ON PLATEAUED FUNCTIONS, LINEAR STRUCTURES, PERMUTATION POLYNOMIALS AND C-DIFFERENTIAL UNIFORMITY

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

BY

KÜBRA KAYTANCI

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

AUGUST 2023

Approval of the thesis:

ON PLATEAUED FUNCTIONS, LINEAR STRUCTURES, PERMUTATION POLYNOMIALS AND C-DIFFERENTIAL UNIFORMITY

submitted by **KÜBRA KAYTANCI** 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
Dean, Graduate School of **Applied Mathematics** ______________

Assoc. Prof. Dr. Oğuz Yayla
Head of Department, **Cryptography** ______________

Prof. Dr. Ferruh Özbudak
Supervisor, **Mathematics, METU** ______________

Examining Committee Members:

Prof. Dr. Murat Cenk
Cryptography, METU ______________

Prof. Dr. Ferruh Özbudak
Mathematics, METU ______________

Assoc. Prof. Dr. Burcu Gülmez Temür
Mathematics, Atılım University ______________

Assist. Prof. Dr. Buket Özkaya
Cryptography, METU ______________

Assist. Prof. Dr. Eda Tekin
Business Administration, 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: KÜBRA KAYTANCI

Signature :

ABSTRACT

ON PLATEAUED FUNCTIONS, LINEAR STRUCTURES, PERMUTATION POLYNOMIALS AND C-DIFFERENTIAL UNIFORMITY

Kaytancı, Kübra
Ph.D., Department of Cryptography
Supervisor : Prof. Dr. Ferruh Özbudak

August 2023, 48 pages

A desired goal in designing good cryptosystems is to construct boolean functions with good cryptographic properties, such as having high nonlinearity, balancedness, high correlation immunity, and high algebraic immunity. In this thesis, we obtain concrete upper bounds on the algebraic immunity of a class of highly nonlinear plateaued functions without linear structures than the one given recently in 2017 by Cusick. Moreover, we extend Cusick's class to a much bigger explicit class, and we show that our class has better algebraic immunity by an explicit example. We also give a new notion of the linear translator, which includes the Frobenius linear translator given in 2018, Cepak, Pasalic, and Muratović-Ribić as a particular case. We find some applications of our new notion of linear translator to the construction of permutation polynomials. Furthermore, we give explicit classes of permutation polynomials over $\mathbb{F}_{q^n}$ using some properties of $\mathbb{F}_q$ and some conditions of 2011, Akbary, Ghioca, and Wang. Additionally, recently Ellingsen et al. introduced a new concept, the c-Difference Distribution Table and the c-differential uniformity, by extending the usual differential notion. The motivation behind this new concept is based on having the ability to resist some known differential attacks, as shown by Borisov et. al. in 2002. In 2022, Hasan et al. gave an upper bound of the c-differential uniformity of the perturbed inverse function H via a trace function $\mathrm{Tr}\left(\frac{x^2}{x+1}\right)$. In their work, they also presented an open question on the exact c-differential uniformity of H. By using a new method based on algebraic curves over finite fields, we solve the open question in the case $Tr(c) = 1 = Tr(\frac{1}{c})$ for $c \in \mathbb{F}_{2^n} \setminus \{0, 1\}$ completely and we show that the exact c-differential uniformity of H is 8. In the remaining case, we almost completely solve the problem, and show that the c-differential uniformity of H is either 8 or 9.

Keywords: Plateaued functions, Linear structure, Permutation polynomials, c-Differential Uniformity

ÖZ

PLATEAUED FONKSİYONLAR, DOĞRUSAL YAPILAR, PERMÜTASYON POLİNOMLARI VE C-DİFERANSİYEL TEKDÜZELİK ÜZERİNE

Kaytancı, Kübra
Doktora, Kriptografi Bölümü
Tez Yöneticisi : Prof. Dr. Ferruh Özbudak

Ağustos 2023, 48 sayfa

İyi şifreleme sistemlerinin tasarlanmasında istenen bir amaç, yüksek doğrusal olmama, dengelilik, yüksek korelasyon bağışıklığı ve yüksek cebirsel bağışıklığa sahip olmak gibi iyi kriptografik özelliklere sahip boole fonksiyonları oluşturmaktır. Bu tezde, son zamanlarda 2017'de Cusick'te verilenden, doğrusal yapıları olmayan yüksek düzeyde doğrusal olmayan plateaued fonksiyonlar sınıfının cebirsel bağışıklığına ilişkin somut üst sınırlar elde ediyoruz. Ayrıca, Cusick'in sınıfını çok daha büyük bir sınıfa genişletiyoruz ve bir örnekle sınıfımızın daha iyi cebirsel bağışıklığa sahip olduğunu gösteriyoruz. Ayrıca 2018'de verilen Frobenius doğrusal çevirici, Cepak, Pasalic ve özel bir durum olarak Muratović-Ribić içeren yeni bir doğrusal çevirici kavramı veriyoruz. Yeni doğrusal çevirici kavramımızın permütasyon polinomlarının inşasında bazı uygulamalarını buluyoruz. Ayrıca, $\mathbb{F}_q$'ın bazı özelliklerini ve 2011'in bazı koşullarını, Akbary, Ghioca ve Wang'ı kullanarak $\mathbb{F}_{q^n}$ üzerinde permütasyon polinomlarının sınıflarını veriyoruz. Ayrıca, son zamanlarda Ellingsen ve diğerleri diferansiyel kavramını genişleterek yeni bir kavram olan c-Fark Dağılım Tablosunu ve c-diferansiyel tekdüzeliği tanıttı. Bu yeni konseptin arkasındaki motivasyon, 2002'de Borisov ve diğerleri tarafından gösterilen bazı bilinen farklı saldırılara direnme yeteneğine sahip olmaya dayanmaktadır. 2002'de Hasan ve diğerleri $\mathrm{Tr}\left(\frac{x^2}{x+1}\right)$ fonksiyonu aracılığıyla H ters fonksiyonla pertürbe edilen c-diferansiyel tekdüzeliğinin bir üst sınırını verdi. Çalışmalarında, H'ın tam c-diferansiyel tekdüzeliği hakkında açık bir soru da sundular. Sonlu cisimler üzerinden cebirsel eğrilere dayalı yeni bir yöntem kullanarak, $c \in \mathbb{F}_{2^n} \setminus \{0, 1\}$ için $Tr(c) = 1 = Tr(\frac{1}{c})$ durumunda açık soruyu tamamen çözüyoruz ve H'ın tam c-diferansiyel tekdüzeliğinin 8 olduğunu gösteriyoruz. Kalan durumda, sorunu neredeyse tamamen çözüyoruz ve H'ın c-diferansiyel tekdüzeliğinin 8 veya 9 olduğunu gösteriyoruz.

Anahtar Kelimeler: Plateaued fonksiyonları, Doğrusal Yapılar, Permütasyon polinomları, c-Diferansiyel Tekdüzelik

ACKNOWLEDGMENTS

First and foremost, I would like to express my great appreciation to my thesis supervisor Prof. Dr. Ferruh Özbudak for his invaluable guidance, motivation, and advice during the development and preparation of this thesis and associated research. His willingness to give his time and share his experiences has brightened my path. It is a great honor to work with him.

I also would like to express my sincere thanks to Prof. Dr. Murat Cenk for his encouragement, advice, and support, both academically and emotionally, during my doctoral study and for being a committee member of my defense.

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

I want to thank Assist. Prof. Eda Tekin, Assist. Prof. Buket Özkaya and Assoc. Prof. Burcu Gülmez Temür for being a committee member of my defense.

I would like to thank The Scientific and Technological Research Council of Turkey (TÜBİTAK) for supporting a part of this work under the Grant No. 115R289.

Also, I would like to thank The Council of Higher Education (YÖK) for supporting a part of this work under the 100/2000 Ph.D. scholarship program.

I want to thank all the academic and administrative staff of the Institute of Applied Mathematics for their valuable assistance throughout my doctoral study. I am particularly grateful to Ebru Gündoğdu, Nejla Erdoğdu, and Serkan Demiröz for their administrative guidance.

Also, I would like to thank Meral Şimşek, Bartu Yünüak, Cem Yavrum, Mustafa Kütük, and Gülçin Akarsu for their sincere friendship, their willingness to help as well as colleagueship in the path of pursuing the degree. Additionally, my special thank goes to Zeynelabidin Karakaş, Esra Günsay, Burcu Ecem Karakaş, İrem Keskinkurt-Paksoy, and Pelin Çiloğlu for their friendship. They all make Institute such a friendly and cheerful atmosphere.

I am grateful to my dearest parent: Behiye Kaytancı, and Tekin Kaytancı, for their invaluable and unconditional support throughout my entire life. They always support me during my long education life and believe in me. Without them, it would be much harder for me to finalize this thesis. I would also like to thank you my sister Merve Kaytancı for her continuous encouragements.

İlkiz Bildik, Fulya Taştan, Fatma Hakkıoğlu, Gülşah Altay, and Saadet Etli deserve special thanks for their sincere friendship and their help during my hard times. Even though we may be far apart, I always feel their support and presence whenever I require it.

Last but not least, my heartfelt thanks to Oğuz Arslan. He was always there cheering me up and listening to my every concern. I cannot express my gratitude for his unwavering presence and support through tough times. Also, my lovely thanks to Minerva aka "Mik Mik", who helped me to overcome the stress with her purrfect way of being.

TABLE OF CONTENTS

CHAPTERS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

$\mathbb{F}_q$	The finite field of order q^n
q	A power of a prime number
$\hat{f}$	The Walsh transform of a function f
$AI(f)$	The algebraic immunity of a function f
$D_F(x,a)$	The derivative of a function F in the direction a
$\Delta_F(a,b)$	The Difference Distribution Table entry at point (a,b)
Δ_F	The differential uniformity of a function F
${}_cD_F(x,a)$	The c-derivative of a function F
${}_c\Delta_F(x,a)$	The c-Difference Distributive Table entry at point (a,b)
${}_c\Delta_F$	The c-differential uniformity of a function F
Tr_n	The trace function from $\mathbb{F}_q^n$ to $\mathbb{F}_q$

CHAPTER 1

INTRODUCTION

In cryptography, in order to design stream and block ciphers, boolean functions play a significant role. Boolean functions with good cryptographic properties have an ability to withstand the known cryptanalytic attacks. One of the properties of Boolean functions is nonlinearity which is defined as the Hamming distance to the closest affine function. Having high nonlinearity is a desired property for good cryptosystems since the systems having low nonlinearity are vulnerable to some attacks such as Linear Cryptanalysis for Block Ciphers, Linear Cryptanalysis for Stream Ciphers, Fast Correlation Attacks, etc. Bent functions attain the highest possible nonlinearity.

In [36], Zheng and Zhang introduced Plateaued functions in 1999 as potentially good cryptographic functions. They are a generalization of bent functions. They are important not only for cryptography but also for some related areas, including coding theory and communication. There have been many results in recent years regarding their construction, existence, and applications. We refer to [4], [7], [10], [9], [11], [14], [23], [26], [28],[32], [33].

Recently, Cusick [15] gave an explicit construction of highly nonlinear plateaued functions without linear structure. In Section 3, we obtain a much larger class of explicit functions having all these good properties and including Cusick's class of functions as a very small subclass. Moreover, we prove that Cusick's class has quite a low algebraic immunity by concrete upper bounds. We also give an explicit example of our class having better algebraic immunity than the functions in Cusick's class.

For the construction of non-trivial mathematical structures, it has been shown that linear structures (and linear translators) are useful. There are important connections between linear translators and permutation polynomials over finite fields (see, [20]). Recently, the authors in [13] gave a generalization of linear translators called the Frobenius linear translator. They also give some applications of their generalization to the construction of permutation polynomials. In Chapter 5, we obtain a further and natural generalization of linear translators using additive polynomials. Our generalization also has applications to the construction of permutation polynomials (see, Theorem 5.1, Theorem 5.2 and Example 2 below).

Akbary, Ghioca, and Wang [1] established a very interesting method to construct permutation polynomials over "big" finite fields. If an explicit class of permutation polynomials that satisfies certain criteria is found over a subfield $\mathbb{F}_q$, it can be used to construct an explicit class of permutation polynomials over an extension field $\mathbb{F}_{q^n}$. For example, the authors in [12] obtained such explicit permutation polynomial classes over $\mathbb{F}_{q^2}$ by using certain properties of $\mathbb{F}_q$. By a similar motivation, we obtain further explicit permutation polynomial classes over $\mathbb{F}_{q^n}$ via $\mathbb{F}_q$ with $n \geq 2$ in Chapter 4.

Differential cryptanalysis is one of the most crucial cryptanalytic methods for evaluating the security of symmetric encryption algorithms such as block ciphers. In 1990, Biham and Shamir first applied this new type of cryptanalytic attack to DES-like cryptosystems in [2]. This new method made a significant improvement in designing the symmetric encryption algorithms.

Later, the differential uniformity was described in [27]. The differential uniformity of a given function measures the resistance against differential attacks. To design a good cryptosystem, functions with low differential uniformity are one of the desired properties to prevent differential attacks on the cipher. Since then, many researchers have worked on constructing functions with low differential uniformity. We refer to [5, 6, 8].

In 2002, Borisov et al. in [3] introduced a new type of differential called multiplicative differential that is used in the differential attack on some ciphers. Hence it can be used to analyze the resistance against an extension of a differential attack. Then, in 2020, Ellingsen et al. in [17] extended this idea and defined the c-Difference Distribution Table and the c-differential uniformity. A low c-differential uniformity is a good cryptographic property as the usual notion of differential uniformity. Later, the c-differential uniformity of some of the functions with known differential uniformity was studied in [18], [19], [29], [30], [34], [35]. Hasan et al. in [19] worked on the c-differential uniformity of some known perfect nonlinear functions and the inverse function. The differential uniformity of the inverse function remains the same under the operation of adding a trace function $Tr\left(\frac{x^2}{x+1}\right)$ to the inverse function. So they worked on the c-differential uniformity of the perturbed inverse function via a trace function $Tr\left(\frac{x^2}{x+1}\right)$ in [19] and gave the upper bound, which is 8 in the case $Tr(c) = 1 = Tr(\frac{1}{c})$ for $c \in \mathbb{F}_{2^n} \setminus \{0,1\}$ and 9 in the remaining case for $c \neq 0$.

