L) satisfies the (C) property?

In [17], the author defines the $\mathcal{C}$ class to be the family of all bent functions of the form $x\pi(y) + \mathbb{1}_{L^\perp}(x)$, where (π^{-1}, L) satisfies the (C) property. However, can we have functions of the same form that are bent but (π^{-1}, L) does not satisfy the (C) property. More specifically, can we have that (π^{-1}, L) satisfies the (C) property but (π_λ^{-1}, L) does not, and furthermore the function $x\pi_\lambda(y) + \mathbb{1}_{L^\perp}(x)$ is bent, where $\lambda \in \mathbb{F}_{2^m}^*$?

Let $n = 2m > 8$ be an even integer and let $G(x, y) = x\pi(y)$ be a bent (n, m)-function, π is a permutation of $\mathbb{F}_{2^m}$, such that G_λ^* satisfies the property (3.2) with $U = \{u_1, \ldots, u_t\}$, $u_i = (\alpha^{i-1}, 0)$, where $\lambda \in \mathbb{F}_{2^m}^*$ and α is a primitive element of $\mathbb{F}_{2^t}$, $t|m$. From Theorem 3.1.3, we know that the function

$$F(x, y) = x\pi(y) + \mathbf{H}(x)$$

with

$$\mathbf{H}(x) = \mathbf{h}(Tr_1^m(x), Tr_1^m(\alpha x), \ldots, Tr_1^m(\alpha^{t-1}x)) = \prod_{i=1}^{t}(Tr_1^m(\alpha^{i-1}x) + 1),$$

is a bent (n, m)-function, where $\mathbf{H}$ is the indicator function in finite field notation. When considering the components of F, they are exactly of the form $x\pi_\lambda(y) + Tr_1^m(\lambda)\mathbf{H}(x)$, $\lambda \in \mathbb{F}_{2^m}^*$, and all of them are bent. However, we did not give any information on the (C) property. Thus, the following question arises.

Question 1: Does there exist a bent (n, m)-function $G(x, y) = x\pi(y)$ such that the conditions of Theorem 3.1.3 with defining set U are satisfied, but (π^{-1}, L) does not satisfy the (C) property and $L = \langle U \rangle$, where U is the defining set in property (3.2).

We note the following result which is a direct consequence of [17, Theorem].

Proposition 6.1.12. *[17] Let $L \times \{0\}$ be any linear subspace in $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$. Then the function $f(x, y) + \mathbb{1}_{L^\perp}(x)$ is bent **if and only if** for any $(\alpha, \beta) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ the restriction of $f^*(x, y)$ to $(\alpha, \beta) + (L \times \{0\})$ is either constant or balanced.*

As a corollary of the above proposition, the author notes that if (π^{-1}, L) satisfies the (C) property, then the restriction of $f^*(x, y)$ to $(\alpha, \beta) + (L \times \{0\})$ is either constant or balanced, which implies the bentness of f^*. However, there might be instances of functions such that (π^{-1}, L) does not satisfy the (C) property but the restriction of $f^*(x, y)$ to $(\alpha, \beta) + (L \times \{0\})$ is still either constant or balanced.

All examples of functions $G \in \mathcal{M}^{\#}$ which satisfy (3.2) are either linear or power permutations. In the case of power permutations the answer is clear. If $\pi(y) = y^d$ is a permutation of $\mathbb{F}_{2^m}$ then its inverse is also a power permutation, say $\phi(y) = \pi^{-1}(y) = y^s$. For $\lambda \in \mathbb{F}_{2^m}^*$ we have that

$$\phi_\lambda(a + L) = \phi(\lambda^{-1}(a + L)) = \lambda^{-s}(a + L)^s = \lambda^{-s}\phi(a + L),$$

that is, if $\phi(a + L)$ is a flat, then $\phi_\lambda(a + L)$ is also a flat and (ϕ_λ, L) satisfies the (C) property.

In connection to this discussion, we give the following example where (ϕ, L) satisfies the (C) property but (ϕ_λ, L) does not.

Example 6.1.13. Let $\phi(x) = x^9 + x^3 + x$ be a permutation defined on $\mathbb{F}_{2^5}$. For $L = \langle \alpha^2 + \alpha, \alpha^4 + 1\rangle$, α is a primitive element of the field $\mathbb{F}_{2^5}$ such that $\alpha^5 + \alpha^2 + 1 = 0$, the pair (ϕ, L) satisfies the (C) property (see [53]). If we take $\lambda = \alpha^2 + \alpha$, then $\lambda^{-1}L = \langle 1, \alpha^3 + 1\rangle$. However, as shown in [53], since $1 \in \lambda^{-1}L$, the pair (ϕ_λ, L), $\phi_\lambda(x) = \phi(\lambda^{-1}x)$, does not satisfy the (C) property.

Thus, an interesting problem for further research can be stated as follows.

Open problem 6.1.14. Find bent (n, m)-functions $G(x, y) = x\pi(y)$ which satisfy property (3.2) and π is not a power permutation.

If such functions G do exist, we might learn more about their behaviour regarding the bentness of F (as constructed in Theorem 3.1.3) and their inclusion in the $\mathcal{C}$ class and connection to the (C) property (Theorem 2.2.6 and Proposition 6.1.12).

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

Up until now, all the examples of vectorial bent functions we gave were weakly outside $\mathcal{M}^{\#}$. The construction of functions that are strongly outside $\mathcal{M}^{\#}$ and additionally of maximal output space is a much harder task. In what follows, we distinguish bent (n, m)-functions which have $2^m - 2$ components outside $\mathcal{M}^{\#}$. In this case, we will say that the function is **almost strongly** outside $\mathcal{M}^{\#}$.

Lemma 6.1.15. *Let α be a primitive element of $\mathbb{F}_{2^m}$. With I_λ we denote the set $\{i : 0 \leq i \leq m - 1, Tr_1^m(\lambda\alpha^i) = 1\}$. Then $|\{\lambda \in \mathbb{F}_{2^m}^* : I_\lambda = \emptyset\}| = 1$.*

Proof. Let us consider the vector

$$v_\lambda = (Tr_1^m(\lambda\alpha), Tr_1^m(\lambda\alpha^2), \ldots, Tr_1^m(\lambda\alpha^{m-1}).$$

Then, $\{v_\lambda : \lambda \in \mathbb{F}_{2^m}\}$ contains all the elements of $\mathbb{F}_2^{m-1}$, each of which appears exactly two times. Obviously, we have $v_\lambda = \mathbf{0}_{m-1}$ for $\lambda = 0$. Thus, there exists a unique $\xi \in \mathbb{F}_{2^m}^*$ for which $v_\xi = \mathbf{0}_{m-1}$. □

Theorem 6.1.16. *Let $n = 2m > 8$ be an even integer and let $G(x, y) = Tr_t^m(x\pi(y))$ be a bent (n, t)-function, π is a permutation of $\mathbb{F}_{2^m}$, such that $(G_\lambda^*)_{\lambda \in \mathbb{F}_{2^t}^*}$ satisfies the property (3.2) with $U = \{u_1, \ldots, u_t\}$, $u_i = (\alpha^{i-1}, 0)$, α is a primitive element of $\mathbb{F}_{2^t}$, $t|m$. If $(\pi_\lambda^{-1}, \langle 1, \tau \rangle)$ satisfies the (C) property for all $\tau \neq 1, \lambda \in \mathbb{F}_{2^t}^*$ and $Tr_1^m(\mu\pi)$ has no nonzero linear structures for $\mu \in \mathbb{F}_{2^m}^*$, then the function*

$$F(x, y) = Tr_t^m(x\pi(y)) + \mathbf{H}(x)$$

with

$$\begin{aligned}\mathbf{H}(x) &= \mathbf{h}(Tr_1^m(x), Tr_1^m(\alpha x), \ldots, Tr_1^m(\alpha^{t-1}x)) \\ &= (Tr_1^m(x) + 1) \cdot \left(\sum_{i=1}^{t-1} \alpha^i \left(Tr_1^m(\alpha^i x) + 1 \right) \right),\end{aligned}$$

is a bent (n, t)-function almost strongly outside $\mathcal{M}^{\#}$.

Proof. From Theorem 6.1.2, we know that F is a bent (n, t)-function. Let $\lambda \in \mathbb{F}_{2^t}^*$ be arbitrary. The component F_λ becomes:

$$\begin{aligned}F_\lambda(x) &= Tr_1^t(\lambda Tr_t^m(x\pi(y))) \\ &\quad + (Tr_1^m(x) + 1) \cdot \left(\sum_{i=1}^{t-1} Tr_1^t(\lambda\alpha^i) \left(Tr_1^m(\alpha^i x) + 1 \right) \right). \qquad (6.2)\end{aligned}$$

First, let us suppose that $I_\lambda = \{i : 1 \leq i \leq t-1,\ Tr_1^t(\lambda\alpha^i) = 1\} \neq \emptyset$. We have that

$$\begin{aligned}\sum_{i=1}^{t-1} Tr_1^t(\lambda\alpha^i) \left(Tr_1^m(\alpha^i x) + 1 \right) &= \sum_{i \in I_\lambda} \left(Tr_1^m(\alpha^i x) + 1 \right) \\ &= \sum_{i \in I_\lambda} Tr_1^m(\alpha^i x) + (|I_\lambda| \mod 2).\end{aligned}$$

Thus, (6.2) becomes:

$$\begin{aligned}F_\lambda(x) &= Tr_1^t(Tr_t^m(x\lambda\pi(y))) \\ &\quad + (Tr_1^m(x) + 1) \cdot \left(\sum_{i \in I_\lambda} Tr_1^m(\alpha^i x) + (|I_\lambda| \mod 2) \right) \\ &= Tr_1^m(x\pi_\lambda(y))) + \underbrace{(Tr_1^m(x) + 1) \cdot (Tr_1^m(\xi_\lambda x) + (|I_\lambda| \mod 2))}_{=\psi_\lambda(x)},\end{aligned}$$

where $\xi_\lambda = \sum_{i \in I_\lambda} \alpha^i$. We distinguish two cases:

1. $|I_\lambda| \mod 2 = 1$. Then ψ_λ is exactly the indicator function of the subspace $\langle 1, \xi_\lambda \rangle^\perp$. Furthermore, $1 \neq \xi_\lambda \in \mathbb{F}_{2^t}^*$ and thus $(\pi_\lambda^{-1}, \langle 1, \xi_\lambda \rangle)$ satisfies the (C) property and the conditions of Theorem 2.2.6, thus it follows that F_λ is in $\mathcal{C}$ outside $\mathcal{M}^\#$.

2. $|I_\lambda| \mod 2 = 0$. Then

$$\begin{aligned} F_\lambda(x) &= Tr_1^m(x\pi_\lambda(y)) + (Tr_1^m(x)+1)Tr_1^m(\xi_\lambda x) \\ &= Tr_1^m(x\pi_\lambda(y)) + (Tr_1^m(x)+1)(Tr_1^m(\xi_\lambda x)+1) + (Tr_1^m(x)+1) \\ &= F'_\lambda(x,y) + (Tr_1^m(x)+1) \end{aligned}$$

   The function F'_λ is a bent function in $\mathcal{C}$ outside $\mathcal{M}^\#$ (see Case 1.). Since $Tr_1^m(x)+1$ is an affine function, by adding it to F'_λ, their sum still remains in $\mathcal{C} \setminus \mathcal{M}^\#$. Hence, F_λ is a bent function in $\mathcal{C}$ outside $\mathcal{M}^\#$. We would like to point out that in this case the function $(Tr_1^m(x)+1)Tr_1^m(\xi_\lambda x)$ represents the indicator function of an affine subspace.

On the other hand, if $I_\lambda = \emptyset$, from Lemma 6.1.15 we know that this occurs for exactly one $\lambda \in \mathbb{F}_{2^t}^*$, then $H_\lambda \equiv 0$ and $F_\lambda \in \mathcal{M}$. Thus, $2^t - 2$ components of F are in $\mathcal{C}$ outside $\mathcal{M}^\#$ and one component is in $\mathcal{M}^\#$. In other words, F is almost strongly outside $\mathcal{M}^\#$. □

Especially, if we consider power permutations we obtain the following results.

Lemma 6.1.17. *Let $s > 1$ be a positive divisor of m such that m/s is odd and $\pi(y) = y^d$ be a permutation of $\mathbb{F}_{2^m}$ such that $d(2^s+1) \equiv 1 (mod\ 2^m - 1)$. Let $\tau \neq 1, \lambda \in \mathbb{F}_{2^s}^*$ be arbitrary. Then $(\pi_\lambda^{-1}, \langle 1, \tau \rangle)$ satisfies the (C) property.*

Proof. Since $\gcd(m, s) = s$ and m/s is odd, from [88, Theorem 9] we know that $(\pi^{-1}, \langle 1, \tau \rangle)$ satisfies the (C) property. Thus, for every $a \in \mathbb{F}_{2^m}$, we have that

$$\pi_\lambda^{-1}(a + \langle 1, \tau \rangle) = (\lambda^{-1}(a + \langle 1, \tau \rangle))^{2^s+1} = \lambda^{-(2^s+1)}\pi^{-1}(a + \langle 1, \tau \rangle)$$

which is again a flat. In other words, $(\pi_\lambda^{-1}, \langle 1, \tau \rangle)$ satisfies the (C) property. □

Proposition 6.1.18. *Let $n = 2m$ and $s \geq 2$ be a positive divisor of m such that m/s is odd. Let $\pi(y) = y^d$ be a permutation on $\mathbb{F}_{2^m}$ such that $d(2^s+1) \equiv 1\ (mod\ 2^m - 1)$ and $\mathrm{wt}(d) \geq 3$. Let $U = \{1, \alpha, \ldots, \alpha^{s-1}\}$, where α is a primitive element of $\mathbb{F}_{2^s}$. Then,*

$$F(x,y) = Tr_s^m(xy^d) + \mathbf{H}(x)$$

with

$$\begin{aligned}\mathbf{H}(x) &= \mathbf{h}(Tr_1^m(x), Tr_1^m(\alpha x), \ldots, Tr_1^m(\alpha^{s-1}x)) \\ &= (Tr_1^m(x)+1)\cdot\left(\sum_{i=1}^{s-1}\alpha^i\left(Tr_1^m(\alpha^i x)+1\right)\right),\end{aligned}$$

is a bent (n,s)-function almost strongly outside $\mathcal{M}^{\#}$.

Proof. From Lemma 6.1.17 we know that $(\pi_\lambda^{-1}, \langle 1, \tau\rangle)$ satisfies the (C) property for all $\tau \neq 1, \lambda \in \mathbb{F}_{2^s}^*$. Since $\mathrm{wt}(d) \geq 3$, $(\pi_\lambda^{-1}, \langle 1, \tau\rangle)$ satisfies the conditions of Theorem 2.2.6. From Theorem 3.2.9 and 6.1.16, it follows that F is a bent (n,s)-function almost strongly outside $\mathcal{M}^{\#}$ with components in $\mathcal{C}$. □

Example 6.1.19. Let $m = 9$ and $s = 3$. Suppose that α is a primitive element of $\mathbb{F}_{2^3}$ and let $U = \{1, \alpha, \alpha^2\}$. Since $284\cdot(2^3+1) \mod 2^9-1 = 1$, let $\pi(y) = y^{284}$ be a permutation on $\mathbb{F}_{2^9}$. Then

$$F(x,y) = Tr_3^9(xy^{284}) + (Tr_1^9(x)+1)(\alpha(Tr_1^9(\alpha x)+1) + \alpha^2(Tr_1^9(\alpha^2 x)+1))$$

is a bent $(18,3)$-function almost strongly outside $\mathcal{M}^{\#}$.

The main difference between Theorems 6.1.11 and 6.1.16 is that the function $\mathbf{H}$ in the former case is Boolean, whereas in the latter (almost strongly) case it is a vectorial Boolean function. When considering the component functions, if $\mathbf{H}$ is Boolean, then $Tr_1^m(\lambda H(X)) = Tr_1^m(\lambda)H(X)$, which is why we have only half of the components outside $\mathcal{M}^{\#}$ in Theorem 6.1.11. On the other hand, we noticed that if we consider $\mathbf{H}$ as a vectorial function of certain form, then we can have more non-zero components $Tr_1^m(\lambda\mathbf{H}(X))$, as seen in Theorem 6.1.16. Nevertheless, we need a more subtle modification of the function $\mathbf{H}$ such that no component $Tr_1^m(\lambda\mathbf{H}(X))$ is zero. A family of such functions is proposed in the next section.

6.1.2 New families of vectorial bent functions strongly outside $\mathcal{M}^{\#}$

We now show that by slightly modifying the function $\mathbf{H}$ in Proposition 6.1.18, we can construct an infinite family of bent (n,s)-functions (where the exponent s is chosen as in Proposition 6.1.18) strongly outside $\mathcal{M}^{\#}$.

Theorem 6.1.20. *Let $n = 2m > 8$ be an even integer and let $G(x,y) = Tr_t^m(x\pi(y))$ be a bent (n,t)-function, π is a permutation of $\mathbb{F}_{2^m}$, such that $(G_\lambda^*)_{\lambda\in\mathbb{F}_{2^t}^*}$ satisfies the property (3.2) with $U = \{u_1, \ldots, u_t\}$, $u_i = (\alpha^{i-1}, 0)$, α is a primitive element of $\mathbb{F}_{2^t}$, $t|m$, $t < m$. If $(\pi_\lambda^{-1}, \langle 1, \tau\rangle)$*

satisfies the (C) property for all $\tau \neq 1, \lambda \in \mathbb{F}_{2^t}^*$ *and* $Tr_1^m(\mu\pi)$ *has no nonzero linear structures for all* $\mu \in \mathbb{F}_{2^m}^*$*, then the function*

$$F(x,y) = Tr_t^m(x\pi(y)) + \mathbf{H}(x)$$

with

$$\mathbf{H}(x) = (Tr_1^m(x)+1)\cdot\left(\sum_{i=1}^{t-1}\alpha^i\left(Tr_1^m(\alpha^i x)+1\right)\right) + (x^{2^m-1}+1),$$

is a bent (n,t)*-function strongly outside* $\mathcal{M}^{\#}$*.*

Proof. Let $\lambda \in \mathbb{F}_{2^t}^*$ be arbitrary. The components of F are of the form

$$F_\lambda(x,y) = Tr_1^m(x\lambda\pi(y)) + (Tr_1^m(x)+1)\cdot\left(\sum_{i=1}^{t-1}Tr_1^t(\lambda\alpha^i)\left(Tr_1^m(\alpha^i x)+1\right)\right) + Tr_1^t(\lambda)(x^{2^m-1}+1).$$

If $Tr_1^t(\lambda)=0$, the component F_λ is bent because of Theorem 3.1.3 (and in particular (3.4)) and if $Tr_1^t(\lambda)=1$, the component F_λ is bent because of Theorem 5.1.1. Thus all components are bent, i.e. F is a bent (n,t)-function.

Now we will show that the components are outside $\mathcal{M}^{\#}$. We will distinguish several cases, depending on the value of $Tr_1^m(\lambda\alpha^i)$, for $i = 0,\ldots,t-1$.

1. $Tr_1^t(\lambda)=0$ and $Tr_1^m(\lambda\alpha^i)=1$ for at least one $i=1,\ldots,t-1$. Then the component F_λ is of the form

$$F_\lambda(x,y) = Tr_1^m(x\lambda\pi(y)) + (Tr_1^m(x)+1)(Tr_1^m(\xi_\lambda x) + (|I_\lambda| \mod 2)), \tag{6.3}$$

   where $\xi_\lambda = \sum_{i\in I_\lambda}\alpha^i$ and $I_\lambda = \{i : Tr_1^m(\lambda\alpha^i)=1,\ 1\le i\le t-1\}$. In Theorem 6.1.16 we have already proved that the Boolean functions of form (6.3) are in $\mathcal{C}$ outside $\mathcal{M}^{\#}$.

2. If $Tr_1^m(\lambda)=1$ and $Tr_1^m(\lambda\alpha^i)=0$ for all $i=1,\ldots,t-1$, then F_λ is of the form

$$\begin{aligned} F_\lambda(x,y) &= Tr_1^m(x\lambda\pi(y)) + (Tr_1^m(x)+1)\cdot 0 + (x^{2^m-1}+1) \\ &= Tr_1^m(x\lambda\pi(y)) + x^{2^m-1} + 1, \end{aligned}$$

   that is, F_λ is in the class $\mathcal{D}_0$, and as such outside $\mathcal{M}^{\#}$.

3. $Tr_1^t(\lambda) = 1$ and $Tr_1^m(\lambda\alpha^i) = 1$ for at least one $i = 1, \ldots, t-1$. Then, F_λ is of the form

$$F_\lambda(x,y) = \underbrace{Tr_1^m(x\lambda\pi(y)) + (Tr_1^m(x)+1)\cdot(Tr_1^m(\xi_\lambda x) + (|I_\lambda| \mod 2))}_{=G_\lambda(x,y)} + (x^{2^m-1}+1),$$

where $\xi_\lambda = \sum_{i\in I_\lambda}\alpha^i$ and $I_\lambda = \{i : Tr_1^m(\lambda\alpha^i) = 1,\ 1 \le i \le t-1\}$. We note that $G_\lambda(x,y)$ is a bent Boolean function in the class $\mathcal{C}$ outside $\mathcal{M}^{\#}$ (again, see proof of Theorem 6.1.16). Thus, from Theorem 5.1.4, it follows that F_λ is a bent function in the class $\mathcal{SC}$ outside $\mathcal{M}^{\#}$.

Thus, for all $\lambda \in \mathbb{F}_{2^t}^*$ the component F_λ is outside $\mathcal{M}^{\#}$, in other words, F is strongly outside $\mathcal{M}^{\#}$. □

Remark 6.1.21. Notice that Theorem 6.1.20 generate vectorial bent functions whose components belong to classes $\mathcal{C}, \mathcal{D}_0$ and $\mathcal{SC}$. The class $\mathcal{SC}$ plays an important role here since it allowed us to extend the functions almost strongly outside $\mathcal{M}^{\#}$ to functions strongly outside $\mathcal{M}^{\#}$.

This knowledge on the choice of $\mathbf{H}$ such that it has no non-zero components, allows us to construct vectorial Boolean functions which are strongly outside $\mathcal{M}^{\#}$. We note that if we would extend $\mathbf{H}$ to be an (m,m)-function, we would again obtain a zero component, in the previous construction. In other words, the design method in Theorem 6.1.20 cannot produce vectorial Boolean functions strongly outside $\mathcal{M}^{\#}$ and with maximal output space.

Specially, we give the following infinite family of bent (n,s)-functions strongly outside $\mathcal{M}^{\#}$.

Corollary 6.1.22. *Let $n = 2m$ and $s \ge 2$ be a positive divisor of m such that m/s is odd. Let $\pi(y) = y^d$ be a permutation on $\mathbb{F}_{2^m}$ such that $d(2^s+1) \equiv 1 \pmod{2^m-1}$ and $\mathrm{wt}(d) \ge 3$. Let $U = \{1, \alpha, \ldots, \alpha^{s-1}\}$, where α is a primitive element of $\mathbb{F}_{2^s}$. Then,*

$$F(x,y) = Tr_s^m(xy^d) + \mathbf{H}(x)$$

with

$$\mathbf{H}(x) = (Tr_1^m(x)+1)\cdot\left(\sum_{i=1}^{s-1}\alpha^i\left(Tr_1^m(\alpha^i x)+1\right)\right) + (x^{2^m-1}+1),$$

is a bent (n,s)-function strongly outside $\mathcal{M}^{\#}$.

Proof. Follows directly from Theorem 6.1.20 and Lemma 6.1.17. □

The following example illustrates the specification of a bent $(18, 3)$-function with all components in $\mathcal{C}$ outside $\mathcal{M}^{\#}$, thus with output dimension larger than two, which was obtained in [67].

Example 6.1.23. Let $m = 9$ and $s = 3$. Suppose that α is a primitive element of $\mathbb{F}_{2^3}$ and let $U = \{1, \alpha, \alpha^2\}$. Since $284 \cdot (2^3+1) \mod 2^9-1 = 1$, let $\pi(y) = y^{284}$ be a permutation on $\mathbb{F}_{2^m}$. Let $F : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_{2^s}$ be a function defined by

$$F(x, y) = Tr_3^9(xy^{284}) + (Tr_1^9(x) + 1)(\alpha(Tr_1^9(\alpha x) + 1) + \alpha^2(Tr_1^9(\alpha^2 x) + 1)) + (Tr_1^9(\alpha x) + 1)(Tr_1^9(\alpha^2 x) + 1).$$

From Theorem 3.2.9, we know that F is bent. Let us consider the components of F. With X_i we will denote $Tr_1^9(\alpha^i + 1)$, $i = 0, 1, 2$. For $\lambda \in \mathbb{F}_{2^3}^*$ we have that

$$F_\lambda(x, y) = Tr_1^9(x\lambda y^{284}) + \underbrace{X_0(Tr_1^3(\lambda\alpha)X_1 + Tr_1^3(\lambda\alpha^2)X_2 + Tr_1^3(\lambda)X_1X_2}_{=\psi_\lambda(x)}$$

Let us consider the vector $v_\lambda = (Tr_1^3(\lambda\alpha), Tr_1^3(\lambda\alpha^2), Tr_1^3(\lambda))$ as λ goes through $\mathbb{F}_{2^3}^*$. Using the mathematical software Sage, we note the following (see Table 6.1).

$\lambda \in \mathbb{F}_{2^3}^*$	v_λ	$\psi_\lambda(x)$	$\psi_\lambda(x) = \varphi_\lambda(x) + l(x)$	L
1	$(0,0,1)$	X_1X_2	-	$\langle \alpha, \alpha^2 \rangle$
α	$(0,1,0)$	X_0X_2	-	$\langle 1, \alpha^2 \rangle$
$\alpha+1$	$(0,1,1)$	$(X_0+X_1)X_2$	$(X_0+X_1+1)X_2 + X_2$	$\langle \alpha+1, \alpha^2 \rangle$
α^2	$(1,0,0)$	X_0X_1	-	$\langle 1, \alpha \rangle$
α^2+1	$(1,0,1)$	$(X_0+X_2)X_1$	$(X_0+X_2+1)X_1 + X_1$	$\langle \alpha, \alpha^2+1 \rangle$
$\alpha^2+\alpha$	$(1,1,0)$	$(X_1+X_2)X_0$	$(X_1+X_2+1)X_0 + X_0$	$\langle 1, \alpha+\alpha^2 \rangle$
$\alpha^2+\alpha+1$	$(1,1,1)$	$X_0(X_1+X_2)+X_1X_2$	$(X_0+X_1+1)(X_1+X_2+1)+X_0+X_1+X_2+1$	$\langle \alpha+1, \alpha^2+1 \rangle$

Table 6.1: Behaviour of the function ψ_λ for $\lambda \in \mathbb{F}_{2^3}^*$

Firstly, we note that by adding an affine function l to a bent function f lying in a class $\mathcal{K}$, we will still remain in the same class $\mathcal{K}$. Thus, when considering ψ_λ we may add an arbitrary number of affine functions to point out the subspace L such that ψ_λ (or φ_λ) (in finite field notation) corresponds to the indicator function $\mathbb{1}_{L^\perp}$ (in vector space notation). The cases corresponding to $\alpha+1, \alpha^2+1, \alpha^2+\alpha$ are easy to see. Let us consider the last case:

$$\begin{aligned}
&X_0(X_1+X_2)+X_1X_2 \\
&= X_0(X_1+X_2+1)+X_0+X_1(X_1+X_2+1)+X_1^2+X_1 \\
&= (X_1+X_2+1)(X_0+X_1)+X_0+X_1+X_1 \\
&= (X_1+X_2+1)(X_0+X_1+1)+X_1+X_2+1+X_0
\end{aligned}$$

Furthermore, from [88, Theorem 9], (π^{-1}, L) satisfies the (C) property for all L in the table above, as well as all the conditions in Theorem 2.2.6. Thus, all the components are in $\mathcal{C}$ outside $\mathcal{M}^{\#}$. Hence, F is a bent $(18, 3)$-function strongly outside $\mathcal{M}^{\#}$.

The following result is an immediate consequence of the previous example.

Proposition 6.1.24. *Let $n = 2m$ and $m/3$ be odd. Let $\pi(y) = y^d$ be a permutation on $\mathbb{F}_{2^m}$ such that $d(2^3+1) \equiv 1 \pmod{2^m-1}$ and $\mathrm{wt}(d) \geq 3$. Let $U = \{1, \alpha, \alpha^2\}$, where α is a primitive element of $\mathbb{F}_{2^3}$. Then,*

$$F(x, y) = Tr_3^m(xy^d) + \mathbf{H}(x)$$

with

$$\begin{aligned}\mathbf{H}(x) = (Tr_1^m(x)+1) \cdot \left(\alpha \left(Tr_1^m(\alpha x)+1\right) + \alpha^2 \left(Tr_1^m(\alpha^2 x)+1\right)\right) \\ + \left(Tr_1^m(\alpha x)+1\right)\left(Tr_1^m(\alpha^2 x)+1\right),\end{aligned}$$

is a bent $(n, 3)$-function strongly outside $\mathcal{M}^{\#}$.

Remark 6.1.25. In [67] the authors give an example of a vectorial $(n, 2)$-function strongly outside $\mathcal{M}^{\#}$. With the previous proposition we are able to extend the output space by one and this is the first example of such functions.

Open problem 6.1.26. The function in Example 6.1.23 is a vectorial bent function strongly outside $\mathcal{M}^{\#}$. However, due to the complexity of this topic, we leave as an open problem how to extend this function to a general form, that is, how to generalize Proposition 6.1.24 to cover (n, m)-functions.

6.2 Vectorial Boolean functions with the maximum number of bent components outside $\mathcal{M}^{\#}$

The construction of (n, m)-MNBC functions outside the $\mathcal{M}^{\#}$ class is a difficult theoretical problem. As presented in [2], several nontrivial constructions of (n, m)-MNBC functions contain vectorial $(n, n/2)$-bent functions, and hence many Boolean bent components from $\mathcal{M}^{\#}$ class. Recently, in [3], the authors provided further examples of (n, n)-MNBC functions of the form $x \mapsto (G(x), H(x))$, where G is a suitably chosen vectorial bent function and H is some vectorial Boolean function. The obtained results are presented via three different approaches and all of the obtained examples had bent components in the $\mathcal{M}^{\#}$ class. Employing a trivial construction, it is also hard to construct (n, m)-MNBC functions outside the $\mathcal{M}^{\#}$ class, since only few examples of $(n, n/2)$-bent functions outside $\mathcal{M}^{\#}$ are known [5, 70, 72]. In this thesis, we construct

several infinite families of nontrivial MNBC functions outside the $\mathcal{M}^{\#}$ class using the extension approach, considered recently in [56, 70] in the context of vectorial bent functions, thus giving a positive answer to [3, Question 1]. The main idea of our approach is to extend vectorial $(n, n/2)$-bent functions by non-bent coordinates in such a way, that the remaining bent components fall into secondary constructions of Boolean bent functions outside the $\mathcal{M}^{\#}$ class, what guarantees that the obtained (n, m)-functions are MNBC and outside $\mathcal{M}^{\#}$.

The rest of the chapter is organized in the following way. In Section 6.2.1, we consider in detail the notion of a t-step extension MNBC function, which we use to distinguish inequivalent MNBC functions, and, particularly, to classify all MNBC functions in six variables. Moreover, we show that some of them are nontrivial and do not belong to the $\mathcal{M}^{\#}$ class. In the sequel, we present several theoretical constructions of such functions based on the analysis of several large classes of Boolean bent functions, namely, $\mathcal{PS}_{ap}$, $\mathcal{D}_0$ and $\mathcal{C}$. In Section 6.2.2, we propose a partial spread construction of 1-step extension MNBC functions based on $\mathcal{PS}_{ap}$ vectorial bent functions. In Section 6.2.3, by applying similar techniques, we provide constructions of 1-step and 2-step extension MNBC functions outside $\mathcal{M}^{\#}$ based on the secondary constructions of Boolean bent functions, namely, $\mathcal{D}_0$, $\mathcal{C}$ and $\mathcal{SC}$ classes. In Section 6.2.4, we combine several techniques presented in Section 6.2.3 for the construction of 1-step and 2-step extension MNBC functions and provide a construction of t-step extension (n, m)-MNBC functions outside the $\mathcal{M}^{\#}$ class, where $3 \leq t \leq n/6$. With these results, we give a solution to the open problem [6, Item 1., p. 9]. The representatives of equivalence classes of MNBC functions on $\mathbb{F}_2^6$ are given in Appendix.

6.2.1 Complete classification of MNBC functions in six variables

For vectorial Boolean functions with the maximum number of bent components below the Nyberg's bound, i.e., vectorial bent functions, CCZ- and EA-equivalence coincide [11, 32, 46]. Recently, it was proven that for a vectorial function (beyond the Nyberg's bound), the MNBC property is invariant under CCZ-equivalence [60]. In view of this recent result, it is reasonable to conjecture, that CCZ-equivalence and EA-equivalence coincide for MNBC functions beyond the Nyberg's bound as well. Now we give an example of two EA-inequivalent, but CCZ-equivalent MNBC functions in six variables.

Example 6.2.1. Let $\mathbf{x} \in \mathbb{F}_2^6$ and $\mathbf{y} \in \mathbb{F}_2^4$. Consider the following 1-step extension MNBC functions $F\colon \mathbb{F}_2^6 \to \mathbb{F}_2^4$ and $F'\colon \mathbb{F}_2^6 \to \mathbb{F}_2^4$ given by

algebraic normal forms:

$$F(\mathbf{x}) = \begin{pmatrix} x_1x_4 + x_2x_5 + x_3x_6 \\ x_2x_4 + x_3x_4 + x_1x_5 + x_2x_5 + x_1x_6 \\ x_1x_4 + x_2x_4 + x_1x_5 + x_2x_5 + x_3x_5 + x_2x_6 \\ x_1x_2 + x_2x_4 + x_3x_4 + x_1x_5 + x_2x_5 + x_1x_6 \end{pmatrix},$$

$$F'(\mathbf{x}) = \begin{pmatrix} x_1x_2x_3 + x_1x_4 + x_2x_5 + x_3x_6 \\ x_1x_3 + x_2x_3 + x_1x_2x_4 + x_1x_5 + x_4x_6 \\ x_1x_3 + x_2x_4 + x_2x_5 + x_1x_2x_5 + x_5x_6 \\ x_1x_2 + x_1x_2x_3 + x_1x_4 + x_2x_5 + x_3x_6 \end{pmatrix}.$$

It is easy to see, that $\deg(F) = 2$ and $\deg(F') = 3$, from what follows that F and F' are EA-inequivalent. However, the functions F and F' are CCZ-equivalent, since $\mathcal{L}(\mathcal{G}_F) = \mathcal{G}_{F'}$, where an affine permutation $\mathcal{L}$ on $\mathbb{F}_2^6 \times \mathbb{F}_2^4$ is given by

$$\mathcal{L}(\mathbf{x}, \mathbf{y}) = \begin{pmatrix} x_2 \\ 1 + x_1 + x_2 \\ x_1 + x_5 + x_6 \\ 1 + x_3 + x_4 \\ x_2 + x_3 + x_5 \\ 1 + x_2 + x_3 + y_2 + y_4 \\ x_1 + x_2 + x_3 + x_6 + y_1 + y_3 \\ 1 + x_3 + x_4 + x_5 + x_6 + y_2 \\ 1 + x_1 + x_2 + x_4 + y_3 \\ x_1 + x_2 + x_3 + x_6 + y_1 + y_2 + y_3 + y_4 \end{pmatrix}.$$

Remark 6.2.2. With Example 6.2.1, we conclude that CCZ-equivalence is more general than EA-equivalence for the class of MNBC functions.

Recently, the complete classification of vectorial bent functions in six variables [70, 72], as well as of quadratic vectorial bent functions in eight variables [69] was obtained. With the same approach, we classify all MNBC functions on $\mathbb{F}_2^6$ and check, which of them belong to the $\mathcal{M}^{\#}$ class. First, we give the following definition.

Definition 6.2.3. Let F be an (n, m)-function. Let the linear code $\mathcal{C}_F$ over $\mathbb{F}_2$ be defined as the row space of the $(n + m + 1) \times 2^n$-matrix over $\mathbb{F}_2$ with columns $(1, x, F(x))^T_{x \in \mathbb{F}_{2^n}}$. We call an (n, m)-MNBC function F with $n/2 + 1 \leq m \leq n$ a t-step extension if $\dim(\mathcal{C}_F) = 1 + n + n/2 + t$, where $1 \leq t \leq n/2$.

Remark 6.2.4. *1.* Let F be a t-step extension (n, m)-MNBC function. The value t gives a measure of non-triviality of MNBC-functions. With Definition 6.2.3, an (n, m)-MNBC function is trivial, if it is a 0-step extension.

2. Note that if two MNBC functions F and F' are t-step and t'-step extension with $t \neq t'$, then F and F' are CCZ-inequivalent, since inequivalent linear codes $\mathcal{C}_F$ and $\mathcal{C}_{F'}$ define CCZ-inequivalent functions [32, Theorem 9].

3. Let $1 \leq t \leq n/2-1$. Given a t-step extension (n,m)-MNBC function F, it is easy to obtain a $(t-1)$-step extension (n,m)-MNBC function F', by removing a suitable non-bent component function of F. On the other hand, it seems to be a difficult problem to find a function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ such that the function $F''\colon x \mapsto (F(x), f(x))$ is a $(t+1)$-step extension $(n, m+1)$-MNBC function.

In the following proposition, we summarize our computational results about the classification of MNBC functions in six variables.

Proposition 6.2.5. *On $\mathbb{F}_2^6$, there exist 40 CCZ-equivalence classes of MNBC functions. Among them, there are:*

1. *13 CCZ-equivalence classes of 0-step extension; these are the $(6,3)$-bent functions in [72, Table A2(c)].*
2. *17 CCZ-equivalence classes of 1-step extension.*
3. *7 CCZ-equivalence classes of 2-step extension.*
4. *3 CCZ-equivalence classes of 3-step extension.*

If an MNBC function F on $\mathbb{F}_2^6$ is a 2-step or a 3-step extension, then $F \in \mathcal{M}$.

Now we briefly discuss the main steps of the used approach. Since any (n,m)-MNBC function F has $2^{m-n/2}$ non-bent components, which form an $(m-n/2)$-dimensional vector space [73, 91], one can represent F in the form

$$F(x) = (b_1(x), \ldots, b_{n/2}(x), n_1(x), \ldots, n_{m-n/2}(x)),$$

where all b_i are bent, all n_j are non-bent and $\langle n_1, \ldots, n_{m-n/2}\rangle$ is a vector space of non-bent functions of dimension $m-n/2$. Applying a non-degenerate linear transformation to the output of F, we get

$$F'(x) = (b_1(x), \ldots, b_{n/2}(x), b_{n/2+1}(x), \ldots, b_m(x)),$$

where $b_{n/2+i} := b_i + n_i$ is bent for $1 \leq i \leq m-n/2$, since by [91, Theorem 3.1], all non-bent components of F belong to $\langle n_1, \ldots, n_{m-n/2}\rangle$. In this way, we may assume that all coordinate functions of an MNBC function F are bent. Consequently, any (n,m)-MNBC function F can be represented as $F(x) = (\bar{F}(x), f(x))$, where $\bar{F}(x)$ is an $(n, m-1)$-MNBC function and f is a Boolean bent function on $\mathbb{F}_2^n$ (for $m = n/2+1$ we let $\bar{F}$ be $(n, n/2)$-bent). In this case, we say that $\bar{F}$ is extendable to F. With this representation of MNBC functions, we start with inequivalent vectorial $(6,3)$-bent functions from [72] and extend them recursively to

$(6, m)$-MNBC functions by appending at each step a Boolean bent function without affine terms exhaustively. The extension relation between the obtained CCZ-equivalence classes is given in Figure 6.1.

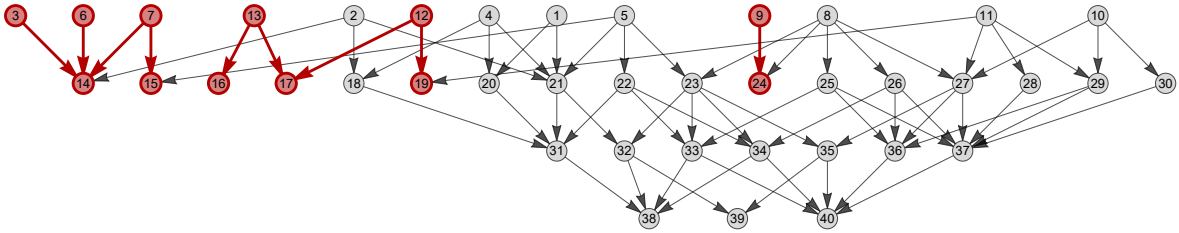

Figure 6.1: The structure of CCZ-equivalence classes of $(6, m)$-MNBC functions. If an equivalence class i is extendable to an equivalence class j, we put a directed edge between them. The equivalence classes denoted by gray are inside $\mathcal{M}^{\#}$ and by red are outside $\mathcal{M}^{\#}$.

We check CCZ-equivalence of MNBC functions F and F' via equivalence of linear codes $\mathcal{C}_F$ and $\mathcal{C}_{F'}$ (see [32, Theorem 9]) with the algebra system Magma [10]. With the implementation [71, Algorithm 1] of Lemma 2.2.4 applied coordinate-wise to all EA-inequivalent MNBC functions contained in a CCZ-equivalence class, we check whether a given CCZ-equivalence class belongs to $\mathcal{M}^{\#}$. Finally, we list representatives of the obtained CCZ-equivalence classes in the Appendix.

Remark 6.2.6. *1.* Alternatively to [71, Algorithm 1], one can use a graph-theoretic approach in order to check, whether a given bent function f on $\mathbb{F}_2^n$ belongs to $\mathcal{M}^{\#}$. Let $G = (V, E)$ be a graph with the vertex-set $V = \mathbb{F}_2^n$ and the edge-set $E = \{\{a, b\} \in V \times V : D_{a,b}f = 0\}$. Then the existence of a vector space $U \subset \mathbb{F}_2^n$ with $\dim(U) = n/2$ s.t. $D_{a,b}f = 0$ for any $a, b \in U$ is equivalent to the existence of a clique U of size $2^{n/2}$ in G, whose elements form a vector space of dimension $n/2$. For details on the implementation, we refer to [65].

2. On $\mathbb{F}_2^6$, there are 17 CCZ-equivalence classes of 1-step extension MNBC functions, and there are 23 EA-equivalence classes of 1-step extension MNBC functions. CCZ-equivalence classes 14 and 21 contain 3 EA-equivalence classes (each), CCZ-equivalence classes 23 and 27 contain 2 EA-equivalence classes (each), and every other CCZ-equivalence class i with $14 \leq i \leq 30$ contains exactly one EA-equivalence class.

With the computational results obtained in this section, one can see that even in a small number of variables nontrivial MNBC functions with components outside $\mathcal{M}^{\#}$ exist. In the sequel, we provide several theoretical constructions of such functions. Finally, we suggest to work on the following problem in order to shed more light on the phenomenon observed in Example 6.2.1.

Open problem 6.2.7. Find explicit constructions of (n, m)-MNBC functions for all $n \geq 6$ and $n/2+1 \leq m \leq n$, which are EA-inequivalent, but CCZ-equivalent.

6.2.2 MNBC functions from the $\mathcal{PS}_{ap}$ class

In the following theorem, we give the partial spread construction of MNBC functions.

Theorem 6.2.8. *Let $n = 2k$ and let G be a vectorial (n, k)-bent function from the $\mathcal{PS}_{ap}$ class. Let also U be a spread line of the form $U = \{(0, y) : y \in \mathbb{F}_{2^k}\}$. Then the function $F : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2^{k+1}$ defined as*

$$F(x, y) = (G(x, y), \mathbb{1}_U(x, y)) \tag{6.4}$$

is an $(n, k + 1)$-MNBC function.

Proof. Since $\mathbb{1}_U : \mathbb{F}_2^n \to \mathbb{F}_2$ is the indicator of the vector space U of dimension k, we have $\mathrm{wt}(\mathbb{1}_U) = 2^k$ and hence $\mathbb{1}_U$ is not bent. In this way, it is enough to show that for any $\mathcal{PS}_{ap}$ Boolean bent function g on $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$, which is a bent component of the function G, the function $g + \mathbb{1}_U$ on $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ is bent. For $a, b \in \mathbb{F}_{2^k}$, we compute the Walsh transform $W_{g+\mathbb{1}_U}(a, b)$ of $g + \mathbb{1}_U$ at $a, b \in \mathbb{F}_{2^k}$, by considering the following two cases.

Case 1. Let $a, b \in \mathbb{F}_{2^k}$ with $b \neq 0$. The Walsh transform of $g + \mathbb{1}_U$ is given by

$$\begin{aligned} W_{g+\mathbb{1}_U}(a, b) &= \sum_{x,y \in \mathbb{F}_{2^k}} (-1)^{g(x,y)+\mathbb{1}_U(x,y)+Tr_1^k(ax+by)} \\ &= \sum_{y \in \mathbb{F}_{2^k}} (-1)^{g(0,y)+\mathbb{1}_U(0,y)+Tr_1^k(by)} \\ &\quad + \sum_{x \in \mathbb{F}_{2^k}^*} \sum_{y \in \mathbb{F}_{2^k}} (-1)^{g(x,y)+\mathbb{1}_U(x,y)+Tr_1^k(ax+by)} = W_g(a, b) = \pm 2^k, \end{aligned}$$

since $\sum_{y \in \mathbb{F}_{2^k}} (-1)^{g(0,y)+\mathbb{1}_U(0,y)+Tr_1^k(by)} = \sum_{y \in \mathbb{F}_{2^k}} (-1)^{Tr_1^k(by)} = 0$ (because $b \neq 0$), and the function g is bent on $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$.

Case 2. Let $a, b \in \mathbb{F}_{2^k}$ with $b = 0$. The Walsh transform of $g + \mathbb{1}_U$ is given by

$$\begin{aligned} W_{g+\mathbb{1}_U}(a, 0) &= \sum_{x,y \in \mathbb{F}_{2^k}} (-1)^{g(x,y)+\mathbb{1}_U(x,y)+Tr_1^k(ax)} \\ &= \sum_{y \in \mathbb{F}_{2^k}} (-1)^{g(0,y)+\mathbb{1}_U(0,y)} + \sum_{x \in \mathbb{F}_{2^k}^*} \sum_{y \in \mathbb{F}_{2^k}} (-1)^{g(x,y)+\mathbb{1}_U(x,y)+Tr_1^k(ax)} \\ &= -2^k + W_g(a, 0) - 2^k. \end{aligned}$$

Since for $\mathcal{PS}_{ap}$ bent function g on $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ the Walsh transform $W_g(a, 0) = +2^k$ for any $a \in \mathbb{F}_{2^k}$, we have that $W_{g+\mathbb{1}_U}(a, 0) = -2^k$. This completes the proof. □

Remark 6.2.9. *1.* In the same way, one can show that for the spread line $U = \{(x, 0) \colon x \in \mathbb{F}_{2^k}\}$ the $(n, k+1)$-function F of the form (6.4) is MNBC.

2. The bent component functions of MNBC functions of the form (6.4) belong to the $\mathcal{PS}_{ap}$ and $\mathcal{PS}^{+}$ classes. Addition of the indicator of the spread line $\mathbb{F}_{2^k} \times \{0\}$ or the indicator of $\{0\} \times \mathbb{F}_{2^k}$ to a $\mathcal{PS}_{ap}$ bent function g on $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ gives a bent function in $\mathcal{PS}^{+}$ class, because the $\mathcal{PS}_{ap}$ bent function g is constant 0 on the mentioned spread lines. Similarly, one can use other spreads (not necessarily Desarguesian) for the construction of MNBC functions.

3. Weng, Feng and Qiu [85] proved that almost every $\mathcal{PS}_{ap}$ bent function on $\mathbb{F}_2^n$ is outside $\mathcal{M}^{\#}$. Since $2^{n/2} - 1$ component functions of MNBC functions of the form (6.4) belong to $\mathcal{PS}_{ap}$, we have that almost every MNBC function of this form is outside $\mathcal{M}^{\#}$. Remarkably, with this construction one can extend a vectorial bent function in $\mathcal{PS}_{ap} \cap \mathcal{M}$ to an MNBC function outside $\mathcal{M}^{\#}$, as the example of equivalence classes 11 and 19 in Figure 6.1 shows; this is the only such an example in six variables, since the only equivalence classes of $(6, 3)$-bent functions inside $\mathcal{PS}_{ap}$ are 11, 12 and 13 (see Figure 6.1 and [72, Table IV.2.]).

4. Any $\mathcal{PS}_{ap}$ vectorial bent function $(x, y) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \mapsto H(x/y)$ in $n = 2k = 6$ variables can be extended to at least two inequivalent 1-step extension MNBC functions from the $\mathcal{PS}_{ap}$ class. With Magma [10], one can show that for any permutation H on $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$, MNBC functions of the form

$$\begin{aligned} F &\colon (x, y) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \mapsto (H(x/y), \mathbb{1}_U(x, y)), \\ F' &\colon (x, y) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \mapsto (H(x/y), \mathbb{1}_V(x, y)), \end{aligned} \tag{6.5}$$

where $U = \{(0, y) \colon y \in \mathbb{F}_{2^k}\}$ and $V = \{(x, 0) \colon x \in \mathbb{F}_{2^k}\}$, are CCZ-inequivalent.

Conjecture 6.2.10. In view of the last observation in Remark 6.2.9, we conjecture that MNBC functions F and F' defined by (6.5) are inequivalent for any permutation H on $\mathbb{F}_{2^k}$.

