PERMUTATION POLYNOMIALS AND CONSTRUCTION OF BENT FUNCTIONS

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

BY

PINAR ONGAN

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

FEBRUARY 2021

Approval of the thesis:

PERMUTATION POLYNOMIALS AND CONSTRUCTION OF BENT FUNCTIONS

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

Prof. Dr. A. Sevtap Selçuk Kestel
Director, Graduate School of **Applied Mathematics** _____

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

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

Assoc. Prof. Dr. Burcu Gülmez Temür
Co-supervisor, **Mathematics, Atılım University** _____

Examining Committee Members:

Prof. Dr. Ersan Akyıldız
Institute of **Applied Mathematics, METU** _____

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

Assoc. Prof. Dr. Murat Cenk
Institute of **Applied Mathematics, METU** _____

Assoc. Prof. Dr. Ayça Çeşmelioğlu Gül
Department of **Mathematics, İstanbul Bilgi University** _____

Assist. Prof. Dr. Eda Tekin
Department of **Management, Karabük 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: PINAR ONGAN

Signature :

ABSTRACT

PERMUTATION POLYNOMIALS AND CONSTRUCTION OF BENT FUNCTIONS

Ongan, Pınar
Ph.D., Department of Cryptography
Supervisor : Assoc. Prof. Dr. Ali Doğanaksoy
Co-Supervisor : Assoc. Prof. Dr. Burcu Gülmez Temür

February 2021, 46 pages

This thesis consists of two main parts: In the first part, a study of several classes of permutation and complete permutation polynomials is given, while in the second part, a method of construction of several new classes of bent functions is described.

The first part consists of the study of several classes of binomials and trinomials over finite fields. A complete list of permutation polynomials of the form $f(x) = x^{\frac{q^n-1}{q-1}+1} + bx \in \mathbb{F}_{q^n}[x]$ is obtained for the case $n = 5$, and a criterion on permutation polynomials of the same type is derived for the general case. Furthermore, it is shown that when q is odd, trinomials of the form $f(x) = x^5 h(x^{q-1}) \in \mathbb{F}_{q^2}[x]$, where $h(x) = x^5 + x + 1$ never permutes $\mathbb{F}_{q^2}$.

A method of constructing several new classes of bent functions via linear translators and permutation polynomials forms the second part of the thesis. First, a way to lift a permutation over $\mathbb{F}_{2^t}$ to a permutation over $\mathbb{F}_{2^m}$ is described, where $t|m$. Then, via this method, 3-tuples of particular permutations that lead to new classes of bent functions are obtained. As a last step, the fact that none of the bent functions obtained here will be contained in Maiorana-McFarland class is proved.

Keywords: Finite Fields, Permutation Polynomials, Complete Permutation Polynomials, Bent Functions, Linear Translators, etc.

ÖZ

PERMÜTASYON POLİNOMLARI VE BÜKÜLMÜŞ FONKSİYONLARIN İNŞASI

Ongan, Pınar
Doktora, Kriptografi Bölümü
Tez Yöneticisi : Doç. Dr. Ali Doğanaksoy
Ortak Tez Yöneticisi : Doç. Dr. Burcu Gülmez Temür

Şubat 2021, 46 sayfa

Bu tez iki ana bölümden oluşmaktadır: İlk kısımda, çeşitli permütasyon ve tam permütasyon polinom sınıflarının incelenmesi verilirken; ikinci kısımda, birkaç yeni bükülmüş fonksiyon sınıfı inşası için bir yöntem tarif edilmektedir.

İlk kısım; sonlu cisimler üzerinde tanımlı çeşitli iki terimli ve üç terimli polinom sınıflarının incelenmesini içermektedir. $\mathbb{F}_{q^n}$ üzerinde tanımlı $f(x) = x^{(q^n-1)/(q-1)+1} + bx$ formundaki permütasyon polinomlarının $n = 5$ iken tamamı bir liste hâlinde sunulurken, her n için geçerli bir kriter de elde edilmektedir. Dahası; q tek iken, $h(x) = x^5 + x + 1$ durumunda $f(x) = x^5 h(x^{q-1}) \in \mathbb{F}_{q^2}[x]$ formundaki üç terimlilerin asla $\mathbb{F}_{q^2}$ cismini permüte etmeyeceği gösterilmektedir.

Doğrusal öteleyiciler ve permütasyon polinomları aracılığıyla birkaç yeni bükülmüş fonksiyon sınıfı inşa etme yöntemi ise tezin ikinci bölümünü oluşturmaktadır. İlk olarak; m'yi bölen $t$ler için, $\mathbb{F}_{2^t}[x]$'teki bir permütasyonu $\mathbb{F}_{2^m}[x]$'teki bir permütasyona yükseltmenin bir yolu tarif ediliyor. Daha sonra, bu yöntemle yeni bükülmüş fonksiyon sınıflarının inşasında kullanılacak olan çeşitli permütasyon 3'lüleri elde edilmektedir. Son olarak, burada elde edilen bükülmüş fonksiyonların hiçbirinin Maiorana-McFarland sınıfında yer almadığı kanıtlanmaktadır.

Anahtar Kelimeler: Sonlu Cisimler, Permütasyon Polinomları, Tam Permütasyon Polinomları, Bükülmüş Fonksiyonlar, Doğrusal Öteleyiciler, v.b.

To all my sisters and brothers who are empowered by each other in solidarity.

ACKNOWLEDGMENTS

I would like to express my deep and sincere gratitude to my co-advisor Burcu Gülmez Temür, advisor Ali Doğanaksoy, and my other Ph.D. Proceeding Committee members Ersan Akyıldız and Murat Cenk for giving me the opportunity to do research and providing invaluable guidance throughout this research. Their vision, sincerity, and motivation have deeply inspired me.

Furthermore, I would like to add that I have been very much aided by the instruction and direction of Ferruh Özbudak throughout a significant part of my Ph.D. study; for this, I am very much obliged. I would like to thank Sihem Mesnager and Yıldırım Akbal, the valuable mathematicians I had the opportunity to work within a part of my Ph.D. study.

I am grateful to have had the opportunity to work with all these mathematicians I have mentioned so far. They have taught me the methodology to carry out the research and present the results as clearly as possible. It was a great privilege and honor to work and study under their guidance. I would also like to thank them for their friendship and empathy.

I am deeply thankful to my parents Emine and İsmail Ongan, for their love, caring, and sacrifices. It is a pleasure to express my special thanks to Ali Ongan, Gün Şahin, Seçkin Şis, Elif Yaman, Cansu Yumuşak, Pınar Çağ, Gökçe Silsüpür, and, of course, again Burcu Gülmez Temür for helping me understand myself and stay strong. Without their support, it would not be so possible for me to continue this Ph.D. research. Their existence in my life made things easier.

Finally, my thanks go to all the friends, comrades, and sisters in solidarity who have supported me to complete the research work directly or indirectly.

TABLE OF CONTENTS

ABSTRACT vii

ÖZ ix

ACKNOWLEDGMENTS xiii

TABLE OF CONTENTS xv

LIST OF TABLES xvii

LIST OF ABBREVIATIONS xviii

CHAPTERS

1 INTRODUCTION 1

1.1 A Background and the Motivation of the Study 1

1.2 Outline of the Thesis 2

2 PRELIMINARIES 5

2.1 Permutation Polynomials and Complete Permutation Polynomials 5

2.2 Boolean Functions 7

2.3 Bent Functions 9

2.4 Linear Translators 11

2.5 The Vandermonde Matrix 11

2.6 Normalized Polynomials 12

2.7 Algebraic Curves 12

3 ON SEVERAL PERMUTATON POLYNOMIALS AND COMPLETE PERMUTATION POLYNOMIALS 15

3.1 Monomials 16

3.2 Several Binomials 16

3.3 Trinomials 22

4 A METHOD TO CONSTRUCT NEW CLASSES OF BENT FUNCTIONS 27

4.1 $(\mathcal{A}_m)$-condition 28

4.2 Several Constructions Using PPs Satisfying $(\mathcal{A}_m)$-condition . 28

4.3 Bent Functions Constructed in the Previous Section are out of the Maiorana-McFarland Class $\mathcal{M}$ 36

5 CONCLUSION 39

REFERENCES 41

CURRICULUM VITAE 45

LIST OF TABLES

Table 2.1 All normalized permutation polynomials of degree 6 over $\mathbb{F}_q$. [30] . 14

Table 3.1 The minimum value of N_q in each q-case, where $q < 77$. 26

LIST OF ABBREVIATIONS

$\forall$	for all
$\exists$	there exists
:	such that
$a\|b$	a divides b
$\mathbb{Z}^+$	the set of positive integers
$\mathbb{F}_q$	the finite field of q elements
$\overline{\mathbb{F}}$	the closure of the field F
γ	a fixed primitive element of $\mathbb{F}_{q^n}$
ζ	a primitive $(q-1)^{th}$ root of unity of $\mathbb{F}_{q^n}$
$\tilde{f}$	the dual of a bent function f
$ind_\gamma(\alpha)$	the discrete logarithm of $\alpha \in \mathbb{F}_{q^n}^*$
PP	permutation polynomial
CPP	complete permutation polynomial
N_q	the number of $\mathbb{F}_q$-rational points on the given curve
$\mathcal{N}_f$	the nonlinearity of a Boolean function f
$\mathcal{M}$	the Maiorana-McFarland Class

CHAPTER 1

INTRODUCTION

This chapter stands for representing a general background on the study of permutation polynomials, complete permutation polynomials, and bent functions. Section 1.1 summarizes our motivation behind this study on permutation polynomials and bent functions after giving a brief historical introduction to these subjects. Section 1.2 provides an outline of this thesis and lists all of our results.

1.1 A Background and the Motivation of the Study

Studies on the permutation property of a polynomial over a finite field have a quite long history. Besides cryptography, they have a raft of applications in coding theory, combinatorial design theory, etc.; therefore, finding new permutation polynomials is of great interest. Chapter 8 of the book [23] presents some up-to-date results on permutation polynomials in a condensed form. Furthermore, [13] is a survey showing more recent contributions related to the subject.

Up to our knowledge, as a subclass of permutation polynomials, complete permutation polynomials were first introduced by Niederreiter and Robinson in [26]. Finding new complete permutation polynomials is not an easy-to-solve problem, and there exist rare classes known. (See [16], [25] and [32] for further studies.)

On the other hand, having an undeniable role in many other areas of mathematics such as coding theory, combinatorics, and probability, both the design and the analysis of Boolean functions have been fascinating subjects for many cryptographers in the

last decades because of the rise in the need for much more cryptographically secure systems. Several cryptographic characteristics measure the employability of Boolean functions in cryptographically secure systems, and nonlinearity is one of the most critical ones. The importance of the study on the Boolean functions with maximum nonlinearity -which are called bent functions- lies here.

It was Oscar Rothaus who first described bent functions in the 1960s, but the research on this subject has intensified in recent decades, and still, there does not exist a complete classification of bent functions; both characterization and construction of them are challenging problems attracting the attention of many mathematicians nowadays. For a detailed survey presenting both the theoretical and application-oriented aspects of the subject, the reader may visit [21].

This thesis essentially consists of two main parts: The first one includes a study on permutation and complete permutation polynomials in which several classes are analyzed, and the second one is a study of bent functions in which a method of construction is described. The author's motivation stems from the relevance of each of these structures to cryptography, but the studies on all three structures are known to be used in other fields of mathematics and also engineering.

1.2 Outline of the Thesis

Together with this chapter, there exist five chapters in this thesis.

Chapter 2 stands for a technical introduction to the subject. Each notion that needs prior knowledge -such as definitions, basic properties, fundamental theorems, etc.- to follow the steps while proceeding towards the results is discussed separately here. So this chapter consists of seven sections: Permutation and complete permutation polynomials, Boolean functions, bent functions, linear translators, the Vandermonde Matrix, normalized polynomials, and algebraic curves.

The results obtained about permutation and complete permutation polynomials during this study are represented in Chapter 3. It starts with a section giving a commonly known result about the permutation property of monomials, and then its focal point

becomes several classes of binomials and trinomials. The main effort of this chapter is to describe all necessary and sufficient conditions on a particular type of polynomial required for getting a permutation (a complete permutation polynomial).

The main results of this chapter are Theorem 3.2.1, 3.2.2, and 3.3.1.

The aim of Chapter 4 is the presentation of new constructions of bent functions using linear translators and permutation polynomials. It starts with the presentation of the result Lemma 4.1.1 of earlier works [[17]] and [[19]] of Mesnager, which forms the foundation of the constructions presented throughout Chapter 4. Then, a way to lift a permutation to a permutation of a higher dimension is described in Proposition 4.2.1. With the help of Proposition 4.2.1 and Lemma 4.1.1, new families of bent functions are constructed in Theorem 4.2.2, 4.2.3, 4.2.4, and 4.2.5. Furthermore, in Section 4.3, it is also shown that the bent functions constructed in Section 4.2 will not be in the Maiorana-McFarland Class.

Finally, Chapter 5 summarizes the work and emphasizes all our contributions.

CHAPTER 2

PRELIMINARIES

This chapter can be taken as a technical introduction to the subject. Definitions, basic properties, and several earlier results which have been helpful to proceed towards the acquisitions of this study can be found in this chapter. Permutation and complete permutation polynomials, Boolean functions, bent functions, linear translators, the Vandermonde Matrix, normalized polynomials, and algebraic curves are the subjects summarized each in separate sections.

Throughout this chapter, let p be a prime number, $q = p^m$, for some $m \in \mathbb{Z}+$ be a power of p, $\mathbb{F}_q$ denote a finite field with q elements.

For any positive integer r and polynomial $h(x) \in \mathbb{F}_q[x]$, a polynomial of the form $x^r h(x^{(q-1)/d})$ where d divides $q-1$ is called *an r^{th} order cyclotomic polynomial of index d over $\mathbb{F}_q$*. Since every polynomial in $\mathbb{F}_q[x]$ can be written as an r^{th} order cyclotomic polynomial of index d over $\mathbb{F}_q$ if it fixes the zero element (for more details, see [33]), the study of cyclotomic polynomials forms a crucial part.

Let $n \in \mathbb{N}$, γ be a fixed primitive element of $\mathbb{F}_{q^n}$, $\zeta = \gamma^{\frac{q^n-1}{q-1}}$ be a primitive $(q-1)^{th}$ root of unity of $\mathbb{F}_{q^n}$, and $ind_\gamma(\alpha)$ denote *the discrete logarithm* of $\alpha \in \mathbb{F}_{q^n}^*$. (i.e. $l = ind_\gamma(\alpha)$ means that $l \in \mathbb{Z}$ such that $0 \leq l \leq q^{n-2}$ and $\gamma^l = \alpha$.)