Finding the exact value of the c-differential uniformity of functions is a challenging problem. In many cases, finding a lower bound for the c-differential uniformity requires different techniques than finding an upper bound. There is no general method in the literature for finding a lower bound of the c-differential uniformity of functions. This method can yield additional results for similar problems within this field. We refer to [25] for another use of algebraic curves in cryptography.

In Chapter 6, we develop a new method using algebraic curves over finite fields, which is not used in the references [18], [19], [29], [30], [34], [35] in order to find an effective lower bound of the c-differential uniformity of a function. By this new method, we almost completely solve the open question in *[19, Remark 10]*. What we mean by almost completely solve is the following: in the case $Tr(c) = 1 = Tr(\frac{1}{c})$ for $c \in \mathbb{F}_{2^n} \setminus \{0,1\}$, we completely solve the question and the exact c-differential uniformity of the perturbed inverse function via a trace function $Tr\left(\frac{x^2}{x+1}\right)$ is 8. In the remaining case, we show that the c-differential uniformity of the perturbed inverse function via a trace function $\mathrm{Tr}\left(\frac{x^2}{x+1}\right)$ is either 8 or 9, which is, in a sense, the next best result.

The thesis is organized as follows: In Chapter 2, some basic definitions and tools will be given, which are required to follow the subsequent chapters. In Chapters 3, 4, 5 and 6, we give details of our corresponding contributions and motivations.

CHAPTER 2

PRELIMINARIES

Let q be a power of a prime number and $\mathbb{F}_{q^n}$ be the finite field of order q^n where $n \geq 1$. The extension field $\mathbb{F}_{q^n}$ can be viewed as an n-dimensional vector space over $\mathbb{F}_q$. The trace function Tr_n from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ is defined as

$$\begin{aligned} Tr_n : \mathbb{F}_{q^n} &\to \mathbb{F}_q \\ \alpha &\mapsto \alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{n-1}}. \end{aligned}$$

A Boolean function f of n-variables is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$.

Definition 2.1. *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function. Then the Walsh transform $\hat{f}$ of f is defined as*

$$\begin{aligned} \hat{f} : \mathbb{F}_2^n &\to \mathbb{Z} \\ w &\mapsto \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+w \cdot x} \end{aligned}$$

where $w = (w_1, w_2, \ldots, w_n)$, $x = (x_1, x_2, \ldots, x_n)$ and $w \cdot x = w_1x_1 + \cdots + w_nx_n$.

Definition 2.2. *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function. Then f has linear structure at $a \in \mathbb{F}_2^n$ if and only if either $f(x + a) + f(x) = 0$ for any $x \in \mathbb{F}_2^n$(a is called a 0-linear structure) or $f(x + a) + f(x) = 1$ for any $x \in \mathbb{F}_2^n$(a is called a 1-linear structure).*

Definition 2.3. *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function. Then f is called an s-plateaued function where $0 \leq s \leq n$ if $|\hat{f}(w)|^2 \in \{0, 2^{n+s}\}$ for any $w \in \mathbb{F}_2^n$ where $|\hat{f}(w)|$ denotes the size of $\hat{f}(w)$.*

Definition 2.4 (See, for example [7]). *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function. The algebraic normal form of f is*

$$f(x) := \bigoplus_{\mathcal{I} \in \mathcal{P}(N)} a_{\mathcal{I}} \left(\prod_{\mathcal{I} \in \mathcal{P}(N)} x^{\mathcal{I}} \right),$$

where $\mathcal{P}(N)$ denotes the power set of $N = \{1, \dots, n\}$. The degree of the algebraic normal form of f is equal to

$$\max\{|\mathcal{I}| : a_{\mathcal{I}} \neq 0\}.$$

Definition 2.5 (See, for example [7]). *Let $f : \mathbb{F}_2^n \to \mathbb{F}$ be a Boolean function. The algebraic immunity $AI(f)$ of f is defined to be the minimal degree of a nonzero function g from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ for which $f \cdot g = 0$ or $(f + 1) \cdot g = 0$, i.e*

$$AI(f) := min\{\deg g : g \in Ann(f) \cup Ann(f + 1)\}$$

where $Ann(f)$ is the set of annihilators of f. A function g is an annihilator of f if $f \cdot g = 0$.

Remark 1. *It is well-known that for any Boolean function f of n-variables, $AI(f) \leq \lceil \frac{n}{2} \rceil$.*

Let $\mathbb{F}_q$ denote the finite field of order $q = 2^n$ where $n \geq 1$. Any map $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ is called a vectorial binary function or (n, m)-function where n, m are positive integers. When $n = m$, the univariate representation of a binary function F is of the form

$$F(x) := \sum_{i=0}^{2^n - 1} a_i x^i, \quad a_i \in \mathbb{F}_{2^n},$$

whose algebraic degree is the maximum Hamming weight of the vector i where $a_i \neq 0$. The absolute trace function Tr_n from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ is defined as

$$\begin{aligned} Tr_n : \mathbb{F}_{2^n} &\to \mathbb{F}_2 \\ \alpha &\mapsto \alpha + \alpha^2 + \alpha^{2^2} + \cdots + \alpha^{2^{n-1}}. \end{aligned}$$

Definition 2.6. *For any function $F : \mathbb{F}_q \to \mathbb{F}_q$ and $a \in \mathbb{F}_q$, the derivative of F in the direction a with $q = 2^n$ is defined as*

$$D_F(x, a) := F(x + a) + F(x) \textit{ for all } x \in \mathbb{F}_q.$$

The Difference Distribution Table entry at point (a, b) for any a,b $\in \mathbb{F}_q$ is defined as

$$\Delta_F(a, b) :=\mid \{x \in \mathbb{F}_q : D_F(x, a) = b\} \mid .$$

The differential uniformity of F is defined as

$$\Delta_F := \max\{\Delta_F(a, b) : a, b \in \mathbb{F}_q, a \neq 0\}.$$

When $\Delta_F := \delta$, the function F is called δ-uniform. Since characteristic of $\mathbb{F}_q$ is 2, then $\delta \geq 2$. If $\delta = 2$, then the function F is called almost perfect nonlinear. Based on this concept, the definition of the c-differential uniformity is as follows.

Definition 2.7. *Let $F : \mathbb{F}_q \to \mathbb{F}_q$ be a function and let a, $c \in \mathbb{F}_q$ be given with $q = 2^n$. The c-derivative of F at a is*

$$_cD_F(x, a) := F(x + a) + cF(x), \textit{ for any } x \in \mathbb{F}_q.$$

For any $a, b \in \mathbb{F}_q$, the c-differential uniformity of $F : \mathbb{F}_q \to \mathbb{F}_q$ is

$$_c\Delta_F := \max\{_c\Delta_F(a, b) : a, b \in \mathbb{F}_q, \textit{ and } a \neq 0 \textit{ if } c = 1\}$$

where the c-Difference Distribution entries are

$$_c\Delta_F(a, b) =\mid \{x \in \mathbb{F}_q : F(x + a) + cF(x) = b\} \mid .$$

When $c = 1$, we have the usual notion of differential uniformity. If $_c\Delta_F = \delta_c$, then δ_c is called the c-differential uniformity of F. If $\delta_c = 1$, then F is perfect c-nonlinear (PcN). If $\delta_c = 2$, then F is almost perfect c-nonlinear (APcN).

The theory of algebraic curves over finite fields is essentially equivalent to the theory of function fields in positive characteristics. From now on, we will use the language of function fields. For notation and further background on function fields, we refer to [31].

Definition 2.8. *A place P of the function field F/K is the maximal ideal of some valuation ring $\mathcal{O}$ of F/K.*

Definition 2.9. *An Artin-Schreier curve is a curve over the algebraically closed field $\overline{\mathbb{F}}_{2^n}$ of the form $y^2 + y = f(x)$ where f is a rational function over $\mathbb{F}_{2^n}$.*

Some important properties of Artin-Schreier extensions are presented in the following proposition which we will use below.

Proposition 2.1 (Artin-Schreier Extensions)**.** *[[31] Prop. 3.7.8] Let F/K be an algebraic function field of characteristic 2. Suppose that $u \in F$ is an element which satisfies the following condition:*

$$u \neq w^2 + w \textit{ for all } w \in F.$$

Let

$$F' = F(y) \textit{ with } y^2 + y = u. \tag{2.1}$$

Such an extension F'/F is called an Artin-Schreier extension of F. For $P \in \mathbb{P}_F$ we define the integer m_P by

$$m_P = \begin{cases} m & \textit{if there is an element } z \in F \textit{ satisfying} \\ & v_P(u + (z^2 + z)) = -m < 0 \textit{ and } m \not\equiv 0 \mod 2, \\ -1 & \textit{if } v_P(u + (z^2 + z)) \geq 0 \textit{ for some } z \in F. \end{cases}$$

(d) If at least one place $Q \in \mathbb{P}_F$ satisfies $m_Q > 0$, then K is algebraically closed in F' and

$$g' = 2g + \frac{1}{2}\Big(-2 + \sum_{P \in \mathbb{P}_F} (m_P + 1) . \deg P \Big),$$

where g'(resp. g) is the genus of F'/K(resp. F/K)).

CHAPTER 3

CUSICK'S HIGHLY NONLINEAR PLATEAUED FUNCTIONS AND THEIR MODIFICATIONS

For integers $d \geq 3$ and $k \geq 1$, Cusick introduced an explicit class of Boolean functions of degree d in $n = 2dk - 1$ variables given by

$$f_k(x_1, x_2, \ldots, x_n) = \sum_{j=0}^{k-1} x_{dj+1} \ldots x_{dj+d} + \sum_{j=1}^{m-1} x_j x_{j+m}. \tag{3.1}$$

where $m = dk$. He proved that these are 1-plateaued, have no linear structure and have nonlinearity $2^{n-1} - 2^{\frac{n-1}{2}}$. They become balanced by adding a concrete linear function. Note that adding a linear function does not change plateauedness, nonlinearity or the set of linear structures. He also states that "... a high algebraic immunity is not to be expected"in [15, page 80, the last paragraph].

In this chapter, we show that indeed algebraic immunity of the functions in (3.1) is low. Note that the largest degree of the class for a fixed odd integer $n \geq 3$ occurs when $k = 1$. Moreover, if $m = \frac{n-1}{2}$ is a prime, then k may only taken to be 1 in (3.1). The following result shows in particular that this class has very low algebraic immunity when k is small.

Proposition 3.1. *For integers $d \geq 3$ and $k \geq 1$, let $n = 2dk - 1$ and $f_k : \mathbb{F}_2^n \to \mathbb{F}_2$ be the Boolean function defined in (3.1). We have:*

i) $AI(f_1) \leq 3$.

ii) *For $k \geq 2$, $AI(f_k) \leq \min\{k+2, \frac{n+1}{2k}\}$.*

Proof. We first prove item i). Put $x = (x_1, x_2, \ldots, x_{m-1})$ and $y = (y_1, \ldots, y_{m-1}) =$

$(x_{m+1}, \dots, x_{2m-1})$ where $m = dk$. Let

$$h(x) = x_1 x_2 \dots x_{m-1} \text{ and } g(x,y) = x_1 y_1 + x_2 y_2 + \cdots + x_{m-1} y_{m-1}.$$

Then it is easy to observe that

$$f_1(x_1, \dots, x_n) = h(x) x_m + g(x,y).$$

It is enough to prove that

$$f_1(x_1, \dots, x_n) \left(g(x,y) + 1\right) (x_m + 1) = 0$$

for all $x, y \in \mathbb{F}_2^{m-1}$ and $x_m \in \mathbb{F}_2$. Indeed, $\deg \left(g(x,y)+1\right)(x_m+1) = 2 + 1 = 3$. Moreover,

$$\begin{aligned} f_1(x_1, \dots, x_n) \left(g(x,y)+1\right)(x_m+1) &= \left(h(x)x_m + g(x,y)\right)\left(g(x,y)+1\right)(x_m+1) \\ &= \left(h(x)x_m g(x,y) + h(x)x_m + g(x,y) + g(x,y)\right)(x_m+1) \\ &= \left(h(x)x_m \left(g(x,y)+1\right)\right)(x_m+1) \\ &= h(x)\left(g(x,y)+1\right)\left(x_m(x_m+1)\right) = 0, \end{aligned}$$

as $(x_m(x_m+1)) = 0$. This completes the proof of item $i)$.

Next, we consider the proof of item $ii)$. Note that

$$f_k(x_1, \dots, x_n) = x_1 \dots x_d + x_{d+1} \dots x_{2d} + \cdots + x_{(k-1)(d+1)} \dots x_{m-1} x_m + g(x,y).$$

Here

$$\begin{aligned} & f_k(x_1, \dots, x_n) \left((x_1+1)(x_d+1) \dots (x_{(k-1)(d+1)}+1\right) \left(g(x,y)+1\right)) \\ &\qquad = x_1(x_1+1) r_1(x_1, \dots, x_n) + x_{d+1}(x_{d+1}+1) r_2(x_1, \dots, x_n) + \dots \\ &\qquad + x_{(k-1)(d+1)}(x_{(k-1)(d+1)}+1) r_k(x_1, \dots, x_n) \\ &\qquad + g(x,y)\left(g(x,y)+1\right) r_{k+1}(x_1, \dots, x_n) \end{aligned}$$

for some polynomials $r_1(x_1, \dots, x_n), \dots, r_{k+1}(x_1, \dots, x_n)$ in algebraic normal form. As

$$x_1(x_1+1) = x_{d+1}(x_{d+1}+1) = \cdots = x_{(k-1)(d+1)}(x_{(k-1)(d+1)}+1) = 0$$

and $g(x,y)\left(g(x,y)+1\right) = 0$ as Boolean functions and

$$\deg \big((x_1+1)(x_{d+1}+1) \dots (x_{(k-1)(d+1)}+1)\left(g(x,y)+1\right)\big) = k+2,$$

we have $AI(f_k) \leq k+2$. Also

$$f_k(x_1,\ldots,x_n)\,(f_k(x_1,\ldots,x_n)+1) = 0.$$

And $\deg\,(f_k(x_1,\ldots,x_n)+1) = d = \frac{n+1}{2k}$. Hence $AI(f_k) \leq \min\{k+2, \frac{n+1}{2k}\}$. □

Next, we define a much larger explicit class of Boolean functions containing Cusick's class as defined in (3.1) as a small subclass. The functions of this class are 1-plateaued, having nonlinearity $2^{n-1} - 2^{\frac{n-1}{2}}$ and balanced up to addition of a concrete linear function as in Cusick's class. Moreover, we also have a characterization whether a function in our class has a linear structure. This condition is easy to apply. Moreover, we give an explicit example demonstrating that the algebraic immunity of a function in our class is much better compared to the class defined in (3.1).

