UNIVERZA NA PRIMORSKEM
FAKULTETA ZA MATEMATIKO, NARAVOSLOVJE IN
INFORMACIJSKE TEHNOLOGIJE

DOKTORSKA DISERTACIJA
(DOCTORAL THESIS)

O NEKATERIH KONSTRUKCIJAH KRIPTOGRAFSKO POMEMBNIH BOOLOVIH FUNKCIJ

(ON CERTAIN CONSTRUCTION METHODS OF CRYPTOGRAPHICALLY SIGNIFICANT BOOLEAN FUNCTIONS)

SAMED BAJRIĆ

KOPER, 2014

UNIVERZA NA PRIMORSKEM
FAKULTETA ZA MATEMATIKO, NARAVOSLOVJE IN
INFORMACIJSKE TEHNOLOGIJE

DOKTORSKA DISERTACIJA
(DOCTORAL THESIS)

O NEKATERIH KONSTRUKCIJAH KRIPTOGRAFSKO POMEMBNIH BOOLOVIH FUNKCIJ

(ON CERTAIN CONSTRUCTION METHODS OF CRYPTOGRAPHICALLY SIGNIFICANT BOOLEAN FUNCTIONS)

SAMED BAJRIĆ

KOPER, 2014

MENTOR: IZR. PROF. DR. ENES PASALIC
SOMENTOR: DOC. DR. MARKO OREL

To my Family

Acknowledgement

I would like to express my sincere gratitude to my supervisor Enes Pasalic for the continuous support of my PhD study and research, for his patience, motivation, enthusiasm, and immense knowledge in cryptography that, taken together, make him a great supervisor. His guidance helped me in all the time of research and writing of this thesis, and his advice on both research as well as on my career have been priceless. I would also like to thank to my co-supervisor Marko Orel for his support, availability and constructive suggestions, which were determinant for the accomplishment of the work presented in this thesis.

I would like to thank the Department of Mathematics at University of Primorska, for giving me the opportunity to do research studies. I am grateful to professor Fehim Dedagić for his help with getting enrolled to the PhD studies at the University of Primorska.

Posebnu zahvalnost upućujem mojim roditeljima kao i mojim iskrenim prijateljima, koji su me podržavali u mojim ciljevima, davali mi snagu i podršku da ustrajem do kraja.

Samed Bajrić

This work is supported part by "Agencija za raziskovalno dejavnost Republike Slovenije", research program and "Mladi raziskovalec" research program.

Contents

List of Figures

List of Tables

Abstract

ON CERTAIN CONSTRUCTION METHODS OF CRYPTOGRAPHICALLY SIGNIFICANT BOOLEAN FUNCTIONS

The certain classes of (vectorial) Boolean functions, such as bent functions for instance, play an important role in symmetric-key cryptography. Even though a complete classification of bent functions seems to be elusive, any new construction methods of bent functions is of great importance. The same holds for related functions such as vectorial bent functions, bent and vectorial bent functions over odd characteristic, and plateaued functions with disjoint spectra. The main purpose of the dissertation is to provide new examples of such functions by specifying their algebraic representation along with a set of conditions that guarantee the bent property of the new classes. The algebraic expressions of certain classes of Boolean functions that might contain bent functions are analyzed in details and some new constructing methods of cryptographically significant functions have been developed.

All related parts in the dissertation address various aspects of designing certain cryptographically significant functions. In particular, a complete characterization of certain classes of vectorial bent functions given in a multiple trace form is given. The existence of both single output and vectorial p-valued bent functions, represented as trace multinomials with Dillon's exponents are provided. Moreover, several infinite classes of semi-bent functions, where each class is characterized by either a different decomposition of such a function with respect to the Walsh spectra of its subfunctions, or by the method used for its derivation, are proposed. Furthermore, two classes of highly nonlinear vectorial semi-bent functions with very good cross-correlation properties are proposed.

Math. Subj. Class (2010): 11T71, 94A60, 14G50, 68P25.

Key words: Boolean functions, Vectorial (generalized) bent functions, Binomial trace functions, Symmetric polynomials, Linearized polynomials, Planar mappings, Disjoint spectra, Plateaued functions, Semi-bent functions, Cross-correlation, Sum-of-squares indicator.

Izvleček

O NEKATERIH KONSTRUKCIJAH KRIPTOGRAFSKO POMEMBNIH BOOLOVIH FUNKCIJ

Nekatere vrste (vektorskih) Boolovih funkcij, npr. zlomljene funkcije, imajo pomembno vlogo v kriptografiji simetričnih ključev. Čeprav se zdi popolna klasifikacija zlomljenih funkcij težko dosegljiva, je vsaka na novo odkrita metoda za konstrukcijo teh funkcij izjemnega pomena. Enako velja za sorodne funkcije, kot so vektorske zlomljene funkcije, zlomljene in vektorske zlomljene funkcije nad liho karakteristiko ter planotske funkcije z disjunktnim spektrom. Poglavitni cilj v disertaciji bo poiskati nove primere tovrstnih funkcij s skrbno izbrano algebraično strukturo in določitev množice pogojev, ki bodo garantirali zlomljenost funkcij. Algebraične lastnosti določenih razredov Boolovih funkcij, ki morebiti vsebujejo zlomljene funkcije, bodo podvržene podrobni analizi. Namen disertacije je tudi razviti nove konstrukcijske metode za nekatere kriptografsko pomembne funkcije.

Vsa sorodna področja v disertaciji preučujejo konstrukcije določene vrste kriptografsko pomembnih funkcij. Posebno, popolna karakterizacija za določene razrede vektorskih zlomljenih funkcij, ki so v multinomni sledni obliki, je podana. Obstoj zlomljenih funkcij, ki slikajo v obseg lihe karakteristike, in njihovih vektorskih analogov, pri emer so funkcije predstavljene kot multinomne sledne funkcije z Dillonivimi eksponenti je podan. Poleg tega v disertaciji je podanih tudi več neskončnih razredov semi-zlomljenih funkcij, kjer so razredi okarakterizirani bodisi z raznovrstnimi dekompozicijami tovrstnih funkcij ali njihovih podfunkcij glede na Walshov spekter bodisi z metodo, ki je uporabljena za njihovo konstrukcijo. Podana sta tudi dva razreda visoko nelinearnih semi-zlomljenih vektorskih funkcij z zelo dobrimi navzkrižno-korelacijskimi lastnostmi.

Math. Subj. Class (2010): 11T71, 94A60, 14G50, 68P25.

Ključne besede: Boolove funkcije, Vektorske (posplošene) zlomljene funkcije, Binomne sledne funkcije, Simetrični polinomi, Linearizirani polinomi, Preslikave ravnine, Disjunktni spekter, Planotske funkcije, Semi zlomljene Boolove funkcije, Navzkrižna korelacija, Indikator vsote kvadratov.

Chapter 1

Introduction

If you cannot explain it simply, you do not understand it well enough.
–Albert Einstein

Cryptography is a Greek word that means "hidden". The verb form of the word, interestingly means "write" and the term eventually stands for the exclusive study of message secrecy, that is cryptography is the science or art of secret writing. Today, cryptography has become a branch of information theory and is used within a mathematical approach to study the transmission of information from place to place. The science of cryptography involves communication in the presence of adversaries. It even enhances the spheres of engineering and pure mathematics. It plays a very important role within the spheres of information technology, authentication and access control. In a modern society, exchange and storage of information in an efficient, reliable and secure manner is of fundamental importance. Cryptology comprises the interrelated areas of cryptography and cryptanalysis. Cryptographic codes, or ciphers, are used to protect information against wiretapping, unauthorized changes and other misuse. A cryptanalyst studies the vulnerabilities of ciphers. Secure communication will be essential for Internet and mobile communication to realize their full potential, enabling the transfer of sensitive data in for example payment systems, e-commerce, m-commerce, health systems etc. For many applications, systems for authentication will be necessary. Cryptology is therefore becoming ever more important for business and industry as well as for society at large.

The solutions to different cryptographic problems are refered to as cryptographic primitives. They are designed for specific purposes with the aim of accomplishing a number of security goals. The four major objectives associated with information security are:

(i) confidentiality - a service used to prevent any unauthorized party of revealing the content of information. Synonym terms for confidentiality are secrecy or privacy.

(ii) data integrity - a service which addresses the unauthorized alternation of data.

(iii) authentication - a service related to identification. This means that two parties in communication should identify each other.

(iv) non-repudiation - a service which prevents an entity from denying previous commitments and actions.

For the sake of simplicity we show a classic cryptosystem model used for confidentiality. Such a cryptosystem primitive, also called symmetric encryption algorithm is depicted in Figure 1.1. The transformation of the plaintext (message) into the ciphertext is called encryption or enciphering and it involves the use of a secret key. The decryption or deciphering algorithm takes as input the ciphertext and the same key used in encryption, and it outputs the plaintext.

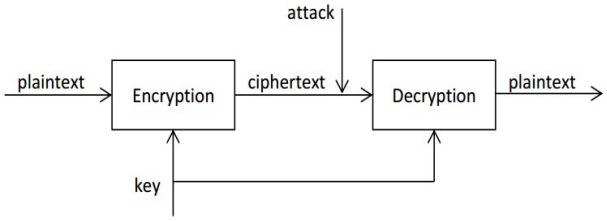

Figure 1.1: Model of classic cryptosystem

Symmetric-key cryptography comprises two large families of cryptographic primitives, namely block and stream ciphers. However, both block and stream ciphers only offer computational security as there is no reduction to a well-known hard problem that would lead to a provable security (as in the case of public-key cryptography), no matter how controversial this notion might be. These ciphers rather follow a heuristic design approach that is based on certain well-accepted design rules mostly supported by the experience and the resistance to current cryptanalysis. In the case of block ciphers, the use of pseudo random permutation based either on Feistel or SP (Substitution Permutation) network is an efficient and well-understood design method that resulted in several strong schemes such as Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES) (current encryption standard) etc.. When stream ciphers are taken into consideration the situation is quite different. Apart from a few exceptions such as RC4 or Grain, most of the recent proposals, including the eSTREAM open competition proposals towards standardization of stream ciphers, have failed in providing the claimed security level and have been successfully cryptanalyzed within a short time frame. Nevertheless, the security of both design schemes heavily relies on the cryptographic robustness of certain primitives known as Substitution boxes (S-boxes), which consists of a single or a set of Boolean functions whose selection and cryptographic properties are application/design dependant.

The concept of public-key cryptography evolved from an attempt to solve two problems, key distribution and the development of digital signatures. It uses an asymmetric-key pair: a public-key and a private-key. The public key is used to encrypt plaintext or to verify a digital signature, whereas the private key is used to decrypt ciphertext or to create a digital signature. But all known public key cryptosystems are much less efficient than symmetric cryptosystems. They produce a much lower data throughput, because they need much time to encrypt long messages, and also need much longer keys to ensure the same level of security. Due to its superior performance in terms of encryption speed compared to public key cryptography, symmetric-key encryption primitives are inevitable building blocks in modern cryptography.

There are four main classes of attacks that can be mounted on a cryptosystem. These classes are encountered below with respect to the power of the adversary.

(i) ciphertext-only - the cryptanalyst tries to recover the encryption key, or a part of the key, or a portion of the plaintext by only observing the ciphertext;

(ii) known-plaintext - the cryptanalyst tries to recover the key or a part of the key, when he has some plaintext and the corresponding ciphertext at his disposal.

(iii) chosen-plaintext - the aim of the attack is to extract the key or decrypt other plaintext. In this case the cryptanalyst is able to choose any plaintext and to obtain the corresponding ciphertext.

(iv) chosen-ciphertext - this case is similar to chosen-plaintext attacks. The main difference is that we assume that the adversary has access to the decryption equipment and can decrypt any ciphertext. Then, the objective is to deduce the key, which can be securely embedded in the equipment, from the ciphertext-plaintext pairs.

Differential cryptanalysis has become a major cryptanalyst's tool when attacking iterated block ciphers. This cryptanalysts' discipline has its origin in the breakthrough paper by Eli Biham and Adi Shamir [6] in 1990. Basically, differential cryptanalysis is a chosen-plaintext attack though it can be modified into a known-plaintext attack provided that sufficiently many plaintexts are available. In brief, differential cryptanalysis analyzes and exploits the effect of certain differences in the plaintext pairs on the differences on the ciphertext pairs. It has been demonstrated by Biham and Shamir that even up to 15 rounds of DES (out of sixteen) could be broken faster than an exhaustive search, whereas a truncated DES version of up to 8 rounds could be broken in few minutes. This technique has later evolved into more advanced attacks such as *differential-linear analysis* by Susan K. Langford and Martin E. Hellman [55], *truncated* and *higher order differential analysis* of Lars Knudsen and Thomas Jakobsen [53, 49].

Linear cryptanalysis was introduced by Mitsuru Matsui [63] and has been considered as one of the most powerful attacks on DES to date. In such an attack the

cryptanalyst exploits a linear relation between some bits of the plaintext, some bits of the ciphertext and some bits of the key. Matsui showed that provided the relation does not hold exactly half the time (the distance of a Boolean function, in some S-box, to a certain linear function is small) then it is possible to extract the key information by applying a large number of known plaintext-ciphertext pairs. The efficiency of such an attack is best illustrated in the original paper of Matsui where breaking twelve rounds of DES took only 50 hours assuming 2^{31} known plaintext-ciphertext pairs.

Boolean functions (that is, functions from the vector space $\mathbb{F}_2^n$ of all binary vectors of length n, to the binary field with two elements $\mathbb{F}_2$) play therefore an important role in the design of symmetric ciphers. They are often used as nonlinear combining functions in stream ciphers based on Linear Feedback Shift Register (LFSR) (shown in Figure 1.2)

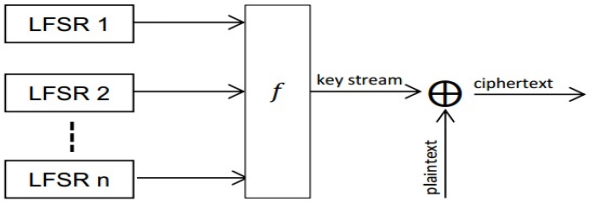

Figure 1.2: LFSR-based stream cipher

Symmetric cryptography is a very attractive research area with several areas of applications such as GSM mobile phones, Bluetooth, WLAN connections, and especially for radio frequency identification (RFID) schemes. The building blocks of these cryptosystems commonly employ Boolean functions but also vectorial Boolean functions, called S-boxes, that output several bits at the time (thus mappings $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$). A necessary condition for a symmetric-key encryption scheme to be unconditionally secure is that the encryption key is at least as long as the message. Also, Shannon [90] introduced two extremely important concepts which have been extensively used in design of modern ciphers, namely *confusion* and *diffusion*. Confusion aims at making the algebraic description of the cipher extremely complex. Furthermore, according to Shannon's postulates the associated equations should involve a great portion of the secret key bits and plaintext/ciphertext bits. It is closely related to the complexity of the involved Boolean functions. Diffusion consists in spreading out the influence of any minor modification of the input data or of the key over all outputs. To provide the robustness of the cipher to known cryptanalytic tools, Boolean functions must satisfy certain cryptographic criteria as:

(i) high algebraic degree - all cryptosystems using Boolean functions for confusion can be attacked if the functions have relatively low degree;

(ii) high nonlinearity - cryptographic functions must have a large distance to all

affine functions, which means that affine approximation of the cipher is rather inefficient when used in so-called affine approximation attacks;

(iii) balancedness - cryptographic functions must be balanced functions (its output column in the truth table contains equal number of 1's and 0's) for avoiding statistical dependence between the input and the output;

(iv) high algebraic immunity of order m - the output of Boolean function must be statistically independent of any linear combination of any subset of m inputs;

(v) resistance to differential cryptanalysis - the function has good differential properties;

(vi) efficient computation and compatibility.

The major problem related to finding cryptographically strong functions is the fact that the multiple criteria mentioned above need to be satisfied simultaneously. In addition, the function space of a Boolean function mapping n binary (input) bits to a single binary (output) bit is enormous 2^{2^n}, thus even when $n = 6$ an exhaustive search for cryptographically strong functions becomes infeasible. The following table shows the function space of Boolean function for n ranging between 4 and 8.

Table 1.1: The function space of Boolean function

n	4	5	6	7	8
2^{2^n}	2^{16}	2^{32}	2^{64}	2^{128}	2^{256}

Bent functions, as a special class of Boolean functions, are extremal combinatorial objects with several areas of application, such as coding theory, maximum length sequences, cryptography, the theory of difference sets to name a few. The term bent Boolean function was introduced by Rothaus [85], and later further investigated by Maiorana and McFarland [66] and Dillon [36]. These functions are actually furthest away from the set of affine functions, implying that these functions offer a highest resistance to affine approximation attacks. Among other equivalent characterization of bent functions, the one that is most often used is a characterization of bent functions as a class of Boolean functions having so-called a flat Walsh spectrum. It means that for any bent function over $\mathbb{F}_2^n$, its Hamming distance to any affine function in n variables is constant, including the distance to the all-zero function (or all-one function).

One of these classes is defined by $f(x, y) = x \cdot \pi(y) \oplus g(y)$ for all $x, y \in \mathbb{F}_2^{n/2}$, where $\pi(y)$ is any permutation on $\mathbb{F}_2^{n/2}$ and g is any Boolean function on $\mathbb{F}_2^{n/2}$. Here $\oplus$ denotes the addition modulo two and "$\cdot$" denotes the inner product in $\mathbb{F}_2^{n/2}$. Another pioneering work on bent functions is also due to Dillon [36], who introduced and analyzed another important class of bent functions called partial spread ($\mathcal{PS}$). He

also studied a subclass of it named the $\mathcal{PS}_{ap}$ class, functions belonging to which could be explicitly represented by bivariate polynomials over finite fields. In 1994, Carlet [19] gave two new classes of bent functions. These combinatorial objects were later extensively studied in many articles, see e.g. [11, 20, 39], and though there are numerous results on the classification of these functions this work seems to be elusive.

The main complexity characteristics for Boolean functions on the vector space $\mathbb{F}_2^n$ which are relevant to cryptography [32, 70, 92] are the algebraic degree and the nonlinearity. Bent functions attain the maximal nonlinearity, hence providing the best resistance to powerful affine approximation attacks [63] when used as primitives in the design of certain key stream algorithms such as filter generators and combiner generators, for the latter see Fig.1.2. Moreover, vectorial bent functions are also suitable as S-boxes in the design of blocks ciphers, due to their exceptional differential properties.

Dealing with error correcting codes [62], where every code of length 2^n can be interpreted as a set of Boolean functions, since every n-variable Boolean function can be represented by its truth table and thus associated with a binary word of length 2^n and vice versa, bent functions are related to Reed-Muller and Kerdock code [15]. This characterization is of particular importance since it provides nonlinear codes with parameters that linear codes cannot achieve. The first order Reed-Muller code consists of all affine functions on $\mathbb{F}_2^n$ and, in the case n is even, bent functions on $\mathbb{F}_2^n$ can be characterized as the functions having the maximal possible distance to all the codewords in the first order Reed-Muller code. On the other hand, Kerdock codes can be seen as a set of quadratic bent functions.

In combinatorics, they are equivalent to difference sets in elementary Abelian 2-groups [35, 64]. A Boolean function f on $\mathbb{F}_2^n$ can be characterized by its support, i.e., by the set $S = \{x \in \mathbb{F}_2^n : f(x) = 1\}$. It is well-known that the set S is a nontrivial difference set in $\mathbb{F}_2^n$ if and only if f is a bent function [83]. Thus, characterizing all nontrivial difference sets in $(\mathbb{F}_2^n, +)$ is equivalent to the characterization of all the bent functions. Partial difference sets are combinatorial objects corresponding to strongly regular graphs [60]. Given a Boolean function $f : \mathbb{F}_2^n \mapsto \mathbb{F}_2$, we can associate the Cayley graph G_f, where the vertex set of G_f is equal to $\mathbb{F}_2^n$, while the set of edges E_f of G_f is defined as $E_f = \{(u, v) \in \mathbb{F}_2^n \times \mathbb{F}_2^n : f(u \oplus v) = 1\}$. It was shown in [4, 5], that f is a bent function if and only if for all vertices u, v the number of vertices adjacent to both u and v is constant, which means that the Cayley graph G_f is a strongly regular graph. Hence, bent functions can be used to construct strongly regular graphs [94], and therefore the constructions of bent functions are very important and have been extensively studied in the literature.

A complete classification of bent functions seems to be elusive today. One special family is the class of *monomial bent functions*, i.e., Boolean function represented as $x \mapsto Tr(ax^d)$ for an exponent d and a fixed coefficient $a \in \mathbb{F}_{2^n}$ (see Section 2.1). This class of bent functions is of particular importance because it provides the only known examples of so-called nonnormal bent functions [12]. Monomial Boolean trace

bent functions of the form $Tr_1^n(ax^d)$ have been considered in several works [9, 26, 38, 56], and according to our best knowledge the functions in these references are the only known classes of monomial trace bent functions (up to affine equivalence). An explicit characterization of the exponent d and the corresponding a that define a bent monomial function on $\mathbb{F}_{2^n}$ is a difficult open problem.

Another special family is the class of *binomial bent functions*, i.e., of Boolean functions constructed via a linear combination of several power functions. Binomial (or generally multiple) trace bent functions are harder to analyze and only a few classes of these functions have been exhibited [25, 39]. The result of Dobbertin and Leander [39] related to so-called linear Niho exponents (that is, the restriction of x^d on $\mathbb{F}_{2^{n/2}}$ is linear) was later generalized in [57], where the existence of bent functions with multiple trace terms consisting of 2^r Niho exponents were confirmed. The framework was later extended in [25], where a characterization of bent Boolean functions was given in terms of Dickson polynomials and Kloosterman sums. A few other classes of binomial hyperbent trace functions [21, 102], using one monomial with absolute trace and the other with relative trace, was reported in [71, 95].

The bent property of Boolean functions may be extended to vectorial mappings $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ by requesting that all nonzero linear combinations of the component functions of F are also bent. This means that representing $F(x) = (f_1(x), \ldots, f_m(x))$ as a collection of m Boolean functions f_i any nonzero linear combination of the form $a_1 f_1(x) + \ldots + a_m f_m(x)$, where a_i are binary, is again bent. In terms of the trace representation using the isomorphism between $\mathbb{F}_2^n$ and $\mathbb{F}_{2^n}$, this corresponds to the property that $Tr_1^m(\lambda F(x))$ is bent for any $\lambda \in \mathbb{F}_{2^m}^*, x \in \mathbb{F}_{2^n}$. The construction of such *vectorial bent functions* has been initially considered by Nyberg in [77]. It has been shown in [77], that vectorial bent functions can only exist for $m \leq n/2$, and can be constructed using some known classes of bent functions, namely the Maiorana-McFarland class [36, 37, 85] and the Dillon's partial spread class [15, 36, 37]. The same problem has also been treated in [39, 100], and more recently in [40, 80]. What is common to all these approaches is the underlying idea of specifying m bent Boolean functions in a particular way, so that their linear combinations remain bent. It was shown in [80] that the function $F(x) = Tr_k^n(ax^d)$, where $n = 2k$ is a vectorial bent function, assuming that $f(x) = Tr_1^n(ax^d)$ is a bent function and x^d is a permutation over $\mathbb{F}_{2^k}$. But the property of x^d being a permutation on $\mathbb{F}_{2^k}$ is only a sufficient condition but not necessary, and furthermore the functions with multiple trace terms have not been treated. The necessary and sufficient conditions for the vectorial functions given in a multiple trace form to be bent, is given in Section 3 (see Theorem 3.3.1).

On the other hand, the vectorial bent property of F can alternatively be expressed in terms of the coefficients of elementary symmetric polynomials [59] related to evaluation of F on the cyclic group of the $(2^k + 1)$th primitive roots of unity in $\mathbb{F}_{2^{2k}}$. The hardness of evaluating these symmetric polynomials for multiple trace functions restricts our analysis to the case of binomial trace functions, but even for these cases only some necessary bent conditions are derived. These conditions

are very useful for the exclusion of certain choices of the coefficients γ, z for which $F(x) = Tr_k^n(x + \gamma z x^{r(2^k-1)})$ cannot be vectorial bent (see Section 3.4). In Section 3.5 it is shown that $Tr_k^n(\lambda x^{r(2^k-1)})$ is never a vectorial bent function of the maximum dimension k.

A generalization of bent functions to nonbinary fields of odd characteristic was first suggested by Kumar, Scholtz and Welch in [54]. The class of p-ary bent functions has not received enough attention yet, and according to our best knowledge only a few classes of binomial trace functions have been characterized in terms of bentness in [105], and recently in [101], and also in [46, 58]. Chapter 4 confirms that the conditions derived originally in [105] are valid for multinomial trace functions $f : \mathbb{F}_{p^n} \mapsto \mathbb{F}_p$ with Dillon's exponents $f(x) = Tr_1^n(\sum_{i=1}^t a_i x^{r_i(p^k-1)})$. It is shown that the choice of a_i and r_i, ensuring that f is bent, is directly related to the image of a certain subset of $\mathbb{F}_{p^n}^*$ into a union of disjoint multiplicative cosets, see Chapter 4). A complete classification of generalized bent functions is naturally a much harder task compared to the binary case.

The construction methods of designing resilient Boolean functions with high algebraic degrees, high nonlinearities and good immunity to (fast) algebraic attacks are of great importance due to the possibility of using (vectorial) Boolean function as filtering functions in certain LFSR-based encryption algorithms such as nonlinear combiner and filtering generators. A great variaty of design methods have been proposed during the last two decades [14, 17, 24, 50, 51, 65, 78, 82, 86, 87, 89, 96, 97]. Satisfying all the relevant cryptographic criteria simultaneously is in many cases impossible due to different trade-offs among the design parameters. For instance, Siegenthaler [91] proved that for n-variable balanced function, of degree d and order of resiliency m, it holds $m + d \leq n - 1$ if $m \leq n - 2$. The exact nature of trade-offs among order of correlation immunity, nonlinearity and algebraic degree has also been investigated in [16, 87, 97, 106]. Recently, a recursive construction method of optimal plateaued functions with relatively large order of resiliency is given in [43]. Chapter 5 generalizes the use of *disjoint spectra functions* by showing that given two n-variable disjoint spectra functions f and g any concatenation of 2^k functions from either $\{f, 1 + f\}$ or from $\{g, 1 + g\}$ will give again a pair of $(n + k)$-variable disjoint spectra functions for any $k \geq 0$ (see Proposition 5.3.1). The importance of this result lies in the fact that we can control the nonlinearity and resiliency of these functions by using a suitable configurations of the function and its complement. The generalization of this approach is then straightforward (see Theorem 5.3.1). An iterative construction method of disjoint spectra functions, which gives a multiple branching tree of infinite sequences of optimal plateaued functions, is proposed in Section 5.3. Moreover, a pair of $(n + k)$-variable disjoint spectra functions represents so called *semi bent Boolean functions* [29]. In general, disjoint spectra (semi-bent) functions, commonly used in iterative constructions of cryptographically strong functions, are not rare combinatorial objects. The construction method of semi-bent function is proposed in Section 5.2.

In [104], Zhang and Zheng introduced the global avalanche characteristic (GAC) to overcome the shortcomings of the propagation criterion and the strict avalanche criterion, to comprehend the overall propagation characteristics of a cryptographic function. It was also shown that the propagation characteristics of any Boolean function refer to certain properties of its derivatives [104].

The motivation behind the characterization of Boolean functions in terms of the cross-correlation properties can be traced back to information theoretic aspects of security such as the two fundamental concepts of confusion and diffusion introduced by Shannon. To achieve a sufficient amount of confusion and diffusion the constituent Boolean functions in the cipher should have a low cross-correlation to each other, as originally proposed by Sarkar and Maitra [88]. In addition, a useful characterization of some important classes of cryptographic Boolean functions in terms of their cross-correlation properties was established in [88] and certain weaknesses of commonly used S-boxes were also identified. The analysis of a given S-box was performed by measuring the cross-correlation between the component functions $f_1, \ldots, f_m$ of the S-box, thus representing an S-box as a vectorial Boolean mapping $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ [88].

Nevertheless, a further generalization of these criteria was considered in [110] by introducing two additional indicators for measuring cross-correlation properties of two Boolean function (as in the case of autocorrelation). Chapter 6 proposes several construction methods of highly nonlinear S-boxes whose cross-correlation properties of their component functions are very good. In Section 6.2 it is shown that a sufficient condition that so-called absolute indicator (cf. Section 2.2) attains its lowest possible value $2^{n/2}$ is that $f + g$ is also a bent function. In addition, a practical method of constructing perfectly uncorrelated S-boxes, for an even number of input variables, is given in Section 6.2.2.

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

- A. Muratović-Ribić, E. Pasalic, and S. Bajrić. Vectorial bent functions from multiple terms trace functions. *IEEE Transaction on Information Theory,* vol. 60, no. 2, pp. 1337–1347, 2014.
- S. Bajrić, E. Pasalic, A. Ribić-Muratović, and S. Gangopadhyay. On generalized bent functions with Dillon's exponents. *Information Processing Letters*, vol. 114, no. 4, pp. 222–227, 2014.
- E. Pasalic, S. Bajrić, M. Djordjević. On cross-correlation properties of S-boxes and their design using semi-bent functions. Accepted for publication in *Security and Communication Networks.*
- S. Bajrić, S. Gangopadhyay, E. Pasalic, and W. Zhang. Designing semi-bent, disjoint spectra and optimal plateaued functions. *Submitted manuscript,* 2014.

Chapter 2

Boolean Functions and S-Boxes

All truths are easy to undestand once they discovered. The point is discover them.

– Galileo Galilei

THE PURPOSE of this chapter is to give some preliminary definitions on Boolean functions and S-boxes relevant to cryptography, and introduce one of the most important tools in cryptography, namely the Walsh transform. The Walsh transform is most efficient tool for examining certain cryptographic properties of (vectorial) Boolean functions.

2.1 Boolean Functions

Let $\mathbb{F}_2^n$ denote the vector space of dimension n over the field $\mathbb{F}_2$ (Galois field with two elements). For two vectors $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ in $\mathbb{F}_2^n$ we define the scalar product as $x \cdot y = x_1 y_1 \oplus \ldots \oplus x_n y_n$, where the multiplication and addition are over $\mathbb{F}_2$. Addition operator over $\mathbb{F}_2$ denoted by $\oplus$, is often replaced with usual addition operator $+$, when no confusion is to arise.

A *Boolean function* on n variables may be viewed as a mapping from $\mathbb{F}_2^n$ into $\mathbb{F}_2$. The set of all n-variable Boolean functions, $f : \mathbb{F}_2^n \mapsto \mathbb{F}_2$, is denoted by $\mathfrak{B}_n$.

Let $\mathbb{F}_{2^n}$ denote the finite Galois field $GF(2^n)$ consisting of 2^n elements. The group of units of $\mathbb{F}_{2^n}$, denoted by $\mathbb{F}_{2^n}^*$, is a cyclic group consisting of $2^n - 1$ elements. An element $\alpha \in \mathbb{F}_{2^n}$ is said to be a primitive element if it is a generator of the multiplicative group $\mathbb{F}_{2^n}^*$. Once the basis of the field is fixed, say $(\gamma_0, \ldots, \gamma_{n-1})$ so that $\alpha = \alpha_0\gamma_0 + \ldots + \alpha_{n-1}\gamma_{n-1}$, where $\gamma_i \in \mathbb{F}_{2^n}$ and $\alpha_i \in \mathbb{F}_2$, there is a natural

isomorphism between $\mathbb{F}_{2^n}$ and $\mathbb{F}_2^n$ given by

$$\alpha_0\gamma_0 + \ldots + \alpha_{n-1}\gamma_{n-1} \in \mathbb{F}_{2^n} \longmapsto (\alpha_0, \ldots, \alpha_{n-1}) \in \mathbb{F}_2^n.$$

Any function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ is said to be a *Boolean function* on n variables.

Truth Table (TT)

A Boolean function $f(x_1, \ldots, x_n)$ is also interpreted as the output column of its *truth table f*, i.e., a binary string of length 2^n,

$$f = [f(0, 0, \ldots, 0), f(1, 0, \ldots, 0), \ldots, f(1, 1, \ldots, 1)].$$

The *Hamming weight* of any binary vector y is $wt(y) = \#\{i : y_i = 1\}$, where $\#A$ denotes the cardinality of any set A. The *Hamming distance* between two functions $f, g \in \mathfrak{B}_n$ [1] is denoted by $d_H(f, g)$ and defined by

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

An n-variable function f is said to be *balanced* if its output column in the truth table contains equal number of 1's and 0's, i.e., its Hamming weight is $wt(f) = 2^{n-1}$.

Algebraic Normal Form (ANF)

Any Boolean function has a unique representation as a multivariate polynomial over $\mathbb{F}_2$, called *algebraic normal form* (ANF),

$$f(x_1, \ldots, x_n) = a_0 + \sum_{1 \leq i \leq n} a_i x_i + \sum_{1 \leq i < j \leq n} a_{ij} x_i x_j + \ldots + a_{12\ldots n} x_1 x_2 \ldots x_n \qquad (2.1)$$

where the coefficients $a_0, a_{ij}, \ldots, a_{12\ldots n}$ belong to $\{0, 1\}$.

The *algebraic degree*, denoted by $deg(f)$, is the number of variables in the highest order monomial with nonzero coefficient. A Boolean function with $deg(f) \leq 1$ is said to be *affine* and the set of all n-variable affine functions is denoted by $\mathcal{A}_n$. An affine function with the constant term equal to zero is called a *linear* function. There is a one-to-one correspondence between the truth table and the ANF via so-called inversion formulae.

Trace Representation

The *trace function* $Tr_m^n : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^m}$, a mapping to the subfield $\mathbb{F}_{2^m}$, where $m \mid n$, is defined as

$$Tr_m^n(x) = x + x^{2^m} + x^{2^{2m}} + \ldots + x^{2^{(n/m-1)m}}, \text{ for all } x \in \mathbb{F}_{2^n}. \qquad (2.2)$$

[1] For shortness, we use the notation f instead of more correct $f(x_1, \ldots, x_n)$. It should be clear from the context, whether by f we refer to the truth table of the function $f(x)$ or to its algebraic normal form.

The absolute trace $Tr_1^n : \mathbb{F}_{2^n} \mapsto \mathbb{F}_2$, also denoted by Tr, then maps to the prime field. A cyclotomic coset modulo $2^n - 1$ of $s \in \mathbb{Z}$ is defined as [62, page 104]

$$C_s = \{s, s2, s2^2, \ldots, s2^{n_s-1}\}, \tag{2.3}$$

where n_s is the smallest positive integer such that $s \equiv s2^{n_s} \pmod{2^n - 1}$. It is a convention to choose the subscript s to be the smallest integer in C_s and refer to it as the coset leader of C_s and n_s is the size of the cyclotomic coset C_s. The *trace representation* [45] of any function $f \in \mathfrak{B}_n$, which is unique, is

$$f(x) = \sum_{s \in \Gamma(n)} Tr_1^{n_s}(A_s x^s) + A_{2^n-1} x^{2^n-1}, \text{ for all } x \in \mathbb{F}_{2^n}, \tag{2.4}$$

where $\Gamma(n)$ is the set of all coset leaders modulo $2^n - 1$, and $A_s \in \mathbb{F}_{2^{n_s}}$, $A_{2^n-1} \in \mathbb{F}_2$, for all $s \in \Gamma(n)$. A Boolean function is said to be a *monomial trace function* or, equivalently, to have a *monomial trace representation* if its trace representation consists of only one trace term, otherwise it is called a *multiple (term) trace function.*

Walsh Transform

The cryptographic properties of a Boolean function are most easily reflected through its Walsh transform.

Definition 1 *The* Walsh transform *of $f \in \mathfrak{B}_n$ in point $\alpha \in \mathbb{F}_2^n$ is denoted by $W_f(\alpha)$ and calculated as,*

$$\alpha \in \mathbb{F}_2^n \longmapsto W_f(\alpha) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+\alpha \cdot x}. \tag{2.5}$$

The values $W_f(\alpha)$ are called the Walsh coefficients of the Boolean function f, and the set $\{W_f(\alpha) : \alpha \in \mathbb{F}_2^n\}$ is called the Walsh spectrum of f.
The Hamming distance between a Boolean function $f(x)$ and an affine function $g(x) = \alpha \cdot x + b$ ($\alpha \in \mathbb{F}_2^n$ and $b \in \mathbb{F}_2$) can be calculated via the Walsh transform

$$d_H(f, g) = 2^{n-1} - \frac{(-1)^b W_f(\alpha)}{2}. \tag{2.6}$$

An important property of Walsh spectrum, referred to as Pareseval's equality [62], states that for any Boolean function $f \in \mathfrak{B}_n$,

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

Over $\mathbb{F}_{2^n}$, the Walsh transform of the Boolean function f can be calculated as (using $Tr_1^n(ax)$ to represent the scalar product $a \cdot x$)

$$a \in \mathbb{F}_{2^n} \longmapsto W_f(a) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+Tr_1^n(ax)}. \tag{2.7}$$

2.2 Basic Definitions on Boolean Functions

Probably the most important measure of the cryptographic strength of Boolean functions is nonlinearity. More or less all known attacks utilize the fact that there must be a correlation between a given function f and some affine function.

Definition 2 *The* nonlinearity *of $f \in \mathfrak{B}_n$, denoted by $\mathcal{N}_f$, is defined to be the Hamming distance from the set of all n variable affine functions,*

$$\mathcal{N}_f = \min_{g \in \mathcal{A}_n} d_H(f, g). \tag{2.8}$$

In terms of the Walsh spectrum, the nonlinearity of f is given by

$$\mathcal{N}_f = 2^{n-1} - \frac{1}{2} \max_{\alpha \in \mathbb{F}_2^n} |W_f(\alpha)|. \tag{2.9}$$

The correlation immunity of function f introduced by Siegenthaler [91] refers to the function's ability not to leak the information from a single or a small number of input variables to the output. This property is of particular importance in the design of certain LFSR-based encryption schemes such as the nonlinear combiner depicted in Fig. 1.2.

Definition 3 *A Boolean function $f(x)$ on n variables is said to be m-th order* correlation immune *(m-CI), if for any m-tuple of independent identically distributed binary random variables $x_{i_1}, x_{i_2}, \ldots, x_{i_m}$, we have*

$$I(x_{i_1}, x_{i_2}, \ldots, x_{i_m}; f(x)) = 0, \quad 1 \le i_1 < i_2 < \cdots < i_m \le n, \tag{2.10}$$

where $I(x; f(x))$ denotes the mutual information [10].

Definition 4 *An m-th order correlation immune function Boolean function f which is balanced, is called an m-*resilient *function.*

In terms of the Walsh spectrum, an n-variable Boolean function is m-th order correlation immune (m-CI) if and only if its Walsh spectrum satisfies

$$W_f(0) = 0, \text{ for all } u \in \mathbb{F}_2^n \text{ such that } 1 \le wt(u) \le m.$$

A function is balanced if and only if $W_f(0) = 0$, i.e., $\#\{x|f(x) = 0\} = \#\{x|f(x) = 1\}$. A balanced m-CI function is said to be m-resilient.

The *concatenation* of the Boolean functions means that their truth tables are merged. For instance, for $f_1, f_2 \in \mathfrak{B}_n$ one may construct $f = x_{n+1}(f_1 + f_2) + f_1 \in \mathfrak{B}_{n+1}$, meaning that the upper half part of the truth table of f corresponds to the truth table of f_1 and the lower half part of the truth table of f corresponds to the truth table of f_2.

Given $f(x) \in \mathfrak{B}_n$, define $AN(f) = \{g(x) \in \mathfrak{B}_n | f(x) \cdot g(x) = 0, \forall x \in \mathbb{F}_2^n\}$. Any function $g \in AN(f)$ is called an *annihilator* of f. *The algebraic immunity*, denoted by $AI_n(f)$, of function $f(x) \in B_n$ is the minimum degree of all non-zero annihilators of $f(x)$ and $f(x) + 1$.

Autocorrelation Properties

The *autocorrelation properties*, also called *propagation properties* or *differential properties*, of f are described by the behavior of its derivatives.

Definition 5 *The* derivative *of $f \in \mathfrak{B}_n$ with respect to any direction $a \in \mathbb{F}_2^n$, is the mapping $D_a f : x \longmapsto f(x) + f(a + x)$.*

The notion of derivative of a Boolean function is extended to higher orders as follows.