2.1 Permutation Polynomials and Complete Permutation Polynomials

The *associated mapping* of the polynomial $f(x) \in \mathbb{F}_q[x]$ is the mapping $F : \mathbb{F}_q \to \mathbb{F}_q$ defined by $F(x) := f(x)$, and a polynomial $f(x) \in \mathbb{F}_q[x]$ is called a *permutation*

polynomial (PP) over $\mathbb{F}_q$ if its associated mapping is bijective. A PP $f(x) \in \mathbb{F}_q[x]$ with associated mapping $F(x)$ is called a *complete permutation polynomial (CPP)* over $\mathbb{F}_q$ if $F(x) + x$ is also a bijection. To start with, linearity is a basic property of PPs.

Lemma 2.1.1. *[24]If $f(x) \in \mathbb{F}_q[x]$ is a PP over $\mathbb{F}_q$, then so is $af(cx + d)$, for all $a, c, d \in \mathbb{F}_q$ satisfying that $a \neq 0$ and $c \neq 0$.*

Deciding whether a given polynomial is a CPP or at least a PP has been on the agenda of mathematicians for the last decades. Although several gaps has been filled recently, there still exist numerous classes of polynomials to be focused on.

If the polynomial under consideration is of the form (2.1), then the following result derived from a previous work of Wang for the field $\mathbb{F}_{q^n}$ with the choice $l = q - 1$ can be used as a useful tool in making this decision.

Theorem 2.1.2. *[34] Let $a_i \in \mathbb{F}_{q^n}^*$, where $0 \leq i \leq q - 2$. The polynomial*

$$f(x) = \frac{1}{q-1} \sum_{i=0}^{q-2} \sum_{j=0}^{q-2} a_i \zeta^{-ji} x^{r_i + js} \in \mathbb{F}_{q^n}[x], \tag{2.1}$$

is a PP over $\mathbb{F}_{q^n}$ if and only if the following statements are satisfied

i. $\gcd(r_i, s) = 1$, *for all $i \in \mathbb{Z}$ such that $0 \leq i \leq q - 2$.*

ii. $\{ind_\gamma(a_i) + ir_i \mid i = 0, 1, ..., q - 2\}$ *is a complete set of residues modulo $q - 1$.*

Moreover,

$$f^{-1}(x) = \frac{1}{q-1} \sum_{k=0}^{q-2} \sum_{j=0}^{q-2} b_k \zeta^{-jk} x^{r_k{}' + js}, \tag{2.2}$$

where

- $k := \varphi(i) \equiv ind_\gamma(a_i) + ir_i \mod q - 1$,
- $r_k{}' \equiv r_i{}^{-1} \mod s$,
- $b_k = a_i{}^{-r_k{}'} \gamma^{i(1 - r_i r_k{}')}$

for each $i \in \mathbb{Z}$ such that $0 \leq i \leq q - 2$.

However, tailoring the given polynomial into the form (2.1) -if it is possible- requires some work, too.

Furthermore, the following two results of Zieve reducing the study of a PP over $\mathbb{F}_{q^n}$ to the study of a permutation over a much more smaller field under certain conditions help researchers in finding a different perspective within the subject.

Theorem 2.1.3. *[37]Let $d, r \in \mathbb{Z}^+$ be such that $d \mid q^n - 1$ and $h(x) \in \mathbb{F}_{q^n}[x]$. Then $f(x) = x^r h\left(x^{(q^n-1)/d}\right)$ is a PP over $\mathbb{F}_{q^n}$ if and only if*

(i) $\gcd\left(r, \dfrac{q^n-1}{d}\right) = 1$,

(ii) $x^r h(x)^{(q^n-1)/d}$ *permutes μ_d, where $\mu_d = \{\alpha \in \mathbb{F}_{q^n}^* \mid \alpha^d = 1\}$.*

Theorem 2.1.4. *[36]Let $r, n, m \in \mathbb{Z}^+$ and $q = p^m$. Let $h(x) \in \mathbb{F}_{q^n}[x]$. Then $f(x) = x^r h\left(x^{\frac{q^n-1}{q-1}}\right)$ is a PP over $\mathbb{F}_{q^n}$ if and only if*

i. $\gcd\left(r, \dfrac{q^n-1}{q-1}\right) = 1$

ii. The polynomial

$$x^r h(x) h^q(x) h^{q^2}(x) ... h^{q^{n-1}}(x) \in \mathbb{F}_q[x]$$

is a PP over $\mathbb{F}_q$, where $h^{q^k}(x)$ denotes the polynomial obtained from $h(x)$ by raising every coefficient to the q^k-th power.

Also, under some circumstances, Bartoli et al. show that a PP of the form (2.3) comes with several restrictions.

Theorem 2.1.5. *[3]Let n be odd, $b \in \mathbb{F}_{q^n}^*$, and $q > \frac{((n-1)(n-2)+\sqrt{n^2+13n-2})^2}{4}$. If*

$$f(x) = x^{\frac{q^n-1}{q-1}+1} + bx \in \mathbb{F}_{q^n}[x] \tag{2.3}$$

is a PP over $\mathbb{F}_{q^n}$, then p divides $(n+1)/2$ and $Tr_1^n(b) = 0$.

2.2 Boolean Functions

Functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ are called *Boolean functions of n variables*. Since there exists a natural homomorphism between the fields $\mathbb{F}_2^n$ and $\mathbb{F}_{2^n}$, they can be taken as

functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$, too. Where $n = 2m$, a Boolean function with domain $\mathbb{F}_{2^n}$ is represantable in a bivariate form $f(x, y)$, where $x, y \in \mathbb{F}_{2^m}$. For a Boolean function f, being *affine* means having the property

$$f(\alpha + \beta) = f(\alpha) + f(\beta) + f(0), \tag{2.4}$$

for all $\alpha, \beta \in \mathbb{F}_{2^n}$.

A useful example of Boolean functions is the *absolute trace function* $Tr_1^n : \mathbb{F}_{2^n} \to \mathbb{F}_2$ which is defined by

$$Tr_1^n(x) := x + x^2 + x^4 + x^8 + ... + x^{2^{n-1}}.$$

The *Walsh transform* of $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is the function $\widehat{\chi_f} : \mathbb{F}_{2^n} \to \mathbb{Z}$ defined by

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

and the *nonlinearity* of $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is defined as

$$\mathcal{N}_f := \min| \{x \in \mathbb{F}_{2^n} \ : \ f(x) \neq A(x)\} |,$$

where the minimum is taken over the set of all affine functions $A(x)$ which are defined over $\mathbb{F}_{2^n}$, and it can also be characterized as

$$\mathcal{N}_f := 2^{n-1} - \frac{1}{2} \max_{\omega \in \mathbb{F}_{2^n}} |\widehat{\chi_f}(\omega)| .$$

Indeed, for a given Boolean function f used in a stream or block cipher, $\mathcal{N}_f$ is one of the significant cryptographical criteria against attacks on the cipher. Having a Boolean function far from easy-to-guess affine ones is one of the goals of a secure system, therefore $\mathcal{N}_f$ should not be low.

Theorem 2.2.1. *[9](Parseval's Relation)*

$$\sum_{\omega \in \mathbb{F}_{2^n}} (\widehat{\chi_f}(\omega))^2 = 2^{2n}.$$

As a result of Theorem 2.2.1, one has the inequality

$$\mathcal{N}_f \leq 2^{n-1} - 2^{\frac{n}{2}-1}. \tag{2.5}$$

In addition to that,

$$D_\alpha f(x) := f(x) + f(x + \alpha) \tag{2.6}$$

is the definition of *the first derivative of f in the direction of* α, and

$$D_\beta D_\alpha f(x) := f(x) + f(x+\alpha) + f(x+\beta) + f(x+\alpha+\beta). \tag{2.7}$$

is the definition of *the second derivative of f in the direction of α and β*, where $\alpha, \beta \in \mathbb{F}_{2^n}$ and f is a Boolean function. Therefore, (2.4) can also be stated as $D_\beta D_\alpha f(x)|_{x=0} = 0$.

A *vectorial Boolean function* is a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ defined as

$$F(x) = (f_1(x),\ f_2(x),\ ...,\ f_m(x))\,,$$

where each f_k is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$.

A Boolean function f is called *balanced* if the number of elements in the pre-image of 1 is equal to the number elements in the pre-image of 0. Such functions play a crucial role in the design of symmetric-key cryptography. For instance, in stream-ciphers, they are used in LFSRs to combine or filter the outputs, and so with the help of them, pseudo-random sequences are produced and can be used in a Vernam-like cipher. Furthermore, in block ciphers, S-boxes are designed by using an appropriate arrangement of a composition of properly chosen nonlinear Boolean functions.

2.3 Bent Functions

$f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is called a *bent function* if its nonlinearity attains its upper bound in (2.5), which is attainable only for even values of n. Therefore, by definition, bent functions exist for only even choices of n. The *algebraic degree* $deg(f)$ of a bent function is the number of variables in the highest order term with nonzero coefficient.

It is also possible to decide whether a given function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ (n even) is bent or not by using the Walsh transform: f will be bent if and only if $\widehat{\chi_f}(\omega) = \pm 2^{\frac{n}{2}}$, for all $\omega \in \mathbb{F}_{2^n}$. Moreover, the *dual function* $\tilde{f}$ of a bent function f is defined by the equality $\widehat{\chi_f}(\omega) = 2^{n/2}(-1)^{\tilde{f}(\omega)}$, $\forall \omega \in \mathbb{F}_{2^n}$. Indeed, the dual of a bent function will definitely be bent. (See [29].) However, the duals of given bent functions are not so easy to compute in general.

The essence of the matter, although having a high nonlinearity is one of the aimed

goals of Boolean functions used in cryptography, bent functions are neither balanced nor strong enough against fast algebraic attacks. Since the algebraic degree of an n-variable bent function is $\leq n/2$ -i.e., too small-, unfortunately, its vulnerability against fast algebraic attacks will still remain even after modifications to balance them.

These kinds of functions had already been studied by Dillon [12] in 1974, while they were first named by Rothaus [29] in 1976. Contradicting to their plain definition, mostly, they have a challenging nature to deal with. Although an extensive work on both classification and characterization of them has been done since the 1970s, they still remain as an interesting subject to study. Accompanied with a historical perspective, in order to investigate the connections of this subject with design theory, coding theory, and cryptography, the reader may visit the survey paper [10]. Furthermore, Mesnager's book [21] published a few years ago represents a full-scale study on the subject.

Construction of bent functions can be considered in two main branches: primary constructions (i.e. constructions from the beginning) and secondary constructions (i.e. constructions using previously constructed ones for designing new ones). Amongst former ones, the widest class is given by the Maiorana-McFarland class $\mathcal{M}$. (For more details, see [7] and Section 7.1 in [21].) A Boolean function $f : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ is said to be *in* $\mathcal{M}$ if it is of the form

$$f(x, y) = Tr_1^m(x, \pi(y)) + h(y),$$

for some $h : \mathbb{F}_{2^m} \to \mathbb{F}_2$ and $\pi : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$.

For a fixed element y of $\mathbb{F}_{2^m}$, take $x_1,\ x_2 \in \mathbb{F}_{2^m}$, then

$$\begin{aligned} f(x_1 + x_2, y) = Tr_1^m(x_1, \pi(y)) + Tr_1^m(x_2, \pi(y)) + h(y) \\ = f(x_1, y) + f(x_2, y) + h(y). \end{aligned}$$

Therefore, for a Boolean function f of $\mathbb{F}_{2^{2m}}$, being an element of Maiorana-McFarland class has exactly the same meaning as being affine in x, for all y. To sum up, $f \in \mathcal{M}$ if and only if

$$D_{(b,0)}D_{(c,0)}|_{x=0} f(x, y) = 0,\ \forall\, b,\ c \in \mathbb{F}_{2^m}. \tag{2.8}$$

2.4 Linear Translators

Take any $m \in \mathbb{Z}^+$ and a positive integer t dividing m. Let $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^t}$ be a map and $a \in \mathbb{F}_{2^t}$, then an element $\alpha \in \mathbb{F}_{2^m}$ is called an *a-linear translator of f* if it satisfies the equality

$$f(x + \alpha b) = f(x) + ab,$$

for all $(x,\ b) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^t}$.

Take $a_1, a_2 \in \mathbb{F}_{2^t}$ and $\alpha_1, \alpha_2 \in \mathbb{F}_{2^m}$. It is a well-konwn fact that, when α_i is an a_i-linear translator of $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^t}$ for each $i \in \{1,\ 2\}$, then $\alpha_1 + \alpha_2$ will be an (a_1+a_2)-linear translator of f and $a\alpha_1$ will be a (aa_1)-linear translator of f, $\forall a \in \mathbb{F}_{2^t}^*$.

Indeed, the functions with linear translators are not so desirable becuse of their weakness against several cryptographic attacks.

2.5 The Vandermonde Matrix

Let ω be a k^{th} root of unity of $\mathbb{F}_{q^n}$, and denote the Vandermonde matrix by $M_k(\omega)$:

$$M_k(\omega) = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{(k-1)} \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{2(k-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{(k-1)} & \omega^{2(k-1)} & \dots & \omega^{(k-1)(k-1)} \end{bmatrix}.$$

Consider the product $M_k(\omega)M_k(\omega^{-1})$. The $(i,j)^{th}$ entry of the resulting matrix will be equal to

$$\begin{bmatrix} 1 & \omega^{(i-1)} & \omega^{2(i-1)} & \dots & \omega^{(k-1)(i-1)} \end{bmatrix} \cdot \begin{bmatrix} 1 \\ \omega^{-(j-1)} \\ \omega^{-2(j-1)} \\ \vdots \\ \omega^{-(k-1)(i-1)} \end{bmatrix}$$
$$= \sum_{l=0}^{k-1} \omega^{l[(i-1)-(j-1)]} = \sum_{l=0}^{k-1} \omega^{l(i-j)}. \quad (2.9)$$

Since ω is a k^{th} root of unity of $\mathbb{F}_{q^n}$, (2.9) turns into

$$\sum_{l=0}^{k-1} \left(\omega^{(i-j)}\right)^l = \frac{\left(\omega^{(i-j)}\right)^k - 1}{\omega^{(i-j)} - 1} = \frac{\left(\omega^k\right)^{i-j} - 1}{\omega^{(i-j)} - 1} = 0,$$

whenever $i \neq j$, which proves the following identity.