We first note that if $h : \mathbb{F}_2^{m-1} \to \mathbb{F}_2$ is an arbitrary map, then we have

$$|\{(\alpha_m,\beta) \in \mathbb{F}_2 \times \mathbb{F}_2^{m-1} : h(\beta)+\alpha_m = 0\}| = 2^{m-1}.$$

Now we are ready to give our much larger class of Boolean functions consisting of 1-plateaued, highly nonlinear functions without linear structure. It is easy to make them balanced by adding a linear term as explained in the theorem as well.

Theorem 3.2. *Let $n \geq 3$ be odd and $n = 2m-1$. Let $\pi : \mathbb{F}_2^{m-1} \to \mathbb{F}_2^{m-1}$ be a permutation map. Let $g_0, g_1 : \mathbb{F}_2^{m-1} \to \mathbb{F}_2$ be Boolean maps. Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be the Boolean map defined as*

$$\begin{aligned} f : \mathbb{F}_2^{m-1} \times \mathbb{F}_2 \times \mathbb{F}_2^{m-1} &\to \mathbb{F}_2 \\ (x, x_m, y) &\mapsto g_0(x) + x_m g_1(x) + \pi(x)\cdot y. \end{aligned}$$

Then we have:

i) f is a 1-plateaued function.

ii) f has no nonzero linear structure if and only if the subset

$$S = \{(\alpha_m,\beta) \in \mathbb{F}_2 \times \mathbb{F}_2^{m-1} : g_1(\pi^{-1}(\beta)) + \alpha_m = 0\} \subseteq \mathbb{F}_2 \times \mathbb{F}_2^{m-1}$$

is not an affine or linear subset (of dimension m-1).

iii) The nonlinearity of f is $2^{n-1}-2^{(n-1)/2}$.

iv) For $(u,\mu,v)\in\mathbb{F}_2^{m-1}\times\mathbb{F}_2\times\mathbb{F}_2^{m-1}$, the function

$$f_{u,\mu,v}(x,x_m,y):=f(x,x_m,y)+u\cdot x+\mu\cdot x_m+v\cdot y$$

is balanced if and only if $g_1(\pi^{-1}(v))+\mu=1$.

Proof. Let $w=(\alpha,\alpha_m,\beta)\in\mathbb{F}_2^{m-1}\times\mathbb{F}_2\times\mathbb{F}_2^{m-1}$. We have

$$\begin{aligned}\hat{f}(w)&=\sum_{x\in\mathbb{F}_2^{m-1}}\sum_{x_m\in\mathbb{F}_2}\sum_{y\in\mathbb{F}_2^{m-1}}(-1)^{g_0(x)+x_mg_1(x)+\pi(x)\cdot y+\alpha\cdot x+\alpha_mx_m+\beta\cdot y}\\&=\sum_{x\in\mathbb{F}_2^{m-1}}\sum_{x_m\in\mathbb{F}_2}(-1)^{g_0(x)+x_mg_1(x)+\alpha\cdot x+\alpha_mx_m}\sum_{y\in\mathbb{F}_2^{m-1}}(-1)^{(\pi(x)+\beta)\cdot y}\\&=2^{m-1}\sum_{x\in\mathbb{F}_2^{m-1}}\sum_{x_m\in\mathbb{F}_2}(-1)^{g_0(x)+x_mg_1(x)+\alpha\cdot x+\alpha_mx_m}\quad\text{for }\pi(x)=\beta\\&=2^{m-1}(-1)^{g_0(\pi^{-1}(\beta))+\alpha\cdot\pi^{-1}(\beta)}\sum_{x_m\in\mathbb{F}_2}(-1)^{(g_1(\pi^{-1}(\beta))+\alpha_m)x_m}.\end{aligned}$$

Hence

$$\hat{f}(w)=\begin{cases}2^m(-1)^{g_0(\pi^{-1}(\beta))+\alpha\cdot\pi^{-1}(\beta)} & \text{if } g_1(\pi^{-1}(\beta))=\alpha_m,\\ 0 & \text{otherwise.}\end{cases}$$

This completes the proof of the item $i)$.

It is well-known that the nonlinearity of an arbitrary Boolean function $f:\mathbb{F}_2^n\to\mathbb{F}_2$ is $2^{n-1}-\frac{1}{2}\max_{w\in\mathbb{F}_2^n}|\hat{f}(w)|$. Hence in our case the nonlinearity of our function f is

$$2^{n-1}-\frac{1}{2}\max_{w\in\mathbb{F}_2^n}|\hat{f}(w)|=2^{n-1}-\frac{1}{2}2^m=2^{n-1}-2^{\frac{n-1}{2}}.$$

This completes the proof of item $iii)$.

It is also well-known that the Walsh value $\hat{f}_{u,\mu,v}(0,0,0)$ of $\hat{f}_{u,\mu,v}(x,x_m,y)$ is $\hat{f}(u,\mu,v)$. Hence

$$\hat{f}_{u,\mu,v}(0,0,0)=0\Longleftrightarrow g_1(\pi^{-1}(v))+\mu=1.$$

Note that $f_{u,\mu,v}(x, x_m, y)$ is balanced if and only if $\hat{f}_{u,\mu,v}(0, 0, 0) = 0$. This completes the proof of item $iv)$.

It only remains to prove the item ii). Let S_f denote the support of the Walsh spectrum of f, that is $S_f = \{w \in \mathbb{F}_2^{m-1} \times \mathbb{F}_2 \times \mathbb{F}_2^{m-1} : \hat{f}(w) \neq 0\}$. Let $S \subseteq \mathbb{F}_2 \times \mathbb{F}_2^{m-1}$ be the subset defined as

$$S = \{(\alpha_m, \beta) \in \mathbb{F}_2 \times \mathbb{F}_2^{m-1} : g_1(\pi^{-1}(\beta)) + \alpha_m = 0\}. \tag{3.2}$$

It follows from the proof of item $i)$ above that $S_f = \mathbb{F}_2^{m-1} \times S$. For $\nu \in \mathbb{F}_2^n$, let $\Delta_f(\nu)$ be the sum

$$\Delta_f(\nu) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x+\nu)+f(x)}.$$

It is clear that ν is a linear structure of f if and only if $\Delta_f(\nu) = \pm 2^n$. Moreover, it is not difficult to observe that

$$\sum_{w \in \mathbb{F}_2^n} \hat{f}(w)^2 (-1)^{\nu \cdot w} = 2^n \Delta_f(\nu),$$

which holds for an arbitrary Boolean map $f : \mathbb{F}_2^n \to \mathbb{F}_2$. In our case f is
1-plateaued and hence

$$\sum_{w \in \mathbb{F}_2^n} \hat{f}(w)^2 (-1)^{\nu \cdot w} = \sum_{w \in S_f} |\hat{f}(w)|^2 (-1)^{\nu \cdot w} = 2^{n+1} \sum_{w \in S_f} (-1)^{\nu \cdot w},$$

where we use our proof of item $i)$ above. These implies that if $\nu \in \mathbb{F}_2^n$, then we have

$$\Delta_f(\nu) = 2 \sum_{w \in S_f} (-1)^{\nu \cdot w}.$$

As $|S_f| = 2^{n-1}$, we conclude that $\nu \in \mathbb{F}_2^n$ is a linear structure of f if and only if ($\nu \cdot w = 0$ for all $w \in S_f$) or ($\nu \cdot w = 1$ for all $w \in S_f$). Assume that $v = (a, a_m, b) \in \mathbb{F}_2^{m-1} \times \mathbb{F}_2 \times \mathbb{F}_2^{m-1}$ is a nonzero linear structure of f. Recall that $S_f = \mathbb{F}_2^{m-1} \times S$ where S is defined in (3.2). First we show that $a = 0$. Indeed otherwise there exist $\alpha, \alpha' \in \mathbb{F}_2^{m-1}$ such that $a \cdot \alpha \neq a \cdot \alpha'$. For fixed $(\alpha_m, \beta) \in S$, both $(\alpha, \alpha_m, \beta)$ and $(\alpha', \alpha_m, \beta)$ are elements of S_f. Then it is impossible that $(a, a_m, b) \cdot (\alpha, \alpha_m, b) = (a, a_m, b) \cdot (\alpha', \alpha_m, b)$ which is a contradiction.

Next, assume that $\nu \cdot w = 0$ for all $w \in S_f$. Then $\nu = (0, a_m, b)$ and $0 = (a_m, b) \cdot (\alpha_m, \beta)$ for all $(\alpha_m, \beta) \in S$. As $\nu \neq 0$, there exist $(c, d) \in \mathbb{F}_2 \times \mathbb{F}_2^{m-1}$ such that

$(a_m, b) \cdot (c, d) \neq 0$. We choose such $(c, d) \in \mathbb{F}_2 \times \mathbb{F}_2^{m-1}$. As S is not a linear space and its cardinality is 2^{m-1}, the $\mathbb{F}_2$-span of S is the whole vector space $\mathbb{F}_2 \times \mathbb{F}_2^{m-1}$. In particular, there exist a subset $T \subseteq S$ such that

$$(c, d) = \sum_{(\alpha_m, \beta) \in T} (\alpha_m, \beta).$$

Multiplying both sides by (a_m, b) (as inner product) we get

$$(a_m, b) \cdot (c, d) = \sum_{(\alpha_m, \beta) \in T} (a_m, b) \cdot (c, d) = \sum_{(\alpha_m, \beta) \in T} 0 = 0.$$

However, this is a contradiction as $(a_m, b) \cdot (c, d) \neq 0$ by definition. This completes the proof of item $ii)$ under the assumption about $\nu \cdot w = 0$ for all $w \in S_f$.

Assume finally that $\nu \cdot w = 1$ for all $w \in S$. We choose $(\alpha_m^{(0)}, \beta^{(0)}) \in S$ and we define

$$S^L = \{(\alpha_m + \alpha_m^{(0)}, \beta + \beta^{(0)}) : (\alpha_m, \beta) \in S\}.$$

Note that S is affine if and only if S^L is linear. Moreover, $\nu = (0, a_m, b)$ is a nonzero linear structure of f if and only if $(a_m, b) \cdot (\alpha_m^L, \beta^L) = 0$ for all $(\alpha_m^L, \beta^L) \in S^L$. The same argument we used in the assumption $\nu \cdot w = 0$ for all $w \in S_f$ applied to S^L completes the proof. □

Example 1. *Let* $n = 2m - 1 = 11$. *Choose the permutation map*

$$\begin{aligned} \pi : \mathbb{F}_2^5 &\to \mathbb{F}_2^5 \\ x = (x_0, x_1, x_2, x_3, x_4) &\mapsto (\pi_1(x), \pi_2(x), \pi_3(x), \pi_4(x), \pi_5(x)) \end{aligned}$$

where

$$\pi_1(x) = x_0x_1x_2 + x_0x_1x_4 + x_0x_2x_3 + x_0x_2x_4 + x_0x_3 + x_0 + x_1x_2x_3x_4 + x_1x_2x_4$$
$$+ x_1x_2 + x_2x_3 + x_2x_4 + x_3x_4,$$
$$\pi_2(x) = x_0x_1x_2 + x_0x_1 + x_0x_2x_3x_4 + x_0x_2x_3 + x_0x_3x_4 + x_0x_3 + x_0x_4 + x_1x_2x_3$$
$$+ x_1x_3x_4 + x_1x_4 + x_1 + x_2x_3 + x_3x_4,$$
$$\pi_3(x) = x_0x_1x_3x_4 + x_0x_1x_3 + x_0x_1x_4 + x_0x_2x_4 + x_0x_2 + x_0x_3x_4 + x_1x_2x_3 + x_1x_2$$
$$+ x_1x_3x_4 + x_1x_4 + x_2x_3x_4 + x_2 + x_3x_4,$$
$$\pi_4(x) = x_0x_1x_2x_4 + x_0x_1x_2 + x_0x_1x_3 + x_0x_1x_4 + x_0x_1 + x_0x_2x_4 + x_0x_2 + x_0x_3$$
$$+ x_0 + x_1x_2x_4 + x_1x_3 + x_2x_3x_4 + x_2x_3 + x_3,$$
$$\pi_5(x) = x_0x_1x_2x_3 + x_0x_1x_2 + x_0x_1x_3 + x_0x_1x_4 + x_0x_2x_3 + x_0x_3x_4 + x_0x_3 + x_0x_4$$
$$+ x_1x_2x_3 + x_1x_2x_4 + x_1x_2 + x_1x_3 + x_1x_4 + x_1 + x_2x_4 + x_3x_4 + x_4.$$

Then take

$$g_0 : \mathbb{F}_2^5 \to \mathbb{F}_2$$
$$(x_0, x_1, x_2, x_3, x_4) \mapsto x_0 + x_2 + x_3$$

and

$$g_1 : \mathbb{F}_2^5 \to \mathbb{F}_2$$
$$(x_0, x_1, x_2, x_3, x_4) \mapsto x_1x_2x_3 + 1.$$

An application of our construction in Theorem 3.2 gives the map

$$f : \mathbb{F}_2^5 \times \mathbb{F}_2 \times \mathbb{F}_2^5 \to \mathbb{F}_2$$
$$(x, x_5, y) \mapsto g_0(x) + x_5g_1(x) + \pi(x)y$$
$$(x_0, x_1, x_2, x_3, x_4, x_5, y_0, y_1, y_2, y_3, y_4) \mapsto x_0 + x_2 + x_3 + (x_1x_2x_3 + 1)x_5 + y_0\pi_1(x)$$
$$+ y_1\pi_2(x) + y_2\pi_3(x) + y_3\pi_4(x) + y_4\pi_5(x)$$

where $\pi_i(x)$ *is defined as before for* $i = 1, \ldots, 5$. *The map is balanced, has no linear structure, has nonlinearity* $992 = 2^{10} - 2^5$ *and has algebraic immunity 4.*

In Example 1, $\pi : \mathbb{F}_2^5 \to \mathbb{F}_2^5$ corresponds to the permutation map $x \mapsto x^{30}$. Note that as $m = 5$ is a prime, there is only one function in Cusick's class, which is f_1 in

(3.1). Moreover, $AI(f_1) \leq 3$. Example 1 gives a concrete example in our class of Theorem 3.2 improving the algebraic immunity while keeping all the good properties of the maps of Cusick's class: high nonlinearity, 1-plateauedness, absence of having nonzero linear structures, and balancedness. Moreover, using different permutations $\pi : \mathbb{F}_2^5 \to \mathbb{F}_2^5$ and other suitable maps $g_0(x)$, $g_1(x)$ we get a lot of different Boolean functions with algebraic immunity 4 easily satisfying the conditions: 1-plateauedness, absence of having nonzero linear structures, and balancedness.