Definition 6 *Suppose $\{a_1, a_2, \ldots, a_k\}$ is a basis of a k-dimensional subspace V of $\mathbb{F}_2^n$. The k-*th derivative *of f with respect to V, denoted by $D_V f$, is a Boolean function defined by*

$$D_V f(x) = D_{a_k} D_{a_{k-1}} \ldots D_{a_1} f(x), \text{ for all } x \in \mathbb{F}_2^n. \tag{2.11}$$

The function $f \in \mathfrak{B}_n$ is said to satisfy propagation criterion (PC) of order p (PC(p)), when $D_a f$ is balanced for any $a \in \mathbb{F}_2^n$ such that $1 \leq wt(a) \leq p$. The strict avalanche criterion (SAC), which also relates to the differential properties of S-boxes, and it actually corresponds to PC(1), implying that $D_a f$ is balanced for all a of weight one.

The main indicators of propagation characteristics, namely, the *absolute indicator* and the *sum-of-squares indicator* were introduced by Xian-Mo Zhang and Yuliang Zheng [107]:

$$\Delta_f = \max_{a \in \mathbb{F}_2^n,\ a \neq 0} \mid W_{D_a f}(a) \mid \quad \text{and} \quad \sigma_f = \sum_{a \in \mathbb{F}_2^n} W_{D_a f}^2(a) \ . \tag{2.12}$$

Notice that $0 \leq \Delta_f \leq 2^n$ and the upper bound corresponds to the existence of so-called linear structures, meaning that the derivative $D_a f(x)$ is constant for some $a \in \mathbb{F}_2^n \setminus \{0\}$. A function exhibits *good propagation characteristics* when its autocorrelation function, defined by

$$A_f(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+f(x+a)},$$

takes "small" (absolute) values.

Definition 7 *The cross-correlation between $f, g \in \mathfrak{B}_n$ at direction $\alpha \in \mathbb{F}_2^n$ is an integer-valued function $C : \mathbb{F}_2^n \to [-2^n, 2^n]$ defined by,*

$$C_{f,g}(\alpha) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+g(x+\alpha)}. \tag{2.13}$$

The two indicators above are then defined in terms of cross-correlation as follows [112]:

$$\Delta_{f,g} = \max_{\alpha \in \mathbb{F}_2^n} \mid C_{f,g}(\alpha) \mid \text{ and } \quad \sigma_{f,g} = \sum_{\alpha \in \mathbb{F}_2^n} C_{f,g}^2(\alpha) \ . \tag{2.14}$$

Two n-variable Boolean functions $f, g \in \mathfrak{B}_n$ are said to be *perfectly uncorrelated* if $C_{f,g} = 0$ for all $\alpha \in \mathbb{F}_2^n$, which is true if and only if $W_f(\alpha)W_g(\alpha) = 0$ for all $\alpha \in \mathbb{F}_2^n$, see [88]. Equivalently, f and g are so-called *disjoint spectra* functions.

2.3 Some special classes of Boolean functions

As already mentioned, bent functions attain the maximal distance to the set of affine functions, thus they achieve the maximum possible nonlinearity. The following definition summarizes some properties of bent functions.

Definition 8 *Let $f(x)$ be a Boolean function on $\mathbb{F}_2^n$, where n is even. The following statements (among other characterizations) are equivalent*

(i) *$f(x)$ is a bent function;*

(ii) *$W_f(\alpha) = \pm 2^{\frac{n}{2}}$ for any $\alpha \in \mathbb{F}_2^n$;*

(iii) *$D_a f(x) = f(x)+f(x+a)$ is balanced for any non-zero $a \in \mathbb{F}_2^n$, that is, f satisfies PC(n);*

(iv) *$f(x) + \alpha \cdot x$ is a bent function for any $\alpha \in \mathbb{F}_2^n$.*

The property *(ii)* means that the bent functions are at the same distance to any linear (affine) function, thus according to the Parseval's equality they achieve the maximum possible nonlinearity $\max_{f \in \mathfrak{B}_n} \mathcal{N}_f = 2^{n-1} - 2^{\frac{n}{2}-1}$. Also, bent functions are clearly neither balanced nor correlation immune of any order. Considering the item *(iii)*, this class of functions is the only one having a perfect balancedness in the autocorrelation domain, that is, all nonzero derivatives are balanced. Remark that the property in item *(iii)* is also known as perfect nonlinearity property, the notion introduced by Willi Meier and Othmar Staffelbach in [69].

To any bent function $f \in \mathfrak{B}_n$ one can uniquely associate its *dual bent* function $\tilde{f}$ defined implicitly as $(-1)^{\tilde{f}(\omega)} = 2^{-n/2} W_f(\omega)$, for all $\omega \in \mathbb{F}_2^n$.

By (n, m, d, N_f) function we specify an n-variable, m-resilient Boolean function f with algebraic degree d and nonlinearity N_f.

Definition 9 *A Boolean function $f(x) \in \mathfrak{B}_n$ is called* plateaued *if its Walsh spectrum only takes three values 0 and $\pm 2^\lambda$, where λ is some positive integer. An m-resilient function $f \in \mathfrak{B}_n$, with $m > n/2 - 2$, is called* optimal plateaued *if f is an $(n, m, n - m - 1, 2^{n-1} - 2^{m+1})$ function.*

Using semi-bent functions have been introduced by Chee *et al.* [29] as a special case of so-called plateaued Boolean functions [107, 108].

Definition 10 *A Boolean function* $f(x) \in \mathfrak{B}_n$ *is said to be* semi-bent function *if*

$$W_f(\omega) \in \begin{cases} \{0, \pm 2^{\frac{n+1}{2}}\}, & \text{if } n \text{ is odd} \\ \{0, \pm 2^{\frac{n+2}{2}}\}, & \text{if } n \text{ is even} \end{cases}, \tag{2.15}$$

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

Notice that the spectrum of plateaued functions is also three-valued of the form $\{0, \pm 2^r\}$, where $r \geq \frac{n+2}{2}$, and therefore semi-bent are maximally nonlinear plateaued functions.

The applications of semi-bent functions are not restricted to cryptography only, but rather these objects are widely used in certain combinatorial designs such as a construction of orthogonal variable spreading factor codes used in Code Division Multiple Access (CDMA) systems [47].

2.4 Vectorial Boolean Functions or S-Boxes

For two positive integers n and m, a function $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ is usually denoted as (n, m)-function and moreover referred to as (n, m) S-box . Representing $F(x) = (f_1(x), \ldots, f_m(x))$, the Boolean functions $f_i(x)$ are called the *coordinate (component)* functions of F. When the numbers m and n are not specified, (n, m)-functions are called *multi-output Boolean functions, vectorial Boolean functions or S-boxes*. Last term, S-box, is the most often used in cryptography, but is dedicated to the vectorial functions whose role is to provide confusion into the system. Such a multiple output function should possess high values in terms of order of resiliency, nonlinearity and algebraic degree.

The nonlinearity of a vectorial function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$, and hereby the resistance to linear cryptanalysis of Matsui [63], is measured through *extended Walsh transform* defined as,

$$W_F(\sigma, \gamma) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr_1^m(\gamma F(x)) + Tr_1^n(\sigma x)}, \ \sigma \in \mathbb{F}_{2^n}, \gamma \in \mathbb{F}_{2^m}^*. \tag{2.16}$$

Alternatively, F is a vectorial bent function if and only if $|W_F(\sigma, \gamma)| = 2^{n/2}$, for any $\gamma \in \mathbb{F}_{2^m}^*$ and any $\sigma \in \mathbb{F}_{2^n}$.

2.5 Generalization to the nonbinary fields

A generalization to nonbinary fields of odd characteristic was first suggested in [54].

The trace function $Tr_m^n : \mathbb{F}_{p^n} \mapsto \mathbb{F}_{p^m}$, a mapping to a subfield $\mathbb{F}_{p^m}$ when $m \mid n$, is defined as

$$Tr_m^n(x) = x + x^{p^m} + x^{p^{2m}} + \ldots + x^{p^{(n/m-1)m}}, \tag{2.17}$$

for all $x \in \mathbb{F}_{p^m}$. The absolute trace $Tr_1^n : \mathbb{F}_{p^n} \to \mathbb{F}_p$, also denoted by Tr, then maps to the prime field.

Definition 11 *The Fourier transform of a function $f : \mathbb{F}_{p^n} \mapsto \mathbb{F}_p$ is defined by*

$$\mathcal{F}(\lambda) = \sum_{x \in \mathbb{F}_{p^n}} \omega^{f(x) - Tr_1^n(\lambda x)}, \quad \lambda \in \mathbb{F}_{p^n}, \tag{2.18}$$

where ω denotes a p-th root of unity, that is, $\omega = e^{\frac{2\pi i}{p}}$, where $i \in \mathbb{C}$ denotes imaginary unit.

A bent function $f(x)$ is called regular if for every $\lambda \in \mathbb{F}_{p^n}$ the normalized Fourier coefficient $p^{-\frac{n}{2}}\mathcal{F}(\lambda)$ equals to complex p-th root of unity, that is, $p^{-\frac{n}{2}}\mathcal{F}(\lambda) = \omega^{g(\lambda)}$ for some function $g : \mathbb{F}_{p^n} \mapsto \mathbb{F}_p$. A binary bent function is always regular. For odd p, a p-ary bent function $f(x)$ may not be regular, but its Fourier transform coefficients satisfy

$$\mathcal{F}(\lambda) = \begin{cases} \pm\omega^{g(\lambda)} p^{\frac{n}{2}}, & \text{if } p^n \equiv 1 \pmod 4 \\ \pm e\omega^{g(\lambda)} p^{\frac{n}{2}}, & \text{if } p^n \equiv 3 \pmod 4 \text{ and } n \text{ is odd} \end{cases}, \tag{2.19}$$

where e is a complex primitive forth root of unity [54].

Chapter 3

Vectorial bent functions from multiple terms trace functions

The weight of evidence for an extraordinary claim must be proportioned to its strangeness.
– Pierre Simon Laplace

THIS CHAPTER is related to several necessary and sufficient conditions for the vectorial functions given in a multiple trace form to be bent. These conditions can be efficiently use for specifying vectorial bent functions given in the particular trace form considered, essentially using the sum of trace monomials with Dillon exponents. The approach based on the use of elementary symmetric polynomials to establish the bentness of binomial trace mappings seems to be an interesting framework for handling the vectorial bent property of these mappings.

The main results are published in [75].

3.1 Introduction

As mentioned, monomial Boolean trace bent functions of the form $Tr_1^n(ax^d)$ have been considered in several works. For $n = 2k$, any monomial trace function $Tr_1^n(ax^d)$ must satisfy certain conditions to be bent. We necessarily have $\gcd(d, 2^n-1) > 1$, and furthermore it was shown that we either have $\gcd(d, 2^k - 1) = 1$ or $\gcd(d, 2^k + 1) = 1$, cf. [56].

Since binomial (or generally multiple) trace bent functions are harder to analyze, only a few classes of these functions have been exhibited [25, 39]. The result of Dobbertin and Leander [39] related to so-called linear Niho exponents was later generalized in [57], where the existence of bent functions with multiple trace terms consisting of 2^r Niho exponents were confirmed. The framework was later extended in [25], where a

characterization of bent Boolean functions on $\mathbb{F}_{2^n}$ of the form $\sum_{r\in R} Tr_1^n(\lambda_r x^{r(2^k-1)})$, where R is a set of representatives of cyclotomic cosets modulo 2^k+1 [25], was given in terms of Dickson polynomials and Kloosterman sums. A few other classes of binomial hyperbent trace functions, using one monomial with absolute trace and the other with relative trace, was reported in [71, 95]. It is well-known that the bent property of Boolean functions may be extended to vectorial mappings $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ by requesting that all nonzero linear combinations of the component functions of F are also bent, i.e., $Tr_1^m(\lambda F(x))$ is bent for any $\lambda \in \mathbb{F}_{2^m}^*$, $x \in \mathbb{F}_{2^n}$. The bent property of functions $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$, for $\mathbb{F}_{2^m} \subset \mathbb{F}_{2^n}$, may be established directly, as it was done in [39] for the binomial trace functions $Tr_1^n(ax^{d_1} + bx^{d_2})$ with Niho's exponents, for $a, b \in \mathbb{F}_{2^n}$, due to the particular choice of the exponents d_1, d_2.

In this chapter, we firstly consider a special class of trace functions of the form $f(x) = Tr_1^n(\sum_{i=1}^r \lambda_i x^{d_i})$ on $\mathbb{F}_{2^n}$ (assuming $n = 2k$) that are possibly bent, and a sufficient condition on d_is is derived so that if f is bent then the vectorial function $F(x) = Tr_m^n(\sum_{i=1}^r \lambda_i x^{d_i})$, $m \mid n$, is also bent. In difference to the approach taken in [39, 57], where linear Niho exponents are used, we consider a more general framework by allowing the use of "nonlinear" exponents, that is $d_i \not\equiv 2^j \pmod{2^m-1}$ in general. Essentially, our idea is to select the exponents so that for a suitably chosen d_1 the remaining exponents d_i are of the form $d_i = d_1 + v_i(2^m - 1)$, for $i = 2, \ldots, r$, and some positive integers v_i. Then, it is shown that if $f(x) = Tr_1^n(\sum_{i=1}^r \lambda_i x^{d_i})$ is bent for suitably chosen $\lambda_i \in \mathbb{F}_{2^n}$, then the sufficient condition for the function $F(x) = Tr_m^n(\sum_{i=1}^r \lambda_i x^{d_i})$ to be a vectorial bent function is that x^{d_1} is a permutation of $\mathbb{F}_{2^m}$ (where d_1 is not necessarily linear in the Niho sense). The condition is not necessary which is demonstrated for some particular choices of d_1, when more precisely $d_1 = 2^m - 1$ so that x^{d_1} is a constant mapping over $\mathbb{F}_{2^m}$.

Nevertheless, our main result concerns the characterization of vectorial bent property of a class of functions of the form $F(x) = Tr_k^{2k}(\sum_{i=1}^t a_i x^{r_i(2^k-1)})$. By utilising the structure of the cyclic group $\mathcal{U}$, three equivalent statements that provide both the necessary and sufficient conditions for F to be a vectorial bent function are derived. While the first condition specifies the bentness of F in terms of certain character sum evaluated over $\mathcal{U}$, its reformulation provides more comprehensive assertion by claiming that F is vectorial bent if and only if $Im(F) = \mathbb{F}_{2^k)} \cup \{0\}$, when F is evaluated on $\mathcal{U}$.

Finally, the vectorial bent property of F can alternatively be expressed in terms of the coefficients of elementary symmetric polynomials related to evaluation of F on $\mathcal{U}$. The hardness of evaluating these symmetric polynomials for multiple trace functions restricts our analysis to the case of binomial trace functions, though even in this case only some necessary bent conditions could be derived. These conditions are in the first place very useful for the exclusion of certain choices of the coefficients γ, z for which $F(x) = Tr_k^{2k}(x + \gamma z x^{r(2^k-1)})$ cannot be vectorial bent. In the case of monomials, it is shown that $Tr_k^{2k}(\lambda x^{r(2^k-1)})$ is never a vectorial bent function of the maximum dimension k. Interestingly enough, it is also shown that linearized

polynomials can be used in an elegant and efficient way for establishing multiple bent property for certain trace binomials.

3.2 Vectorial bent functions with nonlinear Niho exponents

We derive a sufficient condition for a Boolean bent function of the form $f(x) = Tr_1^{2k}(\sum_{i=1}^{r} \lambda_i x^{d_i})$, so that its associated mapping $F : \mathbb{F}_{2^{2k}} \to \mathbb{F}_{2^k}$, where $F(x) = Tr_k^{2k}(\sum_{i=1}^{r} \lambda_i x^{d_i})$, is a vectorial bent function. The sufficient condition applies to certain choices of the exponents d_i. That is, d_1 is such that x^{d_1} is a permutation over $\mathbb{F}_{2^k}$, and $d_i = d_1 + v_i(2^k - 1)$ for $i \geq 2$.

Let $n = 2k$, and denote by L the field $\mathbb{F}_{2^n}$ and its subfield $\mathbb{F}_{2^k}$ by K. In [39], binomial trace bent functions with "linear" Niho exponents d_1 and d_2 were considered. The term "linear" refers to the multiplicative group of K, that is, $d_i \equiv 2^{r_i} \pmod{2^k - 1}$, for $i = 1, 2$, and $r_i < n$ so that $d_i = 2^{r_i} + s_i(2^k - 1)$, with $2 \leq s_i \leq 2^k$. Moreover, a normalized form is obtained for $r_1 = r_2 = 0$, and it was shown that certain choices of s_i give bent exponents d_1 and d_2. The "linearity" of these coefficients was used to demonstrate that the bentness of $f(x) = Tr_1^n(\sum_{i=1}^{t} \lambda_i x^{d_i})$, for suitably chosen d_i and λ_i, is preserved when the function $F : L \to K$ defined as $F(x) = Tr_k^n\big(\sum_{i=1}^{n} \lambda_i x^{d_i}\big)$ is considered. It can be shown (cf. [39]) that $Tr_1^k(\lambda F(x)) = f(\lambda x)$, for $\lambda \in K$, and therefore if $f(x)$ is bent then $f_\lambda(x) = f(\lambda x)$ is bent as well. For completeness, we recall this simple but important observation from [39]. We have,

$$\begin{aligned} Tr_1^k(\lambda F(x)) &= Tr_1^k\big(\lambda Tr_k^n(\sum_{i=1}^{n} \lambda_i x^{d_i})\big) \\ &= Tr_1^k\big(Tr_k^n\big(\lambda \sum_{i=1}^{n} \lambda_i x^{d_i}\big)\big) = Tr_1^n\big(\lambda \sum_{i=1}^{n} \lambda_i x^{d_i})\big) \\ &= Tr_1^n\big(\sum_{i=1}^{n} \lambda_i (\lambda x)^{d_i}\big) = f(\lambda x). \end{aligned}$$

Then, if $f(x)$ is bent then $f_\lambda(x) = f(\lambda x)$ is bent. This nice property is due to the fact that for $\lambda \in K$, we have $\lambda^{d_i} = \lambda$ for $d_i = 1 + s_i(2^k - 1)$.

Assume now that $f(x) = Tr_1^n(\sum_{i=1}^{r} \lambda_i x^{d_i})$ is a bent function, where $d_i = d_1 + v_i(2^m - 1)$ for $v_i \geq 0$, $m \mid n$, and $i = 2, \ldots, r$. For an arbitrary $\beta \in \mathbb{F}_{2^m} \subseteq K \subset L$, we note that $\beta^{2^m - 1} = 1$ implies $\beta^{d_i} = \beta^{d_1}$, for any $i = 1, \ldots, r$. Then, the extended

Walsh transform of $F(x) = Tr_m^n(\sum_{i=1}^r \lambda_i x^{d_i})$ at β^{d_1} is computed as,

$$\begin{aligned} W_F(\sigma, \beta^{d_1}) &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr_1^m(\beta^{d_1} F(x)) + Tr_1^n(\sigma x)} \\ &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr_1^m(Tr_m^n(\sum_{i=1}^r \beta^{d_1} \lambda_i x^{d_i})) + Tr_1^n(\sigma x)} \\ &= \sum_{y \in \mathbb{F}_{2^n}} (-1)^{Tr_1^n(\sum_{i=1}^r \lambda_i y^{d_i}) + Tr_1^n(\sigma \beta^{-1} y)} \\ &= W_F(\sigma\beta^{-1}, 1) \\ &= W_f(\sigma\beta^{-1}) = \pm 2^{n/2} \end{aligned}$$

This calculation shows that if x^{d_1} is a permutation on $\mathbb{F}_{2^m}$ then $Tr_1^m(\gamma F(x))$ is bent for any $\gamma \in \mathbb{F}_{2^m}^*$. We have just proved the following result.

Theorem 3.2.1 *Let $n \geq 4$ be an even positive integer and let $m \mid n$, $m \leq n/2$. Let x^{d_1} be a permutation of $\mathbb{F}_{2^m}$, and let $f(x) = Tr_1^n(\sum_{i=1}^r \lambda_i x^{d_i})$ be a Boolean bent function, where $d_i = d_1 + v_i(2^m - 1)$ for $i = 2, \ldots, r$ and some integers $v_i \geq 0$, and $m|k$. Then, the function $F(x) = Tr_m^n(\sum_{i=1}^r \lambda_i x^{d_i})$ is a vectorial bent function. In particular, this is also true for $m = k = n/2$ so that the dimension of the output vector space is maximal.*

Remark 3.2.2 *The class of binomial bent functions with $d_i = 1 + v_i(2^k - 1)$, considered by Dobbertin et al. in [39], appears to be a special case of this approach. Indeed, we can rewrite $d_1 = 2^k + (v_1 - 1)(2^k - 1)$ and $d_2 = d_1 + (v_2 - v_1)(2^k - 1)$. In this case, x^{d_1} is a (linear) permutation over K and the bentness of the associated mapping $F(x) = Tr_k^n(\lambda_1 x^{d_1} + \lambda_2 x^{d_2})$ for $\lambda_1, \lambda_2, d_1$ and d_2 specified in [39] follows from Theorem 3.2.1.*

Open Problem 3.2.1 *It is of interest to prove a similar result to the above for the functions of the form $f(x) = Tr_1^n(\lambda_1 x^{d_1} + \sum_{i=2}^r \lambda_i x^{d_1 + v_i(2^k - 1)})$, if x^{d_1} is not a permutation polynomial.*

The case when x^{d_1} is a constant mapping on K, given by x^{2^k-1}, is of particular importance due to the existence of binomial bent functions for some particular choices of the coefficient v_2. Such a nonpermuting exponent d_1 has been considered in [25] for $f = Tr_1^n\big(\lambda(x^{2^k-1} + x^{3(2^k-1)})\big)$, and $\lambda \in K^*$. It was shown that f is not (hyper)bent if $Tr_1^k(\lambda) = 1$, for $k \geq 5$, but on the other hand several examples of (hyper)bent functions (thus $Tr_1^k(\lambda) = 0$ is necessary but not sufficient) were also exhibited.

3.3 Necessary and sufficient bent conditions - three equivalent statements

In this section we analyze the conditions imposed on some special kind of polynomials $P(x) \in L[x]$ that might give rise to trace (vectorial) bent functions. More precisely,

for even $n = 2k$, we consider multiple trace functions of the form $F(x) = Tr_k^n(P(x))$, where $P(x) = \sum_{i=1}^{t} a_i x^i$, $a_i \in L$, and each exponent i is of the form $i = r_i(2^k - 1)$ for some suitable $r_i < 2^k + 1$. Then, a set of necessary and sufficient conditions for F to be vectorial bent function on K is summarized in Theorem 3.3.1. Due to somewhat lengthy proofs of these assertions, these conditions are proved separately in the subsequent sections.

Let $\mathcal{U} = \{u \in L : u^{2^k+1} = 1\}$ be the cyclic subgroup of L of order $2^k + 1$, which is essentially the group of $(2^k + 1)$th primitive roots of unity. Then, $\alpha^{2^k-1} = \omega$ is a generator of $\mathcal{U}$, and $\mathcal{U} = \{\alpha^{s(2^k-1)}, s = 0, \ldots, 2^k\}$, where $\alpha \in L$ is a primitive element. Now, any element $x \in L^*$ can be uniquely represented as $x = \gamma u$, where $\gamma \in K^*$ and $u \in \mathcal{U}$, and furthermore $\cup_{u\in\mathcal{U}} uK^* = L^*$.

Theorem 3.3.1 *Let $n = 2k$, and define $F(x) = Tr_k^n(P(x))$, where $P(x) = \sum_{i=1}^{t} a_i x^{r_i(2^k-1)}$. Then the following conditions are equivalent:*

1. *F is a vectorial bent function of dimension k.*
2. *$\sum_{u\in\mathcal{U}} (-1)^{Tr_1^k(\lambda F(u))} = 1$ for all $\lambda \in K^*$.*
3. *There are two values $u \in \mathcal{U}$ such that $F(u) = 0$, and furthermore if $F(u_0) = 0$, then F is one-to-one and onto from $\mathcal{U}_0 = \mathcal{U} \setminus u_0$ to K.*
4. *The elementary symmetric polynomials σ_e, used as coefficients in the expansion of $\prod_{u\in\mathcal{U}}(x - F(u))$, satisfy the following: for any odd e, $1 \le e \le 2^k + 1$, we must have $\sigma_{2^k-1} = 1$, and $\sigma_e = 0$ otherwise.*

3.3.1 The first equivalence: equivalence via character sums over $\mathcal{U}$

We prove that the vectorial bent property is equivalent to the second condition in Theorem 3.3.1, claiming that $\sum_{u\in\mathcal{U}} (-1)^{Tr_1^k(\lambda Tr_k^n(P(u)))} = 1$, for all $\lambda \in K^*$.

Theorem 3.3.2 *Let F be defined as in Theorem 3.3.1. Then, F is a vectorial bent function if and only if*

$$\sum_{u\in\mathcal{U}} (-1)^{Tr_1^k(\lambda Tr_k^n(P(u)))} = 1, \tag{3.1}$$

for all $\lambda \in K^*$.

Proof. Assume that F is a vectorial bent function, and let $\lambda \in K^*$ and $\sigma \in L$. The extended Walsh transform of F at σ is given by,

$$\begin{aligned} W_F(\lambda, \sigma) &= \sum_{x\in L} (-1)^{Tr_1^k(\lambda Tr_k^n(\sum_{i=1}^{t} a_i x^{r_i(2^k-1)})) + Tr_1^n(\sigma x)} \\ &= 1 + \sum_{u\in\mathcal{U}} \sum_{z\in K^*} (-1)^{Tr_1^k(\lambda F(u)) + Tr_1^n(\sigma u z)} \\ &= 1 + \sum_{u\in\mathcal{U}} (-1)^{Tr_1^k(\lambda F(u))} \sum_{z\in K^*} (-1)^{Tr_1^n(\sigma u z)} \end{aligned} \tag{3.2}$$

Especially,

$$W_F(\lambda,0) = 1 + (2^k-1)\sum_{u\in\mathcal{U}}(-1)^{Tr_1^k(\lambda F(u))}.$$

If $W_F(\lambda,0) = -2^k$ we would have a contradiction that $2^k - 1 \mid 2^k + 1$, and thus $W_F(\lambda,0) = 2^k$. Thus, the necessary condition that F is a vectorial bent function is as follows,

$$\sum_{u\in\mathcal{U}}(-1)^{Tr_1^k(\lambda F(u))} = 1, \quad \text{for all } \lambda \in K^*.$$

To show that the above condition is also sufficient we note that

$$Tr_1^n(\sigma u z) = Tr_1^k(Tr_k^n(\sigma u z)) = Tr_1^k(z Tr_k^n(\sigma u)),$$

and for $Tr_k^n(\sigma u) = 0$ we have $\sum_{z\in K}(-1)^{Tr_1^n(\sigma u z)} = 2^k$, and zero otherwise. Thus, (3.2) can be rewritten as,

$$\begin{aligned} W_F(\lambda,\sigma) &= 1 - \sum_{u\in\mathcal{U}, Tr_k^n(\sigma u)\neq 0}(-1)^{Tr_1^k(\lambda F(u))} + (2^k-1)\sum_{u\in\mathcal{U}, Tr_k^n(\sigma u)=0}(-1)^{Tr_1^k(\lambda F(u))} \\ &= 1 - \sum_{u\in\mathcal{U}}(-1)^{Tr_1^k(\lambda F(u))} + 2^k \sum_{u\in\mathcal{U}, Tr_k^n(\sigma u)=0}(-1)^{Tr_1^k(\lambda F(u))}. \end{aligned}$$

Note that the kernel of the function Tr_k^n is the subfield K, and due to the unique decomposition of $x \in L^*$ as $x = u\sigma$ (where $\sigma \in K^*$) there is a unique $u_{(\sigma)}$ such that $\sigma u_{(\sigma)} \in K$, so we can write the last equation as,

$$\begin{aligned} W_F(\lambda,\sigma) &= 1 - \sum_{u\in\mathcal{U}}(-1)^{Tr_1^k(\lambda F(u))} + 2^k(-1)^{Tr_1^k(\lambda F(u_{(\sigma)}))} \\ &= 2^k(-1)^{Tr_1^k(\lambda F(u_{(\sigma)}))} = \pm 2^k, \end{aligned}$$

where we have used the necessary condition that $\sum_{u\in\mathcal{U}}(-1)^{Tr_1^k(\lambda F(u))} = 1$. Therefore, the condition given by (3.1) is also sufficient. ∎

3.3.2 The second equivalence: bentness via image of $F : \mathcal{U} \to K$

Now we show that $F(u)$ takes all possible values of K^* just once and the zero value is taken twice when u ranges over $\mathcal{U}$. Let us first prove that Condition 2 of Theorem 3.3.1 implies the existence of $u_0 \in \mathcal{U}$ such that $F(u_0) = 0$.

Proposition 3.3.1 *Let $F(u) = Tr_k^n(\sum_{i=1}^t a_i u^{r_i})$, $F : \mathcal{U} \to K$. The condition*

$$\sum_{u\in\mathcal{U}}(-1)^{Tr_1^k(\lambda F(u))} = 1, \qquad \textit{for all} \qquad \lambda \in K^*,$$

implies that there is at least one $u_0 \in \mathcal{U}$ such that $F(u_0) = 0$.

PROOF. Assume on contrary that $F(u) \neq 0$ for all $u \in \mathcal{U}$. Let $\beta = \alpha^{2^k+1}$ be a generator of K^* and $\mathcal{U} = \{u_0, u_1, \ldots, u_{2^k}\}$. Then we can write the values $\{Tr_1^k(\lambda F(u)) : \lambda \in K^*, u \in \mathcal{U}\}$ as the following $(2^k - 1) \times (2^k + 1)$ binary matrix,

$$\begin{pmatrix} Tr_1^k(F(u_0)) & Tr_1^k(F(u_1)) & \ldots & Tr_1^k(F(u_{2^k})) \\ Tr_1^k(\beta F(u_0)) & Tr_1^k(\beta F(u_1)) & \ldots & Tr_1^k(\beta F(u_{2^k})) \\ \vdots & \vdots & \ddots & \vdots \\ Tr_1^k(\beta^{2^k-2} F(u_0)) & Tr_1^k(\beta^{2^k-2} F(u_1)) & \ldots & Tr_1^k(\beta^{2^k-2} F(u_{2^k})) \end{pmatrix}.$$

Let us first consider the columns of this matrix. Since by assumption $F(u_i) \in K^*$, and $\beta^j F(u_i)$ permutes K^*, for $j = 0, 1, \ldots, 2^k - 2$, all values of the absolute trace function over K^* are taken. It follows that there are 2^{k-1} ones and $2^{k-1} - 1$ zeros in each column of this matrix. Thus, there are in total $2^{k-1}(2^k + 1)$ ones in the matrix.

Let us now consider the rows of the matrix. Since for each $\lambda \in K^*$ we have $\sum_{u \in \mathcal{U}} (-1)^{Tr(\lambda F(u))} = 1$, it follows that in each row $Tr_1^k(\lambda F(u))$ takes the value "one" 2^{k-1} times and the zero value exactly $2^{k-1} + 1$ times. Summing this up, there are in total $2^{k-1}(2^k - 1)$ ones in the matrix, differing from the result obtained above when we were summing over columns, a contradiction. Thus, there is at least one $u_0 \in \mathcal{U}$ such that $F(u_0) = 0$. ∎

Theorem 3.3.3 *The vectorial bent condition given by*

$$\sum_{u \in \mathcal{U}} (-1)^{Tr_1^k(\lambda F(u))} = 1,$$

holds for all $\lambda \in K^*$ if and only if $F(u)$ takes all the values in K^* exactly once, and the zero value is taken twice when $u \in \mathcal{U}$.

PROOF. By Proposition 3.3.1, there exists $u_0 \in \mathcal{U}$ so that $F(u_0) = 0$. Then, we can consider the set $\mathcal{U}_0 = \mathcal{U} \setminus \{u_0\}$ and we have,

$$\sum_{u \in \mathcal{U}} (-1)^{Tr_1^k(\lambda F(u))} = 1 + \sum_{u \in \mathcal{U}_0} (-1)^{Tr_1^k(\lambda F(u))},$$

which, due to the condition $\sum_{u \in \mathcal{U}} (-1)^{Tr_1^k(\lambda F(u))} = 1$, is then equivalent to

$$\sum_{u \in \mathcal{U}_0} (-1)^{Tr_1^k(\lambda F(u))} = 0.$$

Hence, it is of interest to consider $F : \mathcal{U}_0 \to K$. Since $\#K = \#\mathcal{U}_0$, there is a bijection $\Psi : K \to \mathcal{U}_0$. Recall that $G(x) \in K[x]$ is a permutation if and only if,

$$\sum_{x \in K} (-1)^{Tr_1^k(\lambda G(x))} = 0, \quad \text{for all } \lambda \in K^*.$$

Thus, by setting $u = \Psi(x)$ for $u \in \mathcal{U}_0$, $x \in K$, and letting $G : K \to K$, where $G = F \circ \Psi$, we have the condition

$$\sum_{u \in \mathcal{U}_0} (-1)^{Tr_1^k(\lambda F(u))} = \sum_{\Psi(x), x \in K} (-1)^{Tr_1^k(\lambda F(\Psi(x)))} = \sum_{x \in K} (-1)^{Tr_1^k(\lambda G(x))} = 0,$$

where $F(\Psi(x)) : K \to K$. This is satisfied if and only if $F(\Psi(x))$ is a permutation polynomial over K. Since Ψ is a bijection and $F(\Psi(x))$ is a permutation, then $F : \mathcal{U}_0 \to K$ is also a bijection, i.e., it has a full range. Thus, $F : \mathcal{U}_0 \to K$ is a bijection, and furthermore for $F : \mathcal{U} \to K$ we have shown that $F(u)$ takes all the values in K^* exactly once, and the zero value is taken twice when u ranges over $\mathcal{U}$. ■

3.3.3 The third equivalence: bentness through symmetric polynomials

Now we prove the last equivalence stated in Theorem 3.3.1. This assertion, relating the necessary and sufficient bent conditions to the evaluation of elementary symmetric polynomials, is established using a few preparatory results derived from the fact that $F(u)$ takes all possible values of K^* just once and the zero value is taken twice when u ranges over $\mathcal{U}$.

Theorem 3.3.4 *A necessary and sufficient condition for* $F(x) = Tr_k^n(\sum_{i=1}^t a_i x^{r_i(2^k-1)})$ *to be vectorial bent is that*

$$\prod_{u \in \mathcal{U}} (x - F(u)) = x^{2^k+1} + x^2. \tag{3.3}$$

Proof. The proof follows directly from Theorem 3.3.3, and the fact that 0 is the only multiple root of order two. ■

On the other hand, using symmetric sums (elementary symmetric polynomials, see [59][Chapter 1]) we can write (3.3) as,

$$\begin{aligned} \prod_{u \in \mathcal{U}} (x - F(u)) &= x^{2^k+1} + \sigma_1 x^{2^k} + \sigma_2 x^{2^k-1} + \ldots + \sigma_e x^{2^k+1-e} + \ldots \\ &\quad + \sigma_{2^k-1} x^2 + \sigma_{2^k} x + \sigma_{2^k+1} = x^{2^k+1} + x^2, \end{aligned} \tag{3.4}$$

where

$$\sigma_e = \sum_{0 \le i_1 < i_2 < \ldots < i_e \le 2^k} F(\omega^{i_1}) F(\omega^{i_2}) \cdots F(\omega^{i_e}), \quad e = 1, \ldots, 2^k + 1, \tag{3.5}$$

are elementary symmetric polynomials. Therefore, by Theorem 3.3.4, an alternative statement to the above is as follows.

Theorem 3.3.5 *The function* $F(x) = Tr_k^n(\sum_{i=1}^t a_i x^{r_i(2^k-1)})$ *is vectorial bent if and only if* $\sigma_{2^k-1} = 1$ *and* $\sigma_e = 0$ *for* $e \neq 2^k - 1$, $1 \leq e \leq 2^k + 1$, *where* σ_e *is defined by (3.5).*

The following lemma gives a useful insight at the structure of $\mathcal{U}$. It is used below in the estimation of σ_1 through Newton's formula.

Lemma 3.3.1 *Let* $\mathcal{U} = \{u \in L \mid u^{2^k+1} = 1\}$ *be the cyclic subgroup of* L *of order* $2^k + 1$. *Then,* $\sum_{u\in\mathcal{U}} u = 0$. *Furthermore,*

$$\sum_{u\in\mathcal{U}} u^t = \begin{cases} 1, & \text{if } t \equiv 0 \pmod{2^k+1} \\ 0, & \text{otherwise} \end{cases}.$$

Proof. Since $\prod_{u\in\mathcal{U}}(x-u) = x^{2^k+1} - 1$, considering the corresponding symmetric sums, we have $\sum_{u\in\mathcal{U}} u = 0$. If $\gcd(t, 2^k+1) = 1$ then x^t permutes the set $\mathcal{U}$ and so $\sum_{u\in\mathcal{U}} u^t = 0$. If t strictly divides 2^k+1 then the elements u^t are the roots of $x^{\frac{2^k+1}{t}} - 1$, and we again have that $\sum_{u\in\mathcal{U}} u^t = 0$. Now since $\mathcal{U} = \{\alpha^{s(2^k-1)}, s = 0, \ldots, 2^k\}$, for some primitive element $\alpha \in L$, if $t \equiv 0 \pmod{2^k+1}$ then $\sum_{u\in\mathcal{U}} u^t = 2^k + 1 \equiv 1 \pmod 2$. ∎

According to this result the choice of constants $a_i \in L$, and $r_i \in \mathbb{N}$ must ensure that $\sigma_e = 0$ for all $1 \leq e \leq 2^k+1$ apart from σ_{2^k-1}. The hardness of using these conditions lies in the fact that higher order symmetric polynomials are difficult to calculate, and therefore using this approach we can only derive a few necessary conditions (but not sufficient) that F must satisfy in order to be a vectorial bent function.

For instance, for a normalized binomial trace function $F(u) = Tr_k^n(u + z\gamma u^r)$, we clearly have $F(u) = u + u^{-1} + z\gamma u^r + z\gamma^{-1}u^{-r}$. Then, the first order elementary symmetric polynomial σ_1 is given as,

$$\sigma_1 = \sum_{u\in\mathcal{U}} F(u) = \sum_{u\in\mathcal{U}} u + \sum_{u\in\mathcal{U}} u^{-1} + z\gamma \sum_{u\in\mathcal{U}} u^r + z\gamma^{-1} \sum_{u\in\mathcal{U}} u^{-r},$$

and by Theorem 3.3.5, σ_1 must be zero if F is a vectorial bent function. Since these symmetric polynomials of higher order are hard to calculate we will use Newton's formula (cf. [59][Chapter 1]) to relate them to the sums of the form,

$$s_e = \sum_{u\in\mathcal{U}} F(u)^e, \qquad e = 1, 2, \ldots, 2^k+1, \qquad s_0 = 2^k + 1.$$

Then, for $1 \leq \ell \leq 2^k + 1$, Newton's formula states,

$$s_\ell + \sigma_1 s_{\ell-1} + \sigma_2 s_{\ell-2} + \ldots + \ell\sigma_\ell = 0,$$

where of course all the calculations are performed modulo two without mentioning it explicitly (e.g. in the above formula $-$ signs are turned into $+$ over $\mathbb{F}_2$). Note that

by Lemma 3.3.1, $s_1 = 0$ and thus $\sigma_1 = s_1 = 0$. If we assume that $\sigma_d = s_d = 0$ for all odd d, $d < \ell$, and if ℓ is odd, then Newton's formula implies that $\sigma_\ell = s_\ell$. Therefore, instead of calculating σ_ℓ we will calculate s_ℓ which is much easier.

Example 3.3.1 *Assume that $k = 3$, $F(u) = Tr_k^n(u + \gamma u^r)$, and we need to derive the conditions for γ and r from the requirement that $\sigma_e = 0$ for all $1 \leq e \leq 2^k + 1$ and $\sigma_{2^k-1} = 1$. Since $s_1 = 0$, then $\sigma_1 = 0$. Then, also $s_2 = \sigma_2$, whereas for $\ell = 3$ we have $s_3 + s_2\sigma_1 + s_1\sigma_2 + \sigma_3 = 0$, which then implies $\sigma_3 = s_3$. It is straightforward to derive the remaining equalities.*

Furthermore, the following result significantly reduces the computation of the s_ℓ, since only those s_ℓ for odd ℓ need to be computed. Assume that $\sigma_\ell = 0$, for odd ℓ, $\ell < 2^k + 1$, $\ell \neq 2^k - 1$ and $\sigma_{2^k-1} = 1$. Then the polynomial $\prod_{u \in \mathcal{U}}(x - F(u))$ can be written as

$$h(x) = \prod_{u \in \mathcal{U}}(x - F(u)) = x^{2^k+1} + h_{2^k-1}x^{2^k-1} + \ldots + h_3x^3 + x^2, \quad h_i \in L,$$

having multiple roots. But the following lemma shows that this is impossible.