Proposition 2.5.1.

$$M_k(\omega) M_k(\omega^{-1}) = kI,$$

where ω is a k^{th} root of unity of $\mathbb{F}_{q^n}$ and I is the identity matrix.

2.6 Normalized Polynomials

A permutation polynomial $f \in \mathbb{F}_q[x]$ having the following properties

i. the leading coefficient of f is 1,

ii. f fixes the zero element, and

iii. if the characteristic of $\mathbb{F}_q$ does not divide the degree d of f, then the coefficient of x^{d-1} is zero

is said to be in *normalized form*. For any given PP, it is possible to find a normalized equivalent of it with the help of Lemma 2.1.1, by choosing a, c, d suitably ([24]). While all normalized PPs of degree ≤ 5 were listed by Dickson in [11], there also exists a table suggested by Shallue and Wanless for the ones of degree 6 in [30], which is inserted on page 14 for further interest of this study.

2.7 Algebraic Curves

An *algebraic curve $\mathcal{C}$ over a given field $\mathbb{F}_q$* is the set

$$\mathcal{C} = \left\{(x, y) \in \overline{\mathbb{F}_q} \times \overline{\mathbb{F}_q} \mid f(x, y) = 0\right\},$$

where $f(x, y) \in \mathbb{F}_q[x, y]$. In this setting, f is called *the defining polynomial of $\mathcal{C}$*, and the *degree of $\mathcal{C}$* is the degree of the defining polynomial of the curve. Each element of

$\mathcal{C}$ is called a *point on* $\mathcal{C}$. An $\mathbb{F}_q$*-rational point* is a point (x, y) on the curve $\mathcal{C}$, where $x, y \in \mathbb{F}_q$.

Algebraic curves are useful, while deciding whether a given polynomial is a PP or not: $f(x) \in \mathbb{F}_q$ is a PP over $\mathbb{F}_q$ if and only if the curve

$$\mathcal{C}_f = \left\{ (x, y) \in \overline{\mathbb{F}_q} \times \overline{\mathbb{F}_q} \mid \frac{f(x) - f(x)}{x - y} = 0 \right\},$$

has no $\mathbb{F}_q$-rational point (a, b) satisfying $a \neq b$. (See [2].)

Let N_q denote the number of $\mathbb{F}_q$-rational points on $\mathcal{C}$. The number N_q can be estimated by the very well known Hasse-Weil Bound (see, Theorem 5.2.3 in [31]), which can also be stated in terms of algebraic curves as follows:

Theorem 2.7.1. *[14] If d is the degree of the curve $\mathcal{C}$, then*

$$\left| N_q - q \right| \leq (d-1)(d-2)\sqrt{q} + c(d),$$

where $c(d)$ is a constant depending on d.

With reference to [15], one can choose $c(d) = \dfrac{d(d-1)^2}{2} + 1$, and the following result comes immediately.

Corollary 2.7.2. *If $\mathcal{C}$ is an algebraic curve of degree 4, then*

$$\left| N_q - q \right| \leq 6\sqrt{q} + 19.$$

Table 2.1: All normalized permutation polynomials of degree 6 over $\mathbb{F}_q$. [30]

Cases	q	Normalized PP
1	11	$x^6 \pm 2x$
2	11	$x^6 \pm a^2x^3 + ax^2 \pm 5x$, where $a \in \mathbb{F}_q$ is a nonzero square.
3	11	$x^6 \pm 4a^2x^3 + ax^2 \pm 4x$, where $a \in \mathbb{F}_q$ is either 0 or a non-square.
4	9	$x^6 + a^2x^4 + a^7bx^3 + a^4x^2 + a(2b+1)x$, where $b \in \mathbb{F}_q$ is a root of $x^6 - x^4 + x^3 + x^2 + x$ and $a \in \mathbb{F}_q^*$.
5	9	$x^6 + ax^5 + 2abx^4 + (a^3 + ab^2 + 2b^3)x^3 + (2a^4 + ab^3)x^2 + (2a^5 + a^4b + 2ab^4)x$, where $b \in \mathbb{F}_q$ and $a \in \mathbb{F}_q^*$.
6	9	$x^6 + ax^5 + 2acx^4 + (ac^2 + 2c^3 + a^3e)x^3 + (ac^3 + 2a^4e)x^2 + (a^5e^2 + 2ac^4 + a^4ce)x$, where $a \in \mathbb{F}_q^*$, and $c,\ e \in \mathbb{F}_q\ :\ e$ is a root of $x^4 + 1$.
7	9	$x^6 + ax^5 + 2acx^4 + (2a^3 + ac^2 + 2c^3)x^3 + (a^4 + ac^3)x^2 + (2a^5 + a^5e + 2a^4c + 2ac^4)x$, where $a \in \mathbb{F}_q^*$, and $c,\ e \in \mathbb{F}_q\ :\ e$ is a root of $x^2 + 1$.
8	27	$x^6 + ax^5 + 2acx^4 + (ac^2 + 2c^3)x^3 + (2a^4 + ac^3)x^2 + (a^4c + 2ac^4)x$, where $a \in \mathbb{F}_q^*,\ c \in \mathbb{F}_q$.
9	2^m, where $m \geq 3$ and $m:$ odd	$x^6 + a^2x^4 + a^4x^2$, where $a \in \mathbb{F}_q$.
10	8	$x^6 + a^5c^2x^4 + a^4x^3 + (a^3 + a^3c + a^3c^4)x^2 + a^2c^2x$, where $a \in \mathbb{F}_q^*,\ c \in \mathbb{F}_q$.
11	8	$x^6 + ax^5 + a^2(c^2 + c)x^4 + a^3x^3 + a^4(c^2 + e)x^2 + a^5(c + e)x$, where $a \in \mathbb{F}_q^*,\ c,\ e \in \mathbb{F}_q\ :\ c$ is a root of $x^4 + x^2 + x$, and e is a root of $x^4 + x^3 + x^2 + 1$.
12	8	$x^6 + ax^5 + a^2(c^2 + c)x^4 + a^3ex^3 + a^4(c^4 + ce)x^2 + a^5(c^4 + c^2e)x$, where $a \in \mathbb{F}_q^*,\ c,\ e \in \mathbb{F}_q\ :$ e is a root of $x^3 + x + 1$.
13	8	$x^6 + ax^5 + a^2(c^2 + c + 1)x^4 + a^3x^3 + a^4(c^2 + 1)x^2 + a^5cx$, where $a \in \mathbb{F}_q^*,\ c \in \mathbb{F}_q$.
14	8	$x^6 + ax^5 + a^2(c^2 + c + 1)x^4 + a^3e^3x^3 + a^4(c^4 + ce^3 + e^4)x^2 + a^5(c^4 + c^2e^3 + e^3 + e^4)x$, where $a \in \mathbb{F}_q,\ c,\ e \in \mathbb{F}_q\ :\ e$ is a root of $x^4 + x^2 + x$.
15	16	$x^6 + ax^5 + a^2(c^6 + c^5 + e^4 + e^2 + e)x^4 + a^3x^3 + a^4(c^6 + c^5 + e^4 + e^2)x^2 + a^5(c + e)x$, where $a \in \mathbb{F}_q^*,\ c,\ e \in \mathbb{F}_q\ :\ c$ is a root of $x^7 + x^4 + x^3 + x^2 + x$, and e is a root of $x^8 + x^4 + x^2 + x + 1$.
16	32	$x^6 + ax^5 + a^2(c^2 + c)x^4 + a^4(c^4 + 1)x^2 + a^5c^4x$, where $a \in \mathbb{F}_q^*,\ c \in \mathbb{F}_q$.

CHAPTER 3

ON SEVERAL PERMUTATON POLYNOMIALS AND COMPLETE PERMUTATION POLYNOMIALS

This chapter mainly stands for the representation of the results obtained about PPs and CPPs during this Ph.D. study. After stating a publicly known result in Section 3.1 about monomials to be complete, the focus of the study becomes several classes of binomials and trinomials.

Section 3.2 starts with the work done on binomials of the form $f(x) = x^{\frac{q^n-1}{q-1}+1} + bx \in \mathbb{F}_{q^n}[x]$. The permutation property of these polynomials was already studied by other mathematicians for the cases $n \in \{2,\ 3,\ 4,\ 6\}$, and we give a complete list of all PPs for the case $n = 5$ in Theorem 3.2.1. In the meanwhile, we get a substantial intuition on CPPs of the same form is given. Additionally, we give a fairly well criterion on b rigid for all n making the binomial above a CPP or at least a PP in Theorem 3.2.2 and 3.2.3.

In Section 3.3, the permutation property of a particular class of trinomials $f(x) = x^5 h(x^{q-1}) \in \mathbb{F}_{q^2}[x]$ with $h(x) = x^5 + x + 1$ is studied with the help of algebraic curves over finite fields. The main result of the section is given in Theorem 3.3.1.

The results represented in this chapter have been published as our joint works [27, 28] by B. Gülmez Temür and P. Ongan; and [1] by Y. Akbal, B. Gülmez Temür, and P. Ongan.

Throughout this chapter, let $n \in \mathbb{Z}^+$.

3.1 Monomials

The most uncomplicated polynomials are monomials. Let f be a monomial of degree d with a leading coefficient $a \in \mathbb{F}_q^*$ over $\mathbb{F}_q$. The necessary and sufficient condition making f a PP is the following: $\gcd(d, q-1) = 1$. In addition to that, if $ax^d + x$ is also a PP, then it becomes a CPP.

3.2 Several Binomials

Let $f(x)$ be a cyclotomic polynomial of the form

$$f(x) = x^{s+1} + bx \in \mathbb{F}_{q^n}[x], \tag{3.1}$$

where $b \neq 0$ and $s = \frac{q^n-1}{t}$ with $t \in \mathbb{Z}^+$ satisfying $t \mid (q^n - 1)$.

For $t = q - 1$, PPs and CPPs of the form (3.1) had already been studied for several choices of n (see [5] for $n \in \{2,\ 3\}$, [4] and [35] for $n = 4$, and [3] for $n = 6$.) The gap for the case $n = 5$ can be filled as follows: Let $f(x)$ be a PP of the form (3.1). In the case $q > 114$, p should divide 3 and $Tr_1^5(b)$ should be zero, by Theorem 2.1.5. And, in the case $q \leq 114$, by setting $r = 1$ and $h(x) = x + b$ in Theorem 2.1.4, one gets that $f(x)$ becomes a PP of $\mathbb{F}_{q^5}$ if and only if $h_b(x)$ is a PP of $\mathbb{F}_q$, where

$$h_b(x) = x(x+b)(x+b^q)(x+b^{q^2})(x+b^{q^3})(x+b^{q^4}) \in \mathbb{F}_{q^5}[x]. \tag{3.2}$$

By letting λ_is be defined as follows:

$$\lambda_1 = \sum_{i \in S} b^{q^i},\ \lambda_2 = \sum_{\substack{i,\ j \in S \\ i \neq j}} b^{q^i+q^j},\ \lambda_3 = \sum_{\substack{i,\ j,\ k \in S \\ i,\ j,\ k\text{: all distinct}}} b^{q^i+q^j+q^k},$$

$$\lambda_4 = \sum_{\substack{i,\ j,\ k,\ l \in S \\ i,\ j,\ k,\ l\text{: all distinct}}} b^{q^i+q^j+q^k+q^l},\ \lambda_5 = b^{1+q+q^2+q^3+q^4}, \tag{3.3}$$

where $S = \{0, 1, 2, 3, 4\}$, equation (3.2) turns into

$$h_b(x) = x^6 + \lambda_1 x^5 + \lambda_2 x^4 + \lambda_3 x^3 + \lambda_4 x^2 + \lambda_5 x. \tag{3.4}$$

If p is a divisor of 6 -which is the degree of $h_b(x)$-, then $h_b(x)$ will be a normalized polynomial, and so become a PP only if it is in one of the cases numbered between

4-16 in Table 2.1. On the other hand, if $p \notin \{2,\ 3\}$, a normalized equivalent

$$ah_b(cx+d) \in \mathbb{F}_q[x],$$

of $h_b(x)$ can be found with the following restrictions coming from the definition of being normalized:

i. $a = c^6$.

ii. $d^6 + \lambda_1 d^5 + \lambda_2 d^4 + \lambda_3 d^3 + \lambda_4 d^2 + \lambda_5 d = 0$.

iii. $d = 9\lambda_1$.

So, by choosing $c = 1$, we obtain a normalized equivalent of $h_b(x)$ as follows:

$$x^6 + (6{\lambda_1}^2 + \lambda_2)x^4 + ({\lambda_1}^3 + 3\lambda_1\lambda_2 + \lambda_3)x^3 + (6{\lambda_1}^4 + 2{\lambda_1}^2\lambda_2 + 5\lambda_1\lambda_3 + \lambda_4)x^2 + (9{\lambda_1}^5 + {\lambda_1}^3\lambda_2 + {\lambda_1}^2\lambda_3 + 7\lambda_1\lambda_4 + \lambda_5)x.$$

By taking $h_b(x)$ as itself for the cases $p = \{2,\ 3\}$, and above normalized equivalent of $h_b(x)$ for the case $p = 11$, we obtain the following consequence with the help of Table 2.1.