CHAPTER 4

CONSTRUCTING PERMUTATION POLYNOMIALS

Akbary, Ghioca and Wang [1] recently established a very interesting construction in order to construct polynomials over “big” finite fields using a commutative diagram relating the big field to some smaller subsets and the corresponding conditions on the maps of the commutative diagram. In fact, this construction gives different methods using different commutative diagrams leading to different conditions on different maps and subsets (see, for example [1, Proposition 5.9] and [1, Proposition 5.6]).

They generalized many earlier results and constructed many new permutation polynomial families. They also motivated many research directions in constructing explicit classes of permutation polynomials in “big” finite fields in the following sense: If a class of objects satisfying certain properties can be constructed which are guaranteed to satisfy a full set of conditions of Akbay, Ghioca and Wang in a small set (see, for example [1, Proposition 5.9] or [1, Proposition 5.6]), then it is possible to obtain an explicit class of permutation polynomials in the big finite field.

Recently Cepak, Charpin and Pasalic, among other results, gave such explicit classes in [12]. Namely, in [12, Section 6], they obtain permutation polynomials over $\mathbb{F}_{q^2}$ using certain polynomials over $\mathbb{F}_q$. We refer to Propositions 6, 8, 9 and the corresponding corollaries in [12].

Motivated by these results, we give explicit large class of permutation polynomials over $\mathbb{F}_{q^2}$ starting from polynomials over $\mathbb{F}_q$. We first state the proposition given by Akbary, Ghioca and Wang [1] and then we introduce the notion of b-permutation.

Proposition 4.1. *[[1] Proposition 5.9] Let $\phi(x)$ be an $\mathbb{F}_q$-linear polynomial over $\mathbb{F}_q$*

and $h(x) \in \mathbb{F}_{q^n}[x]$ be any polynomial satisfying $h(x^q - x) \in \mathbb{F}_q^*$ for all $x \in \mathbb{F}_{q^n}$. Let $g(x) \in \mathbb{F}_{q^n}[x]$. Then

i. *$h(x^q - x)\phi(x) + g(x^q - x)$ is a permutation polynomial of $\mathbb{F}_{q^n}$ if and only if*

(a) $\phi(x)$ induces a permutation polynomial of $\mathbb{F}_q$.

(b) $h(x)\phi(x) + g(x)^q - g(x)$ permutes $S = \{\alpha^q - \alpha | \alpha \in \mathbb{F}_{q^n}\}$.

ii. *For each $\phi(x)$ satisfying (a), we have $(q^{n-1})! \cdot q^{q^{n-1}}$ permutation polynomials of $\mathbb{F}_{q^n}$ of the form $\phi(x) + g(x^q - x)$.*

Definition 4.1. *Let $m(x) \in \mathbb{F}_q[x]$ and $b \in \mathbb{F}_q$ be given. We call $m(x)$ a b-permutation over $\mathbb{F}_q$ if the evaluation mapping $x \mapsto m(x) + bx$ defines a permutation over $\mathbb{F}_q$.*

Remark 2. *Note that it is not difficult to construct a b-permutation polynomial starting from a permutation polynomial. Indeed if $x \mapsto h(x)$ is a permutation polynomial, then $x \mapsto h(x) - bx$ is a b-permutation over $\mathbb{F}_q$.*

4.1 Constructing Permutation Polynomials over $\mathbb{F}_{q^2}$ via $\mathbb{F}_q$

First we present our results in characteristic 2. The following proposition indicates that it is easy to construct the corresponding large families of permutation polynomials over $\mathbb{F}_{q^2}$ as the component $g_0(x) \in \mathbb{F}_q[x]$ may be chosen arbitrarily.

Proposition 4.2. *Let $q = 2^k$ for some integer k. Let $\theta \in \mathbb{F}_{q^2}/\mathbb{F}_q$ satisfy $\theta^q + \theta = 1$ and $g_0(x) \in \mathbb{F}_q[x]$ be arbitrary. Then we have:*

- *$F(x) = x + g_0(x^q + x) + \theta(x^{2^i q} + x^{2^i} + x^q + x)$ is a permutation over $\mathbb{F}_{q^2}$ for any $i \geq 1$.*
- *If $q \not\equiv 1 \mod 3$, then*

  $$F(x) = x + g_0(x^q + x) + \theta(x^{3q} + x^{2q+1} + x^{q+2} + x^3 + x^q + x)$$

  is a permutation over $\mathbb{F}_{q^2}$.
- *If $q \not\equiv 1 \mod 5$, then*

  $$F(x) = x + g_0(x^q + x) + \theta(x^{5q} + x^{4q+1} + x^{q+4} + x^5 + x^q + x)$$

is a permutation over $\mathbb{F}_{q^2}$*.*

- *If* $r \geq 1$ *is an integer such that* $\gcd(r, q-1) = 1$*, then*

$$F(x) = x + g_0(x^q + x) + \theta\left((x^q + x)^r + (x^q + x)\right)$$

is a permutation over $\mathbb{F}_{q^2}$*.*

In fact, Proposition 4.2 is just a special subcase of the next theorem. We prefer to state Proposition 4.2 independently as it shows that the conditions of the next theorem are very easy to satisfy. We do not prove it as it follows from the proof of the next theorem.

Theorem 4.3. *Let* $q = 2^k$ *for some integer k. Let* $\theta \in \mathbb{F}_{q^2}/\mathbb{F}_q$ *satisfying* $\theta^q + \theta = 1$*. Let* $g_0(x) \in \mathbb{F}_q[x]$ *be arbitrary and* $g_1(x) \in \mathbb{F}_q[x]$ *be a* 1*-permutation over* $\mathbb{F}_q$*. Then*

$$F(x) = x + g_0(x^q + x) + \theta(g_1(x^q + x))$$

is a permutation over $\mathbb{F}_{q^2}$*.*

Proof. The proof comes from [1, Proposition 5.9], by taking $g(x)$ of the form $g(x) = g_0(x) + \theta g_1(x) \in \mathbb{F}_{q^2}[x]$, $h(x)$ as a constant function equal to 1 and $\varphi(x) = x$. Observe that $S = \{y^q + y | y \in \mathbb{F}_{q^2}\} = \mathbb{F}_q$ since char$(\mathbb{F}_q) = 2$. Then

$$h(x)\varphi(x) + g(x)^q + g(x) = x + g_0(x)^q + \theta^q g_1(x)^q + g_0(x) + \theta g_1(x).$$

If $x \in \mathbb{F}_q$, the equality implies

$$h(x)\varphi(x) + g(x)^q + g(x) = x + g_1(x).$$

Since $g_1(x)$ is a 1-permutation over $\mathbb{F}_q$, the function

$$F(x) = x + g_0(x^q + x) + \theta(g_1(x^q + x))$$

is a permutation over $\mathbb{F}_{q^2}$. □

Next, we present our results in odd characteristic. Again, we first state a special subcase in the next proposition.

Proposition 4.4. *Let* $q = p^k$*, where p is any odd prime number. Let* $\beta \in \mathbb{F}_{q^2}/\mathbb{F}_q$ *and* $\gamma = \beta^q - \beta$*. Let* $g_0(x) \in \mathbb{F}_q[x]$ *be arbitrary. Then we have :*

- *If* $q \not\equiv 1 \mod 3$, *then*
  $$F(x) = x + g_0\left(\frac{x^q}{\gamma^q} - \frac{x}{\gamma}\right) + \beta\left[\frac{x^{3q}}{\gamma^{3q}} - 3\frac{x^{2q+1}}{\gamma^{2q+1}} + 3\frac{x^{q+2}}{\gamma^{q+2}} - \frac{x^3}{\gamma^3} - \frac{x^q}{\gamma^q} + \frac{x}{\gamma}\right]$$
  is a permutation over $\mathbb{F}_{q^2}$.

- *If* $q \not\equiv 1 \mod 5$, *then*
  $$\begin{aligned} F(x) &= x + g_0\left(\frac{x^q}{\gamma^q} - \frac{x}{\gamma}\right) \\ &\quad + \beta\left[\frac{x^{5q}}{\gamma^{5q}} - 5\frac{x^{4q+1}}{\gamma^{4q+1}} + 10\frac{x^{3q+2}}{\gamma^{3q+2}} - 10\frac{x^{2q+3}}{\gamma^{2q+3}} + 5\frac{x^{q+4}}{\gamma^{q+4}} - \frac{x^5}{\gamma^5} - \frac{x^q}{\gamma^q} + \frac{x}{\gamma}\right] \end{aligned}$$
  is a permutation over $\mathbb{F}_{q^2}$.

- *If* $r \geq 1$ *is an integer such that* $\gcd(r, q-1) = 1$, *then*
  $$F(x) = x + g_0\left(\frac{x^q}{\gamma^q} - \frac{x}{\gamma}\right) + \beta\left[\left(\frac{x^q}{\gamma^q} - \frac{x}{\gamma}\right)^r - \left(\frac{x^q}{\gamma^q} - \frac{x}{\gamma}\right)\right]$$
  is a permutation over $\mathbb{F}_{q^2}$.

We do not prove Proposition 4.4 as its proof follows from the next theorem.

Theorem 4.5. *Let* $q = p^k$, *where p is any odd prime number. Let* $\beta \in \mathbb{F}_{q^2}/\mathbb{F}_q$ *and* $\gamma = \beta^q - \beta$. *Let* $g_0(x) \in \mathbb{F}_q[x]$ *be arbitrary and* $g_1(x) \in \mathbb{F}_q[x]$ *be a 1-permutation over* $\mathbb{F}_q$. *Then*
$$F(x) = x + g_0\left(\frac{x^q}{\gamma^q} - \frac{x}{\gamma}\right) + \beta g_1\left(\frac{x^q}{\gamma^q} - \frac{x}{\gamma}\right)$$
is a permutation over $\mathbb{F}_{q^2}$.

Proof. The proof comes from [1, Proposition 5.9], by taking $g(x)$ of the form $g(x) = g_0\left(\frac{x}{\gamma}\right) + \beta g_1\left(\frac{x}{\gamma}\right) \in \mathbb{F}_{q^2}[x]$, $h(x)$ as a constant function equal to 1 and $\varphi(x) = x$. Observe that $S = \{y^q - y | y \in \mathbb{F}_{q^2}\} = \gamma\mathbb{F}_q$. Now consider the map
$$\gamma y \mapsto \gamma y + g(\gamma y)^q - g(\gamma y).$$

Then
$$\begin{aligned} \gamma y + g(\gamma y)^q - g(\gamma y) &= \gamma y + g_0(y)^q + \beta^q g_1(y)^q - g_0(y) - \beta g_1(y) \\ &= \gamma y + (\beta^q - \beta) g_1(y) \\ &= \gamma[y + g_1(y)]. \end{aligned}$$

Since $g_1(y)$ is a 1-permutation over $\mathbb{F}_q$, the function

$$F(x) = x + g_0\left(\frac{x^q}{\gamma^q} - \frac{x}{\gamma}\right) + \beta g_1\left(\frac{x^q}{\gamma^q} - \frac{x}{\gamma}\right)$$

is a permutation over $\mathbb{F}_{q^2}$. □

4.2 Constructing Permutation Polynomials over $\mathbb{F}_{q^n}$ via $\mathbb{F}_q$ with $n \geq 3$

In Section 4.1, we give explicit classes of permutation polynomials over $\mathbb{F}_{q^2}$ using polynomials over $\mathbb{F}_q$.

In this section we give explicit classes of permutation polynomials over $\mathbb{F}_{q^n}$ using polynomials over $\mathbb{F}_q$ with $n \geq 3$. In fact, it is not easy to give such classes using the conditions of Akbary, Ghioca and Wang [1, Proposition 5.9] since we need to consider the subset $S = \{y^{q^n} - y | y \in \mathbb{F}_{q^n}\}$. This subset is easy to handle if $n = 2$, which we applied in Section 4.1. Hence in this section we use a different method of Akbary, Ghioca and Wang, namely [1, Proposition 5.6].

First we present our result for $n = 3$. The next proposition indicates the corresponding permutation polynomial class is large as the chosen components $g_1, g_2 \in \mathbb{F}_q[x]$ are arbitrary and $g_0 \in \mathbb{F}_q[x]$ has to satisfy a certain condition.