Lemma 3.3.2 *A polynomial of the form*

$$h(x) = x^{2^k+1} + h_{2^k-1}x^{2^k-1} + \ldots + h_3x^3 + x^2, \;\; h_i \in L,$$

cannot have multiple roots in the field of characteristic 2, apart from zero.

Proof. Note that

$$h'(x) = x^{2^k} + h_{2^k-1}x^{2^k-2} + \ldots + h_3x^2 + 0,$$

and so $h(x) = xh'(x) + x^2$. If x_0 is a multiple root of $h(x)$, then it is also the root of $h'(x)$, and thus $x_0^2 = 0$ which implies $x_0 = 0$. ∎

Thus, based on the above Lemma 3.3.2 and Equation (3.4), assuming $\sigma_\ell = 0$, for odd ℓ (apart from $\sigma_{2^k-1} = 1$), will imply that $\sigma_\ell = 0$ for even ℓ and consequently Condition 4 of Theorem 3.3.1 is also proved. It reduces the amount of computation since only σ_d for d odd need to be calculated.

Theorem 3.3.6 *The function $F(x) = Tr_k^n(\sum_{i=1}^t a_i x^{r_i(2^k-1)})$ is vectorial bent if and only if $\sigma_e = 0$, for all odd $1 \leq e \leq 2^k + 1$, with the exception of $\sigma_{2^k-1} = 1$.*

3.4 Evaluating symmetric polynomials and induced necessary conditions

In the previous section we have shown that for a given $F(x) = Tr_k^n(\sum_{i=1}^t a_i x^{r_i(2^k-1)})$ ensuring σ_e is nonzero only for $e = 2^k - 1$ is equivalent to saying that F is vectorial

bent. In what follows, we focus on the bentness of binomial trace functions, though the whole approach can be easily generalized to trace functions containing more than two trace terms. On the other hand, the combinatorial aspects of the similar calculations, as given in this section, are much harder to handle.

Our goal now is to calculate s_ℓ for a binomial trace function $F(x) = Tr_k^n(x + \gamma z x^{r(2^k-1)})$ (where $\gamma \in \mathcal{U}$, $z \in K^*$), where ℓ is an odd positive integer. In general, for i_1, i_2, i_3, i_4 being nonnegative integers, using $s_l = \sigma_l$ and the multinomial theorem we have,

$$\begin{aligned} s_\ell &= \sum_{u\in\mathcal{U}} (F(u))^\ell = \sum_{u\in\mathcal{U}} (u + u^{-1} + z\gamma u^r + z\gamma^{-1}u^{-r})^\ell \\ &= \sum_{u\in\mathcal{U}} \sum_{i_1+i_2+i_3+i_4=\ell} \binom{\ell}{i_1, i_2, i_3, i_4} u^{i_1} u^{-i_2} u^{ri_3} u^{-ri_4} z^{i_3+i_4} \gamma^{i_3-i_4} \\ &= \sum_{i_1+i_2+i_3+i_4=\ell} \binom{\ell}{i_1, i_2, i_3, i_4} z^{i_3+i_4}\gamma^{i_3-i_4} \sum_{u\in\mathcal{U}} u^{i_1-i_2+r(i_3-i_4)} \\ &= \sum_{i_1+i_2+i_3+i_4=\ell, i_1-i_2+r(i_3-i_4)\equiv 0 \pmod{2^k+1}} \binom{\ell}{i_1, i_2, i_3, i_4} z^{i_3+i_4}\gamma^{i_3-i_4}, \end{aligned}$$

where $\binom{\ell}{i_1,i_2,i_3,i_4} = \frac{\ell!}{i_1!i_2!i_3!i_4!}$, and Lemma 3.3.1 was used in the last summation.

For those values of ℓ satisfying $\ell r < 2^k + 1$, we can only have the case $i_1 - i_2 + r(i_3 - i_4) = 0$. But then $i_1 - i_2 = rt$, $i_4 - i_3 = t$, i.e., $i_1 = i_2 + rt$ and $i_4 = i_3 + t$, where t is some integer. If t is zero then ℓ is even, which is a contradiction. Substituting i_1 and i_4 from above, we have

$$i_1 + i_2 + i_3 + i_4 = 2(i_2 + i_3) + rt + t = \ell.$$

However, this is only possible if t is odd and r is even. But for even r we can calculate σ_{r+1}. Indeed, in this case $\ell = r + 1$ and $t \neq 0$, implying $i_2 = i_3 = 0$, $i_1 = r$ and $i_4 = 1$ or $i_1 = i_4 = 0$ and $i_3 = 1$ and $i_2 = r$. Thus,

$$s_\ell = z(\gamma + \gamma^{-1}).$$

Since for odd ℓ we must have $s_\ell = \sigma_\ell$ and $\sigma_\ell = 0$, the condition $\gamma + \gamma^{-1} = 0$ then implies $\gamma = 1$. But then $F(u) = F(u^{-1})$ for any $u \in \mathcal{U}$, which contradicts the assumption that $F(\mathcal{U}_0) = K$. Thus, r is necessarily odd, $\gamma \neq 1$, and in this case $\sigma_\ell = s_\ell = 0$ for small values of ℓ, or more precisely for those values satisfying $\ell r < 2^k + 1$.

Theorem 3.4.1 *Let $F(x) = Tr_k^n(x+\gamma z x^{r(2^k-1)})$, where $\gamma \in \mathcal{U}$, $z \in K^*$, be a binomial trace function. Then, if F is a vectorial bent function, then r must be odd and $\gamma \neq 1$.*

In the following subsections we consider some special choices of r, namely we consider the case when $r \mid 2^k + 1$ and show that we necessarily have $r = 3$. In addition, the case when $r \nmid 2^k + 1$ is also analyzed, and a few necessary conditions for F to be a vectorial bent function are derived.

3.4.1 The case $2^k + 1 = rD$

We derive some necessary conditions for the coefficients $z \in K^*$ and $\gamma \in \mathcal{U}$ when $r \mid 2^k+1$. In particular, it is shown that $r = 3$, and some classes of binomial vectorial bent functions satisfying these conditions are also confirmed through simulations.

Theorem 3.4.2 *Let $2^k + 1 = rD$, where D is a positive integer. The necessary conditions for the function $F(x) = Tr_k^n(x^{2^k-1} + \gamma z x^{r(2^k-1)})$ to be a vectorial bent function are that $r = 3$ and*

$$\gamma^D = 1, \qquad \gamma \neq 1, \qquad z = Tr_k^n(\omega^D)(Tr_k^n(\gamma))^{-1}.$$

Proof. Note that since r is odd and $rD = 2^k + 1$ is also odd, then D is also odd. We have

$$s_D = \sum_{i_1+i_2+i_3+i_4=D, i_1-i_2+r(i_3-i_4)\equiv 0 \pmod{2^k+1}} \binom{D}{i_1, i_2, i_3, i_4} z^{i_3+i_4}\gamma^{i_3-i_4}.$$

We already showed that $i_1-i_2+r(i_3-i_4)$ cannot be zero but it can be $\pm(2^k+1)$ since $|i_1 - i_2 + r(i_3 - i_4)| \leq rD$. If $i_1 - i_2 + r(i_3 - i_4) = rD$, then $i_1 - i_2 = r(D - i_3 + i_4)$, and thus $i_1 = i_2 + rh$ and $i_3 = D + i_4 - h$, where $h \in \mathbb{Z}$. Substituting, we have $2(i_2+i_4)+h(r-1)+D = D$, and so $2(i_2+i_4) = -h(r-1)$. Since $0 \leq i_3 = D+i_4-h \leq D$ and $i_4 \geq 0$, we must have $h \geq 0$. But, $r - 1 > 0$ and $2(i_2 + i_4) = -h(r - 1)$ imply $h = 0$. Thus,$i_1 = i_2 = i_4 = 0$ and $i_3 = D$. Similarly, $i_1 - i_2 + r(i_3 - i_4) = -(2^k + 1)$ implies $i_1 = i_2 = i_3 = 0$ and $i_4 = D$. Consequently, in this case we have

$$s_D = z^D(\gamma^D + \gamma^{-D}) = 0,$$

which implies $\gamma^D = 1$, and furthermore it was already shown that $\gamma \neq 1$. Then, using $F(u) = Tr_k^n(u + \gamma z u^r) = u + u^{-1} + z\gamma u^r + z\gamma^{-1}u^{-r}$, we have

$$\begin{aligned} F(\omega^{iD}) &= \omega^{iD} + \omega^{-iD} + z\gamma\omega^{riD} + z\gamma^{-1}\omega^{-riD} \\ &= \omega^{iD} + \omega^{-iD} + z(\gamma + \gamma^{-1}), \end{aligned}$$

where due to $\gamma \neq 1$ we have $Tr_k^n(\gamma) \neq 0$, and $\omega^{rD} = 1$ was used in the last equality. Therefore, $F(\omega^{iD}) = F(\omega^{-iD})$, for all $i = 1, 2, \ldots, r - 1$. Since we have already shown that $F(u)$ takes all possible values of K^* exactly once and 0 is taken twice when u ranges over $\mathcal{U}$, it follows that $r = 3$ and also $\omega^{-D} = \omega^{2D}$. Apparently, $F(\omega^D) = F(\omega^{-D}) = 0$, therefore

$$\omega^D + \omega^{-D} + z(\gamma + \gamma^{-1}) = 0.$$

It follows that z can be calculated from $z = Tr_k^n(\omega^D)(Tr_k^n(\gamma))^{-1}$. Thus if r divides $2^k + 1$, the necessary conditions for the function $F(x)$ to be a vectorial bent function are $r = 3$, $\gamma^D = 1, \gamma \neq 1$, and $z = Tr_k^n(\omega^D)(Tr_k^n(\gamma))^{-1}$, as claimed. ∎

In the above proof, we have only calculated $s_D = 0$, for a fixed $D = (2^k + 1)/3$, and therefore the above conditions are not sufficient. Recall that we have already shown that $s_\ell = \sigma_\ell = 0$ for odd $1 \le \ell r < 2^k + 1$, which implies that $\sigma_\ell = 0$ for odd $\ell \le D$. To obtain further necessary conditions, we also calculate s_{D+2} using the assumption that $3(D + 2) < 6D$, that is, $D > 2$.

Lemma 3.4.1 *If the conditions of Theorem 3.4.2 are satisfied, then* $s_{D+2} = 0$.

Proof. We need to solve $i_1 + i_2 + i_3 + i_4 = D + 2$ and $(i_1 - i_2) + 3(i_3 - i_4) = 3D$ simultaneously, which implies $i_1 - i_2 = 3(D - i_3 + i_4)$. Now,

$$i_1 = i_2 + 3h \quad \text{and} \quad i_3 = D + i_4 - h \le D + 2,$$

imply $h \ge -2$. Again substituting, we get $2(i_2 + i_4) + D + 2h = D + 2$, so that

$$i_2 + i_4 + h = 1,$$

must be satisfied. We have the following cases:

1. $i_2 = 1$, $i_4 = 0$, $h = 0$, $i_1 = 1$, $i_3 = D$. The corresponding multinomial coefficient is of the form $\binom{D+2}{1,1,D,0} = (D + 2)(D + 1) \equiv 0 \pmod 2$, since $D + 1$ is even.

2. $i_2 = 0$, $i_4 = 1$, $h = 0$, $i_1 = 0$, $i_3 = D + 1$. The corresponding multinomial coefficient is of the form $\binom{D+2}{0,0,D+1,1} = D + 2 \equiv 1 \pmod 2$. Note that equaling the elements i_1 and i_2 with $-(2^k+1)$ (the same is true for i_3 and i_4), just change their roles. Thus, in the sum of s_{D+2} we get the term $z^{D+2}(\gamma^D + \gamma^{-D})$, which is 0 by Theorem 3.4.2.

3. $i_2 = 0$, $i_4 = 0$, $h = 1$, $i_1 = 3$, $i_3 = D - 1$. The corresponding multinomial coefficient is of the form $\binom{D+2}{3,0,D-1,0} = \frac{(D+2)(D+1)D}{2\cdot 3}$. Furthermore,

$$D + 1 = \frac{2^k + 1}{3} + 1 = \frac{2^k + 4}{3}.$$

   Thus, $D + 1$ is divisible by 4 (but not by 8), and this coefficient is also even, i.e., equal to zero modulo two.

4. If $h = -1$, i_4 can be either equal to 0 or to 1. If $i_4 = 0$ then $i_2 = 2$, but then $i_1 = 2 - 3 = -1$, a contradiction to $i_1 \ge 0$. If $i_4 = 1$ then $i_3 = D + 2$, $i_2 = 1$, $i_1 = 1 - 3 < 0$, a contradiction.

5. For $h = -2$, from $i_3 = D + i_4 - h$ and $i_3 \le D + 2$, we have $i_4 = 0$. Then, $i_2 = 3$ and $i_1 = 3 - 6 < 0$, a contradiction.

Thus, $s_{D+2} = 0$. ∎

Example 3.4.1 *Let $n = 6$ so that $k = 3$. Then, $3 \mid 2^k + 1$, and furthermore $D = 3$. Since $\mathcal{U} = \{u \in \mathbb{F}_{2^6} : u^9 = 1\}$ the generator of $\mathcal{U}$ is $\omega = \alpha^7$, where α is a primitive element of $\mathbb{F}_{2^6}$. Therefore, $\gamma = \alpha^{21}$, and $\gamma^D = \gamma^3 = 1$. Furthermore, using $\omega^D = \gamma$, we have $z = Tr_k^n(\omega^D)(Tr_k^n(\gamma))^{-1} = 1$. Notice also that, by Theorem 3.4.2, we necessarily have $r = 3$ and consequently $r(2^k - 1) = 21$. Then, indeed, the function $Tr_3^6(x^7 + \alpha^{21}x^{21})$ is a vectorial bent function, which was confirmed by computer simulations. In this case, the previous results imply that $\sigma_1 = \sigma_3 = \sigma_5 = 0$, hence it must be true that $\sigma_7 = 1$ and $\sigma_9 = 0$ for the function $Tr_3^6(x^7 + \alpha^{21}x^{21})$.*

Since the evaluation of σ_{D+2} (essentially s_{D+2}) in Lemma 3.4.1 does not induce further conditions, we consider s_{D+4} for $3(D + 4) < 6D$, that is, $D > 4$.

Lemma 3.4.2 *If the conditions of Theorem 3.4.2 are satisfied, then for $D > 4$ it holds $s_{D+4} = 0$ if and only if*

$$z^{D-2}(\gamma + \gamma^{-1})(\gamma + \gamma^{-1} + z(z^2 + 1)) = 0. \tag{3.6}$$

Proof. We look for the possible solutions of

$$i_1 + i_2 + i_3 + i_4 = D + 4, \qquad (i_1 - i_2) + 3(i_3 - i_4) = 3D.$$

Similarly as before,

$$i_1 = i_2 + 3h, \qquad i_3 = D + i_4 - h \leq D + 4 \quad \Rightarrow \quad h \geq -4,$$

and the substitution gives $2(i_2 + i_4) + D + 2h = D + 4$, i.e.,

$$(i_2 + i_4) + h = 2.$$

Considering all possible cases we have:

1. $i_2 = 0$, $i_4 = 0$, $h = 2$, $i_1 = 6$, $i_3 = D - 2$. The corresponding multinomial coefficient is of the form

$$\binom{D+4}{6, 0, D-2, 0} = \frac{(D+4)(D+3)(D+2)(D+1)D(D-1)}{2^3 \cdot 3 \cdot 5 \cdot 6}.$$

   Since $D + 1$ is divisible by 4 , $D - 1$ and $D + 3$ are divisible by 2, $\binom{D+4}{6,0,D-2,0} \equiv 1 \pmod 2$, and the corresponding term in the sum of s_{D+4} is $z^{D-2}(\gamma^{D-2} + \gamma^{-(D-2)})$.

2. $i_2 = 2$, $i_4 = 0$, $h = 0$, $i_3 = D$, $i_1 = 2$. Then,

$$\binom{D+4}{2, 2, D, 0} = \frac{(D+4)(D+3)(D+2)(D+1)}{4} \equiv 0 \pmod 2.$$

3. $i_2 = 0$, $i_4 = 2$, $h = 0$, $i_1 = 0$, $i_3 = D + 2$. In this case we have $\binom{D+4}{0,0,D+2,2} = \frac{(D+4)(D+3)}{2} \equiv 1 \pmod 2$, but the term in the sum of s_{D+4} is $z^{D+4}(\gamma^D+\gamma^{-D}) = 0$ by Theorem 3.4.2.

4. $i_2 = 1$, $i_4 = 0$, $h = 1$, $i_1 = 4$, $i_3 = D - 1$. Then,

$$\binom{D+4}{4,1,D-1,0} = \frac{(D+4)(D+3)(D+2)(D+1)D}{2 \cdot 3 \cdot 4} \equiv 1 \pmod 2,$$

   and the corresponding term is $z^{D-1}(\gamma^{D-1} + \gamma^{-(D-1)})$.

5. $i_2 = 0$, $i_4 = 1$, $h = 1$, $i_1 = 3$, $i_3 = D$. The corresponding multinomial coefficient is of the form $\binom{D+4}{3,0,D,1} = \frac{(D+4)(D+3)(D+2)(D+1)}{2 \cdot 3} \equiv 0 \pmod 2$.

6. $i_2 = 1$, $i_4 = 1$, $h = 0$, $i_1 = 1$, $i_3 = D + 1$. The multinomial coefficient is of the form $\binom{D+4}{1,1,D+1,1} = (D + 4)(D + 3)(D + 2) \equiv 0 \pmod 2$.

7. $h = -1$ and $i_1 = i_2 - 3 \geq 0$ imply $i_2 = 3$, and further $i_4 = 0$, $i_1 = 0$, $i_3 = D+1$. Then,

$$\binom{D+4}{0,3,D+1,0} = \frac{(D+4)(D+3)(D+2)}{2 \cdot 3} \equiv 1 \pmod 2,$$

   and the corresponding term in the sum is $z^{D+1}(\gamma^{D+1} + \gamma^{-(D+1)})$.

8. The case $h \leq -2$ leads to a contradiction, since $i_1 = i_2 - 6 \geq 0$ implies $i_2 \geq 6$, but then $i_2 + i_4 = 4$ gives $i_2 \leq 4$.

Summing up the above values, we have

$$s_{D+4} = z^{D+1}(\gamma^{D+1} + \gamma^{-(D+1)}) + z^{D-1}(\gamma^{D-1} + \gamma^{-(D-1)}) + z^{D-2}(\gamma^{D-2} + \gamma^{-(D-2)}).$$

Using $\gamma^D = 1$ from Theorem 3.4.2, we obtain,

$$s_{D+4} = z^{D-1}(\gamma + \gamma^{-1})(z^2 + 1) + z^{D-2}(\gamma^2 + \gamma^{-2}) = 0,$$

which can be rewritten as,

$$s_{D+4} = z^{D-2}(\gamma + \gamma^{-1})(z(z^2 + 1) + \gamma + \gamma^{-1}) = 0.$$

■

The necessary condition given by (3.6) excludes many possibilities for the choice of γ and z for $F(x) = Tr_k^n(x^{2^k-1} + z\gamma x^{3(2^k-1)})$. Indeed, if $n = 10$, then $2^k + 1 = 33$ so that $D = 11$. According to Lemma 3.4.2, the coefficient $s_{15} = 0$ if and only if γ and z are chosen so that (3.6) is satisfied. It is easily verified, by analysing (3.6), that selecting $z = 1$ in this case would imply that $\gamma = 1$, thus contradicting the condition that $\gamma \neq 1$ given by Theorem 3.4.2. Thus, when $n = 10$, the function $F(x) = Tr_5^{10}(x^{31}+\gamma x^{3\cdot 31})$ is never vectorial bent for any choice of $\gamma \in \mathcal{U}$, which was also confirmed by simulations.

3.4.2 The case when 3 does not divide $2^k + 1$

This case only applies when k is even or equivalently $n \equiv 0 \pmod 4$. For even k and $3 \nmid 2^k + 1$, the order of the cyclic group $\mathcal{U}$ can be written as $2^k + 1 = 3D + 2$ since $2^k + 1 = 3D + 1$ would imply $3 \mid 2^k$, a contradiction. Since $2^k = 3D + 1$, D is odd.

Lemma 3.4.3 *The coefficient $s_{D+2} = 0$ if and only if $z = Tr_k^n(\gamma^{D+1})$.*

PROOF. Let us consider s_{D+2}. Then we have two equations, $i_1 + i_2 + i_3 + i_4 = D + 2$ and $i_1 - i_2 + 3(i_3 - i_4) = 3D + 2$ that must be satisfied simultaneously. Multiplying the first equation by 3 and subtracting from the other, we obtain $2i_1 + 4i_2 + 6i_4 = 4$, i.e., $i_1 + 2i_2 + 3i_4 = 2$. We only have two cases:

1. $i_1 = 0$, $i_2 = 1$, $i_4 = 0$, $i_3 = D + 1$ with $\binom{D+2}{0,1,D+1,0} = (D + 2) \equiv 1 \pmod 2$, and the corresponding term is $z^{D+1}(\gamma^{D+1} + \gamma^{-(D+1)})$.

2. $i_1 = 2$, $i_2 = 0$, $i_3 = D$, $i_4 = 0$ with $\binom{D+2}{2,0,D,0} = \frac{(D+2)(D+1)}{2}$. Using $D = \frac{2^k-1}{3}$, $D + 1 = \frac{2^k-1+3}{3} = \frac{2^k+2}{3}$ is divisible by 2 but not by 4. Thus, $\binom{D+2}{2,0,D,0} = \frac{(D+2)(D+1)}{2} \equiv 1 \pmod 2$, and the corresponding term is $z^D(\gamma^D + \gamma^{-D})$.

Adding these two terms we get,

$$s_{D+2} = z^{D+1}(\gamma^{D+1} + \gamma^{-(D+1)}) + z^D(\gamma^D + \gamma^{-D}).$$

Noting that $\gamma^{2(D+1)}\gamma^D = \gamma^{2^k+1}$=1, one can easily verify that $Tr_k^n(\gamma^D)$=$(Tr_k^n(\gamma^{D+1}))^2$. Hence,

$$zTr_k^n(\gamma^{D+1}) + Tr_k^n(\gamma^D) = zTr_k^n(\gamma^{D+1}) + (Tr_k^n(\gamma^{D+1}))^2 = 0,$$

i.e., $z = Tr_k^n(\gamma^{D+1})$. Since $\gcd(D + 1, 3D + 2) = 1$, we have a nontrivial solution for all z or $\gamma \neq 1$. ∎

Lemma 3.4.4 *If the conditions of Lemma 3.4.3 hold, then $s_{D+4} = 0$ for $D > 3$.*

PROOF. To calculate s_{D+4}, we need to solve

$$i_1 - i_2 + 3(i_3 - i_4) = 3D + 2, \qquad i_1 + i_2 + i_3 + i_4 = D + 4.$$

Multiplying the second equation by 3 and subtracting from the first, we obtain $i_1 + 2i_2 + 3i_4 = 5$. The cases are:

1. $i_1 = 5$, $i_2 = 0$, $i_4 = 0$ and $i_3 = D - 1$ (using the second equation above). The corresponding multinomial coefficient is of the form,

$$\binom{D+4}{5,0,D-1,0} = \frac{(D+4)(D+3)(D+2)(D+1)D}{2 \cdot 3 \cdot 4 \cdot 5} \equiv 0 \pmod 2,$$

since $D + 3 = \frac{2^k-1}{3} + 3 = \frac{2^k+8}{3}$ is divisible by 8, and $D + 1$ is divisible by 2.

2. $i_1 = 4$ has no solution.

3. $i_1 = 3$, $i_2 = 1$, $i_4 = 0$, $i_3 = D$. We have,

$$\binom{D+4}{3,1,D,0} = \frac{(D+4)(D+3)(D+2)(D+1)}{2 \cdot 3} \equiv 0 \pmod 2.$$

4. $i_1 = 2$, $i_2 = 0$, $i_4 = 1$, $i_3 = D+1$. Then, $\binom{D+4}{2,0,D+1,1} \equiv 0 \pmod 2$.

5. $i_1 = 1$, $i_2 = 2$, $i_4 = 0$, $i_3 = D+1$. In this case, $\binom{D+4}{1,2,D+1,0} \equiv 0 \pmod 2$.

6. $i_1 = 0$, $i_2 = i_4 = 1$, $i_3 = D+2$, and similarly as before,

$$\binom{D+4}{0,1,D+2,1} = (D+4)(D+3) \equiv 0 \pmod 2.$$

Thus, summing up, $s_{D+4} = 0$ whenever $3(D+4) < 6D+4$, i.e., $D > 3$. ■

Lemma 3.4.5 *Let the conditions of Lemma 3.4.3 hold and $D \geq 5$. Then, $s_{D+6} = 0$ if and only if*

$$(Tr_k^n(\gamma^{D+1}))^{-8} = Tr_k^n(\gamma^{D-2}).$$

Proof. Similarly as above, to solve $i_1 - i_2 + 3(i_3 - i_4) = 3D+2$ and $i_1 + i_2 + i_3 + i_4 = D+6$, we end up with the equation $i_1 + 2i_2 + 3i_4 = 8$ and consider all possible cases:

1. $i_1 = 8$, $i_2 = 0$, $i_4 = 0$, $i_3 = D-2$. We have

$$\binom{D+6}{8,0,D-2,0} = \frac{(D+6)(D+5)\cdots(D+1)D(D-1)}{2 \cdot 3 \cdots 7 \cdot 8} \equiv 1 \pmod 2,$$

since $D+3$ is divisible by 8 but not by 16, $D+1$ and $D+5$ are divisible by 2 only, and $D-1$ is divisible by 4 only but not by 8. The corresponding term in the sum is $z^{D-2}(\gamma^{D-2} + \gamma^{-(D-2)})$.

2. $i_1 = 7$ has no solution.

3. $i_1 = 6$, $i_2 = 1$, $i_4 = 0$, $i_3 = D-1$. We have,

$$\binom{D+6}{6,1,D-1,0} = \frac{(D+6)(D+5)(D+4)(D+3)(D+2)(D+1)D}{2 \cdot 3 \cdot 4 \cdot 5 \cdot 6} \equiv 0 \pmod 2,$$

reasoning similarly as above.

4. $i_1 = 5$, $i_2 = 0$, $i_4 = 1$, $i_3 = D$. Then,

$$\binom{D+6}{5,0,D,1} = \frac{(D+6)(D+5)(D+4)(D+3)(D+2)(D+1)}{2 \cdot 3 \cdot 4 \cdot 5} \equiv 0 \pmod 2.$$

5. $i_1 = 4$, $i_2 = 2$, $i_4 = 0$, $i_3 = D$. In this case

$$\binom{D+6}{4,2,D,0} = \frac{(D+6)(D+5)(D+4)(D+3)(D+2)(D+1)}{2\cdot 3\cdot 4\cdot 2} \equiv 0 \pmod 2.$$

6. $i_1 = 3$, $i_2 = 1$, $i_4 = 1$, $i_3 = D+1$. We have,

$$\binom{D+6}{3,1,D+1,1} = \frac{(D+6)(D+5)(D+4)(D+3)(D+2)}{2\cdot 3} \equiv 0 \pmod 2.$$

7. $i_1 = 2$, $i_2 = 3$, $i_4 = 0$, $i_3 = D+1$. Then,

$$\binom{D+6}{2,3,D+1,0} = \frac{(D+6)(D+5)(D+4)(D+3)(D+2)}{2\cdot 3\cdot 2} \equiv 0 \pmod 2.$$

8. $i_1 = 2$, $i_2 = 0$, $i_4 = 2$, $i_3 = D+2$. In this case,

$$\binom{D+6}{2,0,D+2,2} = \frac{(D+6)(D+5)(D+4)(D+3)}{2\cdot 2} \equiv 0 \pmod 2.$$

9. $i_1 = 1$, $i_2 = 2$, $i_4 = 1$, $i_3 = D+2$. We have,

$$\binom{D+6}{1,2,D+2,1} = \frac{(D+6)(D+5)(D+4)(D+3)}{2} \equiv 0 \pmod 2.$$

10. $i_1 = 0$, $i_2 = 4$, $i_4 = 0$, $i_3 = D+2$. Then,

$$\binom{D+6}{0,4,D+2,0} = \frac{(D+6)(D+5)(D+4)(D+3)}{2\cdot 3\cdot 4} \equiv 0 \pmod 2.$$

11. $i_1 = 0$, $i_2 = 1$, $i_4 = 2$, $i_3 = D+3$. We have,

$$\binom{D+6}{0,1,D+3,2} = \frac{(D+6)(D+5)(D+4)}{2} \equiv 1 \pmod 2,$$

with its corresponding term $z^{D+5}(\gamma^{D+1} + \gamma^{-(D+1)})$.

Collecting together the above multinomial coefficients we get,

$$\begin{aligned} s_{D+6} &= z^{D+5}(\gamma^{D+1} + \gamma^{-(D+1)}) + z^{D-2}(\gamma^{D-2} + \gamma^{-(D-2)}) = \\ & z^{D-2}(z^7(\gamma^{D+1} + \gamma^{-(D+1)}) + (\gamma^{D-2} + \gamma^{-(D-2)})) = 0. \end{aligned}$$

Using Lemma 3.4.3, we end up with

$$s_{D+6} = z^{D-2}(z^8 + Tr_k^n(\gamma^{D-2})) = 0,$$

that is, $z^8 = Tr_k^n(\gamma^{D-2})$, which again using Lemma 3.4.3 gives

$$(Tr_k^n(\gamma^{D+1}))^{-8} = Tr_k^n(\gamma^{D-2}),$$

as claimed. ■

This lemma is a very useful tool for testing the functions which are not vectorial bent. Indeed, if we can show that this single condition cannot be satisfied for any $\gamma \in \mathcal{U}$, and for some fixed D such that $2^k+1 = 3D+2$ (where k is even), then $F(x) = Tr_k^n(x+\gamma z x^{r(2^k-1)})$ cannot be vectorial bent. Our computer simulations indicate that when $n = 8$, $k = 4$, there are no vectorial bent functions of the form $Tr_4^8(ax^{15}+bx^{3\cdot 15})$, which means that (setting $D = 5$ in this case) the equation $(Tr_4^8(\gamma^6))^{-8} = Tr_4^8(\gamma^3)$ might not have a solution, for any $\gamma \in \mathcal{U}$. Indeed, the performed simulations show that for $4 \leq n \leq 28$, $n = 2k \equiv 0 \pmod 4$, for a fixed D given by $2^k + 1 = 3D + 2$, the equation $(Tr_k^n(\gamma^{D+1}))^{-8} = Tr_k^n(\gamma^{D-2})$ has no solution for any $\gamma \in \mathcal{U}$. Based on this we propose the following conjecture.

Conjecture 1 *Let $k \geq 2$ be an even positive integer and $n = 2k$. Then, the functionF$(x) = Tr_k^n(x^{2^k-1} + \lambda x^{r(2^k-1)})$, $\lambda \in L^*$, is not a vectorial bent function, for any $\lambda \in L^*$.*

Open Problem 3.4.1 *Let $n = 2k \equiv 0 \pmod 4$, $n \geq 4$, and let D be given by $2^k + 1 = 3D + 2$. Show that the condition $(Tr_k^n(\gamma^{D+1}))^{-8} = Tr_k^n(\gamma^{D-2})$ is never satisfied for any n, and for any $\gamma \in \mathcal{U}$.*

3.5 Monomial bent functions and linearized polynomials

In the previous section we have seen that the derivation of the necessary conditions related to vectorial bent property is quite hard even for binomials. It turns out that monomial functions of the form $Tr_k^n(\lambda x^{r(2^k-1)})$ are easily treated without using symmetric polynomials. More precisely, we show that the function $Tr_k^n(\lambda x^{r(2^k-1)})$ is never a vectorial bent function on K. Also in this section, we relate certain monomial bent functions to vectorial bent binomials through the usage of linearized polynomials.

3.5.1 Monomial trace functions and induced necessary conditions

Boolean functions of the form $f(x) = Tr_1^n(\lambda x^{r(2^k-1)})$ have been extensively studied in [25] in terms of their bentness and hyperbentness. Since $x^{r(2^k-1)}$ is not a permutation on K, the vectorial bent property of the associated mapping $F(x) = Tr_k^n(\lambda x^{r(2^k-1)})$ cannot be established using Theorem 3.2.1. The main results related to $f_{\lambda,r}(x) = Tr_1^n(\lambda x^{r(2^k-1)})$ given in [25], where $\lambda \in K^*$, are summarized as follows. The function $f_{\lambda,r}$ is bent if and only if $\mathcal{K}_k(\lambda) = 0$, where $\mathcal{K}_k(\lambda) = \sum_{y\in K}(-1)^{Tr_1^k(y^{-1}+\lambda y)}$ denotes the Kloosterman sum at point λ. Furthermore, $f_{\lambda,r}$ is bent if and only if $f_{\lambda,1}$ is bent.

Then, for the function $f_\lambda(x) = Tr_1^n(\lambda x^{2^k-1})$ it was shown that f_λ is not bent when $\lambda \in K^*$ belongs to the set $\mathcal{T}_k$ given by,

$$\mathcal{T}_k = \begin{cases} \{1\}, & \text{if } k \text{ is odd} \\ \mathbb{F}_{2^s}^*, & \text{if } k = 2s \text{ and } s \text{ is even }, s > 2 \\ \mathbb{F}_4 \setminus \{0,1\}, & \text{if } k = 4 \\ (\mathbb{F}_{2^s} \cup \mathbb{F}_4)^*, & \text{if } k = 2s \text{ and } s \text{ is odd} \end{cases}.$$

Remark 3.5.1 *Without loss of generality we may consider $\lambda \in K^*$ since any $\lambda \in L^*$ can be written as $\lambda = \gamma u$, $\gamma \in K^*$, $u \in \mathcal{U}$, and f_λ and f_u have the same spectrum, cf. [25].*

Let now $F_a(x) = Tr_k^n(ax^{2^k-1})$. Then, by Theorem 3.3.2, F_a is a vectorial bent function if and only if

$$\sum_{u \in \mathcal{U}} (-1)^{Tr_1^k(\lambda Tr_k^n(au^{2^k-1}))} = 1,$$

for all $\lambda \in K^*$. Now, if $a \in K^*$, substituting λ' for $a\lambda$ we have

$$\sum_{u \in \mathcal{U}} (-1)^{Tr_1^k(\lambda' Tr_k^n(u^{2^k-1}))} = 1,$$

for all $\lambda' \in K^*$. Then, since x^{2^k-1} permutes the set $\mathcal{U}$ when $x \in \mathcal{U}$, the above condition becomes

$$\sum_{u \in \mathcal{U}} (-1)^{Tr_1^k(\lambda' Tr_k^n(u))} = 1,$$

for any $\lambda' \in K^*$. Considering $\mathcal{U}_0 = \mathcal{U} \setminus \{u_0\}$, where $Tr_k^n(u_0^{2^k-1}) = u_0^2 + u_0^{-2} = 0$, $u_0 \neq 1$, we get

$$\sum_{u \in \mathcal{U}_0} (-1)^{Tr_1^k(\lambda' Tr_k^n(u))} = 0.$$

Consequently, the mapping $F(u) = Tr_k^n(u^{2^k-1})$ must be a bijection from $\mathcal{U}_0$ to K if $F_a(x) = Tr_k^n(ax^{2^k-1})$ is a vectorial bent function. On the other hand, this condition implies that the Boolean function $f_{\lambda'} = Tr_1^n(\lambda' x^{2^k-1})$ must be bent for any choice of $\lambda' \in K^*$, which is certainly not true. Thus, we have the following result.

Theorem 3.5.2 *Let $f_\lambda(x) = Tr_1^n(\lambda x^{(2^k-1)})$ be a Boolean bent function for suitably chosen $\lambda \in K^*$. Then, its associated mapping $F_\lambda(x) = Tr_k^n(\lambda x^{(2^k-1)})$ cannot be a vectorial bent function on K.*

3.5.2 Binomial bent functions via linearized polynomials

Some interesting properties related to the preservation of the bent property under the addition of a linearized polynomial are presented bellow. Using the fact that

$$\begin{aligned} Tr(\lambda_j x^{2^j}) &= \sum_{i=0}^{n-1} (\lambda_j x^{2^j})^{2^i} \\ &= \lambda_j x^{2^j} + (\lambda_j x^{2^j})^2 + \ldots + \lambda_j^{2^k} x^{2^{j+k}} + \ldots + (\lambda_j x^{2^j})^{2^{n-1}} \\ &= \lambda_j x^{2^j} + \lambda_j^2 x^{2^{j+1}} + \ldots + \lambda_j^{2^k} x^{2^{j+k}} + \ldots + \lambda_j^{2^{n-1}} x^{2^{j+n-1}} \\ &= \beta_j^{x^{2^j}} x^{2^j} + \beta_j^{2^{j+1}} x^{2^{j+1}} + \ldots + \beta_j x + \ldots + \beta_j^{2^{j-1}} x^{2^{j-1}} \\ &= Tr(\beta_j x), \end{aligned}$$

where $\beta_j = \lambda_j^{2^{n-j}}$, one can easily establish the following well-known result.

Theorem 3.5.3 *Assume that $Tr_1^n(f(x))$ is a bent function, $f(x) \in \mathbb{F}_{2^n}[x]$. Then the function $F(x) = f(x) + \sum_{i=0}^{n-1} \lambda_i x^{2^i}$ is also a bent function.*

Proof. We compute the Walsh transform of F as,

$$\begin{aligned} W_F(\sigma) &= \sum_{x \in L} (-1)^{Tr(f(x) + \sum_{i=0}^{n-1} \lambda_i x^{2^i}) + Tr(\sigma x)} \\ &= \sum_{x \in L} (-1)^{Tr(f(x)) + Tr(\sum_{i=0}^{n-1} \beta_i x) + Tr(\sigma x)} \\ &= \sum_{x \in L} (-1)^{Tr(f(x)) + Tr((\sum_{i=0}^{n-1}) \beta_i x) x)} \\ &= \sum_{x \in L} (-1)^{Tr(f(x)) + Tr(\mu x)} = W_f(\mu), \end{aligned}$$

where $\mu = \sigma + \sum_{i=0}^{n-1} \beta_i$. It is obvious that $F(x)$ is a bent function. ∎

Corollary 3.5.1 *If $Tr_1^n(\lambda_1 x^{d_1})$ is a bent function, then $Tr_1^n(\lambda_1 x^{d_1} + \lambda_2 x^{2^j})$ is also a bent function, for any $\lambda_2 \in L$ and $j \in \mathbb{Z}$. Especially, if x^{d_1} is a permutation on K and there exist $j, v > 0$ such that $2^j = d_1 + v(2^{\frac{n}{2}} - 1)$, then by Theorem 3.2.1, $Tr_k^n(\lambda_1 x^{d_1} + \lambda_2 x^{2^j})$ is a vectorial bent function.*

For instance, assume $d_1 = 2^i + 1$, with $\gcd(i, n) > 1$, $\gcd(2^i + 1, 2^k - 1) = 1$, and furthermore let $\frac{n}{\gcd(i,n)}$ be even. Then we would have the relation $2^j = 2^i + 1 + v(2^{\frac{n}{2}} - 1)$. This gives, for $n = 6$ and taking $i = 3$, $v = 4$, so that $d_1 = 9$, that the previous equality is satisfied for $2^j = 16$. Therefore, if $Tr_1^6(\lambda_1 x^9)$ is a bent function

on $\mathbb{F}_{2^6}$ for some λ_1, then $Tr_3^6(\lambda_1 x^9 + \lambda_2 x^{16})$ is a vectorial bent function for any λ_2. This does not contradict Theorem 3.5.3 that only claims that the bent property of Boolean functions is invariant under the addition of a linearized polynomial, whereas the same addition may give rise to vectorial bent functions even though the monomial itself does not have the vectorial bent property.