6.2.3 MNBC functions from secondary constructions of Boolean bent functions

In this section, using secondary constructions of Boolean bent functions, we construct three families of MNBC functions: two families of 1-step extension stemming from $\mathcal{D}_0$ and $\mathcal{C}$ classes, and one family of 2-step extension stemming from the $\mathcal{SC}$ class, which is a superclass of $\mathcal{D}_0$ and $\mathcal{C}$.

MNBC functions stemming from the $\mathcal{D}_0$ class

In the following, we define $\delta_0 \colon \mathbb{F}_{2^k} \to \mathbb{F}_2$ to be the indicator of $0 \in \mathbb{F}_{2^k}$, i.e., $\delta_0 = \mathbb{1}_{\{0\}}$. With this notation, Boolean functions $f \colon \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$ of the form

$$f(x, y) = Tr_1^k(x\pi(y)) + \delta_0(x) \quad \text{for } x, y \in \mathbb{F}_{2^k}, \tag{6.6}$$

where π is a permutation on $\mathbb{F}_{2^k}$, are bent and the set of bent functions of the form (6.6) is called the $\mathcal{D}_0$ *class* of Boolean bent functions [17]. Carlet [17] proved, that bent functions of the form (6.6), where π is a quadratic permutation such that there is no affine hyperplane of $\mathbb{F}_{2^k}$ on which π is affine, do not belong to the $\mathcal{M}^\#$ class. In a recent work [44], the authors provided complete characterization of $\mathcal{D}_0 \cap \mathcal{M}^\#$, which we summarize in the following theorem.

Theorem 6.2.11. *[44, Theorems 5,7] Let k be an integer, $k \geq 4$. Let π be a permutation of $\mathbb{F}_{2^k}$ with one of the following two properties:*

1. *The algebraic degree of π satisfies* $\deg(\pi) \geq 3$*;*
2. *The permutation π is quadratic and there is no affine hyperplane of $\mathbb{F}_{2^k}$ on which π is affine.*

Then the function $f \colon \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$ defined by $f(x, y) = Tr_1^k(x\pi(y)) + \delta_0(x)$ for $x, y \in \mathbb{F}_{2^k}$ is a bent function in $\mathcal{D}_0$ outside $\mathcal{M}^\#$. Moreover, the second condition is also a necessary one for quadratic permutations.

With the use of bent functions from $\mathcal{D}_0 \setminus \mathcal{M}^\#$ class, we derive the following family of MNBC functions.

Theorem 6.2.12. *Let $n = 2k \geq 8$ and let $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^k}$. Let π be a permutation on $\mathbb{F}_{2^k}$ satisfying one of conditions of Theorem 6.2.11. Then the (n, n)-function F defined by*

$$F(x, y) = x\pi(y) + \gamma\delta_0(x) \text{ for } x, y \in \mathbb{F}_{2^k}, \tag{6.7}$$

is a 1-step extension (n, n)-MNBC function outside the $\mathcal{M}^\#$ class.

Proof. First, we show that the function F has the maximum number of bent components and is outside $\mathcal{M}^\#$. Let $\lambda \in \mathbb{F}_{2^n}^*$ be arbitrary. Then

$$F_\lambda(x, y) = Tr_1^k(x\pi(y)Tr_k^n(\lambda)) + \delta_0(x)Tr_1^n(\lambda\gamma)$$

is not bent if and only if $Tr_k^n(\lambda) = 0$. This holds, if $\lambda \in \mathbb{F}_{2^k}^*$. Thus, there are $(2^n - 1) - (2^k - 1) = 2^n - 2^k$ bent components. Since $|\{x \in \mathbb{F}_{2^n} : Tr_1^n(\gamma x) = 1\}| = |\{x \in \mathbb{F}_{2^n} : Tr_1^n(\gamma x) = 0\}| = 2^{n-1}$, there exist at least $2^n - 2^k - 2^{n-1} = 2^k(2^{k-1} - 1)$ many $\lambda \notin \mathbb{F}_{2^k}$ such that $Tr_1^n(\lambda\gamma) = 1$. In this case, we have that $F_\lambda \in \mathcal{D}_0 \setminus \mathcal{M}^\#$. Now we show that F is a 1-step extension. Since $G(x, y) := x\pi(y)$ is an (n, k)-function, we can write $G(x, y) = (g_1(x, y), \ldots, g_k(x, y))$, where $g_1, \ldots, g_k \colon \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$.

Since $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^k}$, we can construct the function F' in the following form

$$F'(x,y) = (g_1(x,y), \ldots, g_k(x,y), \delta_0(x)).$$

Thus, F' is an MNBC $(n, k+1)$-function, since the non-bent component functions of F' are 0 and δ_0. Furthermore, we note that the dimension of the linear code $\mathcal{C}_{F'}$ is given by $\dim(\mathcal{C}_{F'}) = 1 + n + k + 1$ which, by definition, means that F' is a nontrivial MNBC $(n, k+1)$-function. Consequently, the MNBC (n, n)-function F is a 1-step extension. □

MNBC functions stemming from the $\mathcal{C}$ class

In this section, we present several infinite families of MNBC functions provably outside the $\mathcal{M}^{\#}$ class based on the generic construction of MNBC functions introduced in [4]. It was shown that several Maiorana-McFarland vectorial bent functions $G\colon \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_{2^k}$ satisfy the conditions of Construction 3.1.1. Now we show that for these vectorial bent functions $G\colon \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_{2^k}$ one can specify a vectorial function $\mathbf{h}$, such that MNBC functions, obtained via Construction 3.1.1, are outside the $\mathcal{M}^{\#}$ class. The choice of the function $\mathbf{h}$ is strongly related with $\mathcal{C}$ and $\mathcal{D}_0$ classes of Boolean bent functions, which contain functions provably outside $\mathcal{M}^{\#}$.

Recall that the $\mathcal{C}$ *class* of bent functions introduced by Carlet [17] is the set of Boolean functions $f\colon \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$ of the form

$$f(x,y) = Tr_1^k(x\pi(y)) + \mathbb{1}_{L^{\perp}}(x), \tag{6.8}$$

where L is any vector subspace of $\mathbb{F}_{2^k}$, $\mathbb{1}_{L^{\perp}}$ is the indicator function of the *orthogonal complement* $L^{\perp} = \{x \in \mathbb{F}_{2^k} \colon Tr_1^k(xy) = 0, \forall\, y \in L\}$, and π is any permutation on $\mathbb{F}_{2^k}$ such that

$$(C) \quad \pi^{-1}(a + L) \text{ is a flat (affine subspace), for all } a \in \mathbb{F}_{2^k}.$$

The permutation π^{-1} and the subspace L are then said to satisfy the (C) property. For short, we also write (π^{-1}, L) *has property* (C). Recall that a Boolean function $f\colon \mathbb{F}_{2^n} \to \mathbb{F}_2$ has a *linear structure* if there exists an element $a \in \mathbb{F}_{2^n}^*$ such that $x \mapsto f(x+a) + f(x)$ is a constant function.

Using Construction 3.1.1 and Theorem 2.2.6, we obtain the following family of MNBC functions outside the $\mathcal{M}^{\#}$ class.

Theorem 6.2.13. *Let $U = \{u_1, \ldots, u_\tau\}$ be a set of τ linearly independent elements in $\mathbb{F}_{2^k}^*$, where $n = 2k \geq 8$ and $\tau \mid k$. Let π be a permutation on $\mathbb{F}_{2^k}$ and $G(x,y) = x\pi(y)$, where $x, y \in \mathbb{F}_{2^k}$, be an (n,k)-bent function whose dual bent components $\tilde{G}_\lambda$, $\lambda \in \mathbb{F}_{2^k}^*$, satisfy the property (P_U) with the defining set U. Let $\mathbf{h}\colon \mathbb{F}_2^\tau \to \mathbb{F}_2$ be defined by its ANF as follows*

$$\mathbf{h}(x_1, \ldots, x_\tau) = \prod_{i=1}^{\tau} (x_i + 1). \tag{6.9}$$

If $((\lambda\pi)^{-1}, \langle U\rangle)$ satisfies the (C) property and the conditions of Theorem 2.2.6 for all $\lambda \in \mathbb{F}_{2^k}^*$, then the (n,n)-function F constructed from G and $\mathbf{h}$ *as*

$$F(x,y) = G(x,y) + \gamma \mathbf{h}(Tr_1^k(u_1 x), \ldots, Tr_1^k(u_\tau x)), \tag{6.10}$$

where $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^k}$, is a 1-step extension (n,n)-MNBC function outside $\mathcal{M}^{\#}$.

Proof. From Construction 3.1.1, it follows that the function F is an (n,n)-MNBC function. The function $\mathbf{h}$, defined in such a way, represents the indicator function of the subspace $\langle U\rangle^{\perp}$ of $\mathbb{F}_{2^k}$. If $Tr_1^k(\lambda\gamma) = 1$ for $\lambda \in \mathbb{F}_{2^k}^*$, then $F_\lambda(x,y) = Tr_1^k(x\lambda\pi(y)) + \mathbb{1}_{\langle U\rangle^{\perp}}(x)$. Since $((\lambda\pi)^{-1}, \langle U\rangle)$ satisfies the (C) property and the conditions of Theorem 2.2.6 for all $\lambda \in \mathbb{F}_{2^k}^*$, it follows that $F_\lambda \in \mathcal{C} \setminus \mathcal{M}^{\#}$. If $Tr_1^k(\lambda\gamma) = 0$ then $F_\lambda \in \mathcal{M}^{\#}$, hence F is outside $\mathcal{M}^{\#}$. Now we show that F is a 1-step extension. Since $G(x,y) := x\pi(y)$ is an (n,k)-function, we can write $G(x,y) = (g_1(x,y), \ldots, g_k(x,y))$, where $g_i \colon \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$ for all $1 \le i \le k$. Since $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^k}$, we can construct the function F' (see Remark 6.2.4) in the following form $F'(x,y) = (g_1(x,y), \ldots, g_k(x,y), g_{k+1}(x,y))$, where $g_{k+1}(x,y) := \mathbf{h}(Tr_1^k(u_1 x), \ldots, Tr_1^k(u_\tau x))$. Thus, F' is an $(n,k+1)$-MNBC function, since the non-bent components of F' are 0 and g_{k+1}. Finally, since $\mathcal{C}_F = \mathcal{C}_{F'}$, we have that $\dim(\mathcal{C}_F) = \dim(\mathcal{C}_{F'}) = 1 + n + k + 1$, consequently the (n,n)-MNBC function F is a 1-step extension. □

Following the proof of [5, Proposition 3], we give the following family of 1-step extension (n,n)-MNBC functions outside $\mathcal{M}^{\#}$ by specifying the permutation π to be a power mapping.

Proposition 6.2.14. *Let $k \ge 4$ and s be a positive divisor of k such that k/s is odd. Let $U = \{1, \alpha, \ldots, \alpha^{\tau-1}\}$ be a set of τ linearly independent elements in $\mathbb{F}_{2^s}^*$, α is a primitive element in $\mathbb{F}_{2^s}$ and $\tau \mid k$. Let $G(x,y) = x\pi(y)$, where $x, y \in \mathbb{F}_{2^k}$, $\pi(y) = y^d$ is a permutation on $\mathbb{F}_{2^k}$ for a positive integer d such that $\mathrm{wt}(d) \ge 3$ and $d(2^s+1) \equiv 1 \pmod{2^k - 1}$. Then $(\pi^{-1}, \langle U\rangle)$, satisfies the (C) property and for any $\gamma \notin \mathbb{F}_{2^k}$, the function*

$$F(x,y) = xy^d + \gamma \mathbf{h}(Tr_1^k(x), Tr_1^k(\alpha x), \ldots, Tr_1^k(\alpha^{\tau-1} x)),$$

where $\mathbf{h}$ *is defined by* (6.9)*, is a 1-step extension (n,n)-MNBC function outside the $\mathcal{M}^{\#}$ class.*

Proof. By [4, Proposition 3], the dual bent components $\tilde{G}_\lambda$ of G satisfy the property (P_U) with the defining set U given above for any $\lambda \in \mathbb{F}_{2^k}^*$. Thus, from Construction 3.1.1, it follows that the function F is an (n,n)-MNBC function. We will show that F is outside $\mathcal{M}^{\#}$. Let $\lambda \in \mathbb{F}_{2^k}^*$ be arbitrary. If $Tr_1^k(\lambda\gamma) = 0$, we have that $F_\lambda(x,y) = G_\lambda(x,y) \in \mathcal{M}$. Suppose that $Tr_1^k(\lambda\gamma) = 1$, then $F_\lambda(x,y) = Tr_1^k(\lambda x y^d) + \mathbb{1}_{\langle U\rangle^{\perp}}(x)$. For any

permutation π on $\mathbb{F}_{2^k}$, let $\sigma_\lambda(y) := \lambda\pi(y)$. Note that $\sigma_\lambda^{-1}(y) = \pi^{-1}(\lambda^{-1}y)$. Let $\pi(y) = y^d$, where d is defined above. Then, $\sigma_\lambda^{-1}(y) = \lambda^{-2^s-1}\pi^{-1}(y)$, where $\pi^{-1}(y) = y^{2^s+1}$. We will show that $(\sigma_\lambda^{-1}, \langle U\rangle)$ satisfies the (C) property. Let $a \in \mathbb{F}_{2^k}$ be arbitrary. Then

$$\sigma_\lambda^{-1}(a + \langle U\rangle) = \lambda^{-2^s-1}(a + \langle U\rangle)^{2^s+1} = \lambda^{-s}\pi^{-1}(a + \langle U\rangle)$$

is a flat as $\pi^{-1}(a + \langle U\rangle)$ is a flat by [53, Theorem 5.8]. Since $\mathrm{wt}(d) \geq 3$, by [88, Proposition 5] it follows that $Tr_1^k(\lambda\pi)$ has no nonzero linear structures. Thus by Theorem 2.2.6 it follows that F_λ is in $\mathcal{C}$ outside $\mathcal{M}^{\#}$. Hence, F is outside $\mathcal{M}^{\#}$. Finally, from Theorem 6.2.13, we conclude that F is a 1-step extension.

□

MNBC functions stemming from the $\mathcal{SC}$ class

In [5, Section 3], the first two authors defined a new superclass of bent functions obtained from the $\mathcal{C}$ and $\mathcal{D}_0$ class as follows. Let π be a permutation on $\mathbb{F}_{2^k}$ and let $L \subset \mathbb{F}_{2^k}$ be a linear subspace of $\mathbb{F}_{2^k}$ such that (π^{-1}, L) satisfies the (C) property. Then the class of bent functions $f\colon \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$ containing all functions of the form (5.5) is called $\mathcal{SC}$ and is a superclass of $\mathcal{D}_0$ and $\mathcal{C}$.

As noted in Theorem 5.1.1, under certain conditions, the functions in $\mathcal{SC}$ are outside the completed Maiorana-McFarland class $\mathcal{M}^{\#}$. With the notation of Proposition 6.2.14, we construct the following family of MNBC functions.

Theorem 6.2.15. *Let $x, y \in \mathbb{F}_{2^k}$. The function $F\colon \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_{2^n}$ defined by*

$$F(x,y) = xy^d + \gamma_1\mathbf{h}(Tr_1^k(x), Tr_1^k(\alpha x), \ldots, Tr_1^k(\alpha^{t-1}x)) + \gamma_2\delta_0(x), \tag{6.11}$$

where $t < k$, is a 2-step extension (n,n)-MNBC function outside $\mathcal{M}^{\#}$, for all $\gamma_1, \gamma_2 \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^k}$.

Proof. First, we show that F has the maximum number of bent components and is outside $\mathcal{M}^{\#}$. Let $\lambda \in \mathbb{F}_{2^n}^*$ be arbitrary. Then

$$\begin{aligned} F_\lambda(x,y) &= Tr_1^k(x\pi(y)Tr_k^n(\lambda)) \\ &\quad + \mathbf{h}(Tr_1^k(x), Tr_1^k(\alpha x), \ldots, Tr_1^k(\alpha^{t-1}x))Tr_1^n(\lambda\gamma_1) + \delta_0(x)Tr_1^n(\lambda\gamma_2) \end{aligned}$$

is not bent if and only if $Tr_k^n(\lambda) = 0$. This holds, if $\lambda \in \mathbb{F}_{2^k}^*$. Thus, there are $(2^n-1) - (2^k-1) = 2^n - 2^k$ bent components. Since $|\{x \in \mathbb{F}_{2^n} : Tr_1^n(\gamma_i x) = 1\}| = |\{x \in \mathbb{F}_{2^n} : Tr_1^n(\gamma_i x) = 0\}| = 2^{n-1}$, there exist at least $2^n - 2^k - 2^{n-1} = 2^k(2^{k-1}-1)$ many $\lambda \notin \mathbb{F}_{2^k}$ such

that $Tr_1^n(\lambda\gamma_i) = 1$, for $i = 1, 2$. When $Tr_1^k(\lambda\gamma_1) = Tr_1^k(\lambda\gamma_2) = 1$, the component is in $\mathcal{SC}$ outside $\mathcal{M}^{\#}$, if $Tr_1^k(\lambda\gamma_1) = 1, Tr_1^k(\lambda\gamma_2) = 0$, the component is in $\mathcal{C}$ outside $\mathcal{M}^{\#}$, and if $Tr_1^k(\lambda\gamma_1) = 0, Tr_1^k(\lambda\gamma_2) = 1$, the component is in $\mathcal{D}_0$ outside $\mathcal{M}^{\#}$. Now we show that F is a 2-step extension. Since $G(x, y) := x\pi(y)$ is an (n, k)-function, we can write $G(x, y) = (g_1(x, y), \ldots, g_k(x, y))$, where $g_1, \ldots, g_k \colon \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$. Since $\gamma_1, \gamma_2 \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^k}$, we can construct the function F' in the following form $F'(x, y) = (g_1(x, y), \ldots, g_k(x, y), \mathbf{h}(X), \delta_0(x))$, $X = (Tr_1^k(x), \ldots, Tr_1^k(\alpha^{t-1}x))$. Thus, F' is an MNBC $(n, k + 2)$-function, since the non-bent component functions of F' are $0, \delta_0$ and $\mathbf{h}$. Note that if $t = k$, then $\delta_0 = \mathbf{h}$. Thus, we assume that $t < k$. Furthermore, we note that the dimension of the linear code $\mathcal{C}_{F'}$ is given by $\dim(\mathcal{C}_{F'}) = 1+n+k+2$ which, by definition, means that F' is a nontrivial MNBC $(n, k + 2)$-function. Consequently, the MNBC (n, n)-function F is a 2-step extension. □

Example 6.2.16. Let $n = 12$ and the multiplicative group of $\mathbb{F}_{2^{12}}$ be given by $\mathbb{F}_{2^n}^* = \langle\alpha\rangle$, where the primitive element α satisfies $\alpha^{12} + \alpha^7 + \alpha^6 + \alpha^5 + \alpha^3 + \alpha + 1 = 0$. Let $\lambda = \alpha^{\frac{2^{12}-1}{3}}$. If we choose $L = \langle 1, \lambda\rangle$ and $\pi(y) = y^{38}$, then (π^{-1}, L) satisfies the (C) property (see [88, Example 1]) and $\mathrm{wt}(38) = 3$, that is, π admits no linear structures. Using a computer algebra system, one can check that the following $(12, 12)$-MNBC functions

$$\begin{aligned} F_1(x, y) =& xy^{38} + \alpha^{233}(Tr_1^6(x) + 1)(Tr_1^6(\lambda x) + 1) \text{ and} \\ F_2(x, y) =& xy^{38} + \alpha^{233}(Tr_1^6(x) + 1)(Tr_1^6(\lambda x) + 1) + \alpha^{121}\delta_0(x) \end{aligned}$$

are 1-step and 2-step extension, respectively. That is, the dimensions of the linear codes $\mathcal{C}_{F_1}$ and $\mathcal{C}_{F_2}$, are equal to $1 + n + n/2 + 1 = 20$ and $1 + n + n/2 + 2 = 21$, respectively.

6.2.4 A family of t-step extension MNBC functions

In [5], the authors present the following secondary construction of vectorial bent functions outside $\mathcal{M}^{\#}$, which can be used to construct nontrivial (n, n)-MNBC functions outside $\mathcal{M}^{\#}$.

Theorem 6.2.17. *Let $n = 2k \geq 8$ and $t \geq 3$ be a positive divisor of k such that k/t is odd. Let $\pi(y) = y^d$ be a permutation on $\mathbb{F}_{2^k}$ such that $d(2^t + 1) \equiv 1 \pmod{2^k - 1}$ and $\mathrm{wt}(d) \geq 3$. Let α be a primitive element of $\mathbb{F}_{2^t}$. Then the (n, n)-function F defined by*

$$F(x, y) = xy^d + \mathbf{H}(x), \quad x, y \in \mathbb{F}_{2^k}$$

with

$$\mathbf{H}(x) = \left(Tr_1^k(x) + 1\right) \cdot \left(\sum_{i=1}^{t-1} \gamma_i \alpha^i \left(Tr_1^k(\alpha^i x) + 1\right)\right) + \mu\delta_0(x),$$

where $\gamma_i, \mu \notin \mathbb{F}_{2^k}$, $\gamma_i \neq \gamma_j$ $(i \neq j)$, is a t-step extension (n,n)-function outside $\mathcal{M}^{\#}$.

Proof. Similarly as in the proof of Theorems 6.2.12 and 6.2.15, we note that F has $(2^n-1)-(2^k-1) = 2^n - 2^k$ bent components, some of which are outside $\mathcal{M}^{\#}$.

Let $Tr_1^k(\lambda) = 1$. When $Tr_1^k(\lambda\gamma_i\alpha^i) = 1$ for at least one $i \in \{1,\ldots,t-1\}$ and $Tr_1^k(\lambda\mu) = 0$, the component is in $\mathcal{C}$ outside $\mathcal{M}^{\#}$ (as shown in [5, Proposition 2]). If $Tr_1^k(\lambda\gamma_i\alpha^i) = 1$ for at least one $i \in \{1,\ldots,t-1\}$ and $Tr_1^k(\lambda\mu) = 1$, the component is in $\mathcal{SC}$ outside $\mathcal{M}^{\#}$ (as shown in [5, Corollary 3]). Lastly, if $Tr_1^k(\lambda\gamma_i\alpha^i) = 0$ for all $i \in \{1,\ldots,t-1\}$ and $Tr_1^k(\lambda\mu) = 1$, the component is in $\mathcal{D}_0$ outside $\mathcal{M}^{\#}$. For the remaining cases, it is easy to see that the components are in $\mathcal{M}^{\#}$. Now we show that F is an t-step extension.

Since $G(x,y) := x\pi(y)$ is an (n,k)-function, we can write

$$G(x,y) = (g_1(x,y),\ldots,g_k(x,y)),$$

where $g_i\colon \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$, for $i = 1,\ldots,k$. For $\mu,\gamma_1,\ldots,\gamma_{t-1} \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^k}$ and $1,\alpha,\ldots,\alpha^{t-1} \in \mathbb{F}_{2^t}$, we have that $\{\mu,\gamma_1\alpha,\ldots,\gamma_{t-1}\alpha^{t-1}\}$ is a linearly independent set over $\mathbb{F}_2$ (since α is a primitive element of $\mathbb{F}_{2^t}$). Furthermore, because $\gamma_i,\mu \notin \mathbb{F}_{2^k}$ we have that $\gamma_i\alpha^i,\mu \notin \mathbb{F}_{2^k}$ for $i = 1,\ldots,t-1$, and thus the set

$$\{1,\omega,\ldots,\omega^{k-1},\mu,\gamma_1\alpha,\ldots,\gamma_{t-1}\alpha^{t-1}\}$$

is linearly independent over $\mathbb{F}_2$, where ω is a primitive element of $\mathbb{F}_{2^k}$ with $\omega^{(2^k-1)/(2^t-1)} = \alpha$. Let us show that the functions $h_t = \delta_0, h_i = \mathbb{1}_{\langle 1,\alpha^i\rangle^\perp}$, $i = 1,\ldots,t-1$, are linearly independent. Let us consider their linear combination $\lambda_1 h_1 + \ldots + \lambda_{t-1}h_{t-1} + \lambda_t h_t$. Suppose that for some $i \in \{1,\ldots,t\}$ we have $\lambda_i = 1$.

If $\lambda_t = 1$, then

$$\delta_0 = \sum_{j=1}^{t-1} \lambda_j h_j = \sum_{j\in J} h_j,$$

where $J = \{j : 1 \leq j \leq t-1, \lambda_j = 1\}$. We have that

$$\begin{aligned}
\mathbb{1}_{\langle 1,\alpha,\ldots,\alpha^{k-1}\rangle^\perp} = \delta_0 &= \sum_{j\in J} h_j \\
&= (Tr_1^k(x)+1)\left(Tr_1^k\left(\sum_{j\in J}\alpha^j x\right) + \sum_{j\in J}\lambda_j\right) \\
&= \begin{cases} \mathbb{1}_{\langle 1,\sum_{j\in J}\alpha^j\rangle^\perp}, & \text{if } \sum_{j\in J}\lambda_j = 1 \\ \mathbb{1}_{\langle 1,\sum_{j\in J}\alpha^j\rangle^\perp} + l, & \text{otherwise} \end{cases},
\end{aligned}$$

where $l(x) = Tr_1^k(x) + 1$. It is easy to note that the left- and right-hand side cannot be equal, no matter what the choice of $\lambda_i \in \mathbb{F}_2$ is.

Hence, without loss of generality, we may assume that $\lambda_t = 0$. Suppose that for some $i \in \{1, \ldots, t-1\}$ we have $\lambda_i = 1$. Then

$$h_i = \sum_{i \neq j=1}^{t-1} \lambda_j h_j = \sum_{j \in J} h_j,$$

where $J = \{j : 1 \leq j \leq t-1,\ j \neq i, \lambda_j = 1\}$. Let $\xi = \sum_{j \in J} \alpha^j$. It is easy to compute that

$$\mathbb{1}_{\langle 1, \alpha^i \rangle^\perp} = h_i = (Tr_1^k(x) + 1)(Tr_1^k(\xi x) + \varepsilon),\ \varepsilon = \sum_{j \in J} \lambda_j.$$

If $\varepsilon = 1$, it follows that $\langle 1, \xi \rangle = \langle 1, \alpha^i \rangle$, which implies that $\xi \in \langle 1, \alpha^i \rangle$. This is not possible because ξ is a linear combination of $\{\alpha, \ldots \alpha^{t-1}\} \setminus \{\alpha^i\}$ and α is a primitive element of $\mathbb{F}_{2^t}$. If $\varepsilon = 0$, we have that

$$1 = h_i(0) = (Tr_1^k(0) + 1)(Tr_1^k(\xi 0)) = 0,$$

which is not true. Thus we must have that $\lambda_i = 0$ for all $i = 1, \ldots, t$. In other words, $h_1, \ldots, h_t$ are linearly independent over $\mathbb{F}_2$. Furthermore, the functions $g_1, \ldots, g_k, h_1, \ldots, h_t$ are also linearly independent. Hence we can construct the function F' in the following form

$$F'(x, y) = (g_1(x, y), \ldots, g_k(x, y), h_1(x), \ldots, h_t(x)).$$

Thus, F' is an $(n, k+t)$-MNBC function, since the non-bent component functions of F' are 0 and $v \cdot (h_1, \ldots, h_t)$ for $v \in \mathbb{F}_2^{t^*}$. Furthermore, as the coordinates $g_1, \ldots, g_k, h_1, \ldots, h_t$ are linearly independent, we note that the dimension of the linear code $\mathcal{C}_{F'}$ is given by $\dim(\mathcal{C}_{F'}) = 1 + n + k + t$ which, by definition, means that F' is a nontrivial $(n, k+t)$-MNBC function. Consequently, the (n, n)-MNBC function F is an t-step extension. □

Example 6.2.18. Let $k = 9$ and $t = 3$. Suppose that α is a primitive element of $\mathbb{F}_{2^3}$. Since $284 \cdot (2^3 + 1) \mod 2^9 - 1 = 1$, let $\pi(y) = y^{284}$ be a permutation on $\mathbb{F}_{2^9}$. Let $\gamma_1, \gamma_2, \gamma_3$ be distinct elements in $\mathbb{F}_{2^{18}} \setminus \mathbb{F}_{2^9}$. Then

$$\begin{aligned} F(x, y) = xy^{284} &+ (Tr_1^9(x) + 1)(\gamma_1 \alpha (Tr_1^9(\alpha x) + 1) \\ &+ \gamma_2 \alpha^2 (Tr_1^9(\alpha^2 x) + 1)) + \gamma_3 \delta_0(x) \end{aligned}$$

is a 3-step $(18, 18)$-MNBC function outside $\mathcal{M}^\#$.

Additionally, we specify the bounds for the value of t in Theorem 6.2.17, thus determining a measure of non-triviality of the constructed MNBC-functions.

Remark 6.2.19. Let $n = 2k$ and k/t be odd, i.e., $k = mt$, m odd. Note that $m > 1$ as for $m = 1$ we obtain that $d(2^t + 1) \mod (2^t - 1) = 1$ holds for $d = 2^{t-1}$ and $\mathrm{wt}(d) = 1$ which implies that the function is in $\mathcal{M}^{\#}$. Hence, without loss of generality, we may assume that $m \geq 3$, then $t = \frac{n}{2m} \leq \frac{n}{6}$, i.e., we have that $3 \leq t \leq n/6$. Furthermore, since t is a positive divisor of k and $k/\gcd(k,t) = k/t$ is odd it follows that $\gcd(2^t+1, 2^k-1) = 1$. From [33, Theorem 4.1.-(i)], there exists a unique solution of the linear congruence $d(2^t + 1) \equiv 1 \pmod{2^k - 1}$.

Finally, we give a precise expression of d for $t = 3$, and hence, show that Example 6.2.18 is a particular instance of an explicit infinite family of MNBC functions.

Proposition 6.2.20. *Let $k = 3m$, where $m = 3 + 2l$ for some $l \in \mathbb{N}_0$. Let also*

$$d = 2^{k-1} + \sum_{i=1}^{l+1} \left(2^{k-6i+1} + 2^{k-6i} + 2^{k-6i-1}\right).$$

Then we have that $wt(d) \geq 3$ and $d(2^3 + 1) \equiv 1 \pmod{2^k - 1}$.

Proof. The fact that $\mathrm{wt}(d) \geq 3$ follows from the definition of d. Denote by θ the number $(2^3 + 1)d - 1$ and compute it in the following way:

$$\begin{aligned}
\theta &= 2^{k+2} + 2^{k-1} \\
&+ \sum_{i=1}^{l+1} \left(2^{k-6i+4} + 2^{k-6i+3} + 2^{k-6i+2} + 2^{k-6i+1} + 2^{k-6i} + 2^{k-6i-1}\right) - 1 \\
&= 2^{k+2} + 2^{k-1} + \left(2^{k-2} + 2^{k-3} + 2^{k-4} + 2^{k-5} + 2^{k-6} + 2^{k-7}\right) \\
&+ \left(2^{k-8} + 2^{k-9} + 2^{k-10} + 2^{k-11} + 2^{k-12} + 2^{k-13}\right) + \ldots \\
&+ \left(2^{k-6l-2} + 2^{k-6l-3} + 2^{k-6l-4} + 2^{k-6l-5} + 2^{k-6l-6} + 2^{k-6l-7}\right) \\
&+ 2 + 1 - 2 - 1 - 1 = 2^2(2^k - 1) + (2^k - 1) = (2^k - 1)(2^2 + 1),
\end{aligned}$$

because $k - 6l = 9$ and $2^k - 1 = \sum_{i=0}^{k-1} 2^i$. Since $(2^k - 1)|\theta$, the result follows. □

In addition to the questions raised in Sections 6.2.1 and 6.2.2, we would like to mention the following open problems.

1. In $n = 6$ variables, all $(n/2-1)$-step and $n/2$-step extension MNBC functions belong to the $\mathcal{M}^{\#}$ class. In view of this observation, it is interesting to ask whether $(n/2-1)$-step and $n/2$-step extension MNBC functions outside $\mathcal{M}^{\#}$ can in general exist for $n > 6$.
2. To the best of our knowledge, for a t-step extension (n, n)-MNBC function outside the $\mathcal{M}^{\#}$ class, the largest known value of t is equal to $n/6$ and achieved by the construction in Theorem 6.2.17. In view

of this result, we suggest to find constructions of t-step extension (n, n)-MNBC functions outside the $\mathcal{M}^{\#}$ class with $t > n/6$.

Chapter 7

Explicit infinite families of 4-decompositions outside $\mathcal{M}^{\#}$

In this chapter, we provide some fundamental results related to the inclusion in $\mathcal{M}^{\#}$ and eventually we obtain many infinite families of bent functions that are provably outside $\mathcal{M}^{\#}$. The fact that a bent function f is in/outside $\mathcal{M}^{\#}$ if and only if its dual is in/outside $\mathcal{M}^{\#}$ is employed in the so-called 4-decomposition of a bent function on $\mathbb{F}_2^n$, which was originally considered by Canteaut and Charpin [14] in terms of the second-order derivatives and later reformulated in [39] in terms of the duals of its restrictions to the cosets of an $(n-2)$-dimensional subspace V. For each of the three possible cases of this 4-decomposition of a bent function (all four restrictions being bent, semi-bent, or 5-valued spectra functions), we provide generic methods for designing bent functions provably outside $\mathcal{M}^{\#}$. For instance, for the elementary case of defining a bent function $h(x, y_1, y_2) = f(x) \oplus y_1 y_2$ on $\mathbb{F}_2^{n+2}$ using a bent function f on $\mathbb{F}_2^n$, we show that h is outside $\mathcal{M}^{\#}$ if and only if f is outside $\mathcal{M}^{\#}$. This approach is then generalized to the case when two bent functions are used. More precisely, the concatenation $f_1||f_1||f_2||(1 \oplus f_2)$ also gives bent functions outside $\mathcal{M}^{\#}$ if either f_1 or f_2 is outside $\mathcal{M}^{\#}$. The cases when the four restrictions of a bent function are semi-bent or 5-valued spectra functions are also considered and several design methods of designing infinite families of bent functions outside $\mathcal{M}^{\#}$, using the spectral domain design considered in [37, 39], are proposed.

7.1 Preliminary results on the spectral design

7.1.1 Specifying 5-valued spectra functions through duals

We first recall certain notations, introduced in [39], useful in handling the 5-valued spectra Boolean function which has two different non-zero absolute values.

Let the WHT spectrum of a function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ contain the values $0, \pm c_1, \pm c_2$ ($c_1 \neq c_2$), where $c_1, c_2 \in \mathbb{N}$. Some of the results in [39] are stated in a more general context, but since the 4-decomposition of bent functions is our main objective we only consider the cases $c_1 = 2^{n/2}$ and $c_2 = 2^{(n+2)/2}$ above. For $i = 1, 2$, by $S_f^{[i]} \subset \mathbb{F}_2^n$ we denote the set

$$S_f^{[i]} = \{u \in \mathbb{F}_2^n : |W_f(u)| = c_i\},$$

and we can define the functions $f_{[i]}^* : S_f^{[i]} \to \mathbb{F}_2$ such that the following equality holds:

$$W_f(u) = \begin{cases} 0, & u \notin S_f^{[1]} \cup S_f^{[2]}, \\ c_i \cdot (-1)^{f_{[i]}^*(u)}, & u \in S_f^{[i]}, \ \ i \in \{1, 2\}. \end{cases} \tag{7.1}$$

For $i = 1, 2$, let $v_i \in \mathbb{F}_2^n$ and $E_i = \{e_0^{(i)}, \ldots, e_{2^{\lambda_i}-1}^{(i)}\} \subset \mathbb{F}_2^n$ ($e_0^{(i)} = \mathbf{0}_n$) be lexicographically ordered subsets of cardinality 2^{λ_i} such that

$$S_f^{[i]} = \{\omega_0^{(i)}, \ldots, \omega_{2^{\lambda_i}-1}^{(i)}\} = v_i \oplus E_i,$$

where $\omega_j^{(i)} = v_i \oplus e_j^{(i)}$, for $j \in [0, 2^{\lambda_i} - 1]$. Clearly, the lexicographically ordered set E_i imposes an ordering on $S_f^{[i]}$ with respect to the equality $\omega_j^{(i)} = v_i \oplus e_j^{(i)}$. Using the representation of $S_f^{[i]} = v_i \oplus E_i$ and the fact that the cardinality of $S_f^{[i]}$ is a power of two the function $\overline{f}_{[i]}^*$, as a mapping from $\mathbb{F}_2^{\lambda_i}$ to $\mathbb{F}_2$, is defined as

$$\overline{f}_{[i]}^*(x_j) = f_{[i]}^*(v_i \oplus e_j^{(i)}) = f_{[i]}^*(\omega_j^{(i)}), \ \ j \in [0, 2^{\lambda_i} - 1], \tag{7.2}$$

where $\mathbb{F}_2^{\lambda_i} = \{x_0, \ldots, x_{2^{\lambda_i}-1}\}$ is ordered lexicographically.

A more specific method for designing 5-valued spectra functions on $\mathbb{F}_2^n$ (thus $W_f(u) \in \{0, \pm 2^{n/2}, \pm 2^{\frac{n+2}{2}}\}$), originally considered in [39], will be used in Section 7.2.5 for specifying suitable quadruples of such functions whose concatenation will give bent functions outside $\mathcal{M}^{\#}$.

7.1.2 Decomposition of bent functions

The decomposition of bent functions on $\mathbb{F}_2^n$, n is even, to affine subspaces $a \oplus V$, for some k-dimensional linear subspace $V \subset \mathbb{F}_2^n$, was considered in [14]. For a bent function $\mathfrak{f} \in \mathcal{B}_n$, the restriction to $a \oplus V$ is denoted by $\mathfrak{f}_{a \oplus V}$ and it can be viewed as a function from $\mathbb{F}_2^k \to \mathbb{F}_2$ using

$$\mathfrak{f}_{a \oplus V}(x_i) = \mathfrak{f}_{a \oplus V}(a \oplus v_i), \quad i \in [0, 2^k - 1], \tag{7.3}$$

for lexicographically ordered $V = \{v_0, \ldots, v_{2^k-1}\}$ and $\mathbb{F}_2^k = \{x_0, \ldots, x_{2^k-1}\}$. This identification between V and $\mathbb{F}_2^k$, and thus the definition of $\mathfrak{f}_{a\oplus V} : \mathbb{F}_2^k \to \mathbb{F}_2$, strongly depends on the ordering of V.

The 4-decomposition of a bent function $\mathfrak{f} \in \mathcal{B}_n$, as a special case considered in [14], then defines four subfunctions on the four cosets of some $(n-2)$-dimensional linear subspace. More precisely, for nonzero $a, b \in \mathbb{F}_2^n$ with $a \neq b$ this $(n-2)$-dimensional subspace is defined as $V = \langle a, b\rangle^\perp$, where the *dual* of a linear subspace, say $S \subset \mathbb{F}_2^n$, is defined as $S^\perp = \{x \in \mathbb{F}_2^n : x \cdot y = 0,\ \forall y \in S\}$.

Let (f_1, f_2, f_3, f_4) be such a decomposition, that is, $f_1, \ldots, f_4 \in \mathcal{B}_{n-2}$ are defined on the four cosets $\mathbf{0}_n \oplus V, a \oplus V, b \oplus V, (a \oplus b) \oplus V$ respectively, thus $Q = \langle a, b\rangle$ and $Q \oplus V = \mathbb{F}_2^n$ (with $Q \cap V = \{\mathbf{0}_n\}$). Such a decomposition is called a *bent 4-decomposition* when all f_i ($i \in [1, 4]$), are bent; a *semi-bent 4-decomposition* when all f_i ($i \in [1, 4]$) are semi-bent; a *5-valued 4-decomposition* when all f_i ($i \in [1, 4]$) are 5-valued spectra functions so that $W_{f_i} \in \{0, \pm 2^{(n-2)/2}, \pm 2^{n/2}\}$ [14]. These are the only possibilities and we strictly have that all the restrictions have the same spectral profile, for instance the restrictions cannot be a mixture of bent and semi-bent functions.

The 4-decomposition was fully described in [14] in terms of the second-order derivatives (with respect to a and b) of the dual $\mathfrak{f}^*$ of a bent function $\mathfrak{f}$. Alternatively, the approach that will be used in this thesis, this decomposition can be specified in terms of Walsh supports and duals of its restrictions $f_1, \ldots, f_4$ [39]. Note that functions f_i are considered as functions in $(n-2)$-variables in terms of relation (7.3) (that is when $\dim(V) = k = n - 2$).

Theorem 7.1.1. *[39] Let $\mathfrak{f} \in \mathcal{B}_n$ be a bent function, for even $n \geq 4$. Let $a, b \in \mathbb{F}_2^n \setminus \{\mathbf{0}_n\}$ $(a \neq b)$ and $V = \langle a, b\rangle^\perp$. If we denote by $(f_1, \ldots, f_4)$ the 4-decomposition of $\mathfrak{f}$ with respect to V, then $(f_1, \ldots, f_4)$ is:*

1. *A bent 4-decomposition if and only if it holds that $f_1^* \oplus f_2^* \oplus f_3^* \oplus f_4^* = 1$.*
2. *A semi-bent 4-decomposition if and only if functions f_i ($i \in [1, 4]$) are pairwise disjoint spectra semi-bent functions[1].*
3. *A five-valued 4-decomposition if and only if the following statements hold:*
   a) *The sets $S_{f_i}^{[1]} = \{\vartheta \in \mathbb{F}_2^{n-2} : |W_{f_i}(\vartheta)| = 2^{\frac{n}{2}}\}$ ($i \in [1, 4]$) are pairwise disjoint;*
   b) *All $S_{f_i}^{[2]} = \{\vartheta \in \mathbb{F}_2^{n-2} : |W_{f_i}(\vartheta)| = 2^{\frac{n-2}{2}}\}$ are equal ($i \in [1, 4]$), and for $f_{[2],i}^* : S_{f_i}^{[2]} \to \mathbb{F}_2$ it holds that $f_{[2],1}^* \oplus f_{[2],2}^* \oplus f_{[2],3}^* \oplus f_{[2],4}^* = 1$.*

[1] Two semi-bent functions f_1 and f_2 on $\mathbb{F}_2^{n-2}$, for even n, are said to be disjoint spectra functions if $W_{f_1}(u) = 0 \Rightarrow W_{f_1}(u) = \pm 2^{n/2}$, or vice versa.

In the rest of this thesis, we consider the canonical 4-decomposition so that $a = (0, 0, \ldots, 0, 1)$, $b = (0, 0, \ldots, 1, 0) \in \mathbb{F}_2^n$ and consequently $V = \mathbb{F}_2^{n-2} \times \{(0, 0)\}$ in Theorem 7.1.1. Then, the function $\mathfrak{f}$ is the concatenation of $f_i \in \mathscr{B}_{n-2}$ which we denote by $\mathfrak{f} = f_1||f_2||f_3||f_4$.

7.2 Decomposing bent functions - design methods

From the design perspective, Theorem 7.1.1 allows us to specify (possibly new) bent functions by specifying suitable quadruples of bent, semi-bent, or 5-valued spectra functions. We develop these ideas below more precisely in the rest of this section, but before this we propose an efficient algorithm for testing the inclusion in $\mathcal{M}^{\#}$, which was used throughout the thesis.

7.2.1 An algorithm for determining whether $f \in \mathcal{M}^{\#}$

We first describe an algorithmic approach to determine whether a bent function is outside $\mathcal{M}^{\#}$. The algorithm is based on Lemma 2.2.4 and some graph-theoretical concepts.

Let $f \in \mathcal{B}_n$ be a bent function. Set $\Gamma = (V, E)$ to be a graph with edge set

$$E = \{\{a, b\} : a, b \in \mathbb{F}_{2^n}^*; D_a D_b f \equiv 0\},$$

and vertex set $V \subset \mathbb{F}_{2^n}^*$ consisting of all distinct vertices appearing in the edge set E. For simplicity, we do not add 0 to V as $D_0 D_b f \equiv 0$ for all $b \in \mathbb{F}_{2^n}$. With this approach, we reduce the size of the vertex set V as $D_a D_b f \not\equiv 0$, for some $a, b \in \mathbb{F}_{2^n}^*$. In practice, the size of the vertex set becomes relatively small and for instance in dimension $n = 8$ we could verify that typical values for $|V|$ are 0 and 6. We also remark that we consider the graph Γ to be simple as there are no loops ($D_a D_a f \equiv 0$ holds for all $a \in \mathbb{F}_{2^n}$); and it is not directed since $D_a D_b f = D_b D_a f$ for any $a, b \in \mathbb{F}_{2^n}$.

From Lemma 2.2.4, we know that we need to find an $(n/2)$-dimensional linear subspace V of $\mathbb{F}_{2^n}$ on which the second-order derivatives of f vanish. From the graph-theoretical perspective, this problem corresponds to finding a clique Λ (a complete subgraph) of size $2^{n/2} - 1$ in the graph Γ and additionally checking whether $V(\Lambda) \cup \{0\}$ forms a linear subspace in $\mathbb{F}_2^n$. Finding a clique in a graph is known to be an NP-complete problem and, specifically, the time complexity of this search would be of size $\mathcal{O}(2^{n2^{n/2}})$. However, in practice, this number is much smaller because the number of vertices (namely $|V|$) of the graph Γ is almost negligible compared to 2^n. The full Sage implementation has been added to the appendix. It might be of interest to optimize further the performance of this algorithm so that larger input sizes can be efficiently tested.

We have considered 100 bent functions in dimension 8 and the average

time needed to check whether one function is outside $\mathcal{M}^\#$ was approx. 17 seconds. For $n = 10$, the average time for checking the property of being in or outside $\mathcal{M}^\#$ was 30 minutes. On the other hand, when $n = 12$, the time complexity is approximately 22 hours on average. For the purpose of this thesis, the proposed algorithm is sufficiently efficient and is superior to a straightforward approach of checking all $n/2$-dimensional subspaces and verifying the vanishing property of the second-order derivatives. Most importantly, all the examples provided in this thesis (in certain cases the ANFs are also given) can be efficiently checked using the Sage algorithm given in Section 7.2.1. We also note the following interesting observation.

Remark 7.2.1. We remark that the dual of a bent function $f \in \mathcal{M}$, given by $f(x, y) = x \cdot \pi(y) \oplus h(y)$ for $x, y \in \mathbb{F}_2^{n/2}$, where π is a permutation on $\mathbb{F}_2^{n/2}$ and h is arbitrary, is apparently in $\mathcal{M}$ (see for instance [19] for the specification of f^*). The same is true when $f \in \mathcal{M}^\#$ is considered since the class inclusion is invariant under the EA transform.

7.2.2 Defining suitable bent 4-decompositions

Recently, a quadruple of *distinct* bent functions, satisfying that $f_1^* \oplus f_2^* \oplus f_3^* \oplus f_4^* = 1$, was identified in [7]. It was additionally shown that their concatenation $f_1||f_2||f_3||f_4$ is provably outside the $\mathcal{M}^\#$ class. More precisely, the authors considered a quadruple of bent functions (not all of them being in $\mathcal{M}^\#$) that belong to the $\mathcal{C}$ and $\mathcal{D}$ class of Carlet [17] and their suitable "modifications" for this purpose. Nevertheless, the following results show that the same method can generate new bent functions outside $\mathcal{M}^\#$ when a single bent function (alternatively a pair of bent functions) outside $\mathcal{M}^\#$ is used.

Theorem 7.2.2. *Let n be even and f be a bent function in n variables. Set $h(x, y_1, y_2) = f(x) \oplus y_1 y_2$ for $y_i \in \mathbb{F}_2$, so that $h = f||f||f||f||(1 \oplus f) \in \mathscr{B}_{n+2}$ is also bent. Then, f is outside $\mathcal{M}^\#$ if and only if h is outside $\mathcal{M}^\#$.*

Proof. It is well-known that $h = f||f||f||f||(1 \oplus f) \in \mathscr{B}_{n+2}$ is bent if f is bent. Notice that 'f is outside $\mathcal{M}^\#$ if and only if h is outside $\mathcal{M}^\#$' is equivalent to 'f is in $\mathcal{M}^\#$ if and only if h is in $\mathcal{M}^\#$'.

Suppose first that h is outside $\mathcal{M}^\#$, thus we want to show that f is outside $\mathcal{M}^\#$. Assume on the contrary that f is in $\mathcal{M}^\#$, thus there exists (at least) one linear subspace $V \subset \mathbb{F}_2^n$ with $\dim(V) = n/2$ such that $D_{a'} D_{b'} f \equiv 0$, for any $a', b' \in V$. Let $E = V \times \{(0, 0), (0, 1)\}$ which is a subspace of $\mathbb{F}_2^{n+2}$ of dimension $n/2 + 1$. We then have that

$$D_{(a',a_1,a_2)} D_{(b',b_1,b_2)} h \equiv 0,$$

for any $a', b' \in V$ and $(a_1, a_2), (b_1, b_2) \in \{(0,0),(0,1)\}$, thus the second-order derivative of h vanish on E. Hence, h is in $\mathcal{M}^{\#}$ which contradicts our assumption that h is outside $\mathcal{M}^{\#}$.

Now, we show that f is outside $\mathcal{M}^{\#}$ implies that h is outside $\mathcal{M}^{\#}$. Assuming $f \notin \mathcal{M}^{\#}$, then for any subspace $V \subset \mathbb{F}_2^n$ with $\dim(V) = n/2$, we can always find two vectors a', b' such that $D_{a'}D_{b'}f \not\equiv 0$. Let $E \subset \mathbb{F}_2^n \times \mathbb{F}_2^2$ be any subspace with $\dim(E) = n/2 + 1$. There are two cases to be considered.