Proposition 4.6. *Let $\{\theta_0, \theta_1, \theta_2\}$ be a basis of $\mathbb{F}_{q^3}$ over $\mathbb{F}_q$. We assume that $Tr_3(\theta_0) \neq 0$ without loss of generality. We choose $a_0, a_1, a_2 \in \mathbb{F}_q$ satisfying*

$$(a_0 - a_2)^2 + (a_2 - a_0)(a_1 - a_2) + (a_1 - a_2)^2 \neq 0. \tag{4.1}$$

Let $g_0, g_1, g_2 \in \mathbb{F}_q[x]$ be such that $g_0(x)Tr_3(\theta_0) + g_1(x)Tr_3(\theta_1) + g_2(x)Tr_3(\theta_2)$ is an $(a_0 + a_1 + a_2)$-permutation of $\mathbb{F}_q$. Then

$$F(x) = a_0x + a_0x^q + a_2x^{q^2} + \theta_0 g_0(Tr_3(x)) + \theta_1 g_1(Tr_3(x)) + \theta_2 g_2(Tr_3(x))$$

is a permutation over $\mathbb{F}_{q^3}$.

Proof. We use [1, Proposition 5.6], by taking $g(x)$ of the form

$$g(x) = \theta_0 g_0(x) + \theta_1 g_1(x) + \theta_2 g_2(x)$$

and $h(x)$ as a constant function equal to 1. Let $\varphi(x) = a_0x + a_1x^q + a_2x^{q^2} \in \mathbb{F}_q[x]$ with a_0, a_1, a_2 satisfying (4.1). For $x \in \mathbb{F}_q$ we have

$$\begin{aligned}\varphi(x) + Tr_3(g(x)) &= a_0x + a_1x^q + a_2x^{q^2} + Tr_3(\theta_0 g_0(x) + \theta_1 g_1(x) + \theta_2 g_2(x)) \\ &= (a_0 + a_1 + a_2)x + g_0(x)Tr_3(\theta_0) + g_1(x)Tr_3(\theta_1) + g_2(x)Tr_3(\theta_2).\end{aligned}$$

Since $g_0(x)Tr_3(\theta_0) + g_1(x)Tr_3(\theta_1) + g_2(x)Tr_3(\theta_2)$ is an $(a_0 + a_1 + a_2)$-permutation of $\mathbb{F}_q$, the condition (ii) of [1, Proposition 5.6] is satisfied.

It remains to prove that $\ker\varphi \cap \ker Tr_3 = \{0\}$. As $Tr_3(x) = x + x^q + x^{q^2}$ and $\varphi(x) = a_0x + a_1x^q + a_2x^{q^2} \in \mathbb{F}_q[x]$ considering their q-associates (see, for example, [22, Definition 3.58]) it is enough to prove that

$$\gcd(1 + t + t^2, a_0 + a_1t + a_2t^2) = 1. \tag{4.2}$$

Indeed, if follows from [22, Theorem 3.62] that $\ker\varphi \cap \ker Tr_3 = \{0\}$ if and only if (4.2) holds. By a simple computation we observe that (4.1) is equivalent to the condition

$$\gcd(1 + t + t^2, a_0 + a_1t + a_2t^2) = 1.$$

□

For $n \geq 3$ in general, the condition

$$(a_0 - a_2)^2 + (a_2 - a_0)(a_1 - a_2) + (a_1 - a_2)^2 \neq 0$$

corresponds to the resultant condition, which is well-known in algebraic geometry. We recall its definition (see, for example, [22, Definition 1.93]).

Definition 4.2. *Let $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n \in \mathbb{F}_q[x]$ be a polynomial of degree n and $g(x) = b_0x^m + b_1x^{m-1} + \cdots + b_m \in \mathbb{F}_q[x]$ be a polynomial of degree m with $n, m \in \mathbb{N}^+$. Then the resultant $Res(f, g)$ of the two polynomials is defined by* *the determinant*

$$Res(f,g) = \left|\begin{array}{cccccccc} a_0 & a_1 & \dots & a_n & 0 & & \dots & 0 \\ 0 & a_0 & a_1 & \dots & a_n & 0 & \dots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & \dots & 0 & a_0 & a_1 & & \dots & a_n \\ b_0 & b_1 & \dots & & b_m & 0 & \dots & 0 \\ 0 & b_0 & b_1 & \dots & & b_m & \dots & 0 \\ \vdots & & & & & & & \vdots \\ 0 & \dots & 0 & b_0 & b_1 & & \dots & b_m \end{array}\right| \begin{array}{l} \left.\vphantom{\begin{array}{c} a \\ a \\ \vdots \\ a \end{array}}\right\} m \textit{ rows} \\ \left.\vphantom{\begin{array}{c} a \\ a \\ \vdots \\ a \end{array}}\right\} n \textit{ rows} \end{array}$$

of order $m+n$.

Now we are ready to generalize Proposition 4.6 in the next theorem.

Theorem 4.7. *Let $\{\theta_0, \theta_1, \dots, \theta_{n-1}\}$ be a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. We assume that $Tr_n(\theta_0) \neq 0$ without loss of generality. Let $\varphi(x) = a_0x + a_1x^q \cdots + a_{n-1}x^{q^{n-1}}$ be an $\mathbb{F}_q$-linear polynomial over $\mathbb{F}_q$ satisfying the resultant*

$$Res(a_0 + a_1t + \cdots + a_{n-1}t^{n-1}, 1 + t + \cdots + t^{n-1}) \neq 0. \tag{4.3}$$

Let $g_0, g_1 \dots, g_{n-1} \in \mathbb{F}_q[x]$ be such that $g_0(x)Tr_n(\theta_0) + \cdots + g_{n-1}(x)Tr_n(\theta_{n-1})$ is an $(a_0 + \cdots + a_{n-1})$-permutation of $\mathbb{F}_q$. Then

$$F(x) = \varphi(x) + \theta_0 g_0(Tr_n(x)) + \cdots + \theta_{n-1}g_{n-1}(Tr_n(x))$$

is a permutation over $\mathbb{F}_{q^n}$.

Proof. We use a similar method as in the proof of Proposition 4.6. Take $g(x)$ of the form

$$g(x) = g_0(x)Tr_n(\theta_0) + \cdots + g_{n-1}(x)Tr_n(\theta_{n-1})$$

and $h(x)$ as the constant function equal to 1. Let

$$\varphi(x) = a_0x + a_1x^q \cdots + a_{n-1}x^{q^{n-1}} \in \mathbb{F}_q[x]$$

with a_0, …, a_{n-1} satisfying (4.3). For $x \in \mathbb{F}_q$ we have

$$\varphi(x) + Tr_n(g(x)) = (a_0 + \cdots + a_{n-1})x + g_0(x)Tr_n(\theta_0) + \cdots + g_{n-1}(x)Tr_n(\theta_{n-1}).$$

This is a permutation polynomial over $\mathbb{F}_q$ since

$$g_0(x)Tr_n(\theta_0) + \cdots + g_{n-1}(x)Tr_n(\theta_{n-1})$$

is an $(a_0+\cdots+a_{n-1})$-permutation of $\mathbb{F}_q$. So condition 2 of [1, Proposition 5.6] holds.

The proof of $\ker\varphi\cap\ker Tr_n = \{0\}$ comes from an important property of the resultant [22, page 36] (see also, [21, Corollary 8.4, page 203]). It indicates that the polynomials $1 + t + \cdots + t^{n-1}$ and $a_0 + a_1 t + \cdots + a_{n-1}t^{n-1}$ do not have common root if and only if (4.3) holds. Note that we also use q-associates before this argument. $\square$

CHAPTER 5

A FURTHER GENERALIZATION OF LINEAR TRANSLATORS

For an arbitrary $\mathbb{F}_q$ and a map $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ with $n \geq 2$, the concept of linear structure in Definition 2.2 corresponds to the notion of linear structure: Let $\gamma \in \mathbb{F}_{q^n}$, $b \in \mathbb{F}_q$. Then γ is called b-linear translator of $f : \mathbb{F}_{q^n} \to \mathbb{F}_q$ if

$$f(x + \gamma u) = f(x) + bu \text{ for all } x \in \mathbb{F}_{q^n} \text{ and } y \in \mathbb{F}_q.$$

Note that if $q = 2$, then b is either 0 or 1 and we have either 0-linear translator or 1-linear translator coinciding with 0-linear structure or 1-linear structure.

Recently Cepak, Pasalic and Muratović-Ribić generalized the notion of linear translators and gave an application for constructing permutation polynomials (see [13]).

In this chapter we obtain a further and very natural generalization of the notion of linear translators. We also give two different applications of our more general version to permutation polynomials. Theorem 5.1 is an easy but rather unexpected application. It gives a class of permutation polynomials over $\mathbb{F}_{q^n}$ using a surjective map $f : \mathbb{F}_{q^n} \to S \subseteq \mathbb{F}_q$ and our notion of generalized linear translator.

The proof uses a trick that was used earlier in [24]. Moreover, this method gives the inverse permutation explicitly.

The second application is Theorem 5.2 below and it shows that under certain conditions one can get permutation polynomials on $\mathbb{F}_{q^n}$ again using $f : \mathbb{F}_{q^n} \to S \subseteq \mathbb{F}_q$ and the corresponding generalized linear translator. Finally, we give an explicit example illustrating that there exist generalized linear translators satisfying the conditions of Theorem 5.2 and not being Frobenius linear translators, which is the notion expressed in [13].

We start with our generalization of the notion.

Definition 5.1. *Let $S \subseteq \mathbb{F}_q$ and let $\gamma, b \in \mathbb{F}_{q^n}$. Let $A : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ be an additive map. We say that γ is a (b, A)-linear translator with respect to S for the mapping $f : \mathbb{F}_{q^n} \to S$, if*

$$f(x + \gamma u) = f(x) + bA(u)$$

for all $x \in \mathbb{F}_{q^n}$ and for all $u \in S$.

Now we are ready to present a first application of the notion in Definition 5.1.

Theorem 5.1. *Let $S \subseteq \mathbb{F}_{q^n}$ and $f : \mathbb{F}_{q^n} \to S$ be a surjective map. Let $\gamma \in \mathbb{F}_q$ be a (b, A)-linear translator with respect to S for the map f where A is an additive map and $\gamma, b \in \mathbb{F}_{q^n}$. Then for any $g \in \mathbb{F}_{q^n}[x]$ which maps S into S, we have that $F(x) = x + \gamma g(f(x))$ is a permutation over $\mathbb{F}_{q^n}$ if and only if $\psi(z) = z + bA(g(z))$ is a permutation on S.*

Moreover, if F is a permutation over $\mathbb{F}_{q^n}$, then its inverse function F^{-1} is given explicitly as

$$F^{-1}(z) = z - \gamma g(\psi^{-1}(f(z))).$$

Proof. Let x be any element of $\mathbb{F}_{q^n}$. Then we have $F(x) = x + \gamma g(f(x))$ by definition. By applying f to the both sides of the equality we obtain

$$\begin{aligned} f(F(x)) &= f(x + \gamma g(f(x))) \\ &= f(x) + bA(g(f(x))) \text{ since } f \text{ is } (b, A)\text{-linear translator} \\ &= \psi(f(x)) \text{ by definition of the map } \psi. \end{aligned} \tag{5.1}$$

Therefore we have $\psi(f(x)) = f(F(x))$.

Assume first that ψ is a permutation over S. Let $F(x_1) = F(x_2)$ for some x_1,$x_2 \in \mathbb{F}_{q^n}$. Then applying f to both sides of the equality we have $f(F(x_1)) = f(F(x_2))$. By using (5.1), we obtain

$$\psi(f(x_1)) = f(F(x_1)) = f(F(x_2)) = \psi(f(x_2)).$$

Since ψ is a permutation over S, we get $f(x_1) = f(x_2)$. As $F(x_1) = F(x_2)$ we also have

$$x_1 + \gamma g(f(x_1)) = x_2 + \gamma g(f(x_2)).$$

These imply that $x_1 = x_2$. Therefore F is injective and indeed F is bijective.

Conversely, assume that F is a permutation over $\mathbb{F}_{q^n}$. Let s be any element of S. Since f is a surjective map, there exists $\alpha \in \mathbb{F}_{q^n}$ satisfying $f(\alpha) = s$. Because F is permutation over $\mathbb{F}_{q^n}$, there is $x \in \mathbb{F}_{q^n}$ such that $F(x) = \alpha$. By using (5.1), we have

$$\psi(f(x)) = f(F(x)) = f(\alpha) = s.$$

Therefore ψ is surjective and in fact, ψ is bijective. Then $F(x) = x + \gamma g(f(x))$ is a permutation over $\mathbb{F}_{q^n}$ if and only if $\psi(z) = z + bA(g(z))$ is a permutation over S.

Next, we compute F^{-1} explicitly. Let $y = F(x) = x + \gamma g(f(x))$. Then we have

$$\begin{aligned} f(y) &= f(x + \gamma g(f(x))) \\ &= f(x + \gamma u), \text{ where } u = g(f(x)) \in S \\ &= f(x) + bA(u), \text{ since } \gamma \text{ is a } (b, A)\text{-linear translator} \\ &= f(x) + bA(g(f(x))), \text{ recall } u = g(f(x)) \\ &= z + bA(g(z)), \text{ where } f(x) = z \\ &= \psi(z). \end{aligned}$$

As ψ is a permutation on S we have that for each y there exists $x = y - \gamma g(\psi^{-1}(f(y)))$ satisfying $F(x) = y$. Therefore, $F(x)$ is surjective and the desired result follows. The converse of the statement is proved similarly.

Moreover, $F^{-1}(z) = z - \gamma g(\psi^{-1}(f(z)))$ since $f^{-1}(z) = x$. □

Next, we give another application of Definition 5.1.