Theorem 3.2.1. *[28]Let $q = p^m$. A binomial $f(x) = x^{\frac{q^5-1}{q-1}+1} + bx \in \mathbb{F}_{q^5}[x]$ is a PP if and only if the conditions in one of the following cases are satisfied:*

1) $q = 11$ *and*

i) $\lambda_2 = 5\lambda_1^2$, $\lambda_3 = 6{\lambda_1}^3$, $\lambda_4 = 9{\lambda_1}^4$, *and* $\lambda_5 = 5{\lambda_1}^5 \pm k$, *where* $k \in \{2,\ 4\}$,

ii) $\lambda_2 = 5{\lambda_1}^2$, $\lambda_3 = 6{\lambda_1}^3 \pm a^2$, $\lambda_4 = 9{\lambda_1}^4 + a$, *and* $\lambda_5 = 5{\lambda_1}^5 \pm 5$, *where* $a \in \mathbb{F}_{q^5}^*$ *is a square, or*

iii) $\lambda_2 = 5{\lambda_1}^2$, $\lambda_3 = 6{\lambda_1}^3 \pm 4a^2$, $\lambda_4 = 9{\lambda_1}^4 + a$, *and* $\lambda_5 = 5{\lambda_1}^5 \pm 4$, *where* $a \in \mathbb{F}_{q^5}$ *is not a square.*

2) $q = 3^m$ *and*

i) $m = 2$, $\lambda_1 = 0$, $\lambda_2 = a^2$, $\lambda_3 = a^7 c$, $\lambda_4 = a^4$, $\lambda_5 = a(2c+1)$, *where* $a \in \mathbb{F}_{q^5}^*$, *and* $c \in \mathbb{F}_{q^5}$ *is a root of* $x^6 - x^4 + x^3 + x^2 + x$,

ii) $m = 2$, $\lambda_1 = a$, $\lambda_2 = 2ac$, $\lambda_3 = a^3 + ac^2 + 2c^3$, $\lambda_4 = 2a^4 + ac^3$, *and* $\lambda_5 = 2a^5 + a^4c + 2ac^4$, *where* $a \in \mathbb{F}_{q^5}^*$ *and* $c \in \mathbb{F}_{q^5}$,

iii) $m = 2$, $\lambda_1 = a$, $\lambda_2 = 2ac$, $\lambda_3 = ac^2 + 2c^3 + a^3e$, $\lambda_4 = ac^3 + 2a^4e$, *and* $\lambda_5 = a^5e^2 + 2ac^4 + a^4ce$, *where* $a \in \mathbb{F}_{q^5}^*$, $c \in \mathbb{F}_{q^5}$, *and* $e \in \mathbb{F}_{q^5}$ *is a root of* $x^4 + 1$,

iv) $m = 2$, $\lambda_1 = a$, $\lambda_2 = 2ac$, $\lambda_3 = 2a^3 + ac^2 + 2c^3$, $\lambda_4 = a^4 + ac^3$, *and* $\lambda_5 = 2a^5 + a^5e + 2a^4c + 2ac^4$, *where* $a \in \mathbb{F}_{q^5}^*$, $c \in \mathbb{F}_{q^5}$, *and* $e \in \mathbb{F}_{q^5}$ *is a root of* $x^2 + 1$, *or*

v) $m = 3$, $\lambda_1 = a$, $\lambda_2 = 2ac$, $\lambda_3 = ac^2 + 2c^3$, $\lambda_4 = 2a^4 + ac^3$, *and* $\lambda_5 = a^4c + 2ac^4$, *where* $a \in \mathbb{F}_{q^5}^*$ *and* $c \in \mathbb{F}_{q^5}$.

3) $q = 2^m$ *and*

i) $m \geq 3$ *is odd*, $\lambda_1 = \lambda_3 = 0$, $\lambda_2 = a^2$, $\lambda_4 = a^4$, *and* $\lambda_5 = 1$, *where* $a \in \mathbb{F}_{q^5}$,

ii) $m = 3$, $\lambda_1 = 0$, $\lambda_2 = a^5c^2$, $\lambda_3 = a^4$, $\lambda_4 = a^3 + a^3c + a^3c^4$, *and* $\lambda_5 = a^2c^2$, *where* $a \in \mathbb{F}_{q^5}^*$ *and* $c \in \mathbb{F}_{q^5}$,

iii) $m = 3$, $\lambda_1 = a$, $\lambda_2 = a^2(c^2 + c)$, $\lambda_3 = a^3$, $\lambda_4 = a^4(c^2 + e)$, *and* $\lambda_5 = a^5(c + e)$, *where* $a \in \mathbb{F}_{q^5}^*$, $c \in \mathbb{F}_{q^5}$ *is a root of* $x^4 + x^2 + x$, *and* $e \in \mathbb{F}_{q^5}$ *is a root of* $x^4 + x^3 + x^2 + 1$,

iv) $m = 3$, $\lambda_1 = 5$, $\lambda_2 = a^2(c^2 + c)$, $\lambda_3 = a^3e$, $\lambda_4 = a^4(c^4 + ce)$, *and* $\lambda_5 = a^5(c^4 + c^2e)$, *where* $a \in \mathbb{F}_{q^5}^*$, $c \in \mathbb{F}_{q^5}$ *is arbitrary, and* $e \in \mathbb{F}_{q^5}$ *is a root of* $x^3 + x + 1$,

v) $m = 3$, $\lambda_1 = a$, $\lambda_2 = a^2(c^2 + c + 1)$, $\lambda_3 = a^3$, $\lambda_4 = a^4(c^2 + 1)$, *and* $\lambda_5 = a^5c$, *where* $a \in \mathbb{F}_{q^5}^*$, *and* $c \in \mathbb{F}_{q^5}$ *is arbitrary,*

vi) $m = 3$, $\lambda_1 = a$, $\lambda_2 = a^2(c^2 + c + 1)$, $\lambda_3 = a^3e^3$, $\lambda_4 = a^4(c^4 + ce^3 + e^4)$, *and* $\lambda_5 = a^5(c^4 + c^2e^3 + e^3 + e^4)$, *where* $a \in \mathbb{F}_{q^5}^*$, $c \in \mathbb{F}_{q^5}$ *is arbitrary, and* $e \in \mathbb{F}_{q^5}$ *is a root of* $x^4 + x^2 + x$,

vii) $m = 4$, $\lambda_1 = a$, $\lambda_2 = a^2(c^6 + c^5 + e^4 + e^2 + e)$, $\lambda_3 = a^3$, $\lambda_4 = a^4(c^6 + c^5 + e^4 + e^2)$, *and* $\lambda_5 = a^5(c + e)$, *where* $a \in \mathbb{F}_{q^5}^*$, $c \in \mathbb{F}_{q^5}$ *is a root of* $x^7 + x^4 + x^3 + x^2 + x$, *and* $e \in \mathbb{F}_{q^5}$ *is a root of* $x^8 + x^4 + x^2 + x + 1$, *or*

viii) $m = 5$, $\lambda_1 = a$, $\lambda_2 = a^2(c^2 + c)$, $\lambda_3 = 0$, $\lambda_4 = a^4(c^4 + 1)$, *and* $\lambda_5 = a^5c^4$, *where* $a \in \mathbb{F}_{q^5}^*$, *and* $c \in \mathbb{F}_{q^5}$.

While Theorem 3.2.1 completes the case $n = 5$ for PPs, a few steps further should have been taken for CPPs. Since

$$f(x) + x = x^{\frac{q^5-1}{q-1}+1} + (b+1)x \in \mathbb{F}_{q^5}[x],$$

$f(x)$ will be a CPP over $\mathbb{F}_{q^5}$ if and only if both $h_b(x)$ and $h_{b+1}(x)$ are PPs over $\mathbb{F}_q$ at the same time. Therefore, forming a complete list of all conditions necessary and sufficient to make $f(x)$ a CPP over $\mathbb{F}_{q^5}$ is doable with the help of Table 2.1 and Theorem 3.2.1 by analyzing each q-case separately.

Additionally, with a different point of view, if it is also possible to define a criterion on b rigid for each n making the polynomial $f(x)$ as in (3.1) a CPP or at least a PP as follows:

By setting $r_i = 1$ in (2.1) for each $i \in \mathbb{Z}$ satisfying $0 \leq i \leq q-2$,

$$f(x) = \sum_{i=0}^{q-2} \frac{a_i}{q-1}\, x + \sum_{i=0}^{q-2} \frac{a_i \zeta^{-i}}{q-1}\, x^{s+1} + \sum_{i=0}^{q-2} \frac{a_i \zeta^{-2i}}{q-1}\, x^{2s+1} + \ldots + \sum_{i=0}^{q-2} \frac{a_i \zeta^{-(q-2)i}}{q-1}\, x^{(q-2)s+1}, \quad (3.5)$$

and equating the polynomials (3.5) and (3.1) to each other, one gets the identities:

$$\frac{1}{q-1} \sum_{i=0}^{q-2} a_i \zeta^{-ki} = \begin{cases} b, & \text{if } k = 0, \\ 1, & \text{if } k = 1, \\ 0, & \text{otherwise.} \end{cases}$$

which can also be represented as the following matrix multiplication:

$$\begin{bmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & \zeta^{-1} & \zeta^{-2} & \ldots & \zeta^{-(q-2)} \\ 1 & \zeta^{-2} & \zeta^{-4} & \ldots & \zeta^{-2(q-2)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta^{-(q-2)} & \zeta^{-2(q-2)} & \ldots & \zeta^{-(q-2)(q-2)} \end{bmatrix} \begin{bmatrix} a_0/(q-1) \\ a_1/(q-1) \\ a_2/(q-1) \\ \vdots \\ a_{q-2}/(q-1) \end{bmatrix} = \begin{bmatrix} b \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}. \quad (3.6)$$

Since ζ is already a primitive $(q-1)^{st}$ root of unity, it is possible to denote the

$(q-1)\times(q-1)$-matrix of (3.6) by $M_{q-1}\left(\zeta^{-1}\right)$, which implies

$$\begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{q-2} \end{bmatrix} = (q-1)\left(M_{q-1}\left(\zeta^{-1}\right)\right)^{-1} \begin{bmatrix} b \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}. \tag{3.7}$$

In other respects, the identity

$$M_{q-1}(\zeta)\, M_{q-1}\left(\zeta^{-1}\right) = (q-1)I$$

of Proposition 2.5.1 implies the equality

$$\left(M_{q-1}\left(\zeta^{-1}\right)\right)^{-1} = \frac{1}{q-1} M_{q-1}(\zeta),$$

which reduces (3.7) in the following way:

$$\begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{q-2} \end{bmatrix} = M_{q-1}(\zeta) \begin{bmatrix} b \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} b+1 \\ b+\zeta \\ b+\zeta^2 \\ \vdots \\ b+\zeta^{(q-2)} \end{bmatrix}.$$

Thus and so, by letting $a_i := b+\zeta^i$, for all $0 \le i \le q-2$, it is possible to write (3.1) in the form

$$f(x) = \frac{1}{q-1} \sum_{i=0}^{q-2} \sum_{j=0}^{q-2} \left(b+\zeta^i\right) \zeta^{-ji} x^{js+1} \in \mathbb{F}_{q^n}[x]. \tag{3.8}$$

As a consequence of Lemma 2.1.2, the conditions making the set

$$\left\{ ind_\gamma(b+\zeta^i) + i \mid i = 0, 1, ..., q-2 \right\}$$

a complete set of residues modulo $q-1$ are necessary and sufficient in order to have a PP of the form (3.8) over $\mathbb{F}_{q^n}$.

Now, let $l \in \mathbb{Z}^+$ be satisfying the following equality:

$$l = ind_\gamma(b+\zeta^i) + i = ind_\gamma(b+\zeta^j) + j + r(q-1), \tag{3.9}$$

for some $0 \leq r \leq s-1$ and $0 \leq i < j \leq q-2$. Thuswise, by definition, l becomes the minimum element of $\mathbb{Z}^+$ greater than j holding the equations

$$\gamma^{l-i} = b + \zeta^i \text{ and } \gamma^{l-j} = \gamma^{r(q-1)} \left(b + \zeta^j\right)$$

which can also be stated as

$$b + \zeta^i = \gamma^{j-i+r(q-1)} \left(b + \zeta^j\right)$$

since $\gamma^{l-i} = \gamma^{j-i}\gamma^{l-j}$. So an l satisfying (3.9) would immediately bring

$$b = -\gamma^{sj} + \frac{\gamma^{si} - \gamma^{sj}}{\gamma^{j-i+r(q-1)} - 1},$$

proving the following result.

Theorem 3.2.2. *[27]$f(x) = x^{s+1} + bx \in \mathbb{F}_{q^n}[x]$ is a PP of $\mathbb{F}_{q^n}$ if and only if $b \in \mathbb{F}_{q^n}^*$ satisfies the identity*

$$b \neq -\gamma^{sj} + \frac{\gamma^{si} - \gamma^{sj}}{\gamma^{j-i+r(q-1)} - 1},$$

for every distinct elements i and j of the set $\{0, 1, ..., q-2\}$ and $0 \leq r \leq s-1$.

In order to broaden the area of interest to CPPs, one also needs to study on the polynomials

$$f(x) + x = x^{s+1} + x(b+1)$$

which can be written in the form (2.1) in an analogical manner to the previous one by setting

$$a_i := b + 1 + \zeta^i, \text{ for all } 0 \leq i \leq q-2.$$

Since the question when $f(x) + x$ becomes a PP over $\mathbb{F}_{q^n}$ is converted into what the conditions on b making the set

$$\left\{ind_\gamma(b + 1 + \zeta^i) + i \mid i = 0, 1, ..., q-2\right\}$$

a complete set of residues modulo $q-1$ are, by Lemma 2.1.2, the result below comes directly following similar steps to the proof of Theorem 3.2.2.

Corollary 3.2.3. *[27]$f(x) = x^{s+1} + bx \in \mathbb{F}_{q^n}[x]$ is a CPP of $\mathbb{F}_{q^n}$ if and only if both $b \in \mathbb{F}_{q^n}^*$ and $b + 1 \in \mathbb{F}_{q^n}^*$ are not equal to*

$$-\gamma^{sj} + \frac{\gamma^{si} - \gamma^{sj}}{\gamma^{j-i+r(q-1)} - 1},$$

for any $0 \leq i < j \leq q-2$ and $0 \leq r \leq s-1$.

3.3 Trinomials

Permutation trinomials have been on the agenda of researchers, recently. In this section, a special kind of trinomials over $\mathbb{F}_{p^m}$ -where p is an odd prime- are studied with the help of algebraic curves. Let

$$f(x) = x^5((x^{q-1})^5 + (x^{q-1}) + 1) \tag{3.10}$$

be a polynomial over $\mathbb{F}_{q^2}$, and set

$$P(x) = x^5 \left(x^5 + x + 1\right)^{q-1} \in \mathbb{F}_{q^2}[x]. \tag{3.11}$$

Then, with an appropriate choice of n and r, Lemma 2.1.3 implies that in the case $\gcd(q-1, 5) = 1$,$f(x)$ is a PP over $\mathbb{F}_{q^2}$ if and only if $P(x) = x^5(x^5 + x + 1)^{q-1}$ permutes μ_{q+1}.

When $3 \mid q$, $f(x)$ would not be a PP over $\mathbb{F}_{q^2}$ since $P(1) = 0 \notin \mu_{q+1}$. On the other hand, in the case $q+1$ is divisible by 3, there will exist $x \in \mu_{q+1} \setminus \{1\}$ satisfying $x^3 - 1 = 0$, which is implying $x^2 + x + 1 = 0$. Since $x^5 + x + 1 = (x^2 + x + 1)(x^3 - x^2 + 1)$, $P(x) = 0 \notin \mu_{q+1}$ implying that $P(x)$ would not be a PP over $\mathbb{F}_{q^2}$ in this case, too. The only remaining case to check is the one for $q \equiv 1 \pmod 3$.