1. If $\dim(E \cap (\mathbb{F}_2^n \times \{(0,0)\})) \geq n/2$, then we can find two vectors $(a', 0, 0), (b', 0, 0)$ and consequently
$$D_{(a',0,0)}D_{(b',0,0)}h = D_{a'}D_{b'}f \not\equiv 0.$$

2. If $\dim(E \cap (\mathbb{F}_2^n \times \{(0,0)\})) < n/2$, then we must have $E \cap (\{0_n\} \times \mathbb{F}_2^2) = \{0_n\} \times \mathbb{F}_2^2$ since $\dim(E) = n/2+1$ (using that $\dim(E \cap (\mathbb{F}_2^n \times \mathbb{F}_2^2)) = n/2 + 1$). Here, there are three cases to be considered.
   (a) If $D_{a'}D_{b'}f \equiv 0$ for any two vectors $(a', 0, 0), (b', 0, 0) \in E \cap (\mathbb{F}_2^n \times \{(0,0)\})$, then we can specify $(a_1, a_2) = (1, 0), (b_1, b_2) = (1, 1)$ so that
   $$D_{(a_1,a_2)}D_{(b_1,b_2)}(y_1y_2) = 1.$$
   Thus,
   $$D_{(a',a_1,a_2)}D_{(b',b_1,b_2)}h = D_{a'}D_{b'}f \oplus D_{(a_1,a_2)}D_{(b_1,b_2)}(y_1y_2) \equiv 1 \neq 0.$$

   (b) If $D_{a'}D_{b'}f \equiv 1$ for any two nonzero vectors $(a', 0_2), (b', 0_2) \in E \cap (\mathbb{F}_2^n \times \{0_2\})$, then we select $(a_1, a_2) = (1, 0), (b_1, b_2) = (0, 0)$ so that
   $$D_{(a_1,a_2)}D_{(b_1,b_2)}y_1y_2 \equiv 0.$$
   Thus,
   $$D_{(a',a_1,a_2)}D_{(b',b_1,b_2)}h = D_{a'}D_{b'}f \oplus D_{(a_1,a_2)}D_{(b_1,b_2)}(y_1y_2) \equiv 1 \neq 0.$$

   (c) If $D_{a'}D_{b'}f \neq const.$ for two nonzero vectors $(a', 0_2), (b', 0_2) \in E \cap (\mathbb{F}_2^n \times \{0_2\})$, then
   $$D_{(a',a_1,a_2)}D_{(b',b_1,b_2)}h = D_{a'}D_{b'}f \neq const.$$
   This concludes the proof.

□

Corollary 7.2.3. *Let n and m be even positive integers and h be a bent function in $\mathscr{B}_n$. Then, the function $f(x, y_1, y_2, \ldots, y_m) = h(x) \oplus y_1y_2 \oplus \cdots \oplus y_{m-1}y_m$ is outside $\mathcal{M}^{\#}$ if and only if h is outside $\mathcal{M}^{\#}$.*

Now, we investigate another non-trivial selection of bent quadruples (different from $f = f_1||f_1||f_1||(1 \oplus f_1)$, which satisfy the necessary and sufficient condition $f_1^* \oplus f_2^* \oplus f_3^* \oplus f_4^* = 1$. It turns out that the basic concatenation method of using just two bent functions, where at least one of them is outside $\mathcal{M}^\#$, also generates bent functions outside $\mathcal{M}^\#$.

Using the convention that $f(x,0,0) = f_1(x)$, $f(x,0,1) = f_2(x)$, $f(x,1,0) = f_3(x)$ and $f(x,1,1) = f_4(x)$, the ANF of $f = f_1||f_2||f_3||f_4$ is given by

$$f(x,y_1,y_2) = f_1(x) \oplus y_1(f_1 \oplus f_3)(x) \oplus y_2(f_1 \oplus f_2)(x) \oplus y_1y_2(f_1 \oplus f_2 \oplus f_3 \oplus f_4)(x). \tag{7.4}$$

Theorem 7.2.4. *Let $n = 2m$ be even and $f_1, f_2 \in \mathscr{B}_n$ be two bent functions. Set $f = f_1||f_1||f_2||(f_2 \oplus 1)$, which by (7.4) gives*

$$f(x,y_1,y_2) = (1 \oplus y_1)f_1(x) \oplus y_1f_2(x) \oplus y_1y_2, \ x \in \mathbb{F}_2^n, y_1, y_2 \in \mathbb{F}_2. \tag{7.5}$$

If either f_1 or f_2 are outside $\mathcal{M}^\#$, then $f \in \mathscr{B}_{n+2}$ is bent and outside $\mathcal{M}^\#$.

Proof. Since $f_1^* \oplus f_1^* \oplus f_2^* \oplus (f_2 \oplus 1)^* = 1$, then f is bent.

For convenience, we denote $a = (a', a_2, a_3), b = (b', b_2, b_3) \in \mathbb{F}_2^n \times \mathbb{F}_2 \times \mathbb{F}_2$. Let V be an arbitrary $(m+1)$-dimensional subspace of $\mathbb{F}_2^{n+2}$. From Lemma 2.2.4, it is sufficient to show that for an arbitrary $(m+1)$-dimensional subspace V of $\mathbb{F}_2^{n+2}$ one can always find two vectors $a, b \in V$ such that $D_{(a',a_2,a_3)}D_{(b',b_2,b_3)}f(x,y_1,y_2) \neq 0$ for some $(x,y_1,y_2) \in \mathbb{F}_2^{n+2}$. We have

$$\begin{aligned} D_{(a',a_2,a_3)}D_{(b',b_2,b_3)}f(x,y_1,y_2) = \ & (1 \oplus y_1)D_{a'}D_{b'}f_1(x) \oplus y_1D_{a'}D_{b'}f_2(x) \\ & \oplus a_2D_{b'}\left(f_1 \oplus f_2\right)(x \oplus a') \\ & \oplus b_2D_{a'}\left(f_1 \oplus f_2\right)(x \oplus b') \oplus a_2b_3 \oplus a_3b_2. \end{aligned} \tag{7.6}$$

There are two cases to be considered.

1. Assuming that $\dim\left(V \cap (\mathbb{F}_2^n \times \{(0,0)\})\right) \geq m$ implies the existence of two vectors $a = (a', a_2, a_3), b = (b', b_2, b_3) \in V$ such that $a' \neq b'$, $a_2 = a_3 = b_2 = b_3 = 0$, for which $D_{a'}D_{b'}f_2 \not\equiv 0$ if we suppose that f_2 is outside $\mathcal{M}^\#$. From (7.6), for $y_1 = 1$, we obtain

$$D_{(a',a_2,a_3)}D_{(b',b_2,b_3)}f(x,1,y_2) = D_{a'}D_{b'}f_2(x) \not\equiv 0.$$

Thus, we have found $a, b \in V$ such that $D_aD_bf(x,1,y_2) \neq 0$, which also implies that $D_aD_bf(x,y_1,y_2) \neq 0$.
Now, assume that $f_1 \notin \mathcal{M}^\#$. Similarly, there will exist two vectors $a = (a'', a_2, a_3), b = (b'', b_2, b_3) \in V$ such that $a'' \neq b''$, $a_2 = a_3 =$

$b_2 = b_3 = 0$, for which $D_{a''}D_{b''}f_1 \not\equiv 0$. Setting $y_1 = 0$ in (7.6), we obtain

$$D_{(a',a_2,a_3)}D_{(b',b_2,b_3)}f(x,0,y_2) = D_{a'}D_{b'}f_1(x) \not\equiv 0,$$

and again we conclude that $D_aD_bf(x,y_1,y_2) \neq 0$.

2. When $\dim(V \cap (\mathbb{F}_2^n \times \{(0,0)\})) < m$, we have $V \cap (\{0_n\} \times \mathbb{F}_2^2) = \mathbb{F}_2^2$ since $\dim\left(V \cap (\mathbb{F}_2^n \times \mathbb{F}_2^2)\right) = m+1$. Furthermore, we can find two vectors $a = (a', a_2, a_3), b = (b', b_2, b_3) \in V$ such that $a' = 0_n, b' = 0_n$, $a_2 = 1, b_2 = 0$, and $a_3 = 0, b_3 = 1$. From (7.6), we have

$$D_{(0_n,1,0)}D_{(0_n,0,1)}f(x,y_1,y_2) = 1 \neq 0. \tag{7.7}$$

Thus, there is no $(m+1)$-dimensional linear subspace of $\mathbb{F}_2^{n+2}$ on which the second-order derivatives of f vanish, i.e., f is outside $\mathcal{M}^{\#}$.

□

Example 7.2.5. Let $f_1, f_2 \in \mathcal{B}_8$ be defined by $f_1(x,y) = x \cdot y$ and $f_2(x,y) = x \cdot \pi_2(y) \oplus \delta_0(x)$, respectively, where $\pi_2 = (0,1,2,3,4,5,8,10,6,12,7,15,13,11,9,14)$ is a permutation of $\mathbb{F}_2^4$ in integer form and $x, y \in \mathbb{F}_2^4$. Here, $\delta_0(x) = \prod(1 \oplus x_i)$ is the indicator of the subspace $0_4 \times \mathbb{F}_2^4$. We note that $f_1 \in \mathcal{M}^{\#}$ and $f_2 \in \mathcal{D}_0 \setminus \mathcal{M}^{\#}$, where $\mathcal{D}_0$ is the class of bent functions introduced by Carlet [17] whose members are of the same form as f_2 above. Let $\mathfrak{f}_1 = (f_1, f_1, f_2, f_2 \oplus 1)$ and $\mathfrak{f}_2 = (f_2, f_2, f_1, f_1 \oplus 1)$ be defined via (7.5). Using the algorithm in Section 7.2.1, we have confirmed that $\mathfrak{f}_1, \mathfrak{f}_2 \in \mathcal{B}_{10}$ are both bent functions outside $\mathcal{M}^{\#}$.

An iterative design of bent functions outside $\mathcal{M}^{\#}$ follows easily from Theorem 7.2.4.

Corollary 7.2.6. *Let $f_1, f_2 \in \mathcal{B}_n$ be two bent functions such that either f_1 or f_2 is outside $\mathcal{M}^{\#}$. Set $\mathfrak{f}_1^{(1)} = (f_1, f_1, f_2, f_2 \oplus 1)$ and $\mathfrak{f}_2^{(1)} = (f_2, f_2, f_1, f_1 \oplus 1)$. For $k \geq 2$ we define*

$$\mathfrak{f}_1^{(k)} = (\mathfrak{f}_1^{(k-1)}, \mathfrak{f}_1^{(k-1)}, \mathfrak{f}_2^{(k-1)}, \mathfrak{f}_2^{(k-1)} \oplus 1)$$

and

$$\mathfrak{f}_2^{(k)} = (\mathfrak{f}_2^{(k-1)}, \mathfrak{f}_2^{(k-1)}, \mathfrak{f}_1^{(k-1)}, \mathfrak{f}_1^{(k-1)} \oplus 1).$$

Then, $\mathfrak{f}_1^{(k)}$ and $\mathfrak{f}_2^{(k)}$ are bent functions in $n+2k$ variables outside $\mathcal{M}^{\#}$.

7.2.3 Constructing bent 4-decompositions using $\mathcal{SC}$ and $\mathcal{CD}$

Using Theorem 7.1.1, we show that bent functions stemming from $\mathcal{M}, \mathcal{C}, \mathcal{D}_0$ and $\mathcal{SC}$ form a bent 4-decomposition. To satisfy the conditions of Theorem 7.1.1, we note that f_1 is defined by $f_1(x,y) = Tr_1^m(xy^d) + 1$

instead of $Tr_1^m(xy^d)$, so that the sum $f_1^*+f_2^*+f_3^*+f_4^*$ equals 1 (otherwise it would be 0).

Theorem 7.2.7. *Let $n = 2m$, s be a positive divisor of m such that m/s is odd, and d a positive integer such that $d(2^s+1) \equiv 1 \pmod{2^m-1}$ and $wt(d) \geq 3$. Let $f_1 : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ be defined by $f_1(x,y) = Tr_1^m(xy^d)+1$, and f_2, f_3 and f_4 be defined by (5.16), (5.17) and (5.21), respectively. Then, $f = (f_1, \ldots, f_4)$ is a bent function in $n+2$ variables.*

Proof. Firstly, we note that $f_1^*(x,y) = Tr_1^m(x^{2^s+1}y)+1$, $x, y \in \mathbb{F}_{2^m}$. From Propositions 5.4.2, 5.4.1 and 5.4.8 it is easy to compute that $f_1^*(x,y) + f_2^*(x,y) + f_3^*(x,y) + f_4^*(x,y) = 1$ for all $x, y \in \mathbb{F}_{2^m}$. Thus, by Theorem 7.1.1 it holds that $f = (f_1, \ldots, f_4)$ is a bent 4-decomposition, i.e., it follows that f is a bent function in $n+2$ variables. □

Remark 7.2.8. Explicitly, let $f = (f_1, f_2, f_3, f_4)$ be defined as in Theorem 7.1.1, then by [37, Corollary 1], we can write $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \times \mathbb{F}_{2^2} \to \mathbb{F}_2$ as

$$f(x, y, z_1, z_2) = f_1(x,y) + z_1(f_1+f_3)(x,y) + z_2(f_1+f_2)(x,y), \quad (7.8)$$

for $x, y \in \mathbb{F}_{2^m}$, $z_1, z_2 \in \mathbb{F}_2$ which corresponds to the concatenation $f = f_1||f_2||f_3||f_4$. Let f_1, f_2, f_3, f_4 and f be defined as in Theorem 7.2.7, then (7.8) evaluates to:

$$f(x, y, z_1, z_2) = Tr_1^m(xy^d) + z_1\mathbb{1}_{L^\perp}(x) + z_2\delta_0(x) + z_1 + z_2 + 1,$$

for $x, y \in \mathbb{F}_{2^m}$, $z_1, z_2 \in \mathbb{F}_2$.

Moreover, it turns out that bent functions described in Theorem 7.2.7 do not belong to the completed $\mathcal{M}$ class. For convenience, we use the vector space representation below.

Theorem 7.2.9. *Let $n = 2m$ be even and $f \in \mathcal{B}_n$ be given as in Theorem 7.2.7 so that*

$$f(x, y, z_1, z_2) = \phi(y) \cdot x \oplus z_1\mathbb{1}_{L^\perp}(x) \oplus z_2\delta_0(x) \oplus z_1 \oplus z_2 \oplus 1, \quad (7.9)$$

where $x, y \in \mathbb{F}_2^m$, $z_1, z_2 \in \mathbb{F}_2$. If $c \cdot \phi$ has no nonzero linear structures for any $c \in \mathbb{F}_2^m \setminus \{\mathbf{0}_m\}$, then f is outside $\mathcal{M}^\#$.

Proof. For convenience, we denote $a = (a_1, a_2, a_3, a_4), b = (b_1, b_2, b_3, b_4) \in \mathbb{F}_2^m \times \mathbb{F}_2^m \times \mathbb{F}_2^m \times \mathbb{F}_2^m$. Let V be an arbitrary $(m+1)$-dimensional subspace of $\mathbb{F}_2^{n+2}$. It is sufficient to show that for an arbitrary $(m+1)$-dimensional subspace V of $\mathbb{F}_2^{n+2}$ one can always find two vectors $a, b \in V$ such that $D_{(a_1,a_2,a_3,a_4)}D_{(b_1,b_2,b_3,b_4)}f(x, y, z_1, z_2) \neq 0$ for some $(x, y, z_1, z_2) \in \mathbb{F}_2^{n+2}$. We have

$$\begin{aligned} & D_{(a_1,a_2,a_3,a_4)}D_{(b_1,b_2,b_3,b_4)}f(x, y, z_1, z_2) = D_{a_2}D_{b_2}(\phi(y)) \cdot x \\ \oplus\ & D_{b_2}(\phi(y \oplus a_2)) \cdot a_1 \oplus D_{a_2}(\phi(y \oplus b_2)) \cdot b_1 \\ \oplus\ & z_2 D_{a_1}D_{b_1}\delta_0(x) \oplus z_1 D_{a_1}D_{b_1}\mathbb{1}_{L^\perp}(x) \oplus T(x), \end{aligned} \quad (7.10)$$

where $T(x) = a_3 D_{b_1} \mathbb{1}_{L^\perp}(x \oplus a_1) \oplus b_3 D_{a_1} \mathbb{1}_{L^\perp}(x \oplus b_1) \oplus a_4 D_{b_1}\delta_0(x \oplus a_1) \oplus b_4 D_{a_1}\delta_0(x \oplus b_1)$. There are three cases to be considered.

1. Let $|\{x \in \mathbb{F}_2^m : (x, y, z_1, z_2) \in V\}| > 2$. We can select two vectors $a, b \in V$ such that $a_1 \neq \mathbf{0}_m, b_1 \neq \mathbf{0}_m$ and $a_1 \neq b_1$. From (7.10), we have

$$D_{(a_1,a_2,a_3,a_4)} D_{(b_1,b_2,b_3,b_4)} f(x, y, z_1, z_2) = z_2 D_{a_1} D_{b_1} \delta_0(x) \oplus M(x, y, z_1),$$

where

$$\begin{aligned} M(x, y, z_1) = {} & D_{a_2} D_{b_2}(\phi(y)) \cdot x \oplus D_{b_2}(\phi(y \oplus a_2)) \cdot a_1 \\ & \oplus D_{a_2}(\phi(y \oplus b_2)) \cdot b_1 \oplus z_1 D_{a_1} D_{b_1} \mathbb{1}_{L^\perp}(x) \\ & \oplus T(x). \end{aligned}$$

As $D_{a_1} D_{b_1} \delta_0 \not\equiv 0$, it must hold that $D_a D_b f \not\equiv 0$.

2. Let $|\{x \in \mathbb{F}_2^m : (x, y, z_1, z_2) \in V\}| = 2$. We select $a = (a_1, a_2, a_3, a_4) \in V$ such that $a_1 \neq \mathbf{0}_m$. Since $|V| = 2^{m+1}$, we can select $b = (b_1, b_2, b_3, b_4) \in V$ such that $b_1 = \mathbf{0}_m$ and $b_2 \neq \mathbf{0}_m$. Notice that $b_1 = 0_m$ implies that $D_{a_2}(\phi(y \oplus b_2)) \cdot b_1 = 0$. From (7.10), we deduce that

$$D_{(a_1,0_m,0,0)} D_{(0_m,b_2,0,0)} f(x, y, z_1, z_2)\Big|_{x=0_m, z_1=z_2=0} = D_{b_2}(\phi(y)) \cdot a_1.$$

As $c \cdot \phi$ has no nonzero linear structures for any $c \in \mathbb{F}_2^m \setminus \{\mathbf{0}_m\}$, then $D_{b_2}\phi(y) \cdot a_1$ is not a constant function. Thus, we have found two elements $a, b \in V$ such that $D_a D_b f \not\equiv 0$.

3. Let $|\{x \in \mathbb{F}_2^m : (x, y, z_1, z_2) \in V\}| = 1$. We have $|\{y \in \mathbb{F}_2^m : (x, y, z_1, z_2) \in V\}| \geq 2^{m-1}$. For any $a = (\mathbf{0}_m, a_2, a_3, a_4) \in V$ such that $a_2 \neq \mathbf{0}_m$, we have $D_{a_2}\phi_i \not\equiv const.$, $D_{a_2}\phi_j \not\equiv const.$ and $D_{a_2}(\phi_i \oplus \phi_j) \not\equiv const.$, where $1 \leq i \neq j \leq m$ and $\phi = (\phi_1, \ldots, \phi_m)$, since $c \cdot \phi$ has no nonzero linear structure for any $c \in \mathbb{F}_2^m \setminus \{\mathbf{0}_m\}$. Furthermore,

$$|\{b_2 \in \mathbb{F}_2^m : D_{b_2} D_{a_2} \phi_i = D_{b_2} D_{a_2} \phi_j \equiv 0_m\}| < 2^{m-1},$$

since the maximum cardinality

$$|\{b_2 \in \mathbb{F}_2^m : D_{b_2} D_{a_2} \phi_i = D_{b_2} D_{a_2} \phi_j \equiv 0_m\}| = 2^{m-2}$$

is attained if both $D_{a_2}\phi_i$ and $D_{a_2}\phi_j$ are affine. Hence, we can select two vectors $a, b \in V$ such that $D_{a_2} D_{b_2} \phi \not\equiv 0_m$. Since

$$D_{(\mathbf{0}_m,a_2,a_3,a_4)} D_{(\mathbf{0}_m,b_2,b_3,b_4)} f(x, y, z_1, z_2) = D_{a_2} D_{b_2}(\phi(y)) \cdot x,$$

we conclude that $D_{(a_1,a_2,a_3,a_4)} D_{(b_1,b_2,b_3,b_4)} f \not\equiv 0$.

□

Similarly as in Theorem 7.2.7, we will show that certain functions from $\mathcal{M}, \mathcal{C}, \mathcal{D}$ and $\mathcal{CD}$ can form a bent 4-decomposition.

Theorem 7.2.10. *Let $n = 2m$, s be a positive divisor of m such that m/s is odd, and d a positive integer such that $d(2^s+1) \equiv 1 \pmod{2^m-1}$ and $wt(d) \geq 3$. Let $E_2 = \mathbb{F}_{2^s}$, $L \subset E_2$ be a subspace of $\mathbb{F}_{2^m}$ and $E_1 = E_2^{\perp}$. Let $f_1 : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ be defined by $f_1(x,y) = Tr_1^m(xy^d)+1$, and f_2, f_3 and f_4 be defined by:*

$$\begin{aligned} f_2(x,y) &= Tr_1^m(xy^d) + \mathbb{1}_{L^{\perp}}(x), \\ f_3(x,y) &= Tr_1^m(xy^d) + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y), \\ f_4(x,y) &= Tr_1^m(xy^d) + \mathbb{1}_{L^{\perp}}(x) + \mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y). \end{aligned}$$

Then, $f = (f_1, \ldots, f_4)$ is a bent function in $n+2$ variables.

Proof. From Proposition 5.4.2, Theorem 5.4.7 and Theorem 5.4.9, it is easy to compute that $f_1^*(x,y) + f_2^*(x,y) + f_3^*(x,y) + f_4^*(x,y) = 1$ for all $x, y \in \mathbb{F}_{2^m}$. Thus, by Theorem 7.1.1, it holds that $f = (f_1, \ldots, f_4)$ is a bent 4-decomposition, i.e., it follows that f is a bent function in $n+2$ variables. □

Remark 7.2.11. Let f_1, f_2, f_3, f_4 and f be defined as in Theorem 7.2.10, then (7.8) evaluates to

$$f(x, y, z_1, z_2) = Tr_1^m(xy^d) + z_1\mathbb{1}_{L^{\perp}}(x) + z_2\mathbb{1}_{E_1}(x)\mathbb{1}_{E_2}(y) + z_1 + z_2 + 1,$$

where $x, y \in \mathbb{F}_{2^m}$, $z_1, z_2 \in \mathbb{F}_2$.

7.2.4 Semi-bent case of 4-decomposition

The construction of disjoint spectra semi-bent functions was treated in several articles, see [38] and references therein. In terms of the spectral design method in [38], constructing quadruples of semi-bent functions on $\mathbb{F}_2^n$ (with n even), whose spectra belong to $\{0, \pm 2^{\frac{n+2}{2}}\}$, with pairwise disjoint spectra can be easily achieved by specifying suitable Walsh supports. It has already been observed in [37, 94] that trivial plateaued functions, having an affine subspace as their Walsh support, essentially correspond to partially bent functions introduced by Carlet in [16] which admit linear structures. Nevertheless, the selection of these Walsh supports as affine subspaces or subsets will be shown to be irrelevant for the class inclusion of the resulting bent functions, which will be entirely governed by the bent duals.

Known results on the design methods of plateaued Boolean functions

Before proving the main results of this section, we will give a brief overview of some known useful results obtained in [38] regarding the

construction and properties of s-plateaued Boolean functions. For simplicity, we adopt these results for semi-bent functions, thus $s = 2$, and employ only the parts relevant for our purposes.

Theorem 7.2.12. *[38, Theorem 3.3 (with $s = 2$)] Let $S_f = v \oplus EM = \{\omega_0, \ldots, \omega_{2^{n-2}-1}\} \subset \mathbb{F}_2^n$, for some $v \in \mathbb{F}_2^n$, $M \in GL(n, \mathbb{F}_2)$ and subset $E = \{e_0, e_1, \ldots, e_{2^{n-2}-1}\} \subset \mathbb{F}_2^n$, where n is even. For a function $g : \mathbb{F}_2^{n-2} \to \mathbb{F}_2$ such that $wt(g) = 2^{n-3} + 2^{\frac{n-2}{2}-1}$ or $wt(g) = 2^{n-3} - 2^{\frac{n-2}{2}-1}$ (having bent weight), let the Walsh spectrum of f on $\mathbb{F}_2^n$ be defined (by identifying $x_i \in \mathbb{F}_2^{n-2}$ and $\omega_i \in S_f$ through $e_i \in E$ using (2.4)) as*

$$W_f(u) = \begin{cases} 2^{\frac{n+2}{2}}(-1)^{g(x_i)}, & \text{for } u = v \oplus e_i M \in S_f, \\ 0, & u \notin S_f. \end{cases} \tag{7.11}$$

Then:

i) f is an 2-plateaued (semi-bent) function if and only if g is at bent distance to

$$\Phi_f = \{\phi_u : \mathbb{F}_2^{n-2} \to \mathbb{F}_2 \ : \ \chi_{\phi_u} = ((-1)^{u\cdot\omega_0}, (-1)^{u\cdot\omega_1}, \ldots, (-1)^{u\cdot\omega_{2^{n-2}-1}}), \\ \omega_i \in S_f, \ u \in \mathbb{F}_2^n\}, \tag{7.12}$$

where for a subset $B \subset \mathcal{B}_n$ a function g is said to be at bent distance to B if for all $f \in B$ it holds that $d_H(f, g) = 2^{n-1} \pm 2^{n/2-1}$.

ii) If $E \subset \mathbb{F}_2^n$ is a linear subspace, then f is semi-bent if and only if g is a bent function on $\mathbb{F}_2^{n-2}$.

Remark 7.2.13. Since $|S_f| = 2^{n-2}$ and the absolute value of the Walsh coefficients in Theorem 7.2.12 is $2^{\frac{n+2}{2}}$, Parseval's identity $\sum_{u\in\mathbb{F}_2^n} W_f(u)^2 = 2^{2n}$ is clearly satisfied. For ease of notation, we will consider $f \in \mathscr{B}_{n+2}$ and use a dual bent function $g \in \mathscr{B}_n$. The Walsh support $S_f \subset \mathbb{F}_2^{n+2}$ with $|S_f| = 2^n$, can be specified as a binary matrix of size $2^n \times (n+2)$ of the form $S_f = (c \oplus \mathbb{F}_2^n M) \wr T_{\mu_1} \wr T_{\mu_2}$, $M \in GL(n, \mathbb{F}_2)$ and $c \in \mathbb{F}_2^n$. Here, the part $c \oplus \mathbb{F}_2^n M$ is an affine permutation of $\mathbb{F}_2^n$ and corresponds to the first n columns of S_f; whereas the last two columns $T_{\mu_1} \wr T_{\mu_2}$ of S_f are binary truth tables of $\mu_1, \mu_2 \in \mathscr{B}_n$.

To construct nontrivial semi-bent functions (whose Walsh supports are subsets), one can employ bent functions in the $\mathcal{MM}$ class defined by

$$g(x, y) = x \cdot \psi(y) \oplus t(y); \ \ x, y \in \mathbb{F}_2^{n/2}, \tag{7.13}$$

where ψ is an arbitrary permutation on $\mathbb{F}_2^{n/2}$ and $t \in \mathcal{B}_{n/2}$ is arbitrary. We give below a slightly modified version of Theorem 4.2 in [38] since we are interested in semi-bent functions in even dimensions. Therefore, we define the Walsh support as $S_f = (c \oplus EM) \wr T_\mu \wr T_\mu$ rather than $S_f = (c \oplus EM) \wr T_\mu$ as originally in [38]. Notice that the use of a nonlinear function $\mu : \mathbb{F}_2^n \to \mathbb{F}_2$ ensures that S_f is not an affine/linear subspace.

Theorem 7.2.14. *[38, Theorem 4.2] Let $g(x,y) = x \cdot \psi(y)$, $x, y \in \mathbb{F}_2^{n/2}$, be a bent function, n is even. For an arbitrary matrix $M \in GL(n, \mathbb{F}_2)$ and vector $c \in \mathbb{F}_2^n$, let $S_f = (c \oplus EM) \wr T_\mu \wr T_\mu$, where $E = \mathbb{F}_2^n$ is ordered lexicographically and $\mu \in \mathcal{B}_n$, we have:*

i) Let E_1, E_2 be subspaces of $\mathbb{F}_2^{n/2}$ such that $\psi(E_2) = E_1^\perp$ and define $\mu(x,y) = \phi_{E_1}(x)\phi_{E_2}(y)$, where ϕ_{E_i} denotes the characteristic function of E_i. Then, $f : \mathbb{F}_2^{n+2} \to \mathbb{F}_2$, whose Walsh spectrum is specified by means of (7.11) in Theorem 7.2.12 (with dimension $n+2$ instead of n) is a semi-bent function.

ii) Let L be a subspace of $\mathbb{F}_2^n$ and define $\mu(x,y) = \phi_L(x)$. If $\psi^{-1}(v+L^\perp)$ is an affine subspace for all $v \in \mathbb{F}_2^n$, then $f : \mathbb{F}_2^{n+2} \to \mathbb{F}_2$, whose Walsh spectrum is specified by means of (7.11) in Theorem 7.2.12 (with dimension $n+2$ instead of n), is a semi-bent function.

Bent functions outside $\mathcal{M}^\#$ using semi-bent functions with suitable duals

By employing the above results, the authors in [38] also proposed a construction method of disjoint spectra plateaued functions, see Theorem 4.4 in [38], and additionally showed that these functions can be efficiently utilized for the construction of bent functions. For the particular case of specifying four semi-bent functions on $\mathbb{F}_2^{n+2}$, by using a bent dual $g \in \mathscr{B}_n$, it is convenient to express $\mathbb{F}_2^{n+2} = V \oplus Q$ where for simplicity $V = \mathbb{F}_2^n \times \{(0,0)\}$ and $Q = \mathbf{0}_n \times \mathbb{F}_2^2$. Notice that the choice of V leads to the canonical concatenation/decomposition given by (7.4). The main idea is then to specify disjoint Walsh supports of semi-bent functions f_i on the cosets of V in $\mathbb{F}_2^{n+2}$. The reason for selecting $S_f(c \oplus \mathbb{F}_n^M) \wr T_{t_1} \wr T_{t_2}$ in Theorem 7.2.15 as a non-affine subspace is to demonstrate a somewhat harder design rationale that employs Theorem 7.2.12 *i)*, which requires that the set Φ_f is at bent distance to the bent dual g. Again, the use of a suitable bent dual $g \in \mathscr{B}_n$ (taken outside $\mathcal{M}^\#$) is decisive when the design of bent functions outside $\mathcal{M}^\#$ is considered.

Theorem 7.2.15. *Let n be even and g be a bent function in n variables. For an arbitrary matrix $M \in GL(n, \mathbb{F}_2)$ and vector $c \in \mathbb{F}_2^n$, let $S_f = (c \oplus \mathbb{F}_2^n M) \wr T_{t_1} \wr T_{t_2} \subset \mathbb{F}_2^{n+2}$, where $t_1, t_2 \in \mathcal{B}_n$ such that $g(x,y) \oplus v_1 t_1(x,y) \oplus v_2 t_2(x,y)$ is bent for any $v_1, v_2 \in \mathbb{F}_2$, where $x, y \in \mathbb{F}_2^{n/2}$. Let $Q = \{\mathbf{0}_n\} \times \mathbb{F}_2^2 = \{q_{00}, q_{01}, q_{10}, q_{11}\}$ and set $S_{f_a} = q_a \oplus S_f$, for $q_a \in Q$ and $a \in \mathbb{F}_2^2$. Then, the functions $f_i \in \mathscr{B}_{n+2}$, constructed using Theorem 7.2.12 with S_{f_i} and g, are semi-bent functions on $\mathbb{F}_2^{n+2}$ with pairwise disjoint spectra. Moreover, if $r\text{-}ind(g) < n/2 - 2$, then the function $\mathfrak{f} \in \mathcal{B}_{n+4}$, whose canonical restrictions are $\mathfrak{f}|_{\mathbb{F}_2^{n+2} \times \{a\}} := f_a$, where $a \in \mathbb{F}_2^2$ (thus $\mathfrak{f} = f_{00} || f_{01} || f_{10} || f_{11}$), is a bent function outside $\mathcal{M}^\#$.*

Proof. Let $c \in \mathbb{F}_2^n$ and $M \in GL(n, \mathbb{F}_2)$ be arbitrary. Let $S_f = (c \oplus \mathbb{F}_2^n M) \wr$

$T_{t_1} \wr T_{t_2}$, where $t_1, t_2 \in \mathcal{B}_n$. The columns of $c \oplus \mathbb{F}_2^n M$ correspond to affine functions in n variables, say $l_1, \ldots, l_n \in \mathcal{A}_n$. Thus, by assumption on g, the function $g \oplus v \cdot (l_1, \ldots, l_n, t_1, t_2)$ is bent for any $v \in \mathbb{F}_2^{n+2}$. Hence, g is at bent distance to $\Phi_f = \{\phi_v \in \mathcal{B}_n : T_{\phi_v} = (v \cdot \omega_0, \ldots, v \cdot \omega_{2^n-1}),\ \omega_i \in S_f,\ v \in \mathbb{F}_2^{n+2}\}$. Let $S_{f_a} = q_a \oplus S_f$, for $q_a \in Q$. By Theorem 7.2.12 i), the functions $f_a \in \mathcal{B}_{n+2}$, whose Walsh spectral values at $v \in \mathbb{F}_2^{n+2}$ are defined by:

$$W_{f_a}(v) = \begin{cases} 2^{\frac{n+4}{2}}(-1)^{g(x_i,y_i)}, & v=(c\oplus(x_i,y_i)\cdot M, t_1(x_i,y_i), t_2(x_i,y_i))\oplus q_a \in S_{f_a} \\ 0, & v \notin S_{f_a} \end{cases}, \tag{7.14}$$

are 2-plateaued (semi-bent) functions, for $a \in \mathbb{F}_2^2$. Furthermore, we have $\cup_{q_a \in Q}(q_a \oplus S_f) = \mathbb{F}_2^{n+2}$ and the function $\mathfrak{f} = f_{00}||f_{01}||f_{10}||f_{11} \in \mathcal{B}_{n+4}$ is bent by Theorem 7.1.1 ii). It remains to show that $\mathfrak{f}$ is outside $\mathcal{M}^{\#}$. For convenience, we write $u = (\alpha, \beta, \gamma, \omega) \in \mathbb{F}_2^{n/2} \times \mathbb{F}_2^{n/2} \times \mathbb{F}_2^2 \times \mathbb{F}_2^2$. Then, the Walsh-Hadamard transform of $\mathfrak{f}$ at $u \in \mathbb{F}_2^{n+4}$ evaluates to:

$$\begin{aligned} W_{\mathfrak{f}}(u) &= \sum_{(x,y,z,w)\in(\mathbb{F}_2^{n/2})^2\times(\mathbb{F}_2^2)^2} (-1)^{\mathfrak{f}(x,y,z,w)\oplus(x,y,z,w)\cdot u} \\ &= \sum_{w\in\mathbb{F}_2^2} \sum_{(x,y,z)\in(\mathbb{F}_2^{n/2})^2\times\mathbb{F}_2^2} (-1)^{f_w(x,y,z)\oplus(x,y,z)\cdot(\alpha,\beta,\gamma)\oplus w\cdot\omega} \\ &= \sum_{w\in\mathbb{F}_2^2} (-1)^{w\cdot\omega} \sum_{(x,y,z)\in(\mathbb{F}_2^{n/2})^2\times\mathbb{F}_2^2} (-1)^{f_w(x,y,z)\oplus(x,y,z)\cdot(\alpha,\beta,\gamma)} \\ &= \sum_{w\in\mathbb{F}_2^2} (-1)^{w\cdot\omega} W_{f_w}(\alpha,\beta,\gamma) = (*). \end{aligned}$$

As $\cup_{q\in Q}(q \oplus S_f) = \mathbb{F}_2^{n+2}$ and $q \oplus S_f \cap q' \oplus S_f = \emptyset$ for $q \neq q'$, we have that (α, β, γ) is in exactly one support S_{f_w} for some $w \in \mathbb{F}_2^2$. We note that $(\alpha, \beta) = c \oplus (\alpha', \beta') \cdot M$ for some $(\alpha', \beta') \in \mathbb{F}_2^{n/2} \times \mathbb{F}_2^{n/2}$ and $\gamma = (t_1(\alpha', \beta'), t_2(\alpha', \beta')) \oplus a_\gamma$ for some $a_\gamma \in \mathbb{F}_2^2$, whose choice depends on the value of γ. Hence,

$$(\alpha, \beta, \gamma) = (c \oplus (\alpha', \beta') \cdot M, t_1(\alpha', \beta'), t_2(\alpha', \beta')) \oplus q_{a_\gamma}.$$

Thus, we have that

$$\begin{aligned} (*) &= 2^{\frac{n+4}{2}} \cdot (-1)^{a_\gamma\cdot\omega\oplus g(\alpha',\beta')} \\ &= 2^{\frac{n+4}{2}} \cdot (-1)^{((t_1(((\alpha,\beta)\oplus c)\cdot M^{-1}), t_2(((\alpha,\beta)\oplus c)\cdot M^{-1}))\oplus\gamma)\cdot\omega\oplus g(((\alpha,\beta)\oplus c)\cdot M^{-1})} \end{aligned}$$

which implies that the dual $\mathfrak{f}^* \in \mathcal{B}_{n+4}$ of $\mathfrak{f}$ is defined by

$$\mathfrak{f}^*(x, y, z, w) = ((t_1(((x, y) \oplus c) \cdot M^{-1}), t_2(((x, y) \oplus c) \cdot M^{-1})) \oplus z) \cdot w$$

$$\oplus\, g(((x,y)\oplus c)\cdot M^{-1}),$$

for $x,y\in\mathbb{F}_2^{n/2}$ and $z,w\in\mathbb{F}_2^2$. Without loss of generality, let us consider the function

$$\begin{aligned}\mathfrak{h}(x,y,z,w) &= \mathfrak{f}^*((x,y,z,w)\cdot M'\oplus(c,0_2,0_2))\\ &= ((t_1(x,y),t_2(x,y))\oplus z)\cdot w\oplus g(x,y)\\ &= g(x,y)\oplus z\cdot w\oplus(t_1(x,y),t_2(x,y))\cdot w,\end{aligned}$$

where

$$M'=\left(\begin{array}{c|c} M & O_4\\ \hline O_4 & I_4\end{array}\right).$$

We note that $\mathfrak{h}$ and $\mathfrak{f}^*$ are EA-equivalent functions and thus belong to the same completed class of bent functions.

Let us now consider the second-order derivative of $\mathfrak{h}$. Suppose that V is some $(n+4)/2$-dimensional subspace of $\mathbb{F}_2^{n+4}$ and let $\alpha=(\alpha^{(1)},\alpha^{(2)},\alpha^{(3)},\alpha^{(4)}),\beta=(\beta^{(1)},\beta^{(2)},\beta^{(3)},\beta^{(4)})\in V$ where $\alpha^{(1)},\alpha^{(2)},\beta^{(1)},\beta^{(2)}\in\mathbb{F}_2^{n/2},\alpha^{(3)},\alpha^{(4)},\beta^{(3)},\beta^{(4)}\in\mathbb{F}_2^2$. For easier notation, we will denote with $\alpha_{12}=(\alpha^{(1)},\alpha^{(2)})$ and $\beta_{12}=(\beta^{(1)},\beta^{(2)})$. As w is arbitrary, let $w=\alpha_4\oplus\beta_4$. This further implies that

$$\begin{aligned}D_\alpha D_\beta\mathfrak{h}(x,y,z,w)|_{w=\alpha_4\oplus\beta_4} &= D_{\alpha_{12}}D_{\beta_{12}}g(x,y)\\ &\oplus\alpha_4\cdot(D_{\beta_{12}}t_1(x,y),D_{\beta_{12}}t_2(x,y))\\ &\oplus\beta_4\cdot(D_{\alpha_{12}}t_1(x,y),D_{\alpha_{12}}t_2(x,y))\\ &\oplus\alpha^{(3)}\cdot\beta^{(3)}\oplus\alpha^{(4)}\cdot\beta^{(4)}.\end{aligned}\tag{7.15}$$

First, we note that $\dim(\{(x,y)\in\mathbb{F}_2^{n/2}\times\mathbb{F}_2^{n/2}\colon(x,y,z,w)\in V\})\geq n/2-2$. If

$$\begin{aligned}&\alpha_4\cdot(D_{\beta_{12}}t_1(x,y),D_{\beta_{12}}t_2(x,y))\\ &\oplus\beta_4\cdot(D_{\alpha_{12}}t_1(x,y),D_{\alpha_{12}}t_2(x,y))\\ &\oplus\alpha^{(3)}\cdot\beta^{(3)}\oplus\alpha^{(4)}\cdot\beta^{(4)}=const.,\end{aligned}\tag{7.16}$$

then, from (7.15),

$$D_\alpha D_\beta\mathfrak{h}(x,y,z,w)|_{w=\alpha_4\oplus\beta_4}\neq 0$$

as r-ind$(g)<n/2-2$. On the other hand, if the sum in (7.16) is non-constant, then again from (7.15), we must have

$$D_\alpha D_\beta\mathfrak{h}(x,y,z,w)|_{w=\alpha_4\oplus\beta_4}\neq 0.$$

Thus $\mathfrak{h}\notin\mathcal{M}^\#$, which implies that $\mathfrak{f}^*\notin\mathcal{M}^\#$. By Remark 7.2.1, it means that $\mathfrak{f}$ is outside $\mathcal{M}^\#$. □

Since $g \in \mathscr{B}_n$ is supposed to be a bent function outside $\mathcal{M}^{\#}$, we can employ the class $\mathcal{D}_0$ of Carlet [17] or certain families of bent functions in $\mathcal{C}$ and $\mathcal{D}$ that are provably outside $\mathcal{M}^{\#}$ [45, 88, 89]. Alternatively g can be taken from the recent classes $\mathcal{SC}$ and $\mathcal{CD}$ [5, 7], which are specified in Corollary 7.2.16 below. Notice that the subspaces L, E_1, E_2 used to define g in Corollary 7.2.16 below, satisfy certain conditions with respect to the permutation π, see [17, 89, 88]. However, there exist efficient design methods for specifying bent functions in the above classes that are provably outside $\mathcal{M}^{\#}$ [5, 7, 45, 88, 89]. On the other hand, for $t_1, t_2 \in \mathscr{B}_n$ we use certain indicators that preserve the bentness of $g(x, y) \oplus v_1 t_1(x, y) \oplus v_2 t_2(x, y)$. The results are summarised in the following corollary, where we denote $\delta_0(x) = \prod_{i=1}^{n/2}(x_i \oplus 1)$ which is the indicator function of the subspace $0_{n/2} \times \mathbb{F}_2^{n/2}$.

Corollary 7.2.16. *With the same notation as in Theorem 7.2.15, if a bent function $g \in \mathcal{B}_n$ with r-ind$(g) < n/2 - 2$ and $t_1, t_2 \in \mathcal{B}_n$ are defined by:*

i) $g(x, y) = x \cdot \pi(y) \oplus \delta_0(x) \in \mathcal{D}_0 \setminus \mathcal{M}^{\#}$, $t_1(x, y) = t_2(x, y) = \delta_0(x)$, $x, y \in \mathbb{F}_2^{n/2}$,

ii) $g(x, y) = x \cdot \pi(y) \oplus \mathbf{1}_{L^{\perp}}(x) \in \mathcal{C} \setminus \mathcal{M}^{\#}$, t_1, t_2 *correspond to* $\mathbf{1}_{L^{\perp}}(x)$ *or* $\delta_0(x)$, $x, y \in \mathbb{F}_2^{n/2}$,

iii) $g(x, y) = x \cdot \pi(y) \oplus \mathbf{1}_{L^{\perp}}(x) \oplus \delta_0(x) \in \mathcal{SC} \setminus \mathcal{M}^{\#}$, t_1, t_2 *correspond to* $\mathbf{1}_{L^{\perp}}(x)$ *or* $\delta_0(x)$, $x, y \in \mathbb{F}_2^{n/2}$, *or*

iv) $g(x, y) = x \cdot \pi(y) \oplus \mathbf{1}_{L^{\perp}}(x) \oplus \mathbf{1}_{E_1}(x)\mathbf{1}_{E_2}(y) \in \mathcal{CD} \setminus \mathcal{M}^{\#}$, $t_1(x, y) = t_2(x, y) = \mathbf{1}_{L^{\perp}}(x)$, $x, y \in \mathbb{F}_2^{n/2}$,

then $\mathfrak{f} \in \mathcal{B}_{n+4}$ *is a bent function outside* $\mathcal{M}^{\#}$.

In the following example, we take $g \in \mathcal{D}_0 \setminus \mathcal{M}^{\#}$ in 8 variables to construct a bent function in 12 variables outside $\mathcal{M}^{\#}$ by means of Theorem 7.2.15. The result was also confirmed using our algorithm in Section 7.2.1.

Example 7.2.17. Let $g(x, y) = x \cdot \pi(y) \oplus \delta_0(x)$, $x, y \in \mathbb{F}_2^4$, be a bent function in $\mathcal{D}_0$ (outside $\mathcal{M}^{\#}$), where $\pi = (0, 1, 11, 13, 9, 14, 6, 7, 12, 5, 8, 3, 15, 2, 4, 10)$ is a permutation of $\mathbb{F}_2^4$ represented in integer form. We note that r-ind$(g) = 1$. Let $c \in \mathbb{F}_2^8$ and

$M \in GL(8, \mathbb{F}_2)$ be arbitrary, say,

$$c = (0,0,1,0,1,1,1,1), \quad M = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

Let $S_f = (c \oplus \mathbb{F}_2^8 \cdot M) \wr T_{\delta_0} \wr T_{\delta_0}$, where T_{δ_0} is the truth table of the function $\delta_0(x)$ viewed as a function on $\mathbb{F}_2^8$. That is, $\delta_0(x,y) = \delta_0(x) \in \mathscr{B}_8$. Then, $f_i \in \mathcal{B}_{10}$ defined via S_{f_i} and g, using Theorem 7.2.12, are pairwise disjoint spectra functions, where $S_{f_i} = S_f \oplus q_i$ and $q_i \in Q = \{\mathbf{0}_8\} \times \mathbb{F}_2^2$. In other words, $\mathfrak{f} = (f_0, f_1, f_2, f_3) \in \mathcal{B}_{12}$ is a bent function and can be viewed as a concatenation of four semi-bent functions. Furthermore, using our algorithm in Section 7.2.1, we have confirmed that $\mathfrak{f}$ lies outside $\mathcal{M}^\#$. The ANF of $\mathfrak{f}$ is given by (9.4) in Appendix.

The following remarks are important with respect to the cardinality of bent functions outside $\mathcal{M}^\#$ or the presence linear structures of the constituent semi-bent functions.

Remark 7.2.18. Notice that the number of possibilities of selecting S_{f_i} (which is a binary matrix of size $2^n \times (n+2)$) is quite large. We have 2^n possible choices for $c \in \mathbb{F}_2^n$ and $\prod_{k=0}^{n}(2^n - 2^k)$ choices for $M \in GL(n, \mathbb{F}_2)$. Thus, for fixed Boolean functions $t_1, t_2 \in \mathcal{B}_n$, we have $2^n \prod_{k=0}^{n}(2^n - 2^k)$ choices for S_f. For example, for $n = 8$ this number equals $\approx 2^{70.2}$.

Remark 7.2.19. The existence of linear structures in the semi-bent functions f_i, used in Theorem 7.2.15 to specify $\mathfrak{f}$, is of no importance when determining whether $\mathfrak{f} \notin \mathcal{M}^\#$. We have confirmed this, using our algorithm from Section 7.2.1, by verifying that the resulting bent functions are always outside $\mathcal{M}^\#$ provided that the bent function g used to define the dual of f_i (by means of (7.14)) is outside $\mathcal{M}^\#$. It is completely irrelevant whether these semi-bent functions possess linear structures (having affine supports S_{f_i}) or not.

7.2.5 Four bent decomposition in terms of 5-valued spectra functions

To specify 5-valued spectra Boolean functions, the authors in [39] provided a sufficient and necessary condition that the Walsh spectra of f_i (corresponding to two different amplitudes) must satisfy, see Section 7.1.1. The notion of totally disjoint spectra functions was also introduced in [39], which can be regarded as a sufficient condition so that

the Walsh spectrum specified by (7.1) is a valid spectrum of a Boolean function.

Definition 7.2.20. [39, Definition 4.1] For two disjoint sets $S_f^{[1]}, S_f^{[2]} \subset \mathbb{F}_2^n$, with $\#S_f^{[1]} + \#S_f^{[2]} = 2^{\lambda_1} + 2^{\lambda_2} < 2^n$, we say that the dual functions $f_{[1]}^* : S_f^{[1]} \to \mathbb{F}_2$ and $f_{[2]}^* : S_f^{[2]} \to \mathbb{F}_2$ (in terms of (7.1)) are *totally disjoint spectra functions* if it holds that

$$X_1(u)X_2(u) = 0 \quad \text{and} \quad |X_1(u)| + |X_2(u)| > 0,$$

for all $u \in \mathbb{F}_2^n$, where $X_i(u) = \sum_{\omega \in S_f^{[i]}} (-1)^{f_{[i]}^*(\omega) \oplus u \cdot \omega}$, for $i = 1, 2$.

Remark 7.2.21. Note that the second condition implies the nonexistence of a vector $u \in \mathbb{F}_2^n$ for which $X_1(u) = X_2(u) = 0$. Without this condition, the notion of totally disjoint spectra coincides with non-overlap disjoint spectra functions in [84].

Furthermore, a generic method of specifying totally disjoint spectra functions was also given in [39].