The Dillon exponent of the form $d_1 = i(2^k - 1)$, where $\gcd(i, 2^k + 1) = 1$, is of particular interest since it is closely related to the results in the previous section. In this case we would have $2^j = (i + v)(2^k - 1)$, implying that $2^{\frac{n}{2}} - 1$ is divisible by 2^j, which is clearly impossible. Therefore, even though $Tr_1^n(\lambda_1 x^{d_1})$ is bent for a suitable λ_1 and the function $Tr_1^n(\lambda_1 x^{d_1} + \lambda_2 x^{2^j})$ is also bent for any $\lambda_2 \in L$ and $j \in \mathbb{Z}$, we cannot represent these binomials in the binomial form discussed in the previous section. Furthermore, since x^{d_1} is not a permutation we cannot apply Theorem 3.2.1.

Similar arguments apply to the Kasami exponent $d_1 = 2^{2i} - 2^i + 1$, where $\gcd(i, n) = 1$, and furthermore $\gcd(d_1, 2^k - 1) = 1$. However, it seems to be hard to find suitable λ_1 and d_1 so that $Tr_1^n(\lambda_1 x^{d_1})$ is bent, furthermore satisfying the relation $2^j = d_1 + v(2^{\frac{n}{2}} - 1)$.

Chapter 4

On Generalized Bent Functions With Dillon's Exponents

The art of doing mathematics consists in finding that special case which contains all the germs of generality.

– David Hilbert

THE POSSIBILITY of constructing bent functions over fields with odd characteristic has been considered in this chapter. The existence of both single output and vectorial p-ary bent functions represented as trace multinomials with Dillon's exponents has been established. Also, a secondary construction of vectorial bent functions of dimension $n/2$ is easily derived from the Maiorana-McFarland class of bent functions.

The main results are published in [2].

4.1 Introduction

While in the binary case and for $n = 2k$ the bent property of monomials of the form $Tr_1^n(ax^{r(2^k-1)})$ and binomials $Tr_1^n(x^{2^k-1}+ax^{r(2^k-1)})$ were investigated in several papers, generalized bent functions $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ of the form $Tr_1^n(\sum_{i=1}^t a_i x^{r_i(p^k-1)})$, p being an odd prime, were not analyzed previously. In particular, the construction of vectorial (generalized) bent functions has not been addressed. In this chapter we confirm that the conditions derived originally in [105] are valid for multinomial trace functions $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ with Dillon's exponents, i.e., $f(x) = Tr_1^n(\sum_{i=1}^t a_i x^{r_i(p^k-1)})$, where p is an odd prime, $n = 2k$. The coefficients $a_i \in \mathbb{F}_{p^n}$ and $r_i \in \mathbb{N}$ still need to be specified so that f is bent. It is shown that the choice of a_i and r_i, ensuring that f is bent, is directly related to the image of the subset V. More precisely, f is bent if and only if $f(V) = (\mathbb{F}_p)^{k-1} \cup \{0\}$, which then gives us a possibility of

specifying a_i and r_i. Here, $(\mathbb{F}_p)^{p^{k-1}}$ denotes a multiset containing p^{k-1} copies of $\mathbb{F}_p$, and $V = \{1, \alpha, \alpha^2, \ldots, \alpha^{p^k}\}$ where α is a primitive element of $\mathbb{F}_{p^n}$. The existence of bent coefficients a_i, r_i is confirmed by simulations using the above condition. It is well known that for a prime p, the multiplicative group $\mathbb{F}^*_{p^n}$ can be decomposed in the Cartesian product $\mathbb{F}^*_{p^n} = \mathbb{F}^*_{p^k} \times V$, where $V = \{1, \alpha, \alpha^2, \ldots, \alpha^{p^k}\}$ and α is a primitive element of $\mathbb{F}_{p^n}$.

The single output case of binomial trace functions with Dillon's exponents can be naturally extended to vectorial functions by considering the functions of the form $F_{a,r}(x) = Tr^n_k(\sum_{i=1}^t a_i x^{r_i(p^k-1)})$ instead. In this case, the condition that F is bent is again given in terms of the image set of V, that is, $F(V) = \mathbb{F}_{p^k} \cup \{0\}$. Again, a large number of vectorial bent functions could be found using the condition concerning the image of V. In other direction, some secondary constructions of vectorial bent functions of dimension k, derived from a famous Maiorana-McFarland class, is proposed. Nevertheless, we leave as an interesting open problem the construction of vectorial bent functions of dimension $> n/2$, since there is no evidence that such functions actually exist, apart from those that from planar mappings [34] and are of full dimension n.

4.2 Single output generalized bent functions

Let $f(x) = Tr^n_1(\sum_{i=1}^t a_i x^{r_i(p^k-1)})$, where $n = 2k, a_i \in \mathbb{F}^*_{p^n}, r_i < p^k + 1$. We show that the necessary and sufficient conditions for the multiple trace function $f(x)$ to be bent are the same as originally derived in [105]. To characterize the bentness of the function $f(x)$ we denote an exponential sum over the subset V as,

$$B := \sum_{v \in V} \omega^{f(v)} = \sum_{j=0}^{p^k} \omega^{Tr^n_1(\sum_{i=1}^t a_i \alpha^{r_i(p^k-1)j})}. \tag{4.1}$$

Before we prove the main theorem we need the following preparatory results. Since any $x \in \mathbb{F}^*_{p^n}$ can be uniquely expressed as yv for $y \in \mathbb{F}^*_{p^k}$ and $v \in V$, we have

$$f(x) = f(yv) = Tr^n_1(\sum_{i=1}^t a_i (yv)^{r_i(p^k-1)}) = Tr^n_1(\sum_{i=1}^t a_i v^{r_i(p^k-1)}) = f(v).$$

Then, the Fourier transform can be computed as,

$$\begin{aligned}\mathcal{F}(\lambda) &= \sum_{x\in\mathbb{F}_{p^n}} \omega^{f(x)-Tr_1^n(\lambda x)} = 1+\sum_{v\in V}\sum_{y\in\mathbb{F}^*_{p^k}} \omega^{f(yv)-Tr_1^n(\lambda yv)} \\ &= 1+\sum_{v\in V}\omega^{f(v)}\sum_{y\in\mathbb{F}^*_{p^k}} \omega^{Tr_1^k(-(\lambda v+(\lambda v)^{p^k})y)} \\ &= 1+\sum_{v\in V,\lambda v+(\lambda v)^{p^k}=0}(p^k-1)\omega^{f(v)} - \sum_{v\in V,\lambda v+(\lambda v)^{p^k}\neq 0}\omega^{f(v)} \\ &= 1+p^k\sum_{v\in V,\lambda v+(\lambda v)^{p^k}=0}\omega^{f(v)} - \sum_{v\in V}\omega^{f(v)}. \end{aligned} \tag{4.2}$$

If $\lambda = 0$ then

$$\mathcal{F}(0) = 1+(p^k-1)B. \tag{4.3}$$

If $\lambda \neq 0$ then we know the equation $\lambda x+\lambda^{p^k}x^{p^k}=0$ has a unique solution in V, given by $v_\lambda = \lambda^{-1}\alpha^{\frac{p^k+1}{2}}$. By (4.2) we have

$$\mathcal{F}(\lambda) = 1+p^k\omega^{f(v_\lambda)} - B. \tag{4.4}$$

Hence, the calculation of $\mathcal{F}(\lambda)$ is reduced to determining the exponential sum B.

The main result of this section is the following.

Proposition 4.2.1 *The multiple trace function $f(x)$ is bent if and only if $B=1$.*

Proof. Assume $B=1$. By equations (4.3) and (4.4) we have

$$\mathcal{F}(\lambda) = \begin{cases} p^k\omega^{f(v_\lambda)}, & \text{if } \lambda\neq 0 \\ p^k, & \text{if } \lambda = 0 \end{cases}. \tag{4.5}$$

Thus $f(x)$ is a regular bent function. The converse may be proved using exactly the same arguments as in [105]. For the reader convenience we repeat the proof. Assuming that $f(x)$ is a bent function, then $|\mathcal{F}(\lambda)| = p^k$ for any $\lambda\in\mathbb{F}_{p^n}$. Thus, if $\lambda\neq 0$, by eq. (2.19) we can suppose that $\mathcal{F}(\lambda) = \pm\omega^{k_1}p^k$ for some $0\leq k_1\leq p-1$. Then, let $B := \sum_{v\in V}\omega^{f(v)} = \sum_{i=0}^{p-1}N_i\omega^i$, where $N_i = \#\{v\in V | f(v)=i\}$ for $0\leq i\leq p-1$. Now, it is sufficient to prove

$$N_0-1 = N_1 = \ldots = N_{p-1} = p^{k-1}. \tag{4.6}$$

Note that $N_0+N_1+\ldots+N_{p-1} = p^k+1$. Let $k_2 = f(v_\lambda)$, then equation (4.4) can be written as

$$N_0-1+N_1\omega+\ldots+N_{p-1}\omega^{p-1}\pm p^k\omega^{k_1}-p^k\omega^{k_2}=0. \tag{4.7}$$

Merging together similar items on the left side of above equation gives

$$a_0+a_1\omega+\ldots+a_{p-1}\omega^{p-1}=0. \tag{4.8}$$

Comparing the sequence of nonnegative integers $\{N_0, N_1, \ldots, N_{p-1}\}$ and the sequence of integers $\{a_0, a_1, \ldots, a_{p-1}\}$, we know there are at least $p-3$ indices i such that $a_i = N_i$, for $1 \leq i \leq p-1$. Therefore, using (4.6)

$$a_0 + a_1 + \ldots + a_{p-1} = (N_0 - 1 + N_1 + \ldots + N_{p-1}) \pm p^k - p^k = \pm p^k.$$

Thus $a_0 = a_1 = \ldots = a_{p-1} = \pm p^{k-1}$ since by Eisenstein's criteria [31], $x^{p-1} + \ldots + x^2 + x + 1$ is irreducible over the rational numbers, and by (4.8) it is the unique minimal polynomial of ω over the field of rational numbers.

Assume that $\mathcal{F}(\lambda) = -\omega^{k_1} p^k$. Then $a_0 = a_1 = \ldots = a_{p-1} = -p^{k-1} < 0$, which happens only when $p = 3$, otherwise there will be a negative N_i and in this case we must have $N_0 = 1 - p^{k-1} \leq 0$ and $N_1 = N_2 = p^k - p^{k-1}$, this further happens only when $k = 1$.

Assume that $\mathcal{F}(\lambda) = \omega^{k_1} p^k$. Then $a_0 = a_1 = \ldots = a_{p-1} = p^{k-1}$. By relation of two sequences we have $k_1 = k_2$, otherwise there is some i and $a_i \geq N_i - 1 + p^k \geq p^k - 1 > p^{k-1}$, and $a_0 = N_0 - 1, a_i = N_i$ for $1 \leq i \leq p-1$. Thus $N_0 - 1 = N_1 = \ldots = N_{p-1} = p^{k-1}$. ∎

In order to find alternative characterization for $B = 1$ from the equation (4.1) we notice that (4.6) implies the following.

Theorem 4.2.1 *The function* $f(x) = Tr_1^n(\sum_{i=1}^t a_i x^{r_i(p^k-1)})$ *is bent if and only if* $f(V) = (\mathbb{F}_p)^{k-1} \cup \{0\}$.

Thus, the bent condition is equivalent to requiring that the sequence $\{q_j\}_{j=0}^{p^k}$ defined by $\{q_j\}_{j=0}^{p^k} = Tr_1^n(\sum_{i=1}^t a_i \alpha^{r_i(p^k-1)j})$ is balanced (outputting each of the p values equally) with a single zero value in excess.

Example 4.2.1 *For* $p = 3$ *and* $n = 4$ *there are a lot of pairs* (a, r) *such that* $f_{a,r}(x) = Tr_1^n(x^{p^k-1} + ax^{r(p^k-1)})$ *with Dillon's exponents is bent. For instance, the function* $f_{\alpha,2}(x) = Tr_1^4(x^8 + \alpha x^{16})$ *is a bent function and it holds* $N_0 = 4, N_1 = 3, N_2 = 3$. *The existence of bent functions of this form was also confirmed by computer simulations (not only for binomials) for all prime* $p \leq 10$ *and even* $n \leq 12$.

4.3 Vectorial (generalized) bent functions

We now consider multiple trace functions of the form $F(x) = Tr_k^n(\sum_{i=1}^t a_i x^{r_i(p^k-1)})$ where $n = 2k$ and find the necessary and sufficient conditions for F to be vectorial (generalized) bent function on $\mathbb{F}_{p^k}$.

Theorem 4.3.1 *Let* $F(x) = Tr_k^n(\sum_{i=1}^t a_i x^{r_i(p^k-1)})$, *where* $a_i \in \mathbb{F}_{p^n}, n = 2k \in \mathcal{N}, r_i < p^k + 1$. *Then,* F *is a vectorial bent function if and only if*

$$\sum_{v \in V} \omega^{Tr_1^k(\lambda F(v))} = 1, \quad \textit{for all } \lambda \in \mathbb{F}_{p^k}^*. \tag{4.9}$$

PROOF. Assume that F is bent, and let $\lambda \in \mathbb{F}_{p^k}^*$ and $\mu \in \mathbb{F}_{p^n}$. The extended Fourier transform of F is given by,

$$\begin{aligned}\mathcal{F}(\lambda,\mu) &= \sum_{x\in\mathbb{F}_{p^n}} \omega^{Tr_1^k(\lambda F(x))-Tr_1^n(\mu x)} \\ &= 1+\sum_{v\in V}\sum_{u\in\mathbb{F}_{p^k}^*} \omega^{Tr_1^k(\lambda F(v))-Tr_1^n(\mu vu)} \\ &= 1+\sum_{v\in V}\omega^{Tr_1^k(\lambda F(v))}\sum_{u\in\mathbb{F}_{p^k}^*}\omega^{-Tr_1^n(\mu vu)}. \end{aligned} \tag{4.10}$$

Especially,

$$\mathcal{F}(\lambda,0) = 1+(p^k-1)\sum_{v\in V}\omega^{Tr_1^k(\lambda F(v))}.$$

Thus, the necessary condition that F is bent is as follows,

$$\sum_{v\in V}\omega^{Tr_1^k(\lambda F(v))} = 1, \quad \text{for all } \lambda \in \mathbb{F}_{p^k}^*.$$

To show that the above condition is also sufficient we note that

$$Tr_1^n(\mu vu) = Tr_1^k(Tr_k^n(\mu vu)) = Tr_1^k(uTr_k^n(\mu v)).$$

Then for $Tr_k^n(\mu v) = 0$ we have $\sum_{u\in\mathbb{F}_{p^k}^*}\omega^{-Tr_1^n(\mu vu)} = p^k-1$, and -1 otherwise. Thus, (4.10) can be rewritten as,

$$\begin{aligned}\mathcal{F}(\lambda,\mu) &= 1-\sum_{v\in V, Tr_k^n(\mu v)\neq 0}\omega^{Tr_1^k(\lambda F(v))}+(p^k-1)\sum_{v\in V, Tr_k^n(\mu v)=0}\omega^{Tr_1^k(\lambda F(v))} \\ &= 1-\sum_{v\in V}\omega^{Tr_1^k(\lambda F(v))}+p^k\sum_{v\in V, Tr_k^n(\mu v)=0}\omega^{Tr_1^k(\lambda F(v))}.\end{aligned}$$

But the kernel of the function Tr_k^n is the subfield $\mathbb{F}_{p^k}$ and thus there is a unique v_μ such that $\mu v_\mu \in \mathbb{F}_{p^k}$ so we can write the last equation as,

$$\begin{aligned}\mathcal{F}(\lambda,\mu) &= 1-\sum_{v\in V}\omega^{Tr_1^k(\lambda F(v))}+p^k\omega^{Tr_1^k(\lambda F(v_\mu))} \\ &= p^k\omega^{Tr_1^k(\lambda F(v_\mu))},\end{aligned}$$

where we used (4.9). Thus, the condition given by (4.9) is also sufficient. ■

The result of Theorem 4.3.1 however does not specify the image set of F restricted on V. The following result gives the exact condition for F to be vectorial bent function.

Theorem 4.3.2 *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^k}$ such that*

$$\sum_{v \in V} \omega^{Tr_1^k(\lambda F(v))} = 1, \quad for\ all\ \lambda \in \mathbb{F}_{p^k}^*.$$

Then there are exactly two values $v_0 \in V$ such that $F(v_0) = 0$, and furthermore $F(V) = \mathbb{F}_{p^k} \cup \{0\}$.

Proof. Let $\mathbb{F}_{p^k}^* = K^* = \{\alpha^{(p^k+1)i} : i = 1, \ldots, p^k - 1\}$. For simplicity denote $V = \{v_1, v_2, \ldots, v_{p^k+1}\}$, $K^* = \{\lambda_1, \lambda_2, \ldots, \lambda_{p^k-1}\}$ and $Tr_1^k(\lambda F(v)) = Tr(\lambda F(v))$. Now form a matrix

$$\begin{pmatrix} Tr(\lambda_1 F(v_1)) & Tr(\lambda_1 F(v_2)) & \ldots & Tr(\lambda_1 F(v_{p^k+1})) \\ Tr(\lambda_2 F(v_1)) & Tr(\lambda_2 F(v_2)) & \ldots & Tr(\lambda_2 F(v_{p^k+1})) \\ \vdots & \vdots & \ddots & \vdots \\ Tr(\lambda_{p^k-1} F(v_1)) & Tr(\lambda_{p^k-1} F(v_2)) & \ldots & Tr(\lambda_{p^k-1} F(v_{p^k+1})) \end{pmatrix}.$$

Let us count how many times the element $1 \in \mathbb{Z}_p$ occurs in the matrix. For a fixed λ_i consider the row in the matrix indicated by λ_i. In the sum

$$\sum_{v \in V} \omega^{Tr_1^k(\lambda F(v))} = 1,$$

assume that $Tr_1^k(\lambda F(v)) = i$ for N_i values $v \in V$, and for $i = 0, 1, \ldots, p-1$. Then $N_0 + N_1 + \ldots + N_{p-1} = p^k + 1$. But then $N_0 + N_1\omega + N_2\omega^2 + \ldots + N_{p-1}\omega^{p-1} = 1$ and irreducibility of $1 + x + \ldots + x^{p-1}$ together with sums of N_i implies that $N_0 - 1 = N_1 = \ldots = N_{p-1} = p^{k-1}$. Thus $N_1 = p^{k-1}$ and so value 1 occurs in each row p^{k-1} times and thus in the matrix exactly $p^{k-1}(p^k - 1)$ times.

Let us now consider the columns of this matrix. Assume that $F(v_j) \neq 0$ for fixed j and let λ passes through K^*. Then $\lambda F(v_j)$ permutes K^* and thus value 1 in the j-th column is taken p^{k-1} times. If $F(v_j) = 0$ then all values in the j-th column are equal to the zero. If h is a number of $j \in \{1, 2, \ldots, p^k + 1\}$ such that $F(v_j) \neq 0$ we have that 1 occurs in the matrix exactly hp^{k-1} times. Comparing this with result above when we counted this number using rows we have $hp^{k-1} = p^{k-1}(p^k - 1)$ and thus $h = p^k - 1$. Hence, there are exactly two values $v_i, v_j \in V$ such that $F(v_i) = F(v_j) = 0$.

Assume that $v_0 \in V$ such that $F(v_0) = 0$. Then the condition $\sum_{v \in V} \omega^{Tr_1^k(\lambda F(v))} = 1$, for all $\lambda \in K^*$ implies

$$\sum_{v \in V \setminus \{v_0\}} \omega^{Tr_1^k(\lambda F(v))} = 0,$$

which actually means that $F(V \setminus v_0)$ is a permutation of $\mathbb{F}_{p^k}$, and thus we have $F(V) = \mathbb{F}_{p^k} \cup \{0\}$. ∎

Example 4.3.1 *Let $p = 3$ and $n = 4$. There are a lot of pairs (a, r) such that, for instance, $F(x) = Tr_2^4(x^8 + ax^{r \cdot 8})$ is vectorial bent function. The function $F(x) =$*

$Tr_2^4(x^8 + \alpha^4 x^{32})$ is a vectorial bent function. The existence of bent functions of this form was also confirmed by computer simulations (not only for binomials) for all prime $p \leq 10$ and even $n \leq 12$.

4.4 Secondary constructions of vectorial (generalized) bent functions

We notice that for $p = 2$ and n even the maximal dimension of the bent linear subspace is $n/2$, see [77]. That is, linear combinations of weight at most $n/2$ can be built so that $s_1 f_{i_1} + \ldots + s_{n/2} f_{i_{n/2}}$ is again a bent function for any $(s_1, \ldots, s_{n/2}) \in \mathbb{F}_2^{n/2^*}$, where $\{f_{i_1}, \ldots, f_{i_{n/2}}\} \subset \{f_1, \ldots, f_n\}$. It is well-known that such a bent function is vectorial bent function. On the other hand, when $p \neq 2$ bent functions are closely related to the concept of planar mappings (perfect nonlinear functions) [34] characterized by the property that $F(x + a) - F(x)$ is a permutation for any nonzero $a \in \mathbb{F}_{p^n}$. Since F is planar if and only if all nonzero linear combinations of its coordinate functions $f_i : \mathbb{F}_{p^n} \to \mathbb{F}_p$, $i = 1, \ldots, n$, planar mappings naturally induce vectorial bent functions of maximum dimension n.

These mappings are very rare and therefore to construct vectorial bent functions of smaller dimension appears to be of interest as well. There are two well known construction methods of designing bent functions. The first one is a direct sum construction described as follows [54]. Let $\mathcal{B}_{n,p}$ denote the set of all p-valued bent functions in n variables, that is,

Theorem 4.4.1 *Let m, n be arbitrary positive integers and p be an odd prime. For arbitrary functions $g \in \mathcal{B}_{n,p}$ and $h \in \mathcal{B}_{m,p}$, the function $f(x, y) = g(x) + h(y)$ is a p-valued bent function.*

Furthermore, an analog of Maiorana-McFarland theorem [66] (related to Boolean bent functions when $p = 2$) is also valid:

Theorem 4.4.2 *Let n be even and p be an odd prime. Then,*

$$f(x, y) = x \cdot h(y) + g(y),$$

is a p-valued bent function, where g is an arbitrary p-valued function of $n/2$ variables, and h is an arbitrary permutation of the set $\mathbb{F}_p^{n/2}$.

Theorem 4.4.2 allows us immediately to construct p-valued vectorial bent functions $F : \mathbb{F}_p^n \to \mathbb{F}_p^{n/2}$ of dimension $n/2$ as follows.

Theorem 4.4.3 *Let n be even and p be an odd prime. Let g_i be an arbitrary p-valued function of $n/2$ variables, $g_i : \mathbb{F}_p^{n/2} \to \mathbb{F}_p$, $i = 1, \ldots, n/2$. If $\{\alpha_1, \ldots, \alpha_{n/2}\}$ is a fixed basis of $\mathbb{F}_{p^{n/2}}$ considered as a vector space over $\mathbb{F}_p$, define for $x, y \in \mathbb{F}_p^{n/2}$*

$$h_i(y) = \alpha_i h(y), \quad f_i(x, y) = x \cdot h_i(y) + g_i(y), \quad i = 1, \ldots, n/2,$$

where h is an arbitrary permutation of $\mathbb{F}_p^{n/2}$, and $f_i : \mathbb{F}_p^n \to \mathbb{F}_p$. Then, the function $F : \mathbb{F}_p^n \to \mathbb{F}_p^{n/2}$ defined by $F = (f_1, \ldots, f_{n/2})$, is a p-valued vectorial bent function.

PROOF. We have to show that $s_1 f_1 + \ldots + s_{n/2} f_{n/2}$ is again a bent function for any $(s_1, \ldots, s_{n/2}) \in \mathbb{F}_p^{n/2^*}$. Clearly, $h_i(y) = \alpha_i h(y)$ is a permutation so that $f_i(x, y)$ are p-valued bent functions for $i = 1, \ldots, n/2$. For any fixed $(s_1, \ldots, s_{n/2}) \in \mathbb{F}_p^{n/2^*}$ we have,

$$\begin{aligned} s_1 f_1 + \ldots + s_{n/2} f_{n/2} &= s_1(x \cdot \alpha_1 h(y)) + s_1 g_1(y) + \ldots + s_{n/2}(x \cdot \alpha_{n/2} h(y)) + s_{n/2} g_{n/2}(y) \\ &= s_1(x \cdot \alpha_1 h(y)) + \ldots + s_{n/2}(x \cdot \alpha_{n/2} h(y)) + \sum_{i=1}^{n/2} s_i g_i(y) \\ &= (s_1\alpha_1 + \ldots + s_{n/2}\alpha_{n/2}) x \cdot h(y) + \sum_{i=1}^{n/2} s_i g_i(y). \end{aligned}$$

Since $s = s_1\alpha_1 + \ldots + s_{n/2}\alpha_{n/2} \neq 0$ for any $(s_1, \ldots, s_{n/2}) \in \mathbb{F}_p^{n/2^*}$, then $s_1 f_1 + \ldots + s_{n/2} f_{n/2} = s(x \cdot h(y) + g'(y))$, where $g'(y) = s^{-1} \sum_{i=1}^{n/2} s_i g_i(y)$. Thus, $F = (f_1, \ldots, f_{n/2})$ is a vectorial bent function. ∎

Remark 4.4.4 *The above proof can be fairly simplified by letting $g_i = 0$ and defining a bent function in the Maiorana-McFarland class as $f(x, y) = Tr(\alpha x h(y))$, $f : \mathbb{F}_{p^k} \times \mathbb{F}_{p^k} \to \mathbb{F}_{p^k}$. Since $\alpha h(y)$ is a permutation for any nonzero $\alpha \in \mathbb{F}_{p^k}$, this essentially means that $f(x, y) = \alpha x h(y)$ is a vectorial bent function of dimension k.*

The main problem in increasing the bent space lies in the fact that all known approaches consider the isomorphism of $\mathbb{F}_{p^k} \times \mathbb{F}_{p^k}$ and $\mathbb{F}_{p^{2k}}$ which then naturally yield vectorial bent functions of dimension k. It seems that only planar functions give rise to bent functions of maximum size n, and this important problem is left open.

Open Problem 4.4.1 *Construct a set $\mathcal{F} = \{f_1, \ldots, f_r\}$, $r > k$, of bent functions $f_i : \mathbb{F}_{p^{2k}} \to \mathbb{F}_p$ such that all nonzero linear combinations $a_1 f_1 + \ldots + a_r f_r$ are bent. In addition, the set $\mathcal{F}$ must not be extendable to give the components of some known planar mapping.*

Chapter 5

Designing semi-bent, disjoint spectra and optimal plateaued functions

Mathematics reveals its secrets only to those who approach it with pure love, for its own beauty.

– Archimedes of Syracuse

SEVERAL INFINITE classes of semi-bent functions are proposed, where each class is characterized by either a different decomposition of such a function with respect to the Walsh spectrum of its subfunctions, or by the method used for its derivation. In particular, the exact count of the number of possibilities of decomposing bent functions in a subclass of the Maiorana-McFarland class, whose dual is cubic into four restrictions to $(n-2)-$dimensional subspaces, is given. Due to the close connection of semi-bent functions with disjoint spectra and bent functions, the former concept is of particular importance. It is shown that in general disjoint spectra (semi-bent) functions, commonly used in iterative constructions of cryptographically strong functions, are not rare combinatorial objects. Hence, one can create a multiple branching tree of the so-called optimal plateaued functions, which depending on the location of zero values in their Walsh spectrum then give infinite sequences of highly resilient optimal plateaued or semi-bent functions.

The main results are published in [1].

5.1 Introduction

There are a few methods of constructing semi-bent functions that can be found in the literature. After their introduction [29] semi-bent functions have been partially

treated in [107, 108] and later in [7, 27]. In [27], the quadratic case of both bent and semi-bent functions has been addressed. An important contribution [8] to the even case is the result relating the decomposition of bent functions to $(n-2)$-dimensional subspaces of $\mathbb{F}_2^n$. More precisely, the four restrictions to the cosets of the vector subspace $\langle a, b\rangle^{\perp}$ are all semi-bent functions in $(n-2)$-variables if and only if the second order derivative $D_a D_b(\tilde{f}) = 0$, where $\tilde{f}$ is the dual bent function of f. Some classes of semi-bent functions were also derived in [18, 93], but as pointed out in [22] these methods only cover a small portion of this huge class of functions. Especially, the method in [22] is particularly interesting since it combines two bent functions g and h to construct a semi-bent function of the form $f = g + h$ (where g belongs to the partial spread class $\mathcal{PS}_{ap}$ and h comes from the Niho class of bent functions). It should be noticed that the location of zeros in the spectra of semi-bent functions determines whether these functions possess some additional cryptographic properties (such as balancedness, resiliency) or not. More results regarding of constructing semi-bent functions can be found in [48, 67, 72, 73, 74, 99].

Here we provide several infinite classes of semi-bent functions whose design methods are essentially different. By employing some sufficient conditions (sometimes also necessary) we specify explicitly two classes of quadratic and cubic semi-bent functions. The decomposition of bent functions in a subclass of the Maiorana-McFarland class to four $(n-2)$-dimensional subspaces of $\mathbb{F}_2^n$ is also considered, and the exact count of $(n-2)-$ dimensional spaces for which this decomposition gives either bent, semi-bent or 5-valued spectra functions is derived. This result extends the initiative taken by Canteaut and Charpin in [8] where only the non-existence results concerning the decomposition into four bent functions were given for this class. Moreover, a generic method of constructing pairs of so-called 5-valued spectra functions whose concatenation then gives semi-bent functions is given.

In other direction, a simple result that provides a recursive framework of constructing disjoint spectra semi-bent functions is proposed. Based on that result, some infinite classes of resilient Boolean functions, which belong to the class of optimal plateaued functions (not necessarily semi-bent due to high resiliency order), with very high nonlinearity are exhibited. This result also answers an open problem of finding the explicit form of suitable initial functions in the so-called direct sum construction [17]. Some of the functions belonging to these new classes could not be obtained using the known methods without employing some exceptional instances of Boolean functions found recently by computer search.

5.2 Constructing semi-bent functions

The well-known Maiorana-McFarland class of bent functions, denoted by $\mathcal{M}$, can be defined as follows. Let us, for $n = 2k$, identify $\mathbb{F}_2^n$ with $\mathbb{F}_2^k \times \mathbb{F}_2^k$. Suppose $\pi : \mathbb{F}_2^k \to \mathbb{F}_2^k$ is a permutation and $g \in \mathfrak{B}_k$. A function $f : \mathbb{F}_2^k \times \mathbb{F}_2^k \to \mathbb{F}_2$ defined by

$$f(x, y) = x \cdot \pi(y) + g(y), \text{ for all } x, y \in \mathbb{F}_2^k, \tag{5.1}$$

is a bent function and it belongs to $\mathcal{M}$, (cf. [36, 66, 85]). On the other hand, if $\pi : \mathbb{F}_2^{n-r} \to \mathbb{F}_2^r$, where $r > n - r$, a class of balanced (resilient) functions with nonlinearity $2^{n-1} - 2^{r-1}$ can be derived, cf. for instance [78, 82, 87]. In particular, if $r = n/2 + 1$ this construction yields the balanced (resilient) semi-bent functions with nonlinearity $2^{n-1} - 2^{n/2}$. It should be noted that the degree of semi-bent functions is upper bounded by $n/2$ for even n, and depending on the choice of π a varying algebraic degree can be obtained (easily including the case $\deg(f) = n/2$).

In what follows, we specify some classes of semi-bent functions derived from a semi-bent 4-decomposition of bent functions. On the other hand, we also extend the above observation (related to semi-bent functions in $\mathcal{M}$) by providing a generic method of constructing semi-bent functions in $\mathfrak{B}_n$, for odd n, from two 5-valued spectra functions in $\mathfrak{B}_{n-1}$.

5.2.1 Semi-bent functions from two bent functions

In [93], a sufficient condition on two bent functions g and h used in the construction of semi-bent functions was given.

Theorem 5.2.1 ([93]) *Let n be even, and suppose that f and g are two bent functions in $\mathfrak{B}_n$. If there exists an $a \in \mathbb{F}_2^n$ such that $D_a f(x) = D_a g(x) + 1$, then the function $h(x) = f(x) + g(x) + D_a f(x) + D_a f(x)g(x)$ is a semi-bent function in even number of variables.*

This condition immediately implies the possibility of constructing infinite classes of semi-bent functions using known classes of quadratic bent functions [27, 93]. Notice that all quadratic bent functions are affine equivalent to the canonical form given by $\sum_{i=1}^{n/2} x_{2i-1}x_{2i}$.

Theorem 5.2.2 *Let $g \in \mathfrak{B}_n$, with n even, be a quadratic bent function of the form $g(x) = \sum_{i=1}^n b_i x_i + \sum_{1 \le i < j \le n} c_{i,j} x_i x_j$, for suitably chosen $b_i, c_{i,j} \in \mathbb{F}_2$. Define $f \in \mathfrak{B}_n$ as $f(x) = g(x) + \sum_{i=1}^n \alpha_i x_i$, where $\alpha_i \in \mathbb{F}_2$. Then, if $a \in \mathbb{F}_2^n$ is such that $a \cdot \alpha = 1$, the function*

$$h(x) = f(x) + g(x) + D_a f(x) + D_a f(x)g(x), \tag{5.2}$$

is a quadratic semi-bent function in $\mathfrak{B}_n$.

Proof. Let $l(x) = \sum_{i=1}^n \alpha_i x_i$, then for $a = (a_1, \ldots, a_n) \in \mathbb{F}_2^n$,

$$D_a f(x) + D_a g(x) = D_a l(x) = \alpha_1 a_1 + \ldots + \alpha_n a_n,$$

and since $a \cdot \alpha = 1$, then $D_a f(x) + D_a g(x) = 1$. It remains to show that h is a quadratic semi-bent function. Notice that $fg(x) = [g(x) + l(x)]g(x) = g(x) + l(x)g(x)$ (since in the Boolean ring $g(x)g(x) = g(x)$). Now, the functions $f(x) + g(x) = l(x)$ and $D_a f(x)$ are affine so the degree of h is given by

$$\deg(D_a f(x)g(x)) = \deg[D_a(g(x)) + D_a(l(x)g(x))].$$

It is enough to show that $\deg[D_a(l(x)g(x))] = 2$, which is straightforward. ■

Another related approach, though without restriction on the degree of a single bent function used, is given by the following result.

Theorem 5.2.3 *Let $f \in \mathfrak{B}_n$, n even, be a bent function and define $g(x) = f(x + a) + \alpha \cdot x$, where $\alpha \cdot a = 1$. $a, \alpha \in \mathbb{F}_2^n$. Then,*

$$h(x) = f(x) + g(x) + D_a f(x) + D_a f(x)g(x) \tag{5.3}$$

is a semi-bent function.

Proof. Obviously, g is also a bent function and

$$g(x + a) = f(x) + \alpha \cdot x + \alpha \cdot a. \tag{5.4}$$

We have

$$\begin{aligned} D_a f(x) + D_a g(x) &= [f(x) + f(x + a)] + [g(x) + g(x + a)] \\ &= [g(x) + f(x + a)] + [f(x) + g(x + a)] \\ &= \alpha \cdot x + \alpha \cdot x + \alpha \cdot a \\ &= \alpha \cdot a = 1. \end{aligned}$$

By Theorem 5.2.1, $h(x) = f(x)+g(x)+D_a f(x)+D_a f(x)g(x)$ is a semi-bent function. ■

Open Problem 5.2.1 *Find other examples/classes of bent functions g_1, g_2 satisfying $D_a g_1(x) = D_a g_2(x) + 1$.*

5.2.2 Semi-bent functions through bent 4-decomposition

The 4-decomposition of a Boolean function $f(x) \in \mathfrak{B}_n$ is a decomposition of f into four subfunctions defined on the four cosets of some $(n-2)$-dimensional linear subspace [8]. More precisely, for nonzero $a, b \in \mathbb{F}_2^n$ this $(n-2)$-dimensional subspace is defined as $\langle a, b\rangle^\perp$, where the *dual* of a linear subspace $V \subset \mathbb{F}_2^n$, denoted by $V^\perp$, is defined as $V^\perp = \{x \in \mathbb{F}_2^n : \forall y \in V, x \cdot y = 0\}$. Let (f_1, f_2, f_3, f_4) be such a decomposition, that is, $f_1, \ldots, f_4$ are defined on the four cosets $0+\langle a, b\rangle^\perp, a+\langle a, b\rangle^\perp, b+\langle a, b\rangle^\perp, (a+b)+\langle a, b\rangle^\perp$, respectively. We say that it is a *bent 4-decomposition* when all $f_i, i = 1, \ldots, 4$, are bent; a *semi-bent 4-decomposition* when all $f_i, i = 1, \ldots, 4$, are semi-bent; a *5-valued 4-decomposition* when all $f_i, i = 1, \ldots, 4$, are 5-valued spectra functions.

Another approach of deriving semi-bent functions on $\mathbb{F}_2^{n-2}$ is directly related to the decomposition of bent functions in $\mathfrak{B}_n$ to $(n-2)$-dimensional subspaces of $\mathbb{F}_2^n$ of the form $\langle a, b\rangle^\perp$, through the condition[1] that $D_a D_b \tilde{g} = 0$ for a bent function

[1] For shortness, we sometimes use the notation $D_a f$ instead of more correct $D_a f(x)$.

$g \in \mathbb{F}_2^n$ and its dual $\tilde{g}$ [8]. Therefore, if g is quadratic then $D_a D_b \tilde{g} = 0$ or 1 since $\tilde{g}$ is also quadratic, hence it is relatively easy to find a, b so that $D_a D_b \tilde{g} = 0$. Notice that if $D_a D_b \tilde{g} = 0$ for $a = (1, 0, 0, \ldots, 0)$ and $b = (0, 1, \ldots, 0)$, we get a standard decomposition of g as a concatenation of four semi-bent functions $f_1, \ldots, f_4 \in \mathbb{F}_2^{n-2}$ defined on the subspaces $\mathbb{F}_2^{n-2} \times (\epsilon_1, \epsilon_2)$, for $\epsilon_1, \epsilon_2 \in \mathbb{F}_2$. Since g is quadratic then $\deg(f_i) \leq 2$, and furthermore each f_i must be quadratic.

Nevertheless, a more interesting case arises when non-quadratic bent functions are regarded, since the degree of their dual bent function is not known in general, see e.g. [8]. Let us consider a class of bent functions $g_{\alpha,\gamma} : \mathbf{F}_{2^k} \times \mathbf{F}_{2^k} \to \mathbb{F}_2$ in $\mathcal{M}$ given by its trace representation

$$g_{\alpha,\gamma}(x, y) = Tr(\alpha x^\gamma y), \ x, y \in \mathbf{F}_{2^k}, \tag{5.5}$$

where for $n = 2k$ we must necessarily have $\gcd(\gamma, 2^k - 1) = 1$ so that x^γ is a permutation of $\mathbf{F}_{2^k}$, cf. equation (5.1). Then, $g_{\alpha,\gamma}$ is cubic if and only if $wt(\gamma) = 2$, where $wt(\gamma)$ is the Hamming weight of γ (using its binary representation). The dual $\widetilde{g}_{\alpha,\gamma}$ of the bent function $g_{\alpha,\gamma}$ is [36]

$$\widetilde{g}_{\alpha,\gamma}(x, y) = Tr(\beta x y^\delta), \text{ for all } x, y \in \mathbb{F}_{2^k}, \tag{5.6}$$

where $\gamma\delta \equiv 1 \pmod{(2^k - 1)}$ and $\beta = \alpha^{-\delta}$. Then, by imposing the condition that $D_a D_b \widetilde{g}_{\alpha,\gamma} = 0$, the 4-decomposition gives four semi-bent functions $f_1, \ldots, f_4$ defined on the cosets of $V = \langle a, b \rangle^\perp$ for some nonzero $a, b \in \mathbf{F}_{2^k} \times \mathbf{F}_{2^k}$; $D_a D_b \widetilde{g}_{\alpha,\gamma} = 1$ gives the 4-decomposition for which $f_1, \ldots, f_4$ are bent; otherwise, if $D_a D_b \widetilde{g}_{\alpha,\gamma} \neq 0, 1$, the decomposition yields four 5-valued spectra functions whose concatenation (of two functions) then gives a semi-bent function on $\mathfrak{B}_{n-1}$.