For $x \in \mu_{q+1}$, consider the image of the rational function associated with $P(x)$:

$$\frac{x^5 h(x)^q}{h(x)} = \frac{(x^2 + x + 1)(x^3 - x + 1)}{(x^2 + x + 1)(x^3 - x^2 + 1)} = \frac{x^3 - x + 1}{x^3 - x^2 + 1}. \tag{3.12}$$

If one needs to have $P(x) \in \mu_{q+1}$, for all $x \in \mu_{q+1}$, the denominator of the simplified version of the rational functiton in (3.12) should be nonzero for each choice of $x \in \mu_{q+1}$. So, assume the converse:

$$\exists x \in \mu_{q+1} \ : \ x^3 - x^2 + 1 = 0. \tag{3.13}$$

Each element $x \in \mu_{q+1}$ satisfies the identity $x^q = \dfrac{1}{x}$, so the following equality is immediate.

$$0 = \left(x^3 - x^2 + 1\right)^q = x^{3q} - x^{2q} + 1 = \frac{1}{x^3} - \frac{1}{x^2} + 1 = \frac{x^3 - x + 1}{x^3},$$

implying that

$$0 = x^3 - x + 1. \tag{3.14}$$

Using the equations (3.13) and (3.14), one can easily deduce $x^2 - x = 0$, implying that $x = 0$ or $x = 1$. However, neither of these choices will satisfy the equality $x^3 - x^2 + 1 = 0$, which contradicts to the assumption (3.13). Thus, $x^3 - x^2 + 1 \neq 0$.

Choose an element z from the set $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ arbitrarily, and set the function $\phi : \mathbb{F}_q \cup \{\infty\} \mapsto \mu_{q+1}$ -which is bijective by construction- as follows:

$$\phi(x) = \begin{cases} \dfrac{x+z}{x+z^q}, & \text{if } x \in \mathbb{F}_q \\ 1, & \text{if } x = \infty \end{cases}$$

Then, the inverse of this function will be

$$\phi^{-1}(x) = \begin{cases} \dfrac{z^q x - z}{1-x}, & \text{if } x \in \mu_{q+1} \setminus \{1\} \\ \infty, & \text{if } x = 1 \end{cases}$$

According to this setup, the necessary and sufficient conditions making P an injective function on the set μ_{q+1} are exactly the ones making the composition mapping $(\phi^{-1} \circ P \circ \phi)$ an injection on $\mathbb{F}_q$. By simple calculation,

$$\begin{aligned} &\left(\phi^{-1} \circ P \circ \phi\right)(x) = \\ &\frac{x^3 + (z^q + z)\, x^2 + (2z^{2q} - 3z^{q+1} + 2z^2)\, x + (z^{3q} - z^{2q+1} - z^{q+2} + z^3)}{(x^2 + (z^q + z)\, x + z^{q+1})}. \end{aligned} \tag{3.15}$$

Here, since $-z, -z^q \notin \mathbb{F}_q$, the denominator of (3.15) -which can be factorized as $(x+z)(x+z^q)$- would not be equal to 0, for any choice of $x \in \mathbb{F}_q$.

The algebraic curve defined by the equation

$$\frac{\phi^{-1}(P(\phi(X))) - \phi^{-1}(P(\phi(Y)))}{X - Y} = 0$$

is reducible to

$$\begin{aligned} \mathcal{L}(X,Y) = &\left(Y^2 + (z^q + z)\, Y + z^{q+1}\right) X^2 \\ &+ \left((z^q + z)\, Y^2 + \left(-z^{2q} + 6z^{q+1} - z^2\right) Y + \left(-z^{3q} + 2z^{2q+1} + 2z^{q+2} - z^3\right)\right) X \\ &+ z^{q+1} Y^2 + \left(-z^{3q} + 2z^{2q+1} + 2z^{q+2} - z^3\right) Y \\ &- z^{4q} + 2z^{3q+1} - z^{2q+2} + 2z^{q+3} - z^4 = 0. \end{aligned} \tag{3.16}$$

Since the automorphism $\psi : x \to x^q$ fixes the coefficients of it, $\mathcal{L}(X,Y) \in \mathbb{F}_q[X,Y]$. Next, try to write $\mathcal{L}(X,Y)$ as a product of absolutely irreducible components. Since the degree of the curve w.r.t. X is 2, there exist only three possibilities for $\mathcal{L}(X,Y)$:

I. $\mathcal{L}(X,Y) = A(Y)\,\mathcal{L}_1(X,Y)$, where $\mathcal{L}_1(X,Y)$ is a bivariate polynomial of degree 2 with respect to X.

II. $\mathcal{L}(X,Y) = \mathcal{L}_1(X,Y)\,\mathcal{L}_2(X,Y)$, where each $\mathcal{L}_i(X,Y)$ is a bivariate polynomial of degree 1 with respect to X.

III. $\mathcal{L}(X,Y)$ is absolutely irreducible.

In Case I, $\mathcal{L}_1(X,Y) = B_1(Y)X^2 + B_2(Y)X + B_3(Y)$, for some $B_i(Y)$. If $\deg(A) = 2$, then B_1 would be constant. So, considering the coefficient of X^2 in (3.16), without loss of generality, set $A(Y) = Y^2 + (z^q + z)\,Y + z^{q+1}$. Then $A(-z) = 0$. On the other hand, considering the coefficient of X in (3.16),

$$A(Y)B_2(Y) = (z^q + z)\,Y^2 + \left(-z^{2q} + 6z^{q+1} - z^2\right)Y + \left(-z^{3q} + 2z^{2q+1} + 2z^{q+2} - z^3\right)$$

implying that

$$0 = A(-z)B_2(-z) = z^3\left(-z^{3q-3} + 3z^{2q-2} - 3z^{q-1} + 1\right) = z^3\left(-z^{q-1} + 1\right)^3.$$

However, $z \notin \mathbb{F}_q$ will contracit $z^{q-1} = 1$. If $\deg(A) = 1$, by proceeding with a similar approach to the previous one, either $A(-z^q)$ or $A(-z)$ will be equal to 0, and in both cases $z^{q-1} = 1$ will contradicts to the fact $z \notin \mathbb{F}_q$. Hence, Case I is removed from among the options.

In Case II, $\mathcal{L}_1(X,Y) = A_1(Y)X + A_2(Y)$ and $\mathcal{L}_2(X,Y) = B_1(Y)X + B_2(Y)$, for some $A_i, B_i \in \overline{\mathbb{F}}_q[Y]$, then

$$\mathcal{L}_1(X,Y)\mathcal{L}_2(X,Y) = \left(A_1(Y)B_1(Y)\right)X^2 + \left(A_1(Y)B_2(Y) + A_2(Y)B_1(Y)\right)X + A_2(Y)B_2(Y).$$

If $\deg(A_1) = 2$, without lost of generality, $A_1(Y) = Y^2 + (z^q + z)\,Y + z^{q+1}$ and $B_1(Y) = 1$

Since $\mathcal{L}(X,Y) = \mathcal{L}(Y,X)$, $\mathcal{L}_1$ should either be fixed or be mapped to $\mathcal{L}_2$ under the morphism $\psi : (X,Y) \to (Y,X)$. However, none of these cases will come with the

term Y^2X, so we conclude that $\deg(A_1) \neq 2$. If $\deg(A_1) = 1$, then $\deg(B_1) = \deg(A_2) = \deg(B_2) = 1$ implying that

$$\mathcal{L}_1(X,Y)\,\mathcal{L}_2(X,Y) = (XY + a_iX + a_2Y + a_3)(XY + b_1X + b_2Y + b_3), \tag{3.17}$$

for some a_i and b_i. Without loss of generality, one can set $a_1 = z$ and $b_1 = z^q$, by a comparison on the coefficients of X^2 in (3.17) and (3.16).

Again, by a similar approach to the provious one, since $\mathcal{L}(X,Y) = \mathcal{L}(Y,X)$; $\mathcal{L}_1$ should either be fixed or be mapped to $\mathcal{L}_2$ under the morphism $\psi : (X,Y) \to (Y,X)$. If $\psi(\mathcal{L}_1) = \mathcal{L}_1$, then $\psi(\mathcal{L}_2) = \mathcal{L}_2$, and so $(\, a_1,\, a_2,\, b_1,\, b_2\,) = (\, z,\, z,\, z^q,\, z^q\,)$. After that, applying automorphism $\psi : x \to x^q$ to the coefficients of (3.17) will interchange $\mathcal{L}_1$ and $\mathcal{L}_2$, implying that $b_3 = (a_3)^q$. A comparision of the coefficients of (3.17) to (3.16) would yield the equalities

i) $za_3^q + z^q a_3 = -z^3 + 2z^{q+2} + 2z^{2q+1} - z^{3q}$,

ii) $a_3^q + a_3 = -z^2 + 4z^{q+1} - z^{2q}$,

iii) $a_3^{q+1} = -z^4 + 2z^{q+3} - z^{2q+2} + 2z^{3q+1} - z^{4q}$.

However, writing a_3 in terms of z by using the first two equations, and then plugging a_3 in terms of z into the last equation will bring the equality $z^4\left(z^{q-1} - 1\right)^4 = 0$ which is a contradiction since z is not in $\mathbb{F}_q$. Therefore, $\psi(\mathcal{L}_1) \neq \mathcal{L}_1$.

If $\psi(\mathcal{L}_1) = \mathcal{L}_2$, then $(\, a_1,\, a_2,\, b_1,\, b_2\,) = (\, z,\, z^q,\, z^q,\, z\,)$ and $a_3 = b_3$. A similar comparision on coefficients as above would bring the equalities

i) $2a_3 + z^2 + z^{2q} = -z^2 + 6z^{q+1} - z^{2q}$,

ii) $a_3 z + a_3 z^q = -z^3 + 2z^{q+2} + 2z^{2q+1} - z^{3q}$,

iii) $a_3^2 = -z^4 + 2z^{q+3} - z^{2q+2} + 2z^{3q+1} - z^{4q}$.

However, writing a_3 in terms of z from the first equation, and then plugging a_3 in terms of z into the last equation will bring the equality $z^4\left(z^{q-1} - 1\right)^4 = 0$ which is a contradiction since z is not in $\mathbb{F}_q$. Therefore, $\psi(\mathcal{L}_1) \neq \mathcal{L}_2$, too. Hence Case II is also impossible.

Table 3.1: The minimum value of N_q in each q-case, where $q < 77$.

q	7	13	25	31	37	43	61	67	73
Min(N_q)	4	18	32	34	36	36	54	72	70

All in all, $\mathcal{L}(X, Y)$ should be absolutely irreducible. It is possible to homogenize $\mathcal{L}(X, Y)$ via the change $X \mapsto X/Z$ and $Y \mapsto Y/Z$. Thus the degree of the curve would be 4 implying that it should have at most 4 solutions. So, if $N_q \geq 5$, one of the solutions should be off the line $X = Y$, and by Theorem 2.7.1, this happens only if $q - 6\sqrt{q} - 19 \geq 5$ which is possible only if $q \geq 77$. For the case q is less than 77, N_q will depend on the choice of z.

In each q-case (where q is less than 77), it is possible to calculate N_q for each choice of $z \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ with the help of MAGMA [6]. See Table 3.1 for the minimum values of N_qs in each q-case.

According to the results obtained from MAGMA and placed in 3.1, each minimum value of $min(N_q) \geq 5$, for each q except 7. And, for the case $q = 7$, a solution off the line $X = Y$ will always exist, which can be checked again by MAGMA. To sum up, the following result is obtained as a main result of this section.

Theorem 3.3.1. *[1] A trinomial of the form $f(x) = x^5((x^{q-1})^5 + (x^{q-1}) + 1)$ is not a PP over $\mathbb{F}_{q^2}$ if $\mathbb{F}_q$ is not of even characteristic.*

CHAPTER 4

A METHOD TO CONSTRUCT NEW CLASSES OF BENT FUNCTIONS

This chapter stands for the representation of a method of construction of bent functions in the light of Mesnager's earlier studies.

In Section 4.1, Lemma 4.1.1, which is an earlier work of Mesnager, is introduced as a foundation of the constructions presented here.

In Section 4.2, first, a method of carrying a permutation over a smaller field to a permutation over a larger field is described in Proposition 4.2.1. After that, this method combined with Section 4.1 is used to obtain 3-tuples of particular permutations, which lead to new classes of bent functions: Theorem 4.2.2, 4.2.3, and 4.2.4. Also, in Theorem 4.2.5, a new infinite family of permutations -whose elements can also be used to obtain new bent functions in the same manner- constructed from permutations in a higher dimension is presented.

Lastly, in Section 4.3, it is shown that the bent functions constructed in Section 4.2 are not members of Maiorana-McFarland Class.

The results represented in this chapter have been published as a joint work of S. Mesnager, F. Özbudak, and P. Ongan. (See [22].)

Throughout this chapter, let $m, t \in \mathbb{Z}^+$ be such that $t < m$ and $t|m$.

4.1 $(\mathcal{A}_m)$-condition

A secondary construction, presented earlier by Carlet in [8], has recently been modified by Mesnager. And, this modification has made many fresh paths helpful to generate new primary bent functions in bivariate representation ([17, 18, 19, 20]).

For $m \in \mathbb{Z}^+$, three pairwise distinct PPs over $\mathbb{F}_{2^m}$ are said to *satisfy* $(\mathcal{A}_m)$*-condition* if both their summation also becomes a PP over $\mathbb{F}_{2^m}$, and the inverse of their summation is equal to the summation of their inverses. Besides explicit families of PPs satisfying $(\mathcal{A}_m)$-condition are represented, in [17, 19], it is shown that these kinds of triples can be used in the construction of new bent functions, and the dual of each bent function constructed via this way can also be computed explicitly.