Construction 7.2.22. [39] Let n, m and k be even with $n = m + k$. Let $h \in \mathcal{B}_m$ and $g \in \mathcal{B}_k$ be two bent functions. Let H be any subspace of $\mathbb{F}_2^m$ of co-dimension 1, and let $\overline{H} = \mathbb{F}_2^m \backslash H$. Let also $E_1 = \mathbb{F}_2^k \times H$ and $E_2 = \{\mathbf{0}_k\} \times \overline{H}$. The Walsh spectrum of $f \in \mathcal{B}_n$, with $(\alpha, \beta) \in \mathbb{F}_2^k \times \mathbb{F}_2^m$, can be constructed as follows:

$$W_f(\alpha, \beta) = \begin{cases} (-1)^{g(\alpha) \oplus h(\beta)} \cdot 2^{n/2}, & (\alpha, \beta) \in E_1 \\ (-1)^{h(\beta)} \cdot 2^{m/2+k}, & (\alpha, \beta) \in E_2 \\ 0, & \textit{otherwise.} \end{cases} \tag{7.17}$$

Then, W_f is a valid spectrum of a Boolean function $f \in \mathcal{B}_n$. Let now

$$\begin{aligned} f_1(\alpha, \beta) &= g(\alpha) \oplus h(\beta), \quad (\alpha, \beta) \in E_1 \\ f_2(\alpha, \beta) &= h(\beta), \quad (\alpha, \beta) \in E_2. \end{aligned}$$

Then, $f_1 : E_1 \to \mathbb{F}_2$ and $f_2 : E_2 \to \mathbb{F}_2$ are totally disjoint spectra functions.

Remark 7.2.23. Notice that the sets E_1 and E_2 in Construction 7.2.22 can be defined similarly using any element $\mathbf{v} \in \mathbb{F}_2^k$ instead of $\mathbf{0}_k$, so that $E_2 = \{\mathbf{v}\} \times \overline{H}$ and $E_1 = \mathbb{F}_2^k \times H$ remains the same. Then, E_1 and E_2 are clearly disjoint.

Now, we need to specify a quadruple of 5-valued spectra functions in $\mathcal{B}_{n-2}$ by means of Construction 7.2.22, which additionally satisfies the condition given by item *iii*) of Theorem 7.1.1. More precisely:

a The sets $S_{f_i}^{[1]} = \{\vartheta \in \mathbb{F}_2^{n-2} : |W_{f_i}(\vartheta)| = 2^{\frac{n}{2}}\}$ $(i \in [1, 4])$ are pairwise disjoint;

b All $S_{f_i}^{[2]} = \{\vartheta \in \mathbb{F}_2^{n-2} : |W_{f_i}(\vartheta)| = 2^{\frac{n-2}{2}}\}$ are equal ($i \in [1,4]$), and for $f_{[2],i}^* : S_{f_i}^{[2]} \to \mathbb{F}_2$ it holds that $f_{[2],1}^* \oplus f_{[2],2}^* \oplus f_{[2],3}^* \oplus f_{[2],4}^* = 1$.

When $k = 2$, Construction 7.2.22 can generate suitable quadruples of 5-valued spectra functions (which are individually totally disjoint spectra functions) as shown below. Notice that the subspaces $S_{f_i}^{[1]}$ will correspond to $E_2^{(i)}$ and $S_{f_i}^{[2]}$ to $E_1^{(i)}$ in Theorem 7.2.24.

Theorem 7.2.24. *Let $n = m + 2$ be even so that m is also even. Let $h \in \mathcal{B}_m$ and $g \in \mathcal{B}_k = \mathcal{B}_2$ be two bent functions. Let H be any subspace of $\mathbb{F}_2^m$ of co-dimension 1, and let $\overline{H} = \mathbb{F}_2^m \backslash H$. Let also $E_1^{(i)} = \mathbb{F}_2^2 \times H$ and $E_2^{(i)} = \{c^{(i)}\} \times \overline{H}$, for $i = 1, \ldots, 4$, where $c^{(i)} \in \mathbb{F}_2^2$ are ordered lexicographically so that $c^{(i)} \neq c^{(j)}$ for $1 \leq i \neq j \leq 4$. We specify the spectra of $f_i \in \mathcal{B}_n$ as follows:*

$$W_{f_i}(\alpha,\beta) = \begin{cases} (-1)^{g(\alpha)\oplus h(\beta)\oplus d} \cdot 2^{n/2}, & (\alpha,\beta) \in E_1^{(i)} \\ (-1)^{h(\beta)} \cdot 2^{\frac{n-2}{2}+2}, & (\alpha,\beta) \in E_2^{(i)} \\ 0, & \textit{otherwise}, \end{cases} \tag{7.18}$$

where $d = 1$ if $i = 4$, otherwise $d = 0$. Then, the function $f \in \mathscr{B}_{n+2}$ given as the concatenation $f = f_1||f_2||f_3||f_4$ is a bent function.

Proof. The functions $f_i \in \mathscr{B}_n$, specified by (7.18), are clearly 5-valued spectra functions. We need to verify that their spectra corresponds to Boolean functions. By Construction 7.2.22, corresponding to the definition of $E_1^{(1)}$ and $E_2^{(1)}$ using $\mathbf{c}^{(1)} = (0,0)$, this is true for f_1. Due to the definition of $E_1^{(i)}$ and $E_2^{(i)}$ and Remark 7.2.23, the same is true for any f_i which are all Boolean 5-valued spectra functions. For instance, using $\mathbf{c}^{(2)} = (0,1)$ to define f_2, the condition that $E_1^{(1)} = E_1^{(2)}$ is clearly true and furthermore $(0,0) \times \overline{H} \cap (0,1) \times \overline{H} = \emptyset$, that is $E_2^{(1)} \cap E_2^{(2)} = \emptyset$.

Now, the condition for a valid 4-decomposition into 5-valued spectra functions is given by *iii*) in Theorem 7.1.1. The supports $E_2^{(i)}$ are clearly disjoint by their definition, whereas $E_1^{(i)}$ are defined on the same subspace of $\mathbb{F}_2^n$. The last condition that the bent duals defined on $E_1^{(i)}$ satisfy $f_{[2],1}^* \oplus f_{[2],2}^* \oplus f_{[2],3}^* \oplus f_{[2],4}^* = 1$ follows from the specification of the spectra on $E_1^{(i)}$, using the fact that $d = 1$ only when $i = 4$. □

Remark 7.2.25. Since $d = 1$ when $i = 4$, the complement of the dual is used for the fourth constituent function f_4. This ensures that the bent duals satisfy $f_{[2],1}^* \oplus f_{[2],2}^* \oplus f_{[2],3}^* \oplus f_{[2],4}^* = 1$. Nevertheless, this is not the only choice and the bent duals can be specified in other ways (through the complement operation) as long as their sum equals 1.

The following examples illustrate the details of this construction and the possibility of getting bent functions outside $\mathcal{M}^{\#}$. Notice that the dual h used to specify f is not necessarily in $\mathcal{M}^{\#}$.

Example 7.2.26. Let $n = 8$ and let $h \in \mathcal{B}_6, g \in \mathcal{B}_2$ be defined by $h(x_0, \ldots, x_5) = x_0x_1 \oplus x_2x_3 \oplus x_4x_5 \in \mathcal{M}$ and $g(x_0, x_1) = x_0x_1$. Using the mathematical software Sage, we constructed the functions $f^{(i)} \in \mathcal{B}_8$ for $i = 1, \ldots, 4$ defined by (7.18) and their ANF's are given as follows:

$$\begin{aligned}
f_1(x_0, \ldots, x_7) &= x_0x_1 \oplus x_2x_3 \oplus x_4x_5 \oplus x_4x_6x_7 \oplus x_6x_7,\\
f_2(x_0, \ldots, x_7) &= x_0x_1 \oplus x_2x_3 \oplus x_4x_5 \oplus x_4x_6x_7 \oplus x_4x_6 \oplus x_6x_7,\\
f_3(x_0, \ldots, x_7) &= x_0x_1 \oplus x_2x_3 \oplus x_4x_5 \oplus x_4x_6x_7 \oplus x_4x_7 \oplus x_6x_7,\\
f_4(x_0, \ldots, x_7) &= x_0x_1 \oplus x_2x_3 \oplus x_4x_5 \oplus x_4x_6x_7 \oplus x_4x_6 \oplus x_4x_7 \oplus x_4\\
&\quad \oplus x_6x_7 \oplus 1
\end{aligned}$$

Then, the function $f \in \mathcal{B}_{10}$ given as the concatenation $f = f_1||f_2||f_3||f_4$ is a cubic bent function defined by $f(x_0, \ldots, x_9) = x_0x_1 \oplus x_2x_3 \oplus x_4x_5 \oplus x_4x_6x_7 \oplus x_4x_6x_8 \oplus x_4x_7x_9 \oplus x_4x_8x_9 \oplus x_6x_7 \oplus x_8x_9$. Using our algorithm in Section 7.2.1, we could verify that $f \in \mathcal{M}^{\#}$.

On the other hand, the following two examples illustrate that selecting the dual h to be outside $\mathcal{M}^{\#}$, the resulting bent functions (constructed using Theorem 7.2.24) are outside $\mathcal{M}^{\#}$.

Example 7.2.27. Let $h \in \mathcal{B}_8$ defined by $h(x, y) = Tr_1^4(xy^7) + \delta_0(x)$, $x, y \in \mathbb{F}_{2^4}$, be a bent function in the class $\mathcal{D}_0 \setminus \mathcal{M}^{\#}$ [17, 88], and let $g \in \mathcal{B}_2$ be defined by $g(x_0, x_1) = x_0x_1$. Using Sage we constructed the functions $f_i \in \mathcal{B}_{10}$ for $i = 1, \ldots, 4$ defined by (7.18). Then, the function $f \in \mathcal{B}_{12}$ given as $f = f_1||f_2||f_3||f_4$ is a bent function of algebraic degree 5. This time the function f, whose ANF is given by (9.2) in the appendix, is outside $\mathcal{M}^{\#}$.

Example 7.2.28. Let $n = 10$ and $h \in \mathcal{B}_8, g \in \mathcal{B}_2$ be bent functions, where $g(x_0, x_1) = x_0x_1$. The function $h \in \mathcal{B}_8$, whose ANF is given by (9.1) in Appendix, lies in $\mathcal{PS}^{\#}$ and is outside $\mathcal{M}^{\#}$. Using Sage, we constructed the functions $f_i \in \mathcal{B}_{10}$ for $i = 1, \ldots, 4$ defined by (7.18). Then, the function $f \in \mathcal{B}_{12}$ given as $f = f_1||f_2||f_3||f_4$ is a bent function of algebraic degree 5. Again, it could be confirmed that f is outside $\mathcal{M}^{\#}$ (its ANF is given by (9.3) in Appendix).

The above examples indicate that the conclusions (related to the dual) given in Section 7.2.2 seem to be applicable in this case as well. More precisely, the class belongingness of f in Theorem 7.2.24 is strongly related to the choice of the dual bent functions.

Theorem 7.2.29. *Let $f \in \mathscr{B}_{n+2}$ be constructed by means of Theorem 7.2.24, thus $f = f_1||f_2||f_3||f_4$ where $f_i \in \mathscr{B}_n$. If the dual bent function $h \in \mathscr{B}_{n-2}$ in Theorem 7.2.24 is outside $\mathcal{M}^{\#}$, then f is outside $\mathcal{M}^{\#}$.*

Proof. By Remark 7.2.1, f is outside $\mathcal{M}^{\#}$ if and only if its dual f^* is outside $\mathcal{M}^{\#}$. Hence, it is enough to show that f^* is outside $\mathcal{M}^{\#}$. The "duals" of the restrictions f_i are actually given by (7.18). By the definition of f^*, we have that $(-1)^{f^*(u)} = 2^{-\frac{n+2}{2}} W_f(u)$ for any $u \in \mathbb{F}_2^{n+2}$, since $f \in \mathscr{B}_{n+2}$. For convenience, we write $u = (\alpha, \beta, \gamma) \in \mathbb{F}_2^2 \times \mathbb{F}_2^m \times \mathbb{F}_2^2$ with $n = m + 2$ as used in Theorem 7.2.24. We notice that in general, using that $x = (x', x_{n+1}, x_{n+2}) \in \mathbb{F}_2^n \times \mathbb{F}_2 \times \mathbb{F}_2$, we have

$$\begin{aligned}
&W_f(\alpha, \beta, \gamma) \\
&= \sum_{x \in \mathbb{F}_2^n \times \mathbb{F}_2^2} (-1)^{f(x)+u\cdot x} \\
&= \sum_{x \in \mathbb{F}_2^n \times (0,0)} (-1)^{f(x',0,0)+(\alpha,\beta)\cdot x'} + \sum_{x \in \mathbb{F}_2^n \times (0,1)} (-1)^{f(x',0,1)+(\alpha,\beta)\cdot x'+\gamma_2} \\
&+ \sum_{x \in \mathbb{F}_2^n \times (1,0)} (-1)^{f(x',1,0)+(\alpha,\beta)\cdot x'+\gamma_1} + \sum_{x \in \mathbb{F}_2^n \times (1,1)} (-1)^{f(x',1,1)+(\alpha,\beta)\cdot x'+\gamma_1+\gamma_2} \\
&= W_{f_1}(\alpha, \beta) + (-1)^{\gamma_2} W_{f_2}(\alpha, \beta) + (-1)^{\gamma_1} W_{f_3}(\alpha, \beta) + (-1)^{\gamma_1+\gamma_2} W_{f_4}(\alpha, \beta) \\
&\qquad . \qquad (7.19)
\end{aligned}$$

Hence, for any fixed $\gamma \in \mathbb{F}_2^2$, we can compute the value of $W_f(\alpha, \beta, \gamma)$ by using the Walsh spectra of the constituent functions f_i.

We first notice that $W_{f_i}(\alpha, \beta) = (-1)^{h(\beta)} \cdot 2^{\frac{n-2}{2}+2}$ when $(\alpha, \beta) \in E_2^{(i)}$, and furthermore by construction the sets $E_2^{(i)}$ are mutually disjoint for $i = 1, \ldots, 4$. Hence, if for instance $(\alpha, \beta) \in E_2^{(1)}$ then $W_{f_1}(\alpha, \beta) = (-1)^{h(\beta)} \cdot 2^{\frac{n-2}{2}+2}$ and $W_{f_i}(\alpha, \beta) = 0$ for $2 \leq i \leq 4$, which implies that $W_f(\alpha, \beta, \gamma) = (-1)^{h(\beta)} \cdot 2^{\frac{n}{2}+1}$ when $(\alpha, \beta) \in E_2^{(1)}$. The other cases when $(\alpha, \beta) \in E_2^{(i)}$ for $i \neq 1$ are similar.

Now, considering the case $(\alpha, \beta) \in E_1^{(i)}$, we first notice that $E_1 := E_1^{(1)} = \cdots = E_1^{(4)}$ (by construction), where $E_1 = \mathbb{F}_2^2 \times H$ as in Theorem 7.2.24. In addition, $W_{f_i}(\alpha, \beta) = (-1)^{g(\alpha)\oplus h(\beta)+d} \cdot 2^{n/2}$, where $d = 1$ when $i = 4$ only. This also implies that $W_{f_1}(\alpha, \beta) = W_{f_2}(\alpha, \beta) = W_{f_3}(\alpha, \beta) = -W_{f_4}(\alpha, \beta)$ when $(\alpha, \beta) \in E_1$. Therefore, using (7.19), we have

$$\begin{aligned}
W_f(\alpha, \beta, 0, 0) &= W_{f_1}(\alpha, \beta) + W_{f_2}(\alpha, \beta) + W_{f_3}(\alpha, \beta) - W_{f_4}(\alpha, \beta) \\
&= 2W_{f_1}(\alpha, \beta) \\
W_f(\alpha, \beta, 0, 1) &= W_{f_1}(\alpha, \beta) - W_{f_2}(\alpha, \beta) + W_{f_3}(\alpha, \beta) + W_{f_4}(\alpha, \beta) \\
&= 2W_{f_1}(\alpha, \beta) \\
W_f(\alpha, \beta, 1, 0) &= W_{f_1}(\alpha, \beta) + W_{f_2}(\alpha, \beta) - W_{f_3}(\alpha, \beta) + W_{f_4}(\alpha, \beta) \\
&= 2W_{f_1}(\alpha, \beta) \\
W_f(\alpha, \beta, 1, 1) &= W_{f_1}(\alpha, \beta) - W_{f_2}(\alpha, \beta) - W_{f_3}(\alpha, \beta) - W_{f_4}(\alpha, \beta)
\end{aligned}$$

$$= -2W_{f_1}(\alpha, \beta).$$

Hence, $W_f(\alpha, \beta, \gamma_1, \gamma_2) = 2 \cdot 2^{n/2}(-1)^{g(\alpha)\oplus h(\beta)+\gamma_1\gamma_2}$ when $(\alpha, \beta) \in E_1$, where $g(\alpha) \oplus h(\beta) + \gamma_1\gamma_2$ falls into the framework of Theorem 7.2.2 and additionally Remark 7.2.1 applies. Notice that the case $(\alpha, \beta) \notin E_1$ and at the same time having $W_{f_i}(\alpha, \beta) = 0$ is already covered above since then $(\alpha, \beta) \in E_2^{(j)}$ for some $j \neq i$. This is a consequence of the fact that $E_1 \cup (\cup_{i=1}^4 E_2^{(i)}) = \mathbb{F}_2^n$.

To summarize, the dual f^* is equal to $g(\alpha) \oplus h(\beta) + \gamma_1\gamma_2$ when f^* is restricted to the subspace $(\alpha, \beta, \gamma) \in E_1 \times \mathbb{F}_2^2$ and to $h(\beta)$ when f^* is restricted to the complement of $E_1 \times \mathbb{F}_2^2$. Notice that g is a 2-variable quadratic bent function, thus $g(\alpha_1, \alpha_2) = \alpha_1\alpha_2$. Therefore, using the assumption that $h \notin \mathcal{M}^{\#}$, Remark 7.2.1 and Corollary 7.2.3 imply that $f^* \notin \mathcal{M}^{\#}$ and hence $f \notin \mathcal{M}^{\#}$.

□

Remark 7.2.30. The condition on the dual bent function $h \in \mathscr{B}_{n-2}$ is strictly sufficient and not necessary. There exist bent functions $\{f\}$ in eight variables, represented as $f = f_1||f_2||f_3||f_4$ where f_i are 5-valued spectra functions, that are outside $\mathcal{M}^{\#}$. Since in this case the dual bent function h is defined on $\mathbb{F}_2^4$ it apparently belongs to $\mathcal{M}$.

7.3 5-valued spectra functions from the generalized $\mathcal{M}$ class

Another method of specifying 5-valued spectra functions, also given in [39], uses the generalized Maiorana-McFarland class (GMM) of Boolean functions. For convenience and ease of notation, we use the variable set $x_0, \ldots, x_{n-1}$ instead of $x_1, \ldots, x_n$ for functions on $\mathbb{F}_2^n$.

Theorem 7.3.1. *[39] Let $E_0 \subset \mathbb{F}_2^s$ with $1 \leq s \leq \lfloor n/2 \rfloor$. Let $E_1 = \overline{E_0} \times \mathbb{F}_2^t$, where $\overline{E_0} = \mathbb{F}_2^s \backslash E_0$ and $0 \leq t \leq \lfloor n/2 \rfloor$. Let ϕ_0 be an injective mapping from E_0 to $\mathbb{F}_2^{n-s}$, and ϕ_1 be an injective mapping from E_1 to $\mathbb{F}_2^{n-s-t}$. Let $X = (x_0, \ldots, x_{n-1}) \in \mathbb{F}_2^n$ and $X_{(i,j)} = (x_i, \ldots, x_j) \in \mathbb{F}_2^{j-i+1}$. Let $f \in \mathcal{B}_n$ be defined as follows:*

$$f(X) = \begin{cases} \phi_0(X_{(0,s-1)}) \cdot X_{(s,n-1)}, & if\ X_{(0,s-1)} \in E_0 \\ \phi_1(X_{(0,s+t-1)}) \cdot X_{(s+t,n-1)}, & if\ X_{(0,s+t-1)} \in E_1. \end{cases}$$

Let

$$T_0 = \{\phi_0(\eta) \mid \eta \in E_0\},$$

and

$$T_1 = \{\phi_1(\theta) \mid \theta \in E_1\}.$$

Then, we have

a) $W_f(\omega) \in \{0, \pm 2^{n-s}, \pm 2^{n-s-t}\}$ *if* $t \neq 0$ *and* $T_0 \subset \mathbb{F}_2^t \times \overline{T_1}$, *where* $\overline{T_1} = \mathbb{F}_2^{n-s-t} \backslash T_1$;

b) $W_f(\omega) \in \{0, \pm 2^{n-s}, \pm 2^{n-s+1}\}$ *if* $t = 0$, $T_0 \cap T_1 \neq \emptyset$ *and* $T_0 \neq T_1$.

Example 7.3.2. Let $n = 8, s = 3$ and $t = 1$. Now, we employ Theorem 7.3.1 to construct 5-valued spectra functions $f^{(1)}, \ldots, f^{(4)}$ that satisfy Theorem 7.1.1. The resulting function $f = f^{(1)}||f^{(2)}||f^{(3)}||f^{(4)} \in \mathcal{B}_{10}$ is then bent. Let $\mathbb{F}_2^n = \{v_0^{(n)}, \ldots, v_{2^n-1}^{(n)}\}$ denote the lexicographically ordered n-dimensional vector space over $\mathbb{F}_2$. Furthermore, we note that all sets defined below are also lexicographically ordered. We define $E_0 = \{e_0^{(0)}, e_1^{(0)}, e_2^{(0)}\}$, where $e_i^{(0)} = v_i^{(3)} \in \mathbb{F}_2^3$ for $i = 0, 1, 2$, and $E_1 = \overline{E_0} \times \mathbb{F}_2 = \{e_0^{(1)}, e_1^{(1)}, \ldots, e_9^{(1)}\} \subset \mathbb{F}_2^4$, where $\overline{E_0} = \mathbb{F}_2^3 \setminus E_0$. Let $\phi_1 : E_1 \to \mathbb{F}_2^4$ be defined by

$$\phi_1(e_i^{(1)}) = v_i^{(4)},$$

for $i = 0, \ldots, 9$ Let $T_1 = \{\phi_1(\theta) : \theta \in E_1\}$ and $\overline{T_1} = \mathbb{F}_2^4 \setminus T_1$, where clearly $|\overline{T_1}| = 6$. Let $\Gamma = \mathbb{F}_2 \times \overline{T_1} = \{\gamma_0, \ldots, \gamma_{11}\} \subset \mathbb{F}_2 \times \mathbb{F}_2^4 = \mathbb{F}_2^5$ and let $\phi_0^{(j)} : E_0 \to \mathbb{F}_2^5$ be defined by

$$\phi_0^{(j)}(e_i^{(0)}) = \gamma_{i+3j},\ e_i^{(0)} \in E_0,$$

for $j = 1, \ldots, 4$.

If $T_0^{(j)} = \{\phi_0^{(j)}(\eta) : \eta \in E_0\}$, then $T_0^{(j)} \subset \mathbb{F}_2 \times \overline{T_1}$ (as required in Theorem 7.3.1-(a)), for $j = 1, \ldots, 4$. Now let $X = (x_0, \ldots, x_7) \in \mathbb{F}_2^8$ and $X_{(i,j)} = (x_i, \ldots, x_j) \in \mathbb{F}_2^{j-i+1}$. For $j = 1, 2, 3, 4$, $f^{(j)} \in \mathcal{B}_8$ is defined as follows:

$$f^{(j)}(X) = \begin{cases} \phi_0^{(j)}(X_{(0,2)}) \cdot X_{(3,7)} + \delta_1(j), & if\ X_{(0,2)} \in E_0 \\ \phi_1(X_{(0,3)}) \cdot X_{(4,7)} + \delta_1(j), & if\ X_{(0,3)} \in E_1, \end{cases}$$

where $\delta_1(j) = 1$ for $j = 1$ and 0 otherwise. Let $S_1^{(j)} = \{x \in \mathbb{F}_2^8 : |W_{f^{(j)}}(x)| = 2^5\}$ and $S_2^{(j)} = \{x \in \mathbb{F}_2^8 : |W_{f^{(j)}}(x)| = 2^4\}$. Using Sage we could verify that all $S_1^{(j)}$ are pairwise disjoint and all $S_2^{(j)}$ are equal. Furthermore, by the construction, $f^*_{[2],1} \oplus \ldots \oplus f^*_{[2],4} = 1$. Hence, by Theorem 7.1.1, the function $f = f^{(1)}||f^{(2)}||f^{(3)}||f^{(4)} \in \mathcal{B}_{10}$ of algebraic degree 5 is bent, and its ANF is defined by:

$$f(x_0, \ldots, x_9) = x_0x_1x_2x_3x_4 \oplus x_0x_1x_2x_3x_9 \oplus x_0x_1x_2x_4x_8 \oplus x_0x_1x_2x_4 \oplus x_0x_1x_2x_6 \oplus x_0x_1x_3x_4 \oplus x_0x_1x_3x_9 \oplus x_0x_1x_4x_8 \oplus x_0x_1x_4 \oplus x_0x_1x_6 \oplus x_0x_1x_7 \oplus x_0x_2x_4 \oplus x_0x_2x_5x_8 \oplus x_0x_2x_5 \oplus x_0x_2x_6 \oplus x_0x_4 \oplus x_0x_5x_8 \oplus x_1x_2x_5 \oplus x_1x_2x_6x_8 \oplus x_1x_5 \oplus x_1x_6x_8 \oplus x_1x_6 \oplus x_2x_3x_4 \oplus x_2x_3x_9 \oplus x_2x_4x_8 \oplus x_2x_5x_8 \oplus x_2x_6x_8 \oplus x_2x_7 \oplus x_3x_9 \oplus x_4x_8 \oplus x_5x_8 \oplus x_5 \oplus x_6x_8 \oplus x_7 \oplus x_8x_9 \oplus x_8 \oplus x_9 \oplus 1.$$

Nevertheless, using our algorithm in Section 7.2.1 implemented in Sage, we could confirm that $f \in \mathcal{M}^{\#}$.

As a generalization of the previous example, we give the following result. We assume that all sets are ordered lexicographically and we denote $\mathbb{F}_2^n = \{v_0^{(n)}, v_1^{(n)}, \ldots, v_{2^n-1}^{(n)}\}$.

Remark 7.3.3. We assume that all sets defined in Theorem 7.3.4 are ordered lexicographically, and with $\mathbb{F}_2^k = \{v_0^{(k)}, v_1^{(k)}, \ldots, v_{2^k-1}^{(k)}\}$ (for suitable k) we will denote the elements of the lexicographically ordered k-dimensional vector space over $\mathbb{F}_2$.

Theorem 7.3.4. *Let $n = 2m \geq 8$, $E_0 = \{e_0^{(0)}, \ldots, e_{\tau-1}^{(0)}\} \subset \mathbb{F}_2^{m-1}$ where $\tau < 2^s - 1$ and $4\tau \leq 2^{m+1}$, and $E_1 = \overline{E_0} \times \mathbb{F}_2 = \{e_0^{(1)}, \ldots, e_\lambda^{(1)}\} \subset \mathbb{F}_2^m$, where $\lambda = 2 \cdot (2^{m-1} - \tau) - 1$ and $\overline{E_0} = \mathbb{F}_2^{m-1} \setminus E_0$. Let $\phi_1 : E_1 \to \mathbb{F}_2^m$ be an injective mapping defined by*

$$\phi_1(e_i^{(1)}) = v_i^{(m)}, \ e_i^{(1)} \in E_1,$$

for $i = 0, 1, \ldots, \lambda$, whose image set is denoted by $T_1 = \{\phi_1(\theta) : \theta \in E_1\}$. Now, denoting $\Gamma = \mathbb{F}_2 \times (\mathbb{F}_2^m \setminus T_1) = \{\gamma_0, \gamma_1, \ldots, \gamma_{4\tau-1}\}$, let $\phi_0^{(j)} : E_0 \to \Gamma \subset \mathbb{F}_2^{m+1}$, for $j = 1, \ldots, 4$, be injective mappings defined by

$$\phi_0^{(j)}(e_i^{(0)}) = \gamma_{i+\tau(j-1)}, \ e_i^{(0)} \in E_0.$$

Let $X = (x_0, \ldots, x_{n-1}) \in \mathbb{F}_2^n$ and $X_{(i,j)} = (x_i, \ldots, x_j) \in \mathbb{F}_2^{j-i+1}$. For $j = 1, \ldots, 4$, $f^{(j)} \in \mathcal{B}_n$ is defined as follows:

$$f^{(j)}(X) = \delta_1(j) \oplus \begin{cases} \phi_0^{(j)}(X_{(0,m-2)}) \cdot X_{(m-1,n-1)}, & if \ X_{(0,m-2)} \in E_0 \\ \phi_1(X_{(0,m-1)}) \cdot X_{(m,n-1)}, & if \ X_{(0,m-1)} \in E_1, \end{cases}$$

where $\delta_1(j) = 1$ for $j = 1$ and 0 otherwise. Then, the function $f \in \mathcal{B}_{n+2}$ given as the concatenation $f = f^{(1)}||f^{(2)}||f^{(3)}||f^{(4)}$ is a bent function.

Proof. Firstly, we note that $W_{f^{(j)}}(x) \in \{0, \pm 2^m, \pm 2^{m+1}\}$ by Theorem 7.3.1, for $j = 1, \ldots, 4$ (with $s = m - 1$ and $t = 1$). It remains to show that these functions satisfy the conditions of Theorem 7.1.1-(iii).

Let $S_{f^{(j)}}^{[1]} = \{x \in \mathbb{F}_2^n : |W_{f^{(j)}}(x)| = 2^{m+1}\}$ and $S_{f^{(j)}}^{[2]} = \{x \in \mathbb{F}_2^n : |W_{f^{(j)}}(x)| = 2^m\}$, for $j = 1, \ldots, 4$. The cardinality of Γ can be computed as

$$\begin{aligned} |\Gamma| &= 2 \cdot |\mathbb{F}_2^m \setminus T_1| = 2(2^m - |E_1|) = 2 \cdot (2^m - 2(2^{m-1} - \tau)) \\ &= 2^{m+1} - 2^{m+1} + 4\tau = 4\tau. \end{aligned}$$

Because $|\Gamma| = 4\tau \leq 2^{m+1}$ and $|\phi_0^{(j)}(E_0)| = \tau$, it is easy to see that $\phi_0^{(j)}$ splits Γ into 4 disjoint subsets, that is, $\Gamma = \bigcup_{j=1}^4 \phi_0^{(j)}(E_0)$ and

$\phi_0^{(j)}(E_0) \cap \phi_0^{(j')}(E_0) = \emptyset$ for $j \neq j'$. Consequently, the sets $S^{[1]}_{f^{(j)}}$ are pairwise disjoint for $j = 1, \ldots, 4$. As the function ϕ_1 is the same for all $f^{(j)}$, it follows that all sets $S^{[2]}_{f^{(j)}}$ are equal. The condition that the bent duals defined on $S^{[2]}_{f^{(j)}}$ satisfy $f^*_{[2],1} \oplus f^*_{[2],2} \oplus f^*_{[2],3} \oplus f^*_{[2],4} = 1$, follows from the fact that $\delta_1(j) = 1$ only for $j = 1$. This follows from the fact that $|W_f(x)| = 2^m$ is determined by the value of $\phi_1(X_{(0,m-1)}) \cdot X_{(m,n-1)}$ (cf. proof of [39, Theorem V.6]) and consequently the values of $f^*_{[2],j}$ are the same except for $j = 1$, where we additionally add the constant 1. Thus, the conditions given in item *iii*) of Theorem 7.1.1 are satisfied and $f = f^{(1)}||f^{(2)}||f^{(3)}||f^{(4)} \in \mathscr{B}_{n+2}$ is a bent function. □

Remark 7.3.5. The above statement also holds if E_0 is a collection of arbitrary τ elements in $\mathbb{F}_2^{m-1}$. However, (partial) computer simulations indicate that this approach only generates bent functions inside the $\mathcal{M}^\#$ class, regardless of the choice of E_0.

Open problem 7.3.6. Prove or disprove that the bent functions constructed using Theorem 7.3.4 always belong to $\mathcal{M}^\#$ regardless of the choice of E_0.

Chapter 8

Applications of the indirect sum in the design of several special classes of bent functions outside $\mathcal{M}^{\#}$

Two well-known secondary constructions of bent functions are the direct and indirect sum methods. We show that the direct sum, under more relaxed conditions compared to those in [71], can generate bent functions provably outside the completed Maiorana-McFarland class ($\mathcal{M}^{\#}$). We also show that the indirect sum method, though imposing certain conditions on the initial bent functions, can be employed in the design of bent functions outside $\mathcal{M}^{\#}$. Furthermore, applying this method to suitably chosen bent functions we construct several generic classes of homogenous cubic bent functions (considered as a difficult problem) that might posses additional properties (namely without affine derivatives and/or outside $\mathcal{M}^{\#}$). Our results significantly improve upon the best known instances of this type of bent functions given by Polujan and Pott [71], and additionally we solve an open problem in [71, Open Problem 5.1]. More precisely, we show that one class of our homogenous cubic bent functions is non-decomposable (inseparable) so that h under a non-singular transform B cannot be represented as $h(xB) = f(y) \oplus g(z)$. Finally, we provide a generic class of vectorial bent functions strongly outside $\mathcal{M}^{\#}$ of relatively large output dimensions, which is generally considered as a difficult task.

8.1 Direct and indirect sum methods

The direct sum method is probably one of the best known design rationales when constructing new bent functions form the known ones. Namely, provided that both f and g are bent functions on $\mathbb{F}_2^n$ and on $\mathbb{F}_2^m$ (both n and m are even), respectively, the function $h(x, y) = f(x) \oplus g(y)$ is also bent on $\mathbb{F}_2^{n+m}$. A special case of this approach arises when g is a quadratic bent function given in a canonical form

$g(y) = y_1y_2 \oplus \cdots \oplus y_{m-1}y_m$, which was recently considered in [65]. It was shown that in this particular case h is outside $\mathcal{M}^{\#}$ if and only if f is outside $\mathcal{M}^{\#}$. This motivates us to investigate other choices of g (not only quadratic canonical ones) in this context.

8.1.1 Specifying sufficient conditions for the direct sum method

In this section, we consider the conditions under which $h(x, y) = f(x) \oplus g(y)$ is outside $\mathcal{M}^{\#}$. Special cases of the direct sum constructions have been also addressed in Chapter 6 (cf. Theorem 7.2.2 and Corollary 7.2.3). Before we provide a more general statement of the above result, we provide an important observation useful in the analysis of the direct and indirect sum methods.

Proposition 8.1.1. *Let n be an even positive integer, and let E be a vector subspace of $\mathbb{F}_2^n$ with $\dim(E) \geq n/2 + 1$. Then, for every bent function $f \in \mathcal{B}_n$ and for every $x_0 \in \mathbb{F}_2^n$ there are $a, b \in E$ such that*

$$D_aD_bf(x)|_{x=x_0} \neq 0.$$

Proof. Assume that there is a bent function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ and $x_0 \in \mathbb{F}_2^n$ such that $D_aD_bf(x_0) = 0$, for every $a, b \in E$. We can assume that $x_0 = 0$ (otherwise we can take $f'(x) = f(x \oplus x_0)$), and that $f(0) = 0$ (otherwise we can take $f \oplus 1$). Then, from $D_aD_bf(0) = 0$ we have $f(0) \oplus f(a) = f(b) \oplus f(a \oplus b)$, i.e. $f(a \oplus b) = f(a) \oplus f(b)$ for every $a, b \in E$. This means that f is linear on E and so there is a linear function $L : \mathbb{F}_2^n \to \mathbb{F}_2$ that agrees with f on E. To see this, take a basis $e_1, \ldots, e_k$ of E, extend it to a basis $e_1, \ldots, e_n$ on $\mathbb{F}_2^n$, and define L as $L(\sum_{i=1}^n w_ie_i) = \sum_{i=1}^k w_if(e_i)$, for every $w_1, \ldots, w_n \in \mathbb{F}_2$. Then, L is linear and agrees with f on E. Let $l \in \mathbb{F}_2^n$ be such that $L(x) = l \cdot x$, for every $x \in \mathbb{F}_2^n$. Then, $f(x) \oplus l \cdot x = 0$ for every $x \in E$. By the Poisson summation formula [19, Corollary 1] we have:

$$\sum_{u \in v \oplus E^{\perp}} (-1)^{w \cdot u} \widehat{\varphi}(u) = |E^{\perp}|(-1)^{w \cdot v} \sum_{x \in w \oplus E} (-1)^{v \cdot x} \varphi(x),$$

for any pseudo-Boolean function φ on $\mathbb{F}_2^n$ where $\widehat{\varphi}(u) = \sum_{x \in \mathbb{F}_2^n} \varphi(x)(-1)^{u \cdot x}$ denotes the Fourier transform of φ at point $u \in \mathbb{F}_2^n$. Setting $w = 0, v = l$, $\varphi = (-1)^f$, and denoting by f^* the dual of f, we get:

$$\frac{1}{|E^{\perp}|} \sum_{u \in l \oplus E^{\perp}} 2^{n/2}(-1)^{f^*(u)} = \sum_{x \in E}(-1)^{f(x) \oplus l \cdot x} = \sum_{x \in E}(-1)^0 = 2^{\dim(E)}.$$

But $\sum_{u \in l \oplus E^{\perp}}(-1)^{f^*(u)} \leq |E^{\perp}|$, so we have $2^{\dim(E)} \leq 2^{n/2}$, and this is a contradiction because $\dim(E) \geq n/2 + 1$. □

We also recall a useful concept of relaxed $\mathcal{M}$-subspaces introduced by Polujan and Pott [71].

Definition 8.1.2. [71] A vector subspace $U \subseteq \mathbb{F}_2^n$ is called a relaxed $\mathcal{M}$-subspace of a Boolean function $f \in \mathcal{B}_n$, if for all $a, b \in U$ the second order derivatives $D_a D_b f$ are either constant zero or constant one functions. i.e., $D_a D_b f = 0$ or $D_a D_b f = 1$. We denote by $\mathcal{RMS}_r(f)$ the collection of all r-dimensional relaxed $\mathcal{M}$-subspaces of a Boolean function f and by $\mathcal{RMS}(f)$ the collection

$$\mathcal{RMS}(f) := \bigcup_{r=1}^{n} \mathcal{RMS}_r(f).$$

Definition 8.1.3. [71] For a Boolean function $f \in \mathcal{B}_n$ its relaxed linearity index r-ind(f) is defined by r-ind(f):$= \max_{U \in \mathcal{RMS}(f)} \dim(U)$.

Notice that for a quadratic Boolean function $f \in \mathcal{B}_n$ its relaxed linearity index equals r-ind(f)= n.

Lemma 8.1.4. *[71, Corollary 4.6] Let f and g be two bent function on $\mathbb{F}_2^n$ and $\mathbb{F}_2^m$, respectively. The function h, defined as $h(x, y) = f(x) \oplus g(y)$, is outside $\mathcal{M}^{\#}$ if r-ind$(f) < n/2$ and r-ind$(g) \leqslant m/2$.*

The following result further refines the above claim by dropping the condition that r-ind$(g) \leqslant m/2$.

Theorem 8.1.5. *Let f and g be two bent function on $\mathbb{F}_2^n$ and $\mathbb{F}_2^m$, respectively. The function h, defined as $h(x, y) = f(x) \oplus g(y)$, is outside $\mathcal{M}^{\#}$ if r-ind$(f) < n/2$.*

Proof. Let $a^{(1)}, a^{(2)} \in \mathbb{F}_2^n$ and $b^{(1)}, b^{(2)} \in \mathbb{F}_2^m$. We prove that h does not belong to $\mathcal{M}^{\#}$, by using Lemma 2.2.4. We need to show that there does not exist an $(\frac{n+m}{2})$-dimensional subspace V such that

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

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

$$D_{(a^{(1)}, b^{(1)})} D_{(a^{(2)}, b^{(2)})} h(x, y) = D_{a^{(1)}} D_{a^{(2)}} f(x) \oplus D_{b^{(1)}} D_{b^{(2)}} g(y). \tag{8.1}$$

Let V ba a $(\frac{n+m}{2})$-dimensional subspace of $\mathbb{F}_2^n \times \mathbb{F}_2^m$. There are two cases to be considered.

1. If $\dim(\{x|(x, y) \in V\}) \geqslant n/2$, we can select two $a^{(1)}, a^{(2)} \in \{x|(x, y) \in V\}$ such that

   $$D_{a^{(1)}} D_{a^{(2)}} f(x) \neq constant$$

   since r-ind$(f) < n/2$. Thus, we have

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

for any $b^{(1)}, b^{(2)} \in \{y|(x,y) \in V\}$ since $D_{a^{(1)}} D_{a^{(2)}} f(x)$ only depends on variables x.

2. If $\dim(\{x|(x,y) \in V\}) < n/2$, then we must have

$$\dim(\{y|(0_n,y) \in V\}) > m/2$$

since $\dim(V) = (n+m)/2$ (that is, $||V|| = 2^{(n+m)/2}$). From Proposition 8.1.1, we can select two vectors $b^{(1)}, b^{(2)} \in \{y|(0_n,y) \in V\}$ such that

$$D_{b^{(1)}} D_{b^{(2)}} g(y) \neq 0.$$

Thus, we can select $(0_n, b^{(1)}), (0_n, b^{(2)}) \in V$ such that

$$D_{(0_n,b^{(1)})} D_{(0_n,b^{(2)})} h(x,y) = D_{b^{(1)}} D_{b^{(2)}} g(y) \neq 0.$$

□

Example 8.1.6. Let $f \in \mathcal{B}_8$ be a bent function in $\mathcal{PS}^\#$ outside $\mathcal{M}^\#$ whose truth table in hexadecimal form corresponds to

$0x$813dcc51a81752a59d810e0f1761c3c124a73361682b629908db9455710bfffe,

and let $g \in \mathcal{B}_4$ be defined by $g(x_0, \ldots, x_3) = x_0x_3 \oplus x_1x_2 \oplus x_1x_3$. The function $h \in \mathcal{B}_{12}$ defined as the direct sum of f and g is a bent function outside $\mathcal{M}^\#$, which was checked using the Sage implementation described in Section 7.2.1.

Remark 8.1.7. By Theorem 8.1.5, the function h in Example 8.1.6 is outside $\mathcal{M}^\#$. However, since $r\text{-ind}(g) = m > m/2$, this does not follow from Lemma 8.1.4.

In the other direction, it is necessary that either f or g is outside $\mathcal{M}^\#$ so that $h = f \oplus g$ is outside $\mathcal{M}^\#$.

Theorem 8.1.8. *Let f and g be two bent function on $\mathbb{F}_2^n$ and $\mathbb{F}_2^m$, respectively. If the function h, defined as $h(x,y) = f(x) \oplus g(y)$, is outside $\mathcal{M}^\#$, then either f or g is outside $\mathcal{M}^\#$.*

Proof. Assuming that both f and g are in $\mathcal{M}^\#$ implies the existence of two subspaces $\Delta^{(n)} \in \mathbb{F}_2^n$ and $\Delta^{(m)} \in \mathbb{F}_2^m$ with dimension $n/2$ and $m/2$, respectively, such that $D_{a^{(1)}} D_{a^{(2)}} f = 0$ and $D_{b^{(1)}} D_{b^{(2)}} g = 0$ for any $a^{(1)}, a^{(2)} \in \Delta^{(n)}, b^{(1)}, b^{(2)} \in \Delta^{(m)}$. Hence, we can set $\Delta = \Delta^{(n)} \times \Delta^{(m)}$. Further, we have

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

for any $(a^{(1)}, b^{(1)}), (a^{(2)}, b^{(2)}) \in \Delta$. From Lemma 2.2.4, h is in $\mathcal{M}^\#$, which contradicts the fact that h is outside $\mathcal{M}^\#$. □

Open problem 8.1.9. It is clear that $f \in \mathcal{B}_n$ is outside $\mathcal{M}^\#$ implies that there exist two vectors $a, b \in V \subset \mathbb{F}_2^n$ such that $D_a D_b(f) \neq 0$, for some V with $\dim(V) \geqslant n/2$. From Lemma 2.2.4, we know $f \in \mathcal{B}_n$ is outside $\mathcal{M}^\#$ if $r\text{-ind}(f) < n/2$. However, there might exist bent functions $\{f\}$ with $r\text{-ind}(f) = n/2$ outside $\mathcal{M}^\#$ (that is, for which there exists a subspace V, with $\dim(V) = n/2$, so that $D_a D_b(f) = 0$ or $D_a D_b(f) = 1$). We leave the construction of such functions as an open problem.

8.1.2 Indirect sum method giving rise to bent functions outside $\mathcal{M}^\#$

The indirect sum method, introduced by Carlet [18, 22], is a secondary construction of bent functions that does not impose any additional conditions on the initial bent functions. In this section, we provide sufficient conditions on the bent functions f_i and g_i so that h defined by (8.2) is provably outside $\mathcal{M}^\#$.

Corollary 8.1.10. *[18] Let f_1 and f_2 be bent functions on $\mathbb{F}_2^n$ (n even) and g_1 and g_2 be bent functions defined on $\mathbb{F}_2^m$. Then, $h : \mathbb{F}_2^n \times \mathbb{F}_2^m$ defined as*

$$h(x, y) = f_1(x) \oplus g_1(y) \oplus (f_1 \oplus f_2)(x)(g_1 \oplus g_2)(y), \quad x \in \mathbb{F}_2^n, y \in \mathbb{F}_2^m, \tag{8.2}$$

is a bent function and its dual is obtained from f_1^*, f_2^*, g_1^* and g_2^* by the same formula as h is obtained from f_1, f_2, g_1 and g_2.

It is important to notice that f_i and g_i are arbitrary bent functions, but interestingly enough the condition that both $f_1 \oplus f_2$ and $g_1 \oplus g_2$ are bent implies that h defined by (8.2) is outside $\mathcal{M}^\#$.

Theorem 8.1.11. *Let f_1 and f_2 be bent functions on $\mathbb{F}_2^n$ (n even). Let g_1 and g_2 be bent functions defined on $\mathbb{F}_2^m$ (m even). Let h be defined as in (8.2). If $f_1 \oplus f_2$ and $g_1 \oplus g_2$ are bent, then h is outside $\mathcal{M}^\#$.*

Proof. Let $a^{(1)}, a^{(2)} \in \mathbb{F}_2^n$ and $b^{(1)}, b^{(2)} \in \mathbb{F}_2^m$. We prove that h does not belong to $\mathcal{M}^\#$ by using Lemma 2.2.4. We need to show that there does not exist an $(\frac{n+m}{2})$-dimensional subspace V such that

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

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

$$\begin{aligned}
& D_{(a^{(1)}, b^{(1)})} D_{(a^{(2)}, b^{(2)})} h(x, y) \\
= \; & D_{a^{(1)}} D_{a^{(2)}} f_1(x) \oplus D_{b^{(1)}} D_{b^{(2)}} g_1(y) \oplus (g_1 \oplus g_2)(y) D_{a^{(1)}} D_{a^{(2)}} (f_1 \oplus f_2)(x) \\
& \oplus (f_1 \oplus f_2)(x) D_{b^{(1)}} D_{b^{(2)}} (g_1 \oplus g_2)(y) \oplus D_{a^{(1)}} (f_1 \oplus f_2)(x) D_{b^{(1)}} (g_1 \oplus g_2)(y) \\
& \oplus D_{a^{(2)}} (f_1 \oplus f_2)(x) D_{b^{(2)}} (g_1 \oplus g_2)(y) \\
& \oplus D_{a^{(1)} \oplus a^{(2)}} (f_1 \oplus f_2)(x) D_{b^{(1)} \oplus b^{(2)}} (g_1 \oplus g_2)(y)
\end{aligned} \tag{8.3}$$

There are three cases to be considered.

(i) For $n = m$, there are two subcases.

(a) If $\dim(\{x|(x,y) \in V\}) = \dim(\{y|(x,y) \in V\}) = n$ (that is, $\{x|(x,y) \in V\} = \{y|(x,y) \in V\} = \mathbb{F}_2^n$), then there are two cases to be considered.

i. Assume that either $\deg(f_1 \oplus f_2) > 2$ or $\deg(g_1 \oplus g_2) > 2$. Without loss of generality, we suppose $\deg(f_1 \oplus f_2) > 2$. Then, we can find two vectors $a^{(1)}, a^{(2)} \in \mathbb{F}_2^n$ such that

$$D_{a^{(1)}} D_{a^{(2)}}(f_1 \oplus f_2)(x) \neq constant. \tag{8.4}$$

Since the algebraic degree of $g_1 \oplus g_2$ is strictly greater than the algebraic degree of its derivatives, from (8.3) and (8.4), we obtain

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

ii. For $\deg(f_1 \oplus f_2) = 2$ and $\deg(g_1 \oplus g_2) = 2$, we can find two vectors $a^{(1)}, a^{(2)} \in \mathbb{F}_2^n$ such that

$$D_{a^{(1)}} D_{a^{(2)}}(f_1 \oplus f_2)(x) = 1. \tag{8.5}$$

Since $g_1 \oplus g_2$ is bent and $\deg(g_1 \oplus g_2) = 2$, its derivatives are affine functions. We also know $D_{b^{(1)}} D_{b^{(2)}} g_1(y)$ has nonzero linear structures, since g_1 is a quadratic function. Hence, from (8.3) and (8.5), we get

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

(b) If $\dim(\{x|(x,y) \in V\}) < n$ or $\dim(\{y|(x,y) \in V\}) < n$, then we have $\{y|(0_n,y) \in V\} \neq \emptyset$ or $\{x|(x,0_n) \in V\} \neq \emptyset$. Without loss of generality, we suppose that $\{y|(0_n,y) \in V\} \neq \emptyset$. Hence, we can select $(0_n, b^{(1)}) \in V \cap (\{0_n\} \times \mathbb{F}_2^{n*})$ and $(a^{(2)}, b^{(2)}) \in V \cap (\mathbb{F}_2^{n*} \times \mathbb{F}_2^{n*})$. From (8.3), we have

$$\begin{array}{rl} & D_{(0_n,b^{(1)})} D_{(a^{(2)},b^{(2)})} h(x,y) \\ = & D_{b^{(1)}} D_{b^{(2)}} g_1(y) \oplus (f_1 \oplus f_2)(x) D_{b^{(1)}} D_{b^{(2)}}(g_1 \oplus g_2)(y) \\ & \oplus D_{a^{(2)}}(f_1 \oplus f_2)(x) D_{b^{(1)}}(g_1 \oplus g_2)(y \oplus b^{(2)}) \\ \neq & 0, \end{array} \tag{8.6}$$

since $f_1 \oplus f_2$, $g_1 \oplus g_2$ are bent (that is, $D_{a^{(2)}}(f_1 \oplus f_2)(x) \neq constant$ and $D_{b^{(1)}}(g_1 \oplus g_2)(y \oplus b^{(2)}) \neq constant$) and $\deg((f_1 \oplus f_2)(x)) > \deg(D_{a^{(2)}}(f_1 \oplus f_2)(x))$.