Theorem 5.2.4 *Let $n = 2k$, and $g_{1,\gamma} : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$ in $\mathcal{M}$ be given by its trace representation*

$$g_{1,\gamma}(x, y) = Tr(x^\gamma y), \text{ for all } x, y \in \mathbb{F}_{2^k}, \tag{5.7}$$

such that $\delta = 2^i + 1$, where $\gamma\delta \equiv 1 \pmod{(2^k - 1)}$ and $\gcd(i, k) = e$. Let $(a, b), (c, d) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ be two non-zero distinct elements, $V = \langle (a, b), (c, d) \rangle$ and (f_1, f_2, f_3, f_4) be the 4-decomposition of $g_{1,\gamma}$ with respect to $V^\perp$. Then

1) *$b = d = 0$ implies (f_1, f_2, f_3, f_4) is a semi-bent 4-decomposition.*
2) *Furthermore, (f_1, f_2, f_3, f_4) is a 5-valued 4-decomposition if and only if any one of the following is true:*
   - *(a) $a \neq 0$, $b = 0$, $d \neq 0$ and $a \notin d^{-(2^i+1)} \mathbb{F}_{2^e}^*$;*
   - *(b) $c \neq 0$, $d = 0$, $b \neq 0$ and $c \notin b^{-(2^i+1)} \mathbb{F}_{2^e}^*$;*
   - *(c) $a \neq 0$, $b \neq 0$, $d \neq 0$, $b = d$ and $a \notin d^{-(2^i+1)} \mathbb{F}_{2^e}^*$;*
   - *(d) $a \neq 0$, $b \neq 0$, $d \neq 0$, $b \neq d$ and, $d \notin b\mathbb{F}_{2^e}^*$ or $(ab^{-1}d + c) \notin b^{-(2^i+1)} \mathbb{F}_{2^e}$.*

PROOF. The derivative of the function $\widetilde{g}_{1,\gamma}$ with respect to the 2-dimensional subspace $V = \langle (a,b),(c,d)\rangle$ is

$$\begin{aligned} D_V\widetilde{g}_{1,\gamma}(x,y) &= D_{(c,d)}D_{(a,b)}\widetilde{g}_{1,\gamma}(x,y) = D_{(c,d)}D_{(a,b)}Tr(xy^{2^i+1}) \\ &= Tr(((ad+cb)+(ad^{2^i}+cb^{2^i})^{2^i})y^{2^i}) + Tr((bd^{2^i}+b^{2^i}d)x) \\ &\quad + Tr(ad^{2^i+1}+cb^{2^i+1}) + Tr((a+c)(bd^{2^i}+b^{2^i}d)). \end{aligned} \tag{5.8}$$

We have to characterize all the 2-dimensional subspaces of $\mathbb{F}_{2^k}\times\mathbb{F}_{2^k}$ with respect to which the function $\widetilde{g}_{1,\gamma}$ has either zero or non-constant derivative.

If $b = d = 0$, then $D_{(c,d)}D_{(a,b)}\widetilde{g}_{1,\gamma}(x,y) = 0$ for all $x, y \in \mathbb{F}_{2^k}$, which corresponds to a semi-bent 4-decomposition.

If $b = 0$ and $d \neq 0$, then $D_{(c,d)}D_{(a,b)}\widetilde{g}_{1,\gamma}(x,y) = Tr((ad+(ad^{2^i})^{2^i})y^{2^i})+Tr(ad^{2^i+1})$, which is not constant if and only if

$$\begin{aligned} & ad + (ad^{2^i})^{2^i} \neq 0, \\ i.e.,\ & ad + a^{2^i}d^{2^{2i}} \neq 0, \\ i.e.,\ & a^{2^i-1}d^{2^{2i}-1} \neq 1, \text{ since } d \neq 0 \text{ and } a \neq 0, \\ i.e.,\ & (ad^{2^i+1})^{2^i-1} \neq 1, \\ i.e.,\ & ad^{2^i+1} \notin \mathbb{F}_{2^e}^*, \text{ where } \gcd(i,k) = e. \end{aligned}$$

Therefore, if $b = 0$ and $d \neq 0$, then $D_{(c,d)}D_{(a,b)}\widetilde{g}_{1,\gamma}$ is not constant if and only if $a \notin d^{-(2^i+1)}\mathbb{F}_{2^e}^*$. From symmetry, we have if $d = 0$ and $b \neq 0$, then $D_{(c,d)}D_{(a,b)}\widetilde{g}_{1,\gamma}$ is not constant if and only if $c \notin b^{-(2^i+1)}\mathbb{F}_{2^e}^*$.

If $b \neq 0$ and $d \neq 0$ and $b = d$, then $V = \langle (a,b),(c,d)\rangle = \langle (a,0),(c,d)\rangle$. Therefore, $D_{(c,d)}D_{(a,b)}\widetilde{g}_{1,\gamma}$ is not constant if and only if $a \notin d^{-(2^i+1)}\mathbb{F}_{2^e}^*$.

If $a \neq 0$, $b \neq 0$, $d \neq 0$, $b \neq d$, then $D_{(c,d)}D_{(a,b)}\widetilde{g}_{1,\gamma}$ is not constant if and only if, either $bd^{2^i}+b^{2^i}d \neq 0$ or $ad+cb+(ad^{2^i}+cb^{2^i})^{2^i} \neq 0$. It is to be noted that $bd^{2^i}+b^{2^i}d \neq 0$ implies $d \notin b\mathbb{F}_{2^e}^*$. If $bd^{2^i}+b^{2^i}d = 0$, then there exists $\mu \in \mathbb{F}_{2^e}^*$ such that $d = \mu b$. By [42, Theorem 4] $ad+cb+(ad^{2^i}+cb^{2^i})^{2^i} \neq 0$ if and only if $(a\mu+c) \notin b^{-(2^i+1)}\mathbb{F}_{2^e}$. ■

Corollary 5.2.1 *Let $g_{1,\gamma} : \mathbb{F}_{2^k}\times\mathbb{F}_{2^k} \to \mathbb{F}_2$ be given as in Theorem 5.2.4, where $n = 2k$. If $b = d = 0 \in \mathbb{F}_2^k$, and $a, c \in \mathbb{F}_2^k$ such that $a = (1,0,\ldots,0)$, $c = (0,1,0,\ldots,0)$, then the functions g_i, $i = 1,\ldots,4$, defined on the four cosets of $V = \langle (a,b),(c,d)\rangle^\perp$ are semi-bent functions $g_i : \mathbb{F}_2^{n-2} \to \mathbb{F}_2$.*

PROOF. The statement follows directly from the proof of Theorem 5.2.4, and using the isomorphism between the vector space $\mathbb{F}_2^k$ and the field $\mathbb{F}_{2^k}$ in the definition of V. ■

Open Problem 5.2.2 *Specify $(a,b),(c,d)$, using the condition in Theorem 5.2.4, so that a usual decomposition into four 5-valued spectra functions is obtained, i.e., $f_1,\ldots,f_4$ should be defined on $\mathbb{F}_2^{n-2}\times\epsilon_1\times\epsilon_2$, for $\epsilon_1,\epsilon_2\in\mathbb{F}_2$.*

Now we specify the exact count of the number of bent, semi-bent and 5-valued 4-decompositions of the function $g_{1,\gamma}$. This result extends the initiative taken by Canteaut and Charpin [8, Section VII B], where only the impossibility of bent 4-decomposition for certain $g_{1,\gamma}$ was given. Before proving the main result we first give one preparatory result.

Lemma 5.2.5 *Let $n=2k$ be even, and define $g_{1,\gamma}(x,y)=Tr(x^\gamma y)$, where $\gamma\delta\equiv 1 \pmod{2^k-1}$, for $\delta=2^i+1$. If $\gcd(i,k)=e$, then $\frac{k}{e}$ is an odd integer.*

Proof. Since $\gcd(i,k)=e$, we can write $k=k_1\cdot e$, $i=i_1\cdot e$, where $\gcd(k_1,i_1)=1$. For $\delta=2^i+1$, the condition

$$\gamma(2^{i_1e}+1)\equiv 1 \pmod{2^{k_1e}-1}, \tag{5.9}$$

implies that $\gcd(2^{i_1e}+1,2^{k_1e}-1)=1$. On the other hand, it is well-known that $\gcd(2^{i_1e}+1,2^{k_1e}-1)=1$ if and only if $\frac{k_1e}{gcd(i_1e,k_1,e)}=\frac{k}{e}$ is an odd integer. ∎

Theorem 5.2.6 *Let $n=2k$, and $g_{1,\gamma}:\mathbb{F}_{2^k}\times\mathbb{F}_{2^k}\to\mathbb{F}_2$ in $\mathcal{M}$ given by its trace representation*

$$g_{1,\gamma}(x,y)=Tr(x^\gamma y),\ \text{for all } x,y\in\mathbb{F}_{2^k}, \tag{5.10}$$

such that $\delta=2^i+1$ where $\gamma\delta\equiv 1 \pmod{2^k-1}$ and $\gcd(i,k)=e$. Let $(a,b),(c,d)\in\mathbb{F}_{2^k}\times\mathbb{F}_{2^k}$ be two non-zero distinct elements, $V=\langle(a,b),(c,d)\rangle$ and (f_1,f_2,f_3,f_4) be the 4-decomposition of $g_{1,\gamma}$ with respect to $V^\perp$. Then $g_{1,\gamma}$ has altogether

$$2^{k+e-2}(2^k-1)+\frac{2^{k+e-1}(2^k-1)(2^{e-1}-1)}{3}$$

bent 4-decompositions,

$$2^{k-1}(2^k-1)(2^{e-1}-1)+\frac{(2^k-1)(2^{k-1}-1)}{3}+\frac{2^{k+e-1}(2^k-1)(2^{e-1}-1)}{3}$$

semi-bent 4-decompositions and the rest are 5-valued 4-decompositions.

Proof. As before, the derivative of the function $\widetilde{g}_{1,\gamma}=Tr(xy^\delta)$ with respect to the 2-dimensional subspace $V=\langle(a,b),(c,d)\rangle$ is

$$\begin{aligned}D_V\widetilde{g}_{1,\gamma}(x,y)&=D_{(c,d)}D_{(a,b)}\widetilde{g}_{1,\gamma}(x,y)=D_{(c,d)}D_{(a,b)}Tr(xy^{2^i+1})\\&=Tr(((ad+cb)+(ad^{2^i}+cb^{2^i})^{2^i})y^{2^i})+Tr((bd^{2^i}+b^{2^i}d)x)\\&\quad+Tr(ad^{2^i+1}+cb^{2^i+1})+Tr((a+c)(bd^{2^i}+b^{2^i}d)).\end{aligned} \tag{5.11}$$

If $b = d = 0$, then $D_{(c,d)}D_{(a,b)}\widetilde{g}_{1,\gamma}(x,y) = 0$ for all $(x,y) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$. The total number of distinct 2-dimensional subspaces of the form $V = \langle (a,0),(c,0)\rangle$ is

$$\frac{(2^k-1)(2^k-2)}{6} = \frac{(2^k-1)(2^{k-1}-1)}{3}.$$

This contributes to the count of semi-bent 4-decomposition.

If $b = 0$ and $d \neq 0$, then

$$\begin{aligned} D_{(c,d)}D_{(a,0)}\widetilde{g}_{1,\gamma}(x,y) &= D_{(c,d)}D_{(a,0)}Tr(xy^{2^i+1}) \\ &= Tr((ad + a^{2^i}d^{2^{2i}})y^{2^i}) + Tr(ad^{2^i+1}). \end{aligned} \tag{5.12}$$

The second-derivative $D_{(c,d)}D_{(a,0)}\widetilde{g}_{1,\gamma}$ is constant if and only if $ad + a^{2^i}d^{2^{2i}} = 0$, that is, if and only if $ad^{2^i+1} \in \mathbb{F}^*_{2^e}$, where $e = \gcd(i,k)$. For $ad^{2^i+1} \in \mathbb{F}^*_{2^e}$ and since by Lemma 5.2.5 $\frac{k}{e}$ is odd, we have

$$\begin{aligned} Tr(ad^{2^i+1}) &= Tr_1^e(Tr_e^k(ad^{2^i+1})) \\ &= Tr_1^e(ad^{2^i+1}Tr_e^k(1)) = Tr_1^e(ad^{2^i+1} \cdot 1) = Tr_1^e(ad^{2^i+1}). \end{aligned}$$

Thus, there are 2^{e-1} choices for $ad^{2^i+1} \in \mathbb{F}^*_{2^e}$ such that $Tr_1^e(ad^{2^i+1}) = 1$ and $2^{e-1}-1$ choices so that $Tr_1^e(ad^{2^i+1}) = 0$.

This implies that given any $a \in \mathbb{F}^*_{2^k}$ there are 2^{e-1} and $2^{e-1}-1$ choices of d so that $Tr_1^e(ad^{2^i+1})$ is equal to 1 and 0, respectively. The element $a \in \mathbb{F}^*_{2^k}$ can be chosen in 2^k-1 ways, $c \in \mathbb{F}_{2^k}$ can be chosen in 2^k ways. Therefore, considering the fact that $\langle (a,0),(c,d)\rangle = \langle (a,0),(a+c,d)\rangle$ for any choice of a,c,d, we infer that the total number of distinct 2-dimensional subspaces of the form $V = \langle (a,0),(c,d)\rangle$ on which $D_V\widetilde{g}_{1,\gamma} = 1$ is

$$\frac{2^k(2^k-1)2^{e-1}}{2} = 2^{k+e-2}(2^k-1),$$

whereas the total number of distinct 2-dimensional subspaces of the form $V = \langle (a,0),(c,d)\rangle$ on which $D_V\widetilde{g}_{1,\gamma} = 0$ is

$$\frac{2^k(2^k-1)(2^{e-1}-1)}{2} = 2^{k-1}(2^k-1)(2^{e-1}-1).$$

Finally, consider the case $b \neq 0$, $d \neq 0$ and $b \neq d$. In this case $D_{(c,d)}D_{(a,b)}\widetilde{g}_{1,\gamma}(x,y)$ is constant if and only if

$$(ad + cb) + (ad^{2^i} + cb^{2^i})^{2^i} = 0 \tag{5.13}$$

and

$$bd^{2^i} + b^{2^i}d = 0. \tag{5.14}$$

If $bd^{2^i} + b^{2^i}d = 0$ then $d = \delta b$ where $\delta \in \mathbb{F}_{2^e}^* \setminus \{1\}$, and the second-derivative takes the form

$$\begin{aligned} D_V\widetilde{g}_{1,\gamma}(x,y) &= D_{(c,d)}D_{(a,b)}\widetilde{g}_{1,\gamma}(x,y) = D_{(c,d)}D_{(a,b)}Tr(xy^{2^i+1}) \\ &= Tr(((ad+cb) + (ad^{2^i} + cb^{2^i})^{2^i})y^{2^i}) + Tr(ad^{2^i+1} + cb^{2^i+1}). \end{aligned} \tag{5.15}$$

Putting $d = \delta b$ in (5.13) and referring to the Proof of [42, Theorem 4] we obtain

$$c = a\delta + \frac{\delta'}{b^{2^i+1}}, \tag{5.16}$$

where $\delta' \in \mathbb{F}_{2^e}$. Note that a can be chosen in 2^k ways, b in $2^k - 1$ ways , d in $2^e - 2$ ways and c in 2^e ways and each 2 dimensional subspace has 6 distinct bases satisfying the same conditions. Thus the total number of distinct 2-dimensional subspaces on which the second-derivative is constant is

$$\frac{2^{k+e}(2^k-1)(2^e-2)}{6}. \tag{5.17}$$

If the above conditions are satisfied for (a,b), (c,d), then

$$\begin{aligned} D_{(c,d)}D_{(a,b)}\widetilde{g}_{1,\gamma}(x,y) &= D_{(c,d)}D_{(a,b)}Tr(xy^{2^i+1}) \\ &= Tr(ad^{2^i+1} + cb^{2^i+1}) \\ &= Tr(ab^{2^i+1}\delta(\delta+1)) + Tr(\delta'). \end{aligned} \tag{5.18}$$

Given any choice of a, $b \neq 0$, $d \neq 0$ and $b \neq d$ we have a fixed value of $\delta \in \mathbb{F}_{2^e}^* \setminus \{1\}$. To choose c, we are allowed to vary δ' over $\mathbb{F}_{2^k}$. Thus by (5.18) the second-derivative $D_{(c,d)}D_{(a,b)}\widetilde{g}_{1,\gamma}$ is 0 exactly 2^{e-1} times when c varies over $\mathbb{F}_{2^k}$ and a, b, d are fixed. Referring to (5.17), we infer that the the second-derivative is 0 (a semi-bent 4-decomposition) exactly over $\frac{2^{k+e-1}(2^k-1)(2^e-2)}{6}$ distinct subspaces of dimension two. The second derivative is 1 (a bent 4-decomposition) over the remaining $\frac{2^{k+e-1}(2^k-1)(2^e-2)}{6}$ subspaces, and the result follows. ∎

Remark 5.2.7 *The special case* $\gcd(i,k) = e = 1$ *in Theorem 5.2.6 implies that there are no bent* 4*-decompositions, which is actually Corollary 6 in [8] valid for odd* $k \geq 5$*. Notice that for* $k = 3$ *there are bent 4-decompositions as illustrated in Example 5.2.1*

Example 5.2.1 *Let* $n = 2k = 6$*, and consider the case* $i = 2$ *so that* $\gcd(i,k) = \gcd(2,3) = 1$*. Thus,* $\delta = 5$ *and* $\gamma = 3$*, so we consider the 4-decomposition of* $g_{1,3}(x,y) = Tr(x^3y)$*. In total, there are 651 distinct 2-dimensional subspaces. Then, in accordance to Theorem 5.2.6, there are 28 subspaces that gives a bent 4-decomposition, 7 subspaces correspond to semi-bent 4-decomposition and the remaining 616 subspaces correspond to a 5-valued 4-decomposition, which was also confirmed by computer simulations. In particular, the second derivatives* $D_V\widetilde{g}_{1,3}(x,y)$ *corresponding to 616 subspaces* V *for which* $D_V\widetilde{g}_{1,3}(x,y) \neq 0, 1$ *are always balanced, that is,* $wt(D_V\widetilde{g}_{1,3}) = 2^{n-1}$*.*

5.2.3 Semi-bent functions from 5-valued spectra functions

We notice that for odd n, semi-bent functions, when viewed as concatenation of two functions on $\mathfrak{B}_{n-1}$, must be of the following forms:

1. concatenation of two bent functions;
2. concatenation of two disjoint spectra semi-bent functions;
3. concatenation of two functions with 5-valued spectra.

In what follows, we give, for even n, a generic method of constructing pairs of 5-valued spectra functions in $\mathfrak{B}_n$, whose concatenation yields a semi-bent function on $\mathfrak{B}_{n+1}$. This method is a special case of a much wider framework of generalizing the Maiorana-McFarland class [103]. A recursive method of constructing pairs of disjoint spectra semi-bent functions in higher dimensions by using a pair of disjoint spectra semi-bent functions from a smaller space will be given in the next section.

Theorem 5.2.8 *Let n be an even positive integer. Let $A \cup B = \mathbb{F}_2^{n/2-1}$ with $A \cap B = \emptyset$, $|A| = u_1$ and $|B| = u_2$. Let $C \cup D = \mathbb{F}_2^{n/2}$ with $C \cap D = \emptyset$, $|C| = u_3$ and $|D| = u_4$. Furthermore, let $B' = B \times \mathbb{F}_2$, $C' = \mathbb{F}_2 \times C$, and suppose that $u_1 \leq u_3$ and $2u_2 = u_4$. Let $x = (x_1, \ldots, x_n)$ and define two injective mappings Φ_1 and Φ_2 from A to C' satisfying,*

$$\begin{aligned} &\{\Phi_1(x_1, \ldots, x_{\frac{n}{2}-1}) \mid (x_1, \ldots, x_{\frac{n}{2}-1}) \in \mathbb{F}_2^{n/2-1}\} \\ \cap &\{\Phi_2(x_1, \ldots, x_{\frac{n}{2}-1}) \mid (x_1, \ldots, x_{\frac{n}{2}-1}) \in \mathbb{F}_2^{n/2-1}\} \quad = \emptyset. \end{aligned} \tag{5.19}$$

Let Ψ_1 and Ψ_2 be two bijective mapping from B' to D. We define two n-variable functions as follows:

$$g_1(x) = \begin{cases} \Phi_1(x_1, \ldots, x_{\frac{n}{2}-1}) \cdot (x_{\frac{n}{2}}, \ldots, x_n), \text{ if } (x_1, \ldots, x_{\frac{n}{2}-1}) \in A \\ \Psi_1(x_1, \ldots, x_{\frac{n}{2}-1}, x_{\frac{n}{2}}) \cdot (x_{\frac{n}{2}+1}, \ldots, x_n), \text{ if } (x_1, \ldots, x_{\frac{n}{2}-1}) \in B \end{cases} \tag{5.20}$$

and

$$g_2(x) = \begin{cases} \Phi_2(x_1, \ldots, x_{\frac{n}{2}-1}) \cdot (x_{\frac{n}{2}}, \ldots, x_n), \text{ if } (x_1, \ldots, x_{\frac{n}{2}-1}) \in A \\ \Psi_2(x_1, \ldots, x_{\frac{n}{2}-1}, x_{\frac{n}{2}}) \cdot (x_{\frac{n}{2}+1}, \ldots, x_n), \text{ if } (x_1, \ldots, x_{\frac{n}{2}-1}) \in B \end{cases}. \tag{5.21}$$

Then, $g_1, g_2 \in \mathfrak{B}_n$ are two 5-valued spectra functions, and furthermore

$$f(x, x_{n+1}) = (1 + x_{n+1})g_1(x) + x_{n+1}g_2(x)$$

is a semi-bent function on $\mathfrak{B}_{n+1}$.

PROOF. Let $\alpha = (\alpha'_i, \alpha''_{n-i}) = (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_2^n$, where $\alpha'_i = (\alpha_1, \ldots, \alpha_i)$ and $\alpha''_{n-i} = (\alpha_{i+1}, \ldots, \alpha_n)$. In the same way we denote $x = (x'_i, x''_{n-i})$. The Walsh transform of $g_i(x), i = 1, 2$ at α is computed as

$$\begin{aligned} W_{g_i}(\alpha) &= \sum_{x \in \mathbb{F}_2^n} (-1)^{g_i(x)+\alpha \cdot x} \\ &= \sum_{x \in A \times \mathbb{F}_2^{n/2+1}} (-1)^{g_i(x)+\alpha \cdot x} + \sum_{x \in B' \times \mathbb{F}_2^{n/2}} (-1)^{g_i(x)+\alpha \cdot x}. \end{aligned} \tag{5.22}$$

Note that

$$\begin{aligned} \sum_{x \in A \times \mathbb{F}_2^{n/2+1}} (-1)^{g_i(x)+\alpha \cdot x} &= \sum_{x \in A \times \mathbb{F}_2^{n/2+1}} (-1)^{\Phi_i(x'_{n/2-1}) \cdot x''_{n/2+1} + \alpha'_{n/2-1} \cdot x'_{n/2-1} + \alpha''_{n/2+1} \cdot x''_{n/2+1}} \\ &= \sum_{x'_{n/2-1} \in A} (-1)^{\alpha'_{n/2-1} \cdot x'_{n/2-1}} \sum_{x'' \in \mathbb{F}_2^{n/2+1}} (-1)^{(\Phi_i(x'_{n/2-1}) + \alpha''_{n/2+1}) \cdot x''_{n/2+1}} \\ &= \begin{cases} \pm 2^{n/2+1}, & \text{if } \Phi_i^{-1}(\alpha''_{n/2+1}) \text{ exists} \\ 0, & \text{otherwise} \end{cases}. \end{aligned} \tag{5.23}$$

Similarly,

$$\sum_{x \in B' \times \mathbb{F}_2^{n/2}} (-1)^{g_i(x)+\alpha \cdot x} = \begin{cases} \pm 2^{n/2}, & \text{if } \Psi_i^{-1}(\alpha''_{n/2}) \text{ exists} \\ 0, & \text{otherwise} \end{cases}. \tag{5.24}$$

Since $A \cap B = \emptyset$ and $C \cap D = \emptyset$, we have

$$\sum_{x \in A \times \mathbb{F}_2^{n/2+1}} (-1)^{g_i(x)+\alpha \cdot x} \cdot \sum_{x \in B' \times \mathbb{F}_2^{n/2}} (-1)^{g_i(x)+\alpha \cdot x} = 0.$$

Therefore,

$$W_{g_i}(\alpha) \in \{0, \pm 2^{n/2}, \pm 2^{n/2+1}\}, \tag{5.25}$$

which means that g_i are 5-valued spectra functions.
Then, for $\varepsilon \in \mathbb{F}_2$, we have

$$\begin{aligned} W_f(\varepsilon, \alpha) &= \sum_{(x_{n+1}, x) \in \mathbb{F}_2^n} (-1)^{f(x_{n+1}, x) + (\varepsilon, \alpha) \cdot (x_{n+1}, x)} \\ &= \sum_{(x_{n+1}, x) \in \mathbb{F}_2^{n+1}} (-1)^{(1+x_{n+1}) \cdot g_1(x) + x_{n+1} \cdot g_2(x) + \varepsilon \cdot x_{n+1} + \alpha \cdot x} \\ &= \sum_{\substack{x \in \mathbb{F}_2^n \\ x_{n+1}=0}} (-1)^{g_1(x)+\alpha \cdot x} + (-1)^{\varepsilon} \sum_{\substack{x \in \mathbb{F}_2^n \\ x_{n+1}=1}} (-1)^{g_2(x)+\alpha \cdot x} \\ &= W_{g_1}(\alpha) + (-1)^{\varepsilon} W_{g_2}(\alpha). \end{aligned} \tag{5.26}$$

Since

$$\{\Phi_1(x'_{x_{n/2-1}}) \mid x_{n/2-1} \in \mathbb{F}_2^{n/2-1}\} \cap \{\Phi_2(x'_{x_{n/2-1}}) \mid x_{n/2-1} \in \mathbb{F}_2^{n/2-1}\} = \emptyset,$$

we must have

$$\sum_{x \in A \times \mathbb{F}_2^{n/2+1}} (-1)^{g_1(x)+\alpha \cdot x} \cdot \sum_{x \in A \times \mathbb{F}_2^{n/2+1}} (-1)^{g_2(x)+\alpha \cdot x} = 0. \tag{5.27}$$

If $W_{g_1}(\alpha) = \pm 2^{n/2+1}$ then $W_{g_2}(\alpha) = 0$ and if $W_{g_2}(\alpha) = \pm 2^{n/2+1}$ then $W_{g_1}(\alpha) = 0$. Therefore, when $\alpha''_{n/2+1} \in \{\Phi_i(\alpha'_{n/2-1}) \mid \alpha'_{n/2-1} \in A,\ i = 1, 2\}$, implies that

$$W_f(\varepsilon, \alpha) = \pm 2^{n/2+1}. \tag{5.28}$$

In a similar way, when $\alpha''_{n/2} \in \{\Psi_i(\alpha'_{n/2}) \mid \alpha'_{n/2} \in B',\ i = 1, 2\}$, implies that

$$W_f(\varepsilon, \alpha) = \pm 2^{n/2} + (-1)^{\varepsilon}(\pm 2^{n/2}) \in \{0, \pm 2^{n/2+1}\}. \tag{5.29}$$

Except for the cases above, we always have $W_f(\varepsilon, \alpha) = 0$, which together with the equations (5.28) and (5.29) proves that f is a semi-bent function. ∎

Example 5.2.2 *Let us consider the construction of a semi-bent function on* $\mathbb{F}_2^6$, *i.e.,* $n = 6$. *Let* $A = \{(0,0), (0,1)\}$ *and* $B = \{(1,0), (1,1)\}$ *such that* $A \cup B = \mathbb{F}_2^2$ *and* $A \cap B = \emptyset$. *Let*

$$\begin{aligned} C &= \{(0,0,0), (0,0,1), (0,1,0), (1,0,0)\}, \\ D &= \{(0,1,1), (1,0,1), (1,1,0), (1,1,1)\}, \end{aligned}$$

such that $C \cup D = \mathbb{F}_2^3, C \cap D = \emptyset$ *and* $|D| = 2|B|$. *Let* $B' = B \times \mathbb{F}_2$ *and* $C' = \mathbb{F}_2 \times C$. *We now specify two injective mappings* $\Phi_1, \Phi_2 : A \mapsto C'$ *in the following way*

$$\Phi_1((0,0)) = (1,0,0,1), \quad \Phi_1((0,1)) = (1,1,0,0),$$

and

$$\Phi_2((0,0)) = (1,0,1,0), \quad \Phi_2((0,1)) = (1,0,0,0).$$

Define two bijective mappings $\Psi_1, \Psi_2 : B' \mapsto D$ *in the following way*

$$\begin{aligned} &\Psi_1((1,0,0)) = (1,0,1), \quad \Psi_1((1,0,1)) = (1,1,0), \\ &\Psi_1((1,1,0)) = (1,1,1), \quad \Psi_1((1,1,1)) = (0,1,1), \end{aligned}$$

and

$$\begin{aligned} &\Psi_2((1,0,0)) = (1,1,0), \quad \Psi_2((1,0,1)) = (1,1,1), \\ &\Psi_2((1,1,0)) = (0,1,1), \quad \Psi_2((1,1,1)) = (1,0,1). \end{aligned}$$

Then g_1 can be partially specified as follows

$$\begin{aligned} g_1(0,0,X_1) = x_3 + x_6, \;\; g_1(0,1,X_1) = x_3 + x_4, \;\; &\text{if } (x_1,x_2) \in A \\ g_1(1,0,0,X_2) = x_4 + x_6, \;\; g_1(1,0,1,X_2) = x_4 + x_5, \;\; &\text{if } (x_1,x_2) \in B \\ g_1(1,1,0,X_2) = x_4 + x_5 + x_6, \;\; g_1(1,1,1,X_2) = x_5 + x_6, \;\; &\text{if } (x_1,x_2) \in B \end{aligned}$$

where $X_1 = (x_3, x_4, x_5, x_6)$ and $X_2 = (x_4, x_5, x_6)$.
Similarly, g_2 can be partially specified as follows

$$\begin{aligned} g_2(0,0,X_1) = x_3 + x_5, \;\; g_2(0,1,X_1) = x_3, \;\; &\text{if } (x_1,x_2) \in A \\ g_1(1,0,0,X_2) = x_4 + x_5, \;\; g_1(1,0,1,X_2) = x_4 + x_5 + x_6, \;\; &\text{if } (x_1,x_2) \in B \\ g_1(1,1,0,X_2) = x_5 + x_6, \;\; g_1(1,1,1,X_2) = x_4 + x_6, \;\; &\text{if } (x_1,x_2) \in B \end{aligned}$$

The functions $g_1, g_2 \in \mathfrak{B}_6$ are completely specified, and they are 5-valued spectra functions, i.e., $W_{g_i}(\alpha) = \{0, \pm 8, \pm 16\}$. Consequently, the function $f = (1+x_7)g_1(x) + x_7 g_2(x)$ is a semi-bent function on $\mathfrak{B}_7$.

The above construction gives an explicit method of constructing a large class of semi-bent functions explicitly. Assuming that $|A| = |B|$ and $|C| = |D|$ in Theorem 5.2.8, which stands for the largest portion of the functions in this class, a lower bound on the cardinality of this class of semi-bent functions is estimated below.

Proposition 5.2.1 *The cardinality of this class of semi-bent functions in $\mathfrak{B}_n$ given in Theorem 5.2.8, denoted by $\mathfrak{B}_n^{SB}$, is lower bounded by*

$$\#\mathfrak{B}_n^{SB} > 2 \times \frac{2^{\frac{n}{2}}!}{(2^{\frac{n}{2}} - 2^{\frac{n}{2}-2})!} \times (2^{\frac{n}{2}-1}!)^2$$

Proof. Assuming that $|A| = |B| = 2^{\frac{n}{2}-2}$ and $|C| = |D| = 2^{\frac{n}{2}-1}$, we clearly derive a lower bound. The first factor counts for g_0 and g_1, and the mid term refers to the number of possibilities to inject two sets of cardinality $2^{\frac{n}{2}-2}$ into a set of cardinality $2^{n/2}$. The last term counts for the number of ways of defining two bijective mappings Ψ_1 and Ψ_2 over the sets of cardinality $2^{\frac{n}{2}-1}$. ∎

5.3 A recursive construction of disjoint spectra functions

Recently, a recursive method for constructing a pair of resilient $(n+4, m+3, n-m, 2^{n+3} - 2^{m+4})$ optimal plateaued functions from a pair of $(n, m, n-m-1, 2^{n-1} - 2^{m+1})$ disjoint spectra optimal plateaued functions has been proposed in [43]. This iterative method generates the functions with relatively large order of resiliency, though it only gives one infinite sequence of resilient optimal plateaued functions. Notice that for $m = \lfloor \frac{n}{2} \rfloor - 1$ such an m-resilient function is essentially a semi-bent function. The

modified version of Tarannikov's construction [96], described in [82], proposes a concatenation based iterative method for constructing an $(n+3, m+2, n-m, 2^{n+2}-2^{m+3})$ function in desired form (a function f is in a desired form if it is in the form $f = (1 + x_n)f_1 + x_n f_2$, where f_1, f_2 are two $(n-1, m, d-1, -)$ functions, which is equivalent to the condition that f_1 and f_2 are disjoint spectra functions [82]) from one $(n, m, n-m-1, 2^{n-1} - 2^{m+1})$ function in desired form. Both these constructions have optimal parameters, but due to a relatively large increase of resiliency these sequences may only give semi-bent functions in the first, respectively in the first two steps of iteration. Notice that for odd n, if $f_1, f_2 \in \mathfrak{B}_{n-1}$ are disjoint spectra semi-bent functions with $W_{f_i} \in \{0, \pm 2^{\frac{n+1}{2}}\}$, then we have $W_f \in \{0, \pm 2^{\frac{n+1}{2}}\}$ as well.

In this section, we consider iterative methods for constructing disjoint spectra functions. Firstly, we give an infinite sequence of pairs of optimal plateaued disjoint spectra functions, and then consider a suitable modification in order to generate an infinite sequence of disjoint spectra semi-bent functions.

5.3.1 Disjoint spectra functions

Our main result of this section given in Theorem 5.3.1 (see bellow), in contrast to the above methods [43, 82], allows us to generate optimal plateaued functions for an arbitrary increase of the variable space $k \geq 1$, and with a controllable increase of resiliency so that an infinite sequence of semi-bent functions can be generated iteratively. It is a consequence of the following simple result which allows us to generate disjoint spectra functions iteratively regardless of the choice of concatenation.

Proposition 5.3.1 *Let $f_0, g_0 \in \mathfrak{B}_n$ be a pair of disjoint spectra functions, and let the functions*

$$F(x, y) = f_0(x) + s(y) \quad \text{and} \quad G(x, y) = g_0(x) + t(y),$$

where $s, t \in \mathfrak{B}_k$ be arbitrary k-variable Boolean functions. Then, $F(x, y)$ and $G(x, y)$ are disjoint spectra functions.

Proof. Let $\omega = (\omega_1, \omega_2) \in \mathbb{F}_2^{n+k}$, where $\omega_1 \in \mathbb{F}_2^n$ and $\omega_2 \in \mathbb{F}_2^k$. Then, we have

$$\begin{aligned} W_F(\omega) &= \sum_{(x,y)\in\mathbb{F}_2^{n+k}} (-1)^{F(x,y)+\omega\cdot(x,y)} = \sum_{x\in\mathbb{F}_2^n} (-1)^{f_0(x)+\omega_1\cdot x} \sum_{y\in\mathbb{F}_2^k} (-1)^{s(y)+\omega_2\cdot y} \\ &= W_{f_0}(\omega_1) W_s(\omega_2). \end{aligned}$$

Similarly, $W_G(\omega) = W_{g_0}(\omega_1) W_t(\omega_2)$, and thus $W_F(\omega) W_G(\omega) = 0$, since $W_{f_0}(\omega_1) W_{g_0}(\omega_1) = 0$ holds for any $\omega_1 \in \mathbb{F}_2^n$. ∎

Theorem 5.3.1 *Let f_0, g_0 be a pair of $(n-1, m, n-m-2, 2^{n-2}-2^{m+1})$ optimal plateaued functions with disjoint spectra. Then for any $i = 1, \ldots, k$, the functions f_i and g_i defined by,*

$$f_1 = x_n + f_0, \;\; f_2 = x_{n+1} + f_1 \;\; , \ldots, \;\; f_k = x_{n+k} + f_{k-1}$$
$$g_1 = x_n + g_0, \;\; g_2 = x_{n+1} + g_1, \;\; \ldots, \;\; g_k = x_{n+k} + g_{k-1}$$

are a pair of $(n+i-1, m+i, n-m-2, 2^{n+i-2}-2^{m+i+1})$ optimal plateaued functions with disjoint spectra. Moreover, the function $h_i = (f_i + g_i)x_{n+i} + f_i$ is an $(n+i, m+i, n-m-1, 2^{n+i-1}-2^{m+i+1})$ optimal plateaued function.

Proof. Note that the functions f_i can be written as

$$f_1 = x_n + f_0, \;\; f_2 = x_{n+1} + f_1 = x_{n+1} + x_n + f_0, \ldots, f_i = x_{n+i-1} + x_{n+i-2} + \ldots + x_n + f_0.$$

Also, $g_i = x_{n+i-1} + x_{n+i-2} + \ldots + x_n + g_0$. The functions f_i and g_i are two partially linear functions with order of resiliency $m+i$ [106]. By Proposition 5.3.1 f_i and g_i are pair of disjoint spectra functions. Obviously, the function $h_i = (f_i + g_i)x_{n+i} + f_i$ is an $(n+i, m+i, n-m-1, 2^{n+i-1}-2^{m+i+1})$ optimal plateaued function. ∎

The above theorem provides a recursive method so that the number of variables increases by one in each step. For instance, starting from two $(6, 2, 3, 24)$ disjoint spectra semi-bent functions, this method generates an infinite sequence of $(7+k, 2+k, 4, 2^{7+k-1}-2^{2+k+1})$ optimal plateaued functions, for $k \geq 0$, i.e., the functions $(7, 2, 4, 56)$, $(8, 3, 4, 112), (9, 4, 4, 224), (10, 5, 4, 448)$, $(11, 6, 4, 896), \ldots$. Therefore, a *single* infinite sequence of optimal plateaued functions is obtained. Note that the first two functions in the above sequence are actually semi-bent functions.

Nevertheless, if we would like to increase the degree in the proposed construction, then we may use the modified version of Tarannikov's construction in the first step and proceed with our method so that $(10, 4, 5, 480), (11, 5, 5, 960), (12, 6, 5, 1920), \ldots$ optimal plateaued functions are obtained, where the first function is actually semi-bent function. In the same way our method can be interchanged with the concatenation method in [43] resulting in functions with slightly different (but again optimal) parameters due to the recursion specified through $(n+4, m+3, n-m, 2^{n+3}-2^{m+4})$. Indeed, the second function in this sequence [43] is a $(15, 8, 6, 15872)$ function obtained from $(11, 5, 5, 960)$ (which is in turn obtained from a $(7, 2, 4, 56)$ function). If we adopt the $(10, 4, 5, 480)$ semi-bent function as initial function, which is a concatenation of two $(9, 4, 4, 224)$ disjoint spectra functions, then proceeding the iteration with our method we would get a $(15, 6, 6, 16128)$ semi-bent function. This 6-resilient Boolean function has nonlinearity 16128 and the same degree as the $(15, 8, 6, 15872)$ function generated using the method in [43], so that the lower resiliency (but still moderate and acceptable in most applications) is traded-off against higher nonlinearity.

Consequently, a multiple branching tree of disjoint spectra optimal plateaued functions can be generated from a single pair of disjoint spectra functions.

5.3.2 Disjoint spectra semi-bent functions

In contrast to the case n is odd, if n is even a semi-bent function on $\mathbb{F}_2^n$ cannot be viewed as a concatenation of two disjoint spectra semi-bent functions.

