ON CONSTRUCTIONS AND ENUMERATION OF BENT AND SEMI-BENT FUNCTIONS

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF APPLIED MATHEMATICS
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

NEŞE KOÇAK

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF DOCTOR OF PHILOSOPHY
IN
CRYPTOGRAPHY

AUGUST 2015

Approval of the thesis:

ON CONSTRUCTIONS AND ENUMERATION OF BENT AND SEMI-BENT FUNCTIONS

submitted by **NEŞE KOÇAK** in partial fulfillment of the requirements for the degree of **Doctor of Philosophy in Department of Cryptography, Middle East Technical University** by,

Prof. Dr. Bülent Karasözen
Director, Graduate School of **Applied Mathematics** _____

Prof. Dr. Ferruh Özbudak
Head of Department, **Cryptography** _____

Assoc. Prof. Dr. Ali Doğanaksoy
Supervisor, **Department of Mathematics, METU** _____

Assoc. Prof. Dr. Zülfükar Saygı
Co-supervisor, **Department of Mathematics, TOBB ETU** _____

Examining Committee Members:

Prof. Dr. Ali Aydın Selçuk
Department of Computer Engineering, TOBB ETU _____

Assoc. Prof. Dr. Ali Doğanaksoy
Department of Mathematics, METU _____

Prof. Dr. Ferruh Özbudak
Department of Mathematics, METU _____

Assist. Prof. Dr. Nurdan Saran
Department of Computer Engineering, Çankaya University _____

Assist. Prof. Dr. Fatih Sulak
Department of Mathematics, Atılım University _____

Date: _____

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name: NEŞE KOÇAK

Signature :

ABSTRACT

ON CONSTRUCTIONS AND ENUMERATION OF BENT AND SEMI-BENT FUNCTIONS

Koçak, Neşe

Ph.D., Department of Cryptography

Supervisor : Assoc. Prof. Dr. Ali Doğanaksoy

Co-Supervisor : Assoc. Prof. Dr. Zülfükar Saygı

August 2015, 60 pages

Bent and semi-bent functions play an important role in cryptography and coding theory. They are widely studied as parts of building blocks in symmetric key cryptosystems because they provide resistance to fast correlation attacks and linear cryptanalysis due to their high nonlinearity. Besides, they can possess other desirable cryptographic properties such as low autocorrelation, propagation criteria, resiliency and high algebraic degree. Therefore, parallel to the advances in cryptanalysis techniques, the need for finding and constructing such functions increases day by day. However, as the number of inputs gets higher, it becomes impossible to search exhaustively all bent/semi-bent functions on the entire space. This limitation prompts researchers to deduce new methods to obtain bent/semi-bent functions with reasonable amount of computation power. A lot of research has been devoted to construction, characterization or enumeration of bent/semi-bent functions. For these reasons, we aim to contribute to the knowledge of bent and semi-bent functions by presenting new results on constructions, characterization and enumeration of these functions.

In this thesis, characterization of a class of quadratic Boolean functions for semi-bentness is given and it is proved that semi-bent functions exist only when the input number is a multiple of 6. Furthermore, a generic method for enumeration of semi-bent and bent functions in certain classes is presented. Using this method, exact number of characterized semi-bent functions is found. Moreover, with this method some previous partial and incomplete enumeration results for three other classes of semi-bent/bent

functions in the literature are completed.

Explicit constructions of bent and semi-bent functions of Maiorana-McFarland class via linear structures and linear translators are proposed. Also, by using these explicit constructions as well as other algebraic structures like derivatives, certain quadratic and cubic functions, new secondary constructions of bent and semi-bent functions are obtained.

Keywords : Boolean functions, Bent functions, Semi-bent functions, Polynomial form, Linear Translators

ÖZ

BÜKÜK VE YARI-BÜKÜK FONKSİYONLARIN İNŞAASI VE SAYMASI ÜZERİNE

Koçak, Neşe

Doktora, Kriptografi

Tez Yöneticisi : Doç. Dr. Ali Doğanaksoy

Ortak Tez Yöneticisi : Doç. Dr. Zülfükar Saygı

Ağustos 2015, 60 sayfa

Bükük ve yarı-bükük fonksiyonlar kriptografi ve kodlama teorisinde önemli bir rol oynamaktadır. Bu fonksiyonlar yüksek nonlineeriteye sahip olmaları sebebiyle hızlı korelasyon saldırılarına ve lineer kriptanalize dayanıklı olduklarından simetrik anahtarlı kriptosistemlerde yapıtaşları olarak yaygın bir şekilde kullanılmışlardır. Bunun yanında, düşük otokorelasyon, yayılma kriteri, dayanıklılık ve yüksek cebirsel derece gibi istenen kriptografik özelliklere de sahip olabilirler. Bu nedenle, kriptanaliz tekniklerindeki gelişmelere paralel olarak bu tür fonksiyonları bulma ve inşa etme ihtiyacı gün geçtikçe artmaktadır. Bununla birlikte, girdi sayısı arttıkça tüm bükük ve yarı-bükük fonksiyonları bütün uzayda aramak imkansız hale gelmektedir. Bu kısıtlılık araştırmacıları bükük ve yarı-bükük fonksiyonlar elde etmek için makul bir hesaplama gücüne sahip yeni metotlar bulmaya sevk etmiştir. Bükük ve yarı-bükük fonksiyonların inşaası, sınıflandırılması ve sayılması konusunda oldukça çok araştırma yapılmıştır. Bu sebeplerden dolayı, bükük ve yarı-bükük fonksiyonların bilgi birikimine bunların inşaası, sınıflandırılması ve sayılması konusunda sonuçlar sunarak katkıda bulunulması amaçlanmıştır.

Bu tezde, ikinci derece bir Boole fonksiyon sınıfının yarı-bükülük açısından sınıflandırılması verilmiş ve yarı-bükük fonksiyonların girdi sayısı sadece 6'nın bir katı iken var olabileceği ispatlanmıştır. Ayrıca, belirli sınıflardaki bükük ve yarı-bükük fonksiyonların sayımı için genel bir yöntem önerilmiştir. Bu yöntem kullanılarak sınıflandırılması yapılan yarı-bükük fonksiyonların tam olarak sayısı bulunmuştur. Buna ek olarak,

literatürde var olan bazı bükük/yarı-bükük fonksiyon sınıflarının sayıları ile ilgili sonuçlar genellenmiştir.

Doğrusal yapılar ve çeviriciler kullanılarak Maiorana-McFarland sınıfına ait bükük ve yarı-bükük fonksiyonların inşaaları verilmiştir. Ayrıca, bu inşaalar ve türev gibi diğer cebirsel yapılar ile belirli ikinci ve üçüncü dereceden fonksiyonlar da kullanılarak bükük ve yarı-bükük fonksiyonlar için yeni ikincil inşa sınıfları elde edilmiştir.

Anahtar Kelimeler : Boole fonksiyonlar, Bükük fonksiyonlar, Yarı-bükük Fonksiyonlar, Polinom formu, Doğrusal çeviriciler

To My Family

ACKNOWLEDGMENTS

I would like to express my sincere gratitude to my supervisor Assoc. Prof. Dr. Ali Doğanaksoy for his invaluable guidance and enthusiastic encouragement throughout this thesis.

I wish to express my sincere appreciation to Prof. Dr. Ferruh Özbudak for many interesting ideas, suggestions and contributions. This work would not be completed without his help. My gratitude is extended to my co-supervisor Assoc. Prof. Dr. Zülfükar Saygı for his advices and guidance.

I also would like to thank Prof. Dr. Sihem Mesnager for her valuable advices which helped me a lot in my research.

My sincere thanks go to all my friends for their close friendship and motivation. I would like to thank committee members, academic and administrative staff of the Institute of Applied Mathematics.

I am also grateful to my supervisors Bikem Temürcü and Hamdi Erkan and to my colleagues at ASELSAN.

Very special thanks to my husband Onur for his endless support, patience and love, and also for being with me all the way.

I am grateful to my dearest family for their unconditional love and supporting me throughout my life.

The generous financial support of the Scientific and Technological Research Council of Turkey (TUBITAK) Graduate Scholarship no. 2211 is gratefully acknowledged.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF ABBREVIATIONS

p	A prime number
q	A prime number's power
$\mathbb{F}_{2^n}$	Finite field with 2^n elements
$\mathbb{F}_q$	Finite field with q elements
$\mathbb{F}_2^n$	Vector space of all binary vectors of length n
$\mathcal{B}_n$	The set of all Boolean functions of n variables
$\mathcal{A}_n$	The set of all affine functions of n variables
χ_f	The sign function of a Boolean function f
$\widehat{\chi_f}(\omega)$	The Walsh-Hadamard transform of f at ω
$wt(f)$	The Hamming weight of a Boolean function f
$wt(x)$	The Hamming weight of a binary vector $x \in \mathbb{F}_2^n$
$nl(f)$	The nonlinearity of a Boolean function f
$d_H(f,g)$	The Hamming distance between two functions f and g
$deg(f)$	Algebraic degree of a Boolean function f
$o(j)$	The size of the cyclotomic coset containing j
$Tr_m^n(\cdot)$	The trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$
$Tr_1^n(\cdot)$	The absolute trace : trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$
$\#S$	Cardinality of the set $\mathcal{S}$
$gcd(f,g)$	Greatest common divisor of f and g
$\tilde{f}$	Dual of the function f

CHAPTER 1

INTRODUCTION

1.1 Overview

Boolean functions are nice and well practiced combinatorial objects. They play an essential role not only in cryptography and coding theory but also in combinatorics, complexity theory, probability theory and other areas of mathematics and computer science. Boolean functions can be defined simply as mappings from $\mathbb{F}_{2^n}$ (Finite field with 2^n elements) to $\mathbb{F}_2$, that is for each input they output 0 or 1. An indigenous generalization of Boolean functions known as vectorial Booelan functions are the multi-output Boolean functions. In cryptography, Boolean functions are considered as significant objects since they are used in the construction of building blocks in symmetric cryptosystems. For instance, the so-called Substitution boxes (S-boxes) which are fundamental parts of block ciphers are constituted of vectorial Boolean functions.

Theory of Boolean functions is an important and widely studied research area. Accompanied with the developments in cryptanalysis techniques, the need for the design and analysis of Boolean functions have increased significantly in the last decades.

Designing a symmetric cipher scheme and analyzing its security margins are directly related to the construction of Boolean functions with desirable cryptographic properties. This forces the designers to choose *"cryptographically good"* Boolean functions to be used in the cipher. These choices may depend on several cryptographic features such as nonlinearity, balancedness, algebraic degree, correlation immunity, algebraic immunity, propagation criteria etc. However, a Boolean function satisfying all of these criteria simultaneously seems impossible since there is a conflict between these cryptographic criteria. For instance, according to Siegenthaler's bound [44], algebraic degree of an n-variable m-th order correlation immune Boolean function can be at most $n - m$. This indicates that a Boolean function cannot have high algebraic degree and the maximum possible correlation immunity at the same time. Also, a function with even number of inputs and having maximum nonlinearity can be neither balanced nor of maximal degree. Similarly, a function with maximal algebraic immunity cannot have algebraic degree greater than half of the number of inputs. Therefore, it is obvious that compromises have to be made, and trade-offs need to be evaluated. Indeed, finding the best trade-offs between all criteria and proposing concrete constructions of Boolean functions comprising a good combination of these properties become more

challenging both in theoretical and practical cryptographic purposes.

One of the most significant cryptographic criteria of a Boolean function is the nonlinearity. Bent functions possess the maximum nonlinearity among Boolean functions. They were defined only for even dimensions and first studied by Dillon [20] in 1974 but first introduced by Rothaus [43] in 1976. Especially in the last 20 years, bent functions have been a very actively studied research area since they have applications in cryptography (symmetric key cryptosystems), algebraic coding theory, sequence theory and design theory. A book devoted especially to binary bent functions and containing a complete survey on bent functions is [41]. Open problems on binary bent functions can be found in [7].

Bent functions play a crucial role in the design of stream and block ciphers since they provide confusion in these cryptosytems due to their high nonlinearity. In block ciphers, bent functions are involved in the substitution boxes (S-boxes) in order to add nonlinearity to the cipher and hence to resist differential and linear attacks. On the other hand, bent functions cannot be balanced. Hence, with some modifications, bent functions can be employed in the pseudo-random generator of a stream cipher in order not to leak statistical correlation between the plaintext and the ciphertext.

Bent functions are particular plateaued functions. The notion of plateaued function has been introduced in 1999 by Zheng and Zhang as good candidates for designing cryptographic functions since they possess desirable various cryptographic characteristics. They are defined in terms of the Walsh-Hadamard spectrum. Plateaued functions bring together various nonlinear characteristics and include two important classes of Boolean functions defined in even dimension: the well-known bent functions and the semi-bent functions. Very recently, the study of semi-bent functions has attracted the attention of several researchers. Many progresses in the design of such functions have been made.

A complete classification and enumeration of bent and semi-bent functions are still open problems. Table 1.1 shows the exact number of bent functions for $n \leq 8$ together with the lower and upper bounds on the number of bent functions for $n \leq 10$ in order to emphasize that how difficult to give estimations on these bounds when the dimension gets higher. Therefore, not only the characterization, but also enumeration and construction of bent and semi-bent functions are challenging problems.

Table 1.1: Number of bent functions [32, 48]

n	lower bound	# of bent functions	upper bound
2	8	$8 = 2^3$	8
4	2^9	$896 \approx 2^{9.8}$	2^{11}
6	$2^{28.3}$	$\approx 2^{32.3}$	2^{42}
8	$2^{87.4}$	$\approx 2^{106.3}$	2^{163}
10	2^{262}	$unknown$	2^{638}

1.2 Outline of the Thesis

This thesis consists of five chapters including this introduction chapter.

Chapter 2 contains some concepts, notations and definitions which will be used throughout the thesis. The notions related to the representations of Boolean functions namely algebraic normal form, numerical normal form, trace representation and bivariate representations are recalled. Also, properties of bent and semi-bent functions within the scope of this thesis are mentioned.

In Chapter 3, we give a characterization of a class of semi-bent quadratic Boolean functions and specify the necessary and sufficient conditions for this class of functions to be semi-bent. We also present a generic method for enumeration and complement some previous results on enumeration of semi-bent and bent functions for all n. Additionally, some results on bent functions given in [34] are corrected.

Chapter 4 is devoted to explicit constructions of bent and semi-bent functions via linear translators. We first consider such functions in Maiorana-McFarland type and obtain bent and semi-bent functions Boolean functions having linear structures (linear translators) systematically. Also, using these results we modify many secondary constructions. herefore, we obtain new secondary constructions of bent and semi-bent functions not belonging to the Maiorana-McFarland class. Instead of using bent (semi-bent) functions as ingredients, our secondary constructions use only Boolean (vectorial Boolean) functions with linear structures (linear translators) which are very easy to choose. Moreover, all of them are very explicit and we also determine the duals of the bent functions in our constructions. We show how these linear structures should be chosen in order to satisfy the corresponding conditions coming from using derivatives and quadratic/cubic functions in our secondary constructions.

Finally, Chapter 5 concludes the thesis by summarizing the work and emphasizing the contributions.

CHAPTER 2

PRELIMINARIES

This chapter provides the necessary background and notation used in this thesis. Representations of Boolean functions, namely algebraic normal form, numerical normal form, trace (polynomial) and bivariate representations are described. The definitions of bent and semi-bent functions and the notions related to them are given. The interested reader is referred to [6] and [41] for excellent treatments on these subjects.

2.1 Boolean Functions and Their Representations

Let $\mathbb{F}_2$ denote the Galois field with two elements. A Boolean function is a function from the n-dimensional vector space $\mathbb{F}_2^n$ to $\mathbb{F}_2$ and a function from the vector-space $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ is called vectorial Boolean function.

The n-dimensional vector space $\mathbb{F}_2^n$ can also be endowed with the structure of the finite field with 2^n elements, $\mathbb{F}_{2^n}$:
$\mathbb{F}_{2^n} = \mathbb{F}_2[x]/\big(p(x)\big)$ where $p(x)$ is an irreducible polynomial of degree n over $\mathbb{F}_2$. Let α be a root of $p(x)$ in $\mathbb{F}_{2^n}$. Then, fix a basis $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$. Every element $x \in \mathbb{F}_{2^n}$ can be written as $x = c_0 + c_1\alpha + \ldots + c_{n-1}\alpha^{n-1}$ where $(c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_2^n$. This identification gives an isomorphism between $\mathbb{F}_2^n$ and $\mathbb{F}_{2^n}$ and allows us to define Boolean functions over finite fields as well.

For a given Boolean function there exists several representations. We will only give a brief description of these representations for reasons of completeness.

2.1.1 Algebraic Normal Form

Algebraic Normal Form (ANF) is the classical and the most well known representation of Boolean functions. ANF is a multivariate representation. For a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, its Algebraic Normal Form is given in [6] as

$$f(x_1, x_2, \cdots, x_n) = \bigoplus_{I \in \mathcal{P}(N)} a_I \left(\prod_{i \in I} x_i \right) = \bigoplus_{I \in \mathcal{P}(N)} a_I x^I, \tag{2.1}$$

where $\mathcal{P}(N)$ denotes the power set of $N = \{1, \cdots, n\}$. Every coordinate x_i appears in this polynomial with exponents at most 1 since every bit in $\mathbb{F}_2$ equals its own square. This representation belongs to $\mathbb{F}_2[x_1, \cdots, x_n] / ({x_1}^2 \oplus x_1, \cdots, {x_n}^2 \oplus x_n)$.

Another possible representation of this same ANF uses indexation by means of vectors of $\mathbb{F}_2^n$ instead of N :

$$f(x_1, x_2, \cdots, x_n) = \bigoplus_{u \in \mathbb{F}_2^n} a_u x^u, \tag{2.2}$$

where $x_u = \prod_{j=1}^{n} {x_j}^{u_j}$ for which $u_j = 1$ and $a_u \in \mathbb{F}_2$. Algebraic Normal Form exists for every Boolean function f and is unique [6]. The algebraic degree of the Boolean function f denoted by $deg(f)$ is the maximum degree corresponding to a nonzero coefficient:

$$max_{u \in \mathbb{F}_2^n} \{wt(u) : a_u \neq 0\}.$$

As an example, we can represent all Boolean functions $f : \mathbb{F}_2^3 \to \mathbb{F}_2$ in the Algebraic Normal form as

$$f(x_1, x_2, x_3) = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus a_3 x_3 \oplus a_4 x_1 x_2 \oplus a_5 x_1 x_3 \oplus a_6 x_2 x_3 \oplus a_7 x_1 x_2 x_3$$

where $a_i \in \mathbb{F}_2$ for $0 \leq i \leq 7$. If $a_7 \neq 0$, then $deg(f) = 3$. If $a_7 = 0$ and one of a_4, a_5, a_6 is nonzero then $deg(f) = 2$.

2.1.2 Numerical Normal Form

Numerical Normal Form (NNF) [8] is a very similar multivariate representation which takes the coefficients from integers. Any integer-valued mapping f can be uniquely represented as multivariate polynomial over $\mathbb{Z}$:

$$f(x) = \sum_{u \in \mathbb{F}_2^n} \lambda_u x^u, \tag{2.3}$$

where $x_u = \prod_{j=1}^{n} {x_j}^{u_j}$ and $\lambda_u \in \mathbb{Z}$.