(ii) For $n \neq m$, there are also two cases to be considered.

(a) For $n > m$, we have $(n+m)/2 > m$. Thus, we can select two vectors $(a^{(1)}, 0_m) \in V \cap (\mathbb{F}_2^{n*} \times \{0_m\})$ and $(a^{(2)}, b^{(2)}) \in V \cap (\mathbb{F}_2^{n*} \times$

$\mathbb{F}_2^{m*}$). From (8.3), we have

$$\begin{aligned} & D_{(a^{(1)},0_m)}D_{(a^{(2)},b^{(2)})}h(x,y) \\ = \; & D_{a^{(1)}}D_{a^{(2)}}f_1(x) \oplus (g_1 \oplus g_2)(y)D_{a^{(1)}}D_{a^{(2)}}(f_1 \oplus f_2)(x) \\ & \oplus D_{a^{(1)}}(f_1 \oplus f_2)(x \oplus a^{(2)})D_{b^{(2)}}(g_1 \oplus g_2)(y) \\ \neq \; & 0, \end{aligned} \tag{8.7}$$

since $f_1 \oplus f_2$, $g_1 \oplus g_2$ are bent (that is, $D_{a^{(1)}}(f_1 \oplus f_2)(x \oplus a^{(2)}) \neq$ *constant* and $D_{b^{(2)}}(g_1 \oplus g_2)(y) \neq$ *constant*) and $\deg((g_1 \oplus g_2)(y)) > \deg(D_{b^{(2)}}(g_1 \oplus g_2)(y))$.

(b) For $n < m$, we have $(n+m)/2 > n$. Now, we select $(0_n, b^{(1)}) \in V \cap (\{0_n\} \times \mathbb{F}_2^{m*})$ and $(a^{(2)}, b^{(2)}) \in V \cap (\mathbb{F}_2^{n*} \times \mathbb{F}_2^{m*})$ and from item $(i) - (b)$ we conclude that $D_{(0_n,b^{(1)})}D_{(a^{(2)},b^{(2)})}h(x,y) \neq 0$. This concludes the proof.

□

It is tempting to relax the conditions on the initial functions as illustrated in the following example. The condition that either $\deg(f_1 \oplus f_2) > 2$ or $\deg(g_1 \oplus g_2) > 2$ seems to be sufficient at least for certain choices of the initial functions. However, proving this in general appears to be a difficult task since there exist certain $(n+m)/2$-dimensional subspaces of $\mathbb{F}_2^{(n+m)/2}$, say $\{V\}$, for which this condition is not enough to ensure the existence of $a, b \in V$ so that $D_aD_bh \neq 0$, for h defined by (8.2).

Example 8.1.12. Let $f_1, f_2 \in \mathscr{B}_6$ and $g_1, g_2 \in \mathscr{B}_4$ be bent functions such that $\deg(f_1 \oplus f_2) > 2$. Then, $h \in \mathscr{B}_{10}$ defined by (8.2) is a bent function outside $\mathcal{M}^{\#}$. For example, we may take

$$\begin{aligned} f_1(x_0,\ldots,x_5) &= x_0x_1x_2 \oplus x_0x_1x_3 \oplus x_0x_1x_4 \oplus x_0x_2x_3 \oplus x_0x_2x_5 \oplus x_0x_3x_4 \\ &\quad \oplus x_0x_3x_5 \oplus x_0x_4x_5 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_3x_4 \oplus x_1x_3x_5 \\ &\quad \oplus x_1x_4x_5 \oplus x_2x_3x_4 \oplus x_2x_3x_5 \oplus x_2x_4x_5 \\ f_2(x_0,\ldots,x_3) &= x_0x_1 \oplus x_2x_3 \oplus x_4x_5 \\ g_1(x_0,\ldots,x_3) &= x_0x_1 \oplus x_0x_3 \oplus x_1x_2 \oplus x_0 \oplus x_1 \\ g_2(x_0,\ldots,x_3) &= x_0x_1 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_2 \oplus x_1 \end{aligned}$$

The truth table in hexadecimal form of the function h obtained from (8.2) equals:

0x4874842e842eb78b842e7bd17bd14874842e48747bd17bd1b78b7bd17bd14874842e7bd1
48747bd17bd1b78bb78b842e7bd1b78bb78b842e4874842e842e842e842e7bd17bd17bd14874b7
8bb78b842e7bd1b78b842e842e7bd1842e842e842eb78b48747bd148747bd1842e842e842e7bd18
42e842e842e4874842e842e842e

Using the Sage implementation from Section 7.2.1, we have confirmed that $h \in \mathcal{B}_{10}$ is outside $\mathcal{M}^{\#}$.

Open problem 8.1.13. We leave as an open problem the specification of more relaxed sufficient conditions on the initial bent functions f_i and g_i used to define h in (8.2) so that h is provably outside $\mathcal{M}^{\#}$.

Outside $\mathcal{M}^{\#}$ property from the class membership of the initial functions

We remark that the previous results do not impose any condition on the constituent bent functions in terms of their class membership. However, it turns out that the indirect sum behave quite similarly as the direct sum, though requiring additional constraints on the initial functions which ensure that h is outside $\mathcal{M}^{\#}$. The following lemma is needed in the proof of our main result.

Lemma 8.1.14. *Let f_1 be a bent function on $\mathbb{F}_2^n$. If r-ind$(f_1) < n/2$, then there exist three vectors $a^{(1)}, a^{(2)}, a^{(3)} \in E$ such that $D_{a^{(1)}}D_{a^{(2)}}f_1(x) \neq$ constant, $D_{a^{(1)}}D_{a^{(3)}}f_1(x) \neq$ constant, and $D_{a^{(1)}}D_{a^{(2)}}f_1(x) \oplus D_{a^{(1)}}D_{a^{(3)}}f_1(x) \neq$ constant, where $E \subseteq \mathbb{F}_2^n$ is a subspace with $\dim(E) > n/2$.*

Proof. Since r-ind$(f_1) < n/2$, from Definitions 8.1.2 and 8.1.3, we know $\dim(\mathcal{RMS}(f_1)) < n/2$. Without loss of generality, set $\dim(\mathcal{RMS}(f_1)) = n/2 - 1$ and $\dim(E) = n/2 + 1$.

Let $U \subseteq E$ be a relaxed $\mathcal{M}$-subspace of f_1 such that $U \cup \{\alpha \oplus U\}$ is not a relaxed $\mathcal{M}$-subspace for all $\alpha \in E \setminus U$. Then, we have

$$\dim(E) - \dim(U) \geq \dim(E) - \dim(\mathcal{RMS}(f_1)) \geq 2. \tag{8.8}$$

Without loss of generality, we suppose $\dim(U) = n/2 - 1$. We set $\{\alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(n/2-1)}\}$ to be a basis of U and $\{\alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(n/2+1)}\}$ be a basis of E.

We set $U^{(\alpha)} = \{\gamma : D_\gamma D_\alpha f_1(x) = constant, \gamma \in E\}$, where $\alpha \in \{\alpha^{(n/2)}, \alpha^{(n/2+1)}, \alpha^{(n/2)} \oplus \alpha^{(n/2+1)}\}$. From r-ind$(f_1) < n/2$ and the definition of U, we have

$$U^{(\alpha^{(n/2)})} \subset E, \;\; U^{(\alpha^{(n/2+1)})} \subset E, \;\; U^{(\alpha^{(n/2)} \oplus \alpha^{(n/2+1)})} \subset E. \tag{8.9}$$

We also know $U^{(\alpha^{(n/2)})}$, $U^{(\alpha^{(n/2+1)})}$ and $U^{(\alpha^{(n/2)} \oplus \alpha^{(n/2+1)})}$ are subspaces of E. From (8.9), we have

$$\begin{aligned} \Delta := & \left(E \setminus U^{(\alpha^{(n/2)})}\right) \cap \left(E \setminus U^{(\alpha^{(n/2+1)})}\right) \cap \left(E \setminus U^{(\alpha^{(n/2)} \oplus \alpha^{(n/2+1)})}\right) \\ = & \; E \setminus \left(U^{(\alpha^{(n/2)})} \cup U^{(\alpha^{(n/2+1)})} \cup U^{(\alpha^{(n/2)} \oplus \alpha^{(n/2+1)})}\right) \neq \emptyset. \end{aligned} \tag{8.10}$$

Hence, we can select $a^{(1)} \in \Delta, a^{(2)} = \alpha^{(n/2)}, a^{(3)} = \alpha^{(n/2+1)}$. Further, we have $D_{a^{(1)}}D_{a^{(2)}}f_1(x) \neq$ constant, $D_{a^{(1)}}D_{a^{(3)}}f_1(x) \neq$ constant and $D_{a^{(1)}}D_{a^{(2)}}f_1(x) \oplus D_{a^{(1)}}D_{a^{(3)}}f_1(x) \neq$ constant, since $D_{a^{(1)}}D_{a^{(2)}}f_1(x) \oplus D_{a^{(1)}}D_{a^{(3)}}f_1(x) = D_{a^{(1)}}D_{a^{(2)} \oplus a^{(3)}}f_1(x)$. □

Theorem 8.1.15. *Let f_1 and f_2 be bent functions on $\mathbb{F}_2^n$ (n even). Let g_1 and g_2 be bent functions defined on $\mathbb{F}_2^m$ (m even) such that* $\deg(g_1 \oplus g_2) > 0$. *Let h be defined as in (8.2). If r-ind$(f_1) < n/2$ (hence $f_1 \notin \mathcal{M}^{\#}$) and* $\deg(f_1 \oplus f_2) = 1$, *then h is outside $\mathcal{M}^{\#}$.*

Proof. Let $a^{(1)}, a^{(2)} \in \mathbb{F}_2^n$ and $b^{(1)}, b^{(2)} \in \mathbb{F}_2^m$. We prove that h does not belong to $\mathcal{M}^{\#}$, by using Lemma 2.2.4. We need to show that there does not exist an $(\frac{n+m}{2})$-dimensional subspace V of $\mathbb{F}_2^{n+m}$ such that

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

for any $(a^{(1)}, b^{(1)})$, $(a^{(2)}, b^{(2)}) \in V$. Since $\deg(f_1 \oplus f_2) = 1$, we have

$$\begin{aligned}
& D_{(a^{(1)},b^{(1)})} D_{(a^{(2)},b^{(2)})} h(x,y) \\
= \; & D_{a^{(1)}} D_{a^{(2)}} f_1(x) \oplus D_{b^{(1)}} D_{b^{(2)}} g_1(y) \oplus (f_1 \oplus f_2)(x) D_{b^{(1)}} D_{b^{(2)}} (g_1 \oplus g_2)(y) \\
& \oplus D_{a^{(1)}} (f_1 \oplus f_2)(x) D_{b^{(1)}} (g_1 \oplus g_2)(y) \oplus D_{a^{(2)}} (f_1 \oplus f_2)(x) D_{b^{(2)}} (g_1 \oplus g_2)(y) \\
& \oplus D_{a^{(1)} \oplus a^{(2)}} (f_1 \oplus f_2)(x) D_{b^{(1)} \oplus b^{(2)}} (g_1 \oplus g_2)(y) \\
= \; & D_{a^{(1)}} D_{a^{(2)}} f_1(x) \oplus D_{b^{(1)}} D_{b^{(2)}} g_1(y) \oplus (f_1 \oplus f_2)(x) D_{b^{(1)}} D_{b^{(2)}} (g_1 \oplus g_2)(y) \\
& \oplus \varepsilon_{a^{(1)}} D_{b^{(1)}} (g_1 \oplus g_2)(y) \oplus \varepsilon_{a^{(2)}} D_{b^{(2)}} (g_1 \oplus g_2)(y) \\
& \oplus \varepsilon_{a^{(1)} \oplus a^{(2)}} D_{b^{(1)} \oplus b^{(2)}} (g_1 \oplus g_2)(y),
\end{aligned} \tag{8.11}$$

where $\varepsilon_{a^{(1)}}, \varepsilon_{a^{(2)}}, \varepsilon_{a^{(1)} \oplus a^{(2)}} \in \mathbb{F}_2$. Since r-ind$(f_1) < n/2$, we know $\deg(f_1) \geq 3$.

There are three cases to be considered.

(i) For $\dim(\{x | (x,y) \in V\}) > n/2$, since r-ind$(f_1) < n/2$, from Definitions 8.1.2 and 8.1.3, we know $\dim(\mathcal{RMS}(f_1)) < n/2$. Without loss of generality, set $\dim(\mathcal{RMS}(f_1)) = n/2 - 1$.

From Lemma 8.1.14, we know there exist $(a^{(1)}, b^{(1)}), (a^{(2)}, b^{(2)}), (a^{(3)}, b^{(3)}) \in V$ such that

$$\begin{aligned}
D_{a^{(1)}} D_{a^{(2)}} f_1(x) &\neq \textit{constant}, \\
D_{a^{(1)}} D_{a^{(3)}} f_1(x) &\neq \textit{constant}, \\
D_{a^{(1)}} D_{a^{(2)}} f_1(x) \oplus D_{a^{(1)}} D_{a^{(3)}} f_1(x) = D_{a^{(1)}} D_{a^{(2)} \oplus a^{(3)}} f_1(x) &\neq \textit{constant}.
\end{aligned} \tag{8.12}$$

Since $f_1 \oplus f_2$ is given, from (8.12), we get

$$D_{a^{(1)}} D_{a^{(2)}} f_1(x) \oplus (f_1 \oplus f_2)(x) \neq \textit{constant} \tag{8.13}$$

or

$$D_{a^{(1)}} D_{a^{(3)}} f_1(x) \oplus (f_1 \oplus f_2)(x) \neq \textit{constant}. \tag{8.14}$$

Without loss generality, we assume that (8.13) holds. There are three cases to be considered.

(a) If $D_{b^{(1)}} D_{b^{(2)}} (g_1 \oplus g_2)(y) \neq \textit{constant}$, from (8.11), we obtain

$$D_{(a^{(1)},b^{(1)})} D_{(a^{(2)},b^{(2)})} h(x,y) \neq \textit{constant}.$$

(b) If $D_{b^{(1)}}D_{b^{(2)}}(g_1 \oplus g_2)(y) = 1$, we conclude

$$D_{b^{(1)}}(g_1 \oplus g_2)(y) \neq constant,$$

$$D_{b^{(2)}}(g_1 \oplus g_2)(y) \neq constant$$

and

$$D_{b^{(1)} \oplus b^{(2)}}(g_1 \oplus g_2)(y) \neq constant.$$

If (8.12), (8.13) and (8.11), we deduce

$$D_{(a^{(1)},b^{(1)})}D_{(a^{(2)},b^{(2)})}h(x,y) \neq constant.$$

(c) Finally, when $D_{b^{(1)}}D_{b^{(2)}}(g_1 \oplus g_2)(y) = 0$, from (8.12) and (8.11), we get

$$D_{(a^{(1)},b^{(1)})}D_{(a^{(2)},b^{(2)})}h(x,y) \neq constant.$$

(ii) If $\dim(\{x|(x,y) \in V\}) = n/2$, then there are three cases to be considered.

(a) If $\dim(\{y|(x,y) \in V\}) = m/2$, then

$$V = \{x|(x,0_m) \in V\} \times \{y|(0_n,y) \in V\}$$

since $\dim(V) = (n+m)/2$. Using the assumption that $r\text{-ind}(f_1) < n/2$, there will exist $(a^{(1)},0_m),(a^{(2)},0_m) \in V$ such that

$$D_{a^{(1)}}D_{a^{(2)}}f_1(x) \neq constant.$$

Applying this to (8.11), we deduce that

$$D_{(a^{(1)},0_m)}D_{(a^{(2)},0_m)}h(x,y) \neq constant.$$

(b) Assume now that $m/2 < \dim(\{y|(x,y) \in V\}) < (n+m)/2$. Then, for arbitrary $a_1, a_2 \in \{x|(x,y) \in V\}$, we always have $\{y|(a_1,y) \in V\} \cap \{y|(a_2,y) \in V\} \neq \emptyset$. Hence, we can select two vectors $(a^{(1)},b^{(1)}),(a^{(2)},b^{(2)}) \in V$ such that $b^{(1)} = b^{(2)}$ and $D_{a^{(1)}}D_{a^{(2)}}f_1(x) \neq constant$. Again, using that $D_{a^{(1)}}D_{a^{(2)}}f_1(x) \neq constant$ in (8.11), we conclude

$$D_{(a^{(1)},b^{(1)})}D_{(a^{(2)},b^{(2)})}h(x,y) \neq constant.$$

(c) When $\dim(\{y|(x,y) \in V\}) = (n+m)/2$, we have $\{y|(a_1,y) \in V\} \cap \{y|(a_2,y) \in V\} = \emptyset$ for arbitrary $a_1, a_2 \in \{x|(x,y) \in V\}$ and $\dim(\{y|(0_n,y) \in V\}) = m/2$. Since $\dim(\{\alpha|D_\alpha(f_1 \oplus f_2) = 0\}) = n-1$ and $\dim(\{x|(x,y) \in V\}) = n/2$, we can select one nonzero vector $a \in \{x|(x,y) \in V\}$ such that $D_a(f_1 \oplus f_2) = 0$. Further,

$$\dim(\{(0_n,y)|(0_n,y) \in V\} \cup \{(a,y)|(a,y) \in V\}) = m/2 + 1.$$

Then, by Proposition 8.1.1, we can select two vectors $(a^{(1)}, b^{(1)}), (a^{(2)}, b^{(2)}) \in \{(0_n, y)|(0_n, y) \in V\} \cup \{(a, y)|(a, y) \in V\}$ such that

$$D_{b^{(1)}} D_{b^{(2)}} g_1(y) \neq 0.$$

Setting this in (8.11), we obtain

$$\begin{aligned} & D_{(a^{(1)},b^{(1)})} D_{(a^{(2)},b^{(2)})} h(x, y) \\ = \; & D_{b^{(1)}} D_{b^{(2)}} g_1(y) \oplus (f_1 \oplus f_2)(x) D_{b^{(1)}} D_{b^{(2)}} (g_1 \oplus g_2)(y) \neq 0. \end{aligned} \tag{8.15}$$

(iii) If $\dim(\{x|(x, y) \in V\}) < n/2$, then we have $\dim(\{y|(x, y) \in V\}) \geq m/2 + 1$. Further, we have $\dim(\{y|(0, y) \in V\}) \geq m/2 + 1$ since $\dim(V) = (n + m)/2$. Hence, from Proposition 8.1.1, we can select two vectors $(0_n, b^{(1)}), (0_n, b^{(2)}) \in V$ such that

$$D_{b^{(1)}} D_{b^{(2)}} g_1(y) \neq 0.$$

Again, putting this in (8.11), we have

$$\begin{aligned} & D_{(0_n,b^{(1)})} D_{(0_n,b^{(2)})} h(x, y) \\ = \; & D_{b^{(1)}} D_{b^{(2)}} g_1(y) \oplus (f_1 \oplus f_2)(x) D_{b^{(1)}} D_{b^{(2)}} (g_1 \oplus g_2)(y) \neq 0. \end{aligned} \tag{8.16}$$

□

Remark 8.1.16. We note that the functions f_1 and f_2 as well as g_1 and g_2 in Example 8.1.12 are not affine related, that is, $\deg(f_1 \oplus f_2), \deg(g_1 \oplus g_2) > 1$. This leads us to believe that the condition $\deg(f_1 \oplus f_2) = 1$ in Theorem 8.1.15 seems to be only sufficient but not necessary.

Remark 8.1.17. The main reason for using the condition that $\deg(f_1 \oplus f_2) = 1$ in Theorem 8.1.15 is related to $n/2$-dimensional subspaces V of $\mathbb{F}_2^{n+m}$ with the property that $\dim(\{x|(x, y) \in V\}) \geq n/2$ and $\dim(\{y|(x, y) \in V\}) \geq m/2$. In this case, we cannot ensure that some of the following inequalities $D_{a^{(1)}} D_{a^{(2)}} f_1(x) \neq (f_1 \oplus f_2)(x)$, $D_{a^{(1)}} D_{a^{(2)}} f_1(x) \neq D_{a^{(1)}}(f_1 \oplus f_2)(x)$ and $D_{a^{(1)}} D_{a^{(2)}} f_1(x) \neq D_{a^{(2)}}(f_1 \oplus f_2)(x)$ hold.

Similarly to Theorem 8.1.15, we can prove even a stronger statement which excludes the possibility of having constant second order derivatives of h on any $(n + m)/2$-dimensional subspace. The proof of Theorem 8.1.18 can be found in Appendix.

Theorem 8.1.18. *Let f_1 and f_2 be bent functions on $\mathbb{F}_2^n$ (n even). Let g_1 and g_2 be bent functions defined on $\mathbb{F}_2^m$ (m even) such that $\deg(g_1 \oplus g_2) > 0$. Let h be defined as in (8.2). If $r\text{-}ind(f_1) < n/2$, $\deg(f_1 \oplus f_2) = 1$ and $r\text{-}ind(g_1) < m/2 + 1$, then h is outside $\mathcal{M}^{\#}$ and $r\text{-}ind(h) < (n + m)/2$.*

8.2 Design methods for homogenous bent functions

The design methods for homogenous bent functions are very few and it appears that this subclass of bent functions is quite small. The main progress has been made recently in [71], where the authors efficiently specified new homogenous cubic bent functions using the direct sum and stated the following open problem: Construct homogeneous cubic bent functions without affine derivatives outside the $\mathcal{M}^{\#}$ class without the use of the direct sum. In this section, we positively answer this problem by applying the indirect sum method to suitably selected initial bent functions. Moreover, we improve the results in [71] with respect to the dimension of input variable space, see Table 8.1. In the following section we will be interested in the notion of fast points, which are defined as follows.

Definition 8.2.1. The point $a \in \mathbb{F}_2^n$ is called a *fast point* of a function $f \in \mathcal{B}_n$ if it satisfies $\deg(D_a f) < \deg(f) - 1$. The set of all fast points of f will be denoted with $\mathbb{FP}_f$.

8.2.1 Homogenous bent functions using the indirect sum

In what follows, we construct homogeneous cubic bent functions without affine derivatives outside the $\mathcal{M}^{\#}$ by using the indirect sum and thereby partially solve the open problem in [71].

Theorem 8.2.2. *Let n and m be two positive even integers. Let f_1 and g_1 be two homogeneous cubic bent functions on $\mathbb{F}_2^n$ and $\mathbb{F}_2^m$, respectively. Let $f_2(x) = f_1(x) \oplus c \cdot x$, where $c \in \mathbb{F}_2^n \setminus \{0_n\}$, and $g_2(y) = g_1(y) \oplus Q(y)$ be also bent, where Q is a homogeneous quadratic function. Then, the function $h \in \mathcal{B}_{n+m}$ defined by (8.2) is a homogeneous cubic bent function. Further, if r-ind$(f_1) < n/2$, then h is outside $\mathcal{M}^{\#}$. If f_1 has no affine derivatives and $\mathbb{FP}_{g_1} \cap \mathbb{FP}_{g_1 \oplus g_2} = \{0_m\}$, then h has no affine derivatives.*

Proof. From Corollary 8.1.10, h is a bent function in $n+m$ variables. Since $\deg(f_1 \oplus f_2) = 1$ and Q is a homogeneous quadratic function in m variables, then h is a homogeneous cubic bent function.

From Theorem 8.1.15, since r-ind$(f_1) < n/2$ and $\deg(f_1 \oplus f_2) = 1$, h is outside $\mathcal{M}^{\#}$. For $a^{(1)} \in \mathbb{F}_2^n$ and $b^{(1)} \in \mathbb{F}_2^m$, we have

$$\begin{aligned} &D_{(a^{(1)},b^{(1)})}h(x,y) = D_{a^{(1)}}f_1(x) \oplus D_{b^{(1)}}g_1(y) \\ &\oplus (g_1 \oplus g_2)(y) D_{a^{(1)}}(f_1 \oplus f_2)(x) \oplus (f_1 \oplus f_2)(x) D_{b^{(1)}}(g_1 \oplus g_2)(y). \end{aligned} \tag{8.17}$$

To show that h has no affine derivatives, we consider two cases:

a) If $a^{(1)} = 0_n$, then $b^{(1)} \neq 0_m$. From (8.17), we deduce

$$D_{(0_n,b^{(1)})}h(x,y) = D_{b^{(1)}}g_1(y) \oplus (f_1 \oplus f_2)(x) D_{b^{(1)}}(g_1 \oplus g_2)(y).$$

Since g_1 is cubic and $\mathbb{FP}_{g_1} \cap \mathbb{FP}_{g_1 \oplus g_2} = \{0_m\}$, then $\deg(D_{b^{(1)}} g_1(y)) = 2$ or $\deg(D_{b^{(1)}}(g_1 \oplus g_2)(y)) = 1$. Hence, $\deg(D_{(0_n, b^{(1)})} h) = 2$.

b) If $a^{(1)} \neq 0_n$, then $\deg(D_{a^{(1)}} f_1) = 2$ due to the assumption on f_1. From (8.17), we have $\deg(D_{(a^{(1)}, b^{(1)})} h) = 2$ since $f_1 \oplus f_2$ is a linear function.

□

Remark 8.2.3. One can also set $Q(y) := g_1(y) \oplus g_1(y \oplus a) \oplus A(y)$ in Theorem 8.2.2, where $a \in \mathbb{F}_2^n \setminus \mathbb{FP}_{g_1}$ and $A(y)$ stands for the affine terms of $g_1(y) \oplus g_1(y \oplus a)$.

Corollary 8.2.4. *Let n, m and t be three positive even integers such that $t \leq m$. Let f_1 and g_1 be two homogeneous cubic bent functions on $\mathbb{F}_2^n$ and $\mathbb{F}_2^m$, respectively. Let $f_2(x) = f_1(x) \oplus c \cdot x$, where $c \in \mathbb{F}_2^n \setminus \{0_n\}$, and $g_2(y) = g_1(y \oplus e^{(t)})$, where $e^{(t)} = (e_1^{(t)}, e_2^{(t)}, \ldots, e_m^{(t)}) \in \mathbb{F}_2^m$, $e_i^{(t)} = 1$ if $i = t$, $e_i^{(t)} = 0$ otherwise. Let h be defined as in (8.2). If r-ind$(f_1) < n/2$, then h is a homogeneous cubic bent functions on $\mathbb{F}_2^{n+m}$ outside $\mathcal{M}^{\#}$. If f_1 has no affine derivatives and $\mathbb{FP}_{g_1} \cap \mathbb{FP}_{g_1 \oplus g_2} = \{0_m\}$, then h has no affine derivatives.*

Proof. Since g_1 is a homogeneous cubic bent function, $g_1(y) \oplus g_1(y \oplus e^{(t)})$ is a homogeneous quadratic function. From Theorem 8.2.2, identifying $Q(y) := g_1(y) \oplus g_1(y \oplus e^{(t)})$, we know that h is a homogeneous cubic bent function since $g_2(y) = g_1(y) \oplus \big(g_1(y) \oplus g_1(y \oplus e^{(t)})\big) = g_1(y) + Q(y)$ is a bent function. Furthermore, Theorem 8.2.2 implies that h has no affine derivatives if f_1 has no affine derivatives and $\mathbb{FP}_{g_1} \cap \mathbb{FP}_{g_1 \oplus g_2} = \{0_m\}$. □

Homogeneous cubic bent function without affine derivatives outside $\mathcal{M}^{\#}$ were specified by Polujan and Pott [71, Theorem 4.9] with the number of variables $n \geq 50$. The following example demonstrates that such functions can be specified on much smaller variable spaces compared to [71] (namely for $n = 20$).

Example 8.2.5. Let f_1 be a homogenous cubic bent function without affine derivatives on $\mathbb{F}_2^{10}$, with r-ind$(f_1) = 4$, whose ANF is given as (see [71, Table 4])

$f_1(x_0, \ldots, x_9) = x_0x_1x_5 \oplus x_0x_1x_6 \oplus x_0x_1x_7 \oplus x_0x_1x_9 \oplus x_0x_2x_3 \oplus x_0x_2x_4 \oplus x_0x_2x_6 \oplus x_0x_2x_8 \oplus x_0x_2x_9 \oplus x_0x_3x_4 \oplus x_0x_3x_5 \oplus x_0x_3x_7 \oplus x_0x_3x_8 \oplus x_0x_3x_9 \oplus x_0x_4x_6 \oplus x_0x_5x_6 \oplus x_0x_5x_7 \oplus x_0x_5x_9 \oplus x_0x_6x_8 \oplus x_0x_6x_9 \oplus x_0x_8x_9 \oplus x_1x_2x_4 \oplus x_1x_2x_7 \oplus x_1x_2x_8 \oplus x_1x_2x_9 \oplus x_1x_3x_5 \oplus x_1x_3x_6 \oplus x_1x_3x_7 \oplus x_1x_4x_5 \oplus x_1x_4x_8 \oplus x_1x_5x_6 \oplus x_1x_5x_8 \oplus x_1x_5x_9 \oplus x_1x_6x_7 \oplus x_1x_6x_9 \oplus x_1x_7x_8 \oplus x_1x_7x_9 \oplus x_1x_8x_9 \oplus x_2x_3x_6 \oplus x_2x_3x_8 \oplus x_2x_4x_5 \oplus x_2x_4x_6 \oplus x_2x_4x_7 \oplus x_2x_4x_9 \oplus x_2x_5x_7 \oplus x_2x_5x_8 \oplus x_2x_6x_9 \oplus x_2x_7x_8 \oplus x_2x_7x_9 \oplus x_2x_8x_9 \oplus x_3x_4x_6 \oplus x_3x_4x_8 \oplus x_3x_4x_9 \oplus x_3x_5x_7 \oplus x_3x_5x_9 \oplus x_3x_6x_7 \oplus x_3x_6x_8 \oplus x_3x_6x_9 \oplus x_3x_7x_9 \oplus x_3x_8x_9 \oplus x_4x_5x_7 \oplus x_4x_5x_8 \oplus x_4x_5x_9 \oplus x_4x_6x_8 \oplus x_4x_6x_9 \oplus x_4x_7x_8 \oplus x_4x_7x_9 \oplus x_4x_8x_9 \oplus x_5x_6x_7 \oplus x_5x_7x_9 \oplus x_5x_8x_9 \oplus x_6x_7x_9,$

and let $g_1 = f_1$. Then, from Corollary 8.2.4, the function h defined as in (8.2) via f_1, f_2, g_1, g_2, is a homogeneous cubic bent function without affine derivatives on $\mathbb{F}_2^{20}$ outside $\mathcal{M}^{\#}$.

Seberry, Xia and Pieprzyk in [79, Theorem 8] proved that one can construct homogeneous cubic bent functions for all even $m \neq 8$. Let $F : \mathbb{F}_2^m \to \mathbb{F}_2$ be defined as in [79, Theorem 8]

$$F(y) = \bigoplus_{i=1}^{m/2} y_i y_{i+m/2} \oplus C(y_{m/2+1}, y_{m/2+2}, \ldots, y_m),$$

where $C(y_{m/2+1}, y_{m/2+2}, \ldots, y_m)$ is a certain cubic function. Then, there exists a nonsingular matrix T such that $F(Ty)$ is a homogeneous cubic bent function [79]. Let ϕ be a linear permutation on $\mathbb{F}_2^{m/2}$ such that $\phi \oplus I$ is also a linear permutation, where I is the identity permutation. Thus, $Q'(y) := \big(\phi(y_1, y_2, \ldots, y_{m/2})\big) \cdot (y_{m/2+1}, y_{m/2+2}, \ldots, y_m)$ is bent. Further, we have that

$$F(Ty) \oplus Q(y) \tag{8.18}$$

is a bent function, where $Q(y) = Q'(Ty) \oplus A(y)$ is a homogeneous quadratic function and $A(y)$ is affine.

In [71], the authors provided one 10-variable function, denoted by $h_4^{10} \in \mathcal{B}_{10}$, which is a homogeneous cubic bent function without affine derivatives and r-ind$(h_4^{10}) = 4 < 10/2$, thus $h_4^{10} \notin \mathcal{M}^{\#}$.

Theorem 8.2.2, employing h_4^{10} and $F(Ty)$, implies the following result.

Theorem 8.2.6. *Let $n = 10$ and $m \geq 6$ be a positive even integer such that $m \neq 8$. Let $f_1 = h_4^{10}$, $g_1(y) = F(Ty)$ and $g_2(y) = g_1(y) \oplus Q(y)$, where $F(Ty)$ and $Q(y)$ are defined by (8.18). Let also $f_2(x) = f_1(x) \oplus c \cdot x$, where $c \in \mathbb{F}_2^{10} \setminus \{0_{10}\}$. Then, h defined by (8.2) is a homogeneous cubic bent function in $m+10$ variables without affine derivatives outside $\mathcal{M}^{\#}$.*

Proof. Since r-ind$(h_4^{10}) = 4 < 10/2$, from Theorem 8.2.2, we deduce that h is a homogeneous cubic bent functions in $m + 10$ variables outside the $\mathcal{M}^{\#}$. Since Q is a quadratic bent function, we have $\mathbb{FP}_Q = \mathbb{FP}_{g_1 \oplus g_2} = \{0_m\}$. Theorem 8.2.2 implies that h has no affine derivatives. □

Theorem 8.2.7. *Let n, m be two positive even integers such that $n \geq 6, m \geq 6$. Let f_1 be a (homogeneous) cubic bent function with $\dim(\mathbb{FP}_{f_1}) = 1$ on $\mathbb{F}_2^n$. Without loss of generality, we set $\mathbb{FP}_{f_1} = \{0_n, \varepsilon\}$. Let $c \in \{\alpha | \alpha \in \mathbb{F}_2^n, \alpha \cdot \varepsilon = 1\}$ and define $f_2(x) = f_1(x) \oplus c \cdot x$. Let g_1 be a (homogeneous) cubic bent function without affine derivatives on $\mathbb{F}_2^m$ such that r-ind$(g_1) < m/2$. Define a bent function $g_2(y) = g_1(y) \oplus Q(y)$, where Q is a (homogeneous) quadratic function such that $\deg(D_b g_1(y) \oplus Q(y)) = 2$, for any $b \in \mathbb{FP}_Q \setminus \{0_m\}$. Then, h defined by (8.2) is a (homogeneous) cubic bent function without affine derivatives outside $\mathcal{M}^{\#}$.*

Proof. From Theorem 8.2.2, we know that h is a (homogeneous) cubic bent function outside $\mathcal{M}^{\#}$.

Now we prove h does not have affine derivatives. There are two cases to be considered. Let $a^{(1)} \in \mathbb{F}_2^n$ and $b^{(1)} \in \mathbb{F}_2^m$.

i) If $a^{(1)} \notin \mathbb{FP}_{f_1} = \{0_n, \varepsilon\}$, then $\deg(D_{a^{(1)}} f_1) = 2$. From (8.17), we have $\deg(D_{(a^{(1)},b^{(1)})} h) = 2$ since $f_1 \oplus f_2$ is a linear function.

ii) If $a^{(1)} = \varepsilon$, from (8.17), we have

$$\begin{aligned} D_{(\varepsilon,b^{(1)})} h(x,y) = \; & D_\varepsilon f_1(x) \oplus D_{b^{(1)}} g_1(y) \\ & \oplus (g_1 \oplus g_2)(y) D_\varepsilon (c \cdot x) \oplus (c \cdot x) D_{b^{(1)}} (g_1 \oplus g_2)(y) \\ = \; & D_\varepsilon f_1(x) \oplus D_{b^{(1)}} g_1(y) \oplus Q(y) \oplus (c \cdot x) D_{b^{(1)}} Q(y). \end{aligned} \tag{8.19}$$

There are two cases to be considered.

(a) If $b^{(1)} \in \mathbb{FP}_Q \setminus \{0_m\}$, then $\deg(D_{b^{(1)}} g_1(y) \oplus Q(y)) = 2$. Hence, from (8.19), we have $\deg(D_{(\varepsilon,b^{(1)})} h(x,y)) = 2$.

(b) If $b^{(1)} \notin \mathbb{FP}_Q \setminus \{0_m\}$, from (8.19), we get $\deg(D_{(\varepsilon,b^{(1)})} h(x,y)) = 2$ since $\deg((c \cdot x) D_{b^{(1)}} Q(y)) = 2$ or $b^{(1)} = 0_m$.

□

Remark 8.2.8. Let us consider the homogeneous quadratic function $Q(y) = D_{e^{(t)}} g_1(y)$ as defined in Corollary 8.2.4, where $e^{(t)} = (e_1^{(t)}, e_2^{(t)}, \ldots, e_m^{(t)}) \in \mathbb{F}_2^m$, $e_i^{(t)} = 1$ if $i = t$, $e_i^{(t)} = 0$ otherwise. The vector $e^{(t)}$ is obviously a fast point for the function Q (more precisely, it is a linear structure) because $D_{e^{(t)}} Q(y) = D_{e^{(t)}} D_{e^{(t)}} g_1 \equiv 0$. With respect to the above notation, we have that $D_{e^{(t)}}(g_1(y) \oplus Q(y)) = D_{e^{(t)}} g_1(y) \oplus D_{e^{(t)}} g_1(y) = 0$, thus Q does not satisfy Theorem 8.2.7. We also note that $D_{(\varepsilon,e^{(t)})} h(x,y) = D_\varepsilon f_1(x)$, which is an affine function. Using Sage we observed that ε is the only affine derivative of h.

Based on the above remark, the following open problem is an interesting research challenge.

Open problem 8.2.9. Find instances of quadratic homogeneous bent functions Q which satisfy Theorem 8.2.7 and thus give rise to homogeneous cubic bent functions without affine derivatives outside $\mathcal{M}^{\#}$.

From Theorems 8.1.15 and 8.2.6, we note that [71, Theorem 4.9] (see Theorem 8.2.19) can be generalized as follows:

Theorem 8.2.10. *On $\mathbb{F}_2^n$ there exist homogeneous cubic bent functions (without affine derivatives) outside $\mathcal{M}^{\#}$ for $n \geq 16$, $n \neq 18$.*

8.2.2 Non-decomposability of our bent functions

In this section, we solve an open problem on the decomposability of bent functions raised in [71, Open Problem 5.1]. We essentially show that the homogenous cubic bent functions constructed by means of Theorem 8.2.14 are non-decomposable in the sense of the definition below.

Definition 8.2.11. [95] A function $f \in \mathcal{B}_n$ is said to be decomposable if there exists a nonsingular $n \times n$ matrix B over $\mathbb{F}_2$ and an integer l with $1 \leq l \leq n-1$ such that $f(xB) = g(y) \oplus h(z)$, where $x = (y, z), y \in \mathbb{F}_2^l, z \in \mathbb{F}_2^{n-l}, g \in \mathcal{B}_l$ and $h \in \mathcal{B}_{n-l}$. Otherwise, f is said to be non-decomposable.

Lemma 8.2.12. *[95, Theorem 2] A function $f \in \mathcal{B}_n$ is decomposable if and only if there exists an integer p with $1 \leq p \leq n-1$, a p-dimensional linear subspace W of $\mathbb{F}_2^n$ and a complementary subspace U in $\mathbb{F}_2^n$ (thus $U + W = \mathbb{F}_2^n$) such that for every non-zero vector $\alpha \in W$ and every non-zero vector $\beta \in U$, we have*

$$f(x) \oplus f(x \oplus \alpha) \oplus f(x \oplus \beta) \oplus f(x \oplus \alpha \oplus \beta) = 0.$$

The following result specifies some useful properties of the function h_4^{10} mentioned earlier.

Lemma 8.2.13. *Let $A := (a^{(1)}, a^{(2)}, \ldots, a^{(10)})$ be a basis of $\mathbb{F}_2^{10}$. Then, $||\{\varepsilon \in A \mid D_{a^{(i)}} D_\varepsilon h_4^{10} \neq 0\}|| \geq 3$, for any $a^{(i)} \in A$. Moreover, for disjoint non-empty subsets $S, T \subset A$ that partition A, $S \cup T = A$, there exist two vectors $\alpha^{(1)} \in S$ and $\alpha^{(2)} \in T$ such that $D_{\alpha^{(1)}} D_{\alpha^{(2)}} h_4^{10} \neq 0$.*

Proof. From Theorem 8.2.6, we know that h given by (8.2), defined using h_4^{10}, is a homogeneous cubic bent function in $m + 10$ variables without affine derivatives (with m even). In particular, $\deg(D_{a^{(i)}} h_4^{10}) = 2$, for any $i = 1, \ldots, 10$. Without loss of generality, we set $i = 1$. We also know $\dim(\mathbb{FP}_{D_{a^{(1)}} h_4^{10}}) \leq n - \deg(D_{a^{(1)}} h_4^{10})$. Hence,

$$\dim(\mathbb{FP}_{D_{a^{(1)}} h_4^{10}}) = \dim(\{\varepsilon \mid D_{a^{(1)}} D_\varepsilon h_4^{10} = constant\}) \leq n - 2. \quad (8.20)$$

Since h_4^{10} is bent, $D_{a^{(1)}} h_4^{10}$ is a quadratic balanced function, that is, there exists at least one vector β such that $D_{a^{(1)}} D_\beta h_4^{10} = 1$ (due to the existence of linear terms in the ANF of $D_{a^{(1)}} h_4^{10}$). Furthermore, using (8.20), we have

$$\dim(\{\varepsilon \in \mathbb{F}_2^{10} \mid D_{a^{(1)}} D_\varepsilon h_4^{10} = 0\}) \leq n - 3, \quad (8.21)$$

which implies that

$$\dim(\langle \{\varepsilon \in \mathbb{F}_2^{10} \mid D_{a^{(i)}} D_\varepsilon h_4^{10} \neq 0, \varepsilon \in A\} \rangle) \geq 3, \ \forall a^{(i)} \in A, \quad (8.22)$$

where $\langle \cdot \rangle$ denotes the span of a set.

Now we prove $D_{\alpha^{(1)}} D_{\alpha^{(2)}} h_4^{10} \neq 0$. There are two cases to be considered.

1. For $||S|| \leq 3$ or $||T|| \leq 3$, from (8.22), we must two vectors $\alpha^{(1)} \in S$ and $\alpha^{(2)} \in T$ such that $D_{\alpha^{(1)}} D_{\alpha^{(2)}} h_4^{10} \neq 0$ since $D_\alpha D_\alpha h_4^{10} = 0$ for any $\alpha \in \mathbb{F}_2^{10}$.

2. Let $||S|| = 4$ (resp. 5) and $||T|| = 6$ (resp. 5). There are also two cases to be considered. Since r-ind$(h_4^{10}) = 4$, without loss of generality, let U be a 4-dimensional subspace of $\mathbb{F}_2^{10}$ such that $D_{a^{(1)}} D_{a^{(2)}} h_4^{10} = constant$, for any $a^{(1)}, a^{(2)} \in U$. From Definitions 8.1.2, and 8.1.3, there exist $a^{(1)}, a^{(2)} \in U \cup (\alpha^{(2)} \oplus U)$ for any $\alpha^{(2)} \in \mathbb{F}_2^{10} \setminus U$ such that $D_{a^{(1)}} D_{a^{(2)}} h_4^{10} \neq constant$.

   (a) When either $U \subseteq \langle S \rangle$ or $U \subseteq \langle T \rangle$, using Definitions 8.1.2 and 8.1.3, we can find two vectors $\alpha^{(1)} \in S$ and $\alpha^{(2)} \in T$ such that $D_{\alpha^{(1)}} D_{\alpha^{(2)}} h_{10} \neq 0$.

   In fact, for any $\alpha^{(2)} \in \mathbb{F}_2^{10} \setminus U$, there must exist one vector $\alpha^{(1)} \in U$ such that $D_{\alpha^{(1)}} D_{\alpha^{(2)}} h_{10} \neq 0$ since

$$D_{\alpha^{(1)}} D_{\alpha^{(2)}} h_4^{10} = D_{\alpha^{(1)}} D_{\alpha^{(1)} \oplus \alpha^{(2)}} h_4^{10} = D_{\alpha^{(2)}} D_{\alpha^{(1)} \oplus \alpha^{(2)}} h_4^{10}.$$

   (b) When $U \nsubseteq \langle S \rangle$ and $U \nsubseteq \langle T \rangle$, we know $||S|| = 4$ (resp. 5) and $||T|| = 6$ (resp. 5). Further, $||U \cup \langle S \rangle|| < 2^4$ and $||U \cup \langle T \rangle|| < 2^4$. Hence, we can find two vectors $\alpha^{(1)} \in S$ and $\alpha^{(2)} \in T$ such that $D_{\alpha^{(1)}} D_{\alpha^{(2)}} h_4^{10} \neq 0$.

□

Theorem 8.2.14. *For $n = 10$, and even $m \geq 6$ such that $m \neq 8$, let h be defined as in Theorem 8.2.6. Then, h is a homogeneous non-decomposable cubic bent function in $m + 10$ variables without affine derivatives outside $\mathcal{M}^\#$.*

Proof. From Theorem 8.2.6, $h \in \mathcal{B}_{m+10}$ is a homogeneous cubic bent function without affine derivatives outside $\mathcal{M}^\#$.

It remains to prove that h is non-decomposable. From Lemma 8.2.12, we need to show that for arbitrary integer p with $1 \leq p \leq m+10-1$, any p-dimensional linear subspace W of $\mathbb{F}_2^{n+m}$ and its arbitrary complementary subspace U in $\mathbb{F}_2^{n+m}$, there always exists two vectors $(a^{(w)}, b^{(w)}) \in W$ and $(a^{(u)}, b^{(u)}) \in U$, such that

$$D_{(a^{(w)}, b^{(w)})} D_{(a^{(u)}, b^{(u)})} h \neq 0,$$

where $a^{(w)}, a^{(u)} \in \mathbb{F}_2^n$ and $b^{(w)}, b^{(u)} \in \mathbb{F}_2^m$. Similarly to (8.11), we have

$$\begin{aligned} & D_{(a^{(w)},b^{(w)})}D_{(a^{(u)},b^{(u)})}h(x,y) \\ = \; & D_{a^{(w)}}D_{a^{(u)}}f_1(x) \oplus D_{b^{(w)}}D_{b^{(u)}}g_1(y) \oplus (f_1 \oplus f_2)(x)D_{b^{(w)}}D_{b^{(u)}}(g_1 \oplus g_2)(y) \\ & \oplus D_{a^{(w)}}(f_1 \oplus f_2)(x)D_{b^{(w)}}(g_1 \oplus g_2)(y) \oplus D_{a^{(u)}}(f_1 \oplus f_2)(x)D_{b^{(u)}}(g_1 \oplus g_2)(y) \\ & \oplus D_{a^{(w)}\oplus a^{(u)}}(f_1 \oplus f_2)(x)D_{b^{(w)}\oplus b^{(u)}}(g_1 \oplus g_2)(y). \end{aligned} \tag{8.23}$$

Since W is a p-dimensional linear subspace of $\mathbb{F}_2^{m+10}$ and U is the complementary subspace of W in $\mathbb{F}_2^{m+10}$, we have

$$\begin{aligned} \langle \{x \mid (x,y) \in W\} \cup \{x \mid (x,y) \in U\} \rangle = \mathbb{F}_2^n, \\ \langle \{y \mid (x,y) \in W\} \cup \{y \mid (x,y) \in U\} \rangle = \mathbb{F}_2^m. \end{aligned} \tag{8.24}$$

Further, for any vector $(a,b) \in \mathbb{F}_2^{n+m}$, we have $(a^{(w)}, b^{(w)}) \in W$ and $(a^{(u)}, b^{(u)}) \in U$ such that $(a,b) = (a^{(w)}, b^{(w)}) \oplus (a^{(u)}, b^{(u)})$.