Proposition 5.3.2 *Let n be even and consider any semi-bent function $f \in \mathfrak{B}_n$ so that $W_f \in \{0, \pm 2^{\frac{n+2}{2}}\}$. Then, f cannot be decomposed into a pair of disjoint spectra semi-bent functions.*

Proof. Let $f = x_n(g+h)+g$, where $g, h \in \mathfrak{B}_{n-1}$, and let

$$G = \{\omega \mid W_g(\omega) = 0, \omega \in \mathbb{F}_2^{n-1}\}, \quad H = \{\omega \mid W_h(\omega) = 0, \omega \in \mathbb{F}_2^{n-1}\}.$$

Then, if g and h are a pair of disjoint spectra functions, we must have $|G|+|H| \geq 2^{n-1}$, for $W_g(\omega)W_h(\omega) = 0$ holds for any $\omega \in \mathbb{F}_2^{n-1}$. This implies that either $|G| \geq 2^{n-2}$ or $|H| \geq 2^{n-2}$, and by Parseval's equation (which claims that $\sum_{\omega \in \mathbb{F}_2^{n-1}} W_g^2(\omega) = 2^{2(n-1)}$ and $\sum_{\omega \in \mathbb{F}_2^{n-1}} W_h^2(\omega) = 2^{2(n-1)}$) either g or h is not a semi-bent function. ∎

For the convenience of the reader we recall the so-called modified version of Tarannikov's method [82].

Proposition 5.3.3 ([82]) *Let f be an (n, m, d, N_f) function in the desired form, where f_1, f_2 are both $(n-1, m, d-1, -)$ functions. Let $F = x_{n+2} + x_{n+1} + f$ and $G = (1+x_{n+2}+x_{n+1})f_1+(x_{n+2}+x_{n+1})f_2+x_{n+2}+x_n$. Then, $H = (1+x_{n+3})F+x_{n+3}G$ is an $(n+3, m+2, d+1, 2^{n+1}+4N_f)$ function in the desired form.*

Theorem 5.3.2 *Let $F, G \in \mathcal{B}_{n+2}$ be a pair of $(n+2, m+2, n-m-1, 2^{n+1}-2^{m+3})$ optimal plateaued functions with disjoint spectra constructed by means of the modified version of Tarannikov's method. Then, for $x \in \mathbb{F}_2^{n+2}$ the functions*

$$T(x, x_{n+3}, x_{n+4}) = x_{n+3}x_{n+4} + F(x) \tag{5.30}$$
$$R(x, x_{n+3}, x_{n+4}) = x_{n+3}x_{n+4} + G(x) \tag{5.31}$$

are a pair of $(n+4, m+2, n-m-1, 2^{n+3}-2^{m+4})$ disjoint spectra functions.

Proof. It is easily verified that the concatenation of the form $(1+x_{n+3})F(x) + x_{n+3}F(x) = F(x)$, is an $(n+3, m+2, n-m-1, 2^{n+2}-2^{m+4})$ function, and the concatenation of F and its complement $\overline{F}$ is an $(n+3, m+3, n-m-1, 2^{n+2}-2^{m+4})$ function. Since the ANF of T is $x_{n+3}x_{n+4} + F$, and the above concatenations are disjoint spectra functions, the function T is an $(n+4, m+2, n-m-1, 2^{n+3}-2^{m+4})$ function.
In the same way, we obtain R is an $(n+4, m+2, n-m-1, 2^{n+3}-2^{m+4})$ function. By Proposition 5.3.1, we deduce that T and R are disjoint spectra functions. ∎

Corollary 5.3.1 *Let $T, R \in \mathcal{B}_{n+4}$ be defined as in Theorem 5.3.2. Then the function $H = (T + R)x_{n+5} + T$ is an $(n + 5, m + 2, n - m, 2^{n+4} - 2^{m+4})$ function.*

PROOF. Since $\max_\omega |W_T(\omega)| = \max_\omega |W_R(\omega)| = 2^{m+5}$, and the two spectra are disjoint, then $\max_\omega |W_H(\omega)| = 2^{m+5}$. Thus, $N_H = 2^{n+4} - 2^{m+4}$. The ANF of H is $(F + G)x_{n+5} + F + x_{n+3}x_{n+4}$, and hence H is an $(n + 5, m + 2, n - m, 2^{n+4} - 2^{m+4})$ function. ∎

Another consequence of Theorem 5.3.2 is the following corollary that concerns disjoint spectra semi-bent functions.

Corollary 5.3.2 *Let n be even and $F, G \in \mathcal{B}_n$ be a pair of $(n, m, n - m - 1, 2^{n+1} - 2^{m+1})$ disjoint spectra semi-bent functions. Then, for $x \in \mathbb{F}_2^n$ the functions*

$$T(x, x_{n+1}, x_{n+2}) = x_{n+1}x_{n+2} + F(x) \tag{5.32}$$

$$R(x, x_{n+1}, x_{n+2}) = x_{n+1}x_{n+2} + G(x) \tag{5.33}$$

are a pair of $(n + 2, m, n - m - 1, 2^{n+1} - 2^{m+2})$ disjoint spectra semi-bent functions.

Example 5.3.1 *Consider a $(7, 2, 4, 56)$ which is a concatenation of two $(6, 2, 3, 24)$ disjoint spectra semi-bent functions [82]. Using the two $(6, 2, 3, 24)$ functions, by means of Corollary 5.3.2, an infinite sequence of $(6 + i, 2, 3, 2^{5+i} - 2^{\lfloor \frac{6+i}{2} \rfloor})$, semi-bent functions, $i \geq 0$, can be generated. Notice that for odd $n = 6 + i$, a semi-bent function is simply a concatenation of two disjoint spectra semi-bent functions on $\mathfrak{B}_{n-1}$. On the other hand, Corollary 5.3.1 generates an infinite sequence of $(7 + 5i, 2 + 2i, 4 + i, 2^{7+5i-1} - 2^{3+3i})$ functions, for $i \geq 0$. The first function in this sequence is a $(12, 4, 5, 1984)$ function. The weight divisibility result, i.e., $W_f \equiv 0 \pmod{2^{m+2+\lfloor \frac{n-m-2}{d} \rfloor}}$, implies that for any $(12, 4, 5, N_f)$ function f we have $W_f(\omega) \equiv 0 \pmod{128}$ for any $\omega \in \mathbb{F}_2^{12}$. Since our nonlinearity is $N_H = 2^{n-1} - \frac{1}{2}\max_\omega |W_H(w)| = 1984$ it implies $\max_\omega |W_H(w)| = 128$, and the nonlinearity is maximal. Indeed, due to Parseval's inequality $\max_\omega |W_f(w)| > 2^{n/2} = 64$ (since f is a resilient function) which combined with the divisibility result gives $\max_\omega |W_f(\omega)| \geq 128$ for any 4-resilient function $f \in \mathbb{F}_2^{12}$ of any degree $1 \leq d \leq n - t - 1 = 7$.*

Remark 5.3.3 *It is easily verified that the standard Maiorana-McFarland method (cf. [30, 36]) of concatenating distinct linear (affine) functions is not efficient for constructing a $(12, 4, 5, 1984)$ function. To attain the same nonlinearity as above 32 distinct linear functions in 7 variables are needed and only linear functions in at least 5 variables may be used (due to resiliency order), but there are only $\binom{7}{5} + \binom{7}{6} + \binom{7}{7} = 29$ such functions. Nevertheless, a $(12, 4, 5, 1984)$ function can be easily constructed from a $(9, 3, 5, 240)$ function which was recently found using advanced search algorithms [51, 52, 86].*

Remark 5.3.4 *In addition, a $(12, 4, 5, 1984)$ function cannot be constructed using the direct sum method. Recall that, if $h(x, y) = f(x) + g(y)$, where f is an n_1-variable, m_1-resilient ($m_1 \geq 0$), and g is an n_2-variable, m_2-resilient ($m_2 \geq 0$),*

then h is an (n_1+n_2)- variable, m_1+m_2+1-resilient. Moreover, degree of h is $\max\{deg(f), deg(g)\}$*, and nonlinearity is* $2^{n_1}N_g + 2^{n_2}N_f - 2N_fN_g$*. Indeed, the best one can do is to construct a* $(12,4,4,1984)$ *function using direct sum of a* $(7,2,4,56)$ *and a* $(5,1,3,12)$ *function, but still having a lower degree than our first function in the above sequence.*

5.3.3 A comparison to indirect sum construction

We relate our results from the previous section to the so-called indirect sum construction proposed by Carlet [17]. It will be shown that the construction given by Theorem 5.3.2 and Corollary 5.2.1 can be embedded in the indirect sum framework, and the analysis of the ANF of our function essentially specifies the initial functions to be used in the indirect sum method; thus solving an open problem posed in [17]. We briefly review this construction technique below.

Theorem 5.3.5 *[17] Let r, s, t and m be positive integers such that $t < r$ and $m < s$. Let f_1 and f_2 be two r-variable t-resilient functions. Let g_1 and g_2 be two s-variable m-resilient functions. Then the function*

$$h(x,y) = f_1(x) + g_1(y) + (f_1+f_2)(x)(g_1+g_2)(y),\ x \in \mathbb{F}_2^r, y \in \mathbb{F}_2^s$$

is an $(r+s)$-variable $(t+m+1)$-resilient function. If f_1+f_2 and g_1+g_2 are non-constant, then the algebraic degree of h equals $\max\{deg(f_1), deg(g_1), deg(f_1+f_2) + deg(g_1+g_2)\}$*. The value of Walsh transform of h at $(a,b) \in \mathbb{F}_2^r \times \mathbb{F}_2^s$ equals*

$$W_h(a,b) = \frac{1}{2}W_{f_1}(a)(W_{g_1}(b) + W_{g_2}(b)) + \frac{1}{2}W_{f_2}(a)(W_{g_1}(b) - W_{g_2}(b)).$$

This implies

$$N_h \geq -2^{r+s-1} + 2^s(N_{f_1} + N_{f_2}) + 2^r(N_{g_1} + N_{g_2}) - (N_{f_1} + N_{f_2})(N_{g_1} + N_{g_2}).$$

Moreover, if the Walsh transform of g_1 and g_2 have disjoint supports, then, denoting by f the function $f(x_r, x_{r+1}) = (1+x_{r+1})f_1(x) + x_{r+1}f_2(x)$, we have

$$N_h \geq 2^{s-1}N_f + (2^r - N_f)\min_{i\in\{1,2\}} N_{g_i}.$$

If, additionally, the Walsh transform of f_1 and f_2 have disjoint supports, then

$$N_h = \min_{i,j\in\{1,2\}}\{2^{r+s-2} + 2^{r-1}N_{g_j} + 2^{s-1}N_{f_i} - N_{f_i}N_{g_j}\}$$

In addition, to represent the function h as a concatenation of two disjoint spectra functions (so that it can be used in an iterative manner) the functions g_1, g_2 must fulfil some further conditions, see [17] for further details. Carlet left this issue as an open

problem in general and only a few examples of functions satisfying the aforementioned conditions could be found.

However, we note that our method can be seen in the framework of the indirect sum. Let us consider the construction of disjoint spectra functions given by Theorem 5.3.2 and Corollary 5.2.1. The ANF of the function $H \in \mathfrak{B}_{n+5}$ is $F + (F + G)x_{n+5} + x_{n+3}x_{n+4}$, and since the ANFs of the functions $F, G \in \mathfrak{B}_{n+2}$ are known [82], i.e.,

$$F = f_0 + (f_0 + g_0)x_n + x_{n+1} + x_{n+2}, \tag{5.34}$$

and

$$G = f_0 + (f_0 + g_0)(x_{n+1} + x_{n+2}) + x_n + x_{n+2}, \tag{5.35}$$

we have $H = f_0 + (f_0 + g_0)(x_n + x_nx_{n+5} + x_{n+1}x_{n+5} + x_{n+2}x_{n+5}) + x_{n+1} + x_{n+2} + x_nx_{n+5} + x_{n+1}x_{n+5} + x_{n+3}x_{n+4}$, where $f_0, g_0 \in \mathfrak{B}_{n-1}$. Then the function H can be written as

$$\begin{aligned} H &= f_0 + (x_{n+1} + x_{n+2} + x_nx_{n+5} + x_{n+1}x_{n+5} + x_{n+3}x_{n+4}) + \\ &\quad +(f_0 + g_0)((x_{n+1} + x_{n+2} + x_nx_{n+5} + x_{n+1}x_{n+5} + x_{n+3}x_{x+4}) + \\ &\quad +x_n + x_{n+1} + x_{n+2} + x_{n+2}x_{n+5} + x_{n+3}x_{n+4}), \end{aligned}$$

so that the corresponding relationship to the function h above is given by

$$\begin{aligned} f_1 &= f_0, \quad f_2 = g_0, \\ g_1 &= x_{n+1} + x_{n+2} + x_nx_{n+5} + x_{n+1}x_{n+5} + x_{n+3}x_{n+4}, \\ g_2 &= x_n + x_{n+1} + x_{n+2} + x_{n+2}x_{n+5} + x_{n+3}x_{n+4}. \end{aligned}$$

One can check that the functions g_1, g_2 are two $(6, 1, 2, 24)$ disjoint spectra functions, and the $g_1 + g_2$ is a non-constant function, thus satisfying the set of conditions for the use in the indirect sum method. In the language of indirect sum our functions f_0, g_0 have the form $(n-1, t, n-t-2, 2^{n-2} - 2^{t+1})$, whereas for the quadratic functions g_1, g_2 the above parameters are $s = 6$ and $m = 1$. This case corresponds to the case $m \leq s - 5$ that was left as an open problem by Carlet in [17].

We emphasize that our method, given by Theorem 5.3.1, only requires two optimal plateaued disjoint spectra functions whose any kind of concatenation again yields a pair of optimal plateaued disjoint spectra functions.

5.3.4 Algebraic immunity related to the proposed construction

The bounds on algebraic immunity of a Boolean function can be derived from the algebraic immunities of its restrictions to a given hyperplane and to its complement [33]. For instance, if $f(x_1, \ldots, x_n) = (1 + x_n)f_1(x_1, \ldots, x_{n-1}) + x_nf_2(x_1, \ldots, x_{n-1})$, we have,

$$\begin{aligned} &\text{if} \quad AI(f_1) \neq AI(f_2), \qquad \text{then} \quad AI(f) = \min\{AI(f_1), AI(f_2)\} + 1, \\ &\text{if} \quad AI(f_1) = AI(f_2), \qquad \text{then} \quad AI(f_1) \leq AI(f) \leq AI(f_1) + 1. \end{aligned}$$

Some bounds on the algebraic immunities of some classical constructions, such as the Maiorana-McFarland, can be found in [33, 68, 79].

A trivial bound on algebraic immunity for the functions in our construction can be derived in the following way. Suppose that there are annihilators of functions f_0 and g_0, some functions a and b such that $deg(a) = deg(b) = d$, and d is the minimal degree of all annihilators of functions f_0 and g_0. If we define the function $(1 + x_n)(1 + x_{n+1} + x_{n+2})(1 + x_{n+3})a(x) = k(x)$ of degree $d + 3$, then by multiplying the equation (5.30) by the function k, proves that $T(x) \cdot k(x) = 0$ and shows that $k(x)$ is a nonzero annihilator of $T(x)$ of degree $d + 3$. Note, however, that we could have defined the function $(1 + x_n + x_{n+2})(1 + x_{n+1} + x_{n+2})(1 + x_{n+3})a(x) = l(x)$ of degree $d + 3$, and l is a nonzero annihilator of G of degree $d + 3$.

This upper bound is obviously loose and the actual algebraic immunity of these functions was checked by computer simulations. For instance, the function $(12, 4, 5, 1984)$ mentioned previously has a slightly suboptimal algebraic immunity equal to 5, hence there is no severe deterioration of the algebraic properties due to the simplicity of this construction.

Chapter 6

On cross-correlation properties of S-boxes and their design using semi-bent functions

Lots of people working in cryptography have no deep concern with real application issues. They are trying to discover things clever enough to write papers about.

– Whitfield Diffie

SEVERAL DIFFERENT methods of employing semi-bent functions for constructing substitution boxes (S-boxes) with good cross-correlation properties have been proposed. Most notably, a correct estimate of the cross-correlation absolute indicator of two bent functions is given and the design of vectorial semi-bent functions is introduced. The propagation properties of the design approaches taken here can be further optimized through a careful selection of the input functions.

The main results are published in [81].

6.1 Introduction

A useful characterization of some important classes of cryptographic Boolean functions in terms of their cross-correlation properties was established in [88] and certain weaknesses of commonly used S-boxes were also identified. The analysis of a given S-box was performed by measuring the cross-correlation between the component functions of the S-box. Nevertheless, a further generalization of these criteria was considered in [110] by introducing two additional indicators (as in the case of autocorrelation) the sum-of-squares indicator $\sigma_{f,g}$ and the absolute indicator $\Delta_{f,g}$.

A rather loose lower bound on $\sigma_{f,g}$ was also given in [110], which turned out not to be applicable to balanced functions giving a negative-valued bound. This bound was later improved in [44] for the case of balanced functions f and g, and recently a further refinement of the lower bound, including both the balanced and unbalanced case, was presented in [111]. The bounds on the sum-of-squares indicator $\sigma_{f,g}$, reflecting the cross-correlation properties, was essentially given in terms of the sum-of-squares indicators of individual functions f and g. More precisely, it was shown that $0 \leq \sigma_{f,g} \leq \frac{\sigma_f+\sigma_g}{2}$, thus relating the autocorrelation properties of the considered functions to their cross-correlation value. Some further results, relating cross-correlation properties and other cryptographic criteria, were given recently in [112]. The upper bound on $\sigma_{f,g}$ was further improved in [109], the above arithmetic mean has been replaced by the geometric mean value, thus $0 \leq \sigma_{f,g} \leq \sqrt{\sigma_f \cdot \sigma_g}$.

While the above mentioned works mainly address the issues of tightening the bounds on the two indicators, less attention was devoted to the design of S-boxes with overall good cryptographic properties. Some attempts, regarding the design of balanced Boolean functions satisfying SAC and having a lower (better) values of the absolute indicator (referring to autocorrelation properties of a single function) than previously known classes of functions, have been made in [111]. Also, an analysis of the propagation properties of the inverse function, used as the S-box in the Advanced Encryption Standard (AES), was given in [28]. From a practical point of view, having in mind that global avalanche characteristics mainly concern the design of secure S-boxes used in block ciphers, the main challenge that remains is the design of vectorial mappings $F(x) = (f_1(x), \ldots, f_m(x))$, where $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, so that the indicators σ_{f_i,f_j} and Δ_{f_i,f_j} attain their lowest possible values for all $1 \leq i < j \leq m$.

This chapter proposes several construction methods of highly nonlinear S-boxes whose cross-correlation properties of their component functions are very good. For this purpose, some of the well-known classes of functions such as bent and semi-bent functions are utilized. Our first initiative considers a theoretical investigation related to the lower bound on the absolute indicator $\Delta_{f,g}$ in the case f and g are bent functions. We derive a sufficient condition which ensures that $\Delta_{f,g}$ attains its lowest possible value $2^{n/2}$, which indicates an erroneous conclusion in a recent article of Zhou *et al.* [112]. More precisely, in [112, Corollary 4.2] it was claimed that if f is an n-variable bent function (thus n is even), then $\Delta_{f,g} \geq 2^{n/2}$ for any function g and $\Delta_{f,g} = 2^{n/2}$ if and only if g is an affine function, which is not true. It is shown that a sufficient condition that the absolute indicator $\Delta_{f,g}$ attains its lowest possible value $2^{n/2}$ is that $f + g$ is also a bent function. Thus, a class of vectorial bent functions is characterized by this property since by definition all nonzero linear combinations of its component functions are again bent. This important result has also been confirmed by computer simulations. Furthermore, a class of vectorial semi-bent functions with very good cross-correlation properties is proposed. In addition, a practical method of constructing perfectly uncorrelated S-boxes, for an even number of input variables, is given. Such a mapping $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ necessarily satisfies that $m \leq 4$, and we give an

example of a perfectly uncorrelated S-box of size 4×4. All the classes proposed in this chapter (apart from perfectly uncorrelated S-boxes) can be further optimized with respect to their propagation characteristics. Nevertheless, a theoretical framework for this optimization appears to be difficult due to a complicated dependency on the input functions used. The main challenge in the design of S-boxes whose component functions are semi-bent functions roughly corresponds to the problem of finding a set of semi-bent functions whose Walsh spectra is pairwise disjoint at as many positions as possible.

6.2 S-boxes with good cross-correlation properties

Several construction techniques related to the design of S-boxes with good cross-correlation properties are presented in this section. Since bent functions achieve the highest possible nonlinearity it is natural to investigate their cross-correlation properties in due detail. We show that vectorial bent functions naturally induce a class of bent functions whose cross-correlation absolute indicator attains the lowest possible value $2^{n/2}$. On the other hand, it turns out that a careful selection of a set of semi-bent functions might provide S-boxes with (sub)optimal cross-correlation properties. In difference to bent functions, which can be turned into balanced functions if suitably modified, the use of semi-bent functions may immediately give rise to balanced S-boxes satisfying most of the relevant cryptographic criteria.

6.2.1 The absolute indicator value of bent functions

The use of vectorial bent functions in the design of S-boxes was first suggested by Nyberg [77], and later Carlet [15] also argued that the unbalancedness and relatively low degree of this functions (upper bounded by $n/2$) are not decisive factors to exclude this class of functions for their use in certain cryptographic applications. Nevertheless, even though many classes of bent functions and their construction methods have been proposed (see survey on bent functions by Carlet in [15]), there are essentially a few attempts [77, 102] that deals with vectorial bent functions.

It is well-known [104], that $0 \leq \Delta_f \leq 2^n$ and $2^{2n} \leq \sigma_f \leq 2^{3n}$ for any $f \in \mathfrak{B}_n$, where the lower bound for both indicators is achieved by bent functions only. In [112, Theorem 4.1], it was claimed that if $f \in \mathfrak{B}_n$ is bent and $g \in \mathfrak{B}_n$ is arbitrary, then $\sigma_{f,g} = 2^{2n}$ and $\Delta_{f,g} \geq 2^{n/2}$. Furthermore, it was claimed that $\Delta_{f,g} = 2^{n/2}$ if and only if g is an affine function [112, Corollary 4.2]. This statement appears not to be completely correct, since if g is bent as well, then $\Delta_{f,g}$ can attain its lowest value $2^{n/2}$ as shown below. There is an error in the proof of [112, Corollary 4.2], since it is not necessary that g is affine.

Theorem 6.2.1 *Let $f, g \in \mathfrak{B}_n$ be two bent functions and define the function $h \in \mathfrak{B}_n$ as,*

$$(-1)^{h(\omega)} = \frac{1}{2^n}\mathcal{F}(f + \varphi_\omega)\mathcal{F}(g + \varphi_\omega), \quad \text{for all } \omega \in \mathbb{F}_2^n.$$

Then, $\Delta_{f,g} = 2^{\frac{n}{2}}$ if and only if h is a bent function. In particular, if $f+g$ is a bent function, then $\Delta_{f,g} = 2^{\frac{n}{2}}$.

PROOF. According to the cross-correlation theorem [88],

$$2^n[C_{f,g}(0),\ldots,C_{f,g}(2^n-1)] = [\mathcal{F}(f+\varphi_0)\mathcal{F}(g+\varphi_0),\ldots,\mathcal{F}(f+\varphi_{2^n-1})\mathcal{F}(g+\varphi_{2^n-1})]H_n,$$

where H_n is the Hadamard matrix of order 2^n defined recursively as $H_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, and $H_n = H_1 \otimes H_{n-1}$ for $n > 1$. Here, $\otimes$ denotes the Kronecker product of two matrices and the decimal representation of α is used to denote $C_{f,g}(\alpha)$. Notice that $\sigma_{f,g} = 2^{2n}$ and since $\Delta_{f,g} = \max_{\alpha\in\mathbb{F}_2^n} \mid C_{f,g}(\alpha) \mid \geq 2^{n/2}$ [112], it implies that $\mid C_{f,g}(\alpha) \mid = 2^{n/2}$ for any $\alpha \in \mathbb{F}_2^n$ if $\Delta_{f,g} = 2^{\frac{n}{2}}$. Replacing $\frac{1}{2^n}\mathcal{F}(f+\varphi_\omega)\mathcal{F}(g+\varphi_\omega)$ with $(-1)^{h(\omega)}$, the above equation yields,

$$[C_{f,g}(0),\ldots,C_{f,g}(2^n-1)] = [(-1)^{h(0)},\ldots,(-1)^{h(2^n-1)}]H_n,$$

and therefore $\mid C_{f,g}(\alpha) \mid = 2^{n/2}$ for any $\alpha \in \mathbb{F}_2^n$, if and only if h is a bent function.

In particular, for the dual bent functions $\tilde{f}$ and $\tilde{g}$ defined by $(-1)^{\tilde{f}(\omega)} = 2^{-n/2}\mathcal{F}(f+\varphi_\omega)$ and $(-1)^{\tilde{g}(\omega)} = 2^{-n/2}\mathcal{F}(g+\varphi_\omega)$, we have:

$$(-1)^{\tilde{f}(\omega)+\tilde{g}(\omega)} = \frac{1}{2^n}\mathcal{F}(f+\varphi_\omega)\mathcal{F}(g+\varphi_\omega),$$

which implies that if $\tilde{f}+\tilde{g}$ is bent then $\Delta_{f,g} = 2^{n/2}$. On the other hand, it is well-known that the Walsh spectra of $f+g$ and of $\tilde{f}+\tilde{g}$ attain the same values (see Carlet [15, pp. 66]). Thus, if $f+g$ is bent then so is $\tilde{f}+\tilde{g}$, and consequently $\Delta_{f,g} = 2^{\frac{n}{2}}$. ■

In the next section, we employ this result to provide the evidence concerning the existence of vectorial bent $(n, n/2)$ S-boxes whose cross-correlation absolute indicator attains its minimum value $\Delta_{f,g} = 2^{n/2}$, for any two component bent functions f and g of such an S-box.

6.2.2 S-boxes from vectorial bent functions in the $\mathcal{PS}_{ap}$ class

Even though many classes of bent functions and their construction methods have been proposed (see survey on bent functions by Carlet in [15]), there are essentially a few attempts [77, 102] that deals with the design of vectorial bent functions. In a recent article[1] [75], vectorial bent functions (that stem from the partial spread class $\mathcal{PS}$ class introduced by Dillon [36]) were characterized in terms of the properties of the cyclic group $\mathcal{U}$ of (2^k+1)th roots of unity, that is, $\mathcal{U} = \{u \in \mathbb{F}_{2^n} : u^{2^k+1} = 1\}$.

[1] The result is given in reduced form since there is one more equivalence originally in [75] which is not needed here.

Theorem 6.2.2 *[75] Let $n = 2k$, and define $F(x) = Tr_k^n(P(x))$, where $P(x) = \sum_{i=1}^{t} a_i x^{i(2^k-1)}$ and $t \leq 2^k$. Then the following conditions are equivalent:*

1. *F is a vectorial bent function of dimension k.*
2. *$\sum_{u \in \mathcal{U}} (-1)^{Tr_1^k(\lambda F(u))} = 1$ for all $\lambda \in \mathbb{F}_{2^k}^*$.*
3. *There are two values $u \in \mathcal{U}$ such that $F(u) = 0$, and furthermore if $F(u_0) = 0$, then F is one-to-one and onto from $\mathcal{U}_0 = \mathcal{U} \setminus u_0$ to $\mathbb{F}_{2^k}$.*

Employing Theorem 6.2.1 and noting that any (nonzero) linear combination of the component functions of a vectorial bent function is again bent, we immediately have the following result.

Theorem 6.2.3 *Let $F(x)$ be defined as in Theorem 6.2.2 for a suitable choice of $a_i \in \mathbb{F}_{2^n}$ so that F is a vectorial bent function. Then, for each $\alpha, \beta \in \mathbb{F}_{2^k}^*$, $\alpha \neq \beta$, the linear combinations $f_\alpha(x)$ and $f_\beta(x)$ of the component functions of $F(x)$, given by $Tr_1^n(\alpha F(x))$ and $Tr_1^n(\beta F(x))$ respectively, satisfy*

$$\Delta_{f_\alpha, f_\beta} = 2^{\frac{n}{2}}, \qquad \sigma_{f_\alpha, g_\beta} = 2^{2n}.$$

Example 6.2.1 *The component functions (and all their pairwise distinct linear combinations) of a vectorial bent function given by $F(x) = Tr_3^6(x^7 + \alpha^{21}x^{21})$ have the property that $\Delta_{f_i, f_j} = 2^3 = 8$, where f_i and f_j denote any two distinct nonzero linear combinations of the component functions and α is a primitive element in $\mathbb{F}_{2^6}$.*

Notice that such an S-box, viewed as a mapping $F : \mathbb{F}_2^n \to \mathbb{F}_2^{n/2}$, has many desirable properties: its algebraic degree is $n/2$, the nonlinearity is maximal $\mathcal{N}_F = 2^{n-1} - 2^{\frac{n}{2}-1}$, each linear combination of its component functions satisfy PC(n), and its cross-correlation properties are relatively good.

6.2.3 Perfectly uncorrelated S-boxes from semi-bent functions

Since highly nonlinear perfectly uncorrelated S-boxes are strongly related to disjoint spectra semi-bent functions (cf. [112]), we investigate the possibilities of providing some theoretical framework for designing such S-boxes. We notice that the spectra of any semi-bent function $f \in \mathfrak{B}_n$ contains exactly 2^{n-2} nonzero values and $3 \cdot 2^{n-2}$ zero values, which easily follows from the Parseval equality $\sum_{\alpha \in \mathbb{F}_2^n} \mathcal{F}^2(f + \varphi_\alpha) = 2^{2n}$. This observation immediately leads to the following result.

Proposition 6.2.1 *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ for even n, where for $F = (f_1, \ldots, f_m)$ each $f_i : \mathbb{F}_2^n \to \mathbb{F}_2$ is a semi-bent Boolean function. If F is perfectly uncorrelated with respect to its component functions so that $\Delta_{f_i, f_j} = \sigma_{f_i, f_j} = 0$, for $f_i \neq f_j$, then $m \leq 4$. Furthermore, if $m = 4$ then F is not balanced.*

PROOF. Any two functions f_i, f_j are perfectly uncorrelated if and only if $\mathcal{F}(f_i + \varphi_\alpha)\mathcal{F}(f_j + \varphi_\alpha) = 0$, thus f_i and f_j are disjoint spectra functions. Since $\#\{\alpha \in \mathbb{F}_2^n : \mathcal{F}(f_i + \varphi_\alpha) = 0\} = 3 \cdot 2^{n-2}$, then if any f_i and f_j are disjoint spectra functions for $1 \leq i < j \leq m$, it implies $m = 4$. Also, if $m = 4$ and $f_1, \ldots, f_4$ are pairwise disjoint spectra functions there exists f_i, $1 \leq i \leq 4$, such that $\mathcal{F}(f_i + \varphi_\alpha) \neq 0$, thus F is not balanced. ∎

To demonstrate the possibility of designing perfectly uncorrelated S-boxes of size 4×4, we use the so-called 4-decomposition of bent functions described in [8]. More precisely, given a bent function $g \in \mathfrak{B}_n$, the four functions $f_1, \ldots, f_4 \in \mathfrak{B}_{n-2}$ defined on the cosets of $V = \langle a, b\rangle^\perp$ (for some nonzero $a, b \in \mathbb{F}_2^n$) are pairwise disjoint spectra semi-bent functions if and only if $D_a D_b \widetilde{g}(x) = 0$, where $\widetilde{g}$ is the dual bent function of g. For simplicity, we utilize a recent result in [1], where a subclass of bent functions in the Maiorana-McFarland class, denoted by $\mathcal{M}$, were characterized in terms of those 4-decompositions that explicitly give a decomposition into four semi-bent functions.

Theorem 6.2.4 *[1] Let $n = 2k$, and $g_{\alpha,\gamma} : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$ in $\mathcal{M}$ given by its trace representation*

$$g_{1,\gamma}(x, y) = Tr(x^\gamma y), \text{ for all } x, y \in \mathbb{F}_{2^k}, \tag{6.1}$$

such that $\delta = 2^i + 1$, where $\gamma\delta \equiv 1 \pmod{(2^k - 1)}$. Let $(a, b), (c, d) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ be two non-zero distinct elements, $V = \langle (a, b), (c, d)\rangle$ and (f_1, f_2, f_3, f_4) be the 4-decomposition of $g_{1,\gamma}$ with respect to $V^\perp$. Then,

$$b = d = 0 \text{ implies } (f_1, f_2, f_3, f_4) \text{ is a semi-bent 4-decomposition.}$$

For convenience of the reader we repeat the proof of this result.
PROOF. The derivative of the function $\widetilde{g}_{1,\gamma}$ with respect to the 2-dimensional subspace $V = \langle (a, b), (c, d)\rangle$ is

$$\begin{aligned} D_V \widetilde{g}_{1,\gamma}(x, y) &= D_{(c,d)} D_{(a,b)} \widetilde{g}_{1,\gamma}(x, y) = D_{(c,d)} D_{(a,b)} Tr(xy^{2^i+1}) \\ &= Tr(((ad + cb) + (ad^{2^i} + cb^{2^i})^{2^i})y^{2^i}) + Tr((bd^{2^i} + b^{2^i}d)x) \\ &\quad + Tr(ad^{2^i+1} + cb^{2^i+1}) + Tr((a + c)(bd^{2^i} + b^{2^i}d)). \end{aligned} \tag{6.2}$$

It is not difficult to see, that if $b = d = 0$, then $D_{(c,d)} D_{(a,b)} \widetilde{g}_{1,\gamma}(x, y) = 0$ for all $x, y \in \mathbb{F}_{2^k}$, which corresponds to a semi-bent decomposition. ∎

This result gives us a possibility of finding semi-bent 4-decompositions explicitly (using a standard representation in terms of concatenation) and to construct perfectly uncorrelated S-boxes. If $b = d = 0 \in \mathbb{F}_2^k$, and $a = (1, 0, \ldots, 0)$, $c = (0, 1, 0, \ldots, 0)$ (where $a, c \in \mathbb{F}_2^k$), then the functions $f_i : \mathbb{F}_2^{n-2} \to \mathbb{F}_2$, $i = 1, \ldots, 4$, defined as restrictions of g to the four cosets of $V = \langle (a, b), (c, d)\rangle^\perp$ are semi-bent functions.

Example 6.2.2 *Let $n = 2k = 6$ and consider the case $i = 2$, so that $\gcd(k, i) = \gcd(3, 2) = 1$. Thus, $\delta = 5$ and $\gamma = 3$, so we consider the 4-decomposition of $g_{1,3}(x, y) = Tr(x^3 y)$. Let $b = d = 0 \in \mathbb{F}_2^3$, and $a = (1, 0, 0)$, $c = (0, 1, 0)$. Then, the four functions $f_i : \mathbb{F}_2^4 \to \mathbb{F}_2$ in the 4-decomposition of the function $g_{1,3}(x, y)$ can be written as $f_1 = g(0, 0, x_3, y_1, y_2, y_3)$, $f_2 = g(0, 1, x_3, y_1, y_2, y_3)$, $f_3 = g(1, 0, x_3, y_1, y_2, y_3)$ and $f_4 = g(1, 1, x_3, y_1, y_2, y_3)$. The truth tables of the function g (computed using the Magma software) is given by,*

$$g = [0000000001100011001101010101011001111000000110110100110100101110],$$

where ordering of the vectors is as follows

$$g = [g(0, 0, \ldots, 0), g(1, 0, \ldots, 0), \ldots, g(1, 1, \ldots, 1)].$$

Then, the semi-bent functions f_i are given as bellow.

$$f_1 = 0000000010101010; \quad f_2 = 0010011110001101;$$
$$f_3 = 0011100110010011; \quad f_4 = 0001111010110100;$$

Notice that f_1, for instance, is specified on those values of g whose two first input coordinates are zeros, thus the truth table of f_1 is obtained by taking the first, the fifth, and so on, value from the truth table of g. Since g is bent then $\mathcal{F}(g+\varphi_\alpha) = \pm 8$, for any $\alpha \in \mathbb{F}_2^6$. The component functions f_i being semi-bent has their spectra values in the set $\{0, \pm 8\}$. Thus, any f_i and f_j, $1 \leq i \neq j \leq 4$, are disjoint spectra semi-bent functions, otherwise g is not bent. Therefore, the S-box defined via its component functions $f_1, \ldots, f_4$ (hence a mapping $F : \mathbb{F}_2^4 \to \mathbb{F}_2^4$) satisfies $\Delta_{f_i, f_j} = 0$ and consequently $\sigma_{f_i, f_j} = 0$, for all $1 \leq i \neq j \leq 4$.

6.2.4 S-boxes from vectorial semi-bent functions

A class of vectorial semi-bent functions by combining vectorial bent functions from the partial spread class and Niho class are deduced. It is demonstrated that this class of functions has slightly better cross-correlation properties compared to the inverse function, and further improvements are possible by selecting the input vectorial functions in an optimal way.

In a recent article [22], a new class of semi-bent functions, obtained by adding up two bent functions from different families, was derived. For $n = 2k$, a *spread* is a collection $\{E_i, i = 1, \ldots, 2^k + 1\}$ of k-dimensional disjoint linear subspaces $E_i \subset \mathbb{F}_2^n$ such that $E_i \cap E_j = \{0\}$ for $i \neq j$, and $\cup_{i=1}^{2^k+1} E_i = \mathbb{F}_2^n$. The standard example of spread, through the identification of $\mathbb{F}_{2^k}$ and $\mathbb{F}_2^k$, is $\{u\mathbb{F}_{2^k} : u \in \mathcal{U}\}$ (where $\mathcal{U}$ is the cyclic group mentioned earlier).

Theorem 6.2.5 *[22] Let $k \geq 2$ and $n = 2k$. Let $\{E_i, i = 1, \ldots, 2^k + 1\}$ be a spread in $\mathbb{F}_2^n$ and h a Boolean function whose restriction to every E_i is linear (possibly null). Let S be any subset of $\{1, \ldots, 2^k + 1\}$ and $g = \sum_{i \in S} 1_{E_i} \pmod 2$ where 1_{E_i} is the indicator of E_i. Then $g + h \in \mathfrak{B}_n$ is semi-bent if and only if g and h are bent.*

As remarked by Carlet in [22], the spread $\{u\mathbb{F}_{2^k} : u \in \mathcal{U}\}$ is the only known spread up to linear equivalence. Notice that nonlinear Boolean functions whose restriction to any vector space $u\mathbb{F}_{2^k}$ are linear, are sums of Niho power functions (see [22]), that is, of functions of the form:

$$Tr_1^n(a_s x^{(2^k-1)s+1}) \quad \text{or} \quad Tr_1^k(a_s x^{(2^k-1)s+1}), \;\; 1 \le s \le 2^k, \; a_s \in \mathbb{F}_{2^n}, \tag{6.3}$$

where the letter case applies when $s = 2^{k-1}+1$, that is, $(2^k-1)s+1$ and 2^k+1 are conjugates in this case. Then, taking g to be a bent function in Dillon's $\mathcal{PS}$ class [36] (a union of either 2^{k-1} or $2^{k-1}+1$ disjoint subspaces E_i) and h to be a Niho bent function, several classes of semi-bent functions could be deduced in [22].

In [80], a simple condition for extending Boolean bent functions to vectorial bent functions was given. Namely, assuming that $f(x) = Tr_1^n(\lambda x^d), \lambda \in \mathbb{F}_{2^n}$, is a Boolean bent function in $\mathfrak{B}_n$, then if x^d is not a permutation of $\mathbb{F}_{2^n}$ but x^d permutes $\mathbb{F}_{2^m}$, where $m \mid n$, then $F(x) = Tr_m^n(\lambda x^d)$ is a vectorial bent function, $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$. In particular, this is true for a Niho bent function $h(x) = Tr_1^k(\alpha x^{2^k+1})$, $\alpha \in \mathbb{F}_{2^k}$. Indeed, in the case $n = 2k$, we have $\gcd(2^n-1, 2^k+1) = 2^k+1$ and $\gcd(2^k-1, 2^k+1) = 1$. Therefore, the function $H(x) = Tr_k^n(\alpha x^{2^k+1})$ is a vectorial bent function and moreover all the linear combinations of its component Boolean functions of the form $Tr_1^k(\gamma H(x)) = Tr_1^k(\gamma Tr_k^n(\alpha x^{2^k+1})) = Tr_1^n(\gamma\alpha x^{2^k+1})$, where $\gamma \in \mathbb{F}_{2^k}^*$, are Niho bent functions which are linear on any $E_i = u\mathbb{F}_{2^k}$.