The coefficients in the ANF corresponds to the coefficients in NNF reduced to modulo 2. We can switch off from NNF to ANF by using the conversion between binary and integer arithmetic :

$$a \oplus b = a + b - 2ab.$$

Example 2.1. Let $f : \mathbb{F}_2^4 \to \mathbb{F}_2$ and its ANF is given as $f(x_1, x_2, x_3, x_4) = x_1 \oplus x_4 \oplus x_2 x_3 x_4$. NNF of f can be computed as follows:

$$\begin{aligned} f(x_1, x_2, x_3, x_4) &= (x_1 + x_4 - 2x_1 x_4) \oplus x_2 x_3 x_4 \\ &= (x_1 + x_4 - 2x_1 x_4) + (x_2 x_3 x_4) - 2(x_1 + x_4 - 2x_1 x_4)(x_2 x_3 x_4) \\ &= x_1 + x_4 - 2x_1 x_4 - x_2 x_3 x_4 + 2x_1 x_2 x_3 x_4 \end{aligned}$$

2.1.3 Trace Representation and Polynomial Form

Boolean function as a polynomial in one variable $x \in \mathbb{F}_{2^n}$ of the form $f(x) = \sum_{j=0}^{2^n-1} a_j x^j$ where the a_j's are elements of the field. Such function f is Boolean if and only if a_0 and a_{2^n-1} belong to $\mathbb{F}_2$ and $a_{2j} = a_j^2$ for every $j \notin \{0, 2^n - 1\}$ (where $2j$ is taken modulo $2^n - 1$). This leads to a unique representation which we call the *polynomial form*. First, recall that for any positive integers k, and r dividing k, the trace function from $\mathbb{F}_{2^k}$ to $\mathbb{F}_{2^r}$, denoted by Tr_r^k, is the mapping defined for every $x \in \mathbb{F}_{2^k}$ as:

$$Tr_r^k(x) := \sum_{i=0}^{\frac{k}{r}-1} x^{2^{ir}} = x + x^{2^r} + x^{2^{2r}} + \cdots + x^{2^{k-r}}.$$

In particular, the *absolute trace* over $\mathbb{F}_2$ of an element $x \in \mathbb{F}_{2^n}$ is defined as $Tr_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$. Some of the properties of the trace function can be given as:

1. $Tr_1^n(x) = Tr_1^n(x^2)$, for all $x \in \mathbb{F}_{2^n}$.
2. $Tr_r^k(x) = Tr_r^k(x^{2^r})$, for all $x \in \mathbb{F}_{2^k}$.
3. $Tr_1^k(x) = Tr_1^r(Tr_r^k(x))$, for all $x \in \mathbb{F}_{2^k}$.
4. $Tr_r^k(ax + by) = aTr_r^k(x) + bTr_r^k(y)$, for all $a, b \in \mathbb{F}_{2^r}$, $x, y \in \mathbb{F}_{2^k}$.

Now, the polynomial form[41] of a Boolean function defined on $\mathbb{F}_{2^n}$ is the expression of f as

$$f(x) = \sum_{j \in \Gamma_n} Tr_1^{o(j)}(a_j x^j) + \epsilon(1 + x^{2^n-1})$$

where

- Γ_n is the set of integers obtained by choosing one element in each cyclotomic class of 2 modulo $2^n - 1$ (the most usual choice for j is the smallest element in its cyclotomic class, called the coset leader of the class),
- $o(j)$ is the size of the cyclotomic coset of 2 modulo $2^n - 1$ containing j,
- $a_j \in \mathbb{F}_{2^{o(j)}}$,
- $\epsilon = wt(f)$ modulo 2 where $wt(f)$, is the *Hamming weight* of the image vector of f, that is, the cardinality of its support $supp(f) := \{x \in \mathbb{F}_{2^n} \mid f(x) = 1\}$.

The algebraic degree of f is then equal to the maximum 2-weight of an exponent j for which $a_j \neq 0$ if $\epsilon = 0$ and to n if $\epsilon = 1$. Recall that the 2-weight of an integer j denoted by $w_2(j)$ equals the number of 1's in its binary expansion.

Example 2.2. Let $n = 4$, then $f : \mathbb{F}_{2^4} \to \mathbb{F}_2$,

$$f(x) = \sum_{j \in \Gamma_4} Tr_1^{o(j)}(a_j x^j) + \epsilon(1 + x^{15}),$$

C_j : the cyclotomic coset of 2 modulo $2^n - 1 = 15$ containing j,
$C_j = \left\{j, j \cdot 2, j \cdot 2^2, j \cdot 2^3, \ldots, j \cdot 2^{o(j)-1}\right\}$ where $o(j)$ is the smallest positive integer such that $j2^{o(j)} \equiv j \bmod(2^n - 1)$.

The cyclotomic cosets modulo 15 are :
$\mathbf{C_0} = \{0\}$
$\mathbf{C_1} = \{1, 2, 4, 8\}$
$\mathbf{C_3} = \{3, 6, 12, 9\}$
$\mathbf{C_5} = \{5, 10\}$
$\mathbf{C_7} = \{7, 14, 11, 13\}$
We find $\mathbf{\Gamma_4} = \{0, 1, 3, 5, 7\}$, then

$f(x) = Tr_1^{o(1)}(a_1 x^1) + Tr_1^{o(3)}(a_3 x^3) + Tr_1^{o(5)}(a_5 x^5) + Tr_1^{o(7)}(a_7 x^7) + a_0 + \epsilon(1 + x^{15})$;
$f(x) = Tr_1^4(a_1 x) + Tr_1^4(a_3 x^3) + Tr_1^2(a_5 x^5) + Tr_1^4(a_7 x^7) + a_0 + \epsilon(1 + x^{15})$
where $a_1, a_3, a_7 \in \mathbb{F}_{2^4}$, $a_5 \in \mathbb{F}_{2^2}$ and $a_0, \epsilon \in \mathbb{F}_2$.

2.1.4 Bivariate Representation

The *bivariate representation*[38] of Boolean functions makes sense only when n is an even integer. It plays an important role for defining bent functions and is defined by identifying $\mathbb{F}_{2^n}$ (where $n = 2m$) with $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$. Let f be a Boolean function defined on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$. Then, bivariate representation of f can be shown as

$$f(x, y) = \sum_{0 \le i,j \le 2^m - 1} a_{i,j} x^i y^j$$

where $x, y \in \mathbb{F}_{2^m}$. The algebraic degree of f equals $\max_{(i,j)\,|\,a_{i,j} \neq 0}(w_2(i) + w_2(j))$. The function f being Boolean, its bivariate representation can be written in the (non unique) form $f(x, y) = Tr_1^m(P(x, y))$ where $P(x, y)$ is some polynomial in two variables over $\mathbb{F}_{2^m}$.

Throughout the thesis we will use trace representation and bivariate representation.

2.2 Bent and Semi-bent Functions

The classes of bent and semi-bent functions are special subclasses of the so-called plateaued functions [52]. They are actively studied topics because of their important applications in cryptography, coding theory, combinatorics and information theory.

In cryptography, bent and semi-bent functions are very crucial because having low Hadamard transform values makes these functions suitable for construction of cipher elements that are resistant to linear and fast correlation attacks.

Bent functions were first introduced by Rothaus[43] in 1976, but Dillon[20] also studied these functions in his Ph.D. thesis. Bent functions are nice combinatorial objects which have maximum nonlinearity among Boolean functions. A book devoted especially to binary bent functions and containing a complete survey on bent functions is [41]. Another recent book on bent functions which is brings together all known results and constructions is [49]. Also, an interested reader can find open problems on binary bent functions in [7].

Another family, semi-bent functions, also have low Hadamard transform values. First, Chee, Lee and Kim [19] introduced the notion of semi-bent functions in 1994. In fact, Canteaut et al.[3] had previously investigated these functions known as three-valued almost optimal Boolean functions. Semi-bent functions exist for both even and odd n. For even n, semi-bent functions are also called 2-plateaued functions and for odd n, they are named as 1-plateaued functions. These functions have the highest nonlinearity among quadratic Boolean functions. Besides, they are balanced up to the addition of a linear function, and may possess other desired cryptographic properties like propagation criterion of high order, low autocorrelation and resiliency. A survey containing open problems on semi-bent functions can be found in [39].

In order to give the definitions of bent and semi-bent functions, we need to recall the notions such as nonlinearity and Walsh-Hadamard transform.

Let $\mathcal{B}_n$ denote the set of all Boolean functions of n variables and $\mathcal{A}_n$ denote the set of all affine functions (the functions having degree at most 1). The nonlinearity $nl(f)$ of a Boolean function $f \in \mathcal{B}_n$ is defined as

$$nl(f) = min_{g \in \mathcal{A}_n}(d_H(f, g))$$

where $d_H(f, g)$ is the Hamming distance between f and g, i.e.,

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

Nonlinearity can also be expressed by the Walsh-Hadamard transform of f. To explain the relation between nonlinearity and the Walsh-Hadamard transform, we introduce some notations. Let $x = (x_1, x_2, \ldots, x_n)$ and $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ both belong to $\mathbb{F}_2^n$. The usual inner product of x and α is $x \cdot \alpha = x_1\alpha_1 \oplus x_2\alpha_2 \oplus \ldots \oplus x_n\alpha_n$. For a Boolean function f on $\mathbb{F}_2^n$, the Walsh-Hadamard transform of f is the discrete Fourier transform of the sign function $\chi_f := (-1)^f$ of f, whose value at $\alpha \in \mathbb{F}_2^n$ is defined as

$$\widehat{\chi_f}(\alpha) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+\alpha \cdot x}.$$

The identification of the vector space $\mathbb{F}_2^n$ with the finite field $\mathbb{F}_{2^n}$ allows us to choose the isomorphism such that the canonical scalar product " $\cdot$ " in $\mathbb{F}_2^n$ coincides with the

canonical scalar product in $\mathbb{F}_{2^n}$, which is the trace of the product : $x \cdot y = Tr_1^n(xy)$. Then, for a Boolean function $f \in \mathbb{F}_{2^n}$, the Walsh-Hadamard transform of f at $\alpha \in \mathbb{F}_{2^n}$ is

$$\widehat{\chi_f}(\alpha) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+Tr_1^n(\alpha x)}.$$

The set of Walsh transform values of f for every $\alpha \in \mathbb{F}_{2^n}$ is called the *Walsh spectrum* of f.

Hamming weight of a Boolean function $f \in \mathcal{B}_n$ is denoted $wt(f)$ and defined as $wt(f) = \#\{x \in \mathbb{F}_{2^n} \mid f(x) \neq 0\}$. If $wt(f) = 2^{n-1}$, then we say that f is balanced. Obviously, f is balanced if and only if $\widehat{\chi_f}(0) = 0$. Then, by the Walsh transform, the nonlinearity of a Boolean function f can be computed as

$$nl(f) = 2^{n-1} - \frac{1}{2} max_{\alpha \in \mathbb{F}_{2^n}} \left|\widehat{\chi_f}(\alpha)\right|.$$

A Boolean function has higher nonlinearity when the value of the $max_{\alpha \in \mathbb{F}_{2^n}} |\widehat{\chi_f}(\alpha)|$ is lower. Parseval's equality states that $\sum_{\alpha \in \mathbb{F}_{2^n}} \widehat{\chi_f}(\alpha)^2 = 2^{2n}$. The maximum absolute value of Walsh coefficients can be minimized when all coefficients have the same magnitude :

$$\begin{aligned} \sum_{\alpha \in \mathbb{F}_{2^n}} \widehat{\chi_f}(\alpha)^2 &= 2^{2n} \\ 2^n \widehat{\chi_f}(\alpha)^2 &= 2^{2n} \\ |\widehat{\chi_f}(\alpha)| &= 2^{n/2} \end{aligned}$$

Consequently, $nl(f) \leq 2^{n-1} - 2^{n/2-1}$ for any Boolean function f. The functions achieving the upper bound $2^{n-1} - 2^{n/2-1}$ are called *bent* functions, which only exist for even n. One can give another definition of bent functions in terms of Walsh transform values as follows.

Definition 2.1. Let n be an even integer. A Boolean function f on $\mathbb{F}_{2^n}$ is said to be bent if its Walsh transform satisfies $\widehat{\chi_f}(\alpha) = \pm 2^{\frac{n}{2}}$ for all $\alpha \in \mathbb{F}_{2^n}$.

From this definition, we see that Walsh-Hadamard Transform provides a basic characterization for bentness. An efficient technique for computing the Walsh spectrum of a Boolean function is *Fast Walsh Transform*. The complexity of the fast Walsh transform is $\mathcal{O}(2^n n^2)$ bit operations and $\mathcal{O}(2^n n)$ memory [1]. Therefore, for large n values, characterization by Walsh transform is not efficient and hence other characterization and also construction methods should be found.

Properties of bent functions:

- For a bent function f on $\mathbb{F}_{2^n}$, its *dual function* $\widetilde{f}$ is defined as a Boolean function on $\mathbb{F}_{2^n}$ satisfying the equation : $(-1)^{\widetilde{f}(x)} 2^{\frac{n}{2}} = \widehat{\chi_f}(x)$ for all $x \in \mathbb{F}_{2^n}$. The dual $\widetilde{f}$ of a bent function is also bent.

- Algebraic degree of any bent Boolean function on $\mathbb{F}_{2^n}$ is at most $n/2$.
- Bent functions have Walsh transform values $\pm 2^{n/2}$, hence they are not balanced.

Another family, semi-bent functions, also have low Hadamard transform values. First, Chee, Lee and Kim [19] introduced the notion of semi-bent functions in 1994. They are defined both even and odd n values.

Definition 2.2. Let n be an even integer. A Boolean function f on $\mathbb{F}_{2^n}$ is said to be semi-bent if its Walsh transform satisfies $\widehat{\chi_f}(a) \in \{0, \pm 2^{\frac{n+2}{2}}\}$ for all $a \in \mathbb{F}_{2^n}$.

Properties of semi-bent functions:

- Nonlinearity of a semi-bent function is $2^{n-1} - 2^{n-1/2}$ when n is odd and $2^{n-1} - 2^{n/2}$ when n is even. Semi-bent functions have the maximal nonlinearity among balanced plateaued functions (see Definition 2.3 for the definition of plateaued functions).
- Walsh transform of a semi-bent function can take the value 0, hence they are balanced (up to the addition of a linear function).
- Algebraic degree of any semi-bent Boolean function on $\mathbb{F}_{2^n}$ is at most $n/2$.

Bent and semi-bent functions are subclasses of the so-called plateaued functions. The term of plateaued functions has been introduced by Zheng and Zhang [52] in 1999.

Definition 2.3. A Boolean function f on $\mathbb{F}_{2^n}$ is said to be k-*plateaued* if its Walsh transform satisfies $\widehat{\chi_f}(a) \in \{0, \pm 2^{\frac{n+k}{2}}\}$ for all $a \in \mathbb{F}_{2^n}$ and for some fixed k, $0 \leq k \leq n$.

When n is even, bent functions correspond to 0-*plateaued* functions and semi-bent functions correspond to 2-*plateaued* functions.

CHAPTER 3

CHARACTERIZATION AND ENUMERATION OF A CLASS OF QUADRATIC SEMI-BENT BOOLEAN FUNCTIONS

This chapter presents our results on characterization and enumeration of a class of quadratic semi-bent Boolean functions. First we study characterization of these functions and specify the necessary and sufficient conditions for this class of functions to be semi-bent in Section 3.2. Afterwards, we correct some results on bent functions given in [34]. In Section 3.3, a generic method for enumeration is presented and some previous results on enumeration of semi-bent and bent functions are complemented for all n. The work described here is based on the results of the publication [28].

3.1 Introduction

Quadratic Boolean functions are the ones having algebraic degree 2. They can be expressed in terms of trace functions. A quadratic Boolean function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ can be represented

when n is even:

$$f(x) = \sum_{i=1}^{\frac{n}{2}-1} Tr_1^n(c_i x^{1+2^i}) + Tr_1^{n/2}(c_{n/2} x^{1+2^{n/2}}) \tag{3.1}$$

where $c_i \in \mathbb{F}_{2^n}\ \forall i,\ 0 < i < \frac{n}{2}$ and $c_{n/2} \in \mathbb{F}_{2^{n/2}}$,

when n is odd:

$$f(x) = \sum_{i=1}^{\frac{n-1}{2}} Tr_1^n(c_i x^{1+2^i}) \tag{3.2}$$

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

If $f(x)$ is a quadratic Boolean function with $f(0) = 0$, then its rank can be computed by the bilinear form

$$Q_f(x, y) = f(x) + f(y) + f(x + y).$$

For the quadratic form,

$$Ker(f) = Ker(Q_f) = \{x \in \mathbb{F}_{2^n} : Q_f(x, y) = 0, \forall y \in \mathbb{F}_{2^n}\}.$$

If the dimension of $Ker(f)$ is $n - 2h$, that is, rank of $f(x)$ is $2h$, then

$$Q_f(x, y) = 0, \text{ for any } y \in \mathbb{F}_{2^n}$$

has 2^{n-2h} solutions in x.

There is a relation between the rank of quadratic Boolean functions and the distribution of its Walsh-Hadamard transform values. The following theorem gives the distribution of the Walsh-Hadamard transform values of quadratic Boolean functions.

Theorem 3.1. *[24]*
Let $f(x)$ be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ with algebraic degree 2. If the rank of $f(x)$ is $2h$, $1 \leq h \leq n/2$, then the distribution of the Hadamard transform values of $f(x)$ is given by

$$\widehat{\chi_f}(\omega) = \begin{cases} 0, & 2^n - 2^{2h} \quad \textit{times} \\ 2^{n-h}, & 2^{2h-1} + 2^{h-1} \quad \textit{times} \\ -2^{n-h}, & 2^{2h-1} - 2^{h-1} \quad \textit{times}. \end{cases}$$

Corollary 3.2. *A quadratic Boolean function $f(x)$ is semi-bent if and only if*

$$rank(f) = \begin{cases} n - 1, & \textit{if } n \textit{ is odd} \\ n - 2, & \textit{if } n \textit{ is even}. \end{cases}$$

Known quadratic semi-bent functions on $\mathbb{F}_{2^n}$, $n = 2m$:

- $f(x) = Tr_1^n(x^{1+2^i})$, $gcd(m, i) = 1$
- $f(x) = Tr_1^n(\alpha x^{1+2^i})$, $\alpha \in \mathbb{F}_{2^n}^*$, m odd, i even
- $f(x) = Tr_1^n(\alpha x^{1+2^i})$, m odd, i odd, $gcd(m, i) = 1$, $\alpha \in \{x^3, x \in \mathbb{F}_{2^n}^*\}$
- $f(x) = Tr_1^n(\alpha x^{1+2^i})$, m even, i odd, $\alpha \in \{x^3, x \in \mathbb{F}_{2^n}^*\}$
- $f(x) = \sum_{i=1}^{\frac{n}{2}-1} c_i Tr_1^n(x^{1+2^i})$, $c_i \in \mathbb{F}_2$, $gcd(\sum_{i=1}^{\frac{n}{2}-1} c_i(x^i + x^{n-i}), x^n + 1) = x^2 + 1$
- $f(x) = \sum_{i=1}^{\frac{m-1}{2}} Tr_1^n(c_i x^{1+4^i})$, $c_i \in \mathbb{F}_4$, m even, $gcd(\sum_{i=1}^{\frac{m-1}{2}} c_i(x^i + x^{m-i}), x^m + 1) = x + 1$

3.2 Characterization of a Class of Semi-bent Quadratic Boolean Functions

Semi-bent Boolean functions are used to generate maximum length sequences known as m-sequences. [23] used the function $f(x) = Tr_1^n(x^{1+2^i})$ where n is odd and $gcd(i, n) = 1$ to form a family of m-sequences with low cross correlation, namely Gold sequences. Subsequently, [2] proposed a new construction of binary sequences from Gold-like functions, $f(x) = \sum_{i=1}^{\frac{n-1}{2}} Tr_1^n(x^{1+2^i})$, having identical correlation with Gold sequences. Both Gold function and Boztas-Kumar function are quadratic semi-bent functions defined for odd n. In [26, 27], Khoo et al. generalized Boztas-Kumar function to the functions of the form

$$f(x) = \sum_{i=1}^{\frac{n-1}{2}} c_i Tr_1^n(x^{1+2^i}), \quad c_i \in \mathbb{F}_2, \quad n \text{ odd.} \tag{3.3}$$

They proved that $f(x)$ is semi-bent if and only if $gcd(c(x), x^n + 1) = x + 1$ where $c(x) = \sum_{i=1}^{\frac{n-1}{2}} c_i(x^i + x^{n-i})$. [17] generalized Khoo et al.'s results to even n and showed that

$$f(x) = \sum_{i=1}^{\frac{n}{2}-1} c_i Tr_1^n(x^{1+2^i}), \quad c_i \in \mathbb{F}_2, \quad n \text{ even} \tag{3.4}$$

is semi-bent if and only if $gcd(c(x), x^n+1) = x^2+1$ where $c(x) = \sum_{i=1}^{\frac{n}{2}-1} c_i(x^i + x^{n-i})$. They also examined the conditions on the choice of c_i for odd n leading to new families of quadratic semi-bent functions consisting of three and four trace terms. Recently, [35] presented the number of semi-bent functions of the form (3.4) for $n = 2m$, m odd.