There are two cases to be considered:

a) For $\{x \mid (x,y) \in W\} = \{0_n\}$, from (8.24), we have $\{x \mid (x,y) \in U\} = \mathbb{F}_2^n$ and $W \subseteq \{0_n\} \times \mathbb{F}_2^m$. Further, we can select $(0_n, b^{(w)}) \in W, (a^{(u)}, b^{(u)}) \in U$ such that $D_{a^{(u)}}(f_1 \oplus f_2) = 1$ (since $\deg(f_1 \oplus f_2) = 1$) and

$$D_{b^{(w)}}D_{b^{(u)}}g_1(y) \oplus D_{b^{(w)}}(g_1 \oplus g_2)(y \oplus b^{(u)}) \neq constant, \tag{8.25}$$

since $g_1 \oplus g_2$ is a bent function (that is, $D_{\beta^{(1)}}(g_1 \oplus g_2)(y) \oplus D_{\beta^{(2)}}(g_1 \oplus g_2)(y) = D_{\beta^{(1)}\oplus\beta^{(2)}}(g_1 \oplus g_2)(y \oplus \beta^{(1)}) \neq constant$ if $\beta^{(1)} \neq \beta^{(2)}$) and $\{x \mid (x,y) \in U\} = \mathbb{F}_2^n$. From (8.23), we have

$$\begin{aligned} & D_{(a^{(w)},b^{(w)})}D_{(a^{(u)},b^{(u)})}h(x,y) \\ = \; & D_{b^{(w)}}D_{b^{(u)}}g_1(y) \oplus (f_1 \oplus f_2)(x)D_{b^{(w)}}D_{b^{(u)}}(g_1 \oplus g_2)(y) \\ & \oplus D_{b^{(w)}}(g_1 \oplus g_2)(y \oplus b^{(u)}) \neq 0. \end{aligned} \tag{8.26}$$

b) For $\{x \mid (x,y) \in U\} = \{0_n\}$, from (8.24), we have $\{x \mid (x,y) \in W\} = \mathbb{F}_2^n$ and $U \subseteq \{0_n\} \times \mathbb{F}_2^m$. Similarly to a), we deduce $D_{(a^{(w)},b^{(w)})}D_{(a^{(u)},b^{(u)})}h(x,y) \neq 0$.

c) When both $\{x|(x,y) \in W\} \neq \{0_n\}$ and $\{x \mid (x,y) \in U\} \neq \{0_n\}$, from Lemma 8.2.13, there exist two vectors $a^{(w)} \in \{x \mid (x,y) \in W\}$ and $a^{(u)} \in \{x \mid (x,y) \in U\}$ such that $D_{a^{(w)}}D_{a^{(u)}}f_1 \neq 0$. Then, there must exist $(a^{(w)}, b^{(w)}) \in W$ and $(a^{(u)}, b^{(u)}) \in U$ such that $b^{(w)} = b^{(u)}$,

since $(a^{(w)} \oplus a^{(u)}, 0_m) \in \mathbb{F}_2^{n+m}$. From (8.23), we have

$$\begin{aligned} & D_{(a^{(w)},b^{(w)})}D_{(a^{(u)},b^{(w)})}h(x,y) \\ = \; & D_{a^{(w)}}D_{a^{(u)}}f_1(x) \oplus D_{b^{(w)}}D_{b^{(w)}}g_1(y) \\ & \oplus (f_1 \oplus f_2)(x)D_{b^{(w)}}D_{b^{(w)}}(g_1 \oplus g_2)(y) \\ & \oplus D_{a^{(w)}}(f_1 \oplus f_2)(x)D_{b^{(w)}}(g_1 \oplus g_2)(y) \\ & \oplus D_{a^{(u)}}(f_1 \oplus f_2)(x)D_{b^{(w)}}(g_1 \oplus g_2)(y) \\ & \oplus D_{a^{(w)}\oplus a^{(u)}}(f_1 \oplus f_2)(x)D_{b^{(w)}\oplus b^{(w)}}(g_1 \oplus g_2)(y) \\ = \; & D_{a^{(w)}}D_{a^{(u)}}f_1(x) \oplus D_{a^{(w)}\oplus a^{(u)}}(f_1 \oplus f_2)(x)D_{b^{(w)}}(g_1 \oplus g_2)(y). \end{aligned} \tag{8.27}$$

There are two cases to be considered:

i) If $D_{a^{(w)}\oplus a^{(u)}}(f_1 \oplus f_2) = 0$, then $D_{(a^{(w)},b^{(w)})}D_{(a^{(u)},b^{(w)})}h(x,y) = D_{a^{(w)}}D_{a^{(u)}}f_1(x) \neq 0$.

ii) If $D_{a^{(w)}\oplus a^{(u)}}(f_1 \oplus f_2) = 1$, then $D_{(a^{(w)},b^{(w)})}D_{(a^{(u)},b^{(w)})}h(x,y) = D_{a^{(w)}}D_{a^{(u)}}f_1(x) \oplus D_{b^{(w)}}(g_1 \oplus g_2)(y) \neq 0$ since $g_1 \oplus g_2$ is a bent function.

□

Open problem 8.2.15. [71, Open Problem 5.1] Construct homogeneous cubic bent functions without affine derivatives outside the class $\mathcal{M}^{\#}$ without the use of the direct sum.

Apparently, if h is obtained by using the direct sum of two functions, then h is decomposable. Thus, if h is non-decomposable, then h is a bent function which cannot be represented as a direct sum of two functions on disjoint variable spaces (under an invertible linear transform). The functions constructed by Theorem 8.2.14 are homogeneous cubic bent functions without affine derivatives outside the class $\mathcal{M}^{\#}$ and does not fall into the framework of the direct sum. Hence, we answer positively the open problem above.

8.2.3 Another method of specifying (non-decomposable) cubic bent functions

We now utilize a method of specifying cubic bent functions without affine derivatives specified in [14], suitable to be used in the indirect sum. Before we proceed, recall that the absolute trace function from $\mathbb{F}_{2^k}$ to $\mathbb{F}_2$ is defined as $Tr_1^k(x) = x + x^{2^1} + \cdots + x^{2^{k-1}}$.

Lemma 8.2.16. *[14] Let $m = 2t$ be an even integer $m \geq 6, m \neq 8$, and let j be an integer such that $1 \leq j < t$ and $\gcd(2^j + 1, 2^t - 1) = 1$. The cubic bent function g on $\mathbb{F}_2^m$ defined by $g(z,w) = Tr_1^t(zw^{2^j+1})$ has no affine derivatives.*

This approach can be embedded in the indirect sum method so that the resulting bent functions are without affine derivatives and additionally do not belong to $\mathcal{M}^{\#}$.

Theorem 8.2.17. *Let $n, m = 2t$ be two even integers $n \geq 10, m \geq 6$ and $m \neq 8$ (due to Lemma 8.2.16). Let $1 \leq j < t$ such that $\gcd(2^j + 1, 2^t - 1) = 1$. Let f be a cubic function on $\mathbb{F}_2^n$ without affine derivatives such that r-ind$(f) < n/2$. Define a cubic function g on $\mathbb{F}_2^m$ as $g(z, w) = Tr_1^t(zw^{2^j+1})$ and let the function h on $\mathbb{F}_2^{n+m}$ be given as*

$$h(x, z, w) = f(x) + g(z, w) + Tr_1^n(ax)\left(Tr_1^t(zw^{2^j+1}) + Tr_1^t((z + c)w^{2^j+1})\right),$$

where $x \in \mathbb{F}_{2^n}, z, w \in \mathbb{F}_{2^t}$ and $c \in \mathbb{F}_{2^t} \setminus \{0\}$. Then, h is a cubic bent function without affine derivatives outside $\mathcal{M}^{\#}$.

Proof. From Lemma 8.2.16, we know that g is a bent function in m variables. Set $f'(x) = f(x) + Tr_1^n(ax)$ and $g'(z, w) = g(z, w) + (g(z, w) + g(z + c, w)) = g(z + c, w)$. Then, f' and g' are bent. Corollary 8.1.10 implies that h is a cubic bent function.

By Lemma 8.2.16, g has no affine derivatives. Similarly to the proof of Theorem 8.2.2, one can show that h has no affine derivatives.

Furthermore, r-ind$(f) < n/2$ and $\deg(f + f') = 1$. By Theorem 8.2.2, using the fact that r-ind$(f) < n/2$, h is outside $\mathcal{M}^{\#}$. □

Remark 8.2.18. Theorem 8.2.17 provides a generic construction of cubic bent functions on $\mathbb{F}_2^k$ (with $k = n + m$) without affine derivatives and outside $\mathcal{M}^{\#}$, for even $k \geq 16$ with $k \neq 18$. However, these bent functions are not necessarily homogeneous. A similar approach, based on Lemma 8.2.16 above, was considered by Mandal *et al.* in [51] but without the condition that resulting bent functions are outside $\mathcal{M}^{\#}$.

Nevertheless, referring to the above remark, by selecting $f = h_4^{10}$ the function h in Theorem 8.2.17 is a non-decomposable cubic bent function without affine derivatives outside $\mathcal{M}^{\#}$, see also Section 8.2.2.

In [71], the series of existence results about cubic bent functions with nice cryptographic properties were presented.

Theorem 8.2.19. *[71, Theorem 4.9] On $\mathbb{F}_2^n$ there exist:*

1. *Cubic bent functions outside $\mathcal{M}^{\#}$ for all $n \geq 10$.*
2. *Cubic bent functions without affine derivatives outside $\mathcal{M}^{\#}$ for all $n \geq 26$.*
3. *Homogeneous cubic bent functions outside $\mathcal{M}^{\#}$ for all $n \geq 26$.*
4. *Homogeneous cubic bent functions without affine derivatives outside $\mathcal{M}^{\#}$ for all $n \geq 50$.*

According to Corollary 8.2.4 and Theorem 8.2.17, we substantially improve the above results in terms of decreased variable spaces by provide new instances of (homogenous) cubic bent functions having additional properties (not having affine derivatives and being outside $\mathcal{M}^{\#}$).

Theorem 8.2.20. *On $\mathbb{F}_2^n$ there exist:*

1. *Cubic bent functions outside $\mathcal{M}^{\#}$ for all $n \geq 10$.*
2. *(Non-decomposable) cubic bent functions without affine derivatives outside $\mathcal{M}^{\#}$ for all $n \geq 20$.*
3. *Homogeneous non-decomposable cubic bent functions outside $\mathcal{M}^{\#}$ for all $n \geq 20$.*
4. *Homogeneous non-decomposable cubic bent functions without affine derivatives outside $\mathcal{M}^{\#}$ for all $n \geq 20$.*

Proof. We know that h_4^{10} is a homogeneous cubic bent function without affine derivatives outside $\mathcal{M}^{\#}$. From Theorem 8.1.5, we know cubic bent functions outside $\mathcal{M}^{\#}$ in n variables can be obtained for $n \geq 10$, thus Case 1 holds. Theorems 8.2.14 and 8.2.17 support Case 2., whereas Theorem 8.2.14 implies that Cases 3 and 4 hold. □

Let "(H)CBF" denote "(homogeneous) cubic bent functions"' and "wAD" denote "without affine derivatives". To give a better overview and comparison of the results in this paper with those in [71], we present the following table:

Function	[71] $n \geq$	Missing n	$n \geq$	Missing n
CBF outside $\mathcal{M}^{\#}$	10	-	10	-
CBFwAD outside $\mathcal{M}^{\#}$	26	14, 18* , 24	20	14, 18
HCBF outside $\mathcal{M}^{\#}$	26	12, 14, 18, 24	20	12, 14, 18
HCBFwAD outside $\mathcal{M}^{\#}$	50	12, 14, 16, 18, 24, 26, 28, 38, 48	20	12, 14, 18

Table 8.1: Comparison of bounds for the dimension n obtained in [71] with our results. The entry denoted 18* is the correct value instead of 16 stated in [71].

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

Constructing vectorial bent functions whose all nonzero component functions are outside $\mathcal{M}^{\#}$, named strongly outside $\mathcal{M}^{\#}$ in [66], is considered to be a difficult problem.

Below we use the indirect sum in connection to Theorem 8.1.11 to show the existence of these objects for relatively large output dimensions.

Theorem 8.3.1. *Let $F : \mathbb{F}_2^{2n} \to \mathbb{F}_2^n$ and $G : \mathbb{F}_2^{2m} \to \mathbb{F}_2^m$ be two vectorial bent functions, with $n < m$, whose coordinate representations are $F =$*

$(f_0, \ldots, f_{n-1})$ and $G = (g_0, \ldots, g_n, \ldots, g_{m-1})$, respectively. We set

$$h_i(x, y) = f_i(x) \oplus g_i(y) \oplus (f_i \oplus f_{(i+1) \mod n})(x) g_n(y), \tag{8.28}$$

where $i = 0, 1, \ldots, n-1$. Then, $H = (h_0, h_1, \ldots, h_{n-1})$ is a bent $(2(n+m), n)$-function, i.e. $H : \mathbb{F}_2^{2(n+m)} \to \mathbb{F}_2^n$ is vectorial bent. Furthermore, the $(2(n+m), n-1)$-function $H' = (h_0, h_1, \ldots, h_{n-2})$ is strongly outside $\mathcal{M}^{\#}$.

Proof. We first prove any h_i is a bent function in $n+m$ variables. We know that $f_i, f_{(i+1) \mod n}$ are bent. From Corollary 8.1.10, h_i is bent if g_i and $g_i \oplus g_n$ are bent. Note, that $g_n = g_i \oplus (g_i \oplus g_n)$. Since G is vectorial bent, it follows that h_i is bent.

Let $0 \neq c \in \mathbb{F}_2^{n+m}$ be arbitrary and let us consider the bentness of the component $c \cdot H$. We have:

$$\begin{aligned}
c \cdot H = \; & c \cdot (h_0, h_1, \ldots, h_{n-1})(x, y) \\
= \; & (c_0 h_0 \oplus c_1 h_1 \oplus \cdots \oplus c_{n-1} h_{n-1})(x, y) \\
= \; & (c_0 f_0 \oplus c_1 f_1 \oplus \cdots \oplus c_{n-1} f_{n-1})(x) \\
& \oplus (c_0 g_0 \oplus c_1 g_1 \oplus \cdots \oplus c_{n-1} g_{n-1})(y) \\
& \oplus (c_0(f_0 \oplus f_1) \oplus c_1(f_1 \oplus f_2) \oplus \cdots \oplus c_{n-1}(f_{n-1} \oplus f_0))(x) g_n(y) \\
= \; & (c \cdot F)(x) \oplus (c \cdot G')(y) \oplus (c \cdot F \oplus c \cdot F')(x) g_n(y) \\
= \; & (c \cdot F)(x) \oplus (c \cdot G')(y) \\
& \oplus (c \cdot F \oplus c \cdot F')(x)(c \cdot G' \oplus (c \cdot G' \oplus g_n))(y),
\end{aligned} \tag{8.29}$$

where $G' = (g_0, \ldots, g_{n-1})$ and $F' = (f_1, \ldots, f_{n-1}, f_0)$. We know that $c \cdot F$, $c \cdot F'$, $c \cdot G'$ and $c \cdot G' \oplus g_n$ are bent, as F and G are vectorial bent. Thus, from Corollary 8.1.10, it follows that $c \cdot H'$ is also bent, for all $0 \neq c \in \mathbb{F}_2^{n+m}$. In other words, H is a bent $(2(n+m), n)$-function.

If $c \notin \{0_n, 1_n\}$, then the function $c \cdot F \oplus c \cdot F'$ is bent. We also know that g_n is bent. Hence, from Theorem 8.1.11, the function $c \cdot (h_0, h_1, \ldots, h_{n-1})$ is outside $\mathcal{M}^{\#}$ for $c \in \mathbb{F}_2^n \backslash \{0_n, 1_n\}$ and consequently, $H' = (h_0, h_1, \ldots, h_{n-2})$ is a bent $(2(n+m), n-1)$-function strongly outside $\mathcal{M}^{\#}$. □

Remark 8.3.2. Since G is vectorial bent, the function g_n in (8.28) can be replaced by $d \cdot (g_n, g_{n+1}, \ldots, g_{m-1})$, where $d \in \mathbb{F}_2^{m-n} \backslash \{0_{m-n}\}$.

For $n = m$, from Theorem 8.3.1, we have the following corollary.

Corollary 8.3.3. *Let $F, G : \mathbb{F}_2^{2n} \to \mathbb{F}_2^n$ be two vectorial bent functions, whose coordinate representations are $F = (f_0, \ldots, f_{n-1})$ and $G = (g_0, \ldots, g_{n-1})$, respectively. We set*

$$h_i(x, y) = f_i(x) \oplus g_i(y) \oplus (f_i \oplus f_{i+1})(x) g_{n-1}(y), \; x, y \in \mathbb{F}_2^{2n}, \tag{8.30}$$

where $i = 0, 1, \ldots, n-2$. *Then,* $H' = (h_0, h_1, \ldots, h_{n-2})$ *is a vectorial bent function, where* $H' : \mathbb{F}_2^{4n} \to \mathbb{F}_2^{n-1}$, *and it is strongly outside* $\mathcal{M}^{\#}$.

Example 8.3.4. Let us consider the functions $F(x, y) = xy$ and $G(x, y) = xy^5$, where $x, y \in \mathbb{F}_{2^3}$. From Corollary 8.3.3, the function $H = (h_0, h_1)$, where h_i is defined with (8.30), is a bent $(12, 2)$-function strongly outside $\mathcal{M}^{\#}$.The `base64` representations of h_0 and h_1 are (9.5) and (9.6), which can be found in the appendix. Additionally, the bentness of H and its exclusion from $\mathcal{M}^{\#}$ have been confirmed using Sage.

8.3.1 A generic construction using companion matrices

We now employ the indirect sum and primitive polynomials in the design of vectorial bent functions strongly outside $\mathcal{M}^{\#}$. It is well-known that if $p(z) = z^m + a_{m-1}z^{m-1} + \ldots + a_1 z + 1$, $a_i \in \mathbb{F}_2$ is a primitive polynomial over the field $\mathbb{F}_2$ (which implies that $wt((a_1, \ldots, a_{m-1}))$ is odd), then its order is equal to $2^m - 1$. The companion matrix $\mathbf{A}$ of $p(z)$ is

$$\mathbf{A} = \begin{bmatrix} 0 & 0 & \ldots & 0 & 1 \\ 1 & 0 & \ldots & 0 & a_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & a_{m-1} \end{bmatrix}.$$

Thus, we have $\mathbf{A}^i \neq \mathbf{A}^j$ for $0 \leq i < j \leq 2^m - 2$. Theorem 8.3.1 then induces the following generic construction of vectorial bent functions that are strongly outside $\mathcal{M}^{\#}$.

Theorem 8.3.5. *Let* n, m *be two positive integers such that* $n < m$. *Let* π *and* ϕ *be two arbitrary permutations in* n *and* m *variables, respectively. Let*

$$f_i(x^{(1)}, x^{(2)}) = \mathbf{A}^i \pi(x^{(2)}) \cdot x^{(1)}, \quad g_j(y^{(1)}, y^{(2)}) = \mathbf{B}^j \phi(y^{(2)}) \cdot y^{(1)}, \\ x^{(1)}, x^{(2)} \in \mathbb{F}_2^n, y^{(1)}, y^{(2)} \in \mathbb{F}_2^m, \tag{8.31}$$

where $i = 0, 1, \ldots, n-1, j = 0, 1, \ldots m-1$, *and* $\mathbf{A}, \mathbf{B}$ *be companion matrices of the corresponding primitive polynomials over* $\mathbb{F}_2$ *of degree* n *and* m, *respectively. Let* $F : \mathbb{F}_2^{2n} \to \mathbb{F}_2^n$ *and* $G : \mathbb{F}_2^{2m} \to \mathbb{F}_2^m$ *be two vectorial bent functions, whose coordinate representations are* $F = (f_0, \ldots, f_{n-1})$ *and* $G = (g_0, \ldots, g_n, \ldots, g_{m-1})$, *respectively. Let* h_i *be defined by (8.28). Then,* $H = (h_0, h_1, \ldots, h_{n-1})$ *is a bent* $(2(n+m), n)$*-function. Further, the* $(2(n+m), n-1)$*-function* $H' = (h_0, h_1, \ldots, h_{n-2})$ *is strongly outside* $\mathcal{M}^{\#}$.

Proof. Since $\mathbf{A}, \mathbf{B}$ are companion matrices of the corresponding primitive polynomials over $\mathbb{F}_2$ of degree n and m, respectively, we conclude that $\bigoplus_{i=0}^{n-1} \lambda_i \mathbf{A}^i \pi(x^{(2)})$ and $\bigoplus_{j=0}^{m-1} \lambda_j \mathbf{B}^j \phi(y^{(2)})$ are also permutations in n and m variables, respectively. Hence, F and G are two vectorial bent

functions. From Theorem 8.3.1, H is a bent $(2(n+m), n)$-function and the $(2(n+m), n-1)$-function $H' = (h_0, \ldots, h_{n-2})$ is strongly outside $\mathcal{M}^{\#}$. □

In difference to [66], where the output dimension of this class of vectorial bent functions was only two, the value $n-1$ is a significant improvement. It can be easily verified that $(2(n+m), n-1)$ functions provide a larger output dimension compared to $(n, n/6)$ functions (also strongly outside $\mathcal{M}^{\#}$) recently specified in Section 6.1.2. Notice, however, that the maximal output dimension of a vectorial bent function in $2(n+m)$ variables is $n+m$. Therefore, our approach still does not provide vectorial bent functions strongly outside $\mathcal{M}^{\#}$ with maximal output dimension. The existence of these objects still remains unknown.

Chapter 9

Conclusions

The results of this PhD thesis represent a significant contribution to a number of standing open problems in cryptography, which have been an active topic in the mathematical community for the last five decades.

A major part of the thesis deals with the construction of (vectorial) bent functions outside the completed Maiorana-McFarland class using different methods. We note that all the examples have been confirmed to be outside $\mathcal{M}^{\#}$ using the mathematical software `Sage` and an algorithm developed by us using the notion of cliques in graphs.

The (P_U) property was generalized to obtain a construction method for vectorial bent functions, which covers the previous two methods in [82, 90]. Using this construction we also provided new instances of vectorial functions having maximal number of bent components. Similarly, these results were extended to the p-ary case to develop secondary constructions of p-ary weakly regular bent (n, m)-functions.

By combining the indicators of $\mathcal{C}$ and $\mathcal{D}_0$, and $\mathcal{C}$ and $\mathcal{D}$ we obtained new superclasses of bent functions, $\mathcal{SC}$ and $\mathcal{CD}$, respectively. For both classes we provided conditions under which these functions lie outside $\mathcal{M}^{\#}$. We observed that these classes have many applications. Most notably, in the construction of vectorial bent functions weakly/strongly/almost strongly outside $\mathcal{M}^{\#}$. We note that our instances of vectorial bent functions strongly outside $\mathcal{M}^{\#}$ have the largest (though not maximal) output space in the literature. These functions were also useful in the construction of (n, m)-MNBC functions outside $\mathcal{M}^{\#}$. We also gave a complete classification of MNBC functions in six variables.

The fact that a bent function f is in/outside $\mathcal{M}^{\#}$ if and only if its dual is in/outside $\mathcal{M}^{\#}$ is employed in the so-called 4-decomposition of a bent function on $\mathbb{F}_2^n$, which was originally considered by Canteaut and Charpin [14] in terms of the second-order derivatives and later reformulated in [39] in terms of the duals of its restrictions to the cosets of an $(n-2)$-dimensional subspace V. For each of the three possible cases of this 4-decomposition of a bent function, we provide generic methods

for designing bent functions provably outside $\mathcal{M}^{\#}$. For instance, for the elementary case of defining a bent function $h(x, y_1, y_2) = f(x) \oplus y_1 y_2$ on $\mathbb{F}_2^{n+2}$ using a bent function f on $\mathbb{F}_2^n$, we show that h is outside $\mathcal{M}^{\#}$ if and only if f is outside $\mathcal{M}^{\#}$. This approach is then generalized to the case when two bent functions are used. More precisely, the concatenation $f_1||f_1||f_2||(1 \oplus f_2)$ also gives bent functions outside $\mathcal{M}^{\#}$ if either f_1 or f_2 is outside $\mathcal{M}^{\#}$. The cases when the four restrictions of a bent function are semi-bent or 5-valued spectra functions are also considered and several design methods of designing infinite families of bent functions outside $\mathcal{M}^{\#}$, using the spectral domain design considered in [37, 39], are proposed.

Two well-known secondary constructions of bent functions are the direct and indirect sum methods. We show that the direct sum, under more relaxed conditions compared to those in [71], can generate bent functions provably outside the completed Maiorana-McFarland class ($\mathcal{M}^{\#}$). We also show that the indirect sum method, though imposing certain conditions on the initial bent functions, can be employed in the design of bent functions outside $\mathcal{M}^{\#}$. Furthermore, applying this method to suitably chosen bent functions we construct several generic classes of homogenous cubic bent functions (considered as a difficult problem) that might posses additional properties (namely without affine derivatives and/or outside $\mathcal{M}^{\#}$). Our results significantly improve upon the best known instances of this type of bent functions given by Polujan and Pott [71], and additionally we solve an open problem in [71, Open Problem 5.1]. More precisely, we show that one class of our homogenous cubic bent functions is non-decomposable (inseparable) so that h under a non-singular transform B cannot be represented as $h(xB) = f(y) \oplus g(z)$. Finally, we provide a generic class of vectorial bent functions strongly outside $\mathcal{M}^{\#}$ of relatively large output dimensions, which is generally considered as a difficult task.

The basic tools used in the research range from combinatorial to algebraic cryptographic methods. In addition, we used the mathematical software `Sage`, `Wolfram Mathematica` and the Computational Algebra System Magma to confirm our hypothesizes. The list of `Sage` codes developed throughout the writing of the thesis can be found on `https://kripto.famnit.upr.si/sage/`.

Bibliography

[1] D. C. Adams. The CAST-128 Encryption Algorithm. RFC 2144, May 1997.

[2] N. Anbar, T. Kalaycı, and W. Meidl. Analysis of (n, n)-functions obtained from the Maiorana-McFarland class. *IEEE Transactions on Information Theory*, 67(7):4891–4901, 2021.

[3] N. Anbar, T. Kalaycı, W. Meidl and L. Mérai. On a Class of Functions With the Maximal Number of Bent Components. *IEEE Transactions on Information Theory*, 68(9):6174–6186, 2022

[4] A. Bapić and E. Pasalic. A new method for secondary constructions of vectorial bent functions. *Designs, Codes and Cryptography*, 89(11):2463–2475, 2021.

[5] A. Bapić and E. Pasalic. Constructions of (vectorial) bent functions outside the completed Maiorana–McFarland class. *Discrete Applied Mathematics*, 314:197–212, 2022.

[6] A. Bapić, E. Pasalic, A. Polujan, and A. Pott. Vectorial boolean functions with the maximum number of bent components outside the $\mathcal{M}^{\#}$ class. In *Proceedings of the Twelfth International Workshop on Coding and Cryptography*, 2022.

[7] A. Bapić, E. Pasalic, F. Zhang, and S. Hodžić. Constructing new superclasses of bent functions from known ones. *Cryptography and Communications*, pages 1–28, 2022.

[8] A. Bernasconi and B. Codenotti. Spectral analysis of boolean functions as a graph eigenvalue problem. *IEEE Transactions on Computers*, 48(3):345 – 351, 1999. Cited by: 60.

[9] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe. Present: An ultra-lightweight block cipher. In P. Paillier and I. Verbauwhede, editors, *Cryptographic Hardware and Embedded Systems - CHES 2007*, pages 450–466, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg.

[10] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[11] L. Budaghyan and C. Carlet. On CCZ-equivalence and its use in secondary constructions of bent functions. In *Preproceedings of the International Workshop on Coding and Cryptography, WCC 2009*, pages 19–36, Ullensvang, Norway, 2009.

[12] L. Budaghyan and C. Carlet. Ccz-equivalence of bent vectorial functions and related constructions. *Des. Codes Cryptogr.*, 59(1-3):69–87, 2011.

[13] L. Budaghyan, T. Helleseth, N. Li, and B. Sun. Some results on the known classes of quadratic apn functions. In S. El Hajji, A. Nitaj, and E. M. Souidi, editors, *Codes, Cryptology and Information Security*, pages 3–16, Cham, 2017. Springer International Publishing.

[14] A. Canteaut and P. Charpin. Decomposing bent functions. *IEEE Trans. Inf. Theory*, 49(8):2004–2019, 2003.

[15] A. Canteaut, M. Daum, H. Dobbertin, and G. Leander. Finding nonnormal bent functions. *Discret. Appl. Math.*, 154(2):202–218, 2006.

[16] C. Carlet. Partially-bent functions. *Des. Codes Cryptogr.*, 3(2):135–145, 1993.

[17] C. Carlet. Two new classes of bent functions. In T. Helleseth, editor, *Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings*, volume 765 of *Lecture Notes in Computer Science*, pages 77–101. Springer, 1993.

[18] C. Carlet. On the secondary constructions of resilient functions. In *International Symposium on Information Theory, 2004. ISIT 2004. Proceedings.*, pages 547–547, 2004.

[19] C. Carlet, editor. *Boolean Functions for Cryptography and Coding Theory*. Cambridge University Press, 2020.

[20] C. Carlet, P. Charpin, and V. A. Zinoviev. Codes, bent functions and permutations suitable for des-like cryptosystems. *Des. Codes Cryptogr.*, 15(2):125–156, 1998.

[21] C. Carlet and S. Mesnager. On dillon's class H of niho bent functions and o-polynomials. In *International Symposium on Artificial Intelligence and Mathematics, ISAIM 2012, Fort Lauderdale, Florida, USA, January 9-11, 2012*, 2012.

[22] C. Carlet, F. Zhang, and Y. Hu. Secondary constructions of bent functions and their enforcement. *Advances in Mathematics of Communications*, 6(3):305–314, 2012.

[23] A. Çesmelioglu, W. Meidl, and I. Pirsic. Vectorial bent functions and partial difference sets. *Des. Codes Cryptogr.*, 89(10):2313–2330, 2021.

[24] T. Cusick and P. Stănică. *Cryptographic Boolean Functions and Applications: Second edition.* Elsevier, 2017.

[25] J. Daemen and V. Rijmen. Aes proposal: Rijndael, 1999.

[26] C. De Cannière. Trivium: A stream cipher construction inspired by block cipher design principles. In S. K. Katsikas, J. López, M. Backes, S. Gritzalis, and B. Preneel, editors, *Information Security*, pages 171–186, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg.

[27] P. Delsarte. *An algebraic approach to the association schemes of coding theory.* PhD thesis, Universite Catholique de Louvain,, 1973.

[28] J. F. Dillon. A survey of bent functions. *NSA Tech J*, pages 191–215, 1972.

[29] J. F. Dillon. *Elementary Hadamard Difference Sets.* PhD thesis, University of Maryland, 1974.

[30] H. Dobbertin. Construction of bent functions and balanced boolean functions with high nonlinearity. In B. Preneel, editor, *Fast Software Encryption: Second International Workshop. Leuven, Belgium, 14-16 December 1994, Proceedings*, volume 1008 of *Lecture Notes in Computer Science*, pages 61–74. Springer, 1994.

[31] D. Dong, X. Zhang, L. Qu, and S. Fu. A note on vectorial bent functions. *Inf. Process. Lett.*, 113(22-24):866–870, 2013.

[32] Y. Edel and A. Pott. On the equivalence of nonlinear functions. In B. Preneel, S. M. Dodunekov, V. Rijmen, and S. Nikova, editors, *Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes*, volume 23 of *NATO Science for Peace and Security Series - D: Information and Communication Security*, pages 87–103. IOS Press, 2009.

[33] G. Effinger and G. Mullen. *Elementary Number Theory.* CRC Press, 2021.

[34] P. Ekdahl and T. Johansson. Snow - a new stream cipher. In *PROCEEDINGS OF FIRST OPEN NESSIE WORKSHOP, KU-LEUVEN*, 2000.

[35] M. Hell, T. Johansson, and W. Meier. Grain - a stream cipher for constrained environments. estream, ecrypt stream cipher. Technical report, 2005/010, ECRYPT (European Network of Excellence for Cryptology, 2005.

[36] T. Helleseth and A. Kholosha. Monomial and quadratic bent functions over the finite fields of odd characteristic. *IEEE Trans. Inf. Theory*, 52(5):2018–2032, 2006.

[37] S. Hodzic, E. Pasalic, and Y. Wei. A general framework for secondary constructions of bent and plateaued functions. *Des. Codes Cryptogr.*, 88(10):2007–2035, 2020.

[38] S. Hodžić, E. Pasalic, Y. Wei, and F. Zhang. Designing plateaued boolean functions in spectral domain and their classification. *IEEE Transactions on Information Theory*, 65(9):5865–5879, 2019.

[39] S. Hodžić, E. Pasalic, and W. Zhang. Generic constructions of five-valued spectra boolean functions. *IEEE Transactions on Information Theory*, 65(11):7554–7565, 2019.

[40] R. J. Jenkins. Isaac. In *Proceedings of the Third International Workshop on Fast Software Encryption*, page 41–49, Berlin, Heidelberg, 1996. Springer-Verlag.

[41] S. Kavut, S. Maitra, and M. D. Yucel. Search for boolean functions with excellent profiles in the rotation symmetric class. *IEEE Transactions on Information Theory*, 53(5):1743–1751, 2007.

[42] A. Kerckhoffs. La cryptographie militaire. *Journal des Sciences Militaires*, pages 161–191, 1883.

[43] A. M. Kerdock. A class of low-rate nonlinear binary codes. *Inf. Control.*, 20:182–187, 1972.

[44] S. Kudin and 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*, 2022.

[45] S. Kudin, E. Pasalic, N. Cepak, and F. Zhang. Permutations without linear structures inducing bent functions outside the completed maiorana-mcfarland class. *Cryptography and Communications*, 14, 2022.

[46] G. M. Kyureghyan and A. Pott. Some theorems on planar mappings. In J. von zur Gathen, J. L. Imaña, and Ç. K. Koç, editors, *Arithmetic of Finite Fields*, pages 117–122, Berlin, Heidelberg, 2008. Springer Berlin Heidelberg.

[47] X. Lai and J. L. Massey. A proposal for a new block encryption standard. In I. B. Damgård, editor, *Advances in Cryptology – EUROCRYPT '90*, pages 389–404, Berlin, Heidelberg, 1991. Springer Berlin Heidelberg.

[48] P. Langevin and G. Leander. Counting all bent functions in dimension eight 99270589265934370305785861242880. *Des. Codes Cryptogr.*, 59(1-3):193–205, 2011.

[49] S. Liu and J. J. Komo. Nonbinary kasami sequences over gf(p). *IEEE Trans. Inf. Theory*, 38(4):1409–1412, 1992.

[50] S. Maitra and P. Sarkar. Maximum nonlinearity of symmetric boolean functions on odd number of variables. *IEEE Transactions on Information Theory*, 48(9):2626–2630, 2002.

[51] B. Mandal, S. Gangopadhyay, and P. Stănică. Cubic maiorana-mcfarland bent functions with no affine derivative. *International*

Journal of Computer Mathematics: Computer Systems Theory, 2:1–15, 2017.

[52] B. Mandal, P. Stanica, and S. Gangopadhyay. New classes of p-ary bent functions. *Cryptogr. Commun.*, 11(1):77–92, 2019.

[53] B. Mandal, P. Stănică, S. Gangopadhyay, and E. Pasalic. An analysis of the $\mathcal{C}$ class of bent functions. *Fundamenta Informaticae*, 146:271–292, 2016.

[54] M. Matsui. Linear cryptanalysis method for des cipher. In *Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology*, EUROCRYPT '93, pages 386—397, Berlin, Heidelberg, 1994. Springer-Verlag.

[55] R. L. McFarland. A family of difference sets in non-cyclic groups. *J. Comb. Theory, Ser. A*, 15(1):1–10, 1973.

[56] W. Meidl, A. A. Polujan, and A. Pott. Linear codes and incidence structures of bent functions and their generalizations. *ArXiv*, abs/2012.06866, 2020.

[57] S. Mesnager. Several new infinite families of bent functions and their duals. *IEEE Trans. Inf. Theory*, 60(7):4397–4407, 2014.

[58] S. Mesnager. Bent vectorial functions and linear codes from o-polynomials. *Des. Codes Cryptogr.*, 77(1):99–116, 2015.

[59] S. Mesnager. *Bent Functions - Fundamentals and Results*. Springer, 2016.

[60] S. Mesnager, F. Zhang, C. Tang, and Y. Zhou. Further study on the maximum number of bent components of vectorial functions. *Designs, Codes and Cryptography*, 87:2597–2610, 2019.

[61] A. Muratović-Ribić, E. Pasalic, and S. Bajrić. Vectorial bent functions from multiple terms trace functions. *IEEE Transactions on Information Theory*, 60:1337–1347, 2014.

[62] A. Muratović-Ribić, E. Pasalic, and S. Bajrić. Vectorial hyperbent trace functions from the $\mathcal{PS}_{ap}$ class—their exact number and specification. *IEEE Transactions on Information Theory*, 60:4408–4413, 2014.

[63] K. Nyberg. Perfect nonlinear s-boxes. In D. W. Davies, editor, *Advances in Cryptology - EUROCRYPT '91, Workshop on the Theory and Application of of Cryptographic Techniques, Brighton, UK, April 8-11, 1991, Proceedings*, volume 547 of *Lecture Notes in Computer Science*, pages 378–386. Springer, 1991.

[64] K. Nyberg. S-boxes and round functions with controllable linearity and differential uniformity. In B. Preneel, editor, *Fast Software Encryption: Second International Workshop. Leuven, Belgium, 14-16 December 1994, Proceedings*, volume 1008 of *Lecture Notes in Computer Science*, pages 111–130. Springer, 1994.

[65] E. Pasalic, A. Bapić, F. Zhang, and Y. Wei. Explicit infinite families of bent functions outside $\mathcal{MM}^{\#}$. Cryptology ePrint Archive, Paper 2022/1126, 2022.

[66] E. Pasalic, S. Kudin, A. Polujan, and A. Pott. Vectorial bent-negabent functions - their constructions and bounds. *Submitted*, 2022.

[67] E. Pasalic, F. Zhang, S. Kudin, and Y. Wei. Vectorial bent functions weakly/strongly outside the completed maiorana–mcfarland class. *Discrete Applied Mathematics*, 294:138–151, 2021.

[68] E. Pasalic and W. Zhang. On multiple output bent functions. *Inf. Process. Lett.*, 112(21):811–815, 2012.

[69] A. Polujan and A. Pott. Towards the classification of quadratic vectorial bent functions in 8 variables. In *The 7th International Workshop on Boolean Functions and their Applications*, 2022.

[70] A. A. Polujan. *Boolean and vectorial functions: A design-theoretic point of view*. PhD thesis, Otto-von-Guericke-Universität Magdeburg, 2021.

[71] A. A. Polujan and A. Pott. Cubic bent functions outside the completed Maiorana-McFarland class. *Designs, Codes and Cryptography*, 88(9):1701–1722, 2020.

[72] A. A. Polujan and A. Pott. On design-theoretic aspects of Boolean and vectorial bent functions. *IEEE Transactions on Information Theory*, 67(2):1027–1037, 2021.

[73] A. Pott, E. Pasalic, A. Muratović-Ribić, and S. Bajrić. On the maximum number of bent components of vectorial functions. *IEEE Transactions on Information Theory*, 64(1):403–411, 2018.

[74] Y. Qi, C. Tang, Z. Zhou, and C. Fan. Several infinite families of p-ary weakly regular bent functions. *Adv. Math. Commun.*, 12(2):303–315, 2018.

[75] R. L. Rivest. The rc5 encryption algorithm. In B. Preneel, editor, *Fast Software Encryption*, pages 86–96, Berlin, Heidelberg, 1995. Springer Berlin Heidelberg.

[76] P. Rogaway and D. Coppersmith. A software-optimized encryption algorithm. *Journal of Cryptology*, 11:273–287, 1998.

[77] O. S. Rothaus. On "bent" functions. *J. Comb. Theory, Ser. A*, 20(3):300–305, 1976.

[78] B. Schneier. Description of a new variable-length key, 64-bit block cipher (blowfish). In R. Anderson, editor, *Fast Software Encryption*, pages 191–204, Berlin, Heidelberg, 1994. Springer Berlin Heidelberg.

[79] J. Seberry, T. Xia, and J. Pieprzyk. Construction of cubic homogeneous boolean bent functions. *Australas. J Comb.*, 22:233–246, 2000.

[80] C. E. Shannon. A mathematical theory of communication. *The Bell System Technical Journal*, 27:379–423, 623–656, 1948.

[81] V. M. Sidelnikov. On extremal polynomials used in code size estimation. *Probl. Inform. Transm.*, 16:174–186, 1980.

[82] C. Tang, Z. Zhou, Y. Qi, X. Zhang, C. Fan, and T. Helleseth. Generic construction of bent functions and bent idempotents with any possible algebraic degrees. *IEEE Trans. Inf. Theory*, 63(10):6149–6157, 2017.

[83] N. Tokareva. *Bent Functions: Results and Applications to Cryptography*. Academic Press, Inc., USA, 1st edition, 2015.

[84] Y. Wei, E. Pasalic, F. Zhang, W. Wu, and C. xiang Wang. New constructions of resilient functions with strictly almost optimal nonlinearity via non-overlap spectra functions. *Information Sciences*, 415-416:377–396, 2017.

[85] G. Weng, R. Feng, and W. Qiu. On the ranks of bent functions. *Finite Fields and Their Applications*, 13(4):1096–1116, 2007.

[86] Y. Xu, C. Carlet, S. Mesnager, and C. Wu. Classification of bent monomials, constructions of bent multinomials and upper bounds on the nonlinearity of vectorial functions. *IEEE Trans. Inf. Theory*, 64(1):367–383, 2018.

[87] W. Zhang and E. Pasalic. Highly Nonlinear Balanced S-Boxes With Good Differential Properties. *IEEE Trans. Inf. Theory*, 60(12):7970–7979, 2014.

[88] F. Zhang, N. Cepak, E. Pasalic, and Y. Wei. Further analysis of bent functions from $\mathcal{C}$ and $\mathcal{D}$ which are provably outside or inside $\mathcal{M}^{\#}$. *Discret. Appl. Math.*, 285:458–472, 2020.

[89] F. Zhang, E. Pasalic, N. Cepak, and Y. Wei. Bent functions in C and D outside the completed maiorana-mcfarland class. In S. E. Hajji, A. Nitaj, and E. M. Souidi, editors, *Codes, Cryptology and Information Security - Second International Conference, C2SI 2017, Rabat, Morocco, April 10-12, 2017, Proceedings - In Honor of Claude Carlet*, volume 10194 of *Lecture Notes in Computer Science*, pages 298–313. Springer, 2017.

[90] L. Zheng, H. Kan, J. Peng, and D. Tang. Constructing vectorial bent functions via second-order derivatives. *Discrete Mathematics*, 344(8):112473, 2021.

[91] L. Zheng, J. Peng, H. Kan, L. Jun, and J. Luo. On constructions and properties of (n, m)-functions with maximal number of bent components. *Designs, Codes and Cryptography*, 88:2171–2186, 2020.

[92] L. Zheng, J. Peng, H. Kan, and Y. Li. Several new infinite families of bent functions via second order derivatives. *Cryptography Commun.*, 12(6):1143–1160, 2020.

[93] Y. Zheng, J. Pieprzyk, and J. Seberry. Haval — a one-way hashing algorithm with variable length of output (extended abstract). In J. Seberry and Y. Zheng, editors, *Advances in Cryptology — AUSCRYPT '92*, pages 81–104, Berlin, Heidelberg, 1993. Springer Berlin Heidelberg.

[94] Y. Zheng and X.-M. Zhang. On plateaued functions. *IEEE Transactions on Information Theory*, 47(3):1215–1223, 2001.

[95] Y. Zheng and X.-M. Zhang. Non-separable cryptographic functions. In *International Symposium on Information Theory and Its Applications*, pages 1–5, Honolulu, USA, 2006.

[96] A. Çeşmelioğlu, W. Meidl, and A. Pott. Vectorial bent functions and their duals. *Linear Algebra and its Applications*, 548:305–320, 2018.

Index

4-decomposition
  5-valued, 100
  semi-bent, 100

algebraic degree, 11
algebraic normal form, 10

bent
  regular, 20
  weakly regular, 20
bent function
  $\mathcal{C}$, 16
  $\mathcal{D}$, 16
  $\mathcal{M}$, 14
  $\mathcal{PS}$, 15
  $\mathcal{PS}_{ap}$, 15
  dual, 13
Boolean function, 10
  s-plateaued, 13
  balanced, 10
  derivative, 11
  distance, 10
  nonlinearty, 11
  normal, 60
  semi-bent, 13
  support, 10
  weakly normal, 60

equivalence
  EA, 12

fast point, 134
function
  (n, m)-, 17
  p-ary, 20
  p-ary $(n, m)-$, 21
  component, 18
  coordinate, 18
  MNBC, 32

Hamming
  distance, 9
  weight, 9

linear structure, 17

outside
  almost strongly, 19
  strongly, 19
  weakly, 19

property
  (C), 16
  (P_U), 23

relaxed $\mathcal{M}$-subspace, 125
relaxed linearity index, 125

trace, 10
transform
  inverse Walsh-Hadamard, 12
  generalized Walsh-Hadamard, 20
  Walsh-Hadamard, 12
truth table, 10

Appendix

Sage implementation of Lemma 2.2.4:

```
def is_in_MM(f,n):
s=[];
for a in [1..2^n-1]:
    for b in [a+1..2^n-1]:
        if set(ttab(f.derivative(a).derivative(b)))=={0}:
            s.append([a,b]);
G=Graph();
G.add_edges(s);
cl=list(sage.graphs.cliquer.all_cliques(G,2^(n/2)-1,2^(n/2)-1));
V=VectorSpace(GF(2),n);
V1=sorted(V);
b1=[V.subspace([V1[0]]+[V1[i] for i in s]) for s in cl];
for K in b1:
    if len(K)==2^(n/2):
        return True;
return False;
```

CCZ-inequivalent MNBC functions in six variables

Below we list representatives of CCZ-equivalence classes of MNBC functions in $n = 6$ variables as polynomials $f_i \colon \mathbb{F}_{2^6} \to \mathbb{F}_{2^6}$, where $\mathbb{F}_{2^6}^* = \langle a \rangle$ with $a^6 + a^4 + a^3 + a + 1 = 0$. Note that the representatives f_i of CCZ-equivalence classes $1 \leq i \leq 13$ are univariate representations of the mappings $\mathbf{x} \in \mathbb{F}_2^6 \to (F_i^3(\mathbf{x}), 0)$, where F_i^3 is a vectorial $(6, 3)$-bent function in [72, Table A2(c)] and 0 is the null-vector. For convenience, we sort the representatives of the first 13 CCZ-equivalence classes as in Figure 6.1.