Lemma 4.1.1 ([17, 19])**.** *If ϕ_1, ϕ_2 and ϕ_3 are 3 pairwise-distinct PPs satisfying $(\mathcal{A}_m)$-condition, then the Boolean function $H : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ defined by*

$$H(x,y) = Tr_1^m\big(x\phi_1(y)\big)Tr_1^m\big(x\phi_2(y)\big) + Tr_1^m\big(x\phi_1(y)\big)Tr_1^m\big(x\phi_3(y)\big) + Tr_1^m\big(x\phi_2(y)\big)Tr_1^m\big(x\phi_3(y)\big), \quad (4.1)$$

will become a bent function, and its dual $\tilde{H}$ will be given as follows

$$\tilde{H}(x,y) = Tr_1^m\big(\phi_1^{-1}(x)y\big)Tr_1^m\big(\phi_2^{-1}(x)y\big) + Tr_1^m\big(\phi_1^{-1}(x)y\big)Tr_1^m\big(\phi_3^{-1}(x)y\big) + Tr_1^m\big(\phi_2^{-1}(x)y\big)Tr_1^m\big(\phi_3^{-1}(x)y\big). \quad (4.2)$$

4.2 Several Constructions Using PPs Satisfying $(\mathcal{A}_m)$-condition

Let f be a mapping such that $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^t}$, $L : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ be an $\mathbb{F}_{2^t}$-linear permutation, $g(x)$ be a PP in $\mathbb{F}_{2^t}[x]$, $\alpha \in \mathbb{F}_{2^m}^*$, $a \in \mathbb{F}_{2^t}^*$, and α be an a-linear translator of f with respect to $\mathbb{F}_{2^t}$.

Set $h : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ as follows:

$$h(x) = x + \alpha\left(g(f(x)) + \frac{f(x)}{a}\right).$$

Then, by definition of α, $f(h(x)) = ag(f(x))$ since the characteristic of the field is

even, implying that $f(x) = g^{-1}\left((f(h(x)))/a\right)$. Therefore

$$x = h(x) + \alpha\left(g(f(x)) + \frac{f(x)}{a}\right) = y + \frac{\alpha}{a}\left(f(h(x)) + g^{-1}\left(\frac{f(h(x))}{a}\right)\right),$$

and so, h is a bijection with

$$h^{-1}(x) = x + \frac{\alpha}{a}\left(f(x) + g^{-1}\left(\frac{f(x)}{a}\right)\right).$$

If $x \in \mathbb{F}_{2^m}$ is given, then

$$(L \circ h)(x) = L(x) + L(\alpha)\left(g(f(x)) + \frac{f(x)}{a}\right).$$

Now, set $\phi := L \circ h$, then it will definitely be a PP over $\mathbb{F}_{2^m}$ since it is the composition of two bijections, and ϕ^{-1} will easily be calculated via composition $h^{-1} \circ L^{-1}$ proving the following proposition.

Proposition 4.2.1. *[22] Let $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^t}$ be any mapping, g be a PP over $\mathbb{F}_{2^t}$, and L be an $\mathbb{F}_{2^t}$-linear PP over $\mathbb{F}_{2^m}$. Suppose that α is an a-linear translator of f with respect to $\mathbb{F}_{2^t}$, where $(\alpha, a) \in \mathbb{F}_{2^m}^* \times \mathbb{F}_{2^t}^*$. Set $\phi : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ as follows*

$$\phi(x) := L(x) + L(\alpha)\left[g(f(x)) + \frac{f(x)}{a}\right], \tag{4.3}$$

then ϕ becomes a PP over $\mathbb{F}_{2^m}$ and

$$\phi^{-1}(x) = L^{-1}(x) + \frac{\alpha}{a}\left[f(L^{-1}(x)) + g^{-1}\left(\frac{f(L^{-1}(x))}{a}\right)\right]. \tag{4.4}$$

Having L, f and g satisfying the properties given in the premise of Proposition 4.2.1, we take three pairwise a-linear translators α_1, α_2 and α_3 of f, and let $\psi := \phi_1 + \phi_2 + \phi_3$. Then, since $\alpha_1 + \alpha_2 + \alpha_3$ will also be an a-linear translator of f,

$$\psi(x) = L(x) + [L(\alpha_1) + L(\alpha_2) + L(\alpha_3)]\left[g(f(x)) + \frac{f(x)}{a}\right]$$

will be a PP, by Proposition 4.2.1. After that, we take any element $x \in \mathbb{F}_{2^m}$, then

$$\begin{aligned}\left({\phi_1}^{-1} + {\phi_2}^{-1} + {\phi_3}^{-1}\right)(x) \\ &= L^{-1}(x) + \left(\frac{\alpha_1}{a} + \frac{\alpha_2}{a} + \frac{\alpha_3}{a}\right)\left[f(L^{-1}(x)) + g^{-1}\left(\frac{f(L^{-1}(x))}{a}\right)\right] \\ &= \psi^{-1}(x),\end{aligned}$$

meaning that ϕ_1, ϕ_2, ϕ_3 satisfy $(\mathcal{A}_m)$-condition, and by applying Lemma 4.1.1, the following theorem is obtained.

Theorem 4.2.2. *[22] Let $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^t}$ be any mapping, g be a PP over $\mathbb{F}_{2^t}$, L be an $\mathbb{F}_{2^t}$-linear permutation of $\mathbb{F}_{2^m}$. Assume $\alpha_1,\ \alpha_2,\ \alpha_3$ be 3 pairwise-distinct a-linear translators of f with respect to $\mathbb{F}_{2^t}$, where $\alpha_1,\ \alpha_2,\ \alpha_3 \in \mathbb{F}_{2^m}^*$ and $a \in \mathbb{F}_{2^t}^*$. Suppose $\alpha_1 + \alpha_2 + \alpha_3 \neq 0$. Set $\rho : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ as $\rho(x) := g(f(x)) + \frac{f(x)}{a}$ and $\tilde{\rho} : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ as $\tilde{\rho}(x) := \frac{1}{a}\left(g^{-1}\left(\frac{f(x)}{a}\right) + f(x)\right)$. Then,*

$$\begin{aligned} H(x,y) = Tr_1^m\big(xL(y)\big) + Tr_1^m\big(L(\alpha_1)x\rho(y)\big)Tr_1^m\big(L(\alpha_2)x\rho(y)\big) + \\ Tr_1^m\big(L(\alpha_1)x\rho(y)\big)Tr_1^m\big(L(\alpha_3)x\rho(y)\big) + \\ Tr_1^m\big(L(\alpha_2)x\rho(y)\big)Tr_1^m\big(L(\alpha_3)x\rho(y)\big) \end{aligned} \tag{4.5}$$

becomes bent, and $\tilde{H}$ is given by

$$\begin{aligned} \tilde{H}(x,y) = Tr_1^m\big(yL^{-1}(x)\big) + Tr_1^m\big(\alpha_1 y\tilde{\rho}(L^{-1}(x))\big)Tr_1^m\big(\alpha_2 y\tilde{\rho}(L^{-1}(x))\big) + \\ Tr_1^m\big(\alpha_1 y\tilde{\rho}(L^{-1}(x))\big)Tr_1^m\big(\alpha_3 y\tilde{\rho}(L^{-1}(x))\big) + \\ Tr_1^m\big(\alpha_2 y\tilde{\rho}(L^{-1}(x))\big)Tr_1^m\big(\alpha_3 y\tilde{\rho}(L^{-1}(x))\big). \end{aligned} \tag{4.6}$$

An example of the application of Theorem 4.2.2: Fix $m = 6$ and $t = 3$, consider $\mathbb{F}_8 = \mathbb{F}_2(\omega)$ with $\omega^3 + \omega + 1 = 0$, and $\mathbb{F}_{64} = \mathbb{F}_2(\xi)$ with $\xi^6 + \xi^4 + \xi^3 + \xi + 1 = 0$. Define $f : \mathbb{F}_{64} \to \mathbb{F}_8$ by $f(x) = x + x^8$, $L : \mathbb{F}_{64} \to \mathbb{F}_{64}$ by $L(x) = x$, $g : \mathbb{F}_8 \to \mathbb{F}_8$ by $g(x) = x$, and take $a := \omega$, $\alpha_1 := \xi$, $\alpha_2 := \xi^8$ and $\alpha_3 := \xi^{56}$. Then, α_is are a-linear translators of f with respect to $\mathbb{F}_8$ with the property $\alpha_1 + \alpha_2 + \alpha_3 = \xi^7 \neq 0$. In this special case, ϕ_is in (4.3) will be $\phi_i : \mathbb{F}_{64} \to \mathbb{F}_{64}$ defined as

$$\phi_i(x) = x + \omega^2\alpha_i f(x), \ \text{ where } i \in \{1,\ 2,\ 3\}\,. \tag{4.7}$$

So, by Proposition 4.2.1, ϕ_is of (4.7) are PPs of $\mathbb{F}_{64}$ satisfying $(\mathcal{A}_4)$-condition, and they will define a bent function $H : \mathbb{F}_{64} \times \mathbb{F}_{64} \to \mathbb{F}_2$ by Theorem 4.2.2. $\square$

Now, let $f,\ L,\ a$ and α be chosen as earlier, but this time, take three permutations g_1, g_2 and g_3 of $\mathbb{F}_{2^t}$ satisfying $(\mathcal{A}_t)$-condition. For $i \in \{1, 2, 3\}$, set $\phi_i : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ as

$$\phi_i(x) := L(x) + L(\alpha)\left[g_i(f(x)) + \frac{f(x)}{a}\right], \tag{4.8}$$

and let $\psi : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ as $\psi := \phi_1 + \phi_2 + \phi_3$. Then

$$\psi(x) = L(x) + L(\alpha)\left[\big(g_1 + g_2 + g_3\big)(f(x)) + \frac{f(x)}{a}\right].$$

will be a permutation, and

$$\psi^{-1}(x) = L^{-1}(x) + \frac{\alpha}{a}\left[f(L^{-1}(x)) + \big(g_1 + g_2 + g_3\big)^{-1}\left(\frac{f(L^{-1}(x))}{a}\right)\right],$$

by Proposition 4.2.1. On the other hand,

$$\big(\phi_1^{-1} + \phi_2^{-1} + \phi_3^{-1}\big)(x) = \\ L^{-1}(x) + \frac{\alpha}{a}\left[f(L^{-1}(x)) + \big(g_1^{-1} + g_2^{-1} + g_3^{-1}\big)\left(\frac{f(L^{-1}(x))}{a}\right)\right].$$

implying $\psi^{-1} = \phi_1^{-1} + \phi_2^{-1} + \phi_3^{-1}$. Therefore, ϕ_1, ϕ_2 and ϕ_3 will satisfy $(\mathcal{A}_m)$-condition, and the following construction is achievable with the help of Proposition 4.1.1.

Theorem 4.2.3. *[22] Let f be a mapping from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^t}$, L be an $\mathbb{F}_{2^t}$-linear permutation of $\mathbb{F}_{2^m}$, and g_1, g_2 and g_3 be PPs over $\mathbb{F}_{2^t}$ satisfying $(\mathcal{A}_t)$-condition. Let $a \in \mathbb{F}_{2^t}^*$, and $\alpha \in \mathbb{F}_{2^m}^*$ be an a-linear translator of f with respect to $\mathbb{F}_{2^t}$. For $i \in \{1,2,3\}$, set $\rho_i : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ as $\rho_i(x) := g_i(f(x)) + \frac{f(x)}{a}$ and $\tilde{\rho}_i : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ as $\tilde{\rho}_i(x) := \frac{1}{a}\left(g_i^{-1}\left(\frac{f(x)}{a}\right) + f(x)\right)$. Then,*

$$H(x,y) = Tr_1^m\big(xL(y)\big) + Tr_1^m\big(L(\alpha)x\rho_1(y)\big)Tr_1^m\big(L(\alpha)x\rho_2(y)\big) + \\ Tr_1^m\big(L(\alpha)x\rho_1(y)\big)Tr_1^m\big(L(\alpha)x\rho_3(y)\big) + Tr_1^m\big(L(\alpha)x\rho_2(y)\big)Tr_1^m\big(L(\alpha)x\rho_3(y)\big) \tag{4.9}$$

becomes bent, and $\tilde{H}$ is given by

$$\tilde{H}(x,y) = Tr_1^m\big(yL^{-1}(x)\big) + Tr_1^m\big(\alpha y\tilde{\rho}_1(L^{-1}(x))\big)Tr_1^m\big(\alpha y\tilde{\rho}_2(L^{-1}(x))\big) + \\ Tr_1^m\big(\alpha y\tilde{\rho}_1(L^{-1}(x))\big)Tr_1^m\big(\alpha y\tilde{\rho}_3(L^{-1}(x))\big) + \\ Tr_1^m\big(\alpha y\tilde{\rho}_2(L^{-1}(x))\big)Tr_1^m\big(\alpha y\tilde{\rho}_3(L^{-1}(x))\big). \tag{4.10}$$

An example of the application of Theorem 4.2.3: Fix $m = 4$ and $t = 2$, consider $\mathbb{F}_4 = \mathbb{F}_2(\omega)$ with $\omega^2 + \omega + 1 = 0$, and $\mathbb{F}_{16} = \mathbb{F}_2(\xi)$ with $\xi^4 + \xi + 1 = 0$. Define $L : \mathbb{F}_{16} \to \mathbb{F}_{16}$ by $L(x) = x$, $f : \mathbb{F}_{16} \to \mathbb{F}_4$ by $f(x) = x + x^4$, and take $a := \omega$ and $\alpha := \xi^6$, so α will be an a-linear translator of f with respect to $\mathbb{F}_4$. Additionally, set three permutations $g_1,\ g_2,\ g_3$ of $\mathbb{F}_4$, as $g_1(x) = x$, $g_2(x) = x^2$ and $g_3(x) = x^2 + 1$, so that they will satisfy $(\mathcal{A}_2)$-condition. In this special case, $\phi_1,\ \phi_2$ and ϕ_3 become

permutations of $\mathbb{F}_{16}$ defined by

$$\phi_i(x) = \begin{cases} (1+\omega\xi^6)x + \omega\xi^6 x^4, & \text{for } i=1 \\ (1+\omega^2\xi^6)x + \xi^6 x^2 + \omega^2\xi^6 x^4 + \xi^6 x^8, & \text{for } i=2 \\ \xi^6 + (1+\omega^2\xi^6)x + \xi^6 x^2 + \omega^2\xi^6 x^4 + \xi^6 x^8, & \text{for } i=3 \end{cases} \tag{4.11}$$

And since they are satisfying $(\mathcal{A}_4)$-condition, they can be used in the construction defined in Theorem 4.2.3. $\square$