On the other hand, by combining the construction methods proposed by [26, 27, 50], [34] studied a new class of bent functions of the form

$$f(x) = \sum_{i=1}^{\frac{n}{2}-1} c_i Tr_1^n(x^{1+2^i}) + Tr_1^{n/2}(x^{1+2^{n/2}}),\ c_i \in \mathbb{F}_2,\ i = 1, 2, \ldots, n/2 - 1. \tag{3.5}$$

They proved that $f(x)$ is a bent function if and only if $gcd(c(x), x^n + 1) = 1$ where $c(x) = \sum_{i=1}^{\frac{n}{2}-1} c_i(x^i + x^{n-i}) + x^{n/2}$.

[51] presented the construction of all quadratic bent functions of the form (3.5) for $n = 2^v p^r$ with $v, r \geq 1$ by giving necessary and sufficient conditions on c_i's and gave enumeration results for $n = 2^v p$ and $n = 2^v p^2$ for some special prime p. After that, [25] improved the enumeration results for $n = 2^v p^r$.

In this section, we consider the semi-bentness of quadratic Boolean functions for even n of the form

$$f(x) = \sum_{i=1}^{\frac{n}{2}-1} c_i Tr_1^n(x^{1+2^i}) + Tr_1^{n/2}(x^{1+2^{n/2}}), \quad c_i \in \mathbb{F}_2, \quad x \in \mathbb{F}_{2^n} \tag{3.6}$$

and show that f is semi-bent if and only if $6 \mid n$ and $gcd(c(x), x^n + 1) = x^2 + x + 1$, where $c(x) = \sum_{i=1}^{\frac{n}{2}-1} c_i(x^i + x^{n-i}) + x^{n/2}$. Furthermore, we present a generic enumeration method for certain classes of semi-bent and bent functions. Using this method, we give the number of semi-bent functions of the form (3.6) and complement the earlier enumeration results for semi-bent functions given by [47] and the enumeration results for bent functions given by [25] and [46]. The interested reader is referred to [36, 37, 39] containing surveys devoted to semi-bent and bent functions. In this section, we examine a class of semi-bent quadratic functions and give a characterization for semi-bentness. These are stated in the following theorem.

Theorem 3.3. *Let n be an even integer. Then*

$$f(x) = \sum_{i=1}^{\frac{n}{2}-1} c_i Tr_1^n(x^{1+2^i}) + Tr_1^{n/2}(x^{1+2^{n/2}}), \quad c_i \in \mathbb{F}_2, \quad x \in \mathbb{F}_{2^n},$$

is a semi-bent function if and only if $6 \mid n$ and $gcd(c(x), x^n + 1) = x^2 + x + 1$, where $c(x) = \sum_{i=1}^{\frac{n}{2}-1} c_i(x^i + x^{n-i}) + x^{n/2}$.

Proof. In order to prove semi-bentness of $f(x)$, we will examine $Ker(Q_f)$.

$$\begin{aligned}
Q_f(x,y) &= f(x) + f(y) + f(x+y) \\
&= \sum_{i=1}^{\frac{n}{2}-1} c_i Tr_1^n(x^{1+2^i}) + Tr_1^{n/2}(x^{1+2^{n/2}}) + \sum_{i=1}^{\frac{n}{2}-1} c_i Tr_1^n(y^{1+2^i}) + Tr_1^{n/2}(y^{1+2^{n/2}}) \\
&\quad + \sum_{i=1}^{\frac{n}{2}-1} c_i Tr_1^n((x+y)^{1+2^i}) + Tr_1^{n/2}((x+y)^{1+2^{n/2}}) \\
&= \sum_{i=1}^{\frac{n}{2}-1} c_i Tr_1^n(xy^{2^i} + x^{2^i}y) + Tr_1^{n/2}(xy^{2^{n/2}} + x^{2^{n/2}}y) \\
&= \sum_{i=1}^{\frac{n}{2}-1} c_i Tr_1^n\left(x\left(y^{2^i} + y^{2^{n-i}}\right)\right) + Tr_1^{n/2}\left(Tr_{n/2}^n\left(xy^{2^{n/2}}\right)\right) \\
&= \sum_{i=1}^{\frac{n}{2}-1} c_i Tr_1^n\left(x\left(y^{2^i} + y^{2^{n-i}}\right)\right) + Tr_1^n(xy^{2^{n/2}}) \\
&= Tr_1^n\left[x\left(\sum_{i=1}^{\frac{n}{2}-1} c_i\left(y^{2^i} + y^{2^{n-i}}\right) + y^{2^{n/2}}\right)\right] \\
&= Tr_1^n\left(xL\left(y\right)\right)
\end{aligned}$$

where $L(y) = \sum_{i=1}^{\frac{n}{2}-1} c_i\left(y^{2^i} + y^{2^{n-i}}\right) + y^{2^{n/2}}$. By Corollary 3.2, we know that $f(x)$ is semi-bent if and only if $rank(f) = n - 2$ which means $dim(Ker(Q_f)) = 2$.

Now,

$$Ker(Q_f) = \left\{ x \in \mathbb{F}_{2^n} | \sum_{i=1}^{\frac{n}{2}-1} c_i \left(x^{2^i} + x^{2^{n-i}} \right) + x^{2^{n/2}} = 0 \right\} = Ker\left(L(x)\right)$$

In order to prove that $dim(Ker(Q_f)) = 2$, we need to show that $L(x) = 0$ has 4 solutions. By [33, Defn. 3.58], the polynomials

$$l(x) = \sum_{i=0}^{n} a_i x^i \text{ and } L(x) = \sum_{i=0}^{n} a_i x^{q^i}$$

over $\mathbb{F}_{q^m}$ are called q-associates of each other. Then, one can define *2-associate* of $L(x)$ by $c(x) = \sum_{i=1}^{\frac{n}{2}-1} c_i(x^i + x^{n-i}) + x^{n/2}$. Hence, by [33, Thm. 3.62],

$$deg\left(gcd\left(L(x), x^{2^n} + x\right)\right) = 4$$

if and only if

$$deg\left(gcd\left(c(x), x^n + 1\right)\right) = 2.$$

As $x^n + 1$ is not divisible by x, $gcd(c(x), x^n + 1)$ can be either $x^2 + 1$ or $x^2 + x + 1$. However, $x^2 + 1$ does not divide $c(x) = \sum_{i=1}^{\frac{n}{2}-1} c_i \left(x^i + x^{n-i}\right) + x^{n/2}$ since 1 is a not root of $c(x)$. Therefore, $f(x)$ is semi-bent if and only if $gcd(c(x), x^n + 1) = x^2 + x + 1$. Also, we know that $(x+1)(x^2+x+1) \mid (x^{3k}+1)$, $k \geq 1$ an integer. So, (x^2+x+1) divides $x^n + 1$ when $3 \mid n$, but since in our case n is even, we should have $6 \mid n$.

□

Corollary 3.4. *Let $n = 2m$ be an even integer and $f_i(x)$ be the function*

$$f_i(x) = Tr_1^n(x^{1+2^i}) + Tr_1^m(x^{1+2^m}), \quad 1 \leq i \leq m-1. \tag{3.7}$$

Then, f_i is semi-bent if and only if $6 \mid n$, $(m-i)$ is odd and $gcd(m, i) = 1$.

Proof. By Theorem 3.3, f_i is semi-bent if and only if $gcd(c(x), x^n + 1) = x^2 + x + 1$ where $c(x) = x^i + x^{n-i} + x^m$. Let

$$\begin{aligned} g(x) &= gcd\left(x^i + x^{n-i} + x^m, x^n + 1\right) \\ &= gcd\left(x^i\left(1 + x^{m-i} + x^{2(m-i)}\right), x^n + 1\right) \\ &= gcd\left(\left(1 + x^{m-i} + x^{2(m-i)}\right), x^n + 1\right) \end{aligned}$$

Since $gcd(1 + x^{m-i}, 1 + x^{m-i} + x^{2(m-i)}) = 1$,

$$\begin{aligned} g(x) &= gcd\left(\left(1 + x^{m-i} + x^{2(m-i)}\right), x^n + 1\right) \\ &= \frac{gcd\left(\left(x^{3(m-i)} + 1\right), x^n + 1\right)}{gcd\left(\left(x^{m-i} + 1\right), x^n + 1\right)} \\ &= \frac{x^{gcd(3(m-i),n)} + 1}{x^{gcd(m-i,n)} + 1}. \end{aligned}$$

Let $gcd\,(m-i,n) = d$. Then, $gcd\,(3\,(m-i)\,,n)$ is either d or $3d$. However, if $gcd\,(3\,(m-i)\,,n) = d$, then

$$\begin{aligned} g(x) &= \frac{x^{gcd(3(m-i),n)}+1}{x^{gcd(m-i,n)}+1} \\ &= \frac{x^d+1}{x^d+1} \\ &= 1 \end{aligned}$$

in which case f cannot be semi-bent. Hence, if $gcd\,(3\,(m-i)\,,n) = 3d$, then we have

$$\begin{aligned} g(x) &= \frac{x^{gcd(3(m-i),n)}+1}{x^{gcd(m-i,n)}+1} \\ &= \frac{x^{3d}+1}{x^d+1} \\ &= x^{2d}+x^d+1. \end{aligned}$$

In this case, $g(x) = x^2+x+1$ if and only if $d = 1$ which means $gcd\,(m-i,n) = 1$ and $gcd\,(3\,(m-i)\,,n) = 3$. These conditions imply that $3 \mid n$, but since n is even, we have $6 \mid n$. Also, $gcd\,(m-i,n) = gcd\,(m-i,2m) = 1$ shows that $m-i$ is odd. Then, we have $gcd\,(m-i,2m) = gcd\,(m-i,2i) = gcd\,(m,i)$.

□

Remark 3.1. If $\frac{n}{gcd(n,i)}$ is even for $1 \le i < n/2$, then the Gold function $Tr_1^n(x^{1+2^i})$ is bent. Also, $Tr_1^m(x^{1+2^m})$ is a Niho bent function. However, since the restriction of $Tr_1^n(x^{1+2^i})$ to the spread $\{u\mathbb{F}_{2^m}; u \in U\}$ where U is the multiplicative group $\left\{u \in \mathbb{F}_{2^n}; u^{2^m+1} = 1\right\}$ is not constant, the function f_i in Corollary 3.4 is not involved in [9, Thm.1].

3.2.1 Correction of Some Previous Results in [34]

In Section 3.2, we investigated semi-bentness of the functions in the following form

$$f_i(x) = Tr_1^n(x^{1+2^i}) + Tr_1^{n/2}(x^{1+2^{n/2}}), \quad 1 \le i \le n/2-1$$

as a corollary to Theorem 3.3. Bentness of the functions having exactly the same form were considered by [34]. They gave a characterization for bentness and stated the following corollary.

Corollary 3.5. *[34, Cor. 5] Let $n = 2m$. The function*

$$f(x) = Tr_1^n(x^{1+2^i}) + Tr_1^m(x^{1+2^m}), \quad 1 \le i \le m-1$$

is a bent function if and only if $gcd(3i,m) = 1$.

However, it is easy to check that this condition is not sufficient and may led to false positives. [25] pointed out that the result in [34] is not quite right and indicated that when n is a power of 2, f is bent. But, for the other values of n, the assertion given in [34, Cor. 5] is still not completely right. In the following remark, we give the necessary and sufficient condition for f to be bent for all even n values.

Remark 3.2. Let $n = 2m$ and m_0 be the maximum odd positive divisor of m. Then, the function

$$f(x) = Tr_1^n(x^{1+2^i}) + Tr_1^m(x^{1+2^m}), \quad 1 \leq i \leq m-1$$

is a bent function if and only if $gcd(i, m_0) = gcd(3i, m_0)$.

Proof. We know that f is bent if and only if $gcd(c(x), x^n + 1) = 1$ where $c(x) = x^i + x^{n-i} + x^m$ [34]. Now, $gcd(c(x), x^n+1) = gcd(x^i c(x), x^n+1)$ and $gcd(x^i c(x), x^n+1) = 1$ if and only if $gcd(x^i c(x), x^{m_0} + 1) = 1$.

$$\begin{aligned} x^i c(x) \; mod \, (x^{m_0} + 1) &\equiv \left(x^n + x^{m+i} + x^{2i}\right) mod \, (x^{m_0} + 1) \\ &\equiv \left(1 + x^i + x^{2i}\right) mod \, (x^{m_0} + 1) \, . \end{aligned}$$

$$\begin{aligned} gcd\left(1 + x^i + x^{2i}, x^{m_0} + 1\right) &= \frac{gcd\left(x^{3i} + 1, x^{m_0} + 1\right)}{gcd\left(x^i + 1, x^{m_0} + 1\right)} \\ &= \frac{x^{gcd(3i, m_0)} + 1}{x^{gcd(i, m_0)} + 1} \end{aligned}$$

We have $gcd(c(x), x^n + 1) = 1$ if and only if $\frac{x^{gcd(3i,m_0)}+1}{x^{gcd(i,m_0)}+1} = 1$, i.e., $gcd(i, m_0) = gcd(3i, m_0)$. □

As an example, for $m = 6$ and $i = 3$, $f(x) = Tr_1^{12}(x^9) + Tr_1^6(x^{65})$ is a bent function. However, Cor. 5 of [34] implies that it is not bent since $gcd(3i, m) \neq 1$.

Moreover, similar case applies to Corollary 6 of [34] as it shares the same miscalculation with Corollary 5 of [34]. In the following, [34, Cor.6] is stated as given in the paper.

Corollary 3.6. *[34, Cor. 6] Let $n = 2m$,*

$$f(x) = Tr_1^n\left(x^{1+2^1} + x^{1+2^2} + \cdots + x^{1+2^{i-1}} + x^{1+2^{i+1}} + \cdots + x^{1+2^{m-1}}\right) + Tr_1^m(x^{1+2^m})$$

on $\mathbb{F}_{2^n}$, i.e., f consists of all but one trace term i. Then f is a bent function if and only if $gcd(3i, m) = 1$.

We give the corrected characterization for these functions to be bent as follows.

Remark 3.3. Let $n = 2m$ and m_0 be the maximum odd positive divisor of m. Then, the function

$$f(x) = Tr_1^n \left(x^{1+2^1} + x^{1+2^2} + \cdots + x^{1+2^{i-1}} + x^{1+2^{i+1}} + \cdots + x^{1+2^{m-1}} \right) + Tr_1^m(x^{1+2^m})$$

is bent if and only if $gcd(i, m_0) = gcd(3i, m_0)$.

3.3 Enumeration

In this section, we present a general method to obtain the number of quadratic semi-bent and bent functions in certain classes. The main idea is to modify and extend the idea employed in [21, 22]. This method was also used in [35] rather directly. For various classes of quadratic semi-bent or bent functions, the characterization of semi-bent or bent functions involves extra conditions. These extra conditions do not allow the idea of [21, 22] to apply directly in many cases. However, we could modify and extend the idea of [21, 22] in all the classes we worked in order to obtain correct enumeration results for all n. These results give the exact enumeration result for the semi-bent functions studied in Theorem 3.3, and moreover they complement partial enumeration results obtained by [25], [46] and [47].

We believe in that by modifying the idea of [21, 22] accordingly, it should be possible to obtain exact enumeration results for special s-plateaued functions in various classes of quadratic functions. Therefore, we introduce our rather generic method in detail in Section 3.3.1 which leads to Theorem 3.14. We apply this method in Section 3.3.2 to complement the partial enumeration results of [25], [46] and [47].

3.3.1 A Generic Method for Enumeration

We first introduce some necessary definitions and notations.

Definition 3.1. The reciprocal $f^*(x)$ of a polynomial $f(x)$ of degree n is defined by $f^*(x) = x^n f\left(\frac{1}{x}\right)$. A polynomial is called self-reciprocal if $f^*(x) = f(x)$.

Some properties of self-reciprocal polynomials which will be used throughout this section are stated in the following lemma.

Lemma 3.7. *Let $f \in \mathbb{F}_q[x]$.*

(i) If f is self-reciprocal and $g \in \mathbb{F}_q[x]$, then fg is self-reciprocal if and only if g is self-reciprocal.

(ii) If f, g are self-reciprocal polynomials, then $gcd\,(f, g)$ is also self-reciprocal.

Proof. (i) If f is a self-reciprocal polynomial of degree s, then by definition we have $x^s \cdot f\left(\frac{1}{x}\right) = f(x)$. Let $deg(g) = t$. Reciprocal of fg is equal to

$$\begin{aligned} x^{s+t} \cdot fg\left(\frac{1}{x}\right) &= x^s \cdot x^t \cdot f\left(\frac{1}{x}\right) \cdot g\left(\frac{1}{x}\right) \\ &= f(x) \cdot x^t \cdot g\left(\frac{1}{x}\right) \\ &= f(x) \cdot g(x) \\ &= fg(x) \end{aligned}$$

if and only if $x^t \cdot g\left(\frac{1}{x}\right) = g(x)$, i.e., g is self-reciprocal.

(ii) Let f, g are self-reciprocal polynomials and $gcd(f, g) = d$. We know that if α is a nonzero root of f, then α^{-1} is also a root of f. Assume that α_i, $1 \leq i \leq r$, are common roots of f and g. Then, since f and g are self-reciprocal polynomials, α_i^{-1}, $1 \leq i \leq r$, are also roots of f and g. Since d is the greatest common divisor of f and g, α_i and α_i^{-1}, $1 \leq i \leq r$, are roots of d. Hence, d is self-reciprocal.

□

For a monic polynomial $f \in \mathbb{F}_q[x]$ with $deg(f) \geq 1$, we define the following.

$\mathcal{S} := \{f \in \mathbb{F}_q[x] : f \text{ is monic, self-reciprocal and } f(1) \neq 0\}$.

For $f, d \in \mathcal{S}$ and k a nonnegative even integer,

$\mathcal{C}_k(f) := \{c \in \mathcal{S} : deg(c) \leq deg(f) + k\}$,

$\mathcal{R}_k(f) := \{h \in \mathcal{C}_k(f) : gcd(h, f) = 1\}$,

$\phi_k(f) := |\mathcal{R}_k(f)|$,

$\mathcal{T}_k(f, d) := \{h \in \mathcal{C}_k(f) : gcd(h, f) = d\}$.

Note that $\mathcal{R}_k(f) = \mathcal{T}_k(f, 1)$.

Our aim is to derive a general formula for $\phi_k(f)$.

Remark 3.4. One of the differences of our method with the methods of [21, 22] and [35] is already apparent at this point. Because of the extra conditions of semi-bentness in the class of Theorem 3.3, we need to introduce and study $\phi_k(f)$ for all integers $k \geq 0$. It was enough to study $\phi_k(f)$ only for $k = 0$ in [21, 22] and [35].

We begin with the following lemma.

Lemma 3.8. *Let $f \in \mathcal{S}$ and k be a nonnegative even integer. Then,*

$$|\mathcal{C}_k(f)| = q^{\frac{deg(f)+k}{2}}.$$

Proof. First note that $\mathcal{C}_k(f) = \mathcal{C}_{k+deg(f)}(1)$. Let $u = \frac{deg(f)+k}{2}$. Then,

$$\left|\mathcal{C}_{k+deg(f)}(1)\right| = 1 + (q-1) + q(q-1) + \cdots + q^{u-1}(q-1) = q^u.$$

□

Lemma 3.9. *Let $f \in \mathcal{S}$ and k be a nonnegative even integer. Then,*

$$\mathcal{C}_k(f) = \bigsqcup_{d|f} \mathcal{T}_k(f,d)$$

where the disjoint union is taken over all polynomials $d \in \mathcal{S}$ with $d \mid f$.

Proof. For every d dividing f, $\mathcal{T}_k(f,d) \subseteq \mathcal{C}_k(f)$ by definition of $\mathcal{T}_k(f,d)$. Hence, it follows that $\bigcup_{d|f} \mathcal{T}_k(f,d) \subseteq \mathcal{C}_k(f)$. Conversely, let $h \in \mathcal{C}_k(f)$ and $d = gcd\,(h,f)$. Now, $f \in \mathcal{S}$ and by definition of $\mathcal{C}_k(f)$, $h \in \mathcal{S}$. From Lemma 3.7, $d \in \mathcal{S}$ and clearly $d \mid f$. Hence, $\mathcal{C}_k(f) \subseteq \bigcup_{d|f} \mathcal{T}_k(f,d)$. If $d_1 \neq d_2$ with $d_1 \mid f$ and $d_2 \mid f$, then it is obvious that $\mathcal{T}_k(f,d_1) \neq \mathcal{T}_k(f,d_2)$.