Theorem 5.2. *Let f be a function from $\mathbb{F}_{q^n}$ onto $\mathbb{F}_q$, $\gamma \in \mathbb{F}_{q^n}^*$. Let γ be a (b, A)-linear translator of f where $b \in \mathbb{F}_q$ and $A(x) \in \mathbb{F}_{q^n}[x]$ is an additive map satisfying the following conditions:*

1. *A is $\mathbb{F}_q$-linear.*

2. *$A(\gamma) \neq 0$.*

3. *$A(\gamma a) = A(\gamma)A(a)$ for all $a \in \mathbb{F}_q$.*

4. *For any $x \in \mathbb{F}_{q^n}$: If $A(\gamma x) \in A(\gamma)\mathbb{F}_q$, then $x \in \mathbb{F}_q$.*

5. *$A|_{\mathbb{F}_q}$ is onto.*

For any map $h : \mathbb{F}_q \to \mathbb{F}_q$ consider the map

$$\begin{aligned} G : \mathbb{F}_{q^n} &\to \mathbb{F}_{q^n} \\ x &\mapsto A(x) + A(\gamma)h(f(x)). \end{aligned}$$

Then G is a permutation over $\mathbb{F}_{q^n}$ if and only if the following derived map depending on h and b

$$\begin{aligned} g : \mathbb{F}_q &\to \mathbb{F}_q \\ u &\mapsto u + bh(u) \end{aligned}$$

is a permutation over $\mathbb{F}_q$.

Proof. We use a method similar to the ones in [20] or [13]. Let $x, \alpha \in \mathbb{F}_{q^n}$ satisfy $G(x) = G(x + \gamma\alpha)$. Then

$$\begin{aligned} G(x) &= A(x) + A(\gamma)h(f(x)), \\ G(x + \gamma\alpha) &= A(x + \gamma\alpha) + A(\gamma)h(f(x + \gamma\alpha)) \\ &= A(x) + A(\gamma\alpha) + A(\gamma)h(f(x + \gamma\alpha)) \text{ by condition 1,} \end{aligned}$$

and hence

$$A(\gamma)h(f(x)) = A(\gamma\alpha) + A(\gamma)h(f(x + \gamma\alpha)). \tag{5.2}$$

Divide both sides of equation (6.1) by $A(\gamma)$, since $A(\gamma) \neq 0$ by condition 2. Then we have

$$h(f(x)) = \frac{A(\gamma\alpha)}{A(\gamma)} + h(f(x + \gamma\alpha)).$$

As $f(x), f(x+\gamma\alpha) \in \mathbb{F}_q[x]$, $h \in \mathbb{F}_q[x]$ and $\frac{A(\gamma\alpha)}{A(\gamma)} \in \mathbb{F}_q$, by condition 4 we get $\alpha \in \mathbb{F}_q$. Taking $a = \alpha \in \mathbb{F}_q$, we have

$$h(f(x)) = \frac{A(\gamma a)}{A(\gamma)} + h(f(x + \gamma a)).$$

Note that $A(\gamma a) = A(\gamma)A(a)$ by condition 3, so we get

$$h(f(x)) = A(a) + h(f(x + \gamma a))$$

and hence by using that γ is a (b, A)-linear translator for f, we get

$$h(f(x)) = A(a) + h(f(x) + bA(a)).$$

Then substituting $u = f(x) \in \mathbb{F}_q[x]$, we have

$$h(u) = A(a) + h(u + bA(a)). \tag{5.3}$$

Consider

$$\begin{aligned} g(u) &= u + bh(u) \\ g(u + bA(a)) &= u + bA(a) + b(h(u + bA(a))) \\ &= u + b\left(A(a) + h(u + bA(a)\right) \\ &= u + bh(u) \\ &= g(u). \end{aligned}$$

Here as x runs through $\mathbb{F}_{q^n}$, $u = f(x)$ runs through $\mathbb{F}_q$ as f is onto. Then we get

$$g(u) = g(u + bA(a)). \tag{5.4}$$

Thus the mapping G is a permutation over $\mathbb{F}_{q^n}$ if and only if the only a satisfying equation (5.4) is $a = 0$. If $b = 0$, then we obtain that $A(a) = 0$ as g is permutation. As $A|_{\mathbb{F}_q}$ is one-to-one, we get $a = 0$. If $b = 0$, then from equation (5.3) we have

$$h(u) = A(a) + h(u + bA(a)) = A(a) + h(u).$$

Hence $A(a) = 0$. Therefore, $a = 0$. □

The next example illustrates a simple situation when the conditions of Theorem 5.2 hold. Note that the polynomial $A(x)$ in the next example is not in the form of a Frobenius linear translator. Moreover, the next example illustrates that the conditions of Theorem 5.1 hold easily as its conditions are weaker.

Example 2. *Let $q = 2$ and $n = 4$. Take $A(x) = \alpha^2 x + \alpha^7 x^2 + \alpha^3 x^4 + \alpha^5 x^8 \in \mathbb{F}_{2^4}[x]$ where $\alpha^4 = 1 + \alpha$ and $\gamma = \alpha^3 \in \mathbb{F}_{2^4}^*$. Then $A(x)$ satisfies the following conditions:*

1. *A is $\mathbb{F}_2$-linear since A is additive.*

2. *$A(\gamma) \neq 0$ since $A(\gamma) = A(\alpha^3) = \alpha^4 \neq 0$.*

3. *$A(\gamma a) = A(\gamma)A(a)$ for all $a \in \mathbb{F}_2$ since*

$$A(a) = \alpha^2 a + \alpha^7 a^2 + \alpha^3 a^4 + \alpha^5 a^8 = a(\alpha^2 + \alpha^7 + \alpha^3 + \alpha^5) = a$$

and

$$A(\gamma a) = \alpha^2(\alpha^3 a) + \alpha^7(\alpha^3 a)^2 + \alpha^3(\alpha^3 a)^4 + \alpha^5(\alpha^3 a)^8 = aA(\gamma) = A(a)A(\gamma).$$

4. *For any $x \in \mathbb{F}_{q^n}$: If $A(\gamma x) \in A(\gamma)\mathbb{F}_q$, then $x \in \mathbb{F}_q$. Consider $\theta = \alpha^i \in \mathbb{F}_{2^4}/\mathbb{F}_2$ for $1 \leq i \leq 14$, then we have*

$$A(\gamma\theta) = A(\gamma\alpha^i) \notin A(\gamma)\mathbb{F}_2 \text{ where } A(\gamma) = \alpha^4 \text{ for } 1 \leq i \leq 14.$$

Indeed, we have $\{A(\gamma\alpha^i) : 1 \leq i \leq 14\} = \mathbb{F}_{16} \setminus \{0, \alpha^4\}$. For example, $A(\gamma\alpha) = \alpha^8$ and $A(\gamma\alpha^{11}) = \alpha$.

5. *$A|_{\mathbb{F}_2}$ is onto.*

Let $f : \mathbb{F}_{2^4} \to \mathbb{F}_2$ be the map $x \mapsto Tr_4(x)$. Then α^3 is a $(1, A)$-linear translator of f since we have

$$\begin{aligned} f(x + \gamma u) = f(x + \alpha^3 u) &= Tr_4(x + \alpha^3 u) = Tr_4(x) + uTr_4(\alpha^3) \\ &= Tr_4(x) + u = f(x) + u \end{aligned}$$

for all $x \in \mathbb{F}_{2^4}$ and for all $u \in \mathbb{F}_2$.

CHAPTER 6

THE C-DIFFERENTIAL UNIFORMITY OF THE PERTURBED INVERSE FUNCTION

Consider the perturbed inverse function $H(x)$ via a trace function $Tr\left(\frac{x^2}{x+1}\right)$. In [19], Hasan et. al give an upper bound of the c-differential uniformity of H and they leave an open question whether the upper bound is attained. By using Theorem 6.1, Remark 3, Remark 4 and Example 3 below, we determine the exact c-differential uniformity of H in the case $Tr(c) = 1 = Tr(1/c)$ for $c \in \mathbb{F}_{2^n} \backslash \{0, 1\}$. In particular, in Theorem 6.1 below, the upper bound 8 for the exact c-differential uniformity is attained in the case $Tr(c) = 1 = Tr(1/c)$. In the remaining case, we show that the c-differential uniformity of $H(x)$ is either 8 or 9 for $n \geq 11$.

Theorem 6.1. *Let us consider $c \in \mathbb{F}_{2^n} \backslash \{0, 1\}$ and the function $H(x) = \frac{1}{x} + Tr\left(\frac{x^2}{x+1}\right)$ over $\mathbb{F}_{2^n}$ where $n \geq 11$. Then the following statements hold:*

1. *If $Tr(c) = 1 = Tr(1/c)$, then ${}_c\Delta_H = 8$.*
2. *Otherwise, $8 \leq_c \Delta_H \leq 9$.*

Proof. The c-differential uniformity of H is

$$\max\{{}_c\Delta_H : a, b \in \mathbb{F}_{2^n}, \text{ and } a \neq 0 \text{ if } c = 1\},$$

where the c-Difference Distribution entries ${}_c\Delta_H = \{x \in \mathbb{F}_{2^n} : H(x + a) + cH(x) = b\}$. Our aim is to find the exact number of solutions in x to the equation

$$\frac{1}{x+a} + Tr\left(\frac{(x+a)^2}{x+a+1}\right) + c\frac{1}{x} + cTr\left(\frac{x^2}{x+1}\right) = b, \tag{6.1}$$

for any a,$b \in \mathbb{F}_{2^n}$ and $c \in \mathbb{F}_{2^n} \backslash \{0,1\}$.
If $a = 0$, then Equation (6.1) turns into $\frac{1}{x} + Tr\left(\frac{x^2}{x+1}\right) + c\frac{1}{x} + cTr\left(\frac{x^2}{x+1}\right) = b$. It gives us exactly one solution for any $b \in \mathbb{F}_{2^n}$. Let us assume that $a \neq 0$. We divide the problem into 4 cases according to the prescribed values of the trace function.

Case 1. Assume that $Tr\left(\frac{(x+a)^2}{x+a+1}\right) = 0 = Tr\left(\frac{x^2}{x+1}\right)$ holds. So we have $bx^2 + (ab + c + 1)x + ac = 0$. When $b = 0$, the solution is $x = \frac{ac}{c+1}$. Consider $b \neq 0$, we have $x^2 + \frac{ab+c+1}{b}x + \frac{ac}{b} = 0$. Put $x_1 := \frac{ab+c+1}{b}x$. Now consider the curves:

$$\begin{aligned} E_{1,1} &: y_{1,1}^2 + y_{1,1} = \frac{x^2 + a^2}{x + a + 1} \\ E_{1,2} &: y_{1,2}^2 + y_{1,2} = \frac{x^2}{x + 1} \\ E_1 &: x_1^2 + x_1 = \frac{acb}{a^2b^2 + c^2 + 1}. \end{aligned}$$

Case 2. Assume that $Tr\left(\frac{(x+a)^2}{x+a+1}\right) = 1$ and $Tr\left(\frac{x^2}{x+1}\right) = 0$ hold. Then Equation (6.1) turns into $(b + 1)x^2 + (ab + a + c + 1)x + ac = 0$. When $b + 1 = 0$, the solution is $x = \frac{ac}{c+1}$. Consider $b + 1 \neq 0$, we have $x^2 + \frac{ab+a+c+1}{b+1}x + \frac{ac}{b+1} = 0$. Put $x_2 := \frac{ab+a+c+1}{b+1}x$. Now consider the curves:

$$\begin{aligned} E_{2,1} &: y_{2,1}^2 + y_{2,1} = \frac{x^2 + a^2}{x + a + 1} + 1 \\ E_{2,2} &: y_{2,2}^2 + y_{2,2} = \frac{x^2}{x + 1} \\ E_2 &: x_2^2 + x_2 = \frac{ac(b + 1)}{a^2b^2 + a^2 + c^2 + 1}. \end{aligned}$$

Case 3. Assume that $Tr\left(\frac{(x+a)^2}{x+a+1}\right) = 0$ and $Tr\left(\frac{x^2}{x+1}\right) = 1$ hold. Then Equation (6.1) becomes $(b + c)x^2 + (ab + ac + c + 1)x + ac = 0$. When $b + c = 0$, the solution is $x = \frac{ac}{c+1}$. Consider $b + c \neq 0$, we have $x^2 + \frac{ab+ac+c+1}{b+c}x + \frac{ac}{b+c} = 0$. Put $x_3 := \frac{ab+ac+c+1}{b+c}x$. Now consider the curves:

$$\begin{aligned} E_{3,1} &: y_{3,1}^2 + y_{3,1} = \frac{x^2 + a^2}{x + a + 1} \\ E_{3,2} &: y_{3,2}^2 + y_{3,2} = \frac{x^2}{x + 1} + 1 \\ E_3 &: x_3^2 + x_3 = \frac{ac(b + c)}{a^2b^2 + a^2c^2 + c^2 + 1}. \end{aligned}$$

Case 4. Assume that $Tr\left(\frac{(x+a)^2}{x+a+1}\right) = 1 = Tr\left(\frac{x^2}{x+1}\right)$. Then we have the following equation $(b+c+1)x^2+(ab+ac+a+c+1)x+ac=0$. When $b+c+1=0$, the solution is $x=\frac{ac}{c+1}$. Consider $b+c+1\neq 0$, we have $x^2+\frac{ab+ac+a+c+1}{b+c+1}x+\frac{ac}{b+c+1}=0$. Put $x_4 := \frac{ab+ac+a+c+1}{b+c+1}x$. Now consider the curves:

$$\begin{aligned}
E_{4,1} &: y_{4,1}^2+y_{4,1} = \frac{x^2+a^2}{x+a+1}+1\\
E_{4,2} &: y_{4,2}^2+y_{4,2} = \frac{x^2}{x+1}+1\\
E_4 &: x_4^2+x_4 = \frac{ac(b+c+1)}{a^2b^2+a^2c^2+a^2+c^2+1}.
\end{aligned}$$

The poles s_i of E_i in the variable b for $1\leq i\leq 4$ are as follows:

$$\begin{aligned}
s_1 &= \frac{c+1}{a} \text{ with multiplicity 2,}\\
s_2 &= \frac{a+c+1}{a} \text{ with multiplicity 2,}\\
s_3 &= \frac{ac+c+1}{a} \text{ with multiplicity 2,}\\
s_4 &= \frac{ac+a+c+1}{a} \text{ with multiplicity 2.}
\end{aligned}$$