Thus, for even $n = 2k$, there is a possibility of constructing vectorial semi-bent functions by combining vectorial bent functions of Dillon and Niho type.

Theorem 6.2.6 *Let for $n = 2k$ the function $F(x) = Tr_k^n(\sum_{i=1}^t a_i x^{i(2^k-1)})$, $t \le 2^k$, be vectorial bent for suitably chosen a_i, and let $G(x) = Tr_k^n(\alpha x^{2^k+1})$ be a vectorial Niho type bent function. Then,*

$$H(x) = F(x) + G(x) = Tr_k^n\Big(\sum_{i=1}^{t} a_i x^{i(2^k-1)} + \alpha x^{2^k+1}\Big),$$

is a vectorial semi-bent function. Furthermore, if

$$e = \max_{1 \le i < j \le k} \#\{\alpha \in \mathbb{F}_2^n : |\mathcal{F}(h_i + \varphi_\alpha)| = |\mathcal{F}(h_j + \varphi_\alpha)| = 2^{k+1}\},$$

then $\Delta_{h_i,h_j} \le 4e$ and $\sigma_{h_i,h_j} \le 16e2^n$, for $1 \le i < j \le k$.

Proof. We have to show that $Tr_1^k(\gamma H(x))$ is a Boolean semi-bent function for any $\gamma \in \mathbb{F}_{2^k}^*$, which is true since both $Tr_1^k(\gamma F(x))$ and $Tr_1^k(\gamma G(x))$ satisfy the conditions of Theorem 6.2.5. Then, any $\alpha \in \mathbb{F}_2^n$ such that $|\mathcal{F}(h_i + \varphi_\alpha)| = |\mathcal{F}(h_j + \varphi_\alpha)| = 2^{k+1} \neq 0$, $1 \le i < j \le k$, gives a nonzero value on the right hand side of the equation,

$$2^n[C_{h_i,h_j}(0), \ldots, C_{h_i,h_j}(2^n-1)] = [\mathcal{F}(h_i+\varphi_0)\mathcal{F}(h_j+\varphi_0), \ldots, \mathcal{F}(h_i+\varphi_{2^n-1})\mathcal{F}(h_j+\varphi_{2^n-1})]H_n,$$

which implies that $\max_\alpha |C_{h_i,h_j}(\alpha)| \leq e2^{n+2}2^{-n} = 4e$.

On the other hand, using the definition of e and defining

$$A = \{\alpha \in \mathbb{F}_2^n : |\mathcal{F}(h_i + \varphi_\alpha)| = |\mathcal{F}(h_j + \varphi_\alpha)| = 2^{k+1}\},$$

we have

$$\begin{aligned}
\sigma_{h_i,h_j} &= \frac{1}{2^n}\sum_{\alpha\in\mathbb{F}_2^n} \mathcal{F}^2(h_i+\varphi_\alpha)\mathcal{F}^2(h_j+\varphi_\alpha) \\
&= \frac{1}{2^n}\sum_{\alpha\in A} \mathcal{F}^2(h_i+\varphi_\alpha)\mathcal{F}^2(h_j+\varphi_\alpha) + \frac{1}{2^n}\sum_{\alpha\in\mathbb{F}_2^n\setminus A} \mathcal{F}^2(h_i+\varphi_\alpha)\mathcal{F}^2(h_j+\varphi_\alpha) \\
&\leq \frac{1}{2^n} e2^{n+2}2^{n+2} = 16e2^n.
\end{aligned}$$

■

The cross-correlation properties of this class have been checked by computer simulations. For instance, for the two vectorial semi-bent functions $H_1(x) = Tr_3^6(\gamma^6(x^7 + a^{21}x^{21} + \alpha^2 x^9))$ for $n = 6$, and $H_2(x) = Tr_4^8(\gamma(x^{225} + a^{184}x^{120} + a^{226}x^{90} + \alpha x^{17}))$ for $n = 8$, the following values of the absolute and the sum-of-squares indicator are obtained (cf. Table 6.1 and Table 6.2). Notice that for $n = 6$ each h_i is balanced function of degree 3 with algebraic immunity 3 and nonlinearity 24. The functions h_1 and h_2 have resiliency order 0, whereas h_3 has resiliency order 1. Similarly, for $n = 8$ each h_i is balanced function of degree 4 with algebraic immunity 4 and nonlinearity 112. The functions h_1, h_3 and h_4 have resiliency order 0, whereas h_2 has resiliency order 1.

Table 6.1: Vectorial semi-bent function $H_1(x)$

$H_1(x) = Tr_3^6(\gamma^6(x^7 + a^{21}x^{21} + \alpha^2 x^9)),\ \ n = 6, k = 3$			
e	$\Delta_{h_1,h_2}/\sigma_{h_1,h_2}$	$\Delta_{h_1,h_3}/\sigma_{h_1,h_3}$	$\Delta_{h_2,h_3}/\sigma_{h_2,h_3}$
6	$8/2^{11}$	$8/2^{11}$	$16/2^{12}$

Remark 6.2.7 *The values of the cross-correlation indicators for functions H_1 and H_2 in Table 6.1 and Table 6.2 have not been optimized, hence there might exist better choices for F and G in Theorem 6.2.6 providing even better values of σ_{h_i,h_j} and Δ_{h_i,h_j}. We leave the issue of finding these optimal choices of input instances as an interesting research problem.*

The cross-correlation properties of the semi-bent functions $H_1(x)$ and $H_2(x)$ can be compared to some known classes of functions with good propagation properties, which

Table 6.2: Vectorial semi-bent function $H_2(x)$

$H_2(x) = Tr_4^8(\gamma(x^{225} + a^{184}x^{120} + a^{226}x^{90} + \alpha x^{17}))$, $n = 8, k = 4$			
e	$\Delta_{h_1,h_2}/\sigma_{h_1,h_2}$	$\Delta_{h_1,h_3}/\sigma_{h_1,h_3}$	$\Delta_{h_1,h_4}/\sigma_{h_1,h_4}$
16	40/49152	40/65536	48/65536
e	$\Delta_{h_2,h_3}/\sigma_{h_2,h_3}$	$\Delta_{h_2,h_4}/\sigma_{h_2,h_4}$	$\Delta_{h_3,h_4}/\sigma_{h_3,h_4}$
16	40/57344	32/40960	40/49152

Table 6.3: Comparison of the cross-correlation indicators for different designs

Reference	n even	$\mathcal{N}_H$	Δ_{h_i,h_j}	σ_{h_i,h_j}
x^{-1}, Charpin *et al.* [28]	$n \geq 4$	$2^{n-1} - 2^{n/2}$	$2^{(n+2)/2}$	$2^{2n+1} + 2^{n+3}$
Zhou *et al.* [111]	$n \geq 6$	$2^{n-1} - 2^{n/2}$	2^{n-3}	2^{2n+2}
Bent S-box in Th. 6.2.3	$n \geq 6$	$2^{n-1} - 2^{n/2-1}$	$2^{n/2}$	2^{2n}
Semi-bent $H(x)$ in Th. 6.2.6	$n \geq 6$	$2^{n-1} - 2^{n/2}$	$\leq 4e$	$\leq 16e2^n$

is summarized in Table 6.3. Notice that Construction 1, proposed by Zhou *et al.* in [111], concerns the design of a single Boolean function. Thus, the values in the second row of Table 6.3 rather refer to autocorrelation properties, though an upper bound on $\sigma_{f,g}$ can be deduced using $0 \leq \sigma_{f,g} \leq \sqrt{\sigma_f \cdot \sigma_g}$. In the worst case, our sum-of-squares indicator attains the value $\sigma_{h_i,h_j} = 2^{2n}$ (cf. Table 6.1 and Table 6.2), which is better than the value $2^{2n+1} + 2^{n+3}$ of the inverse function. The results in [28], however, establish the autocorrelation properties of linear combinations of the component functions of x^{-1}, whereas in our case we consider pairwise cross-correlation properties of the component functions. On the other hand, the cross-correlation properties of the component functions of x^{-1} appear to be slightly worse compared to our vectorial semi-bent functions. Indeed, it may be checked that taking for instance $h_1(x) = Tr_1^n(\alpha x^{-1})$ and $h_2(x) = Tr_1^n(\alpha^2 x^{-1})$, where α is a primitive element in $\mathbb{F}_{2^n}$ (using the convention $0^{-1} = 0$), the values of the two indicators (for $n = 6, 8$) are given as in Table 6.4. Thus, σ_{h_1,h_2} is larger than the maximum value in Table 6.2, for $n = 8$.

Table 6.4: Cross-correlation properties of $h_1(x) = Tr_1^n(\alpha x^{-1}), h_2(x) = Tr_1^n(\alpha^2 x^{-1})$

Two component functions of x^{-1}	n	Δ_{h_1,h_2}	σ_{h_1,h_2}
$h_1(x), h_2(x)$	6	16	4096
	8	32	66560

6.3 Further design of S-boxes based on semi-bent functions

In difference to the previous section, where the design of vectorial mappings was based on the use of relative trace function, we attempt here to design the component functions individually. The exact analysis of the cryptographic criteria becomes rather difficult in this case and therefore we mostly rely on computer simulations performed for small sized S-boxes.

In a recent work [1], a generic method of constructing semi-bent functions was proposed. The result is strongly related to the properties of the first order derivatives of bent functions derived in [93].

Theorem 6.3.1 ([93]) *Let n be even, and suppose that f and g are two bent functions in $\mathfrak{B}_n$. If there exists an $a \in \mathbb{F}_2^n$ such that $D_a f(x) = D_a g(x) + 1$, then the function $h(x) = f(x) + g(x) + D_a f(x) + D_a fg(x)$ is a semi-bent function in $\mathfrak{B}_n$.*[2]

For convenience of the reader, we also give the proof of the result related to the construction of semi-bent functions in [1].

Theorem 6.3.2 ([1]) *Let n be even and $f \in \mathfrak{B}_n$ a bent function. Define $g(x) = f(x + a) + \alpha \cdot x$, where $\alpha \cdot a = 1$. Then,*

$$h(x) = f(x) + g(x) + D_a f(x) + D_a fg(x) \tag{6.4}$$

is a semi-bent function.

Proof. Obviously, g is also a bent function and $g(x + a) = f(x) + \alpha \cdot x + \alpha \cdot a$. Therefore,

$$\begin{aligned} D_a f(x) + D_a g(x) &= [f(x) + f(x + a)] + [g(x) + g(x + a)] \\ &= [g(x) + f(x + a)] + [f(x) + g(x + a)] \\ &= \alpha \cdot x + \alpha \cdot x + \alpha \cdot a = \alpha \cdot a = 1. \end{aligned}$$

By Theorem 6.3.1, $h(x) = f(x) + g(x) + D_a f(x) + D_a fg(x)$ is a semi-bent function. ■

This result enables us to construct, for even n, an infinite sequence of semi-bent functions from bent functions, thus there is a possibility of designing $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ in a similar manner.

Notice that the standard derivation rule for multiplication does not apply for our definition of derivatives. Indeed, the derivative $D_a fg(x) = f(x+a)g(x+a)+f(x)g(x)$

[2]For shortness we use the notation $D_a fg(x)$ to avoid more accurate but lengthy notation $D_a f(x)g(x)$, the former being especially preferred when f and g depend on more than one variable.

is different from $g(x)D_af(x)+f(x)D_ag(x) = f(x+a)g(x)+f(x)g(x+a)$. Furthermore, using the fact that $D_aD_af(x) = 0$ for any $f \in \mathfrak{B}_n$, we have $D_ah(x) = D_af(x) + D_ag(x) = \alpha \cdot a = 1$. Thus, the element a is always a linear structure of $h(x)$. Nevertheless, we show that (under certain conditions) a is the only linear structure of $h(x)$.

Theorem 6.3.3 *Let h be defined as in Theorem 6.3.2, and assume that a bent function $f \in \mathfrak{B}_n$ is such that $\deg(D_\beta f(x)) > 1$, for any $\beta \in \mathbb{F}_2^{n*}$. Then h has a single linear structure, that is, $D_\beta h(x) = h(x) + h(x+\beta)$ is a constant function only for $\beta = a$.*

Proof. By definition of f and g we have,

$$\begin{aligned} D_\beta f(x) + D_\beta g(x) &= [f(x) + f(x+\beta)] + [g(x) + g(x+\beta)] \\ &= [f(x) + f(x+\beta)] + [f(x+a) + \alpha \cdot x + f(x+a+\beta) + \alpha \cdot (x+\beta)] \\ &= D_\beta D_a f(x) + \alpha \cdot \beta, \end{aligned}$$

where $D_\beta D_a f(x) = f(x) + f(x+a) + f(x+\beta) + f(x+a+\beta)$, and therefore

$$D_\beta h(x) = D_\beta D_a f(x) + \alpha \cdot \beta + D_\beta D_a f(x) + D_\beta D_a fg(x) = D_\beta D_a fg(x) + \alpha \cdot \beta.$$

Hence, $D_\beta h(x)$ is constant if and only if $D_\beta D_a fg(x)$ is constant. But,

$$\begin{aligned} D_\beta D_a fg(x) &= D_\beta[f(x+a)g(x+a) + f(x)g(x)] \\ &= D_\beta[f(x+a)(f(x) + \alpha \cdot (x+a)) + f(x)(f(x+a) + \alpha \cdot x)] \\ &= D_\beta[(f(x+a) + f(x))(\alpha \cdot x) + f(x+a)(\alpha \cdot a)] \\ &= D_\beta[(f(x+a) + f(x))(\alpha \cdot x) + f(x+a)] \\ &= (\alpha \cdot x) D_\beta D_a f(x) + (\alpha \cdot \beta)(f(x+\beta) + f(x+a+\beta)) \\ &\quad + f(x+a) + f(x+a+\beta). \end{aligned}$$

Thus, if $\alpha \cdot \beta = 0$, then $D_\beta h(x)$ is constant if and only if

$$(\alpha \cdot x) D_\beta D_a f(x) = f(x+a) + f(x+a+\beta),$$

i.e.,

$$\begin{aligned} (\alpha \cdot x)[f(x) + f(x+a) + f(x+\beta) + f(x+a+\beta)] &= f(x+a) + f(x+a+\beta) \\ (\alpha \cdot x + 1)[f(x+a) + f(x+a+\beta)] + (\alpha \cdot x)[f(x) + f(x+\beta)] &= 0 \\ (\alpha \cdot x + 1) D_\beta f(x+a) + (\alpha \cdot x) D_\beta f(x) &= 0 \\ (\alpha \cdot x) D_\beta f(x+a) + (\alpha \cdot x) D_\beta f(x) + D_\beta f(x+a) &= 0 \end{aligned}$$

There are four possible cases:

1. $(\alpha \cdot x) D_\beta f(x+a) = (\alpha \cdot x) D_\beta f(x) = D_\beta f(x+a) = 0$, i.e.,
   $D_\beta f(x+a) = 0 \Leftrightarrow f(x+a) = f(x+a+\beta) \Rightarrow \beta = 0$. A contradiction.

2. $(\alpha \cdot x)D_\beta f(x+a) = (\alpha \cdot x)D_\beta f(x) = 1 \ \wedge \ D_\beta f(x+a) = 0$, i.e., $D_\beta f(x+a) = 0 \Rightarrow \beta = 0$. A contradiction.

3. $(\alpha \cdot x)D_\beta f(x+a) = 0 \ \wedge \ (\alpha \cdot x)D_\beta f(x) = D_\beta f(x+a) = 1$, i.e., $D_\beta f(x+a) = 0 \Rightarrow \beta = 0$. A contradiction.

4. $(\alpha \cdot x)D_\beta f(x+a) = D_\beta f(x+a) = 1 \ \wedge \ (\alpha \cdot x)D_\beta f(x) = 0$, i.e., $D_\beta f(x) = 0 \Rightarrow \beta = 0$. A contradiction.

On the other hand, if $\alpha \cdot \beta = 1$, then $D_\beta h(x)$ is constant if and only if

$$(\alpha \cdot x)D_\beta D_a f(x) = f(x+a) + f(x+\beta),$$

i.e.,

$$(\alpha \cdot x)[f(x) + f(x+a) + f(x+\beta) + f(x+a+\beta)] = f(x+a) + f(x+\beta),$$

so that

$$(\alpha \cdot x + 1)[f(x+a) + f(x+\beta)] + (\alpha \cdot x)[f(x) + f(x+a+\beta)] = 0.$$

It is obvious that $f(x+a) = f(x+\beta)$ is equivalent to $f(x) = f(x+a+\beta)$. Thus, the above equation is constant (for all $x \in \mathbb{F}_2^n$) if and only if $f(x+a) = f(x+\beta)$, which implies that $a = \beta$. The sufficiency of this condition is obvious. For the necessity, we first observe that for $a \neq \beta$ the functions $f(x+a)+f(x+\beta)$ and $f(x)+f(x+a+\beta)$, being derivatives of a bent function f, are both nonconstant (and more precisely balanced functions). Then, assuming that

$$D_\beta D_a f(x) = f(x+a) + f(x+\beta) + f(x) + f(x+a+\beta) = 0,$$

would imply that $f(x+a)+f(x+\beta)$ is constant, a contradiction. On the other hand, the function $(\alpha \cdot x)D_\beta D_a f(x)$ cannot be balanced, unless $D_\beta D_a f(x) = \alpha \cdot x$. Due to the assumption that $\deg(f(x+a)+f(x+\beta)) > 1$ and therefore cannot be equal to $\alpha \cdot x$. ■

Remark 6.3.4 *The condition in Theorem 6.3.3 that* $\deg(D_\beta f(x)) > 1$ *is sufficient but may not be necessary.*

Remark 6.3.5 *An analysis of other cryptographic criteria appears to be difficult due to the dependency of* h *on the choice of a bent function* f *and the use of the derivative* $D_a fg(x)$ *in its definition, which is illustrated in Example 6.3.1 for the simplest case when* f *is a quadratic bent function in the Maiorana-McFarland class.*

Example 6.3.1 *Let* n *be even and* $f(x,y) = x \cdot y$, *where* $x, y \in \mathbb{F}_2^k$. *Thus,* f *is a bent function and belongs to the Maiorana-McFarland class. Then, defining* $g(x,y) =$

$f(x+a, y+b)+(\alpha,\beta)\cdot(x,y)$ for a nonzero $(a,b)\in\mathbb{F}_2^k\times\mathbb{F}_2^k$ such that $(\alpha,\beta)\cdot(a,b)=1$ we have

$$g(x,y)=x\cdot y+(\alpha+b)\cdot x+(a+\beta)\cdot y+a\cdot b,$$

which is clearly a bent function obtained by adding an affine function to f. Similarly, $D_{(a,b)}f(x,y)=x\cdot b+a\cdot y+a\cdot b$, so that

$$f(x,y)+g(x,y)+D_{(a,b)}f(x,y)=\alpha\cdot x+\beta\cdot y.$$

Then, using the idempotent property of Boolean ring,

$$\begin{aligned} fg(x,y) &= [x\cdot y][x\cdot y+(\alpha+b)\cdot x+(a+\beta)\cdot y+a\cdot b] \\ &= (1+a\cdot b)(x\cdot y)+[(\alpha+b)\cdot x+(a+\beta)\cdot y](x\cdot y). \end{aligned}$$

Note that the first term is a quadratic function and the second term is cubic. After some simplifications we have

$$\begin{aligned} D_{(a,b)}fg(x,y) &= x\cdot y+(b\cdot x+a\cdot y+a\cdot b)\cdot(1+a\cdot b+\alpha\cdot x+\alpha\cdot a+b\cdot x+a\cdot b \\ &\quad +a\cdot y+a\cdot b+\beta\cdot y+\beta\cdot b) \\ &= x\cdot y+(b\cdot x+a\cdot y+a\cdot b)\cdot(\alpha\cdot x+b\cdot x+a\cdot y+\beta\cdot y+a\cdot b+\beta\cdot b) \\ &= x\cdot y+(b\cdot x+a\cdot y+a\cdot b)\cdot((\alpha+b)\cdot x+(\beta+a)\cdot y+a\cdot b+\beta\cdot b). \end{aligned}$$

Finally,

$$\begin{aligned} h(x,y) &= f(x,y)+g(x,y)+D_af(x,y)+D_afg(x,y) \\ &= x\cdot y+(\alpha\cdot x+\beta\cdot y)\cdot(b\cdot x+a\cdot y+a\cdot b+1) \\ &\quad +(b\cdot x+a\cdot y+a\cdot b)\cdot(1+\beta\cdot b). \end{aligned}$$

The existence of a single linear structure a does not exclude the possibility of designing semi-bent functions with good propagation and cross-correlation properties. Indeed, since the only condition in Theorem 6.3.2, imposed on function g, is that $\alpha\cdot a=1$, we can select a to have the highest possible Hamming weight $wt(a)=n$ thus allowing h to possibly satisfy PC of high order.

Theorem 6.3.6 *Let n be even and $f\in\mathfrak{B}_n$ a bent function. Define $g_i(x)=f(x+a)+\alpha^{(i)}\cdot x$, where $a,\alpha\in\mathbb{F}_2^n$ are given by $a=(1,1,\ldots,1)$ and $\alpha^{(i)}=(0,\ldots,1,\ldots,0)$ so that $\alpha_j^{(i)}=0$ for $j\neq i$, $1\leq i\leq n$ (the only nonzero value of $\alpha^{(i)}$ is at the i-th position). Then,*

$$h_i(x)=f(x)+g_i(x)+D_af(x)+D_afg_i(x) \tag{6.5}$$

are semi-bent functions for $1\leq i\leq n$, having a single linear structure at $a=(1,1,\ldots,1)$.

PROOF. Clearly, $\alpha^{(i)} \cdot a = 1$ for all $1 \leq i \leq n$, thus, by Theorem 6.3.2, $h_i(x)$ is a semi-bent function. The existence of a single linear structure at a, for any h_i, follows from Theorem 6.3.3. ∎

Example 6.3.2 *Let us again consider the function $h(x, y)$ in Example 6.3.1 in view of the above result. Using the same notation as in Theorem 6.3.6, in the context of Example 6.3.1, we have that $(a, b) \in \mathbb{F}_2^k \times \mathbb{F}_2^k$ is given as $(a, b) = (1, \ldots, 1)$. Furthermore, for $\alpha^{(i)}, \beta^{(i)} \in \mathbb{F}_2^k$ we can define,*

$$h_i(x,y) = x \cdot y + (\alpha^{(i)} \cdot x + \beta^{(i)} \cdot y) \cdot (b \cdot x + a \cdot y + a \cdot b + 1) + (b \cdot x + a \cdot y + a \cdot b) \cdot (1 + \beta^{(i)} \cdot b),$$

where

$$\alpha_j^{(i)} = 1 \Leftrightarrow j = i \text{ and } 1 \leq i \leq k,$$

$$\beta_j^{(i)} = 1 \Leftrightarrow j = i \text{ and } k+1 \leq i \leq n.$$

For instance, assuming that k is even we get,

$$h_1(x,y) = x \cdot y + x_1(x_1 + \ldots + x_k + y_1 + \ldots + y_k + 1) + x_1 + \ldots + x_k + y_1 + \ldots + y_k,$$

which is a semi-bent function. In the same way h_i can be computed for all $1 \leq i \leq n$.

Nevertheless, the main problem with this approach is a lack of understanding of the cryptographic properties of linear combinations of these functions and their cross-correlation properties. For instance, even though we know that the nonlinearity of any h_i is given by $\mathcal{N}_{h_i} = 2^{n-1} - 2^{n/2}$, it is hard to estimate the nonlinearity of their linear combinations.

In the following table the properties of the cross-correlation for semi-bent functions of the form $h_i(x, y), h_j(x, y), 1 \leq i \neq j \leq n$, as in Example 6.3.1, are derived. Notice that all semi-bent functions $h_i(x, y)$ in Table 6.5 are quadratic.

Table 6.5: Semi-bent functions $h_i(x, y)$ as in Example 6.3.1

n even	Δ_{h_i}	σ_{h_i}	$\Delta_{h_i,h_j(j\neq i)}$	$\sigma_{h_i,h_j(j\neq i)}$
6	2^6	2^{14}	2^5	2^{13}
8	2^8	2^{18}	2^7	2^{17}

The nonlinearity of the functions $h_i + h_j$ is $\mathcal{N}_{h_i+h_j(j\neq i)} = 2^{n-1} - 2^{n/2+1}$, while the nonlinearity of the functions $h_i + h_j + h_k$ is $\mathcal{N}_{h_i+h_j+h_k(i\neq j, i\neq k, j\neq k)} = 2^{n-1} - 2^{n/2}$ (which means that $h_i + h_j + h_k$ is a semi-bent function again). Most notably, the linear combinations consisting of an odd number of h_i result in functions which are semi-bent again, whereas for an even number of h_i the nonlinearity appears to be

$2^{n-1} - 2^{n/2+1}$. Notice that in Example 6.3.2 the function $f(x, y) = x \cdot y$ is quadratic and its derivative is an affine function. Therefore, the condition of Theorem 6.3.3 is not satisfied and h_i can have more than one linear structure. It was also confirmed by computer simulations and the dimension of the space of linear structures of h_i in Example 6.3.2 equals to two. That is, four different linear structures could be found including the all zero vector being a trivial linear structure.

We leave the analysis of cryptographic properties (including the cross-correlation properties) of this class of functions as an interesting research problem. The cross-correlation and nonlinearity values of these functions as given above may be somehow misleading due to the choice of quadratic bent functions in the analysis. Therefore, it might be of interest to investigate the propagation properties of nonquadratic bent functions in the Maiorana-McFarland class.

Chapter 7

Conclusions

Science never solves a problem
without creating ten more.
– G. B. Shaw

The major part of this thesis deals with the possibilities of obtaining vectorial bent functions for both binary and nonbinary alphabets. The necessary and sufficient conditions for certain classes of these functions, represented in a multiple trace form, are derived. These results enabled an explicit specification of the coefficients of $Tr_k^{2k}(\sum_{i=0}^{2^k} a_i x^{i(2^k-1)})$ and the exact number of vectorial bent functions in this form [76]. Since for nonbinary alphabet bent functions are closely related to the concept of planar mappings, our results contain a construction method for vectorial (generalized) bent functions in dimension $n/2$ though planar mappings induce vectorial (generalized) bent functions of maximum dimension n. This important problem is left open.

The PhD Thesis contains several different methods for constructing infinite sequences of disjoint spectra, optimal plateaued and semi-bent functions. In particular, the design of vectorial semi-bent functions by combining suitable vectorial bent functions from the partial spread and Niho class is given. The approaches taken here can be further optimized with respect to the propagation properties of obtained S-boxes through a careful selection of the input functions. This problem is however left as an interesting research topic.

Bibliography

[1] S. Bajrić, S. Gangopadhyay, E. Pasalic, and W. Zhang. Designing semi-bent, disjoint spectra and optimal plateaued functions. *Submitted manuscript,* 2014.

[2] S. Bajrić, E. Pasalic, A. Ribić-Muratović, and S. Gangopadhyay. On generalized bent functions with Dillons exponents. *Information Processing Letters*, vol. 114, no. 4, pp. 222–227, 2014.

[3] E. R. Berlekamp and L. R. Welch. Weight distributions of the cosets of the $(32, 6)$ Reed–Muller code. *IEEE Trans. on Inform. Theory*, vol. 18, no. 1, pp. 203–207, 1972.

[4] A. Bernasconi and B. Codenotti Spectral Analysis of Boolean Functions as a Graph Eigenvalue Problem. *IEEE Trans. on Inform. Theory*, vol. 48, no. 3, pp. 345–351, 1999.

[5] A. Bernasconi, B. Codenotti and J. VanderKam A Characterization of Bent Functions in Terms of Strongly Regular Graphs. *IEEE Trans. on Inform. Theory*, vol. 50, no. 9, pp. 984–985, 2001.

[6] E. Biham and A. Shamir. Differential cryptanalysis of the Data Encryption Standard. Springer–Verlag, New York, 1993.

[7] A. Canteaut, C. Carlet, P. Charpin, and C. Fontaine. On cryptographic properties of the cosets of $R(1, m)$. *IEEE Trans. on Inform. Theory*, vol. 47, no. 4, pp. 1494–1513, 2001.

[8] A. Canteaut and P. Charpin. Decomposing bent functions. *IEEE Trans. on Inform. Theory*, vol. 49, no. 8, pp. 2004–2018, 2003.

[9] A. Canteaut, P. Charpin, and G. Kyureghyan. A new class of monomial bent functions. *Finite Fields and Their Applications*, vol. 14, no. 1, pp. 221–241, 2008.

[10] T. M. Cover and J. A. Thomas. Elements of information theory. John Wiley and Sons, New York, 1991.

[11] A. Canteaut, M. Daum, H. Dobbertin, and G. Leander. Normal and non normal bent functions. In *Discrete Applied Mathematics*, vol. 156, no. 2, pp. 202–218, 2003.

[12] A. Canteaut, M. Daum, H. Dobbertin, and G. Leander. Finding nonnormal bent functions. *Discrete Applied Mathematics*, vol. 156, no. 2, pp. 202–218, 2006.

[13] A. Canteaut and M. Trabbia. Improved fast correlation attacks using parity-check equations of weight 4 and 5. In *Advances in Cryptology—EUROCRYPT 2000*, vol. LNCS 1807, pp. 573–588. Springer–Verlag, 2000.

[14] C. Carlet. A larger class of cryptographic Boolean functions via a study of the Maiorana-McFarland constructions. In *Advances in Cryptology—CRYPTO 2002*, LNCS 2442, pp. 549–564. Springer–Verlag, 2002.

[15] C. Carlet. Boolean functions for cryptography and error correcting codes. Cambridge University Press, 2010.

[16] C. Carlet. On the coset weight divisibility and nonlinearity of resilient and correlation-immune functions. *Discrete Mathematics and Theoretical Computer Science*, 2001.

[17] C. Carlet. On the secondary constructions of resilient and bent functions. In *Coding, Cryptogrpahy and Combinatorics, Progr. Comput. Sci. Appl. Logic*, vol. 23, pp. 3–28. Birkahauser Verlag, Basel, 2004.

[18] C. Carlet. Partially-bent functions. *Designs, Codes and Cryptography*, vol. 3, pp. 135–145, 1993.

[19] C. Carlet. Two new classes of bent functions. In *Advances in Cryptology—EUROCRYPT'93*, vol. LNCS 765, pp. 77–101, Springer–Verlag, 1993.

[20] C. Carlet, P. Charpin, and V. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Designs, Codes and Cryptography*, vol. 15, no. 2, pp. 125–156, 1998.

[21] C. Carlet and P. Gabborit. Hyperbent functions and cyclic codes. *Journal of Combinatorial Theory, Series A*, vol. 113, no. 3, pp. 466–482, 2006.

[22] C. Carlet and S. Mesnager. On semibent Boolean functions. *IEEE Trans. on Inform. Theory*, vol. 58, no. 5, pp. 3287–3292, 2012.

[23] C. Carlet and S. Mesnager. On Dillon's class H of Niho bent functions and o-polynomials. In *In International Symposium on Artificial Intelligence and Mathematics,*, ISAIM, 2012.

[24] C. Carlet and P. Sarkar. Spectral domain analysis of correlation immune and resilient Boolean functions. *Finite Fields and Their Applications*, vol. 8, no. 1, pp. 120–130, 2002.

[25] P. Charpin and G. Gong. Hyperbent functions, Kloosterman sums and Dickson polynomials. *IEEE Trans. on Inform. Theory*, vol. 54, no. 9, pp. 4230–4238, 2008.

[26] P. Charpin and G. Kyureghyan. Cubic monomial bent functions: a subclass of $\mathcal{M}$. *SIAM Journal of Discrete Math.*, vol. 22, no. 2, pp. 650–665, 2008.

[27] P. Charpin, E. Pasalic, and C. Tavernier. On bent and semi–bent quadratic Boolean functions. *IEEE Trans. on Inform. Theory*, vol. 51, no. 12, pp. 4286–4298, 2005.

[28] P. Charpin, T. Helleseth, and V. Zinoviev. Propagation characteristics of $x \mapsto x^{-1}$ and Kloosterman sums. *Finite Fields and Their Applications*, vol. 13, no. 2, pp. 366–381, 2007.

[29] S. Chee, S. Lee, and K. Kim. On semi bent functions. In *Advances in Cryptology–ASIACRYPT 1994*, vol. LNCS 917, pp. 107–118. Springer–Verlag, 1995.

[30] S. Chee, S. Lee, D. Lee, and H. S. Sung. On the correlation immune functions and their nonlinearity. In *Advances in Cryptology–ASIACRYPT'96*, vol. LNCS 1163, pp. 232–243. Springer–Verlag, 1996.

[31] D. A. Cox. Why Eisenstein proved the Eisenstein criterion and why Schnemann discovered it first. *Amer. Math. Mon.*, vol. 118, no. 1, pp. 3–21, 2011.

[32] T. W. Cusick and P. Stanica. *Cryptographic Boolean Functions and Applications*. Academic Press, 1st edition, 2009.

[33] D.K. Dalai, K.C. Gupta, and S. Maitra. Results on algebraic immunity of cryptographically signifficant Boolean functions. In *Advances in Cryptology–INDOCRYPT 2004*, vol. LNCS 3348, pp. 92–106. Springer–Verlag, 2004.

[34] P. Dembowski and T. G. Ostrom. Planes of order n with collineation groups of order n^2. *Mathematische Zeitschrift*, vol. 103, no. 3, pp. 239–258, 1968.

[35] U. Dempwolff. Automorphisms and Equivalence of Bent Functions and of Difference Sets in Elementary Abelian 2-Groups. *Comunications in Algebra*, vol.34, pp. 1077–1131, 2006.

[36] J. F. Dillon. Elementary Haddamard Difference Sets. Ph. D. thesis, University of Maryland, U.S.A., 1974.

[37] J.F. Dillon. Elementary Hadamard Difference Sets. *In proceedings of 6th S. E. Conference of Combinatorics, Graph Theory, and Computing*, pp. 65–76. Utility Mathematics, Winnipeg,1975.

[38] J. Dillon and H. Dobbertin. New cyclic difference sets with singer parameters. *Finite Fields and Their Applications*, vol. 10, no. 3, pp. 342–389, 2004.

[39] H. Dobbertin, G. Leander, A. Canteaut, C. Carlet, P. Felke, and P. Gaborit. Construction of bent functions via Niho power functions. *Journal of Combinatorial Theory, Series A*, vol. 113, pp. 779–798, 2006.

[40] K Feng and J Yang. Vectorial Boolean functions with good cryptographic properties. *Int. J. Found. Comput. Sci.*, vol. 22, no. 6, pp. 1271–1282, 2011.

[41] J. B. Fraleigh. *A first course in abstract algebra.* Addison Wesley, 7th edition, 2002.

[42] S. Gangopadhyay. Affine inequivalence of cubic Maiorana–McFarland type bent functions, *Discrete Applied Mathematics*, vol. 161, no. 7–8, pp. 1141–1146, 2013.

[43] S. Gao, W. Ma, Y. Zhao, and Z. Zhuo. Walsh spectrum of cryptographically concatenating functions and its applications in constructing resilient Boolean functions. *Journal of Computational Information Systems*, vol. 7, no. 4, pp. 1074–1081, 2011.

[44] S. Gao, W. Ma, Z. Zhuo and F. Wang. On cross-correlation indicators of an S-box. *Frontiers of Computer Science in China*, vol. 5, no. 4, pp. 448–453. Springer Verlag, 2011.

[45] S. W. Golomb and G. Gong. Signal design for good correlation: for wireless communication, cryptography and radar. Cambridge University Press, 2005.

[46] T. Helleseth and A. Kholosha. New binomial bent functions over the finite fields of odd characteristic. *IEEE Trans. on Inform. Theory*, vol. 56, no. 9, pp. 4646–4652, 2010.

[47] F. H. Hunt, and D. H. Smith. The Construction of orthogonal variable spreading factor codes from semi-bent functions. *IEEE Transactions on Wireless Communications*, vol. 11, no. 8, pp. 2970–2975, 2012.

[48] J. Y. Hyun, H. Lee, and Y. Lee. Nonexistence of certain types of plateaued functions. *Discrete Applied Mathematics*, vol. 161, no. 16–17, pp. 2745–2748, 2013.

[49] T. Jakobsen and L. R. Knudsen. The interpolation attack on block ciphers. In *Fast Software Encryption'97*, vol. LNCS 1267, pp. 28–40. Springer–verlag, 1997.

[50] S. Kavut and M. D. Yücel. 9-variable Boolean functions with nonlinearity 242 in the generalized rotation symmetric class. *Information and Computing*, vol. 208, no. 4, pp. 341–350, 2010.

[51] S. Kavut, M. D. Yücel, and S. Maitra. Construction of resilient functions by the concatenation of Boolean functions having nonintersecting Walsh spectra. In *Proc. of Third International Workshop on Boolean Functions: Cryptography and Applications, BFCA '07*, pp. 43–62. Paris, France, 2–3 May, 2007.

[52] A. Khalyavin. The constructing of 3–resilient Boolean functions of 9 variables with nonlinearity 240. Cryptology ePrint Archive, 2007/212. Available at `http://eprint.iacr.org/`.

[53] L. R. Knudsen. Truncated and higher order differentials. In *Fast Software Encryption'95*, vol. LNCS 1008, pp. 196–211. Springer–Verlag, 1995.

[54] P. V. Kumar, R. A. Scholtz, and L. R. Welch. Generalized bent functions and their properties. *Journal of Combinatorial Theory, Series A*, vol. 40, no. 1, pp. 90–107, 1985.

[55] S. K. Langford and M. E. Hellman. Differential-linear cryptanalysis. In *Advances in Cryptology—CRYPTO'94*, vol. LNCS 839, pp. 17–25. Springer.-Verlag, 1994.

[56] N. G. Leander. Monomial bent functions. *IEEE Trans. on Inform. Theory*, vol. 52, no. 2, pp. 738–743, 2006.

[57] N. G. Leander and A. Kholosha. Bent functions with 2^r Niho exponents. *IEEE Trans. on Inform. Theory*, vol. 52, no. 12, pp. 5529–5532, 2006.

[58] N. Li, T. Helleseth, X. Tang, and A. Kholosha. Several new classes of bent functions from Dillon exponents. *IEEE Trans. on Inform. Theory*, vol. 59, no. 3, pp. 1818–1831, 2013.

[59] R. Lidl and R. E. Niederreiter. *Finite fields.* Cambridge University Press, Second Edition, 1997.

[60] S. L. Ma. A survey of partial difference sets. *Designs, Codes and Cryptography*, vol. 4, pp. 221–261, 1994.

[61] , R. L. McFarland A family of difference sets in non-cyclic groups, *Journal of Combinatorial Theory, Series A*, vol. 15, no. 1, pp. 1–10, 1973.

[62] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes.* North–Holland, Amsterdam, 1977.

[63] M. Matsui. Linear cryptanalysis method for DES cipher. In *Advances in Cryptology—EUROCRYPT'93*, vol. LNCS 765, pp. 386–397. Springer–Verlag, 1993.

[64] B. Mann. Difference sets in elementary Abelian groups. *Ill. J. Math.*, vol.9, pp. 212–219, 1965.

[65] S. Maitra and E. Pasalic. Further constructions of resilient Boolean functions with very high nonlinearity. *IEEE Trans. on Inform. Theory*, vol. 48, no. 7, pp. 1825–1834, 2002.

[66] R. L. McFarland. A family of difference sets in non-cyclic groups. *Journal of Combinatorial Theory, Series A*, vol. 15, no. 1, pp. 1–10, 1973.

[67] W. Meidl and A. Topuzoğlu. Quadratic functions with prescribed spectra. *Designes, Codes and Cryptography*, vol. 66, no. 1–3, pp. 257–273, 2013.

[68] W. Meier, E. Pasalic, and C. Carlet. Algebraic attacks and decomposition of Boolean functions. In *Advances in Cryptology–EUROCRYPT 2004*, vol. LNCS 3027, pp. 474–491. Springer–Verlag, 2004.

[69] W. Meier and O. Staffelbach. Correlation properties of combiners with memory in stream ciphers. In *Journal of Cryptology*, vol. 5, no. 1, pp. 67–86. Springer–Verlag, 1992.

[70] A. Menezes, P. van Oorschot, and S. Vanstone. *Handbook of Applied Cryptography*. CRC Press, Boca Raton, 1997.

[71] S. Mesnager. A new class of bent and hyper-bent functions in polynomial form and their link with some exponential sums and dickson polynomials. *IEEE Trans. on Inform. Theory*, vol. 57, no. 9, pp. 5996–6009, 2011.