□

Lemma 3.10. *Let $f, d \in \mathcal{S}$, $d \mid f$ and k be a nonnegative even integer. Then,*

$$|\mathcal{T}_k(f,d)| = \left|\mathcal{R}_k\left(\frac{f}{d}\right)\right| = \phi_k\left(\frac{f}{d}\right).$$

Proof. To complete the proof, we need to show that there is a one-to-one correspondence between $\mathcal{T}_k(f,d)$ and $\mathcal{R}_k\left(\frac{f}{d}\right)$. First, let us define a map

$$\begin{aligned} \Psi_1 : \mathcal{T}_k(f,d) &\to \mathcal{R}_k\left(\frac{f}{d}\right) \\ h &\mapsto h_1. \end{aligned}$$

$h \in \mathcal{T}_k(f,d)$ means $gcd(f,h) = d$. We can write $h = dh_1$ and $f = df_1$ for some h_1 and f_1. Then, $h_1, f_1 \in \mathcal{S}$ by Lemma 3.7 and $gcd(f_1,h_1) = 1$. Hence, $h_1 \in \mathcal{R}_k\,(f_1)$ as $h_1 \in \mathcal{C}_k\,(f_1)$ and $deg\,(h_1) \leq deg\,(f_1) + k$. Now, define another map

$$\begin{aligned} \Psi_2 : \mathcal{R}_k\left(\frac{f}{d}\right) &\to \mathcal{T}_k(f,d) \\ h_1 &\mapsto h. \end{aligned}$$

$h_1 \in \mathcal{R}_k\left(\frac{f}{d}\right)$ implies by definition that $h_1 \in \mathcal{C}_k\left(\frac{f}{d}\right)$ and $gcd\left(\frac{f}{d}, h_1\right) = 1$. Then, $gcd\left(f, dh_1\right) = d$ and $dh_1 = h \in \mathcal{T}_k(f, d)$. □

Thanks to Lemma 3.7, Lemma 3.8 and Lemma 3.10, one can prove the following corollary.

Corollary 3.11. *Let $f \in \mathcal{S}$ and k be a nonnegative integer. Then,*

$$q^{\frac{deg(f)+k}{2}} = |\mathcal{C}_k\left(f\right)| = \sum_{d|f} \phi_k(d)$$

where the summation is over all $d \in \mathcal{S}$ with $d \mid f$.

Lemma 3.12. *Let $f \in \mathcal{S}$, r is a monic irreducible polynomial dividing f and r^* is the reciprocal of r such that $r^* \neq r$. Then, rr^* divides f.*

Let $f \in \mathcal{S}$ and $deg(f) \geq 1$. The unique factorization of f is as follows:

$$f = g_1^{e_1} g_2^{e_2} \dots g_s^{e_s} \left[h_1^{f_1} h_2^{f_2} \dots h_t^{f_t}\right] \left[h_1^{*f_1} h_2^{*f_2} \dots h_t^{*f_t}\right]$$

where $s \geq 0$, $t \geq 0$, $e_1, \dots, e_s \geq 1$, $f_1, \dots, f_t \geq 1$, $g_1, g_2, \dots g_s$ are distinct, monic, self-reciprocal, irreducible polynomials, h_i, h_i^* are distinct, monic, irreducible polynomials for $1 \leq i \leq t$ and h_i^* is the reciprocal polynomial of h_i.

Now, we define the Möbius function μ on the set of monic, self-reciprocal polynomials from $\mathbb{F}_q[x]$ as follows. For $f \in \mathcal{S}$ with $deg\left(f\right) \geq 1$, we define

$$\mu(f) = \begin{cases} 1 & \text{if } f = 1, \\ (-1)^{s+t} & \text{if } deg(f) \geq 1 \text{ and } e_1 = \dots = e_s = f_1 = \dots = f_t = 1, \\ 0 & \text{if } deg(f) \geq 1 \text{ and } e_i \geq 2 \text{ or } f_j \geq 2. \end{cases}$$

An argument similar to that for the classical Möbius function on the set of positive integers [33, Lemma 3.23] implies that for $f \in \mathcal{S}$, we have

$$\sum_{d|f} \mu(d) = \begin{cases} 1 & \text{if } f = 1, \\ 0 & \text{otherwise.} \end{cases}$$

In the following lemma, we give the general formula for $\phi_k(f)$.

Lemma 3.13. *Let $f \in \mathcal{S}$, $k = 2k_1$ is a nonnegative even integer. Then,*

$$\phi_k(f) = q^{k_1} \sum_{d|f} \mu(d) q^{\frac{deg(f)-deg(d)}{2}}$$

where the summation is over all $d \in \mathcal{S}$ with $d \mid f$.

Proof. Consider right hand side:

$$\begin{aligned} q^{k_1}\sum_{d|f}\mu(d)\,q^{\frac{deg(f)-deg(d)}{2}} &= q^{k_1}\sum_{d|f}\mu\left(\frac{f}{d}\right)q^{\frac{deg(f)-deg(f/d)}{2}} \\ &= \sum_{d|f}\mu\left(\frac{f}{d}\right)q^{\frac{deg(d)}{2}+k_1} \\ &= \sum_{d|f}\mu\left(\frac{f}{d}\right)\sum_{d_1|d}\phi_k(d_1), \text{ by Corollary 3.11} \\ &= \sum_{d_1|f}\phi_k(d_1)\sum_{g|\frac{f}{d_1}}\mu(g). \end{aligned}$$

For $d_1 \mid f$, we have

$$\sum_{g|\frac{f}{d_1}}\mu(g) = \begin{cases} 1 & \text{if } f = d_1, \\ 0 & \text{otherwise.} \end{cases}$$

Hence, $q^{k_1}\sum_{d|f}\mu(d)q^{\frac{deg(f)-deg(d)}{2}} = \phi_k(f)$. □

We now focus on the case $p = 2$. Our aim is to find the number of $c(x)$ such that $gcd\,(c(x), x^n+1) = x^2+x+1$, where $c(x) = \sum_{i=1}^{\frac{n}{2}-1} c_i(x^i + x^{n-i}) + x^{n/2}$, $n = 2m$ and $6 \mid n$. Let $c(x) = x \cdot \widetilde{c}(x)$ and

$$\mathcal{N} = \#\left\{c(x) : gcd\,(c(x), x^n+1) = x^2+x+1\right\}.$$

It is obvious that $\widetilde{c}(x) \in \mathcal{S}$ and

$$\mathcal{N} = \#\left\{\widetilde{c}(x) : gcd\,(\widetilde{c}(x), x^n+1) = x^2+x+1\right\}.$$

We can write $x^n + 1 = (1+x)^e \cdot f(x)$ where e is the greatest integer such that $gcd\,(f(x), x+1) = 1$. Note that $f \in \mathcal{S}$ and $e = 2e_1$ with $e_1 \geq 1$ since n is even. Now, $deg\,(f) = 2m-e \leq 2m-2$ and $deg\,(\widetilde{c}) \leq 2m-2$. Set $k = 2m-2-(2m-e) = e-2$.

$$\begin{aligned} \mathcal{N} &= \#\left\{\widetilde{c}(x) \in \mathcal{S} : deg\,(\widetilde{c}) \leq deg\,(f)+k, gcd\,(\widetilde{c}, f) = x^2+x+1\right\} \\ &= \left|\mathcal{T}_k\left(f, 1+x+x^2\right)\right|. \end{aligned}$$

Then, by Lemma 3.10 we get $|\mathcal{T}_k\,(f, 1+x+x^2)| = \phi_k\left(\frac{f}{1+x+x^2}\right)$. Finally, using Lemma3.13, we obtain the number of semi-bent functions of the form (3.6) as stated in the next theorem.

Theorem 3.14. *Let $n = 2m$ and $x^n + 1 = (1+x)^e \cdot f(x)$ where f is a monic, self-reciprocal polynomial and e is the greatest integer such that $f(1) \neq 0$. Then, the number of semi-bent functions given in Theorem 3.3 is equal to*

$$\mathcal{N} = 2^{\frac{e}{2}-1}\sum_{d|\frac{f}{1+x+x^2}}\mu(d)\,2^{\frac{deg(f)-deg(d)-2}{2}},$$

where the summation is over all monic, self-reciprocal polynomials d dividing $\frac{f}{1+x+x^2}$.

The following table demonstrates the number of these semi-bent functions.

Table 3.1: Number of semi-bent quadratic functions given in Theorem 3.3

n	# functions	n	# functions
6	1	36	28672
12	8	42	225792
18	56	48	2097152
24	512	54	14651392
30	2880	60	94371840

Example 3.1. As an application of Theorem 3.14, let us find the number of semi-bent functions given in Theorem 3.3 for $n = 18$ and $n = 24$.

For $n = 18$, we have

$$x^{18} + 1 = (x + 1)^2(x^2 + x + 1)^2(x^6 + x^3 + 1)^2.$$

Here $e = 2$, $f(x) = (x^2 + x + 1)^2(x^6 + x^3 + 1)^2$ and $deg(f) = 16$. Therefore, $d \in \{1, x^2 + x + 1, x^6 + x^3 + 1, (x^6 + x^3 + 1)^2, (x^2 + x + 1)(x^6 + x^3 + 1), (x^2 + x + 1)(x^6 + x^3 + 1)^2\}$. By definition of the Möbius function μ on the set of monic, self-reciprocal polynomials, we have $\mu\left((x^6 + x^3 + 1)^2\right) = 0$ and $\mu\left((x^2 + x + 1)(x^6 + x^3 + 1)^2\right) = 0$. Hence, there is no need to write them in the following formula.

$$\begin{aligned}
\mathcal{N} &= 2^{\frac{e}{2}-1} \sum_{d \mid \frac{f}{1+x+x^2}} \mu(d)\, 2^{\frac{deg(f)-deg(d)-2}{2}} \\
&= 2^0 \sum_{d \mid (x^2+x+1)(x^6+x^3+1)^2} \mu(d)\, 2^{\frac{14-deg(d)}{2}} \\
&= \mu(1)2^7 + \mu(x^2 + x + 1)2^6 + \mu(x^6 + x^3 + 1)2^4 \\
&+ \mu\left((x^2 + x + 1)(x^6 + x^3 + 1)\right) 2^3 \\
&= 2^7 - 2^6 - 2^4 + 2^3 = 56.
\end{aligned}$$

For $n = 24$, we have

$$x^{24} + 1 = (x + 1)^8(x^2 + x + 1)^8.$$

Here $e = 8$, $f(x) = (x^2 + x + 1)^8$ and $deg(f) = 16$. Therefore,
$d \in \{(x^2 + x + 1)^i, 0 \leq i \leq 7\}$ and for $d = (x^2 + x + 1)^i$ where $i \geq 2$, $\mu(d) = 0$.

$$\begin{aligned}
\mathcal{N} &= 2^{\frac{e}{2}-1} \sum_{d \mid \frac{f}{1+x+x^2}} \mu(d)\, 2^{\frac{deg(f)-deg(d)-2}{2}} \\
&= 2^3 \sum_{d \mid (x^2+x+1)^7} \mu(d)\, 2^{\frac{14-deg(d)}{2}} \\
&= 2^3 \left[\mu(1) \cdot 2^7 + \mu(x^2 + x + 1) \cdot 2^6\right] \\
&= 2^3(2^7 - 2^6) = 512.
\end{aligned}$$

3.3.2 Complementing Some Partial Enumeration Results

In this section, we complement some earlier partial enumeration results on semi-bent and bent functions. As a reminder, we first state the original results as given in the papers and then present our results.

Tang et al.[47] proposed a new class of semi-bent quadratic Boolean functions of the form

$$f(x) = \sum_{i=1}^{\lfloor \frac{m-1}{2} \rfloor} Tr_1^n(c_i x^{1+4^i}), \quad c_i \in \mathbb{F}_4,\ x \in \mathbb{F}_{2^n},\ n = 2m. \tag{3.8}$$

They characterized f as a semi-bent function if and only if $gcd(c(x), x^m + 1) = x + 1$ where $c(x) = \sum_{i=1}^{\lfloor \frac{m-1}{2} \rfloor} c_i \left(x^i + x^{m-i}\right)$ and they noted that for m even, f is not semi-bent. They also gave a formula on the number of functions of the form (3.8) for $n = 2p^r$ where $r \geq 1$, p is not a Wieferich prime, $p \equiv 3 \bmod 4$, $ord_p(2) = p - 1$ or $\frac{p-1}{2}$. Using the method given in Section 3.3.1, it is possible to extend this result for all $n = 2m$ with m odd since the number of semi-bent functions for m even is zero. This result is stated in Theorem 3.15.

Theorem 3.15. *Let $n = 2m$ with m odd and $x^m + 1 = (x + 1) \cdot f(x)$. The number of semi-bent functions of the form (3.8) is*

$$\mathcal{N}_s = \sum_{d|f} \mu(d) \left[4^{\lfloor \frac{deg(f) - deg(d)}{2} \rfloor} - 1\right].$$

Proof. Let $n = 2m$ with m odd and $x^m + 1 = (x + 1) \cdot f(x)$.

$$\begin{aligned} \mathcal{N}_s &= \#\{c(x) : gcd(c(x), x^m + 1) = x + 1\} \\ &= \#\{\widetilde{c}(x) : gcd(\widetilde{c}(x), f(x)) = 1\} \end{aligned}$$

where $\widetilde{c}(x) = \frac{c(x)}{x(x+1)}$. Hence, $deg(\widetilde{c}) \leq deg(f) - 2$.

Now, we will modify the definitions in Section 3.3.1 according to this case. For a monic polynomial $f \in \mathbb{F}_q[x]$ with $deg(f) \geq 1$,

$\mathcal{S} := \{f \in \mathbb{F}_q[x] : f \text{ is monic, self-reciprocal}\}$.

For $f, d \in \mathcal{S}$,

$\mathcal{C}_{-2}(2, f) := \{c \in \mathcal{S} : deg(c) \leq deg(f) - 2,\ deg(c) : even\}$,

$\mathcal{R}_{-2}(2, f) := \{h \in \mathcal{C}_{-2}(2, f) : gcd(h, f) = 1\}$,

$\phi_{-2}(2,f) := |\mathcal{R}_{-2}(2,f)|$,

$\mathcal{T}_{-2}(2,f,d) := \{h \in \mathcal{C}_{-2}(2,f) : gcd\,(h,f) = d\}$.

Following the steps in Section 3.3.1, we have

$$|\mathcal{T}_{-2}(2,f,d)| = \left|\mathcal{R}_{-2}\left(2,\frac{f}{d}\right)\right| = \phi_{-2}\left(2,\frac{f}{d}\right), \quad \text{and}$$

$$\frac{q^{\lfloor \frac{deg(f)}{2} \rfloor} - 1}{q-1} = |\mathcal{C}_{-2}\,(2,f)| = \sum_{d|f} \phi_{-2}(2,d),$$

where the summation is over all $d \in \mathcal{S}$ with $d \mid f$. Employing the Möbius function μ on the set of monic, self-reciprocal polynomials, we obtain

$$\phi_{-2}(2,f) = \sum_{d|f} \mu\,(d) \left[\frac{q^{\lfloor \frac{deg(f)-deg(d)}{2} \rfloor} - 1}{q-1}\right].$$

This number gives us the monic, self-reciprocal polynomials $c(x)$ with even degree such that $gcd(c,f) = 1$. However, we need to count all $c(x)$ not only monic ones. Therefore, with $q-1$ choices for the leading coefficient, we get the desired number as

$$(q-1)\phi_{-2}(2,f) = \sum_{d|f} \mu\,(d) \left[q^{\lfloor \frac{deg(f)-deg(d)}{2} \rfloor} - 1\right].$$

Since $q = 4$ in this case, we have

$$\mathcal{N}_s = \sum_{d|f} \mu\,(d) \left[4^{\lfloor \frac{deg(f)-deg(d)}{2} \rfloor} - 1\right].$$

□

The enumeration method presented in Section 3.3.1 can also be applicable for finding the number of quadratic bent functions. Now, we complement two results related to number of bent functions. Ma et al.[34] studied bentness of the functions with the form

$$f(x) = \sum_{i=1}^{\frac{n}{2}-1} c_i Tr_1^n(x^{1+2^i}) + Tr_1^{n/2}(x^{1+2^{n/2}}), \quad c_i \in \mathbb{F}_2. \tag{3.9}$$

They showed that f is bent if and only if $gcd(c(x), x^n + 1) = 1$ where $c(x) = \sum_{i=1}^{\frac{n}{2}-1} c_i(x^i + x^{n-i}) + x^{n/2}$. Hu and Feng[25] presented numerical results for bent functions having this form for $n = 2^v p^r$ with $v \geq 1$, $r \geq 1$ where p is odd prime with $ord_p(2) = p-1$, or $ord_p(2) = \frac{p-1}{2}$ with $\frac{p-1}{2}$ odd. This result is improved to for all even n as stated in the following theorem.

Theorem 3.16. *Let $n = 2m$ and $x^n + 1 = (1 + x)^e \cdot f(x)$ where f is a monic, self-reciprocal polynomial and e is the greatest integer such that $f(1) \neq 0$. Then, the number of bent functions of the form (3.9) is equal to*

$$\mathcal{N}_b = 2^{\frac{e}{2}-1} \sum_{d|f} \mu(d)\, 2^{\frac{deg(f)-deg(d)}{2}}$$

where the summation is over all monic, self-reciprocal polynomials d dividing f.

Proof. The proof is similar to that of Theorem 3.14. Since $gcd(c(x), x^n + 1) = 1$, in this case the sum is over all self-reciprocal polynomials d dividing f, not $\frac{f}{1+x+x2}$.

□

As another class, Tang et al.[46] investigated the bent functions of the form

$$f(x) = \sum_{i=1}^{\frac{m}{2}-1} Tr_1^n(c_i x^{1+2^{ei}}) + Tr_1^{n/2}(c_{m/2} x^{1+2^{n/2}}), \tag{3.10}$$

where $n = me$, m even, and $c_i \in \mathbb{F}_{2^e}$ for $1 \leq i \leq m/2$. They stated that f is bent if and only if $gcd\left(c\left(x\right), x^m + 1\right) = 1$ where $c(x) = \sum_{i=1}^{\frac{m}{2}-1} c_i(x^i + x^{m-i}) + c_{m/2}x^{m/2}$ and presented enumeration results for $n = 2^v p^r$ with $v, r \geq 1$ and $n = 2^v pq$, p and q are special primes. Theorem 3.17 complements this result.

Theorem 3.17. *Let $n = me$, m even. Then, the number of bent functions of the form (3.10) is equal to*

$$\mathcal{N}_b = \sum_{d|x^m+1} \mu(d) \left[2^{e(\lfloor \frac{m-deg(d)}{2} \rfloor)} - 1\right]$$

where the sum is over all monic, self-reciprocal polynomials d dividing $x^m + 1$.

Proof. The proof is analogous to the proof of Theorem 3.15 and taking $q = 2^e$ yields the result. □

Finally, we finish this section by presenting the number of semi-bent functions introduced in Corollary 3.4.

Theorem 3.18. *Let $n = 2m$ and $6 \mid n$. The number of the semi-bent functions of the form*

$$f_i(x) = Tr_1^n(x^{1+2^i}) + Tr_1^{n/2}(x^{1+2^{n/2}}), \quad 1 \leq i \leq n/2 - 1$$

is

$$\#(SB_i) = \begin{cases} \varphi(m) & \text{if } m \text{ is even}, \\ \varphi(m)/2 & \text{if } m \text{ is odd} \end{cases}$$

where $\varphi(m)$ is the Euler's totient function.

Proof. By Corollary 3.4, f_i is semi-bent if and only if $gcd(i, m) = 1$ and $m - i$ is odd. If m is even, then i values such that $gcd(i, m) = 1$ should be odd and all of these i values satisfy the condition $m - i$ is odd. Hence, the number of i values is $\varphi(m)$. If m is odd, then half of the i values satisfying $gcd(i, m) = 1$ are even and half of them are odd. In this case, half of the i values which are even fulfill the condition $m - i$ is odd. So, the number of i values is $\varphi(m)/2$ in this case. □

CHAPTER 4

SECONDARY CONSTRUCTIONS OF BENT AND SEMI-BENT FUNCTIONS VIA LINEAR TRANSLATORS

4.1 Introduction

The concept of a linear translator exists of p-ary function (see for instance [30]) but it was introduced in cryptography, mainly for Boolean functions (see for instance [12]). Functions with linear structures are considered as weak for some cryptographic applications. For instance, a recent attack on hash functions proposed in [4] exploits a similar weakness of the involved mappings. All Boolean functions using a linear translator have been characterized by Lai [31]. Further, Charpin and Kyureghyan have done the characterization for the functions in univariate variables from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ of the form $Tr_{\mathbb{F}_{p^n}/\mathbb{F}_p}(F(x))$, where $F(x)$ is a function over $\mathbb{F}_{p^n}$ and $Tr_{\mathbb{F}_{p^n}/\mathbb{F}_p}$ denotes the trace function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$. The result of Lai in [31] has been formulated recently by Charpin and Sarkar [18].