0-step extension:

f_3. $a^8x^{48} + a^{57}x^{40} + a^{13}x^{36} + a^{20}x^{34} + a^3x^{33} + a^{60}x^{32} + a^{47}x^{24} + a^{10}x^{20} + a^{45}x^{18} + a^{59}x^{17} + a^{35}x^{16} + a^{10}x^{12} + a^2x^{10} + a^{48}x^9 + a^{47}x^8 + a^{50}x^6 + a^{55}x^5 + a^{18}x^4 + a^{47}x^3 + a^{25}x$

f_6. $a^{35}x^{56} + a^{21}x^{52} + a^{10}x^{50} + a^{55}x^{49} + a^{41}x^{48} + a^{3}x^{44} + a^{18}x^{42} + a^{50}x^{41} + a^{22}x^{40} + a^{9}x^{38} + a^{20}x^{37} + a^{16}x^{36} + a^{34}x^{35} + a^{48}x^{34} + a^{62}x^{33} + a^{12}x^{32} + a^{26}x^{28} + a^{59}x^{26} + a^{11}x^{24} + a^{51}x^{22} + a^{51}x^{21} + a^{40}x^{20} + a^{46}x^{19} + a^{32}x^{18} + a^{26}x^{17} + a^{50}x^{16} + a^{62}x^{14} + a^{32}x^{13} + a^{7}x^{12} + a^{12}x^{11} + a^{43}x^{10} + a^{30}x^{9} + a^{16}x^{8} + a^{62}x^{7} + a^{2}x^{6} + a^{34}x^{5} + a^{42}x^{3} + a^{23}x^{2} + a^{3}x$

f_7. $a^{58}x^{56} + a^{38}x^{52} + a^{27}x^{50} + a^{59}x^{49} + a^{58}x^{48} + a^{28}x^{44} + a^{16}x^{42} + a^{17}x^{41} + a^{36}x^{40} + a^{23}x^{38} + a^{23}x^{37} + a^{51}x^{36} + a^{25}x^{35} + a^{52}x^{34} + a^{37}x^{33} + a^{21}x^{32} + a^{10}x^{28} + x^{26} + a^{57}x^{25} + a^{16}x^{24} + a^{40}x^{22} + a^{4}x^{21} + a^{14}x^{20} + a^{38}x^{19} + a^{53}x^{18} + a^{45}x^{17} + a^{36}x^{16} + a^{15}x^{14} + a^{46}x^{13} + a^{29}x^{12} + a^{24}x^{11} + a^{39}x^{10} + a^{37}x^{9} + a^{39}x^{8} + a^{50}x^{7} + a^{22}x^{6} + a^{6}x^{5} + a^{46}x^{4} + a^{36}x^{3} + a^{16}x^{2} + x$

f_{13}. $a^{52}x^{56} + a^{42}x^{52} + a^{22}x^{50} + a^{28}x^{49} + a^{21}x^{48} + a^{4}x^{44} + a^{58}x^{42} + a^{57}x^{41} + a^{13}x^{40} + a^{26}x^{38} + a^{6}x^{37} + a^{53}x^{36} + a^{20}x^{35} + a^{51}x^{34} + a^{12}x^{33} + a^{37}x^{32} + a^{53}x^{28} + a^{61}x^{26} + a^{53}x^{25} + a^{50}x^{24} + a^{29}x^{22} + a^{25}x^{21} + a^{14}x^{20} + a^{42}x^{19} + a^{22}x^{18} + a^{24}x^{17} + a^{39}x^{16} + a^{48}x^{14} + a^{30}x^{13} + a^{41}x^{12} + a^{17}x^{11} + a^{41}x^{10} + a^{16}x^{9} + a^{59}x^{8} + a^{23}x^{7} + a^{8}x^{6} + a^{53}x^{5} + a^{15}x^{4} + a^{28}x^{3} + a^{6}x^{2} + a^{46}x$

f_2. $a^{34}x^{48} + a^{58}x^{40} + a^{28}x^{36} + a^{39}x^{34} + a^{14}x^{33} + a^{36}x^{32} + a^{25}x^{24} + a^{24}x^{20} + a^{5}x^{18} + a^{13}x^{17} + a^{17}x^{16} + a^{35}x^{12} + a^{54}x^{10} + a^{14}x^{9} + a^{26}x^{8} + a^{6}x^{6} + a^{6}x^{5} + a^{57}x^{4} + a^{60}x^{3} + a^{50}x^{2} + a^{18}x$

f_{12}. $a^{48}x^{56} + a^{9}x^{52} + a^{41}x^{50} + a^{25}x^{49} + a^{37}x^{48} + a^{38}x^{44} + a^{58}x^{42} + a^{61}x^{41} + a^{5}x^{40} + a^{5}x^{38} + a^{32}x^{37} + a^{58}x^{36} + a^{38}x^{35} + a^{6}x^{34} + a^{13}x^{33} + a^{61}x^{32} + a^{32}x^{28} + a^{23}x^{26} + a^{12}x^{25} + a^{32}x^{22} + a^{25}x^{21} + a^{15}x^{20} + a^{58}x^{19} + a^{34}x^{18} + a^{8}x^{17} + a^{32}x^{16} + a^{35}x^{14} + a^{22}x^{13} + a^{60}x^{12} + a^{47}x^{11} + a^{3}x^{10} + a^{62}x^{9} + a^{54}x^{8} + a^{33}x^{7} + a^{34}x^{6} + a^{34}x^{5} + a^{47}x^{4} + a^{2}x^{3} + a^{25}x^{2} + a^{19}x$

f_4. $a^{19}x^{56} + a^{3}x^{52} + a^{40}x^{50} + a^{36}x^{49} + a^{55}x^{48} + a^{43}x^{44} + a^{44}x^{42} + a^{4}x^{41} + a^{32}x^{40} + a^{10}x^{38} + a^{15}x^{37} + a^{25}x^{36} + a^{7}x^{35} + a^{5}x^{34} + a^{11}x^{33} + a^{21}x^{32} + a^{42}x^{28} + a^{34}x^{26} + a^{21}x^{25} + a^{41}x^{24} + a^{54}x^{22} + a^{23}x^{21} + a^{55}x^{20} + a^{6}x^{19} + a^{39}x^{18} + a^{60}x^{17} + a^{54}x^{16} + a^{22}x^{14} + a^{18}x^{13} + a^{11}x^{12} + a^{28}x^{11} + a^{48}x^{10} + a^{24}x^{9} + a^{56}x^{8} + a^{12}x^{7} + a^{48}x^{6} + a^{34}x^{5} + a^{12}x^{4} + a^{62}x^{3} + a^{20}x^{2} + a^{27}x$

f_1. $a^{42}x^{48} + a^{23}x^{40} + a^{21}x^{36} + a^{27}x^{33} + a^{22}x^{32} + a^{57}x^{24} + a^{7}x^{20} + a^{26}x^{18} + a^{30}x^{17} + a^{30}x^{16} + a^{13}x^{12} + a^{29}x^{10} + a^{35}x^{9} + a^{45}x^{8} + a^{7}x^{6} + a^{14}x^{5} + a^{23}x^{4} + ax^{3} + a^{25}x^{2} + a^{19}x$

f_5. $a^{13}x^{56} + a^{56}x^{52} + a^{28}x^{50} + a^{39}x^{49} + a^{53}x^{48} + a^{25}x^{44} + a^{24}x^{42} + a^{34}x^{41} + a^{27}x^{40} + a^{49}x^{38} + a^{57}x^{37} + a^{16}x^{36} + a^{42}x^{35} + a^{17}x^{34} + a^{30}x^{33} + a^{32}x^{32} + a^{8}x^{28} + a^{61}x^{26} + a^{33}x^{25} + a^{41}x^{24} + a^{14}x^{22} + a^{55}x^{21} + a^{30}x^{20} + a^{2}x^{19} + a^{32}x^{18} + a^{29}x^{17} + a^{26}x^{16} + a^{37}x^{14} + a^{43}x^{13} + a^{56}x^{12} + a^{14}x^{11} + a^{56}x^{10} + a^{30}x^{9} + a^{6}x^{8} + a^{53}x^{7} + a^{6}x^{6} + a^{21}x^{5} + a^{34}x^{4} + a^{6}x^{3} + a^{48}x^{2} + a^{11}x$

f_9. $a^{56}x^{56} + a^{4}x^{52} + a^{42}x^{50} + a^{49}x^{49} + a^{22}x^{48} + a^{55}x^{44} + a^{60}x^{42} + a^{3}x^{41} + a^{20}x^{40} + a^{55}x^{38} + a^{61}x^{37} + a^{9}x^{36} + a^{57}x^{35} + a^{39}x^{34} + a^{11}x^{33} + a^{31}x^{32} + a^{7}x^{28} + a^{52}x^{26} + a^{51}x^{24} + a^{56}x^{22} + a^{9}x^{21} + a^{24}x^{20} + a^{41}x^{19} + a^{36}x^{18} + a^{35}x^{17} + a^{56}x^{16} + a^{22}x^{14} + a^{8}x^{13} + a^{15}x^{12} + a^{37}x^{11} + a^{60}x^{10} + a^{18}x^{9} + a^{29}x^{8} + a^{52}x^{7} + a^{13}x^{6} + a^{12}x^{5} + a^{28}x^{4} + a^{26}x^{3} + a^{53}x^{2} + a^{59}x$

f_8. $a^{16}x^{52} + a^{9}x^{50} + a^{33}x^{49} + a^{57}x^{48} + a^{35}x^{44} + a^{27}x^{42} + a^{32}x^{41} + a^{9}x^{40} + a^{48}x^{38} + a^{57}x^{37} + a^{42}x^{36} + a^{61}x^{35} + a^{33}x^{34} + a^{28}x^{33} + a^{35}x^{32} + a^{53}x^{28} + a^{40}x^{26} + a^{56}x^{25} + a^{57}x^{24} + a^{11}x^{22} + a^{10}x^{21} + a^{25}x^{20} + a^{18}x^{19} + a^{30}x^{18} +$

$a^{44}x^{17} + a^{17}x^{16} + a^{17}x^{14} + a^{25}x^{13} + a^{16}x^{12} + a^{22}x^{11} + a^{26}x^{10} + a^{41}x^9 + a^{41}x^8 + a^{24}x^7 + a^{12}x^6 + a^{36}x^5 + ax^4 + a^{53}x^3 + a^4x^2 + a^3x$

f_{11}. $a^{55}x^{56} + a^{39}x^{50} + a^8x^{49} + a^{14}x^{48} + a^{14}x^{44} + a^{27}x^{42} + a^{52}x^{41} + a^{18}x^{40} + a^{55}x^{38} + a^{46}x^{37} + a^{53}x^{36} + a^{56}x^{35} + x^{34} + a^{17}x^{33} + a^{35}x^{32} + a^{42}x^{28} + a^{39}x^{26} + a^{50}x^{25} + a^{45}x^{24} + ax^{22} + a^{10}x^{21} + a^2x^{20} + a^{62}x^{19} + a^{22}x^{18} + a^{34}x^{17} + a^{11}x^{16} + a^{24}x^{14} + a^3x^{13} + a^{22}x^{12} + a^{45}x^{11} + a^{31}x^{10} + a^{16}x^9 + a^{21}x^8 + a^{44}x^7 + a^{40}x^6 + a^{48}x^5 + a^{18}x^4 + a^{46}x^3 + a^{33}x^2 + a^3x$

f_{10}. $a^{55}x^{56} + a^{39}x^{50} + a^8x^{49} + a^{57}x^{48} + a^{14}x^{44} + a^{27}x^{42} + a^{52}x^{41} + a^{42}x^{40} + a^{55}x^{38} + a^{46}x^{37} + a^{32}x^{36} + a^{56}x^{35} + a^{24}x^{34} + a^{11}x^{33} + a^8x^{32} + a^{42}x^{28} + a^{39}x^{26} + a^{50}x^{25} + a^{48}x^{24} + ax^{22} + a^{10}x^{21} + a^{12}x^{20} + a^{62}x^{19} + a^{36}x^{18} + a^{19}x^{17} + a^{16}x^{16} + a^{24}x^{14} + a^3x^{13} + a^{29}x^{12} + a^{45}x^{11} + a^{24}x^{10} + a^{51}x^9 + a^{49}x^8 + a^{44}x^7 + a^{57}x^6 + a^{13}x^5 + a^{42}x^4 + a^{52}x^3 + a^{14}x^2 + a^{47}x$

1-step extension:

f_{14}. $a^{62}x^{48} + a^{17}x^{40} + a^{29}x^{36} + a^{26}x^{34} + a^{26}x^{33} + a^{48}x^{32} + a^{49}x^{24} + a^8x^{20} + a^{13}x^{18} + a^{26}x^{17} + a^{27}x^{16} + a^{31}x^{12} + a^{41}x^{10} + a^9x^9 + a^{42}x^8 + a^{16}x^6 + a^8x^5 + a^{25}x^4 + a^{23}x^3 + a^{11}x^2 + a^{62}x$

f_{15}. $a^2x^{56} + a^{32}x^{52} + a^{18}x^{50} + a^{46}x^{49} + a^{52}x^{48} + a^{54}x^{44} + a^{45}x^{42} + a^{56}x^{41} + a^7x^{40} + a^{46}x^{38} + a^{32}x^{37} + a^6x^{36} + a^{44}x^{35} + a^{41}x^{34} + a^{50}x^{33} + a^{21}x^{32} + a^{34}x^{28} + a^{49}x^{26} + a^{50}x^{25} + x^{24} + a^{60}x^{22} + a^{15}x^{21} + a^{34}x^{20} + a^{46}x^{19} + a^{47}x^{18} + a^4x^{17} + a^7x^{16} + a^{50}x^{14} + a^7x^{13} + a^5x^{12} + a^{57}x^{11} + a^{17}x^{10} + a^{12}x^9 + a^{17}x^8 + a^{60}x^6 + a^2x^5 + a^7x^4 + a^{23}x^3 + a^{49}x^2 + a^{34}x$

f_{16}. $a^{52}x^{56} + a^{43}x^{52} + a^{34}x^{50} + a^{28}x^{49} + a^{31}x^{48} + a^{60}x^{44} + a^{58}x^{42} + a^{54}x^{41} + a^{46}x^{40} + a^{55}x^{38} + a^9x^{37} + a^{15}x^{36} + a^{20}x^{35} + a^{42}x^{34} + a^{54}x^{33} + a^{38}x^{32} + a^{53}x^{28} + a^{40}x^{26} + a^{29}x^{25} + a^{49}x^{24} + a^{62}x^{22} + a^{25}x^{21} + a^{17}x^{20} + a^{48}x^{19} + a^{26}x^{18} + a^{13}x^{17} + a^3x^{16} + a^{48}x^{14} + a^{59}x^{13} + a^{44}x^{12} + a^8x^{11} + a^{21}x^{10} + a^{32}x^9 + a^{43}x^8 + a^{23}x^7 + a^{20}x^6 + a^{38}x^5 + a^{49}x^4 + a^{32}x^3 + a^{27}x^2 + a^6x$

f_{17}. $a^{27}x^{56} + a^{27}x^{52} + a^{17}x^{50} + a^{23}x^{49} + a^{31}x^{48} + a^{44}x^{44} + a^2x^{42} + a^{53}x^{41} + a^{29}x^{40} + a^{48}x^{38} + a^{23}x^{37} + a^{24}x^{36} + a^{26}x^{35} + a^{43}x^{34} + a^{17}x^{33} + a^8x^{32} + a^4x^{28} + a^{20}x^{26} + a^2x^{25} + a^{30}x^{24} + a^7x^{22} + a^{49}x^{21} + a^{39}x^{20} + a^{26}x^{19} + a^{24}x^{18} + a^{62}x^{17} + a^{37}x^{16} + a^{49}x^{14} + a^{53}x^{13} + a^{37}x^{12} + a^{37}x^{11} + a^{28}x^{10} + a^2x^9 + a^{51}x^8 + a^{53}x^7 + a^{45}x^6 + a^{18}x^5 + a^{38}x^4 + a^{34}x^3 + a^{52}x^2 + a^{15}x$

f_{18}. $a^{20}x^{56} + a^4x^{52} + a^{41}x^{50} + a^{37}x^{49} + a^8x^{48} + a^{44}x^{44} + a^{45}x^{42} + a^5x^{41} + a^{12}x^{40} + a^{11}x^{38} + a^{16}x^{37} + a^{61}x^{36} + a^8x^{35} + a^{34}x^{34} + a^{37}x^{33} + a^{35}x^{32} + a^{43}x^{28} + a^{35}x^{26} + a^{22}x^{25} + a^{59}x^{24} + a^{55}x^{22} + a^{24}x^{21} + a^{30}x^{20} + a^7x^{19} + a^{52}x^{18} + a^{25}x^{17} + a^{22}x^{16} + a^{23}x^{14} + a^{19}x^{13} + a^{26}x^{12} + a^{29}x^{11} + a^{26}x^{10} + a^{26}x^9 + a^{18}x^8 + a^{13}x^7 + a^{52}x^6 + a^7x^5 + a^{51}x^4 + a^{50}x^3 + a^{37}x^2 + a^{22}x$

f_{19}. $a^{15}x^{56} + a^{25}x^{52} + a^{33}x^{49} + a^{14}x^{48} + a^{61}x^{44} + a^{18}x^{42} + a^{14}x^{41} + a^2x^{40} + a^{39}x^{38} + a^{27}x^{37} + a^{55}x^{36} + a^{53}x^{35} + a^{62}x^{34} + a^{17}x^{33} + a^{22}x^{32} + a^{20}x^{28} + a^9x^{26} + a^2x^{25} + a^{45}x^{24} + a^{34}x^{22} + a^{26}x^{21} + a^{19}x^{20} + a^{43}x^{19} + a^{14}x^{18} + a^{59}x^{17} + a^{24}x^{16} + a^{45}x^{14} + a^{46}x^{13} + a^{22}x^{12} + a^{62}x^{11} + a^{49}x^{10} + a^{47}x^9 + a^6x^8 + a^{27}x^7 + a^{40}x^6 + a^{16}x^5 + a^{22}x^4 + a^{46}x^3 + a^{58}x^2 + a^{32}x$

f_{20}. $a^{20}x^{56} + a^4x^{52} + a^{41}x^{50} + a^{37}x^{49} + a^{46}x^{48} + a^{44}x^{44} + a^{45}x^{42} + a^5x^{41} + a^{46}x^{40} + a^{11}x^{38} + a^{16}x^{37} + a^{57}x^{36} + a^8x^{35} + ax^{34} + a^{11}x^{33} + a^{48}x^{32} +$

$a^{43}x^{28} + a^{35}x^{26} + a^{22}x^{25} + a^{16}x^{24} + a^{55}x^{22} + a^{24}x^{21} + a^{44}x^{20} + a^{7}x^{19} + a^{14}x^{18} + a^{34}x^{17} + a^{6}x^{16} + a^{23}x^{14} + a^{19}x^{13} + ax^{12} + a^{29}x^{11} + a^{10}x^{10} + a^{31}x^{9} + a^{19}x^{8} + a^{13}x^{7} + a^{49}x^{6} + a^{33}x^{5} + a^{41}x^{4} + a^{23}x^{3} + a^{59}x^{2} + a^{34}x$

f_{21}. $a^{42}x^{48} + a^{47}x^{40} + a^{30}x^{36} + a^{58}x^{34} + a^{27}x^{33} + a^{55}x^{32} + a^{57}x^{24} + a^{32}x^{20} + a^{22}x^{18} + a^{58}x^{17} + a^{5}x^{16} + a^{13}x^{12} + a^{59}x^{10} + a^{60}x^{9} + a^{22}x^{8} + a^{7}x^{6} + a^{59}x^{5} + a^{48}x^{4} + ax^{3} + ax^{2} + a^{23}x$

f_{22}. $a^{20}x^{56} + a^{4}x^{52} + a^{41}x^{50} + x^{48} + a^{44}x^{44} + a^{45}x^{42} + a^{59}x^{41} + a^{31}x^{40} + a^{11}x^{38} + a^{43}x^{37} + a^{6}x^{36} + a^{17}x^{35} + a^{55}x^{34} + a^{2}x^{33} + a^{58}x^{32} + a^{43}x^{28} + a^{35}x^{26} + a^{31}x^{25} + a^{17}x^{24} + a^{55}x^{22} + a^{15}x^{21} + a^{45}x^{20} + a^{52}x^{19} + a^{47}x^{18} + a^{10}x^{17} + a^{32}x^{16} + a^{23}x^{14} + ax^{13} + a^{19}x^{12} + a^{47}x^{11} + a^{20}x^{10} + a^{12}x^{9} + a^{56}x^{8} + a^{49}x^{7} + a^{31}x^{6} + a^{24}x^{5} + a^{44}x^{4} + a^{37}x^{3} + a^{13}x^{2} + a^{3}x$

f_{23}. $a^{21}x^{56} + a^{16}x^{52} + a^{31}x^{50} + a^{23}x^{49} + a^{62}x^{48} + a^{10}x^{44} + a^{3}x^{42} + a^{49}x^{41} + a^{23}x^{40} + a^{44}x^{38} + a^{40}x^{37} + a^{32}x^{36} + a^{23}x^{35} + a^{56}x^{34} + a^{23}x^{33} + a^{22}x^{32} + a^{12}x^{28} + a^{41}x^{26} + a^{45}x^{25} + a^{6}x^{24} + a^{38}x^{22} + a^{20}x^{21} + a^{58}x^{20} + a^{32}x^{19} + a^{46}x^{18} + a^{8}x^{17} + a^{45}x^{16} + a^{39}x^{14} + a^{60}x^{13} + a^{29}x^{12} + a^{48}x^{11} + x^{10} + a^{39}x^{9} + a^{62}x^{8} + ax^{7} + a^{28}x^{6} + a^{50}x^{5} + a^{49}x^{4} + a^{56}x^{3} + a^{33}x^{2} + a^{52}x$

f_{24}. $a^{30}x^{56} + a^{53}x^{52} + a^{53}x^{50} + a^{11}x^{49} + a^{48}x^{48} + a^{13}x^{44} + a^{18}x^{42} + a^{26}x^{41} + a^{55}x^{40} + a^{43}x^{38} + a^{8}x^{37} + a^{52}x^{36} + a^{51}x^{35} + a^{18}x^{34} + a^{29}x^{33} + a^{62}x^{32} + a^{15}x^{28} + a^{58}x^{26} + a^{24}x^{25} + a^{30}x^{24} + a^{5}x^{22} + a^{26}x^{21} + a^{24}x^{20} + a^{12}x^{19} + a^{48}x^{18} + a^{15}x^{17} + a^{50}x^{16} + a^{5}x^{14} + a^{24}x^{13} + a^{46}x^{12} + a^{47}x^{11} + a^{24}x^{10} + a^{56}x^{9} + a^{18}x^{8} + a^{50}x^{7} + a^{22}x^{5} + a^{35}x^{4} + a^{55}x^{3} + a^{47}x^{2} + a^{51}x$

f_{25}. $a^{9}x^{56} + a^{55}x^{52} + a^{42}x^{50} + a^{6}x^{49} + a^{24}x^{48} + a^{56}x^{44} + a^{18}x^{42} + a^{28}x^{41} + a^{8}x^{40} + a^{11}x^{38} + a^{9}x^{37} + a^{19}x^{36} + a^{42}x^{35} + a^{28}x^{34} + a^{33}x^{33} + a^{23}x^{32} + a^{4}x^{28} + ax^{26} + a^{21}x^{25} + a^{2}x^{24} + a^{55}x^{22} + a^{26}x^{21} + a^{13}x^{20} + a^{39}x^{19} + a^{21}x^{18} + a^{35}x^{17} + x^{16} + a^{2}x^{14} + ax^{13} + a^{18}x^{12} + a^{18}x^{11} + a^{33}x^{10} + a^{55}x^{9} + a^{15}x^{8} + a^{33}x^{7} + a^{58}x^{6} + a^{52}x^{5} + a^{24}x^{4} + x^{3} + a^{8}x^{2} + a^{57}x$

f_{26}. $a^{9}x^{56} + a^{55}x^{52} + a^{42}x^{50} + a^{6}x^{49} + a^{62}x^{48} + a^{56}x^{44} + a^{18}x^{42} + a^{28}x^{41} + a^{30}x^{40} + a^{11}x^{38} + a^{9}x^{37} + a^{13}x^{36} + a^{42}x^{35} + a^{15}x^{34} + a^{4}x^{33} + a^{13}x^{32} + a^{4}x^{28} + ax^{26} + a^{21}x^{25} + a^{34}x^{24} + a^{55}x^{22} + a^{26}x^{21} + a^{11}x^{20} + a^{39}x^{19} + a^{43}x^{17} + a^{33}x^{16} + a^{2}x^{14} + ax^{13} + a^{23}x^{12} + a^{18}x^{11} + a^{38}x^{10} + a^{49}x^{9} + a^{58}x^{8} + a^{33}x^{7} + a^{50}x^{6} + a^{18}x^{5} + a^{28}x^{4} + a^{5}x^{3} + a^{19}x^{2} + a^{5}x$

f_{27}. $a^{34}x^{56} + a^{15}x^{52} + a^{36}x^{50} + a^{61}x^{49} + a^{9}x^{48} + a^{20}x^{44} + a^{44}x^{42} + a^{61}x^{41} + a^{10}x^{40} + a^{10}x^{38} + a^{11}x^{37} + a^{52}x^{36} + a^{11}x^{35} + a^{14}x^{34} + a^{23}x^{33} + a^{16}x^{32} + x^{28} + a^{50}x^{26} + a^{58}x^{25} + a^{44}x^{24} + a^{13}x^{22} + a^{11}x^{21} + a^{52}x^{20} + a^{48}x^{19} + a^{48}x^{18} + a^{38}x^{17} + a^{36}x^{16} + a^{41}x^{14} + a^{50}x^{13} + a^{43}x^{12} + a^{46}x^{11} + a^{4}x^{10} + a^{56}x^{9} + a^{42}x^{8} + a^{57}x^{7} + a^{61}x^{6} + a^{19}x^{5} + a^{3}x^{4} + a^{43}x^{3} + a^{22}x^{2} + a^{34}x$

f_{28}. $a^{55}x^{56} + a^{35}x^{52} + a^{43}x^{50} + a^{8}x^{49} + a^{49}x^{48} + a^{32}x^{44} + a^{27}x^{42} + a^{23}x^{41} + a^{56}x^{40} + a^{26}x^{38} + a^{28}x^{37} + a^{15}x^{36} + a^{56}x^{35} + a^{26}x^{34} + a^{31}x^{33} + a^{60}x^{32} + a^{42}x^{28} + a^{13}x^{26} + a^{44}x^{25} + a^{55}x^{24} + a^{14}x^{22} + a^{10}x^{21} + a^{60}x^{20} + a^{25}x^{19} + a^{26}x^{18} + a^{20}x^{17} + a^{54}x^{16} + a^{24}x^{14} + a^{10}x^{13} + a^{50}x^{12} + a^{32}x^{11} + a^{29}x^{10} + a^{32}x^{9} + a^{3}x^{8} + a^{44}x^{7} + a^{34}x^{6} + a^{26}x^{5} + a^{7}x^{4} + a^{22}x^{3} + a^{4}x^{2} + a^{21}x$

f_{29}. $a^{55}x^{56} + a^{35}x^{52} + a^{43}x^{50} + a^{8}x^{49} + a^{56}x^{48} + a^{32}x^{44} + a^{27}x^{42} + a^{23}x^{41} + a^{14}x^{40} + a^{26}x^{38} + a^{28}x^{37} + a^{40}x^{36} + a^{56}x^{35} + a^{19}x^{34} + a^{53}x^{33} + a^{3}x^{32} + a^{42}x^{28} + a^{13}x^{26} + a^{44}x^{25} + a^{9}x^{24} + a^{14}x^{22} + a^{10}x^{21} + a^{41}x^{20} + a^{25}x^{19} +$

$a^{55}x^{18} + a^{27}x^{17} + a^{2}x^{16} + a^{24}x^{14} + a^{10}x^{13} + a^{5}x^{12} + a^{32}x^{11} + a^{4}x^{10} + a^{29}x^{9} + a^{50}x^{8} + a^{44}x^{7} + a^{49}x^{6} + a^{61}x^{5} + a^{31}x^{4} + a^{16}x^{3} + a^{36}x^{2} + a^{61}x$

f_{30}. $a^{55}x^{56} + a^{35}x^{52} + a^{43}x^{50} + a^{8}x^{49} + a^{35}x^{48} + a^{32}x^{44} + a^{27}x^{42} + a^{23}x^{41} + a^{6}x^{40} + a^{26}x^{38} + a^{28}x^{37} + a^{46}x^{36} + a^{56}x^{35} + a^{60}x^{34} + a^{57}x^{33} + a^{54}x^{32} + a^{42}x^{28} + a^{13}x^{26} + a^{44}x^{25} + a^{5}x^{24} + a^{14}x^{22} + a^{10}x^{21} + a^{46}x^{20} + a^{25}x^{19} + a^{15}x^{18} + a^{58}x^{17} + a^{44}x^{16} + a^{24}x^{14} + a^{10}x^{13} + a^{24}x^{12} + a^{32}x^{11} + a^{42}x^{10} + a^{9}x^{9} + a^{56}x^{8} + a^{44}x^{7} + a^{7}x^{6} + a^{44}x^{5} + a^{19}x^{4} + a^{12}x^{3} + a^{29}x^{2} + a^{44}x$

2-step extension:

f_{31}. $a^{21}x^{56} + a^{5}x^{52} + a^{42}x^{50} + a^{38}x^{49} + a^{24}x^{48} + a^{45}x^{44} + a^{46}x^{42} + a^{6}x^{41} + a^{24}x^{40} + a^{12}x^{38} + a^{17}x^{37} + a^{10}x^{36} + a^{9}x^{35} + a^{3}x^{34} + a^{19}x^{33} + a^{35}x^{32} + a^{44}x^{28} + a^{36}x^{26} + a^{23}x^{25} + a^{55}x^{24} + a^{56}x^{22} + a^{25}x^{21} + a^{17}x^{20} + a^{8}x^{19} + a^{58}x^{18} + a^{2}x^{17} + a^{42}x^{16} + a^{24}x^{14} + a^{20}x^{13} + a^{37}x^{12} + a^{30}x^{11} + a^{5}x^{9} + a^{57}x^{8} + a^{14}x^{7} + a^{53}x^{6} + a^{31}x^{5} + a^{53}x^{4} + a^{62}x^{3} + a^{52}x^{2} + a^{19}x$

f_{32}. $ax^{48} + a^{29}x^{36} + a^{57}x^{34} + a^{12}x^{33} + a^{12}x^{32} + a^{6}x^{24} + a^{27}x^{20} + a^{40}x^{18} + a^{23}x^{17} + a^{55}x^{16} + a^{2}x^{12} + a^{9}x^{10} + a^{34}x^{9} + a^{49}x^{8} + a^{24}x^{6} + a^{39}x^{5} + a^{41}x^{4} + a^{42}x^{3} + a^{21}x^{2} + a^{30}x$

f_{33}. $a^{14}x^{56} + a^{9}x^{52} + a^{24}x^{50} + a^{62}x^{49} + a^{11}x^{48} + a^{3}x^{44} + a^{59}x^{42} + a^{15}x^{41} + a^{11}x^{40} + a^{37}x^{38} + a^{34}x^{37} + a^{36}x^{36} + a^{10}x^{35} + a^{18}x^{34} + a^{12}x^{33} + a^{61}x^{32} + a^{5}x^{28} + a^{34}x^{26} + a^{27}x^{25} + a^{56}x^{24} + a^{31}x^{22} + a^{18}x^{21} + a^{3}x^{20} + a^{10}x^{19} + a^{25}x^{18} + a^{48}x^{17} + a^{52}x^{16} + a^{32}x^{14} + a^{3}x^{13} + a^{44}x^{12} + a^{15}x^{11} + a^{13}x^{10} + a^{8}x^{9} + a^{46}x^{8} + a^{43}x^{7} + a^{8}x^{6} + a^{6}x^{5} + a^{8}x^{4} + a^{53}x^{3} + a^{52}x^{2} + a^{35}x$

f_{34}. $a^{14}x^{56} + a^{9}x^{52} + a^{24}x^{50} + a^{62}x^{49} + a^{61}x^{48} + a^{3}x^{44} + a^{59}x^{42} + a^{15}x^{41} + a^{57}x^{40} + a^{37}x^{38} + a^{34}x^{37} + a^{36}x^{36} + a^{10}x^{35} + a^{35}x^{34} + a^{14}x^{33} + a^{23}x^{32} + a^{5}x^{28} + a^{34}x^{26} + a^{27}x^{25} + a^{17}x^{24} + a^{31}x^{22} + a^{18}x^{21} + ax^{20} + a^{10}x^{19} + a^{25}x^{18} + ax^{17} + a^{13}x^{16} + a^{32}x^{14} + a^{3}x^{13} + a^{14}x^{12} + a^{15}x^{11} + a^{29}x^{10} + a^{8}x^{9} + a^{61}x^{8} + a^{43}x^{7} + a^{12}x^{6} + a^{30}x^{5} + a^{23}x^{4} + a^{39}x^{3} + a^{4}x^{2} + a^{32}x$

f_{35}. $a^{28}x^{52} + a^{54}x^{50} + a^{57}x^{49} + a^{53}x^{48} + a^{14}x^{44} + a^{40}x^{42} + a^{43}x^{41} + a^{2}x^{40} + a^{40}x^{38} + a^{28}x^{37} + a^{61}x^{36} + a^{25}x^{35} + a^{29}x^{34} + a^{31}x^{33} + a^{51}x^{32} + a^{40}x^{28} + a^{3}x^{26} + a^{6}x^{25} + a^{51}x^{24} + a^{29}x^{22} + a^{50}x^{21} + a^{39}x^{20} + a^{49}x^{19} + a^{3}x^{18} + a^{11}x^{17} + a^{32}x^{16} + a^{58}x^{14} + a^{8}x^{13} + a^{49}x^{12} + a^{21}x^{11} + a^{16}x^{10} + a^{61}x^{9} + a^{11}x^{8} + a^{4}x^{7} + a^{4}x^{6} + a^{33}x^{5} + a^{46}x^{4} + a^{38}x^{2} + a^{55}x$

f_{36}. $a^{51}x^{56} + x^{52} + a^{25}x^{50} + a^{52}x^{49} + a^{27}x^{48} + a^{45}x^{44} + a^{30}x^{42} + a^{11}x^{41} + a^{9}x^{40} + a^{46}x^{38} + a^{2}x^{37} + a^{10}x^{36} + a^{50}x^{35} + a^{50}x^{34} + a^{5}x^{33} + a^{26}x^{32} + a^{8}x^{28} + a^{15}x^{26} + a^{54}x^{25} + a^{23}x^{24} + a^{45}x^{22} + a^{27}x^{21} + a^{5}x^{20} + a^{51}x^{19} + a^{41}x^{18} + a^{33}x^{17} + a^{8}x^{16} + a^{9}x^{14} + a^{51}x^{13} + a^{54}x^{12} + a^{53}x^{11} + x^{10} + a^{42}x^{9} + a^{16}x^{8} + a^{19}x^{7} + a^{41}x^{6} + a^{47}x^{5} + x^{4} + a^{50}x^{3} + a^{13}x^{2} + a^{11}x$

f_{37}. $a^{51}x^{56} + x^{52} + a^{25}x^{50} + a^{52}x^{49} + a^{43}x^{48} + a^{45}x^{44} + a^{30}x^{42} + a^{11}x^{41} + a^{46}x^{38} + a^{2}x^{37} + a^{30}x^{36} + a^{50}x^{35} + a^{30}x^{34} + a^{2}x^{33} + a^{48}x^{32} + a^{8}x^{28} + a^{15}x^{26} + a^{54}x^{25} + a^{19}x^{24} + a^{45}x^{22} + a^{27}x^{21} + a^{43}x^{20} + a^{51}x^{19} + a^{47}x^{18} + a^{62}x^{17} + a^{13}x^{16} + a^{9}x^{14} + a^{51}x^{13} + a^{24}x^{12} + a^{53}x^{11} + a^{42}x^{10} + a^{37}x^{9} + a^{46}x^{8} + a^{19}x^{7} + a^{49}x^{6} + a^{57}x^{5} + a^{29}x^{4} + a^{4}x^{3} + a^{36}x^{2} + a^{24}x$

3-step extension:

f_{38}. $a^{22}x^{56} + a^6x^{52} + a^{43}x^{50} + a^{39}x^{49} + a^{35}x^{48} + a^{46}x^{44} + a^{47}x^{42} + a^7x^{41} + a^{36}x^{40} + a^{13}x^{38} + a^{18}x^{37} + a^{46}x^{36} + a^{10}x^{35} + a^{21}x^{34} + a^{46}x^{33} + a^3x^{32} + a^{45}x^{28} + a^{37}x^{26} + a^{24}x^{25} + a^{51}x^{24} + a^{57}x^{22} + a^{26}x^{21} + a^{22}x^{20} + a^9x^{19} + a^9x^{18} + a^{52}x^{17} + a^{12}x^{16} + a^{25}x^{14} + a^{21}x^{13} + a^{52}x^{12} + a^{31}x^{11} + a^{49}x^{10} + a^{49}x^9 + a^{10}x^8 + a^{15}x^7 + a^{50}x^6 + a^{34}x^5 + a^{11}x^4 + a^{50}x^3 + x^2 + a^{25}x$

f_{39}. $a^{15}x^{40} + a^{46}x^{36} + a^{34}x^{34} + a^{31}x^{33} + a^{54}x^{32} + a^{16}x^{24} + a^{49}x^{20} + a^9x^{18} + a^9x^{17} + ax^{16} + a^{51}x^{12} + a^{14}x^{10} + a^{49}x^9 + a^{55}x^8 + a^{13}x^6 + a^{61}x^5 + a^{33}x^4 + a^{39}x^3 + a^{59}x^2 + a^{26}x$

f_{40}. $a^{23}x^{56} + a^{15}x^{52} + a^{12}x^{50} + a^{55}x^{49} + a^{45}x^{48} + a^{61}x^{44} + a^9x^{42} + a^{20}x^{41} + a^{57}x^{40} + a^3x^{38} + a^3x^{37} + a^6x^{36} + a^{37}x^{35} + a^{40}x^{34} + a^{61}x^{33} + x^{32} + a^{20}x^{28} + a^{54}x^{26} + a^9x^{25} + a^{15}x^{24} + a^{52}x^{22} + a^{41}x^{21} + a^{48}x^{20} + a^{56}x^{19} + a^{52}x^{18} + a^{13}x^{17} + a^{15}x^{16} + a^{17}x^{14} + a^{22}x^{13} + a^{20}x^{12} + a^{59}x^{11} + a^{56}x^{10} + a^6x^9 + ax^8 + a^{52}x^7 + a^{59}x^6 + a^{46}x^5 + a^{36}x^4 + a^4x^3 + a^4x^2 + a^{49}x$

ANF representations of certain bent functions:

$$x_0x_1x_2x_4 \oplus x_0x_1x_2x_6 \oplus x_0x_1x_3x_4 \oplus x_0x_1x_3x_5 \oplus x_0x_1x_3x_7 \oplus x_0x_1x_4x_5 \oplus x_0x_1x_4x_7 \oplus x_0x_1x_4 \oplus x_0x_1x_5x_7 \oplus x_0x_1x_6x_7 \oplus x_0x_2x_3x_6 \oplus x_0x_2x_3x_7 \oplus x_0x_2x_4x_5 \oplus x_0x_2x_5x_6 \oplus x_0x_2x_5x_7 \oplus x_0x_2x_5 \oplus x_0x_2x_6x_7 \oplus x_0x_3x_4x_6 \oplus x_0x_3x_4x_7 \oplus x_0x_3x_4 \oplus x_0x_3x_5x_7 \oplus x_0x_3x_6x_7 \oplus x_0x_3x_6 \oplus x_0x_3x_7 \oplus x_0x_4x_5x_6 \oplus x_0x_4x_5 \oplus x_0x_4x_6 \oplus x_0x_5x_6x_7 \oplus x_0x_5x_6 \oplus x_0x_5x_7 \oplus x_0x_7 \oplus x_1x_2x_3x_5 \oplus x_1x_2x_3x_6 \oplus x_1x_2x_4x_5 \oplus x_1x_2x_4x_6 \oplus x_1x_2x_4 \oplus x_1x_2x_5x_6 \oplus x_1x_2x_5 \oplus x_1x_2x_6x_7 \oplus x_1x_2x_7 \oplus x_1x_3x_4x_7 \oplus x_1x_3x_5x_6 \oplus x_1x_3x_5 \oplus x_1x_3x_6 \oplus x_1x_3x_7 \oplus x_1x_4x_6x_7 \oplus x_1x_4x_7 \oplus x_1x_4 \oplus x_1x_5x_6 \oplus x_1x_5x_7 \oplus x_1x_6 \oplus x_2x_3x_4x_5 \oplus x_2x_3x_4x_7 \oplus x_2x_3x_4 \oplus x_2x_3x_5x_6 \oplus x_2x_3x_5x_7 \oplus x_2x_3x_5 \oplus x_2x_4x_5x_6 \oplus x_2x_4x_5x_7 \oplus x_2x_4x_5 \oplus x_2x_4x_7 \oplus x_2x_4 \oplus x_2x_6x_7 \oplus x_2x_7 \oplus x_3x_4x_5x_7 \oplus x_3x_4x_6x_7 \oplus x_3x_5x_6 \oplus x_3x_5 \oplus x_3x_6x_7 \oplus x_3x_6 \tag{9.1}$$

$$x_0x_1x_2x_6 + x_0x_1x_2x_7 + x_0x_1x_2x_8x_9 + x_0x_1x_2x_8x_{10} + x_0x_1x_2x_9x_{11} + x_0x_1x_2x_{10}x_{11} + x_0x_1x_3x_4 + x_0x_1x_3x_5 + x_0x_1x_4 + x_0x_1x_7 + x_0x_1x_8x_9 + x_0x_1x_8x_{10} + x_0x_1x_9x_{11} + x_0x_1x_{10}x_{11} + x_0x_2x_3x_6 + x_0x_2x_4 + x_0x_2x_5 + x_0x_2x_7 + x_0x_2x_8x_9 + x_0x_2x_8x_{10} + x_0x_2x_9x_{11} + x_0x_2x_{10}x_{11} + x_0x_3x_4 + x_0x_3x_5 + x_0x_3x_6 + x_0x_3x_7 + x_0x_3x_8x_9 + x_0x_3x_8x_{10} + x_0x_3x_9x_{11} + x_0x_3x_{10}x_{11} + x_0x_6 + x_1x_2x_3x_4 + x_1x_2x_4 + x_1x_2x_6 + x_1x_3x_5 + x_1x_3x_6 + x_1x_5 + x_1x_6 + x_1x_7 + x_1x_8x_9 + x_1x_8x_{10} + x_1x_9x_{11} + x_1x_{10}x_{11} + x_2x_3x_4 + x_2x_3x_5 + x_2x_3x_6 + x_2x_4 + x_2x_6 + x_2x_7 + x_2x_8x_9 + x_2x_8x_{10} + x_2x_9x_{11} + x_2x_{10}x_{11} + x_3x_4 + x_4x_5x_6x_7 + x_4x_5x_6x_8x_9 + x_4x_5x_6x_8x_{10} + x_4x_5x_6x_9x_{11} + x_4x_5x_6x_{10}x_{11} + x_4x_5x_6 + x_4x_5x_7 + x_4x_5x_8x_9 + x_4x_5x_8x_{10} + x_4x_5x_9x_{11} + x_4x_5x_{10}x_{11} + x_4x_5 + x_4x_6x_7 + x_4x_6x_8x_9 + x_4x_6x_8x_{10} + x_4x_6x_9x_{11} + x_4x_6x_{10}x_{11} + x_4x_6 + x_4x_7 + x_4x_8x_9 + x_4x_8x_{10} + x_4x_9x_{11} + x_4x_{10}x_{11} + x_4 + x_5x_6x_7 + x_5x_6x_8x_9 + x_5x_6x_8x_{10} + x_5x_6x_9x_{11} + x_5x_6x_{10}x_{11} + x_5x_6 + x_5x_7 + x_5x_8x_9 + x_5x_8x_{10} + x_5x_9x_{11} + x_5x_{10}x_{11} + x_5 + x_6x_7 + x_6x_8x_9 + x_6x_8x_{10} + x_6x_9x_{11} + x_6x_{10}x_{11} + x_6 + x_7 + x_8x_{10} + x_9x_{11} + 1 \tag{9.2}$$

$$x_0x_1x_2x_5 \oplus x_0x_1x_2x_6 \oplus x_0x_1x_3x_6 \oplus x_0x_1x_3x_7 \oplus x_0x_1x_3x_8x_9 \oplus x_0x_1x_3x_8x_{10} \oplus x_0x_1x_3x_9x_{11} \oplus x_0x_1x_3x_{10}x_{11} \oplus x_0x_1x_4x_6 \oplus x_0x_1x_4x_7 \oplus x_0x_1x_4x_8x_9 \oplus$$

$$x_0x_1x_4x_8x_{10}\oplus x_0x_1x_4x_9x_{11}\oplus x_0x_1x_4x_{10}x_{11}\oplus x_0x_1x_4\oplus x_0x_1x_5x_6\oplus x_0x_1x_6x_7\oplus x_0x_1x_6x_8x_9 \oplus x_0x_1x_6x_8x_{10} \oplus x_0x_1x_6x_9x_{11} \oplus x_0x_1x_6x_{10}x_{11} \oplus x_0x_1x_6 \oplus x_0x_2x_3x_5 \oplus x_0x_2x_4x_7 \oplus x_0x_2x_4x_8x_9 \oplus x_0x_2x_4x_8x_{10} \oplus x_0x_2x_4x_9x_{11} \oplus x_0x_2x_4x_{10}x_{11} \oplus x_0x_2x_5x_6 \oplus x_0x_2x_5 \oplus x_0x_2x_6 \oplus x_0x_2x_7 \oplus x_0x_2x_8x_9 \oplus x_0x_2x_8x_{10}\oplus x_0x_2x_9x_{11}\oplus x_0x_2x_{10}x_{11}\oplus x_0x_3x_4x_5\oplus x_0x_3x_4x_7\oplus x_0x_3x_4x_8x_9\oplus x_0x_3x_4x_8x_{10} \oplus x_0x_3x_4x_9x_{11} \oplus x_0x_3x_4x_{10}x_{11} \oplus x_0x_3x_4 \oplus x_0x_3x_5x_7 \oplus x_0x_3x_5x_8x_9 \oplus x_0x_3x_5x_8x_{10} \oplus x_0x_3x_5x_9x_{11} \oplus x_0x_3x_5x_{10}x_{11} \oplus x_0x_3x_6x_7 \oplus x_0x_3x_6x_8x_9 \oplus x_0x_3x_6x_8x_{10} \oplus x_0x_3x_6x_9x_{11} \oplus x_0x_3x_6x_{10}x_{11} \oplus x_0x_4x_5x_7 \oplus x_0x_4x_5x_8x_9 \oplus x_0x_4x_5x_8x_{10} \oplus x_0x_4x_5x_9x_{11} \oplus x_0x_4x_5x_{10}x_{11} \oplus x_0x_4x_6x_7 \oplus x_0x_4x_6x_8x_9 \oplus x_0x_4x_6x_8x_{10} \oplus x_0x_4x_6x_9x_{11} \oplus x_0x_4x_6x_{10}x_{11} \oplus x_0x_4x_6 \oplus x_0x_4x_7 \oplus x_0x_4x_8x_9 \oplus x_0x_4x_8x_{10} \oplus x_0x_4x_9x_{11} \oplus x_0x_4x_{10}x_{11} \oplus x_0x_5x_7 \oplus x_0x_5x_8x_9 \oplus x_0x_5x_8x_{10} \oplus x_0x_5x_9x_{11} \oplus x_0x_5x_{10}x_{11} \oplus x_0x_5 \oplus x_0x_6x_7 \oplus x_0x_6x_8x_9 \oplus x_0x_6x_8x_{10} \oplus x_0x_6x_9x_{11} \oplus x_0x_6x_{10}x_{11} \oplus x_0x_7 \oplus x_0x_8x_9 \oplus x_0x_8x_{10} \oplus x_0x_9x_{11} \oplus x_0x_{10}x_{11} \oplus x_1x_2x_3x_4 \oplus x_1x_2x_3x_7 \oplus x_1x_2x_3x_8x_9 \oplus x_1x_2x_3x_8x_{10} \oplus x_1x_2x_3x_9x_{11} \oplus x_1x_2x_3x_{10}x_{11} \oplus x_1x_2x_4x_5 \oplus x_1x_2x_4x_6 \oplus x_1x_2x_4\oplus x_1x_2x_5x_6\oplus x_1x_2x_5x_7\oplus x_1x_2x_5x_8x_9\oplus x_1x_2x_5x_8x_{10}\oplus x_1x_2x_5x_9x_{11}\oplus x_1x_2x_5x_{10}x_{11} \oplus x_1x_2x_5 \oplus x_1x_2x_7 \oplus x_1x_2x_8x_9 \oplus x_1x_2x_8x_{10} \oplus x_1x_2x_9x_{11} \oplus x_1x_2x_{10}x_{11}\oplus x_1x_3x_4x_5\oplus x_1x_3x_4x_6\oplus x_1x_3x_4x_7\oplus x_1x_3x_4x_8x_9\oplus x_1x_3x_4x_8x_{10}\oplus x_1x_3x_4x_9x_{11} \oplus x_1x_3x_4x_{10}x_{11} \oplus x_1x_3x_5 \oplus x_1x_3x_6x_7 \oplus x_1x_3x_6x_8x_9 \oplus x_1x_3x_6x_8x_{10}\oplus x_1x_3x_6x_9x_{11}\oplus x_1x_3x_6x_{10}x_{11}\oplus x_1x_3x_6\oplus x_1x_3x_7\oplus x_1x_3x_8x_9\oplus x_1x_3x_8x_{10}\oplus x_1x_3x_9x_{11}\oplus x_1x_3x_{10}x_{11}\oplus x_1x_4x_5x_6\oplus x_1x_4x_5x_7\oplus x_1x_4x_5x_8x_9\oplus x_1x_4x_5x_8x_{10} \oplus x_1x_4x_5x_9x_{11} \oplus x_1x_4x_5x_{10}x_{11} \oplus x_1x_5x_6 \oplus x_1x_6 \oplus x_1x_7 \oplus x_1x_8x_9\oplus x_1x_8x_{10}\oplus x_1x_9x_{11}\oplus x_1x_{10}x_{11}\oplus x_2x_3x_4x_5\oplus x_2x_3x_4x_6\oplus x_2x_3x_5x_6\oplus x_2x_3x_6x_7 \oplus x_2x_3x_6x_8x_9 \oplus x_2x_3x_6x_8x_{10} \oplus x_2x_3x_6x_9x_{11} \oplus x_2x_3x_6x_{10}x_{11} \oplus x_2x_3x_6 \oplus x_2x_3x_7 \oplus x_2x_3x_8x_9 \oplus x_2x_3x_8x_{10} \oplus x_2x_3x_9x_{11} \oplus x_2x_3x_{10}x_{11} \oplus x_2x_4x_5x_6 \oplus x_2x_4x_6x_7 \oplus x_2x_4x_6x_8x_9 \oplus x_2x_4x_6x_8x_{10} \oplus x_2x_4x_6x_9x_{11} \oplus x_2x_4x_6x_{10}x_{11} \oplus x_2x_4x_6 \oplus x_2x_4 \oplus x_2x_5x_6x_7 \oplus x_2x_5x_6x_8x_9 \oplus x_2x_5x_6x_8x_{10} \oplus x_2x_5x_6x_9x_{11}\oplus x_2x_5x_6x_{10}x_{11}\oplus x_2x_5x_7\oplus x_2x_5x_8x_9\oplus x_2x_5x_8x_{10}\oplus x_2x_5x_9x_{11}\oplus x_2x_5x_{10}x_{11} \oplus x_2x_7 \oplus x_2x_8x_9 \oplus x_2x_8x_{10} \oplus x_2x_9x_{11} \oplus x_2x_{10}x_{11} \oplus x_3x_4x_5x_7 \oplus x_3x_4x_5x_8x_9 \oplus x_3x_4x_5x_8x_{10} \oplus x_3x_4x_5x_9x_{11} \oplus x_3x_4x_5x_{10}x_{11} \oplus x_3x_4x_6 \oplus x_3x_5x_6x_7 \oplus x_3x_5x_6x_8x_9 \oplus x_3x_5x_6x_8x_{10} \oplus x_3x_5x_6x_9x_{11} \oplus x_3x_5x_6x_{10}x_{11} \oplus x_3x_5x_6\oplus x_3x_5\oplus x_3x_6x_7\oplus x_3x_6x_8x_9\oplus x_3x_6x_8x_{10}\oplus x_3x_6x_9x_{11}\oplus x_3x_6x_{10}x_{11}\oplus x_3x_6 \oplus x_8x_9 \oplus x_{10}x_{11}$$