[72] S. Mesnager. Semibent functions from Dillon and Niho exponents, Kloosterman sums, and Dickson polynomials. *IEEE Trans. on Inform. Theory*, vol. 57, no. 11, pp. 7443–7458, 2011.

[73] S. Mesnager. Semi-bent functions from oval polynomials. In *14th IMA Conference on Cryptography and Coding*, vol. LNCS 8308, pp. 1–15. Springer–Verlag, 2013.

[74] S. Mesnager. Semi-bent functions with multiple trace terms and hyperelliptic curves. In *Progress in Cryptology–LATINCRYPT 2012*, vol. LNCS 7533, pp. 18–36. Springer–Verlag, 2012.

[75] A. Muratović-Ribić, E. Pasalic, and S. Bajrić. Vectorial bent functions from multiple terms trace functions. *IEEE Transaction on Information Theory,* vol. 60, no. 2, pp. 1337–1347, 2014.

[76] A. Muratović-Ribić, E. Pasalic, and S. Ribić. Vectorial hyperbent trace functions from the $\mathcal{PS}_ap$ class - their exact number and specification. *Submitted manuscript,* 2014.

[77] K. Nyberg. Perfect nonlinear S-boxes. In *Advances in Cryptology—EUROCRYPT'91*, vol. LNCS 547, pp. 378–385, Springer-Verlag, 1991.

[78] E. Pasalic. Degree optimized resilient Boolean functions from Maiorana–McFarland class. In *9th IMA Conference on Cryptography and Coding*, vol. LNCS 2898, pp. 195–114. Springer–Verlag, 2003.

[79] E. Pasalic. On algebraic immunity of Maiorana-McFarland like functions and applications of algebraic attacks in attacking some stream cipher schemes. Presented at Symmetric-Key Encryption Workshop, Aarhus, Denmark, May 26-27, 2005.

[80] E. Pasalic and W. G. Zhang. On multiple output bent functions. *Information Processing Letters*, vol. 112, no. 21, pp. 811–815, 2012.

[81] E. Pasalic, S. Bajrić and M. Djordjević. On cross-correlation properties of S-boxes and their design using semi-bent functions. *Security and Communication Networks*. In Press. `http://dx.doi.org/10.1002/sec.1035`.

[82] E. Pasalic, T. Johansson, S. Maitra, and P. Sarkar. New constructions of resilient and correlation immune Boolean functions achieving upper bounds on nonlinearity. In *Workshop on Coding and Cryptography Proceedings*, vol. 6, pp. 425–435. Elsevier Science, 2001.

[83] A. Pott, P. V. Kumar, T. Helleseth and D. Jugnickel. Difference Sets, Sequences and their Correlation Properties. *In Proceedings of the NATO Advanced Study Institute*, vol. 542, 1998.

[84] B. Preneel, W.V. Leekwijck, L.V. Linden, R. Govaerts, and J. Vandewalle. Propagation characteristics of Boolean functions. In *Advances in Cryptology—EUROCRYPT'90*, vol. LNCS 437, pp. 155–165. Springer–Verlag, 1991.

[85] O. S. Rothaus. On bent functions. *Journal of Combinatorial Theory, Series A*, vol. 20, pp. 300–305, 1976.

[86] Z. Saber, M. Faisal Uddin, and A. Youssef. On the existence of (9,3,5,240) resilient functions. *IEEE Trans. on Inform. Theory*, vol. 52, no. 5, pp. 2269–2270, 2006.

[87] P. Sarkar and S. Maitra. Construction of nonlinear Boolean functions with important cryptographic properties. In *Advances in Cryptology–EUROCRYPT 2000*, vol. LNCS 1807, pp. 485-506. Springer–Verlag, 2000.

[88] S. Sarkar and S. Maitra. Cross-correlation analysis of cryptographically useful Boolean functions and S–boxes. *Theory of Computing Systems*, vol. 35, no. 1, pp. 39–57, 2002.

[89] P. Sarkar and S. Maitra. Nonlinearity bounds and constructions of resilient Boolean functions. In *Advances in Cryptology—CRYPTO 2000*, LNCS 1880, pp. 515–532. Springer-Verlag, 2000.

[90] C. E. Shannon. Communication theory of secrecy systems. *Bell system technical journal*, vol. 28, pp. 656–715, 1949.

[91] T. Siegenthaler. Correlation–immunity of nonlinear combining functions for cryptographic applications. *IEEE Trans. on Inform. Theory*, vol. 30, pp. 776–780, 1984.

[92] D. R. Stinson. *Cryptography: Theory and Practice*. CRC Press, Boca Raton, 3rd edition, 2006.

[93] G. Sun and C. Wu. Construction of semi–bent Boolean functions in even number of variables. *Chinese Journal of Electronics*, vol. 18, no. 2, pp. 231–237, 2009.

[94] Y. Tan, A. Pott and T. Feng. Strongly regular graphs associated with ternary bent functions. *Journal of Comb. Theory, Series A*, vol. 117, no. 6, pp. 668–682, 2010.

[95] C. Tang, Y. Qi, M. Xu, B. Wang, and Y. Yang. A new class of hyper-bent Boolean functions in binomial forms. *arXiv*: 1112.0062v1 [cs.IT], 1 Dec. 2011.

[96] Y. Tarannikov. New constructions of resilient Boolean functions with maximal nonlinearity. In *Fast Software Encryption 2001*, vol. LNCS 2355, pp. 66–77. Springer–Verlag, 2001.

[97] Y. Tarannikov. On resilient Boolean functions with maximal possible nonlinearity. In *Proceedings of Indocrypt*, LNCS 1977, pp. 19–30. Springer–Verlag, 2000.

[98] A.F. Webster and S.E. Tavares. On the design of S–boxes. In *Advances in Cryptology—CRYPTO'85*, vol. LNCS 219, pp. 523–534. Springer–Verlag, 1985.

[99] J. Wolfmann. Special bent and near-bent functions. *Advances in Mathematics of Communications*, vol. 8, no. 1, pp. 21–33, 2014.

[100] J. Wu, Y. Wei, and X. Wang. An optimized method for multiple output bent functions. *Acta Electronica Sinica*, vol. 33, no. 3, pp. 521–523, 2005.

[101] G. Xu and X. Cao. A new class of ternary bent functions in binomial forms. *Journal of Information & Computational Science*, vol. 9, no. 16, pp. 4785–4792, 2012.

[102] A. M. Youssef and G. Gong. Hyper-bent functions. In *Advances in Cryptology—EUROCRYPT 2001*, vol. LNCS 2045, pp. 406–419, Springer-Verlag, 2001.

[103] W. Zhang, and E. Pasalic. Generalized Maiorana–McFarland construction of resilient Boolean functions with high nonlinearity and good algebraic properties. *Submitted manuscript*, 2013.

[104] X.-M. Zhang and Y. Zheng. GAC — the criterion for global avalanche characteristics of cryptographic functions. *Journal of Universal Computer Science*, vol. 1, no. 5, pp. 320–337, 1995.

[105] D. Zheng, X. Zeng, and L. Hu. A family of p-ary binomial bent functions. Cryptology ePrint Archive, 2009/563. Available at `http://eprint.iacr.org/`.

[106] Y. Zheng and X. M. Zhang. Improving upper bound on nonlinearity of high order correlation immune functions. In *Selected Areas in Cryptography–SAC'2000*, vol. LNCS 2012, pp. 264–274. Springer–Verlag, 2000.

[107] Y. Zheng and X. M. Zhang. Relationships between bent functions and complementary plateaued functions. In *Information Security and Cryptology, ICISC'99*, vol. LNCS 1787, pp. 60–75, 2000.

[108] Y. Zheng and X. M. Zhang. Plateaued functions. In *Proc. Int. Conf. Inf. Commun. Signal Process.*, vol. LNCS 1726, pp. 284-300, 1999.

[109] Y. Zhou. On the distribution of auto-correlation value of balanced Boolean functions. *Advances in Mathematics of Communications*, vol. 7, no. 3, pp. 335–347, 2013.

[110] Y. Zhou, M. Xie and G. Z. Xiao. On the global avalanche characteristics between two Boolean functions and the higher order nonlinearity. *Information Sciences*, vol. 180, no. 2, pp. 256–265, 2010.

[111] Y. Zhou, X. Dong, W. Zhang and B. Zeng. New bounds on the sum–of–squares indicator. *7th International Conference on Communications and Networking, CHINACOM–2012*, pp. 173–178, 2012.

[112] Y. Zhou, W. Zhang, S. Zhu, and G. Xiao. The global avalanche characteristics of two Boolean functions and algebraic immunity. *International Journal of Computer Mathematics*, vol. 89, no. 16, pp. 2165–2179, 2012.

Index

Povzetek v slovenskem jeziku

O NEKATERIH KONSTRUKCIJAH KRIPTOGRAFSKO POMEMBNIH BOOLOVIH FUNKCIJ

Nekatere vrste (vektorskih) Boolovih funkcij, npr. zlomljene funkcije, imajo pomembno vlogo v kriptografiji simetričnih ključev. Čeprav se zdi popolna klasifikacija zlomljenih funkcij težko dosegljiva, je vsaka na novo odkrita metoda za konstrukcijo teh funkcij izjemnega pomena. Enako velja za sorodne funkcije, kot so vektorske zlomljene funkcije, zlomljene in vektorske zlomljene funkcije nad liho karakteristiko ter planotske funkcije z disjunktnim spektrom. Poglavitni cilj v disertaciji bo poiskati nove primere tovrstnih funkcij s skrbno izbrano algebraično strukturo in določitev množice pogojev, ki bodo zagotovili zlomljenost funkcij. Algebraične lastnosti določenih razredov Boolovih funkcij, ki morebiti vsebujejo zlomljene funkcije, bodo podvržene podrobni analizi. Poleg tega je namen disertacije razviti nove konstrukcijske metode za nekatere kriptografsko pomembne funkcije.

V posebnem disertacija vsebuje popolno karakterizacijo za določene razrede vektorskih zlomljenih funkcij, ki so v multinomni sledni obliki. Preučevana je tako zlomljenost funkcij, ki slikajo v obseg lihe karakteristike, kot tudi njihovih vektorskih analogov, pri čemer so funkcije predstavljene kot multinomne sledne funkcije z Dillonivimi eksponenti. Poleg tega je v disertaciji podanih več neskončnih razredov semi-zlomljenih funkcij, kjer so razredi okarakterizirani bodisi z raznovrstnimi dekompozicijami tovrstnih funkcij ali njihovih podfunkcij glede na Walshov spekter bodisi z metodo, ki je uporabljena za njihovo konstrukcijo. Podana sta tudi dva razreda visoko nelinearnih semi-zlomljenih vektorskih funkcij z zelo dobrimi navzkrižno-korelacijskimi lastnostmi.

Opis raziskave

Kriptografija je grška beseda, ki pomeni ,,skrito". V glagolski obliki pomeni tako ,,pisati", kot tudi preučevati skrita sporočila napisanega. Drugače povedano, kriptografija je znanost oz. umetnost skrivnega pisanja. Danes je kriptografija področje informacijske teorije, ki z matematičnim pristopom preučuje prenos informacije iz enega v drug kraj, pri čemer so pri prenosu lahko navzoči nasprotniki. Prepleta tako uporabno kot teoretično matematiko, pomembno vlogo pa ima tudi v informacijski tehnologiji ter pri kontroli dostopa in avtentikacije. V moderni družbi je učinkovita, zanesljiva in varna izmenjava ter hramba podatkov bistvenega pomena. Kriptologija zaobjame med sabo povezana področja kriptografije in kriptoanalize. Kriptografske kode ali šifre se uporabljajo pri zaščiti pred prisluškovanjem, nepooblaščenimi spremembami podatkov ter ostalimi zlorabami. Kriptoanalitiki preučujejo šibke točke šifer. Varen pretok informacij bo ključnega pomena za popoln razcvet internetne in mobilne komunikacije na področjih kot so npr. plačilni sistemi, mobilna in e-trgovina ter zdravstveni sistemi, saj je tam žaščita občutljivih informacij izjemnega pomena. Marsikatera aplikacija bo potrebovala avtentikacijski sistem. Kriptologija postaja tako vse pomembnejša v poslu, industriji ter tudi v družbi na splošno.

Rešitve raznovrstnih kriptografskih problemov podajajo kriptografski gradniki. Skonstruirani so za specifične namene, zadostovati pa morajo številnim varnostnim pogojem. Štiri pomembnejši varnostni cilji so:

(i) zaupnost - preprečuje, da bi se nepooblaščena oseba dokopala do vsebine informacij. Sopomenska izraza sta tudi tajnost in zasebnost.

(ii) integriteta podatkov - preprečuje, da bi nepooblaščena oseba spremenila podatke.

(iii) avtentikacija - omogoča identifikacijo. Pomeni, da se komunicirajoča sogovornika lahko prepoznata.

(iv) nezatajljivost - preprečuje subjektu, da bi zavrnil predhodno dogovorjene obveze.

Za boljše razumevanje bomo prikazali preprost primer kriptosistemskega modela, ki zagotavlja zaupnost. Tovrstni kriptografski gradnik, poznan tudi kot kriptogafija simetričnih ključev, je skiciran na sliki 7.1. Transformacija čistopisa (sporočila) v šifropis imenujemo šifriranje. Dešifriranje nam iz šifropisa povrne čistopis, pri tem pa potrebuje poseben ključ. Kriptografija simetričnih ključev zajema dve veliki skupini kriptografskih gradnikov, tj. bločne in tokovne šifre. Omenjena dvojica predstavlja nepogrešljiv del v moderni kriptografiji, saj omogoča bistveno hitrejšo enkripcijo, kot jo dobimo pri kriptografiji javnega ključa. Kljub temu nam gradniki v simetrični kriptografiji (enako velja za kriptografijo javnega ključa) nudijo le t.i. računsko varnost, saj matematična redukcija na kak znan računsko težek problem, ki bi potrdil t.i. dokazljivo varnost, ni poznana. Šifre v kriptografiji simetričnih ključev uporabljajo hevristično strukturo, ki temelji na nekaterih dobro sprejetih dizajnerskih pravilih,

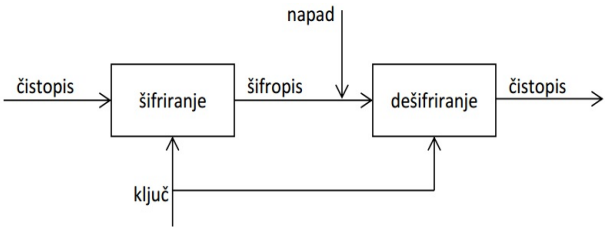

Figure 7.1: Model klasičnega kriptosistema

podprtih s prakso in odpornostjo pred kriptoanalizo današnjega časa. Pri bločnih šifrah je uporaba psevdo naključne permutacije, ki temelji bodisi na Feistelovem bodisi na SP omrežju, učinkovita in dobro preučena dizajnerska metoda. Na njeni osnovi so bile razvite nekatere močne sheme kot so Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), Advanced Encryption Standard (AES) (trenutni enkripcijski standard), itd. Pri tokovnih šifrah je zadeva precej drugačna. Razen nekaj izjem kot je RC4, večina predlogov, vključno s predlogi eSTREAM projekta za standardizacijo tokovnih šifer, ni zagotovila želene varnosti, saj so podlegli kriptoanalizi v zelo kratkem času. Kljub temu je varnost obeh vrst shem močno odvisna od robustnosti nekaterih kriptografskih gradnikov, imenovanih S-škatle. Slednje sestavlja posamezna ali množica Boolovih funkcij, izbira katerih je odvisna od uporabe oz. dizajna.

Koncept kriptografije javnega ključa se je razvil zaradi problema distribucije ključev in razvoja digitalnih podpisov. Uporablja nesimetričen par ključev: javni ključ in zasebni ključ. Javni ključ se uporablja za šifriranje čistopisa ali za preverbo digitalnega podpisa, medtem ko se zasebni ključ uporablja za dešifriranje šifropisa ali za generiranje digitalnega podpisa. Efektivnost poznanih kriptosistemov javnega ključa je bistveno nižja od simetričnih kriptosistemov. Njihova podatkovna propustnost je precej nižja, saj potrebujejo precej več časa za šifriranje dolgih sporočil, potrebujejo pa tudi daljše ključe za dosego enakega nivoja varnosti. Zaradi superiornih lastnosti pri hitrosti šifriranja (v primerjavi s kriptografijo javnih ključev) so gradniki kriptografije simetričnih ključev nepogrešljivi v moderni kriptografiji.

Obstajajo štiri glavne vrste napadov na kriptosistem, ki se razlikujejo glede na znane podatke:

(i) poznan je le šifropis - kriptoanalitik poskuša pridobiti šifrirni ključ oz. del ključa ali del čistopisa, pri čemer mu je poznan le šifropis;

(ii) poznan čistopis - kriptoanalitik poskuša pridobiti šifrirni ključ ali del ključa, pri čemer ima na voljo del čistopisa in pripadajoči del šifropisa;

(iii) izbran čistopis - cilj napada je pridobiti ključ ali dešifrirati določen čistopis. V tem primeru lahko kriptoanalitik šifrira katerikoli izbran čistopis.

(iv) izbran šifropis - ta primer je podoben prejšnjemu. Glavna razlika je v tem, da ima tukaj nasprotnik na voljo dešifrirno napravo in lahko dešifrira katerikoli šifropis. Cilj napada je pridobiti ključ, ki je lahko varno shranjen v napravi.

Differenčna kriptoanaliza je postala močno kriptoanalitsko orodje za napad na iterativne bločne šifre. Ta kriptoanalitska disciplina ima svoje korenine v prebojnem članku avtorjev Eli Biham in Adi Shamir [6] iz leta 1990. V osnovi je differenčna kriptoanaliza napad tipa ,,izbran čistopis", ki pa se lahko modificira v napad tipa ,,poznan čistopis", če je na voljo dovolj čistopisov. Differenčna kriptoanaliza v grobem analizira nastalo razliko v šifropisu, pri opravljeni spremembi v čistopisu. Biham in Shamir sta pokazala, da lahko s tovrstno tehniko hitreje razbijemo do 15 rund DES (od 16), kot bi to opravili s preverbo vseh možnosti. Pri skrajšani DES verziji pa lahko v nekaj minutah razbijemo do 8 rund. Tovrstna tehnika se je kasneje razvila v bolj napredne napade kot so *diferenčno-linearna analiza* avtorjev Susan K. Langford in Martina E. Hellmana [55] ter *skrajšana diferenčna analiza* in *diferenčna analiza višjega reda* avtorjev Larsa Knudsena in Thomasa Jakobsena [53, 49].

Linearno kriptoanalizo je uvedel Mitsuru Matsui [63] in velja do danes za enega najboljših napadov na DES. V takem napadu kriptoanalist preučuje linearno relacijo med nekaj biti čistopisa, šifropisa in ključa. Matsui je pokazal, da v kolikor relacija ne velja natanko polkrat (razdalja med Boolovo funkcijo v neki S-škatli in neko linearno funkcijo je majhna), potem lahko informacijo o kluču pridobimo z uporabo številnih znanih parov čistopisa in šifropisa. Efektivnost tovrstnega napada je najbolje prikazana v Matsuijevem članku, kjer je bilo 12 rund DES razbitih v samo 50 urah, pri čemer je bilo poznanih 2^{31} parov čistopisa in šifropisa.

Boolove funkcije (tj., funkcije, ki slikajo iz n-razsežnega binarnega vektorskega prostora $\mathbb{F}_2^n$ v obseg $\mathbb{F}_2$ z dvema elementoma) imajo pomembno vlogo pri konstrukcijah simetričnih šifer. Pogosto se jih uporablja kot nelinearne kombinirajoče funkcije v tokovnih šifrah, ki bazirajo na LFSR (prikazano na sliki 7.2). Simetrična kriptogra-

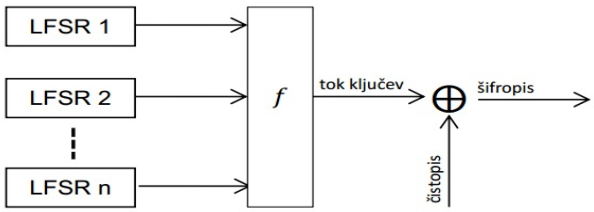

Figure 7.2: LFSR-osnovna tokovna šifra

fija predstavlja atraktivno področje raziskovanja s številnimi aplikacijami pri GSM telefonih, Bluetooth in WLAN omrežju, ter pri RFID-shemah. Gradniki teh kriptosistemov pogosto uporabljajo tako Boolove funkcije, kot tudi vektorske Boolove funkcije, imenovane tudi S-škatle (tj. preslikave oblike $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$). Potreben pogoj za brezpogojno varnost pri šifrirni shemi simetričnih ključev je to, da je dolžina

šifrirnega ključa dolga vsaj toliko, kot je sporočilo. Shannon [90] je vpeljal dva zelo pomembna pojma, ki ju pogosto srečamo pri konstrukciji modernih šifer. To sta *zmeda* in *razpršitev*. Namera zmede je prikriti kakršnokoli algebraično strukturo v sistemu. Tesno je povezana z zahtevnostjo vpletenih Boolovih funkcij. Razpršitev predstavlja širitev majhne modifikacije vhodnih podatkov ali ključa po vseh izhodnih podatkih. Da so šifre dovolj robustne pred znanimi kriptoanalitskimi orodji, morajo Boolove funkcije zadoščati določenim kriptografskim kriterijem:

(i) visoka algebraična stopnja - vsi kriptosistemi, ki uporabljajo Boolove funkcije za zmedo, niso zaščiteni, če je stopnja funkcij nizka;

(ii) visoka nelinearnost - kriptografske funkcije morajo biti dovolj stran (dovolj različne) od vseh afinih funkcij;

(iii) uravnoteženost - kriptografske funkcije morajo biti uravnotežene (izhodni stolpec v pravilnostni tabeli mora imeti enako število enk in ničel) zato, da med vhodnimi in izhodnimi podatki ni statistične odvisnosti;

(iv) visoka algebraična imunost reda m - izhoden podatek Boolove funkcije mora biti statistično neodvisen od katerekoli kombinacije m vhodnih podatkov;

(v) zaščita pred diferenčno kriptoanalizo - funkcija mora imeti dobre diferenčne lastnosti;

(vi) efektivna izračunljivost in kompatibilnost.

Največja ovira pri iskanju dobrih kriptografskih funkcij je dejstvo, da morajo biti zgornji kriteriji zadoščeni simultano. Poleg tega je Boolovih funkcij, ki binarne n-terice slikajo v 0 oz. 1, ogromno, tj. 2^{2^n}. Kar pomeni, da je računalniška preverba vseh funkcij, ki bi morebiti imele želene lastnosti, nemogoča že za $n = 6$. Spodnja tabela prikazuje število Boolovih funkcij za $4 \leq n \leq 8$. Zlomljene funkcije,

Table 7.1: Prostor Boolovih funkcij

n	4	5	6	7	8
2^{2^n}	2^{16}	2^{32}	2^{64}	2^{128}	2^{256}

kot posebna vrsta Boolovih funkcij, so ekstremni kombinatorični objekti s tevilnimi področji uporabe, kot so npr. teorija kodiranja, teorija MLS, kriptografija, teorija diferenčnih množic itd. Pojem *zlomljene funkcije* je prvi vpeljal Rothaus [85], in kasneje sta jih Maiorana-McFarland [66] in Dillon [36] posplošil. Med vsemi ekvivalentnimi kriteriji za karakterizacijo zlomljenih funkcij je najpogosteje uporabljen tisti, ki jih opiše kot Boolove funkcije z ravnim Walshevim spektrom. Slednje pomeni, da je vsaka zlomljena funkcija v n spremenljivkah na konstantni Hammingovi razdalji do vseh afinih funkcij, vključno z funkcijama, ki vse slikata v 0 oz. 1.

En tovrsten razred predstavljajo funkcije, za katere velja $f(x,y) = x \cdot \pi(y) \oplus g(y)$ for all $x, y \in \mathbb{F}_2^{n/2}$, kjer je $\pi(y)$ permutacija na $\mathbb{F}_2^{n/2}$ in g je Boolova funkcija na $\mathbb{F}_2^{n/2}$. Tukaj $\oplus$ pomeni seštevanje po modulu 2 in "$\cdot$" je notranji produkt v $\mathbb{F}_2^{n/2}$. Enega prvih rezultatov o zlomljenih funkcijah je tudi predstavil Dillon [36], ki je analiziral t.i. $\mathcal{PS}$ razred zlomljenih funkcij. Preučeval je tudi $\mathcal{PS}_{ap}$ podrazred, pri katerem je funkcije lahko eksplicitno opisal s polinomi v dveh spremenljivkah nad končnimi obsegi. Leta 1994 je Carlet [19] predstavil dva nova razreda zlomljenih funkcij. Čeprav so bili ti kombinatorični objekti preučevani še v številnih drugih člankih (glej npr. [11, 20, 39]), se njihova celovita klasifikacija trenutno ne zdi mogoča.

Iz kriptografskega stališča sta stopnja in nelinearnost Boolove funkcije na vektorskem prostoru $\mathbb{F}_2^n$ njena glavna podatka [32, 70, 92]. Ker zlomljene funkcije dosežejo maksimalno stopnjo nelinearnosti, zagotovijo najboljšo zaščito pri linearnih napadih [63], če jih uporabimo pri takih algoritmih za generiranje toka ključev, kot sta filtrirni generator in kombinirni generator. Poleg tega so vektorske zlomljene funkcije primerne kot S-škatle pri konstrukciji bločnih šifer, saj so dobri gradniki osnova za katerokoli varno kriptografsko shemo.

V teoriji kodiranja [62] lahko vsako kodo dolžine 2^n interpretiramo kot Boolovo funkcijo. Zlomljene funkcije so v tem pogledu tesno povezane z Reed-Mullerjivimi in Kerdockovimi kodami [15]. Ta karakterizacija je še posebej pomembna zato, ker poda nelinerane kode, ki imajo boljše parametre od linearnih kod. Reed-Mullerjevo kodo prvega reda sestavljajo vse afine funkcije na prostoru $\mathbb{F}_2^n$. Če je n sod, potem so zlomljene funkcije ravno tiste funkcije, ki imajo maksimalno možno razdaljo do besed v Reed-Mullerjevi kodi prvega reda. Kerdockovo kodo lahko interpretiramo kot množico kvadratnih zlomljenih funkcij.

V kombinatoriki so zlomljene funkcije ekvivalentne diferenčnim množicam v elementarnih abelovih 2-grupah [35, 64]. Boolovo funkcijo f na množici $\mathbb{F}_2^n$ lahko opišemo z njenim nosilcem, tj. z množico $S = \{x \in \mathbb{F}_2^n : f(x) = 1\}$. Dobro je znano, da je množica S netrivialna diferenčna množica v prostoru $\mathbb{F}_2^n$ natanko tedaj, ko je f zlomljena funkcija [83]. Zato je karakterizacija vseh netrivialnih differečnih množic v grupi $(\mathbb{F}_2^n, +)$ ekvivalentna karakterizaciji vseh zlomljenih funkcij. Delne diferenčne množice so kombinatorični objekti, ki ustrezajo krepko-regularnim grafom [60]. Za vsako Boolovo funkcijo $f : \mathbb{F}_2^n \mapsto \mathbb{F}_2$ lahko skonstruiramo Cayleyev graf G_f, ki ima $\mathbb{F}_2^n$ za množico točk, množica povezav pa je podana kot $E_f = \{(u,v) \in \mathbb{F}_2^n \times \mathbb{F}_2^n : f(u \oplus v) = 1\}$, kjer je $\oplus$ seštevanje vektorjev po modulu 2. V člankih [4, 5] je pokazano, da je f zlomljena funkcija natanko tedaj, ko je za poljuben par vozlišč u, v število vozlišč, ki so sosedna tako u kot v, konstantno, graf G_f pa je krepko-regularen. Zato lahko zlomljene funkcije uporabljamo tudi pri konstrukciji krepko-regularnih grafov [94]. Konstrukcija zlomljenih funkcij je tako zelo zanimiv in obširno preučevan problem.

Posebno družino zlomljenih funkcij tvorijo *monomske zlomljene funkcije*, tj. Boolove funkcije (vsaka Boolova funkcija je oblike $f(x) = Tr(F(x))$, kjer je F preslikava oblike $F : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$, $Tr : \mathbb{F}_{2^n} \to \mathbb{F}_2$ pa je absolutna sled), ki so oblike $x \mapsto Tr(ax^d)$ za nek eksponent d in fiksni skalar $a \in \mathbb{F}_{2^n}$. Omenjen razred zlomljenih funkcij je

pomemben zato, ker poda edini poznan primer nenormalnih zlomljenih funkcij [12]. Boolove funkcije oblike $Tr_1^n(ax^d)$ so bile preučevane v številnih delih [9, 26, 38, 56]. Kolikor nam je znano, so funkcije, ki so podane v teh delih, edini poznan razred zlomljenih funkcij take oblike (do afine ekvivalence natančno). Natančna karakterizacija eksponentov d in skalarjev a, pri katerih je dana Boolova funkcija zlomljena, je težek problem.

Drug poseben razred predstavljajo *binomske zlomljene funkcije*, tj. Boolove funkcije, ki so skonstruirane s pomočjo linearne kombinacije dveh potenčnih funkcij. Binomske (oz. multinomske) sledne funkcije je težje analizirati. Le nekaj takih zlomljenih funkcij je poznanin [25, 39]. Rezultat Dobbertina in Leandera [39], ki je soroden s t.i. linearnimi Nihovimi eksponenti (tj. zožitev funkcije x^d na $\mathbb{F}_{2^{n/2}}$ je linearna), je bil kasneje posplošen v članku [57], kjer so pokazali obstoj zlomljenih slednih funkcij z 2^r Nihovimi eksponenti. V članku [25] so zlomljene Boolove funkcije klasificirali v kontekstu Dicksonovih polinomov in Kloostermanovih vsot. Nekaj dodatnih razredov binomskih hiperzlomljenih (glej [21, 102]) slednih funkcij, kjer je en monom kombiniran z absolutno sledjo, drug pa z relativno sledjo, je bilo odkritih v delih [71, 95].

Zlomljene Boolove funkcije lahko posplošimo do vektorskih preslikav $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, če zahtevamo, da vse neničelne linearne kombinacije komponent preslikave F tudi tvorijo zlomljeno funkcijo, tj. funkcija $Tr_1^m(\lambda F(x))$ je zlomljena za vse $\lambda \in \mathbb{F}_{2^m}^*$, $x \in \mathbb{F}_{2^n}$. Prvo konstrukcijo takih *vektorskih zlomljenih funkcij* je odkrila Nyberg [77]. V članku [77] je bilo pokazano, da vektorske zlomljene funkcije lahko obstajajo le, če velja $m \leq n/2$. Nekaj njihovih konstrukcij je bilo dobljenih s pomočjo Maiorana-McFarlandovega razreda zlomljenih funkcij [36, 37, 85] ter s pomočjo Dillonovega razreda [15, 36, 37]. Rezultate podobnih tipov najdemo tudi v delih [39, 40, 80, 100]. Vsi ti rezultati temeljijo na konstrukciji takih m Boolovih zlomljenih funkcij, katerih linearna kombinacija ostane zlomljena. V članku [80] je bilo pokazano, da je vektorska funkcija $F(x) = Tr_k^n(ax^d), n = 2k$ zlomljena, če je $f(x) = Tr_1^n(ax^d)$ zlomljena funkcija, x^d pa je permutacija obsega $\mathbb{F}_{2^k}$. Slednji pogoj o permuaticiji je bil le zadosten in ne nujno tudi potreben. Prav tako je bil polinom v sledi le monom, medtem ko funkcije z bolj splošnim polinomom niso bile obravnavane. Potrebni in zadostni pogoji za zlomljenost multinomne sledne funkcije so podani v razdelku 3 (glej izrek 3.3.1).

Po drugi strani lahko zlomljenost vektorske funkcije F opišemo tudi s koeficienti elementarnih simetričnih polinomov[59], ki so povezani z vrednostmi preslikave F na $\mathcal{U}$. Zaradi težavnosti izračuna vrednosti teh simetričnih polinomov pri multinomski sledni funkciji, se naša analiza omeji na binomski primer, kjer dobimo le nekaj potrebnih pogojev za zlomljenost. Ti pogoji so v prvi vrsti koristni za izločevanje koeficientov γ, z, pri katerih vektorska funkcija $F(x) = Tr_k^n(x + \gamma z x^{r(2^k-1)})$ ne more biti zlomljena (glej razdelek 3.4). V razdelku 3.5 je pokazano, da $Tr_k^n(\lambda x^{r(2^k-1)})$ ni nikoli vektorska zlomljena funkcija z maksimalno dimenzijo k.

Posplošitev zlomljenih funkcij na končne obsege lihe karakteristike so prvi obravnavali Kumar, Scholtz in Welch [54]. Razred p-arnih zlomljenih funkcij še ni bil

preučevan v zadovoljivem obsegu. Kolikor nam je znano, so bili pogoji za zlomljenost preučevani le za nekaj razredov binomskih slednih funkcij [46, 58, 101, 105]. V poglavju 4 je pokazano, da so pogoji iz rezultata [105] veljavni tudi v primeru multinomnih slednih funkcij $f : \mathbb{F}_{p^n} \mapsto \mathbb{F}_p;\ f(x) = Tr_1^n(\sum_{i=1}^{t} a_i x^{r_i(p^k-1)})$ z Dillonivimi eksponenti ($d = p^k - 1$). Za zlomljenost bodo morali koeficienti $a_i \in \mathbb{F}_{p^n}$ in $r_i \in \mathbb{N}$ še vedno ustrezati določenim pogojem. Le ti bodo direktno povezani s sliko funkcije na množici $V = \{1, \alpha, \alpha^2, \ldots, \alpha^{p^k}\}$, kjer je α primitiven element obsega $\mathbb{F}_{p^n}$ (glej izrek 4.3.1). Kompletna klasifikacija posplošenih zlomljenih funkcij je seveda precej težji problem, kot je klasifikacija v binarnem primeru.

Konstrukcije prožnih Boolovih funkcij z visoko stopnjo, visoko nelinearnostjo in dobro imunostjo pred algebraičnimi napadi so pomembne zaradi aplikacij v tokovnih šifrah, kjer uporabimo kombiniran model. Pomembnost teh funkcij ponazori tudi obsežna literatura [14, 17, 24, 50, 51, 65, 78, 82, 86, 87, 89, 96, 97], ki jih obravnava. Konstrukcija Boolovih funkcij z vnaprej danimi omenjenimi parametri je še vedno odprt problem . Izkaže se, da vsi parametri ne morejo hkrati zavzeti maksimalnih vrednosti. Siegenthaler je pokazal, da za uravnoteženo funkcijo n spremenljivk, ki je stopnje d in reda pronosti m, velja $m + d \leq n - 1$, če je $m \leq n - 2$ [91]. Kompromisne meje med redom korelacijske imunosti, nelinearnostjo in stopnjo so bile preučevane tudi v člankih [16, 87, 97, 106]. Rekurzivna metoda za konstrukcijo optimalnih planotskih funkcij z relativno velikim redom prožnosti je preučevana v članku [43]. V poglavju 5, ki preučuje *funkcije disjunktnega spektra*, je pokazano, da s katerokoli konkatenacijo 2^k funkcij iz množice $\{f, 1 + f\}$ oz. $\{g, 1 + g\}$ dobimo spet par funkcij disjunktnega spektra v $(n + k)$ spremenljivkah. To velja za poljuben $k \geq 0$ (glej trditev 5.3.1). Omenjeno bo omogočalo kontrolo nad nelinearnostjo in prožnostjo teh funkcij, če bomo uporabili pravilno konfiguracijo funkcije in njenega komplementa. S posplošitvijo tega postopka smo razvili iterativno metodo za konstrukcijo funkcij disjunktnega spektra, ki nam poda večkratno razvejitveno drevo neskončnega zaporedja optimalnih planotskih funkcij (glej razdelek 5.3). Par funkcij disjunktnega spektra v $(n + k)$ spremenljivkah predstavlja t.i. *semi-zlomljene Boolove funkcije* [29]. (Semi-zlomljene) funkcije disjunktnega spektra, ki se uporabljajo pri iterativnih konstrukcijah kriptografsko močnih funkcij, v splošnem niso redek kombinatoričen objekt. Konstrukcijska metoda semi-zlomljenih funkcij je podana v razdelku 5.2.

V članku [104] sta Zhang in Zheng vpeljala pojem *globalne plazovne karakteristike* (GAC), da bi odpravila pomanjkljivosti v kriteriju razširjanja in v strogem plazovnem kriteriju, ter tako razumela vse karakteristike razširjanja kriptografske funkcije. V njunem članku je bilo pokazano tudi, da so karakteristike razširjanja katerihkoli Boolovih funkcij v povezavi z določenimi lastnostmi njihovih odvodov.

Motivacija za karakterizacijo z navzkrižno-korelacijskimi lastnostmi izhaja iz informacijsko teoretičnih aspektov varnosti, kot sta fundamentalna koncepta zmede in razpršitve, ki ju je vpeljal Shannon. Da bi Boolove funkcije v šifri zagotavljale dovoljšnjo mero zmede in razpršitve, morajo med sabo imeti nizko navzkrižno-korelacijo, kar sta predlagala Sarkar in Maitra [88]. S pomočjo navzkrižno-korelacijskih lastnosti

je bila v članku [88] podana tudi uporabna karakterizacija nekaterih razredov kriptografskih Boolovih funkcij, prikazane pa so bile tudi nekatere pomanjkljivosti pogosto uporabljenih S-škatel. Analiza dane S-škatle je bila opravljena z meritvijo navzkrižne-korelacije med komponentnimi funkcijami $f_1, \ldots, f_m$ S-škatle. S-škatla je bila tako upodobljena kot vektorska Boolova preslikava $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ [88].

Nadaljnja posplošitev teh kriterijev je bila obravnavana v članku [110], kjer sta bila vpeljana dva nova indikatorja, za meritev navzkrižne-korelacije dveh Boolovih funkcij (tudi za meritev autokorelacije).

V poglavju 6 so podane številne metode za konstrukcijo visoko nelinearnih S-škatel, katerih komponentne funkcije imajo zelo dobre navzkrižno-korelacijske lastnosti. V razdelku 6.2 je prikazano, da je zlomljenost funkcije $f+g$ zadosten pogoj, da absolutni indikator zavzame minimalno možno vrednost $2^{n/2}$. Opisana je tudi praktična metoda za konstrukcijo perfektno nekoreliranih S-škatel z sodo mnogo vhodnimi spremenljivkami (glej 6.2.2).

Zaključek

Glavni del disertacije obravnava možnosti za konstrukcijo vektorskih zlomljenih funkcij nad končnim obsegom karakteristike 2 in končnim obsegom lihe karakteristike. Podani so potrebni in zadostni pogoji za določene vrste funkcij, ki so v multinomni sledni obliki. Ti rezultati so omogočili eksplicitno določitev koeficientov funkcij tipa $Tr_k^{2k}(\sum_{i=0}^{2^k} a_i x^{i(2^k-1)})$ in natančno število vektorskih zlomljenih funkcij v tej obliki [76]. Ker so zlomljene funkcije nad končnim obsegom lihe karakteristike tesno povezane z ravninskim preslikavam, naši rezultati vesbujejo konstrukcijsko metodo vektorske (posplošene) zlomljene funkcije dimenzije $n/2$ čeprav ravninske preslikave inducirajo vektorske (posplošene) zlomljene funkcije maksimalne dimenzije n. Ta pomemben problem je ostal odprt.

V doktorski disertaciji je podano več različnih načinov za konstrukcijo neskončnega zaporedja disjunktnega spektra, optimalnih planotskih in semi-zlomljenih funkcij. V posebnem je opisano dizajniranje vektorskih semi-zlomljenih funkcij s kombiniranjem vektorskih zlomljenih funkcij iz Nihovega razreda in razreda $\mathcal{PS}$. Predvidevamo, da bo s skrbnim izborom komponentnih fukcij iz S-škatel mogoče pristop iz disertacije izboljšati tako, da bodo lastnosti razširjanja S-škatel optimizirane. Slednje ostaja odprt problem in izziv za nadaljnje raziskovanje.

Stvarno kazalo

Declaration

I declare that this thesis does not contain any materials previously published or written by another person except where due reference is made in the text.

Samed Bajrić