For a Boolean map, linear structures or linear translators are not desirable and are generally considered as a defect. In this paper, we show that one can recycle such Boolean functions to get Boolean functions with optimal or very high nonlinearity. More precisely, we show that one can obtain primary constructions of bent and semi-bent functions from Boolean maps having linear structures or linear translator in Sections 4.2, 4.3 and 4.4. All the primary constructions proposed in the paper belong to the well-known class of Maiorana-McFarland. However, an important feature of the bent functions presented in this paper is that their dual functions can be explicitly computed. Next, we focus on secondary constructions presented in [11] and in [5] (see also [40]). Note that several primary constructions have been derived in [40] and in [42] from a Carlet's result ([5], Theorem 3) which has been completed in ([40], Theorem 4). We show how to obtain new secondary constructions by reusing bent functions presented in the paper. Our new secondary constructions are very explicit and they use Boolean functions (vectorial Boolean functions) with certain linear structures (linear translators) as ingredients instead of bent or semi-bent functions. The conditions on such linear structures (linear translators) in our secondary constructions are easily satisfied. Finally, we show that one can construct bent functions from bent functions of Sections 4.2 and 4.3 by adding a quadratic or cubic function appropriately chosen. The work described here is based on the results of the publication [29].

We begin by recalling the definitions of linear translator and linear structure.

Definition 4.1. Let $n = rk$, $1 \leq k \leq n$. Let f be a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^k}$, $\gamma \in \mathbb{F}_{2^n}^*$ and b be a constant of $\mathbb{F}_{2^k}$. Then γ is a *b-linear translator* of f if $f(x)+f(x+u\gamma) = ub$ for all $x \in \mathbb{F}_{2^n}$ and $u \in \mathbb{F}_{2^k}$. If $f(x) + f(x + \gamma) = b$ for all $x \in \mathbb{F}_{2^n}$, then γ is called a *b-linear structure* of f.

The notion of *b-linear translator* is well known in the literature (see for example [30]). The notion of *b-linear structure is usually given for functions $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$, that is $k = 1$ (see for example [14]).*

Remark 4.1. Note that being b-linear translator is stronger than being b-linear structure if $k > 1$ and they are the same if $k = 1$. For example, let $f : \mathbb{F}_{2^4} \to \mathbb{F}_{2^2}$ be a function defined as $f(x) = Tr_2^4(x^2 + \gamma x)$ where $\gamma \in \mathbb{F}_{2^4} \backslash \mathbb{F}_{2^2}$. Then, γ is a 0-linear structure of f but it is not a 0-linear translator of f as $f(x + u\gamma) \neq f(x)$ for $u \in \mathbb{F}_{2^2} \backslash \mathbb{F}_2$.

The notions of linear structures, linear translators and derivatives are related.

Definition 4.2. Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$. For $a \in \mathbb{F}_{2^n}$, the function D_aF given by $D_aF(x) = F(x) + F(x + a), \forall x \in \mathbb{F}_{2^n}$ is called the derivative of F in the direction of a.

Note that $D_\gamma f(x) = b$ for each $x \in \mathbb{F}_{2^n}$ if and only if γ is a b-linear structure of f. Similarly, $D_{u\gamma} f(x) = ub$ for each $x \in \mathbb{F}_{2^n}$ and each $u \in \mathbb{F}_{2^k}$ if and only if γ is a b-linear translator of f.

4.2 Constructions of Bent and Semi-bent Boolean Functions from the Class of Maiorana-McFarland Using One Linear Structure

A function $H : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ is said to be in the class of Maiorana-McFarland if it can be written in bivariate form as

$$H(x, y) = Tr_1^m (x\phi(y)) + h(y) \tag{4.1}$$

where ϕ is a map from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$ and h is a Boolean function on $\mathbb{F}_{2^m}$. It is well-known that we can choose ϕ so that H is bent or H is semi-bent. Indeed, it is well-known that bent functions of the form (4.1) come from one-to-one maps while 2-to-1 maps lead to semi-bent functions.

Proposition 4.1. *([6, 20, 38]) Let H be defined by (4.1). Then,*

1. *H is bent if and only if ϕ is a permutation and its dual function is $\tilde{H}(x, y) = Tr_1^m (y\phi^{-1}(x)) + h(\phi^{-1}(x))$.*
2. *H is semi-bent if ϕ is 2-to-1.*

As a first illustration of Proposition 4.1, let us consider a first class of maps from $\mathbb{F}_{2^m}$ to itself: $\phi : y \mapsto y + \gamma f(y)$ where γ is a linear structure of f. This class has the property that it only contains one-to-one maps or 2-to-1 maps. Therefore, by Proposition 4.1, one can obtain the following infinite families of bent and semi-bent functions.

Proposition 4.2. *Let f and h be two Boolean functions over $\mathbb{F}_{2^m}$.*

Let H be the Boolean function defined on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ by

$$H(x, y) = Tr_1^m(xy + \gamma x f(y)) + h(y),\ \gamma \in \mathbb{F}_{2^m}.$$

H is bent (resp. semi-bent) if and only if γ is a 0-linear (resp. 1-linear) structure of f. Furthermore, if H is bent, then its dual is

$$\tilde{H}(x, y) = Tr_1^m\big(yx + \gamma y f(x))\big) + h(x + \gamma f(x)).$$

Proof. Properties of $\phi : y \mapsto y + \gamma f(y)$ are well-known and firstly developed in [13, 14] (see also [15, 30]). Bijectivity is given by Theorem 2 of [13]. For the 2-to-1 property, see Theorems 3,6 in [14]. The proof is then immediately obtained. Also, note that since ϕ is an involution (see also [15, 16, 30]), we have $\tilde{H}(x, y) = Tr_1^m\big(y\phi(x))\big) + h(\phi(x))$. □

In order to show that the hypotheses of Proposition 4.2 hold in certain cases, we give the following examples which are direct applications of Theorems 3, 4 in [13].

Example 4.1. Let $\gamma \in \mathbb{F}_{2^m}^\star$ and $\beta \in \mathbb{F}_{2^m}$ such that $Tr_1^m(\beta\gamma) = 0$ (resp. $Tr_1^m(\beta\gamma) = 1$). Let $H : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ be an arbitrary mapping and h be any Boolean function on $\mathbb{F}_{2^m}$. Then the function g defined over $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ by

$$g(x, y) = Tr_1^m(xy + \gamma x Tr_1^m(H(y^2 + \gamma y) + \beta y)) + h(y)$$

is bent (resp. semi-bent).

Example 4.2. Let $0 \leq i \leq m - 1$, $i \notin \{0, \frac{m}{2}\}$ and δ, $\gamma \in \mathbb{F}_{2^m}$ such that $\delta^{2^i-1} = \gamma^{1-2^{2i}}$. Let h be any Boolean function on $\mathbb{F}_{2^m}$ and g be the Boolean function defined on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ by

$$g(x, y) = Tr_1^m(xy + \gamma x Tr_1^m(\delta y^{2^i+1})) + h(y).$$

If $Tr_1^m(\delta\gamma^{2^i+1}) = 0$ (resp. $Tr_1^m(\delta\gamma^{2^i+1}) = 1$) then g is bent (resp. semi-bent).

Observe that if we compose ϕ at left by a linearized permutation polynomial L, any output has the same number of preimages under ϕ than under $L \circ \phi$. Hence, one can slightly generalize Proposition 4.2 as follows.

Proposition 4.3. *Let f and h be two Boolean functions over $\mathbb{F}_{2^m}$ and $\gamma \in \mathbb{F}_{2^m}$. Let L be a linearized permutation polynomial of $\mathbb{F}_{2^m}$. The Boolean function H defined by*

$$H(x, y) = Tr_1^m\left(xL(y) + L(\gamma)xf(y)\right) + h(y)$$

is bent (resp. semi-bent) if and only if γ is a 0-linear (resp. 1-linear) structure of f. Moreover, if H is bent then its dual function $\tilde{H}$ is given by

$$\tilde{H}(x, y) = Tr_1^m(yL^{-1}(x) + \gamma y f(L^{-1}(x)) + h(L^{-1}(x) + \gamma f(L^{-1}(x))).$$

4.3 Constructions of Bent and Semi-bent Boolean Functions From the Class of Maiorana-McFarland Using Two Linear Structures

In this section we consider the functions H of the form (4.1) :

$$H(x,y) = Tr_1^m\left(x\phi(y)\right) + h(y) \text{ with } \phi(y) = \pi_1\left(\pi_2(y) + \gamma f(\pi_2(y)) + \delta g(\pi_2(y))\right) \tag{4.2}$$

where f, g and h are Boolean functions over $\mathbb{F}_{2^m}$, $\gamma, \delta \in \mathbb{F}_{2^m}^\star$, $\gamma \neq \delta$ and π_1, π_2 are permutations of $\mathbb{F}_{2^m}$ (not necessarily linear). The class (4.2) contains the functions involved in Proposition 4.1 and in Proposition 4.3 (which corresponds to the case where $f = g$). In the line of Section 4.2, we study the cases where γ and δ are linear structures of the Boolean functions involved in ϕ. Then one can exhibit conditions of bentness or semi-bentness as those of Propositions 4.1 and 4.3 that we present in the following two propositions. We indicate that, despite their similarities with Proposition 4.1 and 4.3, we obtain bent functions that do not fall in the scope of Proposition 4.1 and 4.3.

Proposition 4.4. *Let H be defined by equation (4.2). Then H is bent if one of the following conditions holds:*

(i) *γ is a 0-linear structure of f, δ is a 0-linear structure of f and g,*

(ii) *γ is a 0-linear structure of f, δ is a 1-linear structure of f and $\delta + \gamma$ is a 0-linear structure of g,*

(iii) *δ is a 0-linear structure of g, γ is a 0-linear structure of f and g,*

(iv) *δ is a 0-linear structure of g, γ is a 1-linear structure of g and $\delta + \gamma$ is a 0-linear structure of f,*

(v) *δ is a 1-linear structure of f, γ is a 1-linear structure of f and g,*

(vi) *γ is a 1-linear structure of g, δ is a 1-linear structure of f and g.*

Moreover, if H is bent then its dual is $\tilde{H}(x,y) = Tr_1^m\left(y\phi^{-1}(x)\right) + h(\phi^{-1}(x))$ where $\phi^{-1} = {\pi_2}^{-1} \circ \rho^{-1} \circ {\pi_1}^{-1}$ and ρ^{-1} is given explicitly in the Appendix as Proposition A.1. In particular, choosing $\pi_1(x) = L(x)$ as a linearized permutation polynomial and π_2 as the identity, we get that

$$H(x,y) \;=\; Tr_1^m\left(xL(y) + L(\gamma)xf(y) + L(\delta)xg(y)\right) + h(y) \tag{4.3}$$

is bent in the conditions above and $\tilde{H}(x,y) = Tr_1^m\big(y\rho^{-1}(L^{-1}(x))\big) + h(\rho^{-1}(L^{-1}(x))$.

Proof. We give the proof for only case (i) since the proofs for the other cases are very similar. It suffices to show that $\rho : y \mapsto y + \gamma f(y) + \delta g(y)$ is a permutation. Suppose that $\rho(y) = \rho(z)$, i.e.,

$$y + \gamma f(y) + \delta g(y) = z + \gamma f(z) + \delta g(z). \tag{4.4}$$

Taking f of both sides we obtain $f\big(y+\gamma f(y)+\delta g(y)\big) = f\big(z+\gamma f(z)+\delta g(z)\big)$. Since γ and δ are 0-linear structures of f, we have

$$f(y) = f(z). \tag{4.5}$$

Combining equations (4.4) and (4.5), we get $y+\delta g(y) = z+\delta g(z)$. Taking g of both sides we obtain $g(y+\delta g(y)) = g(z+\delta g(z))$. Since δ is a 0-linear structure of g, we conclude

$$g(y) = g(z). \tag{4.6}$$

Combining equations (4.4), (4.5) and (4.6), we reach that $y = z$. For the dual function, ρ^{-1} is written explicitly in the Appendix as Proposition A.1 and the proof for ρ^{-1} for case (i) is given. □

Remark 4.2. The converse of Proposition 4.4 is not always true. For example, for $f(x) = Tr_1^3(x^3+\alpha^5 x)$, $g(x) = Tr_1^3(\alpha x^3+\alpha^5 x)$, $\gamma = \alpha$ and $\delta = \alpha^3$ where α is a primitive element of $\mathbb{F}_{2^3}$, ϕ is a permutation but none of the conditions given in Proposition 4.4 is satisfied.

The following result shows in which cases ϕ is 2-to-1 and hence H is semi-bent.

Proposition 4.5. *Let H be defined by (4.2). Then H is semi-bent if one of the following conditions holds:*

(i) *γ, δ are 1-linear structures of f and γ is a 0-linear structure of g,*

(ii) *δ is a 1-linear structure of f and γ, δ are 0-linear structures of g,*

(iii) *γ, δ are 0-linear structures of f and δ is a 1-linear structure of g,*

(iv) *δ is a 0-linear structure of f and γ, δ are 1-linear structures of g,*

(v) *γ is a 0-linear structure of f, δ is a 1-linear structure of f and $\gamma+\delta$ is a 1-linear structure of g,*

(vi) *γ is a 1-linear structure of g, δ is a 0-linear structure of g and $\gamma+\delta$ is a 1-linear structure of f.*

In particular, choosing $\pi_1(x) = L(x)$ as a linearized permutation polynomial and π_2 as the identity, we get that

$$H(x,y) = Tr_1^m\left(xL(y)+L(\gamma)xf(y)+L(\delta)xg(y)\right)+h(y)$$

is semi-bent in the conditions above.

Proof. We give the proof for case (i) only since the proofs for other cases are similar. Now, we need to show that $\rho(y): y \mapsto y+\gamma f(y)+\delta g(y)$ is 2-to-1. Let $\rho(y) = a$ for some $a \in \mathbb{F}_{2^m}$. Then, $y \in \{a, a+\gamma, a+\delta, a+\gamma+\delta\}$. As γ is a 1-linear structure of f and 0-linear structure of g, we have $\rho(a) = \rho(a+\gamma)$ and $\rho(a+\delta) = \rho(a+\gamma+\delta)$. Moreover, $\rho(a+\delta) = a+\delta+\gamma f(a+\delta)+\delta g(a+\delta) = a+\delta+\gamma+\gamma f(a)+\delta g(a+\delta)$ where

we use that δ is a 1-linear structure of f. We observe that $\rho(a) = a + \gamma f(a) + \delta g(a) \neq \rho(a+\delta)$. Indeed, otherwise if the equality holds, then $\gamma + \delta + \delta\big(g(a) + g(a+\delta)\big) = 0$. This is a contradiction as $\gamma \neq \delta$ and $\gamma \neq 0$. This implies that $\rho^{-1}(a) = \{a, a+\gamma\}$ or $\rho^{-1}(a) = \{a+\delta, a+\gamma+\delta\}$ which shows that ρ is 2-to-1. □

Remark 4.3. The converse of Proposition 4.5 is not always true. For example, for $f(x) = Tr_1^3(\alpha^4 x^3 + \alpha^4 x)$, $g(x) = Tr_1^3(\alpha x^3 + \alpha^2 x)$, $\gamma = \alpha$ and $\delta = \alpha^3$ where α is a primitive element of $\mathbb{F}_{2^3}$, ϕ is 2-to-1 but none of the conditions given in Proposition 4.5 is satisfied.

4.4 Constructions of Bent and k-Plateaued Functions Using Linear Translators

In the preceding sections, we have shown that one can construct bent and semi-bent functions from Boolean functions having linear structures, that is, having constant derivatives. An extension of these constructions is to consider Boolean maps taking its values in a subfield of the ambient field instead of Boolean functions in (4.1). In that case, the natural notion replacing linear structures is the notion of linear translators. We still adopt the approach of the preceding sections and aim to construct bent functions in the class of Maiorana-McFarland. To this end, one can apply results on permutations constructed from Boolean maps having linear translators presented in [30] and obtain the following infinite families of bent and plateaued functions.

Proposition 4.6. *Let m be a positive integer and k be a divisor of m. Let f be a function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^k}$ and h be a Boolean function on $\mathbb{F}_{2^m}$. Let H be the function defined on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ by*

$$H(x,y) = Tr_1^m(xy + \gamma x f(y)) + h(y), \quad \gamma \in \mathbb{F}_{2^m}^\star.$$

(i) If γ is a c-linear translator of f where $c \in \mathbb{F}_{2^m}$ and $c \neq 1$, then H is bent and its dual function is given as

$$\tilde{H}(x,y) = Tr_1^m\left(y\left(x + \gamma\frac{f(x)}{1+c}\right)\right) + h\left(x + \gamma\frac{f(x)}{1+c}\right).$$

Moreover, $H(x,y) = Tr_1^m(xL(y) + L(\gamma)xf(y)) + h(y)$ where L is an $\mathbb{F}_{2^k}$-linearized permutation polynomial, is also bent under these conditions and its dual is

$$\tilde{H}(x,y) = Tr_1^m\left(y\left(L^{-1}(x) + \gamma\frac{f(L^{-1}(x))}{1+c}\right)\right) + h\left(L^{-1}(x) + \gamma\frac{f(L^{-1}(x))}{1+c}\right).$$

(ii) If γ is a 1-linear translator of f and $h = 0$ then H is k-plateaued with Walsh transform values

$$\widehat{\chi_H}(a,b) = \begin{cases} \pm 2^{m+k} & \text{if } Tr_k^m(b\gamma) = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Let $\phi(y) = y + \gamma f(y)$. Assume that $\phi(y) = a$ where $a \in \mathbb{F}_{2^m}$. Then $y = a + \gamma f(y)$ implies that $y \in \{a + u\gamma \mid u \in \mathbb{F}_{2^k}\}$.

(i)

$$\begin{aligned} y &= a + \gamma f(y) \\ f(y) &= f(a + \gamma f(y)) \\ f(y) &= f(a) + cf(y), \quad \text{since } \gamma \text{ is a } c\text{-linear translator of } f. \end{aligned}$$

This gives that $f(y) = \frac{f(a)}{1+c}$. Therefore, number of solutions of y such that $\phi(y) = a$ is one, namely $y = a + \gamma\left(\frac{f(a)}{1+c}\right)$. This concludes that ϕ is permutation and hence g is bent.

(ii) $y = a + \gamma f(y)$ gives $f(y) = f(a + \gamma f(y))$. Since γ is a 1-linear translator of f, $f(a + \gamma f(y)) = f(a) + f(y)$. This results in $f(a) = 0$. Now, there are at most 2^k solutions in y where $y \in \{a + u\gamma \mid u \in \mathbb{F}_{2^k}\}$.

$$\begin{aligned} \phi(a + u\gamma) &= a + u\gamma + \gamma f(a + u\gamma) \\ &= a + u\gamma + \gamma(f(a) + u) \\ &= a \end{aligned}$$

Hence, $a + u\gamma \in \phi^{-1}(a)$ and ϕ is $2^k - to - 1$.

Walsh transform of g at (a, b) is:

$$\begin{aligned} \widehat{\chi_g}(a, b) &= 2^m \sum_{y \in \phi^{-1}(a)} (-1)^{Tr_1^m(by)} \\ &= 2^m \sum_{u \in \mathbb{F}_{2^k}} (-1)^{Tr_1^m(b(a+u\gamma))} \\ &= 2^m (-1)^{Tr_1^m(ba)} \sum_{u \in \mathbb{F}_{2^k}} (-1)^{Tr_1^m(bu\gamma)}. \end{aligned}$$

Thus,

$$\widehat{\chi_g}(a, b) = \begin{cases} \pm 2^{m+k} & \text{if } Tr_k^m(b\gamma) = 0 \\ 0 & \text{otherwise.} \end{cases}$$

□

Note that Proposition 4.6 generalizes partially Proposition 4.2 (extending the condition 0-linear structure to c-linear translator with $c \neq 1$). Furthermore, one can derive from Proposition 4.4 and Proposition 4.5 similar statements if $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^k}$ instead of being a Boolean function. Indeed, it suffices to change the 0-linear structures (resp. 1-linear structures) with 0-linear translators. (resp. 1-linear translators). This is stated in the following proposition.