(9.3)

$$\mathfrak{f}(x_0,\ldots,x_{11}) = x_0x_1x_2x_3x_8 \oplus x_0x_1x_2x_3x_9 \oplus x_0x_1x_2x_4x_8 \oplus x_0x_1x_2x_4x_9 \oplus x_0x_1x_2x_5x_8 \oplus x_0x_1x_2x_5x_9 \oplus x_0x_1x_2x_5 \oplus x_0x_1x_2x_6x_8 \oplus x_0x_1x_2x_6x_9 \oplus x_0x_1x_2x_6 \oplus x_0x_1x_2x_7x_8 \oplus x_0x_1x_2x_7x_9 \oplus x_0x_1x_2x_7 \oplus x_0x_1x_2x_8 \oplus x_0x_1x_2x_9 \oplus x_0x_1x_2 \oplus x_0x_1x_3x_6x_8 \oplus x_0x_1x_3x_6x_9 \oplus x_0x_1x_3x_6 \oplus x_0x_1x_3x_8 \oplus x_0x_1x_3x_9 \oplus x_0x_1x_4x_5 \oplus x_0x_1x_4x_6x_8 \oplus x_0x_1x_4x_6x_9 \oplus x_0x_1x_4x_6 \oplus x_0x_1x_4x_7 \oplus x_0x_1x_4x_8 \oplus x_0x_1x_4x_9 \oplus x_0x_1x_4 \oplus x_0x_1x_5x_6x_8 \oplus x_0x_1x_5x_6x_9 \oplus x_0x_1x_5x_6 \oplus x_0x_1x_5x_8 \oplus x_0x_1x_5x_9 \oplus x_0x_1x_6x_7x_8 \oplus x_0x_1x_6x_7x_9 \oplus x_0x_1x_6x_7 \oplus x_0x_1x_6x_8 \oplus x_0x_1x_6x_9 \oplus x_0x_1x_6 \oplus x_0x_1x_7x_8 \oplus x_0x_1x_7x_9 \oplus x_0x_1x_7 \oplus x_0x_1x_8 \oplus x_0x_1x_9 \oplus x_0x_2x_3x_4x_8 \oplus x_0x_2x_3x_4x_9\oplus x_0x_2x_3x_5\oplus x_0x_2x_3x_6x_8\oplus x_0x_2x_3x_6x_9\oplus x_0x_2x_3x_6\oplus x_0x_2x_3x_7\oplus x_0x_2x_3x_8 \oplus x_0x_2x_3x_9 \oplus x_0x_2x_3 \oplus x_0x_2x_4x_5x_8 \oplus x_0x_2x_4x_5x_9 \oplus x_0x_2x_4x_7x_8 \oplus x_0x_2x_4x_7x_9 \oplus x_0x_2x_4x_8 \oplus x_0x_2x_4x_9 \oplus x_0x_2x_4 \oplus x_0x_2x_5x_6x_8 \oplus x_0x_2x_5x_6x_9 \oplus x_0x_2x_5x_6 \oplus x_0x_2x_5x_7 \oplus x_0x_2x_5x_8 \oplus x_0x_2x_5x_9 \oplus x_0x_2x_6x_7x_8 \oplus x_0x_2x_6x_7x_9 \oplus x_0x_2x_6x_7 \oplus x_0x_2x_6x_8 \oplus x_0x_2x_6x_9 \oplus x_0x_2x_6 \oplus x_0x_2x_7x_8 \oplus x_0x_2x_7x_9 \oplus$$

$$x_0x_2x_8 \oplus x_0x_2x_9 \oplus x_0x_2 \oplus x_0x_3x_4x_6x_8 \oplus x_0x_3x_4x_6x_9 \oplus x_0x_3x_4x_6 \oplus x_0x_3x_4x_7 \oplus x_0x_3x_4x_8 \oplus x_0x_3x_4x_9 \oplus x_0x_3x_6x_8 \oplus x_0x_3x_6x_9 \oplus x_0x_3x_7 \oplus x_0x_3x_8 \oplus x_0x_3x_9 \oplus x_0x_3 \oplus x_0x_4x_5x_6x_8 \oplus x_0x_4x_5x_6x_9 \oplus x_0x_4x_5x_6 \oplus x_0x_4x_5x_8 \oplus x_0x_4x_5x_9 \oplus x_0x_4x_6x_7x_8 \oplus x_0x_4x_6x_7x_9 \oplus x_0x_4x_6x_7 \oplus x_0x_4x_6x_8 \oplus x_0x_4x_6x_9 \oplus x_0x_4x_7x_8 \oplus x_0x_4x_7x_9 \oplus x_0x_4x_7 \oplus x_0x_4x_8 \oplus x_0x_4x_9 \oplus x_0x_4 \oplus x_0x_5x_6x_8 \oplus x_0x_5x_6x_9 \oplus x_0x_5x_8 \oplus x_0x_5x_9 \oplus x_0x_5 \oplus x_0x_6x_7x_8 \oplus x_0x_6x_7x_9 \oplus x_0x_6x_8 \oplus x_0x_6x_9 \oplus x_0x_6 \oplus x_0x_7x_8 \oplus x_0x_7x_9 \oplus x_0x_7 \oplus x_0x_8 \oplus x_0x_9 \oplus x_1x_2x_3x_4 \oplus x_1x_2x_3x_5x_8 \oplus x_1x_2x_3x_5x_9 \oplus x_1x_2x_3x_5 \oplus x_1x_2x_3x_6x_8 \oplus x_1x_2x_3x_6x_9 \oplus x_1x_2x_3x_6 \oplus x_1x_2x_3x_8 \oplus x_1x_2x_3x_9 \oplus x_1x_2x_4x_5x_8 \oplus x_1x_2x_4x_5x_9 \oplus x_1x_2x_4x_6x_8 \oplus x_1x_2x_4x_6x_9 \oplus x_1x_2x_4x_6 \oplus x_1x_2x_4x_7 \oplus x_1x_2x_4x_8 \oplus x_1x_2x_4x_9 \oplus x_1x_2x_5x_6 \oplus x_1x_2x_5x_7x_8 \oplus x_1x_2x_5x_7x_9 \oplus x_1x_2x_5x_7 \oplus x_1x_2x_5x_8 \oplus x_1x_2x_5x_9 \oplus x_1x_2x_5 \oplus x_1x_2x_6x_7x_8 \oplus x_1x_2x_6x_7x_9 \oplus x_1x_2x_6x_8 \oplus x_1x_2x_6x_9 \oplus x_1x_2x_6 \oplus x_1x_2x_7x_8 \oplus x_1x_2x_7x_9 \oplus x_1x_2x_7 \oplus x_1x_2x_8 \oplus x_1x_2x_9 \oplus x_1x_2 \oplus x_1x_3x_4x_5 \oplus x_1x_3x_4x_6 \oplus x_1x_3x_4x_7 \oplus x_1x_3x_5x_6x_8 \oplus x_1x_3x_5x_6x_9 \oplus x_1x_3x_5x_6 \oplus x_1x_3x_5x_8 \oplus x_1x_3x_5x_9 \oplus x_1x_3x_6x_8 \oplus x_1x_3x_6x_9 \oplus x_1x_3x_7 \oplus x_1x_3x_8 \oplus x_1x_3x_9 \oplus x_1x_4x_5x_6x_8 \oplus x_1x_4x_5x_6x_9 \oplus x_1x_4x_5x_6 \oplus x_1x_4x_5x_8 \oplus x_1x_4x_5x_9 \oplus x_1x_4x_6x_8 \oplus x_1x_4x_6x_9 \oplus x_1x_4x_7 \oplus x_1x_4x_8 \oplus x_1x_4x_9 \oplus x_1x_5x_6x_7x_8 \oplus x_1x_5x_6x_7x_9 \oplus x_1x_5x_6x_7 \oplus x_1x_5x_6x_8 \oplus x_1x_5x_6x_9 \oplus x_1x_5x_7x_8 \oplus x_1x_5x_7x_9 \oplus x_1x_5x_8 \oplus x_1x_5x_9 \oplus x_1x_5 \oplus x_1x_6x_7x_8 \oplus x_1x_6x_7x_9 \oplus x_1x_6x_7 \oplus x_1x_6x_8 \oplus x_1x_6x_9 \oplus x_1x_6 \oplus x_1x_7x_8 \oplus x_1x_7x_9 \oplus x_1x_8 \oplus x_1x_9 \oplus x_2x_3x_4x_5x_8 \oplus x_2x_3x_4x_5x_9 \oplus x_2x_3x_4x_6x_8 \oplus x_2x_3x_4x_6x_9 \oplus x_2x_3x_4x_6 \oplus x_2x_3x_4x_8 \oplus x_2x_3x_4x_9 \oplus x_2x_3x_5x_6x_8 \oplus x_2x_3x_5x_6x_9 \oplus x_2x_3x_5x_6 \oplus x_2x_3x_5x_7 \oplus x_2x_3x_5x_8 \oplus x_2x_3x_5x_9 \oplus x_2x_3x_5 \oplus x_2x_3x_6x_7 \oplus x_2x_3x_6x_8 \oplus x_2x_3x_6x_9 \oplus x_2x_3x_6 \oplus x_2x_3x_8 \oplus x_2x_3x_9 \oplus x_2x_3 \oplus x_2x_4x_5x_6x_8 \oplus x_2x_4x_5x_6x_9 \oplus x_2x_4x_5x_7x_8 \oplus x_2x_4x_5x_7x_9 \oplus x_2x_4x_5x_7 \oplus x_2x_4x_5x_8 \oplus x_2x_4x_5x_9 \oplus x_2x_4x_5 \oplus x_2x_4x_6x_7x_8 \oplus x_2x_4x_6x_7x_9 \oplus x_2x_4x_6x_7 \oplus x_2x_4x_6x_8 \oplus x_2x_4x_6x_9 \oplus x_2x_4x_7x_8 \oplus x_2x_4x_7x_9 \oplus x_2x_4x_8 \oplus x_2x_4x_9 \oplus x_2x_5x_6x_7x_8 \oplus x_2x_5x_6x_7x_9 \oplus x_2x_5x_6x_7 \oplus x_2x_5x_6x_8 \oplus x_2x_5x_6x_9 \oplus x_2x_5x_6 \oplus x_2x_5x_7x_8 \oplus x_2x_5x_7x_9 \oplus x_2x_5x_7 \oplus x_2x_5x_8 \oplus x_2x_5x_9 \oplus x_2x_5 \oplus x_2x_6x_7x_8 \oplus x_2x_6x_7x_9 \oplus x_2x_6x_8 \oplus x_2x_6x_9 \oplus x_2x_7x_8 \oplus x_2x_7x_9 \oplus x_2x_8 \oplus x_2x_9 \oplus x_2 \oplus x_3x_4x_5x_6x_8 \oplus x_3x_4x_5x_6x_9 \oplus x_3x_4x_5x_8 \oplus x_3x_4x_5x_9 \oplus x_3x_4x_5 \oplus x_3x_4x_6x_7 \oplus x_3x_4x_6x_8 \oplus x_3x_4x_6x_9 \oplus x_3x_4x_6 \oplus x_3x_4x_8 \oplus x_3x_4x_9 \oplus x_3x_5x_6x_8 \oplus x_3x_5x_6x_9 \oplus x_3x_5x_7 \oplus x_3x_5x_8 \oplus x_3x_5x_9 \oplus x_3x_6x_8 \oplus x_3x_6x_9 \oplus x_3x_7 \oplus x_3x_8 \oplus x_3x_9 \oplus x_4x_5x_6x_7x_8 \oplus x_4x_5x_6x_7x_9 \oplus x_4x_5x_6x_8 \oplus x_4x_5x_6x_9 \oplus x_4x_5x_7x_8 \oplus x_4x_5x_7x_9 \oplus x_4x_5x_8 \oplus x_4x_5x_9 \oplus x_4x_5 \oplus x_4x_6x_7x_8 \oplus x_4x_6x_7x_9 \oplus x_4x_6x_7 \oplus x_4x_6x_8 \oplus x_4x_6x_9 \oplus x_4x_6 \oplus x_4x_7x_8 \oplus x_4x_7x_9 \oplus x_4x_8 \oplus x_4x_9 \oplus x_4 \oplus x_5x_6x_7x_8 \oplus x_5x_6x_7x_9 \oplus x_5x_6x_7 \oplus x_5x_6x_8 \oplus x_5x_6x_9 \oplus x_5x_7x_8 \oplus x_5x_7x_9 \oplus x_5x_7 \oplus x_5x_8 \oplus x_5x_9 \oplus x_5 \oplus x_6x_7x_8 \oplus x_6x_7x_9 \oplus x_6x_7 \oplus x_6x_8 \oplus x_6x_9 \oplus x_6 \oplus x_7x_8 \oplus x_7x_9 \oplus x_8x_{11} \oplus x_8 \oplus x_9x_{10} \oplus x_9 \oplus 1 \tag{9.4}$$

The `base64` representations of h_0 and h_1 in Example 8.3.4:

AE0eU3Q5aicATR5TdDlqJwBNHlN0OWonAE0eU3Q5aicATR5TdDlqJwBNHlN0OWonAE0eU3Q5aicATR5TdDlqJwBNHlN0OWon/6yVxtiLsuEAU2o5J3RNHv+y4ayLxpXYAE0eU3Q5aif/rJXG2Iuy4QBTajkndE0e/7LhrIvGldgATR5TdDlqJwBTajkndE0eAE0eU3Q5aicAU2o5J3RNHv+y4ayLxpXY/6yVxtiLsuH/suGsi8aV/6yVxtiLsuH/suGsi8aV/6yVxtiLsuEATajkndE0e/7LhrIvGldgATajkndE0eAE0eU3Q5aicAU2o5J3RNHv+y4ayLxpXY/6yVxtiLsuH/rJXG2Iuy4QBTajkndE0eAE0eU3Q5aicAU2o5J3RNHv+y4ayLxpXY/6yVxtiLsuEATR5TdDlqJwBNHlN0OWonAE0eU3Q5aicATR5TdDlqJwBNHlN0OWon/6yVxtiLsuEAU2o5J3RNHgBNHlN0OWonAE0eU3Q5aif/suGsi8aV/6yVxtiLsuEAFNqOSd0TR4AU2o5J3RNHv+slcbYi7LhAE0eU3Q5aif/suGsi8aV/6yVxtiLsuEATR5TdDlqJ/+slcbYi7Lh/6yVxtiLsuEATajkndE0e/7LhrIvGldj/suGsi8aV2ABTajkndE0eAE0eU3Q5aicAU2o5J3RNHv+y4ayLxpXY/6yVxtiLsuH/rJXG

2Iuy4f+y4ayLxpXYAFNqOSd0TR4ATR5TdDlqJwBNHlN0OWon/7LhrIvGldj/rJXG2Iuy4
QBTajkndE0e/6yVxtiLsuEAU2o5J3RNHgBNHlN0OWon/7LhrIvGldg=

(9.5)

ACc5Hk1qdFMAJzkeTWp0UwAnOR5NanRTACc5Hk1qdFMAJzkeTWp0UwAnOR5NanR
TACc5Hk1qdFMAJzkeTWp0UwAnOR5NanRTACc5Hk1qdFP/xrKL4dislf/Gsovh2KyVAD
lNdB4nU2oAOU10HidTav/YxuGylYus/9jG4bKVi6wAJzkeTWp0U//Gsovh2KyVADlNdB
4nU2r/2MbhspWLrP/Gsovh2KyVACc5Hk1qdFP/2MbhspWLrAA5TXQeJ1NqACc5Hk1qd
FP/xrKL4dislf/YxuGylYusADlNdB4nU2r/2MbhspWLrAA5TXQeJ1NqACc5Hk1qdFP/xr
KL4dislQAnOR5NanRTADlNdB4nU2r/xrKL4dislf/YxuGylYus/9jG4bKVi6wA5TXQeJ1Nq
ACc5Hk1qdFMAJzkeTWp0UwA5TXQeJ1NqACc5Hk1qdFMAOU10HidTav/YxuGylYusACc5
Hk1qdFP/2MbhspWLrACc5Hk1qdFMAOU10HidTav/8ayi+HYrJUAOU10HidTagAnOR5NanRT/9j
G4bKVi6wAOU10HidTav/Gsovh2KyVACc5Hk1qdFP/2MbhspWLrAA5TXQeJ1Nq/8ayi+
HYrJU=

(9.6)

Proof of Theorem 8.1.18

Proof. Let $a^{(1)}, a^{(2)} \in \mathbb{F}_2^n$ and $b^{(1)}, b^{(2)} \in \mathbb{F}_2^m$. We prove that $r\text{-ind}(h) < (n+m)/2$, by using Definitions 8.1.2 and 8.1.3. We need to show that there does not exist an $(\frac{n+m}{2})$-dimensional subspace V of $\mathbb{F}_2^{n+m}$ such that

$$D_{(a^{(1)},b^{(1)})}D_{(a^{(2)},b^{(2)})}h = constant,$$

for any $(a^{(1)}, b^{(1)})$, $(a^{(2)}, b^{(2)}) \in V$. There are three cases to be considered.

(i) For $\dim(\{x|(x,y) \in V\}) > n/2$, the proof is same with the proof of Theorem 8.1.15.

(ii) If $\dim(\{x|(x,y) \in V\}) = n/2$, then there are three cases to be considered.

  (a) For $\dim(\{y|(x,y) \in V\}) = m/2$, the proof is same with the proof of Theorem 8.1.15.

  (b) For $m/2 < \dim(\{y|(x,y) \in V\}) < (n+m)/2$, the proof is same with the proof of Theorem 8.1.15.

  (c) For $\dim(\{y|(x,y) \in V\}) = (n+m)/2$, we have $\{y|(a_1,y) \in V\} \cap \{y|(a_2,y) \in V\} = \emptyset$ for arbitrary $a_1, a_2 \in \{x|(x,y) \in V\}, a_1 \neq a_2$ and $\dim(\{y|(0_n,y) \in V\}) = m/2$. Since $\dim(\{\alpha|D_\alpha(f_1 \oplus f_2) = 0\}) = n-1$ and $\dim(\{x|(x,y) \in V\}) = n/2$, we can select one nonzero vector $a \in \{x|(x,y) \in V\}$ such that $D_a(f_1 \oplus f_2) = 0$. Further,

$$\dim(\{(0_n,y)|(0_n,y) \in V\} \cup \{(a,y)|(a,y) \in V\}) = m/2 + 1.$$

Thus, from $r\text{-ind}(g_1) < m/2+1$, we can select two vectors $(a^{(1)}, b^{(1)}), (a^{(2)}, b^{(2)}) \in \{(0_n, y)|(0_n, y) \in V\} \cup \{(a, y)|(a, y) \in V\}$ such that

$$D_{b^{(1)}} D_{b^{(2)}} g_1(y) \neq constant.$$

From (8.11), we have

$$\begin{aligned} & D_{(a^{(1)},b^{(1)})} D_{(a^{(2)},b^{(2)})} h(x,y) \\ = \; & D_{b^{(1)}} D_{b^{(2)}} g_1(y) \oplus (f_1 \oplus f_2)(x) D_{b^{(1)}} D_{b^{(2)}} (g_1 \oplus g_2)(y) \neq constant. \end{aligned} \tag{9.7}$$

(iii) If $\dim(\{x|(x, y) \in V\}) < n/2$, then we have $\dim(\{y|(x, y) \in V\}) \geq m/2+1$. Further, we have $\dim(\{y|(0, y) \in V\}) \geq m/2+1$ since $\dim(V) = (n+m)/2$. Hence, from $r\text{-ind}(g_1) < m/2+1$, we can select two vectors $(0_n, b^{(1)}), (0_n, b^{(2)}) \in V$ such that

$$D_{b^{(1)}} D_{b^{(2)}} g_1(y) \neq constant.$$

From (8.11), we have

$$\begin{aligned} & D_{(0_n,b^{(1)})} D_{(0_n,b^{(2)})} h(x,y) \\ = \; & D_{b^{(1)}} D_{b^{(2)}} g_1(y) \oplus (f_1 \oplus f_2)(x) D_{b^{(1)}} D_{b^{(2)}} (g_1 \oplus g_2)(y) \neq constant. \end{aligned} \tag{9.8}$$

□

Povzetek v slovenskem jeziku

Želja ljudi, da bi nekatere informacije ostale zaupne, predstavlja začetek *kriptografije* - discipline, ki po današnji definiciji omogoča dvema osebama varno komuniciranje preko ne povsem varnega kanala. Seveda želja, da bi nekaj ostalo tajno, ne ustreza vsem, ki bi radi vedeli, kaj se skriva za to tajnostjo. To je privedlo do razvoja *kriptoanalize* - znanosti o razbijanju šifer in razkrivanju izvirnega sporočila. Kriptografija in kriptoanaliza skupaj tvorita področje *kriptologije*, katerega preučevanje in pomen sta z razvojem sodobne znanosti, kot jo poznamo danes, eksponentno narasla.

Pred moderno dobo je bil sprva glavni namen kriptografije zagotavljanje tajnosti komunikacij povezanih z vojno in diplomatskimi zadevami. V zadnjih desetletjih se je področje razširilo in se med drugim ukvarja s preverjanjem celovitosti sporočil, avtentikacijo identitete pošiljatelja/prejemnika, digitalnimi podpisi, interaktivnimi dokazi in varnim računanjem. Informacije, ki jih želimo poslati, morajo potovati po nezanesljivih kanalih prek strežnikov, nad katerimi nimamo nadzora, kljub temu pa želimo, da informacije ostanejo zasebne.

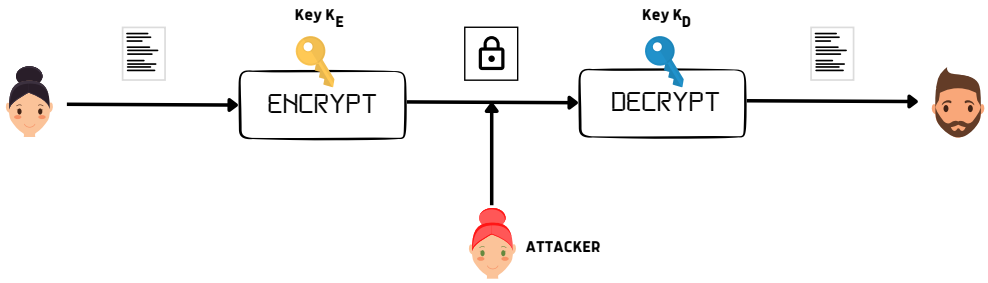

Figure 9.1: Shema klasičnega kriptosistema

Ključni cilj kriptografije je omogočiti dvema osebama, običajno ju imenujemo Ana (pošiljateljica) in Boris (prejemnik), varno komunikacijo po nezavarovanem kanalu. To pomeni, da nobena tretja oseba (*nasprotnik*), običajno imenovana Eva, iz opazovanega šifriranega besedila ne more pridobiti nobenih informacij o izvornem besedilu. Sporočilo, ki si ga Ana in Boris želita izmenjati, se imenuje *čistopis*, sporočilo, ki ga pošljeta po

kanalu pa *tajnopis*. Ana *šifrira* čistopis m in pridobi tajnopis c z uporabo nekega šifrirnega ključa K_E. Šifrirano besedilo c nato posreduje Bobu, ki s postopkom dešifriranja skupaj s šifriranim besedilom in dešifrirnim ključem K_D pridobi izvirno sporočilo m. Klasični primer takega kriptosistema je prikazan na sliki 9.1. Če sta šifrirni in dešifrirni ključ enaka ($K_E = K_D$), govorimo o *kriptografiji s simetričnim ključem*. Po drugi strani pa, če je šifrirni ključ javen, z drugimi besedami, če lahko vsakdo pošlje Borisu šifrirano sporočilo, ki ga lahko samo on dešifrira s svojim tajnim dešifrirnim ključem, govorimo o *kriptografiji z javnim ključem*. Glavna prednost kriptografije s simetričnim ključem pred kriptografijo z javnim ključem je, da je hitra in učinkovita za velike količine podatkov. Po drugi strani pa se kriptografija javnega ključa lahko uporablja ne le za varno komunikacijo, temveč tudi za preverjanje pristnosti z digitalnimi podpisi. V primerjavi s simetričnimi ključi para javnega in zasebnega ključa ni treba tako pogosto spreminjati.

Pri simulaciji napadov na kriptosisteme se predpostavlja, da Eva pozna algoritme za šifriranje in dešifriranje. To pomeni, da varnost kriptografskega sistema ne sme biti odvisna od tajnosti šifrirnega algoritma, temveč le od tajnosti ključev. Ta načela je navedel A. Kerckhoffs v [42].

Osredotočili se bomo predvsem na simetrično kriptografijo, saj teme v disertaciji obravnavajo lastnosti kriptografskih sistemov, povezanih z njo. Simetrična kriptografija vsebuje dve veliki družini kriptografskih sistemov, in sicer *bločne šifre* (slika 9.2) in *tokovne šifre* (slika 9.3).

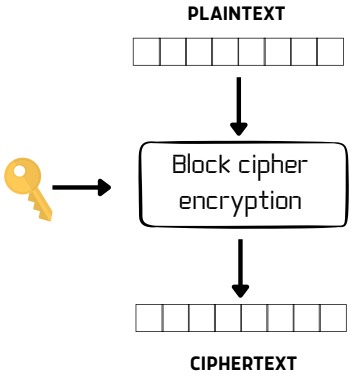

Figure 9.2: Primer bločne šifre

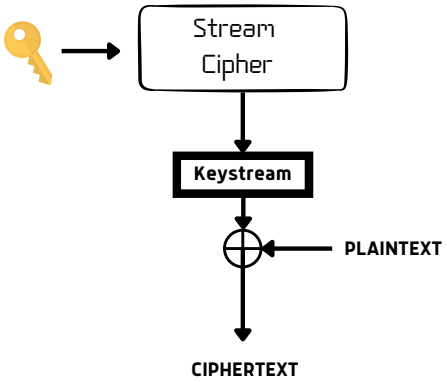

Figure 9.3: Primer tokovne šifre

Tokovne šifre generirajo psevdonaključno zaporedje (zdi se, da je statistično naključno, čeprav je bilo ustvarjeno s popolnoma determinističnim in ponovljivim postopkom) bitov, imenovano *ključni tok*, ki se običajno sešteje po modulu 2 z odprtim besedilom, da dobimo šifrirano besedilo. Nekateri znani šifrirni algoritmi, ki spadajo v družino tokovnih šifer, so SEAL [76], SNOW [34], ISAAC [40], Trivium [26] in Grain [35].

Po drugi strani je splošna zamisel pri načrtovanju bločnih šifer, da se odprto besedilo razdeli na *bloke* (dolžine 2^k, običajno je vrednost k enaka 64, 128 ali 256) in šifrira vsak blok posebej, s čimer dobimo šifro, sestavljeno iz blokov šifriranega besedila. Dve priljubljeni strukturi, ki se uporabljata v bločnih šifrah, temeljita na *Feistelovi strukturi* in na *substitucijsko-permutacijskem omrežju*. Sodobne zasnove bločnih šifer uporabljajo iterativno uporabo več enakih krogov za izdelavo bloka šifriranega besedila. Ključni vidik je, da ti krogi izvajajo koncept *konfuzije* in *difuzije*, ki ju je uvedel C. E. Shannon v svojem poročilu [80]. Vloga konfuzije je, da mora biti vsak bit šifriranega besedila zelo zapleteno odvisen od izvornega besedila in tajnega ključa. Po drugi strani pa lahko difuzijo v grobem razlagamo kot lastnost, da so biti šifrirnega besedila po uporabi enega kroga šifriranja odvisni od številnih vhodnih bitov. Z drugimi besedami, sprememba enega samega bita v izvornem besedilu bi morala povzročiti spremembo približno polovice bitov v šifriranem besedilu.

V substitucijsko-permutacijskem omrežju (SPN) sta pomembna dva pojma: S-škatle in P-škatle. *Substitucijska škatla* (S-škatla) uporablja Shannonovo načelo konfuzije in zamenja majhen blok vhodnih bitov z drugim blokom bitov. Na splošno je to preslikava, ki n bitov preslika v m bitov, pri čemer n ni nujno enako kot m. Na primer S-škatla, ki se uporablja v DES šifri (definicija sledi), preslika 6 vhdnih bitov v 4 izhodne bite. Druga komponenta v SPN je tako imenovana *permutacijska škatla* (P-škatla), ki permutira vse izhode S-škatel. Načeloma P-škatla uporablja Shannonovo načelo difuzije.

Za eno izmed prvih bločnih šifer velja šifra Lucifer, ki so jo pri IBM-u razvili v sedemdesetih letih 20. stoletja na podlagi dela Horsta Feistla. Pozneje je bila prilagojena različica Luciferja uporabljena kot standard ameriške vlade FIPS (Federal Information Processing Standard), ki se je imenoval "Data Encription Standard" (DES), ki je bil javno objavljen leta 1976 in se je pogosto uporabljal v vladnih in zasebnih organizacijah.

Takoj, ko so bile specifikacije standarda DES objavljene, je šifra postala predmet polemik. Dvomi o varnosti šifre DES so se pojavili zaradi dejstva, da je bil prvotni 128-bitni tajni ključ Luciferja zmanjšan na 56 bitov in tudi zato, ker načela zasnove njegovih substitucijskih in permutacijskih tabel niso bila nikoli objavljena.

Leta 1992 je Matsui predstavil koncept linearne kriptoanalize [54] in ga uporabil za napad na DES. Nekaj let pozneje je v okviru projekta DESCHALL javno razkril šifrirano sporočilo DES. Postalo je jasno, da je DES zaradi majhne dolžine ključa dovzeten za napade z grobo silo, zato je bilo potrebno izbrati nov standard šifriranja. DES je kot zvezni standard Združenih držav nadomestil *Advanced Encryption Standard* (AES), ki ga je leta 2001 po petletnem javnem natečaju sprejel National Institute of Standards and Technology (NIST). Razvila sta ga Joan Daemen in Vincent Rijmen, na natečaj pa sta ga prijavila pod imenom *Rijndael*. [25]. Nekatere druge znane bločne šifre so na primer še IDEA [47],

Blowfish [78], RC5 [75], PRESENT [9], če naštejemo le nekatere.

Na splošno obstajajo štiri glavne kriptanalitične predpostavke scenarijev v kriptoanalizi glede na to, kakšne informacije so napadalcu na voljo.

- ⋆ V najšibkejšem scenariju *samo-tajnopis* ima napadalec dostop le do nekaj šifrirnih besedil, ki jih je ustvaril ciljni bločni šifrirnik z uporabo neznanega tajnega simetričnega ključa. Njegov cilj je obnoviti dele (ali kar celotno) izvorno besedilo ali pa obnoviti (del) tajnega ključa. Ta scenarij je najbolj praktičen, po drugi strani pa je kriptoanalizo najtežja izvesti.
- ⋆ V primeru scenarija *znan-čistopis* ima napadalec na voljo veliko parov čistopis/tajnopis, njegov cilj pa je odkriti (del) skrivnega ključa.
- ⋆ Scenarij *izbrani-čistopis* je podoben napadu z znanim-čistopisom s to razliko, da ima napadalec dostop do šifrirne naprave in lahko šifrira poljubna sporočila (čistopise) po svoji izbiri. Cilj je ponovno obnoviti tajni ključ ali njegov del.
- ⋆ Scenarij *izbrani-tajnopis* je podoben prejšnjemu, čeprav napadalec dešifrira šifrirne tekste po svoji izbiri in tako pridobi ustrezne čistopise.

Za zagotavljanje visoke varnosti morajo funkcije v bločnih šifrah izpolnjevati različne pogoje/lastnosti. V nadaljevanju se bomo ukvarjali predvsem z varnostjo S-škatel, ki jih lahko obravnavamo kot zbirko preslikav iz $\mathbb{F}_2^n \to \mathbb{F}_2$, znanih kot *Boolove funkcije*. Tu z $\mathbb{F}_2^n$ označujemo n-razsežni vektorski prostor nad $\mathbb{F}_2 = \{0, 1\}$. Kot smo že omenili, je Matsui razvil pojem linearne kriptoanalize, ki razbije celotno 16-rundno šifro DES z 2^{47} pari čistopis/tajnopis.

Za zagotovitev dovolj visoke zaščite pred tovrstnimi napadi je bil uveden pojem *nelinearnost* (glej poglavje 2). Boolove funkcije, ki so na največji možni razdalji do množice vseh afinih funkcij (preslikave $l_a : \mathbb{F}_2^n \to \mathbb{F}_2$, definirane z $l_a(x) = a \cdot x \oplus b$, $a \in \mathbb{F}_2^n$, $b \in \mathbb{F}_2$), imajo največjo nelinearnost in se imenujejo *ukrivljene funkcije*, izraz, ki ga je uvedel O. Rothaus leta 1976 [77]. Poleg visoke nelinearnosti so druge kriptografsko pomembne lastnosti Boolovih funkcij povezane s pojmom uravnoteženosti, strogim kriterijem plazu in kriterijem širjenja, algebrsko stopnjo in korelacijsko odpornostjo, če omenimo le nekatere. Za več podrobnosti o teh lastnostih predlagamo bralcu ogled knjig [19, 24]. V celotni disertaciji nas bodo zanimali predvsem pojmi nelinearnosti in ukrivljenih funkcij.

V zadnjih petdesetih letih je bilo opravljenih veliko raziskav o ukrivljenih funkcijah in njihovih aplikacijah. V teoriji kodiranja je problem določanja tako imenovanega pokrivnega polmera za Reed-Mullerjevo kodo $RM(r, n)$ reda 1 enakovreden problemu iskanja določenih ukrivljenih funkcij [41, 50]. Nekatere posebne primere kvadratnih ukrivljenih funkcij lahko uporabimo za konstrukcijo Kerdockovih kod [43], ki so optimalne in imajo velike kodne razdalje, ki rastejo z dolžino kode [27, 81].

Problem konstruiranja *Hadamardovih matrik* je znan kombinatorični problem, ki ostaja nerešen od leta 1893. Če je velikost matrike $N = 2^n$ (n je sodo pozitivno število), potem lahko ta problem (z nekaterimi omejitvami) pretvorimo v nalogo konstruiranja ukrivljenih funkcij z n spremenljivkami [77]. Ukrivljene funkcije lahko opišemo tudi z uporabo *krepko regularnih grafov* s parametri (v, k, λ, μ). To pomeni, da graf vsebuje v vozlišč, kjer ima vsak stopnjo k, in za poljubni vozlišči a in b je število vozlišč, ki sočasno pripadajo soseščini a in b, enako λ ali μ, kar je odvisno od prisotnosti oziroma odsotnosti povezave med a in b. V članku [8] je bilo pokazano, da je Boolova funkcija f ukrivljena natanko tedaj, ko je njen Cayleyjev graf G_f krepko regularen in $\lambda = \mu$. Ukrivljene funkcije so bile preučevane tudi zaradi njihove povezave z diferencialnimi množicami. Naj bo $(G, +)$ abelova grupa reda v. Podmnožica $D \subseteq G$ velikosti k se imenuje *diferenčna množica* s parametri (v, k, λ), če lahko vsak neničelni $g \in G$ predstavimo kot $g = b - d$ na natanko λ načinov, kjer so $b, d \in D$. V [28] je bilo dokazano, da je Boolova funkcija f v n spremenljivkah ukrivljena natanko tedaj, ko je množica $D = \{(x, f(x)) : x \in \mathbb{F}_2^n\}$ diferenčna množica s parametri $(2^{n+1}, 2^n, 2^{n-1})$ v aditivni grupi $\mathbb{Z}_2^{n+1}$. Čeprav se zdi, da so Boolove funkcije popolna izbira za varne kriptografske preslikave, je njihova pomanjkljivost v tem, da niso uravnotežene. Kljub temu, da jih ni mogoče uporabiti neposredno, pa lahko ukrivljene funkcije spremenimo in dobimo nove funkcije, ki imajo še vedno visoko nelinearnost in so uporabne pri gradnji bločnih in tokovnih šifer. Na primer, šifri CAST [1] in Grain [35] ter razpršilna funkcija HAVAL [93] uporabljajo določene modifikacije ukrivljenih funkcij pri svoji konstrukciji. Za več podrobnosti o ukrivljenih funkcijah predlagamo bralcu ogled knjig Carleta, Sihema in Tokareve [19, 59, 83].

Čeprav je bilo na področju ukrivljenih funkcij opravljenih veliko raziskav, je še vedno veliko odprtih problemov. Med njimi omenjamo problem določanja števila ukrivljenih funkcij za fiksno število spremenljivk, njihovo načrtovanje in karakterizacijo. Metode konstrukcije ukrivljenih funkcij lahko razdelimo v dva razreda: *primarne* in *sekundarne*, ki se nanašata na zasnove, ki te funkcije zgradijo iz nič in alternativno z uporabo znanih funkcij.

Pri obravnavi razredov ukrivljenih funkcij obstajata dva primarna razreda, Dillonov [29] razred delnega razpona ($\mathcal{PS}$) in Maiorana-McFarland ($\mathcal{M}$) razred [55]. Izraz primarni se nanaša na konstrukcijo, ki ne uporablja znanih ukrivljenih funkcij za generiranje novih (kar je vzrok za tako imenovane sekundarne metode), temveč uporablja ustrezno množico afinih funkcij (značilno za metodo Maiorana-McFarland [55]) ali zbirko nepovezanih $n/2$-razsežnih podprostorov za konstrukcijo ukrivljene funkcije na $\mathbb{F}_2^n$ (značilno za razred delnih razponov, ki ga je predstavil Dillon [29]). Drugi splošni razred, označen z $\mathcal{N}$, je predstavil Dobbertin [30] in vključuje tako $\mathcal{M}$ kot podrazred $\mathcal{PS}$, običajno označen s $\mathcal{PS}_{ap}$. Neizčrpen seznam različnih sekundarnih konstrukcij je na voljo

v naslednjih delih [17, 18, 22, 37, 57, 92]. Leta 1993 je Carlet [17] na podlagi Dillonovih rezultatov uvedel dva sekundarna razreda ukrivljenih funkcij, ki imata pomembno vlogo v tej doktorski disertaciji, označena z $\mathcal{C}$ in $\mathcal{D}$, ki sta izpeljana z ustrezno modifikacijo ukrivljenih funkcij iz razreda $\mathcal{M}$. Glavna težava pri sekundarnih konstrukcijah je, da je težko odgovoriti na vprašanje o klasifikaciji tako generiranih ukrivljenih funkcij. Natančneje, lahko se zgodi, da nekatere od teh sekundarnih konstrukcij preprosto generirajo ukrivljene funkcije, ki pripadajo znanim primarnim razredom ukrivljenih funkcij in v tem primeru je pomembna le njihova eksplicitna predstavitev. Kljub temu je prikaz nevključenosti v popolne primarne razrede (za definicijo popolnega razreda glej definicijo 2.2.3) običajno težka naloga, še posebej v primeru tako imenovanega razreda $\mathcal{PS}$ zaradi pomanjkanja učinkovitih indikatorjev. V bistvu je problem mogoče zmanjšati na problem iskanja največje klike v grafu, za katerega je znano, da je NP-težak [88]. V primeru zaključenega razreda $\mathcal{M}$ tak indikator obstaja (prim. Lemma 2.2.4), vendar postane računsko neučinkovit za $n \geq 14$ (prim. razdelek 7.2.1).

Drug eksplicitni razred, ki ga je izpeljal Carlet in vsebuje primere, ki ne pripadajo $\mathcal{M}$ ali $\mathcal{PS}$, se imenuje $\mathcal{D}_0$, njegova kardinalnost pa je približno enako velika kot pri $\mathcal{M}$. To dejstvo nima posebnega vpliva na popolno klasifikacijo ukrivljenih funkcij, saj ta dva primarna razreda predstavljata le del $\approx 2^{76}$ ukrivljenih funkcij na $\mathbb{F}_2^8$, medtem ko je njihova skupna količina približno 2^{106} [48]. V nedavnih člankih [89, 88, 45] je bila analiza teh dveh sekundarnih razredov izpeljana naprej v smeri določitve zadostnega nabora pogojev, da so dobljene ukrivljene funkcije dokazljivo tudi izven $\mathcal{M}^{\#}$, kjer zgornji indeks "#" na splošno označuje popolno različico obravnavanega razreda. Zaradi težavnosti splošnih pogojev je zagotavljanje, da so določene ukrivljene funkcije hkrati v $\mathcal{C}$ ali $\mathcal{D}$ in dodatno izven $\mathcal{M}^{\#}$ (morda tudi izven $\mathcal{PS}^{\#}$), precej težka naloga. Eden od glavnih ciljev te disertacije je dodatno razširiti število ukrivljenih funkcij, ki ležijo izven razreda $\mathcal{M}^{\#}$.

Lastnost ukrivljenosti je bila razširjena na splošne (n, m)-funkcije, tj. na preslikave iz $\mathbb{F}_2^n$ v $\mathbb{F}_2^m$ (prim. razdelek 2.3). Kot je pokazala Nyberg [64], te funkcije obstajajo samo za $m \leq n/2$. Metode konstrukcije vektorskih ukrivljenih funkcij lahko prav tako razdelimo v dve kategoriji: *primarni* in *sekundarni*. Za nekatere znane konstrukcije (primarne in sekundarne) tako Boolovih kot vektorskih ukrivljenih funkcij se sklicujemo na [21, 31, 58, 61, 62, 63, 68, 86]. Drugi cilj te disertacije je dodatno obravnavati oblikovanje vektorskih ukrivljenih funkcij, ki so šibko/močno ali skoraj močno izven $\mathcal{M}^{\#}$ (prim. definicija 2.3.5), pojem, ki je bil uveden v [67]. Večina konstrukcij temelji na posplošeni konstrukciji, ki jo navdihujejo dela v [82, 90] prek tako imenovane lastnosti (P_τ) (imenujemo jo lastnost (P_U), prim. lema 3.1.5). Podobno kot v Boolovem primeru lahko ti vektorski objekti omogočijo boljše razumevanje, povezano s popolnejšo klasifikacijo teh struktur.

Preostali del disertacije je organiziran na naslednji način. V poglavju

2 podamo osnovne pojme, definicije in rezultate, ki se uporabljajo v celotni disertaciji. Vendar pa bodo nekateri pojmi uvedeni skozi celotno disertacijo, ko se bo zdelo primerno in potrebno.

Poglavji 3 in 4 predstavljata novo metodo za sekundarno konstrukcijo ukrivljenih (n, m)-funkcij in p-arnih šibko regularnih ukrivljenih (n, m)-funkcij (za definicijo glej poglavje 2.4) prek tako imenovane lastnosti (P_U). Ta konstrukcija bo zelo pomembna za pridobivanje funkcij, ki so šibko/močno/skoraj močno izven $\mathcal{M}^{\#}$.

Poglavje 5 obravnava konstrukcijo dveh novih superrazredov $\mathcal{SC}$ (superrazred razredov $\mathcal{C}$ in $\mathcal{D}_0$) in $\mathcal{CD}$ (superrazred razredov $\mathcal{C}$ in $\mathcal{D}$) ter podaja zadostne pogoje, za katere so te funkcije izven $\mathcal{M}^{\#}$. Na koncu poglavja podamo izrecne definicije dualov nekaterih funkcij v $\mathcal{SC}$ in $\mathcal{CD}$.

V poglavju 6 podamo pregled uporabe novo zgrajenih razredov $\mathcal{SC}$ in $\mathcal{CD}$ za konstrukcijo vektorskih ukrivljenih funkcij šibko/močno/močno izven $\mathcal{M}^{\#}$ ter tako imenovanih MNBC funkcij, vektorske (n, m)- funkcije z največjim številom ukrivljenih komponent (prim. definicijo 3.3.1), šibko/-močno izven $\mathcal{M}^{\#}$.

Poglavje 7 dodatno razširja število ukrivljenih funkcij izven razreda $\mathcal{M}^{\#}$, ki jih obravnavamo kot tako imenovane 4-dekompozicije. Dobimo tudi primere tako imenovanih ukrivljenih 4-dekompozicij izven $\mathcal{M}^{\#}$ prek razredov $\mathcal{SC}$ in $\mathcal{CD}$.

V poglavju 8 obravnavamo dve znani sekundarni konstrukciji - neposredno in posredno vsoto ter podamo pogoje, za katere te funkcije ležijo izven $\mathcal{M}^{\#}$. Podamo tudi primere (homogenih) kubičnih ukrivljenih funkcij (brez afinnih derivatov) in močno povečamo meje [71] za razsežnosti, v katerih obstajajo. Pokažemo tudi, da je eden od konstruiranih razredov nerazgradljiv (neločljiv), in podamo tudi vektorske ukrivljene funkcije močno izven $\mathcal{M}^{\#}$ z razmeroma veliko izhodno dimenzijo.

Zaključki

Rezultati te doktorske disertacije predstavljajo pomemben prispevek k številnim odprtim problemom na področju kriptografije, ki so v zadnjih petih desetletjih aktivna tema v matematični skupnosti.

Večji del disertacije se ukvarja z gradnjo (vektorskih) ukrivljenih funkcij izven popolnega Maiorana-McFarland razreda z uporabo različnih metod. Poudarjamo, da smo za vse primere potrdili, da so izven $\mathcal{M}^{\#}$ z uporabo matematične programske opreme `Sage` in algoritma, ki smo ga razvili z uporabo lastnosti klike v grafih.

Lastnost (P_U) smo posplošili, da bi dobili metodo za konstrukcijo vektorskih ukrivljenih funkcij, ki zajema prejšnji dve metodi v [82, 90]. S to konstrukcijo smo podali tudi nove primere vektorskih funkcij, ki imajo

maksimalno število ukrivljenih komponent. Podobno smo te rezultate razširili na p-arni primer in razvili sekundarne konstrukcije p-arnih šibko regularnih ukrivljenih (n, m)-funkcij.

Z združitvijo kazalnikov $\mathcal{C}$ in $\mathcal{D}_0$ ter $\mathcal{C}$ in $\mathcal{D}$ smo dobili nova superrazreda ukrivljenih funkcij, $\mathcal{SC}$ oziroma $\mathcal{CD}$. Za oba razreda smo določili pogoje, pod katerimi te funkcije ležijo izven $\mathcal{M}^{\#}$. Opazili smo, da imata ta razreda veliko možnosti uporabe. Predvsem pri konstrukciji vektorskih ukrivljenih funkcij, ki so šibko/močno/močno izven $\mathcal{M}^{\#}$. Opazili smo, da imajo naši primeri vektorskih ukrivljenih funkcij močno izven $\mathcal{M}^{\#}$ največji (čeprav ne največji po definiciji) izhodni prostor v literaturi. Te funkcije so bile uporabne tudi pri konstrukciji funkcij (n, m)-MNBC izven $\mathcal{M}^{\#}$. Podali smo tudi popolno klasifikacijo funkcij MNBC v šestih spremenljivkah.

Dejstvo, da je ukrivljena funkcija f v/izven $\mathcal{M}^{\#}$ natanko tedaj, ko je njen dual v/izven $\mathcal{M}^{\#}$, smo uporabili v tako imenovani 4-dekompoziciji ukrivljene funkcije nad $\mathbb{F}_2^n$, ki sta jo Canteaut in Charpin [14] prvotno obravnavali v primeru odvodov drugega reda, pozneje pa sta jo v [39] preoblikovali v primeru dualov in njenih omejitev na odseke $(n-2)$-razsežnega podprostora V. Za vsakega od treh možnih primerov te 4-dekompozicije ukrivljene funkcije podamo splošne metode za načrtovanje ukrivljenih funkcij dokazljivo izven $\mathcal{M}^{\#}$. Na primer, za osnovni primer definiranja ukrivljene funkcije $h(x, y_1, y_2) = f(x) \oplus y_1 y_2$ na $\mathbb{F}_2^{n+2}$ z uporabo ukrivljene funkcije f na $\mathbb{F}_2^n$ pokažemo, da h leži izven $\mathcal{M}^{\#}$ natanko tedaj, ko je f izven $\mathcal{M}^{\#}$. Ta pristop nato posplošimo na primer, ko uporabimo dve ukrivljeni funkciji. Natančneje, konkatenacija $f_1||f_1||f_2||(1 \oplus f_2)$ prav tako daje ukrivljene funkcije izven $\mathcal{M}^{\#}$, če je bodisi f_1 bodisi f_2 izven $\mathcal{M}^{\#}$. Obravnavani so tudi primeri, ko so štiri omejitve ukrivljene funkcije semi-ukrivljene ali petvrednostne spektralne funkcije, in predlaganih je več metod načrtovanja neskončnih družin ukrivljenih funkcij izven $\mathcal{M}^{\#}$ z uporabo načrtovanja spektralne metode, obravnavane v [37, 39].

Dve znani sekundarni konstrukciji ukrivljenih funkcij sta metodi neposredne in posredne vsote. Pokažemo, da lahko neposredna vsota pod bolj sproščenimi pogoji v primerjavi s tistimi v [71] dokazljivo generira ukrivljene funkcije izven popolnega razreda Maiorana-McFarland ($\mathcal{M}^{\#}$). Pokažemo tudi, da lahko metodo posredne vsote, čeprav postavlja določene pogoje za začetne ukrivljene funkcije, uporabimo pri oblikovanju ukrivljenih funkcij izven $\mathcal{M}^{\#}$. Poleg tega z uporabo te metode za ustrezno izbrane ukrivljene funkcije konstruiramo več splošnih razredov homogenih kubičnih ukrivljenih funkcij (kar je težaven problem), ki bi lahko imeli dodatne lastnosti (namreč brez afinskih odvodov in-/ali izven $\mathcal{M}^{\#}$). Naši rezultati bistveno izboljšajo najbolj znane primere tovrstnih ukrivljenih funkcij, ki sta jih podala Polujan in Pott [71], poleg tega pa rešimo še odprt problem v [71, Open Problem 5.1]. Natančneje, pokažemo, da je en razred naših homogenih kubičnih ukrivljenih funkcij

nerazgradljiv (neločljiv), tako, da h pod nesingularno transformacijo B ni mogoče predstaviti kot $h(xB) = f(y) \oplus g(z)$. Nazadnje podamo splošen razred vektorskih ukrivljenih funkcij, ki so močno izven $\mathcal{M}^{\#}$ z relativno velikih izhodnih dimenzij, kar na splošno velja za težko nalogo.

Osnovna orodja, uporabljena v disertaciji, segajo od kombinatoričnih do algebrskih kriptografskih metod. Poleg tega smo uporabili matematično programsko opremo `Sage`, `Wolfram Mathematica` in `Magma`, za potrditev naše hipoteze. Seznam `Sage` kod, ki smo jih razvili med pisanjem disertacije, je na voljo na spletni strani `https://kripto.famnit.upr.si/sage/`.

Declaration

I declare that this doctoral dissertation does not contain any materials previously published or written by another person except where due reference is made in the text.

Amar Bapić