One can easily observe that we have different poles since the below cases:

$$\begin{aligned}
&s_1\neq s_2,\\
&s_3\neq s_4,\\
&s_1 = s_3 \text{ if and only if } ac=0,\\
&s_1 = s_4 \text{ if and only if } a(c+1)=0,\\
&s_2 = s_3 \text{ if and only if } a(c+1)=0,\\
&s_2 = s_4 \text{ if and only if } ac=0
\end{aligned}$$

are satisfied. Since we have different poles for each curve E_i for $1\leq i\leq 4$, we can see that they have different function fields by using Theorem 3.4.13, Theorem 3.5.10 and Proposition 3.7.8 in [31]. Now we need to show that each $E_{i,1}$ and $E_{i,2}$ over E_i for $1\leq i\leq 4$ are similarly split over an algebraic closure $\overline{\mathbb{F}}_2$ of $\mathbb{F}_{2^n}$. By substituting each x_i to $E_{i,1}$ and $E_{i,2}$ for $1 \leq i \leq 4$, we get

$$\begin{aligned}
E_{1,1} : y_{1,1}^2 + y_{1,1} &= \frac{x^2+a^2}{x+a+1} = \frac{\frac{x_1^2b^2}{a^2b^2+c^2+1}+a^2}{\frac{x_1b}{ab+c+1}+a+1} \\
&= \frac{x_1^2b^2+a^4b^2+a^2c^2+a^2}{(x_1b+a^2b+ac+a+ab+c+1)(ab+c+1)}, \\
E_{1,2} : y_{1,2}^2 + y_{1,2} &= \frac{x^2}{x+1} = \frac{\frac{x_1^2b^2}{a^2b^2+c^2+1}}{\frac{x_1b}{ab+c+1}+1} = \frac{x_1^2b^2}{(x_1b+ab+c+1)(ab+c+1)}, \\
E_{2,1} : y_{2,1}^2 + y_{2,1} &= \frac{x^2+a^2}{x+a+1}+1 = \frac{\frac{x_2^2(b^2+1)}{a^2b^2+a^2+c^2+1}+a^2}{\frac{x_2(b+1)}{ab+a+c+1}+a+1}+1 \\
&= \frac{x_2^2b^2+x_2^2+a^4b^2+a^4+a^2c^2+a^2}{(x_2b+x_2+a^2b+a^2+ac+ab+c+1)(ab+a+c+1)}+1, \\
E_{2,2} : y_{2,2}^2 + y_{2,2} &= \frac{x^2}{x+1} \\
&= \frac{\frac{x_2^2(b^2+1)}{a^2b^2+a^2+c^2+1}}{\frac{x_2(b+1)}{ab+a+c+1}+1} = \frac{x_2^2b^2+x_2^2}{(x_2b+x_2+ab+a+c+1)(ab+a+c+1)}, \\
E_{3,1} : y_{3,1}^2 + y_{3,1} &= \frac{x^2+a^2}{x+a+1} = \frac{\frac{x_3^2(b^2+c^2)}{a^2b^2+a^2c^2+c^2+1}+a^2}{\frac{x_3(b+c)}{ab+ac+c+1}+a+1} \\
&= \frac{x_3^2b^2+x_3^2c^2+a^4b^2+a^4c^2+a^2c^2+a^2}{(x_3b+x_3c+a^2b+a^2c+a+ab+c+1)(ab+ac+c+1)}, \\
E_{3,2} : y_{3,2}^2 + y_{3,2} &= \frac{x^2}{x+1}+1 = \frac{\frac{x_3^2(b^2+c^2)}{a^2b^2+a^2c^2+c^2+1}}{\frac{x_3(b+c)}{ab+ac+c+1}+1}+1 \\
&= \frac{x_3^2b^2+x_3^2c^2}{(x_3b+x_3c+ab+ac+c+1)(ab+ac+c+1)}+1, \\
E_{4,1} : y_{4,1}^2 + y_{4,1} &= \frac{x^2+a^2}{x+a+1}+1 = \frac{\frac{x_4^2(b^2+c^2+1)}{a^2b^2+a^2c^2+a^2+c^2+1}+a^2}{\frac{x_4(b+c+1)}{ab+ac+a+c+1}+a+1}+1 \\
&= \frac{x_4^2b^2+x_4^2c^2+x_4^2+a^4b^2+a^4c^2+a^4+a^2c^2+a^2}{(x_4b+x_4c+x_4+a^2b+a^2c+a^2+ab+c+1)(ab+ac+a+c+1)}+1, \\
E_{4,2} : y_{4,2}^2 + y_{4,2} &= \frac{x^2}{x+1}+1 = \frac{\frac{x_4^2(b^2+c^2+1)}{a^2b^2+a^2c^2+a^2+c^2+1}}{\frac{x_4(b+c+1)}{ab+ac+a+c+1}+1}+1 \\
&= \frac{x_4^2b^2+x_4^2c^2+x_4^2}{(x_4b+x_4c+x_4+ab+ac+a+c+1)(ab+ac+a+c+1)}+1.
\end{aligned}$$

The poles $t_{i,j}$ of $E_{i,j}$ for $1 \leq i \leq 4$ and $1 \leq j \leq 2$ are of the form:

$$\begin{aligned}
t_{1,1} &= \frac{a^2b+ac+a+ab+c+1}{b} && \text{with multiplicity } 1, \\
t_{1,2} &= \frac{ab+c+1}{b} && \text{with multiplicity } 1,
\end{aligned}$$

$$
\begin{aligned}
t_{2,1} &= \frac{a^2b + a^2 + ac + ab + c + 1}{b+1} && \text{with multiplicity } 1,\\
t_{2,2} &= \frac{ab + a + c + 1}{b+1} && \text{with multiplicity } 1,\\
t_{3,1} &= \frac{a^2b + a^2c + a + ab + c + 1}{b+c} && \text{with multiplicity } 1,\\
t_{3,2} &= \frac{ab + ac + c + 1}{b+c} && \text{with multiplicity } 1,\\
t_{4,1} &= \frac{a^2b + a^2c + a^2 + ab + c + 1}{b+c+1} && \text{with multiplicity } 1,\\
t_{4,2} &= \frac{ab + ac + a + c + 1}{b+c+1} && \text{with multiplicity } 1.
\end{aligned}
$$

Recall that $\overline{\mathbb{F}}_2$ is a fixed algebraic closure of $\mathbb{F}_2$. Let $\overline{E}_{1,1}/\overline{\mathbb{F}}_2$ be the constant field extension of $E_{1,1}/\mathbb{F}_2$. Let $T_1 \subseteq \overline{\mathbb{F}}_2$ be the set consisting of $\alpha \in T_1$ such that there exists a place P_1 of $\overline{E}_{1,1}$ corresponds to a pole of $y_{1,1}$. Let $P_1(b) = \prod_{\alpha \in T_1}(b-\alpha)$. The arguments above imply that $\alpha \in T_1$ if and only if $P_1(\alpha) = 0$, where $P_1(b)$ satisfies

$$P_1(b) := (a+1)(ab+c+1)^3[(a+1)(ab+c+1)+b] + acb^3.$$

Similarly for $E_{1,2}$, we define

$$P_2(b) := (ab+c+1)^3(ab+c+1+b) + acb^3.$$

For $E_{2,1}$, we define

$$P_3(b) := (a+1)(a(b+1)+c+1)^2[(a+1)(ab+a+c+1)+b+1] + ac(b+1)^3.$$

For $E_{2,2}$, we define

$$P_4(b) := (a(b+1)+c+1)^3(a(b+1)+c+1+(b+1)) + ac(b+1)^3.$$

For $E_{3,1}$, we define

$$P_5(b) := (a+1)(a(b+c)+c+1)^3[(a+1)(a(b+c)+c+1)+(b+c)] + ac(b+c)^3.$$

For $E_{3,2}$, we define

$$P_6(b) := (a(b+c)+c+1)^3(a(b+c)+c+1+(b+c)) + ac(b+c)^3.$$

For $E_{4,1}$, we define

$$P_7(b) := (a+1)(a(b+c+1)+c+1)^3[(a+1)(a(b+c+1)+c+1)+(b+c+1)]+ac(b+c+1)^3.$$

For $E_{4,2}$, we define

$$P_8(b) := (a(b+c+1)+c+1)^3(a(b+c+1)+c+1+(b+c+1))+ac(b+c+1)^3.$$

One can observe that there is a relation as follows:

$$\begin{aligned} P_7(b) &= P_5(b+1) = P_3(b+c) = P_1(b+c+1) \\ P_8(b) &= P_6(b+1) = P_4(b+c) = P_2(b+c+1). \end{aligned}$$

We want to show that each P_i for $1 \leq i \leq 8$

$$P_i \not| \prod_{\substack{1 \leq j \leq 8 \\ j \neq i}} P_j. \tag{6.2}$$

When we show the Equation (6.2) is satisfied, then we can conclude that each curve $E_{i,j}$ for $1 \leq i \leq 4$ and $1 \leq j \leq 2$ is irreducible. Moreover, it gives us that there are at least 8 solutions of the system (6.1). So each curve $E_{i,1}$ and $E_{i,2}$ have different function fields by Theorem 3.4.13, Theorem 3.5.10 and Proposition 3.7.8 in [31]. We need to check the ideals whether $< P_i(b), P_j(b) >= 1$ for $1 \leq i, j \leq 8$ and $i \neq j$.

Consider

$$\begin{aligned} P_1(b) &:= A_4b^4 + A_3b^3 + A_2b^2 + A_1b + A_0, \\ P_2(b) &:= B_4b^4 + B_3b^3 + B_2b^2 + B_1b + B_0. \end{aligned}$$

Since $B_4 \neq 0$, we can define

$$C_3 := \frac{B_3}{B_4}, C_2 := \frac{B_2}{B_4}, C_1 := \frac{B_1}{B_4} \text{ and } C_0 := \frac{B_0}{B_4}.$$

Then we obtain

$$\begin{aligned} < P_1(b), P_2(b) > &=< P_1(b), b^4 + C_3b^3 + C_2b^2 + C_1b + C_0 > \\ &=< P_1, (A_3 + A_4C_3)b^3 + (A_2 + A_4C_2)b^2 + (A_1 + A_4C_1)b \\ &+ (A_0 + A_4C_0) > . \end{aligned}$$

Assume that $A_3 + A_4C_3 \neq 0$. Then let us denote

$$D_2 := \frac{A_2 + A_4C_2}{A_3 + A_4C_3}, D_1 := \frac{A_1 + A_4C_1}{A_3 + A_4C_3} \text{ and } D_0 := \frac{A_0 + A_4C_0}{A_3 + A_4C_3}.$$

So we have

$$\begin{aligned} < P_1(b), P_2(b) > &=< P_1, b^3 + D_2b^2 + D_1b + D_0 > \\ &=< (A_3 + A_4D_2)b^3 + (A_2 + A_4D_1)b^2 + (A_1 + A_4D_0)b + A_0, \\ & b^3 + D_2b^2 + D_1b + D_0 > . \end{aligned}$$

Assume that $A_3 + A_4D_2 \neq 0$. Then let us denote

$$E_2 := \frac{A_2 + A_4D_1}{A_3 + A_4D_2}, E_1 := \frac{A_1 + A_4D_0}{A_3 + A_4D_2} \text{ and } E_0 := \frac{A_0}{A_3 + A_4D_2}.$$

So we have

$$\begin{aligned} & < P_1(b), P_2(b) >= \\ & < (E_2 + D_2)b^2 + (E_1 + D_1)b + (E_0 + D_0), b^3 + D_2b^2 + D_1b + D_0 > . \end{aligned}$$

Assume $E_2 + D_2 \neq 0$. Then let us denote

$$F_1 := \frac{E_1 + D_1}{E_2 + D_2} \text{ and } F_0 := \frac{E_0 + D_0}{E_2 + D_2}.$$

So we have

$$\begin{aligned} < P_1(b), P_2(b) > &=< b^2 + F_1b + F_0, b^3 + D_2b^2 + D_1b + D_0 > \\ &=< b^2 + F_1b + F_0, (D_2 + F_1)b^2 + (F_0 + D_1)b + D_0 > . \end{aligned}$$

Assume $D_2 + F_1 \neq 0$. Then let us denote

$$G_1 := \frac{F_0 + D_1}{D_2 + F_1} \text{ and } G_0 := \frac{D_0}{D_2 + F_1}.$$

So we have

$$< P_1(b), P_2(b) >=< (F_1 + G_1)b + (F_0 + G_0), b^2 + G_1b + G_0 > .$$

Assume $F_1 + G_1 \neq 0$. Then let us denote

$$H_0 := \frac{F_0 + G_0}{F_1 + G_1} \text{ and } K_0 := \frac{G_0}{H_0 + G_1}.$$

So we have

$$< P_1(b), P_2(b) >=< b + H_0, b + K_0 > .$$

Assume $H_0 \neq K_0$. Then we obtain

$$< P_1(b), P_2(b) >= 1.$$

Here in order to show $< P_1(b), P_2(b) >= 1$ we need to exclude the values of a satisfying the following equalities :

$$\begin{aligned}
&B_4 = 0,\\
&A_3 + A_4C_3 = 0,\\
&A_3 + A_4D_2 = 0,\\
&E_2 + D_2 = 0,\\
&D_2 + F_1 = 0,\\
&F_1 + G_1 = 0,\\
&H_0 = K_0.
\end{aligned} \tag{6.3}$$

Observe that

$$\begin{aligned}
A_4 &= (a+1)a^3(a^2+a+1), & B_4 &= a^3(a+1),\\
A_3 &= (a+1)a^2(c+1)+ac & B_3 &= a^2(c+1)+ac,\\
A_2 &= (a+1)a(c+1)^2, & B_2 &= a(c+1)^2,\\
A_1 &= (a+1)(c+1)^3, & B_1 &= (c+1)^3,\\
A_0 &= (a+1)^2(c+1)^4, & B_0 &= (c+1)^4.
\end{aligned} \tag{6.4}$$

Our goal is to find the number of values of a such that the given Equations in (6.3) are satisfied. Here the degree of the polynomials will give the upper bound, which we look for that is 77.