Proposition 4.7. *Let m be a positive integer and k be a divisor of m. Let f, g be functions from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^k}$ and $\gamma, \delta \in \mathbb{F}_{2^m}^\star$. Set $\phi(y) := y + \gamma f(y) + \delta g(y)$. $\phi(y)$ is a permutation if one of the following conditions holds:*

(i) *γ is a 0-linear translator of f, δ is a 0-linear translator of f and g,*

(ii) *γ is a 0-linear translator of f, δ is a 1-linear translator of f and $\delta+\gamma$ is a 0-linear translator of g,*

(iii) *δ is a 0-linear translator of g, γ is a 0-linear translator of f and g,*

(iv) *δ is a 0-linear translator of g, γ is a 1-linear translator of g and $\delta+\gamma$ is a 0-linear translator of f,*

(v) *δ is a 1-linear translator of f, γ is a 1-linear translator of f and g,*

(vi) *γ is a 1-linear translator of g, δ is a 1-linear translator of f and g.*

Proof. We will give only the proof for the first case. Proofs for other cases are similar. Assume that γ is a 0-linear translator of f, δ is a 0-linear translator of f and g. Let $\phi(y) = \phi(z)$, then

$$\begin{aligned} y + \gamma f(y) + \delta g(y) &= z + \gamma f(z) + \delta g(z) \\ y &= z + \gamma\left[f(y) + f(z)\right] + \delta\left[f(z) + g(z)\right] \\ f(y) &= f\left(z + \gamma\left[f(y) + f(z)\right] + \delta\left[f(z) + g(z)\right]\right) \\ f(y) &= f\left(z + \gamma\left[f(y) + f(z)\right]\right), \text{ since } \delta \text{ is 0-linear translator of } f \\ f(y) &= f\left(z\right), \text{since } \gamma \text{ is 0-linear translator of } f. \end{aligned}$$

This gives us

$$\begin{aligned} y + \delta g(y) &= z + \delta g(z) \\ g(y + \delta g(y)) &= g(z + \delta g(z)) \\ g(y) &= g(z), \text{since } \delta \text{ is 0-linear translator of } g. \end{aligned}$$

Therefore, $y = z$ and ϕ is a permutation. □

4.5 Bent Functions not Belonging to the Class of Maiorana-McFarland Using Linear Translators

In the following we are now interested in investigating constructions of bent functions that do not necessary belong to the class of Maiorana- McFarland contrary to the preceding sections. To this end, we are particularly interested in the secondary construction of the form $f(x) = \phi_1(x)\phi_2(x) + \phi_1(x)\phi_3(x) + \phi_2(x)\phi_3(x)$ presented in [5] and next completed in [40]. More precisely, it is proven in [5] that if ϕ_1, ϕ_2 and ϕ_3 are bent, then if $\psi := \phi_1 + \phi_2 + \phi_3$ is bent and if $\tilde{\psi} = \tilde{\phi_1} + \tilde{\phi_2} + \tilde{\phi_3}$, then f is bent, and

$\tilde{f} = \tilde{\phi_1}\tilde{\phi_2} + \tilde{\phi_1}\tilde{\phi_3} + \tilde{\phi_2}\tilde{\phi_3}$. Next, it is proven in [40] that the converse is also true: if ϕ_1, ϕ_2, ϕ_3 and ψ are bent, then f is bent if and only if $\widetilde{\psi} + \tilde{\phi_1} + \tilde{\phi_2} + \tilde{\phi_3} = 0$ (where $\psi := \phi_1 + \phi_2 + \phi_3$). In this section, we show that one can reuse Boolean functions of the shape presented in the preceding sections in the construction of [40, 42].

Firstly, one can derive easily bent functions f, whose dual functions are very simple, by choosing functions H_i in the class of Maiorana-McFarland such that the permutation involving in each H_i is built in terms of an involution and a linear translator. More explicitly, each H_i is a Boolean function over $\mathbb{F}_{2^m}$ defined by $H_i(y) = Tr_1^m\Big(L(y) + L(\gamma_i)h(g(y))\Big)$ where L is a $\mathbb{F}_{2^k}$-linear involution on $\mathbb{F}_{2^m}$ (k being a divisor of m); carefully chosen according to the hypothesis of [16, Corollary 2], g is a function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^k}$, h is a mapping from $\mathbb{F}_{2^k}$ to itself, and γ_1, γ_2 and γ_3 are three pairwise distinct elements of $\mathbb{F}_{2^m}^\star$ which are 0-linear translators of g such that $\gamma_1 + \gamma_2 + \gamma_3 \neq 0$. Bent functions f are therefore obtained from a direct application of [40, Theorem 4] and [16, Corollary 2].

Secondly, we extend a result from [42] by considering two linear structures instead of one. This result uses linear structures as in the first case of Proposition 4.4. Similarly, for the other five cases we can construct bent functions and their duals. These results are presented in the Appendix as Propositions A.2, A.3, A.4, A.5, A.6.

Proposition 4.8. *Let f and g be functions from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$. For $i \in \{1, 2, 3\}$ set $\phi_i(y) := y + \gamma_i f(y) + \delta_i g(y)$ where*

(i) δ_1, δ_2, δ_3 are elements of $\mathbb{F}_{2^m}^\star$ which are 0-linear structures of f and g;

(ii) γ_1, γ_2 and γ_3 are elements of $\mathbb{F}_{2^m}^\star$ which are 0-linear structures of f;

(iii) $\gamma_1 + \gamma_2$ and $\gamma_1 + \gamma_3$ are 0-linear structures of g.

Then the function h defined on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ by

$$\begin{aligned} h(x,y) &= Tr_1^m\Big(x\phi_1(y)\Big)Tr_1^m\Big(x\phi_2(y)\Big) + Tr_1^m\Big(x\phi_1(y)\Big)Tr_1^m\Big(x\phi_3(y)\Big) \\ &\quad + Tr_1^m\Big(x\phi_2(y)\Big)Tr_1^m\Big(x\phi_3(y)\Big) \end{aligned}$$

is bent and the dual of h is given by

$$\begin{aligned} \tilde{h}(x,y) &= Tr_1^m\Big(y\phi_1^{-1}(x)\Big)Tr_1^m\Big(y\phi_2^{-1}(x)\Big) + Tr_1^m\Big(y\phi_1^{-1}(x)\Big)Tr_1^m\Big(y\phi_3^{-1}(x)\Big) \\ &\quad + Tr_1^m\Big(y\phi_2^{-1}(x)\Big)Tr_1^m\Big(y\phi_3^{-1}(x)\Big) \end{aligned}$$

where $\phi_i^{-1}(x) = x + \gamma_i f(x) + \delta_i \left[g(x)\big(1 + f(x)\big) + g(x + \gamma_i)f(x)\right]$.

Proof. Let $\psi_i(x, y) = Tr_1^m\Big(x\phi_i(y)\Big)$. Then by Proposition 4.4, ψ_i is bent for $i = 1, 2, 3$. Let $\gamma = \gamma_1 + \gamma_2 + \gamma_3$ and $\delta = \delta_1 + \delta_2 + \delta_3$. Then, $\psi(x, y) = Tr_1^m\Big(x(y +$

$\gamma f(y) + \delta g(y))\Big)$ is bent since γ is a 0-linear structure of f and δ is a 0-linear structure of f and g. Now, it remains to show that $\tilde{\psi} = \tilde{\psi}_1 + \tilde{\psi}_2 + \tilde{\psi}_3$. $\tilde{\psi} = Tr_1^m\Big(x\phi^{-1}(y)\Big)$ and $\phi^{-1}(x)$ is given in Proposition A.1 in the Appendix.

Note that $\tilde{\psi} = \tilde{\psi}_1 + \tilde{\psi}_2 + \tilde{\psi}_3$ if and only if $g(x+\gamma_1)$=$g(x+\gamma_2)$=$g(x+\gamma_3)$=$g(x+\gamma_1+\gamma_2+\gamma_3)$ which means $\gamma_1+\gamma_2$ and $\gamma_1+\gamma_3$ are 0-linear structures of g.

□

4.6 A Secondary Construction of Bent and Semi-bent Functions Using Derivatives and Linear Translators

In this section, we consider a new kind of secondary construction. That construction has been proposed by Carlet and Yucas [11] and is presented below.

Theorem 4.9. *Let f and g be two bent functions over $\mathbb{F}_{2^n}$. Assume that there exists $a \in \mathbb{F}_{2^n}$ such that $D_a f = D_a g$. Then the function $h : \mathbb{F}_{2^n} \to \mathbb{F}_2$ defined by $h(x) = f(x) + D_a f(x)\big(f(x) + g(x)\big)$ is bent and its dual is $\tilde{h}(x) = \tilde{f}(x) + Tr_1^n(ax)(\tilde{f}(x) + \tilde{g}(x))$.*

In the line of Theorem 4.9 and of the preceding sections, we shall derive from Theorem 4.9 new secondary constructions of bent and semi-bent functions in Theorem 4.11 and Theorem 4.12. To this end, we will use the following lemma.

Lemma 4.10. *Let $b \in \mathbb{F}_{2^m}$ and $\mathcal{W} \subseteq \mathbb{F}_{2^m}$ be an $m-1$ dimensional linear subspace with $b \notin \mathcal{W}$. Let $\mu : \mathbb{F}_{2^m} \to \mathbb{F}_2$ be a Boolean function such that b is a 0-linear structure of μ. Choose arbitrary functions $h_1 : \mathbb{F}_{2^m} \to \mathbb{F}_2$ and $u : \mathcal{W} \to \mathbb{F}_2$ and define the Boolean function $h_2 : \mathbb{F}_{2^m} \to \mathbb{F}_2$ by $h_2(w) = u(w) + h_1(w)$ and $h_2(w+b) = u(w) + h_1(w+b) + \mu(w)$ for $w \in \mathcal{W}$. Then $D_b h_1(y) + D_b h_2(y) = \mu(y)$ for all $y \in \mathbb{F}_{2^m}$.*

Proof. We observe that $h_2(w+b) + h_2(w) = h_1(w+b) + h_1(w) + \mu(w)$ for all $w \in \mathcal{W}$ by definition. Using the fact that b is a 0-linear structure of μ we complete the proof. □

Note that Lemma 4.10 gives a construction of a Boolean function $h_2 : \mathbb{F}_{2^m} \to \mathbb{F}_2$ with the property $D_b h_1(y) + D_b(h_2(y) = \mu(y)$ for all $y \in \mathbb{F}_{2^m}$ for given $b \in \mathbb{F}_{2^m}$, $h_1 : \mathbb{F}_{2^m} \to \mathbb{F}_2$ and μ having b with 0-linear structure. The construction uses $m-1$ free variables in the form of the function $u : \mathcal{W} \to \mathbb{F}_2$.

Using Lemma 4.10, Theorem 4.9 and results from Section 4.4, we present below a new secondary construction of bent functions.

Theorem 4.11. *Let $1 \leq k < m$ be integers with $k \mid m$. Let f, g be functions from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^k}$. Assume that $\gamma, \delta \in \mathbb{F}_{2^m}^\star$ are 0-linear translators of f and g, respectively.*

Further assume that $b \in \mathbb{F}_{2^m}$ is a 0-linear structure of f and g. Let $a \in \mathbb{F}_{2^m}$ be an arbitrary element. For arbitrary function $h_1 : \mathbb{F}_{2^m} \to \mathbb{F}_2$ construct $h_2 : \mathbb{F}_{2^m} \to \mathbb{F}_2$ satisfying $D_b h_1(y) = D_b h_2(y) + Tr_1^m\big(a(\gamma f(y+b) + \delta g(y+b))\big)$ for all $y \in \mathbb{F}_{2^m}$ using Lemma 4.10. Set $F(x,y) := Tr_1^m(xy + \gamma x f(y)) + h_1(y)$ and $G(x,y) := Tr_1^m(xy + \delta x g(y)) + h_2(y)$. The function defined by

$$H(x,y) = F(x,y) + D_{a,b}F(x,y)\big(F(x,y) + G(x,y)\big)$$

is bent and its dual is

$$\begin{aligned}\tilde{H}(x,y) \;=\; & Tr_1^m\big(yx + \gamma y f(x)\big) + h_1(x + \gamma f(x)) \\ & + Tr_1^m(ax + by)\left[Tr_1^m\big(y(\gamma f(x) + \delta g(x))\big) + h_1(x + \gamma f(x)) + h_2(x + \delta g(x))\right].\end{aligned}$$

Proof. First, recall that $D_{a,b}F(x,y) = F(x,y) + F(x+a, y+b)$. Now, F and G are bent by Proposition 4.6. Using the fact that b is a 0-linear structure of f and g we get that $D_{a,b}F(x,y) = Tr_1^m\big(xb + a(y + b + \gamma f(y+b))\big) + D_b h_1(y)$ and $D_{a,b}G(x,y) = Tr_1^m\big(xb + a(y + b + \delta g(y+b))\big) + D_b h_2(y)$. Hence $D_{a,b}F(x,y) = D_{a,b}G(x,y)$ and the proof follows from Theorem 4.9 and Proposition 4.6.

□

Using [45, Theorem 16] instead of Theorem 4.9 we obtain the following secondary construction of semi-bent functions.

Theorem 4.12. *Under notation and assumptions of Theorem 4.11 we construct $h_2 : \mathbb{F}_{2^m} \to \mathbb{F}_2$ satisfying $D_b h_1(y) = D_b h_2(y) + Tr_1^m\big(a(\gamma f(y+b) + \delta g(y+b))\big) + 1$ (instead of $D_b h_1(y) = D_b h_2(y) + Tr_1^m\big(a(\gamma f(y+b) + \delta g(y+b))\big)$) for all $y \in \mathbb{F}_{2^m}$. Set F and G in the same way. Then the function defined by*

$$H(x,y) = F(x,y) + G(x,y) + D_{a,b}F(x,y) + D_{a,b}FG(x,y)$$

is semi-bent.

Note that Theorem 4.12 gives a secondary construction of semi-bent functions of high degree by choosing the arbitrary function $h_1 : \mathbb{F}_{2^m} \to \mathbb{F}_2$ of large degree. Moreover it gives a different construction than the one given in [39, Section 4.2.5] and hence it is an answer to Problem 4 of [39].

4.7 A Secondary Construction of Bent Functions Using Certain Quadratic and Cubic Functions Together with Linear Structures

In this section we consider Boolean functions that are the sum of a bent function of Section 4.2 or Section 4.3 and a quadratic or cubic function. We show that one can choose appropriately the quadratic and cubic function so that those Boolean functions are bent again. Furthermore, the dual functions of those bent functions can be explicitly computed as in the preceding sections. The main results are Theorems 4.14, 4.15, 4.17 and 4.18.

Theorem 4.14 is based on [10, Lemma 1]. We note that the bent functions of Theorem 4.14 is different from the two classes of plateaued functions in Section 6 of [10]. First of all we obtain bent functions while two classes of functions in Section 6 of [10] produce only plateaued functions.

Theorem 4.17 is a further generalization of Theorem 4.14 using cubic functions instead of quadratic functions.

Lemma 4.13. *[10] Let $w_1, w_2, u \in \mathbb{F}_{2^m}$ with $\{w_1, w_2\}$ linearly independent over $\mathbb{F}_{2^m}$. We have*

$$\sum_{x\in\mathbb{F}_{2^m}} (-1)^{Tr_1^m(w_1x)Tr_1^m(w_2x)+Tr_1^m(ux)} = \begin{cases} 0 & \text{if } u \notin \langle w_1, w_2\rangle = \{0, w_1, w_2, w_1+w_2\}, \\ 2^{m-1} & \text{if } u \in \{0, w_1, w_2\}, \\ -2^{m-1} & \text{if } u = w_1 + w_2. \end{cases}$$

In Lemma 4.13, for any given $\mathbb{F}_2$-linearly independent set, the Boolean function on $\mathbb{F}_{2^m}$ given by $x \mapsto Tr_1^m(w_1x)Tr_1^m(w_2x)$ is a quadratic function.

Theorem 4.14. *Let $w_1, w_2, \gamma \in \mathbb{F}_{2^m}$ with $\{w_1, w_2\}$ linearly independent over $\mathbb{F}_2$. Assume that $f, h : \mathbb{F}_{2^m} \to \mathbb{F}_2$ are Boolean functions such that w_1 and w_2 are 0-linear structures of f and h. Moreover, we assume that γ is a 0-linear structure of f. Then the Boolean function F defined on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ by*

$$F(x, y) = Tr_1^m(xw_1)Tr_1^m(xw_2) + Tr_1^m\big(xy + \gamma x f(y)\big) + h(y) \tag{4.7}$$

is bent and its dual function is

$$\tilde{F}(x, y) = Tr_1^m(yw_1)Tr_1^m(yw_2) + Tr_1^m\big(yx + \gamma y f(x)\big) + h(x + \gamma f(x)).$$

Moreover, $F(x, y) = Tr_1^m(xw_1)Tr_1^m(xw_2) + Tr_1^m\big(xL(y) + L(\gamma)xf(y)\big) + h(y)$ where L is a linearized permutation polynomial of $\mathbb{F}_{2^m}$ is also bent under the same conditions and its dual function is

$$\tilde{F}(x, y) = Tr_1^m(yw_1)Tr_1^m(yw_2) + Tr_1^m\big(yL^{-1}(x) + \gamma y f(L^{-1}(x))\big) + h(L^{-1}(x) + \gamma f(L^{-1}(x))).$$

Proof. One has for every $(a, b) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$,

$$\widehat{\chi_F}(a, b) = \sum_{y\in\mathbb{F}_{2^m}} (-1)^{h(y)+Tr_1^m(by)} \sum_{x\in\mathbb{F}_{2^m}} (-1)^{Tr_1^m(xw_1)Tr_1^m(xw_2)+Tr_1^m\left(xy+\gamma xf(y)+ax\right)}$$

Let $\phi(y) = y + \gamma f(y)$ and $\mathcal{S} = \sum_{x\in\mathbb{F}_{2^m}} (-1)^{Tr_1^m(xw_1)Tr_1^m(xw_2)+Tr_1^m\left(x(\phi(y)+a)\right)}$. Then by Lemma 4.13, we have

$$\mathcal{S} = \begin{cases} 0 & \text{if } \phi(y) + a \notin \{0, w_1, w_2, w_1 + w_2\}, \\ 2^{m-1} & \text{if } \phi(y) + a \in \{0, w_1, w_2\}, \\ -2^{m-1} & \text{if } \phi(y) + a = w_1 + w_2. \end{cases}$$

Now, $f(a) = f(a + w_1) = f(a + w_2) = f(a + w_1 + w_2)$ since w_1 and w_2 are 0-linear structures of f. We have two cases, namely $f(a) = 0$ and $f(a) = 1$.

Assume $f(a) = 0$. Then $\phi(y) + a \in \{0, w_1, w_2\}$ when $y \in \mathcal{A} = \{a, a + w_1, a + w_2\}$ and $\phi(y) + a = w_1 + w_2$ when $y = a + w_1 + w_2$. Hence,

$$\widehat{\chi_F}(a,b) = 2^{m-1}\left[\sum_{y\in\mathcal{A}}(-1)^{h(y)+Tr_1^m(by)} - (-1)^{h(a+w_1+w_2)+Tr_1^m(b(a+w_1+w_2))}\right].$$

Since w_1 and w_2 are 0-linear structures of h, we obtain

$$\widehat{\chi_F}(a,b) \;=\; 2^{m-1}\left[(-1)^{h(a)+Tr_1^m(ba)}\right]\mathcal{S}_1$$

where

$$\mathcal{S}_1 \;=\; \left[1 + (-1)^{Tr_1^m(bw_1)} + (-1)^{Tr_1^m(bw_2)} - (-1)^{Tr_1^m(b(w_1+w_2))}\right]. \tag{4.8}$$

Note that

$$\mathcal{S}_1 = \begin{cases} 2 & \text{if } Tr_1^m(bw_1)Tr_1^m(bw_2) = 0, \\ -2 & \text{if } Tr_1^m(bw_1)Tr_1^m(bw_2) = 1. \end{cases}$$

Combining these we obtain that F is bent and its dual $\tilde{F}$ satisfies that

$$\tilde{F}(x,y) = Tr_1^m(yw_1)Tr_1^m(yw_2) + Tr_1^m\big(yx + y\gamma f(x)\big) + h(x + \gamma f(x)).$$

Assume $f(a) = 1$. The proof for this case is very similar to that of the first case. $\phi(y)+a \in \{0, u, v\}$ when $y \in \mathcal{B} = \{a + \gamma, a + u + \gamma, a + v + \gamma\}$ and $\phi(y)+a = u+v$ when $y = a + u + v + \gamma$. Then,

$$\widehat{\chi_F}(a,b) = 2^{m-1}\left[\sum_{y\in\mathcal{B}}(-1)^{g(y)+Tr_1^m(by)} - (-1)^{g(a+u+v+\gamma)+Tr_1^m(b(a+u+v+\gamma))}\right].$$

Similarly, we obtain

$$\begin{aligned}\widehat{\chi_F}(a,b) &= 2^{m-1}(-1)^{g(a+\gamma)+Tr_1^m(b(a+\gamma))}\left[1 + (-1)^{Tr_1^m(bu)} + (-1)^{Tr_1^m(bv)} - (-1)^{Tr_1^m(b(u+v))}\right] \\ &= \pm 2^m.\end{aligned}$$

□

Remark 4.4. In Theorem 4.14, for given $\mathbb{F}_2$-linearly independent subset $\{w_1, w_2\}$, the Boolean function on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ given by $(x, y) \mapsto Tr_1^m(xw_1)Tr_1^m(xw_2)$ is a quadratic function, which is used as the first summand in the definition of $F(x, y)$ in equation (4.7). In the proof of Theorem 4.14, we apply Lemma 4.13 for this quadratic function. Note that if $\gamma \neq 0$ and $1 + deg(f)$, $deg(h)$ and 2 are distinct, then the degree of $F(x, y)$ is $max\{1 + deg(f), deg(h), 2\}$, which may be much larger than 2.