Similarly, let f and a and α be chosen as earlier, $g : \mathbb{F}_{2^t} \to \mathbb{F}_{2^t}$ be an automorphism on $\mathbb{F}_{2^t}$ and L_i be three $\mathbb{F}_{2^t}$-linear permutations of $\mathbb{F}_{2^m}$ satisfying $(\mathcal{A}_m)$-condition. We set $\phi_i : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ as

$$\phi_i(x) := L_i(x) + L_i(\alpha)\left[g(f(x)) + \frac{f(x)}{a}\right], \tag{4.12}$$

for $i \in \{1,2,3\}$, and let $\psi : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ as $\psi := \phi_1 + \phi_2 + \phi_3$. Then

$$\psi(x) = \big(L_1 + L_2 + L_3\big)(x) + \big[\big(L_1 + L_2 + L_3\big)(\alpha)\big]\left[g(f(x)) + \frac{f(x)}{a}\right].$$

By construction, $L_1 + L_2 + L_3$ will definitely be an $\mathbb{F}_{2^t}$-linear permutation, and since g is an automorphism between finite fields, it will be a PP. So, since L_is are satisfying $(\mathcal{A}_m)$-condition, by Proposition 4.2.1, ψ will be a PP whose inverse is easily calculated as follows:

$$\psi^{-1}(x) = \left(L_1^{-1} + L_2^{-1} + L_3^{-1}\right)(x) + \\ \frac{\alpha}{a}\left[f\left(\left(L_1^{-1} + L_2^{-1} + L_3^{-1}\right)(x)\right) + g^{-1}\left(\frac{f\left(\left(L_1^{-1} + L_2^{-1} + L_3^{-1}\right)(x)\right)}{a}\right)\right].$$

In addition to that,

$$\left(\phi_1^{-1} + \phi_2^{-1} + \phi_3^{-1}\right)(x) = \left(L_1^{-1} + L_2^{-1} + L_3^{-1}\right)(x) + \\ \frac{\alpha}{a}\left[\sum_{i\in\{1,2,3\}} (f \circ L_i^{-1})(x) + \sum_{i\in\{1,2,3\}} g^{-1}\left(\frac{f(L_i^{-1}(x))}{a}\right)\right],$$

and the linearity of f and bijectivity of g implies that $\psi^{-1} = \phi_1^{-1} + \phi_2^{-1} + \phi_3^{-1}$, i.e. ϕ_is defined as in (4.12) will also satisfy $(\mathcal{A}_m)$-condition. Therefore the following construction is immediate by Proposition 4.1.1.

Theorem 4.2.4. *[22] Let $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^t}$ be a linear mapping, $g : \mathbb{F}_{2^t} \to \mathbb{F}_{2^t}$ be an automorphism of $\mathbb{F}_{2^t}$, α be an a-linear translator of f with respect to $\mathbb{F}_{2^t}$, where $\alpha \in \mathbb{F}_{2^m}^*$ and $a \in \mathbb{F}_{2^t}^*$. Let $L_i : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ be an $\mathbb{F}_{2^t}$-linear PP over $\mathbb{F}_{2^m}$, for $i \in \{1, 2, 3\}$. Suppose that L_1, L_2 and L_3 satisfies $(\mathcal{A}_m)$-condition. Set $\rho : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ as $\rho(x) := g(f(x)) + \frac{f(x)}{a}$ and $\tilde{\rho} : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ as $\tilde{\rho}(x) := \frac{1}{a}\left(g^{-1}\left(\frac{f(x)}{a}\right) + f(x)\right)$. Then,*

$$\begin{aligned} H(x,y) = {} & Tr_1^m\big(xL_1(y)\big)Tr_1^m\big(xL_2(y)\big) + Tr_1^m\big(xL_1(y)\big)Tr_1^m\big(xL_3(y)\big) + \\ & Tr_1^m\big(xL_2(y)\big)Tr_1^m\big(xL_3(y)\big) + Tr_1^m\big(xL_1(y)\big)Tr_1^m\big((L_2(\alpha) + L_3(\alpha))x\rho(y)\big) + \\ & Tr_1^m\big(xL_2(y)\big)Tr_1^m\big((L_1(\alpha) + L_3(\alpha))x\rho(y)\big) + \\ & Tr_1^m\big(xL_3(y)\big)Tr_1^m\big((L_1(\alpha) + L_2(\alpha))x\rho(y)\big) + \\ & Tr_1^m(L_1(\alpha)x\rho(y))Tr_1^m(L_2(\alpha)x\rho(y)) + \\ & Tr_1^m(L_1(\alpha)x\rho(y))Tr_1^m(L_3(\alpha)x\rho(y)) + \\ & Tr_1^m(L_2(\alpha)x\rho(y))Tr_1^m(L_3(\alpha)x\rho(y)) \end{aligned} \quad (4.13)$$

becomes a bent function. Furthermore,

$$\begin{aligned} \tilde{H}(x,y) = {} & Tr_1^m\big(yL_1^{-1}(x)\big)Tr_1^m\big(yL_2^{-1}(x)\big) + Tr_1^m\big(yL_1^{-1}(x)\big)Tr_1^m\big(yL_3^{-1}(x)\big) + \\ & Tr_1^m\big(yL_2^{-1}(x)\big)Tr_1^m\big(yL_3^{-1}(x)\big) + \\ & Tr_1^m\big(yL_1^{-1}(x)\big)Tr_1^m\big(\alpha y(\tilde{\rho}(L_2^{-1}(x)) + L_3^{-1}(x))\big) + \\ & Tr_1^m\big(yL_2^{-1}(x)\big)Tr_1^m\big(\alpha y(\tilde{\rho}(L_1^{-1}(x)) + L_3^{-1}(x))\big) + \\ & Tr_1^m\big(yL_3^{-1}(x)\big)Tr_1^m\big(\alpha y(\tilde{\rho}(L_1^{-1}(x)) + L_2^{-1}(x))\big) + \\ & Tr_1^m\big(\alpha y\tilde{\rho}(L_1^{-1}(x))\big)Tr_2^m\big(\alpha y\tilde{\rho}(L_2^{-1}(x))\big) + \\ & Tr_1^m\big(\alpha y\tilde{\rho}(L_1^{-1}(x))\big)Tr_3^m\big(\alpha y\tilde{\rho}(L_3^{-1}(x))\big) + \\ & Tr_2^m\big(\alpha y\tilde{\rho}(L_2^{-1}(x))\big)Tr_3^m\big(\alpha y\tilde{\rho}(L_3^{-1}(x))\big). \end{aligned} \quad (4.14)$$

An example of application of Theorem 4.2.4: Fix $m = 4$ and $t = 2$, consider $\mathbb{F}_{16} = \mathbb{F}_2(\rho)$ with $\rho^4 + \rho + 1 = 0$ and $\mathbb{F}_4 = \mathbb{F}_2(\omega)$ with $\omega^2 + \omega + 1 = 0$. Define $f : \mathbb{F}_{16} \to \mathbb{F}_4$ by $f(x) = x + x^4$, $g : \mathbb{F}_4 \to \mathbb{F}_4$ by $g(x) = x$, and take $a := \omega$, and $\alpha := \rho$, so α will

be an a-linear translator of f with respect to $\mathbb{F}_4$. Furthermore, set $L_i : \mathbb{F}_{16} \to \mathbb{F}_{16}$ as

$$L_i(x) = \begin{cases} \rho^{14}x^8 + \rho^{13}x^4 + \rho^5x^2 + \rho^{13}x, & \text{for } i = 1 \\ \rho^{13}x^8 + \rho^4x^4 + \rho^7x^2 + \rho^{10}x, & \text{for } i = 2 \\ \rho^5x^8 + \rho^2x^4 + \rho^3x^2 + \rho^8x, & \text{for } i = 3 \end{cases} \tag{4.15}$$

so that they will satisfy $(\mathcal{A})_4$-condition. With this setup, $\phi_i : \mathbb{F}_{16} \to \mathbb{F}_{16}$ defined as

$$\phi_i(x) = \begin{cases} \rho^{14}x^8 + \rho^8x^4 + \rho^5x^2 + \rho^8x, & \text{for } i = 1 \\ \rho^{13}x^8 + \rho^7x^4 + \rho^7x^2 + \rho^{12}x, & \text{for } i = 2 \\ \phi_3(x) = \rho^5x^8 + \rho^6x^4 + \rho^3x^2 + \rho^{13}x, & \text{for } i = 3 \end{cases} \tag{4.16}$$

will satisfy $(\mathcal{A}_4)$-condition, and so they can be used to define a bent function $H : \mathbb{F}_{16} \times \mathbb{F}_{16} \to \mathbb{F}_2$ with the help of Theorem 4.2.4. $\square$

Now, let f be a defined as earlier, h be defined in a similar manner to f, and $g_1, g_2 \in \mathbb{F}_{2^t}[x]$. Also let $\alpha_1, \alpha_2 \in \mathbb{F}_{2^m}^*$ be such that α_i is an a_i-linear translator of f and b_i-linear translator of h with respect to $\mathbb{F}_{2^t}$, for some $a_i,\ b_i \in \mathbb{F}_{2^t}^*$, where $i \in \{1,\ 2\}$. Set $\phi : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ as

$$\phi(x) := x + \alpha_1 g_1(f(x)) + \alpha_2 g_2(h(x)). \tag{4.17}$$

For a fixed $x \in \mathbb{F}_{2^m}$, say $y \in \mathbb{F}_{2^m}$ is the image of x on ϕ, then

$$f(x) + a_1 g_1(f(x)) + a_2 g_2(h(x)) = f(y) \text{ and } h(x) + b_1 g_1(f(x)) + b_2 g_2(h(x)) = h(y) \tag{4.18}$$

because of the choice of α_is. Now, let $\psi : \mathbb{F}_{2^t} \times \mathbb{F}_{2^t} \to \mathbb{F}_{2^t} \times \mathbb{F}_{2^t}$ be a permutation defined as follows

$$\psi(x, y) := \big(x + a_1 g_1(x) + a_2 g_2(y),\ y + b_1 g_1(x) + b_2 g_2(y)\big).$$

Then $\psi\big(f(x), h(x)\big) = \big(f(y), h(y)\big)$ implying that $\big(f(x), h(x)\big) = \psi^{-1}\big(f(y), h(y)\big)$. For $\pi_1 : \mathbb{F}_{2^t} \times \mathbb{F}_{2^t} \to \mathbb{F}_{2^t}$ and $\pi_2 : \mathbb{F}_{2^t} \times \mathbb{F}_{2^t} \to \mathbb{F}_{2^t}$ are projections defined as

$$\pi_1((x, y)) := x \text{ and } \pi_2((x, y)) := y,$$

from $y = \phi(x)$, one gets

$$x = y + \alpha_1 g_1(\pi_1 \circ \psi^{-1}((f(y), h(y)))) + \alpha_2 g_2(\pi_2 \circ \psi^{-1}((f(y), h(y)))),$$

showing that ϕ is a PP and

$$\phi^{-1}(x) = x + \sum_{i \in \{1,2\}} \alpha_i (g_i \circ \pi_i \circ \psi^{-1})(f(x), h(x)). \tag{4.19}$$

If one takes three permutations $\phi_i : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ with $i \in \{1,\ 2,\ 3\}$ of the form (4.17) as follows

$$\phi_i(y) = y + \alpha_{1i} g_1(f(y)) + \alpha_{2i} g_2(h(y)),$$

and $\phi := \phi_1 + \phi_2 + \phi_3$, then ϕs will satisfy (A_m)-condition by construction, and thanks to Proposition 4.1.1,

$$H(x,y) = Tr_1^m(x\phi_1(y))Tr_1^m(x\phi_2(y)) + Tr_1^m(x\phi_1(y))Tr_1^m(x\phi_3(y)) + Tr_1^m(x\phi_2(y))Tr_1^m(x\phi_3(y))$$

will be bent, implying the following theorem.

Theorem 4.2.5. *Let f and h be functions from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^t}$. For $i \in \{1,\ 2,\ 3\}$ and $k \in \{1,\ 2\}$, let g_k be polynomials over $\mathbb{F}_{2^t}$, and α_{ki} be both an a_k-linear translator of f and b_k-linear translator of h with respect to $\mathbb{F}_{2^t}$, where $\alpha_{ki} \in \mathbb{F}_{2^m}^*$, and $a_k,\ b_k \in \mathbb{F}_{2^t}^*$. Assume $\psi : \mathbb{F}_{2^t} \times \mathbb{F}_{2^t} \to \mathbb{F}_{2^t} \times \mathbb{F}_{2^t}$ defined as*

$$\psi(x,y) := (x + a_1 g_1(x) + a_2 g_2(y), y + b_1 g_1(x) + b_2 g_2(y))$$

is a PP. Then

$$\begin{aligned}
H(x,y) &= Tr_1^m(xy) + Tr_1^m(x\alpha_{11}g_1(f(y)))Tr_1^m(x\alpha_{12}g_1(f(y))) \\
&+ Tr_1^m(x\alpha_{11}g_1(f(y)))Tr_1^m(x\alpha_{13}g_1(f(y))) + Tr_1^m(x\alpha_{11}g_1(f(y)))Tr_1^m(x\alpha_{22}g_2(h(y))) \\
&+ Tr_1^m(x\alpha_{11}g_1(f(y)))Tr_1^m(x\alpha_{23}g_2(h(y))) + Tr_1^m(x\alpha_{12}g_1(f(y)))Tr_1^m(x\alpha_{13}g_1(f(y))) \\
&+ Tr_1^m(x\alpha_{12}g_1(f(y)))Tr_1^m(x\alpha_{21}g_2(h(y))) + Tr_1^m(x\alpha_{12}g_1(f(y)))Tr_1^m(x\alpha_{23}g_2(h(y))) \\
&+ Tr_1^m(x\alpha_{13}g_1(f(y)))Tr_1^m(x\alpha_{21}g_2(h(y))) + Tr_1^m(x\alpha_{13}g_1(f(y)))Tr_1^m(x\alpha_{22}g_2(h(y))) \\
&+ Tr_1^m(x\alpha_{21}g_2(h(y)))Tr_1^m(x\alpha_{22}g_2(h(y))) + Tr_1^m(x\alpha_{21}g_2(h(y)))Tr_1^m(x\alpha_{23}g_2(h(y))) \\
&+ Tr_1^m(x\alpha_{22}g_2(h(y)))Tr_1^m(x\alpha_{23}g_2(h(y)))
\end{aligned} \tag{4.20}$$

becomes a bent function.