Now let consider the ideal $< P_1(b), P_1(b+1) >$. The following cases must be satsfied:

$$\begin{aligned}
&A_3 \neq 0,\\
&A_4 + A_3 \neq 0,\\
&C_2 + 1 \neq 0 \quad \text{where} \quad C_2 = \frac{K_0A_4 + A_2}{A_4 + A_3}, \quad K_0 = \frac{A_4 + A_3 + A_2 + A_1}{A_3},\\
&D_1 + 1 \neq 0 \quad \text{where} \quad D_1 = \frac{C_1 + K_0}{C_2 + 1}, \quad C_1 = \frac{A_1}{A_4 + A_3},\\
&E_0 + 1 \neq 0 \quad \text{where} \quad E_0 = \frac{D_0 + K_0}{D_1 + 1}, \quad D_0 = \frac{C_0}{C_2 + 1}, \quad C_0 = \frac{A_0}{A_4 + A_3}\\
&E_0 \neq F_0 \quad \text{where} \quad F_0 = \frac{K_0}{E_0 + 1}.
\end{aligned} \tag{6.5}$$

The maximum number of a's that must be excluded for the above inequalities (6.5) equals 39. When one can do the same calculation for each $< P_i(b), P_j(b) >$ for $1 \leq i, j \leq 8$ and $i \neq j$, then the total number of such a's is less than $2048 = 2^{11}$. If you eliminate such values of a, the system is irreducible and gives us a full split. So we can conclude that if we work on the field of order 2^{11}, then by Theorem 3.4.13, Theorem 3.5.10 and Proposition 3.7.8 in [31] we have a full split in the algebraic closure $\bar{\mathbb{F}}_{2^{11}}$. Here is the diagram we have:

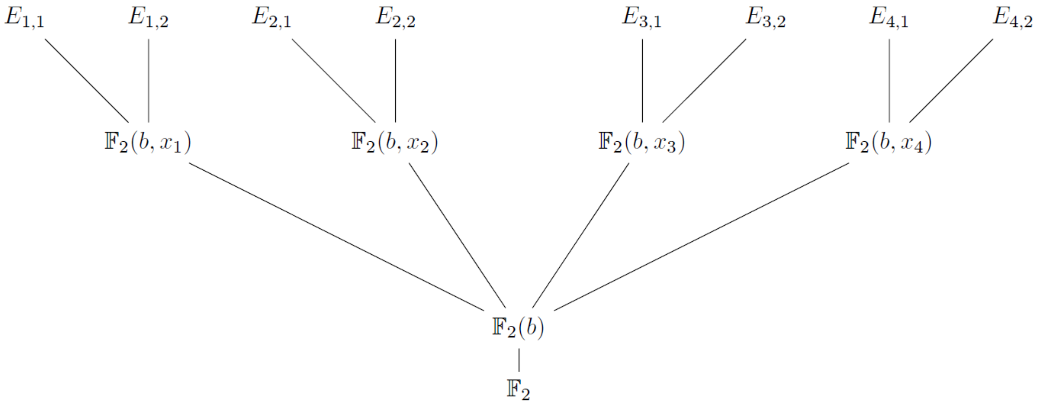

Figure 6.1: The Hasse diagram over $\mathbb{F}_2(b)$

Therefore we can deduce that the number of solutions of the system is greater than or equal to 8. By using Theorem 9 in [19], we get the following result:

1. If $Tr(c) = 1 = Tr(1/c)$, then ${}_c\Delta_H = 8$;

2. Otherwise, $8 \leq_c \Delta_H \leq 9$.

□

Remark 3. *In* ([19, TABLE I])*, up to $n = 8$, Hasan et al. gives the c-differential uniformity of the function $H(x)$ for $c \in \mathbb{F}_{2^n} \setminus \{0, 1\}$ when $Tr(c) = 1 = Tr(\frac{1}{c})$. In our Table 6.1, we update their table and the only difference is for $n = 3$. Note that there are no such $c \in \mathbb{F}_{2^n} \setminus \{0, 1\}$ satisfying $Tr(c) = 1 = Tr(\frac{1}{c})$. Therefore we express the c-differential uniformity of $H(x)$ for $n = 3$ as 0 in Table 6.1.*

Remark 4. *For $n = 9$, we implemented the algorithm for the c-differential uniformity of the function $H(x)$ in MAGMA software. The algorithm ran in parallel for about*

Table 6.1: The c-differential uniformity of H over $\mathbb{F}_{2^n}$

n	when $Tr(c) = 1 = Tr(\frac{1}{c})$
2	1
3	0
4	4
5	6
6	6
7	6
8	7
9	7
10	8

3 days on Magma software. We get the exact c-differential uniformity of the function $H(x)$ *which is* 7.

Example 3. *For* $n = 10$, $a = w^{216}$, $b = w^{699}$, $c = w^{1004}$ *where* w *is the generator of* $\mathbb{F}_{2^n}^*$ *satisfying* $w^{10} + w^6 + w^5 + w^3 + w^2 + w + 1 = 0$, *one can easily find that the* w^{1004}*-differential uniformity of* H *is* 8 *in the case* $Tr(c) = 1 = Tr(\frac{1}{c})$. *Moreover, by using Theorem 9 in [19] we can conclude that the c-differential uniformity of* H *is 8.*

CHAPTER 7

CONCLUSION

In this thesis, we define a new class of Boolean functions which includes Cusick's class of functions [15] as a small subclass. We obtain explicit permutation polynomial classes over $\mathbb{F}_{q^2}$ via $\mathbb{F}_q$ and also over $\mathbb{F}_{q^n}$ via $\mathbb{F}_q$ with $n \geq 3$. We give a natural generalization of the notion of linear translators, which is called (b,A)-linear translator. By using the connection between linear translators and permutation polynomials over finite fields, we obtain a class of permutation polynomials over $\mathbb{F}_{q^n}$. For applications, our class of Boolean functions would be preferable compared to Cusick's class of functions mentioned above as our class is much larger, having cryptographic properties as good as (or even better than) the class of Cusick's functions. Using our methods and a new notion of (b,A)-linear translator, it would be possible to construct further interesting algebraic structures like permutation polynomials or special functions. In 2009, Edel and Pott in [16] showed that the perturbation method can construct new APN classes. This suggests studying the perturbation of some cryptographically interesting functions, such as the study stated in [19] for the perturbed inverse function via trace function. There is an open question presented in [19] to obtain the c-differential uniformity of the perturbed inverse function via trace function. We find the exact value of the c-differential uniformity of the function $H(x)$ in the case $Tr(c) = 1 = Tr(\frac{1}{c})$. Moreover, we give a lower bound of the c-differential uniformity of the function for $n \geq 11$. Therefore we provide an almost complete solution to the given open problem in *([19, Remark 10])*. Using our method, it can be possible to get information about the c-Difference Distribution Table and the c-differential uniformity of functions. We remarked that our method gives new uses of algebraic curves over finite fields, which are not in the literature.

REFERENCES

[1] A. Akbary, D. Ghioca, and Q. Wang, On constructing permutations of finite fields, Finite Fields and Their Applications, 17(1), pp. 51–67, 2011, ISSN 1071-5797.

[2] E. Biham and A. Shamir, Differential cryptanalysis of DES-like cryptosystems, Journal of Cryptology, 4(1), pp. 3–72, jan 1991.

[3] N. Borisov, M. Chew, R. Johnson, and D. Wagner, Multiplicative differentials, in *Fast Software Encryption*, pp. 17–33, Springer Berlin Heidelberg, 2002.

[4] S. Boztaş, F. Özbudak, and E. Tekin, Explicit full correlation distribution of sequence families using plateaued functions, IEEE Transactions on Information Theory, 64(4), pp. 2858–2875, 2018.

[5] C. Bracken and G. Leander, A highly nonlinear differentially 4 uniform power mapping that permutes fields of even degree, Finite Fields and Their Applications, 16(4), pp. 231–242, jul 2010.

[6] L. Budaghyan and A. Pott, On differential uniformity and nonlinearity of functions, Discrete Mathematics, 309(2), pp. 371–384, jan 2009.

[7] C. Carlet, Boolean functions for cryptography and error-correcting codes, in *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, pp. 257–397, Cambridge University Press, jun 2010.

[8] C. Carlet, On known and new differentially uniform functions, in *Information Security and Privacy*, pp. 1–15, Springer Berlin Heidelberg, 2011.

[9] C. Carlet, Boolean and vectorial plateaued functions and apn functions, IEEE Transactions on Information Theory, 61(11), pp. 6272–6289, 2015.

[10] C. Carlet, On the properties of vectorial functions with plateaued components and their consequences on APN functions, in *Lecture Notes in Computer Science*, pp. 63–73, Springer International Publishing, 2015.

[11] C. Carlet, S. Mesnager, F. Özbudak, and A. Sınak, Explicit characterizations for plateaued-ness of p-ary (vectorial) functions, in S. El Hajji, A. Nitaj, and E. M. Souidi, editors, *Codes, Cryptology and Information Security*, pp. 328–345, Springer International Publishing, Cham, 2017, ISBN 978-3-319-55589-8.

[12] N. Cepak, P. Charpin, and E. Pasalic, Permutations via linear translators, Finite Fields and Their Applications, 45, pp. 19–42, 2017, ISSN 1071-5797.

[13] N. Cepak, E. Pasalic, and A. Muratović-Ribić, Frobenius linear translators giving rise to new infinite classes of permutations and bent functions, 2018.

[14] T. Cusick and P. Stănică, *Cryptographic Boolean Functions and Applications*, Elsevier, 2017.

[15] T. W. Cusick, Highly nonlinear plateaued functions, IET Information Security, 11(2), pp. 78–81, 2017.

[16] Y. Edel and A. Pott, A new almost perfect nonlinear function which is not quadratic, Cryptology ePrint Archive, Paper 2008/313, 2008, `https://eprint.iacr.org/2008/313`.

[17] P. Ellingsen, P. Felke, C. Riera, P. Stănică, and A. Tkachenko, C-differentials, multiplicative uniformity, and (almost) perfect c-nonlinearity, IEEE Transactions on Information Theory, 66(9), pp. 5781–5789, 2020.

[18] S. U. Hasan, M. Pal, C. Riera, and P. Stănică, On the c-differential uniformity of certain maps over finite fields, Designs, Codes and Cryptography, 89(2), pp. 221–239, nov 2020.

[19] S. U. Hasan, M. Pal, and P. Stănică, The c-differential uniformity and boomerang uniformity of two classes of permutation polynomials, IEEE Transactions on Information Theory, 68(1), pp. 679–691, jan 2022.

[20] G. Kyureghyan, Constructing permutations of finite fields via linear translators, Journal of Combinatorial Theory, Series A, 118, pp. 1052–1061, 04 2011.

[21] S. Lang, *Algebra*, Springer New York, 2002.

[22] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, Cambridge University Press, 2 edition, 1996.

[23] S. Mesnager, *Bent Functions*, Springer International Publishing, 2016.

[24] S. Mesnager, P. Ongan, and F. Özbudak, New bent functions from permutations and linear translators, in *Codes, Cryptology and Information Security*, pp. 282–297, Springer International Publishing, 2017.

[25] S. Mesnager and F. Özbudak, Boomerang uniformity of power permutations and algebraic curves over $\mathbb{F}_2^n$, Advances in Geometry, 23(1), pp. 107–134, 2023.

[26] S. Mesnager, F. Özbudak, and A. Sinak, Linear codes from weakly regular plateaued functions and their secret sharing schemes, Designs, Codes and Cryptography, 87, 2019.

[27] K. Nyberg, Differentially uniform mappings for cryptography, in *Advances in Cryptology EUROCRYPT '93*, pp. 55–64, Springer Berlin Heidelberg, 1994.

[28] C. Riera, P. Solé, and P. Stănică, A complete characterization of plateaued boolean functions in terms of their cayley graphs, in *Progress in Cryptology AFRICACRYPT 2018*, pp. 3–10, Springer International Publishing, 2018.

[29] P. Stănică and A. Geary, The c-differential behavior of the inverse function under the EA-equivalence, Cryptography and Communications, 13(2), pp. 295–306, jan 2021.

[30] P. Stănică, C. Riera, and A. Tkachenko, Characters, weil sums and c-differential uniformity with an application to the perturbed gold function, Cryptography and Communications, 13(6), pp. 891–907, apr 2021.

[31] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer Berlin Heidelberg, 2009.

[32] C. Tang, N. Li, Y. Qi, Z. Zhou, and T. Helleseth, Linear codes with two or three weights from weakly regular bent functions, IEEE Transactions on Information Theory, 62(3), pp. 1166–1176, 2016.

[33] N. Tokareva, *Bent Functions: Results and Applications to Cryptography*, Academic Press, Boston, 2015, ISBN 978-0-12-802318-1.

[34] H. Yan, On (-1)-differential uniformity of ternary APN power functions, Cryptography and Communications, 14(2), pp. 357–369, aug 2021.

[35] Z. Zha and L. Hu, Some classes of power functions with low c-differential uniformity over finite fields, Designs, Codes and Cryptography, 89(6), pp. 1193–1210, apr 2021.

[36] Y. Zheng and X.-M. Zhang, Plateaued functions, in *Information and Communication Security*, pp. 284–300, Springer Berlin Heidelberg, 1999.

CURRICULUM VITAE

PERSONAL INFORMATION

Surname, Name: Kaytancı, Kübra

EDUCATION

Degree	Institution	Year of Graduation
M.S.	Boğaziçi University, Department of Mathematics	2017
B.S.	Boğaziçi University, Department of Mathematics	2015

PROFESSIONAL EXPERIENCE

Year	Place	Enrollment
2015-2017	Boğaziçi University, Department of Mathematics	Teaching Assistant
2020-	METU, Institute of Applied Mathematics	Research Assistant

PUBLICATIONS

International Conference Publications

- S. Mesnager, K. Kaytancı, F. Özbudak, On Plateaued Functions, Linear Structures and Permutation Polynomials, in *Codes, Cryptology and Information Security. C2SI 2019. Lecture Notes in Computer Science()*, 11445. Springer (2019).

International Journal Publications

- K. Kaytancı, F. Özbudak, The c-Differential Uniformity of the Perturbed Inverse Function via a Trace Function $\mathrm{Tr}\left(\frac{x^2}{x+1}\right)$. (accepted)