In the following we present a straightforward generalization of Theorem 4.14 using two linear structures instead of one linear structure.

Theorem 4.15. *Let $w_1, w_2, \gamma, \delta \in \mathbb{F}_{2^m}$ with $\{w_1, w_2\}$ linearly independent over $\mathbb{F}_2$. Assume that $f, g, h : \mathbb{F}_{2^m} \to \mathbb{F}_2$ are Boolean functions such that w_1 and w_2 are 0-linear structures of f, g and h. Moreover, we assume that γ is a 0-linear structure of*

f and δ is a 0-linear structure of f and g. Then the Boolean function F defined on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ by

$$F(x,y) = Tr_1^m(xw_1)Tr_1^m(xw_2) + Tr_1^m\big(x(L(y) + L(\gamma)f(y) + L(\delta)g(y))\big) + h(y)$$

is bent and its dual function is

$$\tilde{F}(x,y) = Tr_1^m(yw_1)Tr_1^m(yw_2) + Tr_1^m\big(y\rho^{-1}(x)\big) + h(\rho^{-1}(x)) \text{ where}$$

$$\begin{aligned}\rho^{-1}(x) &= L^{-1}(x) + \gamma f(L^{-1}(x)) \\ &\quad + \delta\left[g(L^{-1}(x))\big(1 + f(L^{-1}(x))\big) + g(L^{-1}(x) + \gamma)f(L^{-1}(x))\right].\end{aligned}$$

We now give the analogue of Lemma 4.13 which improves Lemma 1 of [10].

Lemma 4.16. *Let $w_1, w_2, w_3, u \in \mathbb{F}_{2^m}$ with $\{w_1, w_2, w_3\}$ linearly independent over $\mathbb{F}_{2^m}$. We have*

$$\sum_{x\in\mathbb{F}_{2^m}} (-1)^{Tr_1^m(w_1x)Tr_1^m(w_2x)Tr_1^m(w_3x)+Tr_1^m(ux)} = \begin{cases} 0 & \text{if } u \notin \langle w_1, w_2, w_3\rangle, \\ 3.2^{m-2} & \text{if } u = 0, \\ 2^{m-2} & \text{if } u \in \{w_1, w_2, w_3, w_1+w_2+w_3\}, \\ -2^{m-2} & \text{if } u \in \{w_1+w_2, w_1+w_3, w_2+w_3\}. \end{cases}$$

Proof. Let $\mathcal{T}$ denotes the sum in the statement of the lemma. Let $\mathcal{T}_1$ and $\mathcal{T}_2$ be the sums as

$$\mathcal{T}_1 = \sum_{x\in\mathbb{F}_{2^m} | Tr_1^m(w_1x)=0} (-1)^{Tr_1^m(ux)}$$

and

$$\mathcal{T}_2 = \sum_{x\in\mathbb{F}_{2^m} | Tr_1^m(w_1x)=1} (-1)^{Tr_1^m(w_2x)Tr_1^m(w_3x)+Tr_1^m(ux)}.$$

We have that $\mathcal{T} = \mathcal{T}_1 + \mathcal{T}_2$. It is clear that

$$\mathcal{T}_1 = \begin{cases} 0 & \text{if } u \notin \langle 0, w_1\rangle = \{0, w_1\}, \\ 2^{m-1} & \text{if } u \in \{0, w_1\}. \end{cases}$$

Using Lemma 4.13 we obtain that

$$\mathcal{T}_2 = \begin{cases} 0 & \text{if } u \notin \langle w_1, w_2, w_3\rangle, \\ 2^{m-2} & \text{if } u \in \{0, w_1, w_2, w_3, w_1+w_2+w_3\}, \\ -2^{m-2} & \text{if } u \in \{w_1+w_2, w_1+w_3, w_2+w_3\}. \end{cases}$$

Combining $\mathcal{T}_1$ and $\mathcal{T}_2$ we complete the proof. □

Remark 4.5. This remark is analogous to Remark 4.4. In Theorem 4.17, for given $\mathbb{F}_2$-linearly independent subset $\{w_1, w_2, w_3\}$, the Boolean function on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ given by

$$(x, y) \mapsto Tr_1^m(xw_1)Tr_1^m(xw_2)Tr_1^m(xw_3)$$

is a cubic function, which is used as the first summand in the definition of $F(x, y)$ in equation (4.9). In the proof of Theorem 4.17, we apply Lemma 4.16 for this cubic function. As in Remark 4.4, the degree of $F(x, y)$ is $max\{1 + deg(f), deg(h), 3\}$ under suitable conditions, which may be much larger than 3.

Theorem 4.17. *Let f and h be two Boolean functions on $\mathbb{F}_{2^m}$. Let $w_1, w_2, w_3 \in \mathbb{F}_{2^m}$ be linearly independent and $\gamma \in \mathbb{F}_{2^m}$. Assume that γ is a 0-linear structure of f, and w_1, w_2, w_3 are 0-linear structures of f and h. Then, the function F defined on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ by*

$$F(x, y) = Tr_1^m(xw_1)Tr_1^m(xw_2)Tr_1^m(xw_3)+Tr_1^m\big(x(L(y)+L(\gamma)f(y))\big)+h(y) \quad (4.9)$$

is bent and its dual is

$$\begin{aligned}\tilde{F}(x, y) &= Tr_1^m(yw_1)Tr_1^m(yw_2)Tr_1^m(yw_3) + Tr_1^m\big(y(L^{-1}(x) + \gamma f(L^{-1}(x)))\big)\\ &+ h(L^{-1}(x) + \gamma f(L^{-1}(x))).\end{aligned}$$

Proof. Let $\phi(y) = y + \gamma f(y)$. For every $(a, b) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$,

$$\widehat{\chi_F}(a, b) = \sum_{y\in\mathbb{F}_{2^m}} (-1)^{h(y)+Tr_1^m(by)} \sum_{x\in\mathbb{F}_{2^m}} (-1)^{Tr_1^m(w_1x)Tr_1^m(w_2x)Tr_1^m(w_3x)+Tr_1^m\left(x(\phi(y)+a)\right)}.$$

For the case $f(a) = 0$,

- $\phi(y) + a = 0$ when $y = a$,
- $\phi(y) + a \in \{w_1, w_2, w_3, w_1 + w_2 + w_3\}$ when $y \in \mathcal{A}_1 = \{a + w_1, a + w_2, a + w_3, a + w_1 + w_2 + w_3\}$
- $\phi(y) + a \in \{w_1 + w_2, w_1 + w_3, w_2 + w_3\}$ when $y \in \mathcal{A}_2 = \{a + w_1 + w_2, a + w_1 + w_3, a + w_2 + w_3\}$.

Then, following the steps in proof of Theorem 4.14 and using Lemma 4.16, we get

$$\begin{aligned}\widehat{\chi_F}(a, b) &= 3.2^{m-2}(-1)^{Tr_1^m(ba)+h(a)} + 2^{m-2}\sum_{y\in\mathcal{A}_1}(-1)^{Tr_1^m(by)+h(y)}\\ &\quad -2^{m-2}\sum_{y\in\mathcal{A}_2}(-1)^{Tr_1^m(by)+h(y)}\\ &= 2^{m-2}\left[(-1)^{Tr_1^m(ba)+h(a)}\right]\mathcal{S}\end{aligned}$$

where

$$\mathcal{S} \;=\; \left[3+\mathcal{S}_1+\mathcal{S}_2\right], \tag{4.10}$$

$\mathcal{S}_1 = (-1)^{Tr_1^m(bw_1)} + (-1)^{Tr_1^m(bw_2)} + (-1)^{Tr_1^m(bw_3)} + (-1)^{Tr_1^m(b(w_1+w_2+w_3)}$ and $\mathcal{S}_2 = (-1)^{Tr_1^m(b(w_1+w_2))} + (-1)^{Tr_1^m(b(w_1+w_3))} + (-1)^{Tr_1^m(b(w_2+w_3))}$. Let $(-1)^{Tr_1^m(bw_i)} = c_i$ where $c_i \in \mathbb{F}_2$, for $i = 1, 2, 3$. Then, $3 + \mathcal{S}_1 + \mathcal{S}_2 = \pm 4$ and hence $\widehat{\chi_F}(a, b) = \pm 2^m$. The proof for the case $f(a) = 1$ is very similar. □

As in Theorem 4.15, in the following we get a modification of Theorem 4.17 using two linear structures instead of one linear structure.

Theorem 4.18. *Let f, g and h be Boolean functions on $\mathbb{F}_{2^m}$. Let $w_1, w_2, w_3 \in \mathbb{F}_{2^m}$ be linearly independent and $\gamma, \delta \in \mathbb{F}_{2^m}$, $\gamma \neq \delta$. Assume that γ is a 0-linear structure of f, δ is a 0-linear structure of f and g. Moreover, assume that w_1, w_2, w_3 are 0-linear structures of f, g and h. Then, the function F defined on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ by*

$$F(x,y) = Tr_1^m(xw_1)Tr_1^m(xw_2)Tr_1^m(xw_3) + Tr_1^m\big(x(L(y)+L(\gamma)f(y)+L(\delta)g(y))\big) + h(y)$$

is bent and its dual is

$$\tilde{F}(x,y) \;=\; Tr_1^m(yw_1)Tr_1^m(yw_2)Tr_1^m(yw_3) + Tr_1^m\big(y\rho^{-1}(x)\big) + h(\rho^{-1}(x))$$

where

$$\begin{aligned}\rho^{-1}(x) \;=\;& L^{-1}(x) + \gamma f(L^{-1}(x)) \\ &+ \delta\left[g(L^{-1}(x))\big(1+f(L^{-1}(x))\big) + g(L^{-1}(x)+\gamma)f(L^{-1}(x))\right].\end{aligned}$$

CHAPTER 5

CONCLUSION

Bent and semi-bent functions are widely studied concepts and have enjoyed a lot of interest in the literature because of their applications in cryptography. Among Boolean functions they are very rare and there is not a systematic method for their classification and enumeration. In this thesis, we studied characterization, enumeration and construction of bent and semi-bent functions. Chapter 1 describes the general overview and motivation of the thesis. In Chapter 2 preliminary technical information related to the other chapters is given. The first part of the main work in this thesis is presented in Chapter 3. We contribute to the knowledge of semi-bent functions by proposing a characterization for the class of quadratic functions with the form

$$f(x) = \sum_{i=1}^{\frac{n}{2}-1} c_i Tr_1^n(x^{1+2^i}) + Tr_1^{n/2}(x^{1+2^{n/2}}), \quad c_i \in \mathbb{F}_2, \quad x \in \mathbb{F}_{2^n}. \tag{5.1}$$

We give a characterization of these functions for semi-bentness by specifying the necessary and sufficient condition on c_i's. Furthermore, we present a generic method for enumeration of quadratic bent and semi-bent functions and give the number of semi-bent functions of the form (5.1). The method that we proposed for counting quadratic functions is rather comprehensive since it is applicable for counting all quadratic functions whose characterization is given via *gcd* computation. By utilizing this method, we complement the enumeration results for quadratic semi-bent functions of the form (3.8) and for quadratic bent functions of the form (A.3) and (3.10). We also correct some results on bent functions given by Ma et al.[34].

Chapter 4 constitutes the second part of the main work in this thesis by proposing several constructions of bent and semi-bent functions. Our first motive is to study the functions belong to the Maiorana-McFarland class which are of the form $H(x, y) = Tr_1^m(x\phi(y)) + h(y)$. We give explicit constructions of bent and semi-bent functions. Also, using these constructions and other algebraic structures we obtain secondary constructions of bent and semi-bent functions. Chapter 4 is composed of six sections and the contributions are listed as follows.

- In Section 4.2, we first investigate the case where $\phi(y) = y+\gamma f(y)$ and construct bent and semi-bent functions of the form

$$H(x, y) = Tr_1^m(xy + \gamma x f(y)) + h(y)$$

by identifying the linear structures $\gamma \in \mathbb{F}_{2^m}^\star$ of the Boolean function f. Also, we proved that the results are analogous when we have $\phi(y) = L(y) + L(\gamma)f(y)$ where $L(y)$ is a linearized polynomial.

- In Section 4.3, we extend the case in Section 4.2 to the case where there are two linear structures. We present constructions of bent and semi-bent functions of the form
$$H(x, y) = Tr_1^m(xy + \gamma x f(y) + \delta x g(y)) + h(y)$$
where $\gamma, \delta \in \mathbb{F}_{2^m}^\star$ are linear structures of Boolean functions f and g.

- Section 4.4 is a generalization of Section 4.2. It deals with the functions of the same form as in Section 4.2 but with differences where f is a function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^k}$ and γ is a linear translator of f instead of a linear structure. Then, it is shown that $H(x, y)$ is bent when γ is a c-linear translator of f, $c \in \mathbb{F}_{2^m}$ and $c \neq 1$, and $H(x, y)$ is k-plateaued when γ is a 1-linear translator of f and $h(y) = 0$. For the bentness case, the dual of H is given explicitly and for the k-plateaued case, Walsh-Hadamard transform values of H are computed.

- In Section 4.5, we focus on bent functions of the shape $g(x) = f_1(x)f_2(x) + f_1(x)f_3(x) + f_2(x)f_3(x)$ studied in [40] where f_1, f_2 and f_3 are three pairwise distinct bent functions over $\mathbb{F}_{2^n}$. We construct bent functions of this form by using linear translators of the functions f_1, f_2 and f_3 and compute dual functions $\tilde{g}$. The functions $g(x)$ studied in this section do not belong to the class of Maiorana Mc-Farland.

- In Section 4.6, a secondary construction of bent and semi-bent functions using derivatives and linear translators is presented.

- In Section 4.7, a secondary construction of bent functions of the form
$$F(x, y) = Tr_1^m(xw_1)Tr_1^m(xw_2) + Tr_1^m\big(xy + \gamma x f(y)\big) + h(y)$$
using certain quadratic and cubic functions together with linear structures is shown.

REFERENCES

[1] J. Arndt, *Matters Computational - Ideas, Algorithms, Source Code [The fxtbook]*, www.jjj.de, 2010.

[2] S. Boztas and P. V. Kumar, Binary sequences with gold-like correlation but larger linear span, IEEE Transactions on Information Theory, 40(2), pp. 532–537, 1994.

[3] A. Canteaut, C. Carlet, P. Charpin, and C. Fontaine, On cryptographic properties of the cosets of r(1, m), IEEE Transactions on Information Theory, 47(4), pp. 1494–1513, 2001.

[4] A. Canteaut and M. Naya-Plasencia, Structural weakness of mappings with a low differential uniformity, in *Conference on Finite Fields and Applications*, 2009.

[5] C. Carlet, On bent and highly nonlinear balanced/resilient functions and their algebraic immunities, in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, 16th International Symposium, AAECC-16*, pp. 1–28, 2006.

[6] C. Carlet, Boolean functions for cryptography and error correcting codes, In Chapter of the monography "Boolean Models and Methods in Mathematics, Computer Science, and Engineering" published by Cambridge University Press, Yves Crama and Peter L. Hammer (eds.), pp. 257–397, 2010.

[7] C. Carlet, Open problems on binary bent functions, in *Open Problems in Mathematics and Computational Science*, pp. 203–241, Springer International Publishing, 2014, ISBN 978-3-319-10682-3.

[8] C. Carlet and P. Guillot, A new representation of boolean functions, in M. Fossorier, H. Imai, S. Lin, and A. Poli, editors, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, volume 1719 of *Lecture Notes in Computer Science*, pp. 94–103, Springer Berlin Heidelberg, 1999.

[9] C. Carlet and S. Mesnager, On semibent boolean functions, IEEE Transactions on Information Theory, 58(5), pp. 3287–3292, 2012.

[10] C. Carlet and E. Prouff, On plateaued functions and their constructions, in *Fast Software Encryption, 10th International Workshop, FSE 2003, Lund, Sweden, February 24-26, 2003*, pp. 54–73, 2003.

[11] C. Carlet and J. L. Yucas, Piecewise constructions of bent and almost optimal boolean functions, Des. Codes Cryptography, 37(3), pp. 449–464, 2005.

[12] P. Charpin and G. Kyureghyan, Monomial functions with linear structure and permutation polynomials, in *Proceedings of the 9th Int. Conference on Finite Fields and their ApplicationsF_q9, Comtemporary Mathematics, AMS*, volume 518, pp. 99–111, 2010.

[13] P. Charpin and G. M. M. Kyureghyan, On a class of permutation polynomials over f_{2^m}, in *Sequences and Their Applications - SETA 2008, 5th International Conference, Lexington, KY, USA, September 14-18, 2008, Proceedings*, pp. 368–376, 2008.

[14] P. Charpin and G. M. M. Kyureghyan, When does g(x)+gammatr(h(x)) permute f_{p^n}?, Finite Fields and Their Applications, 15(5), pp. 615–632, 2009.

[15] P. Charpin, G. M. M. Kyureghyan, and V. Suder, Sparse permutations with low differential uniformity, Finite Fields and Their Applications, 28, pp. 214–243, 2014.

[16] P. Charpin, S. Mesnager, and S. Sarkar, On involutions of finite fields, in *Proceedings of 2015 IEEE International Symposium on Information Theory, ISIT*, 2015.

[17] P. Charpin, E. Pasalic, and C. Tavernier, On bent and semi-bent quadratic boolean functions, IEEE Transactions on Information Theory, 51(12), pp. 4286–4298, 2005.

[18] P. Charpin and S. Sarkar, Polynomials with linear structure and maiorana-mcfarland construction, IEEE Transactions on Information Theory, 57(6), pp. 3796–3804, 2011.

[19] S. Chee, S. Lee, and K. Kim, Semi-bent functions, in J. Pieprzyk and R. Safavi-Naini, editors, *Advances in Cryptology — ASIACRYPT'94*, volume 917 of *Lecture Notes in Computer Science*, pp. 105–118, Springer Berlin Heidelberg, 1995.

[20] J. F. Dillon, Elementary Hadamard Difference Sets, Ph.D. Dissertation, Univ. of Maryland, 1974.

[21] F. Fu, H. Niederreiter, and F. Özbudak, Joint linear complexity of arbitrary multisequences consisting of linear recurring sequences, Finite Fields and Their Applications, 15(4), pp. 475–496, 2009.

[22] F. Fu, H. Niederreiter, and F. Özbudak, Joint linear complexity of multisequences consisting of linear recurring sequences, Cryptography and Communications, 1(1), pp. 3–29, 2009.

[23] R. Gold, Maximal recursive sequences with 3-valued recursive cross-correlation functions, Information Theory, IEEE Transactions on, 14(1), pp. 154–156, 1968.

[24] T. Helleseth and P. V. Kumar, Sequences with low correlation, Handbook of coding theory, 2, pp. 1765–1853, 1998.

[25] H. Hu and D. Feng, On quadratic bent functions in polynomial forms, IEEE Transactions on Information Theory, 53(7), pp. 2610–2615, 2007.

[26] K. Khoo, G. Gong, and D. Stinson, A new family of gold-like sequences, in *Proceedings IEEE International Symposium on Information Theory*, volume 181, 2002.