An example of the application of Theorem 4.2.5: Fix $m = 4$ and $t = 2$, consider $\mathbb{F}_{16} = \mathbb{F}_2(\rho)$ with $\rho^4 + \rho + 1 = 0$ and $\mathbb{F}_4 = \mathbb{F}_2(\omega)$ satisfying the equation $\omega^2 + \omega + 1 =$

0. Define $f,\ h : \mathbb{F}_{16} \to \mathbb{F}_4$ as $f(x) = h(x) = x + x^4$, and $g_1,\ g_2 : \mathbb{F}_4 \to \mathbb{F}_4$ as $g_1(x) = x^2 + \omega x$ and $g_2(x) = x^2 + x$. Take $a_1 = a_2 = b_1 = b_2 = 1$, $\alpha_{11} = \rho$, $\alpha_{12} = \alpha_{31} = \rho^2$, $\alpha_{21} = \alpha_{32} = \rho^4$, and $\alpha_{22} = \rho^8$, so each α_{ik} will be a 1-linear translator of f (and also h) with respect to $\mathbb{F}_4$. Furthermore, set $\phi_i : \mathbb{F}_{16} \to \mathbb{F}_{16}$ as

$$\phi_i = \begin{cases} x + \alpha_{11}g_1(x + x^4) + \alpha_{12}g_2(x + x^4), & \text{for } i = 1 \\ x + \alpha_{21}g_1(x + x^4) + \alpha_{22}g_2(x + x^4, & \text{for } i = 2 \\ x + \alpha_{31}g_1(x + x^4) + \alpha_{32}g_2(x + x^4), & \text{for } i = 3 \end{cases} \tag{4.21}$$

so that they will satisfy $(\mathcal{A})_4$-condition, and so they can be used to define a bent function $H : \mathbb{F}_{16} \times \mathbb{F}_{16} \to \mathbb{F}_2$ with the help of Theorem 4.2.5. $\square$

4.3 Bent Functions Constructed in the Previous Section are out of the Maiorana-McFarland Class $\mathcal{M}$

This section aims to prove that none of the bent functions constructed in Section 4.2 is in $\mathcal{M}$ which is notably significant since the widest class of primarily constructed bent functions is given by $\mathcal{M}$.

Take one of the bent functions $H : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_2$ constructed in Section 4.2. Since each one of them is of the form (4.1), taking first the first, then the second derivative of H, and then evaluating this second derivative at $x = 0$ will result in

$$\begin{aligned} D_{(b,0)}D_{(c,0)}H(x,y) = {} & Tr_1^m\big(b\phi_1(y)\big)Tr_1^m\big(c\phi_2(y)\big) + Tr_1^m\big(c\phi_1(y)\big)Tr_1^m\big(b\phi_2(y)\big) \\ & + Tr_1^m\big(b\phi_1(y)\big)Tr_1^m\big(c\phi_3(y)\big) + Tr_1^m\big(c\phi_1(y)\big)Tr_1^m\big(b\phi_3(y)\big) \\ & + Tr_1^m\big(b\phi_2(y)\big)Tr_1^m\big(c\phi_3(y)\big) + Tr_1^m\big(c\phi_2(y)\big)Tr_1^m\big(b\phi_3(y)\big). \end{aligned} \tag{4.22}$$

Therefore, with reference to 2.8, finding two elements $b,\ c \in \mathbb{F}_{2^m}^*$ having the property

$$D_{(b,0)}D_{(c,0)}H(x,y) \neq 0 \tag{4.23}$$

will definitely show that $H \notin \mathcal{M}$.

Consider the examples presented just after each theorem in Section 4.2. Via a brief search on MAGMA [6], we showed that (4.23) is satisfied for numerous choices of $(b,\ c)$-pairs in each case. For instance, take $(b,c) = (\xi^4, \xi^2)$, $(b,c) = (\xi, \xi^3)$, $y = \rho^3$

with $(b,\ c) = (\rho^7,\ \rho^5)$ and $(b, c) = (\rho, \rho^3)$ in the examples right after Theorems 4.2.2, 4.2.3, 4.2.4, and 4.2.5, respectively. Hence, none of the bent functions constructed in Section 4.2 is in $\mathcal{M}$.

CHAPTER 5

CONCLUSION

In this thesis, several types of permutation and/or complete permutation polynomials are studied, and also a construction of several new classes of bent functions is given. A general background, a motivation, and an outline are given in Chapter 1. Chapter 2 includes preliminary definitions and basic facts about the notions used in this study. Chapter 3 constitutes the first part of the main work of this thesis, and the focus of this chapter is several classes of binomials and trinomials. It starts with studying the binomials of the form

$$f(x) = x^{\frac{q^n-1}{q-1}+1} + bx \in \mathbb{F}_{q^n}[x]. \tag{5.1}$$

The permutation property of these kinds of binomials was studied earlier by other mathematicians for the cases $n \in \{2,\ 3,\ 4,\ 6\}$, so the gap in the study for the case $n = 5$ is filled by giving a complete list of all PPs in Theorem 3.2.1 and an intuition on CPPs of the same form is also given to enrich the study. After that, common criteria on b valid for any n making the binomial of the form (5.1) a CPP or at least a PP are defined in Theorem 3.2.2 and Corollary 3.2.3. Then, the trinomials of the form

$$f\left(x\right) = x^5 h\left(x^{q-1}\right),\ \text{where } h\left(x\right) = x^5 + x + 1 \tag{5.2}$$

are taken into consideration, the permutation property of them is studied with the help of algebraic curves, and the result is given in Theorem 3.3.1.

Chapter 4 forms the second main part of this thesis. Obtaining new constructions of bent functions with the help of linear translators and permutation polynomials is the main goal of that part. To start with, a method of upgrading a permutation of $\mathbb{F}_{2^t}$ to a permutation of $\mathbb{F}_{2^m}$ is described, where $t|m$. Then, this method is used to obtain

3-tuples of special permutations which lead to new classes of bent functions:

- 3-tuples of special a-linear translator α_is of $\mathbb{F}_{2^m}$, or
- 3-tuples of special permutation g_is of $\mathbb{F}_{2^t}$, or
- 3-tuples of special $\mathbb{F}_{2^t}$-linear permutation L_is of $\mathbb{F}_{2^m}$

will all bring new 3-tuples of permutations of $\mathbb{F}_{2^m}$ having the desired property, and so generates a bent function. (See Theorem 4.2.2, 4.2.3 and 4.2.4.) Furthermore, a new infinite family of permutations -whose elements can be used to construct bent functions in the same manner- is constructed using 6-tuples of linear translators with several properties. (See Theorem 4.2.5.) In addition to that, it is proven that none of the bent functions obtained here will become in $\mathcal{M}$, which is the widest known class of bent functions.

All in all, although bent functions, permutations, and complete permutation polynomials have been studied for decades, neither the classification nor the construction of them has been complete yet. Since they are interesting combinatorial objects, and also becuse of their applications in cryptography, design theory, coding theory and other domains; the notions studied here will have seem to attract mathematicians for a long time.

REFERENCES

[1] Y. Akbal, B. G. Temür, and P. Ongan, A short note on permutation trinomials of prescribed type, Communications in Algebra, 48(4), pp. 1608–1612, 2020.

[2] D. Bartoli and M. Giulietti, Permutation polynomials, fractional polynomials, and algebraic curves, Finite Fields and their Applications, 51, 08 2017.

[3] D. Bartoli, M. Giulietti, and G. Zini, On monomial complete permutation polynomials, Finite Fields and Their Applications, 41, pp. 132 – 158, 2016, ISSN 1071-5797.

[4] L. Bassalygo and V. Zinoviev, One class of permutation polynomials over finite fields of even characteristic, Moscow Mathematical Journal, 15, pp. 703–713, 10 2015.

[5] L. Bassalygo and V. Zinoviev, Permutation and complete permutation polynomials, Finite Fields and Their Applications, 33, pp. 198 – 211, 2015, ISSN 1071-5797.

[6] W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system. I. The user language. computational algebra and number theory (london, 1993), J. Symbolic Comput., 24(3-4), pp. 235–265, 1997, ISSN 0747-7171.

[7] C. Carlet, On the confusion and diffusion properties of maiorana–mcfarland's and extended maiorana–mcfarland's functions, J. Complexity, 20, pp. 182–204, 04 2004.

[8] C. Carlet, On bent and highly nonlinear balanced/resilient functions and their algebraic immunities, pp. 1–28, 02 2006, ISBN 978-3-540-31423-3.

[9] C. Carlet, Boolean functions for cryptography and error correcting codes, 11 2007.

[10] C. Carlet and S. Mesnager, Four decades of research on bent functions, Designs, Codes and Cryptography, 78, 01 2016.

[11] L. E. Dickson, The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group., Annals of Mathematics, 11(1/6), pp. 65–120, 1896, ISSN 0003486X.

[12] J. Dillon, Elementary hadamard difference sets, University of Maryland College Park, Ann Arbor, USA, 1974.

[13] X. dong Hou, Permutation polynomials over finite fields — a survey of recent advances. special issue : Second decade of ffa, Finite Fields and Their Applications, 32, pp. 82 – 119, 2015, ISSN 1071-5797.

[14] X. dong Hou, Applications of the hasse–weil bound to permutation polynomials, Finite Fields and Their Applications, 54, pp. 113 – 132, 2018, ISSN 1071-5797.

[15] X. dong Hou, Lectures on finite fields, 2018.

[16] Y. Laigle-Chapuy, Permutation polynomials and applications to coding theory, Finite Fields and Their Applications, 13(1), pp. 58 – 70, 2007, ISSN 1071-5797.

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

[18] S. Mesnager, A note on constructions of bent functions from involutions, Cryptology ePrint Archive, Report 2015/982, 2015, `https://eprint.iacr.org/2015/982`.

[19] S. Mesnager, Further constructions of infinite families of bent functions from new permutations and their duals, Cryptography and Communications, 8(2), pp. 229–246, Apr 2016, ISSN 1936-2455.

[20] S. Mesnager, On constructions of bent functions from involutions, in *2016 IEEE International Symposium on Information Theory (ISIT)*, pp. 110–114, 2016.

[21] S. Mesnager, *Bent Functions: Fundamentals and Results*, Springer, 2018.

[22] S. Mesnager, P. Ongan, and F. Özbudak, New bent functions from permutations and linear translators, Codes, Cryptology and Information Security Lecture Notes in Computer Science, p. 282–297, 2017.

[23] G. Mullen and D. Panario, *Handbook of Finite Fields*, 06 2013, ISBN 9780429105197.

[24] G. Mullen and Q. Wang, Permutation polynomials of one variable, Handbook of Finite Fields, pp. 215–229, 01 2013.

[25] G. L. Mullen and H. Niederreiter, Dickson polynomials over finite fields and complete mappings, Canadian Mathematical Bulletin, 30(1), p. 19–27, 1987.

[26] H. Niederreiter and K. H. Robinson, Complete mappings of finite fields, Journal of the Australian Mathematical Society. Series A. Pure Mathematics and Statistics, 33(2), p. 197–212, 1982.

[27] P. Ongan and B. G. Temür, Some permutations and complete permutation polynomials over finite fields, Turkish Journal of Mathematics, 2019.

[28] P. Ongan and B. G. Temür, A specific type of permutation and complete permutation polynomials over finite fields, Journal of Algebra and Its Applications, 19(04), p. 2050067, 2020.

[29] O. Rothaus, On "bent" functions, Journal of Combinatorial Theory, Series A, 20(3), pp. 300 – 305, 1976, ISSN 0097-3165.

[30] C. Shallue and I. Wanless, Permutation polynomials and orthomorphism polynomials of degree six, Finite Fields and Their Applications, 20, p. 84–92, 03 2013.

[31] H. Stichtenoth, *Algebraic function fields and codes*, Universitext, Springer, 1993, ISBN 978-3-540-56489-8.

[32] D. Wan, On a problem of niederreiter and robinson about finite fields, Journal of the Australian Mathematical Society, 41, pp. 336 – 338, 12 1986.

[33] Q. Wang, Cyclotomic mapping permutation polynomials over finite fields, pp. 119–128, 01 2007, ISBN 978-3-540-77403-7.

[34] Q. Wang, A note on inverses of cyclotomic mapping permutation polynomials over finite fields, Finite Fields and Their Applications, 45, pp. 422–427, 05 2017.

[35] G. Wu, N. Li, T. Helleseth, and Y. Zhang, Some classes of complete permutation polynomials over $\mathbb{F}_q$, Science China Mathematics, 58, 01 2015.

[36] M. Zieve, Permutation polynomials induced from permutations of subfields, and some complete sets of mutually orthogonal latin squares, 12 2013.

[37] M. E. Zieve, On some permutation polynomials over $\mathfrak{O}_q$ of the form $x^r h(x^{(q-1)/d})$, Proceedings of the American Mathematical Society, 137(7), pp. 2209–2216, 2009, ISSN 00029939, 10886826.

CURRICULUM VITAE

PERSONAL INFORMATION

Surname, Name: Ongan, Pınar
Nationality: Turkish (TC)
Date and Place of Birth: 17.02.1986, Denizli
Marital Status: Single
Phone: 0 533 1200414

EDUCATION

Degree	Institution	Year of Graduation
M.S.	Sabancı University	2011
B.S.	Boğaziçi University	2009
High School	Denizli Anatolian High School	2004

PROFESSIONAL EXPERIENCE

Year	Place	Enrollment
Sept. 2020 - ...	Uğur Kurs, Denizli	Math Teacher
July 2019 - Aug. 2020	PEK Akademi High Sch., Denizli	Math Teacher
Jan. 2019 - June 2019	Prestij Dershanesi, Denizli	Math Teacher
Sept. 2018 - Dec. 2018	canlidershane.net, Denizli	Geometry Teacher
Feb. 2015 - June 2018	Atılım University, Ankara	Instructor (part-time)
Sept. 2009 - Aug. 2011	Sabancı University, Ankara	Teaching Assistant

PUBLICATIONS

International Conference Publications

Sihem Mesnager, Pınar Ongan, and Ferruh Özbudak. New Bent Functions from Permutations and Linear Translators. March 2017. Lecture Notes in Computer Science.

International Journal Publications

Yıldırım Akbal, Burcu Gülmez Temür, and Pınar Ongan. A short note on permutation trinomials of prescribed type. November 2019. Communications in Algebra.

Pınar Ongan, and Burcu Gülmez Temür. A specific type of permutation and complete permutation polynomials over finite fields. April 2019. Journal of Algebra and Its Applications.

Pınar Ongan, Burcu Gülmez Temür. Some permutations and complete permutation polynomials over finite fields. 2019. Turkish Journal of Mathematics.