[27] K. Khoo, G. Gong, and D. R. Stinson, A new characterization of semi-bent and bent functions on finite fields, Des. Codes Cryptography, 38(2), pp. 279–295, 2006.

[28] N. Koçak, O. Koçak, F. Özbudak, and Z. Saygi, Characterisation and enumeration of a class of semi-bent quadratic boolean functions, Int. J. of Information and Coding Theory, 3(1), pp. 39–57, 2015.

[29] N. Koçak, S. Mesnager, and F. Özbudak, Bent and semi-bent functions via linear translators, in *Fifteenth IMA International Conference on Cryptography and Coding*, 2015.

[30] G. M. Kyureghyan, Constructing permutations of finite fields via linear translators, J. Comb. Theory, Ser. A, 118(3), pp. 1052–1061, 2011.

[31] X. Lai, Additive and linear structures of cryptographic functions, in *Fast Software Encryption: Second International Workshop. Leuven, Belgium, 14-16 December 1994, Proceedings*, pp. 75–85, 1994.

[32] P. Langevin and G. Leander, Counting all bent functions in dimension eight 99270589265934370305785861242880, Designs, Codes and Cryptography, 59(1-3), pp. 193–205, 2011, ISSN 0925-1022.

[33] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, Cambridge University Press, 1997.

[34] W. Ma, M. Lee, and F. Zhang, A new class of bent functions, IEICE Trans. Fundam. Electron. Commun. Comput. Sci., E88-A(7), pp. 2039–2040, 2005.

[35] W. Meidl, S. Roy, and A. Topuzoglu, Enumeration of quadratic functions with prescribed walsh spectrum, IEEE Transactions on Information Theory, 60(10), pp. 6669–6680, 2014.

[36] S. Mesnager, Bent and hyper-bent functions in polynomial form and their link with some exponential sums and dickson polynomials, IEEE Transactions on Information Theory, 57(9), pp. 5996–6009, 2011.

[37] S. Mesnager, *Contributions on Boolean Functions for Symmetric Cryptography and Error Correcting Codes*, HdR (Habilitation to Direct Research) thesis in Mathematics, University of Paris VIII, 2012.

[38] S. Mesnager, Semi-bent functions from oval polynomials, in *Cryptography and Coding - 14th IMA International Conference, IMACC 2013, Oxford, UK, December 17-19, 2013. Proceedings*, pp. 1–15, 2013.

[39] S. Mesnager, On semi-bent functions and related plateaued functions over the galois field f_{2^n}, in C. K. Koç, editor, *Open Problems in Mathematics and Computational Science*, pp. 243–273, Springer International Publishing, 2014, ISBN 978-3-319-10682-3.

[40] S. Mesnager, Several new infinite families of bent functions and their duals, IEEE Transactions on Information Theory, 60(7), pp. 4397–4407, 2014.

[41] S. Mesnager, *Bent functions: fundamentals and results*, Springer, To Appear, 2015.

[42] S. Mesnager, Further constructions of infinite families of bent functions from new permutations and their duals, Journal of Cryptography and Communications (CCDS), To appear, 2015.

[43] O. S. Rothaus, On "bent" functions, J. Comb. Theory, Ser. A, 20(3), pp. 300–305, 1976.

[44] T. Siegenthaler, Correlation-immunity of nonlinear combining functions for cryptographic applications, IEEE Transactions on Information Theory, 30(5), pp. 776–780, 1984.

[45] G. Sun and C. Wu, Construction of Semi-Bent Boolean Functions in Even Number of Variables , Chin. J. Electron., 18(2), pp. 231–237, 2009.

[46] C. Tang and Y. Qi, Effective construction of a class of bent quadratic boolean functions, CoRR, abs/1308.2798, 2013.

[47] C. Tang and Y. Qi, A new class of semi-bent quadratic boolean functions, IACR Cryptology ePrint Archive, 2013/493.

[48] N. Tokareva, On the number of bent functions from iterative constructions: lower bounds and hypotheses, Adv. in Math. of Comm., 5(4), pp. 609–621, 2011.

[49] N. Tokareva, *Bent functions: results and applications to cryptography*, Elsevier, 2015.

[50] P. Udaya, Polyphase and frequency hopping sequences obtained from finite rings, Ph. D. dissertation, Indian Inst. Technol., Kanpur, India, 1992.

[51] N. Y. Yu and G. Gong, Constructions of quadratic bent functions in polynomial forms, IEEE Transactions on Information Theory, 52(7), pp. 3291–3299, 2006.

[52] Y. Zheng and X. Zhang, Plateaued functions, in *Information and Communication Security, Second International Conference, ICICS'99*, pp. 284–300, 1999.

APPENDIX A

Results Related to Propositions 4.4 and 4.8

The following proposition is related to Proposition 4.4 in Section 4.3.

Proposition A.1. *Let H be defined by equation (4.2), γ and δ be defined as in Proposition 4.4. Then the dual of H is $\tilde{H}(x,y) = Tr_1^m\left(y\phi^{-1}(x)\right) + h(\phi^{-1}(x))$ where $\phi^{-1} = {\pi_2}^{-1} \circ \rho^{-1} \circ {\pi_1}^{-1}$ and $\rho^{-1}(x)$ is given as follows.*

(i) If γ is a 0-linear structure of f, δ is a 0-linear structure of f and g, then

$$\rho^{-1}(x) = x + \gamma f(x) + \delta\left[g(x)(1+f(x)) + g(x+\gamma)f(x)\right].$$

(ii) If γ is a 0-linear structure of f, δ is a 1-linear structure of f and $\delta+\gamma$ is a 0-linear structure of g, then

$$\begin{aligned}\rho^{-1}(x) &= x + \gamma\left[g(x) + f(x)\big(1+g(x)+g(x+\gamma)\big)\right] \\ &\quad + \delta\left[g(x)(1+f(x)) + g(x+\gamma)f(x)\right].\end{aligned}$$

(iii) If δ is a 0-linear structure of g, γ is a 0-linear structure of f and g, then

$$\rho^{-1}(x) = x + \gamma\left[f(x)(1+g(x)) + f(x+\delta)g(x)\right] + \delta g(x).$$

(iv) If δ is a 0-linear structure of g, γ is a 1-linear structure of g and $\delta+\gamma$ is a 0-linear structure of f, then

$$\begin{aligned}\rho^{-1}(x) &= x + \gamma\left[f(x)(1+g(x)) + f(x+\delta)g(x)\right] \\ &\quad + \delta\left[f(x)(1+g(x)) + \big(1+f(x+\delta)\big)g(x)\right].\end{aligned}$$

(v) If δ is a 1-linear structure of f or δ is a 0-linear structure of g, then

$$\rho^{-1}(x) = x + \gamma\left[f(x)(1+g(x+\delta)) + \big(1+f(x)\big)g(x)\right] + \delta f(x).$$

(vi) If γ is a 1-linear structure of g, δ is a 1-linear structure of f and g, then

$$\rho^{-1}(x) = x + \gamma g(x) + \delta\left[f(x)(1+g(x)) + f(x+\gamma)g(x)\right].$$

Proof. We give only the proof for the case (i). Assume that γ is a 0-linear structure of f, δ is a 0-linear structure of f and g, then we claim that

$$\rho^{-1}(x) = \begin{cases} x & \text{if } f(x) = 0 \text{ and } g(x) = 0 \\ x + \delta & \text{if } f(x) = 0 \text{ and } g(x) = 1 \\ x + \gamma & \text{if } f(x) = 1 \text{ and } g(x + \gamma) = 0 \\ x + \gamma + \delta & \text{if } f(x) = 1 \text{ and } g(x + \gamma) = 1 \end{cases} \tag{A.1}$$

Let $\rho(y) = a$. Then,

$$y + \gamma f(y) + \delta g(y) \;\; = \;\; a \tag{A.2}$$

Taking f of both sides gives $f(y + \gamma f(y) + \delta g(y)) = f(a)$. Since γ and δ are 0-linear structures of f, we get

$$f(y) \;\; = \;\; f(a). \tag{A.3}$$

Note that, $\big(f(a), g(a)\big) \in \{(0,0),(0,1),(1,0),(1,1)\}$. These four cases correspond to the cases in equation (A.1). We prove only the first case in equation (A.1) and the proofs of other cases are similar. Hence, we assume that $(f(a), g(a)) = (0,0)$. Then, by equation (A.3), $f(y) = 0$ and by equation (A.2), $y + \delta g(y) = a$. Taking g of both sides and using that δ is a 0-linear structure of g, we obtain that $g(y + \delta g(y)) = g(y) = g(a)$. As $g(a) = 0$ by our assumption, we get $g(y) = 0$ and putting $f(y) = g(y) = 0$ in equation (A.2) we conclude that $y = a$.
Finally, the equation (A.1) can be written in the form

$$\rho^{-1}(x) = x + \gamma f(x) + \delta \left[g(x)(1 + f(x)) + g(x + \gamma) f(x) \right].$$

□

The following five propositions are related to Proposition 4.8 in Section 4.5.

Proposition A.2. *Let f and g be functions from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$. For $i \in \{1,2,3\}$ set $\phi_i(y) := y + \gamma_i f(y) + \delta_i g(y)$ where*

(i) *γ_1, γ_2, γ_3 are elements of $\mathbb{F}_{2^m}^\star$ which are 0-linear structures of f;*

(ii) *δ_1, δ_2 and δ_3 are elements of $\mathbb{F}_{2^m}^\star$ which are 1-linear structures of f;*

(iii) *$\gamma_1 + \delta_1$, $\gamma_2 + \delta_2$, $\gamma_3 + \delta_3$ are 0-linear structures of g;*

(iv) *$\gamma_1 + \gamma_2$ and $\gamma_1 + \gamma_3$ are 0-linear structures of g.*

Then the function h defined on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ by

$$\begin{aligned} h(x,y) \;\; &= \;\; Tr_1^m\Big(x\phi_1(y)\Big) Tr_1^m\Big(x\phi_2(y)\Big) + Tr_1^m\Big(x\phi_1(y)\Big) Tr_1^m\Big(x\phi_3(y)\Big) \\ &+ \;\; Tr_1^m\Big(x\phi_2(y)\Big) Tr_1^m\Big(x\phi_3(y)\Big) \end{aligned}$$

is bent and the dual of h is given by

$$\begin{aligned}\tilde{h}(x,y) &= Tr_1^m\Big(y\phi_1^{-1}(x)\Big)Tr_1^m\Big(y\phi_2^{-1}(x)\Big)+Tr_1^m\Big(y\phi_1^{-1}(x)\Big)Tr_1^m\Big(y\phi_3^{-1}(x)\Big)\\ &+ Tr_1^m\Big(y\phi_2^{-1}(x)\Big)Tr_1^m\Big(y\phi_3^{-1}(x)\Big)\end{aligned}$$

where

$$\begin{aligned}\phi_i^{-1}(x) &= x+\gamma\left[g(x)+f(x)\big(1+g(x)+g(x+\gamma)\big)\right]\\ &+ \delta\left[g(x)(1+f(x))+g(x+\gamma)f(x)\right].\end{aligned}$$

Proposition A.3. *Let f and g be functions from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$. For $i \in \{1,2,3\}$ set $\phi_i(y) := y+\gamma_i f(y)+\delta_i g(y)$ where*

(i) γ_1, γ_2, γ_3 are elements of $\mathbb{F}_{2^m}^\star$ which are 0-linear structures of f and g;

(ii) δ_1, δ_2 and δ_3 are elements of $\mathbb{F}_{2^m}^\star$ which are 0-linear structures of g;

(iii) $\delta_1+\delta_2$ and $\delta_1+\delta_3$ are 0-linear structures of f.

Then the function h defined on $\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$ by

$$\begin{aligned}h(x,y) &= Tr_1^m\Big(x\phi_1(y)\Big)Tr_1^m\Big(x\phi_2(y)\Big)+Tr_1^m\Big(x\phi_1(y)\Big)Tr_1^m\Big(x\phi_3(y)\Big)\\ &+ Tr_1^m\Big(x\phi_2(y)\Big)Tr_1^m\Big(x\phi_3(y)\Big)\end{aligned}$$

is bent and the dual of h is given by

$$\begin{aligned}\tilde{h}(x,y) &= Tr_1^m\Big(y\phi_1^{-1}(x)\Big)Tr_1^m\Big(y\phi_2^{-1}(x)\Big)+Tr_1^m\Big(y\phi_1^{-1}(x)\Big)Tr_1^m\Big(y\phi_3^{-1}(x)\Big)\\ &+ Tr_1^m\Big(y\phi_2^{-1}(x)\Big)Tr_1^m\Big(y\phi_3^{-1}(x)\Big)\end{aligned}$$

where $\phi_i^{-1}(x) = x+\gamma\left[f(x)(1+g(x))+f(x+\delta)g(x)\right]+\delta g(x)$.

Proposition A.4. *Let f and g be functions from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$. For $i \in \{1,2,3\}$ set $\phi_i(y) := y+\gamma_i f(y)+\delta_i g(y)$ where*

(i) γ_1, γ_2, γ_3 are elements of $\mathbb{F}_{2^m}^\star$ which are 1-linear structures of g;

(ii) δ_1, δ_2 and δ_3 are elements of $\mathbb{F}_{2^m}^\star$ which are 0-linear structures of g;

(iii) $\gamma_1+\delta_1$, $\gamma_2+\delta_2$, $\gamma_3+\delta_3$ are 0-linear structures of f;

(iv) $\delta_1+\delta_2$ and $\delta_1+\delta_3$ are 0-linear structures of f.

Then the function h defined on $\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$ by

$$\begin{aligned}h(x,y) &= Tr_1^m\Big(x\phi_1(y)\Big)Tr_1^m\Big(x\phi_2(y)\Big)+Tr_1^m\Big(x\phi_1(y)\Big)Tr_1^m\Big(x\phi_3(y)\Big)\\ &+ Tr_1^m\Big(x\phi_2(y)\Big)Tr_1^m\Big(x\phi_3(y)\Big)\end{aligned}$$

is bent and the dual of h is given by

$$\begin{aligned}\tilde{h}(x,y) &= Tr_1^m\Big(y\phi_1^{-1}(x)\Big)Tr_1^m\Big(y\phi_2^{-1}(x)\Big)+Tr_1^m\Big(y\phi_1^{-1}(x)\Big)Tr_1^m\Big(y\phi_3^{-1}(x)\Big)\\ &+ Tr_1^m\Big(y\phi_2^{-1}(x)\Big)Tr_1^m\Big(y\phi_3^{-1}(x)\Big)\end{aligned}$$

where

$$\begin{aligned}\phi_i^{-1}(x) &= x+\gamma\left[f(x)(1+g(x))+f(x+\delta)g(x)\right]\\ &+ \delta\left[f(x)(1+g(x))+\big(1+f(x+\delta)\big)g(x)\right].\end{aligned}$$

Proposition A.5. *Let f and g be functions from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$. For $i\in\{1,2,3\}$ set $\phi_i(y):=y+\gamma_i f(y)+\delta_i g(y)$ where*

(i) γ_1, γ_2, γ_3 are elements of $\mathbb{F}_{2^m}^\star$ which are 1-linear structures of f and g;

(ii) δ_1, δ_2 and δ_3 are elements of $\mathbb{F}_{2^m}^\star$ which are 1-linear structures of f;

(iii) $\delta_1+\delta_2$ and $\delta_1+\delta_3$ are 0-linear structures of g.

Then the function h defined on $\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$ by

$$\begin{aligned}h(x,y) &= Tr_1^m\Big(x\phi_1(y)\Big)Tr_1^m\Big(x\phi_2(y)\Big)+Tr_1^m\Big(x\phi_1(y)\Big)Tr_1^m\Big(x\phi_3(y)\Big)\\ &+ Tr_1^m\Big(x\phi_2(y)\Big)Tr_1^m\Big(x\phi_3(y)\Big)\end{aligned}$$

is bent and the dual of h is given by

$$\begin{aligned}\tilde{h}(x,y) &= Tr_1^m\Big(y\phi_1^{-1}(x)\Big)Tr_1^m\Big(y\phi_2^{-1}(x)\Big)+Tr_1^m\Big(y\phi_1^{-1}(x)\Big)Tr_1^m\Big(y\phi_3^{-1}(x)\Big)\\ &+ Tr_1^m\Big(y\phi_2^{-1}(x)\Big)Tr_1^m\Big(y\phi_3^{-1}(x)\Big)\end{aligned}$$

where $\phi_i^{-1}(x)=x+\gamma\left[f(x)(1+g(x+\delta))+\big(1+f(x)\big)g(x)\right]+\delta f(x)$.

Proposition A.6. *Let f and g be functions from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$. For $i\in\{1,2,3\}$ set $\phi_i(y):=y+\gamma_i f(y)+\delta_i g(y)$ where*

(i) γ_1, γ_2, γ_3 are elements of $\mathbb{F}_{2^m}^\star$ which are 1-linear structures of g;

(ii) δ_1, δ_2 and δ_3 are elements of $\mathbb{F}_{2^m}^\star$ which are 1-linear structures of f and g;

(iii) $\gamma_1+\gamma_2$ and $\gamma_1+\gamma_3$ are 0-linear structures of f.

Then the function h defined on $\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$ by

$$\begin{aligned}h(x,y) &= Tr_1^m\Big(x\phi_1(y)\Big)Tr_1^m\Big(x\phi_2(y)\Big)+Tr_1^m\Big(x\phi_1(y)\Big)Tr_1^m\Big(x\phi_3(y)\Big)\\ &+ Tr_1^m\Big(x\phi_2(y)\Big)Tr_1^m\Big(x\phi_3(y)\Big)\end{aligned}$$

is bent and the dual of h *is given by*

$$\begin{aligned}\tilde{h}(x,y) &= Tr_1^m\Big(y\phi_1^{-1}(x)\Big)Tr_1^m\Big(y\phi_2^{-1}(x)\Big) + Tr_1^m\Big(y\phi_1^{-1}(x)\Big)Tr_1^m\Big(y\phi_3^{-1}(x)\Big) \\ &+ Tr_1^m\Big(y\phi_2^{-1}(x)\Big)Tr_1^m\Big(y\phi_3^{-1}(x)\Big)\end{aligned}$$

where $\phi_i^{-1}(x) = x + \gamma g(x) + \delta\left[f(x)(1+g(x)) + f(x+\gamma)g(x)\right]$.

CURRICULUM VITAE

PERSONAL INFORMATION

Surname, Name: Koçak, Neşe
Nationality: Turkish
Date and Place of Birth: 1984, Kocaeli
Marital Status: Married

EDUCATION

Degree	**Institution**	**Year of Graduation**
M.S.	Department of Cryptography, METU	2009
B.S.	Department of Mathematics, METU	2007
High School	Karamürsel Anatolian High School	2002

PROFESSIONAL EXPERIENCE

Year	**Place**	**Enrollment**
01.2015-	ASELSAN Inc.	Expert Algorithm Designer
10.2011-12.2014	IAM, METU	Res. Asst.
11.2007-10.2011	GSNAS, METU	Res. Asst.

PUBLICATIONS

N. Koçak, S. Mesnager, F. Özbudak, *Bent and Semi-bent Functions via Linear Translators*, Fifteenth IMA International Conference on Cryptography and Coding, Oxford, UK, 2015.

N. Koçak, O. Koçak, F. Özbudak, Z.Saygı, *Characterisation and Enumeration of a Class of Semi-Bent Quadratic Boolean Functions*, Int. J. Information and Coding Theory, vol.3, no 2, 39-57, 2015.

O. Koçak, O. Kurt, N. Öztop, Z.Saygı, *Notes on Bent Functions in Polynomial Forms*, Int. J. Information Security Science, vol.1, no 2, 43-48, 2012.

O. Koçak, N. Öztop, *Cryptanalysis of TWIS Block Cipher*, WEWORC 2011, LNCS 7242, 109-121. Springer, Heidelberg, 2012.

B. Bilgin, N. Öztop, E. Uyan, *A Survey on Rebound Attack*, 4th International Information Security and Cryptology Conference, Ankara, Turkey, 2010.

A. Doğanaksoy, A. Darbuka, D. Özberk, N. Öztop, F. Sulak, *A Survey of the Attacks on AES*, 3rd International Information Security and Cryptology Conference, Ankara, Turkey, 2008.

A. Doğanaksoy, A. Darbuka, D. Özberk, N. Öztop, F. Sulak, *A Survey of the Related-Key Attacks on AES*, 3rd International Information Security and Cryptology Conference, Ankara, Turkey, 2008.