CONTRIBUTIONS ON PLATEAUED (VECTORIAL) FUNCTIONS FOR SYMMETRIC CRYPTOGRAPHY AND CODING THEORY

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

BY

AHMET SINAK

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

SEPTEMBER 2017

Approval of the thesis:

CONTRIBUTIONS ON PLATEAUED (VECTORIAL) FUNCTIONS FOR SYMMETRIC CRYPTOGRAPHY AND CODING THEORY

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

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

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

Prof. Dr. Ferruh Özbudak
Supervisor, **Department of Mathematics / IAM, METU** _____

Prof. Dr. Sihem Mesnager
Co-supervisor, **Department of Mathematics, University of Paris VIII, Paris, France** _____

Examining Committee Members:

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

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

Prof. Dr. Ersan Akyıldız
Department of Mathematics / IAM, METU _____

Assoc. Prof. Dr. Sedat Akleylek
Department of Computer Engineering, Ondokuz Mayıs University _____

Assist. Prof. Dr. Burcu Gülmez Temur
Department of Mathematics, Atılım University _____

Date: _____

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

Name, Last Name: AHMET SINAK

Signature :

ABSTRACT

CONTRIBUTIONS ON PLATEAUED (VECTORIAL) FUNCTIONS FOR SYMMETRIC CRYPTOGRAPHY AND CODING THEORY

Sınak, Ahmet
Ph.D., Department of Cryptography
Supervisor : Prof. Dr. Ferruh Özbudak
Co-Supervisor : Prof. Dr. Sihem Mesnager

September 2017, 171 pages

Plateaued functions, used to construct nonlinear functions and linear codes, play a significant role in cryptography and coding theory. They can possess various desirable cryptographic properties such as high nonlinearity, low autocorrelation, resiliency, propagation criteria, balanced-ness and correlation immunity. In fact, they provide the best possible compromise between resiliency order and nonlinearity. Besides they resist against linear cryptanalysis and fast correlation attacks due to their low Walsh-Hadamard transform values. Indeed, cryptographic algorithms are usually designed by appropriate composition of nonlinear functions, hence plateaued functions have a great effect on the security of these algorithms. Additionally, plateaued functions are closely related to linear codes, the most significant class of codes in coding theory, which have diverse applications in secret sharing schemes, authentication codes, communication, data storage devices and consumer electronics.

The main objectives of this thesis are twofold: to study in detail the explicit characterizations for plateaued-ness of functions over finite fields from a cryptographic point of view, and to construct linear codes from weakly regular plateaued functions in coding theory.

In this thesis, we first analyse characterizations of plateaued (vectorial) functions over a finite field $\mathbb{F}_p$ with p a prime number. More precisely, we obtain a large

number of their characterizations in terms of their Walsh power moments, derivatives and autocorrelation functions, with the aim of both clarifying their structure and obtaining information about their construction. In particular, we observe the nonexistence of a homogeneous cubic bent function (and in some cases a (homogeneous) cubic plateaued function) over $\mathbb{F}_p$ with p an odd prime. Moreover, we show the nonexistence of a function whose absolute Walsh transform takes exactly three distinct values (one being zero), and introduce a new class of functions whose absolute Walsh transform takes exactly four distinct values (one being zero). Furthermore, we study partially bent and plateaued functions over a finite field $\mathbb{F}_q$, with q a prime power, and obtain some of their characterizations in order to understand their behaviour over this field.

In addition, we introduce the notion of (non)-weakly regular plateaued functions over $\mathbb{F}_p$, with p an odd prime, and provide the secondary constructions of these functions. We then construct three-weight linear p-ary (resp. binary) codes from weakly regular p-ary plateaued (resp. Boolean plateaued) functions and determine their weight distributions. Finally, we show that the constructed linear codes can be used to construct secret sharing schemes with "nice" access structures. To the best of our knowledge, the construction of linear codes from plateaued functions over $\mathbb{F}_p$, with p an odd prime, is studied in this thesis for the first time in the literature.

Keywords: Boolean functions, vectorial functions, p-ary functions, bent, partially bent, plateaued, (non)-weakly regular plateaued, linear codes, secret sharing schemes

ÖZ

SİMETRİK KRİPTOGRAFİ VE KODLAMA TEORİSİ İÇİN (VEKTÖREL) PLATO FONKSİYONLAR ÜZERİNE KATKILAR

Sınak, Ahmet
Doktora, Kriptografi Bölümü
Tez Yöneticisi : Prof. Dr. Ferruh Özbudak
Ortak Tez Yöneticisi : Prof. Dr. Sihem Mesnager

Eylül 2017, 171 sayfa

Doğrusal olmayan fonksiyonlar ve doğrusal kodlar inşa etmek için kullanılan plato fonksiyonlar kriptografide ve kodlama teorisinde çok önemli rol oynamaktadır. Bu fonksiyonlar yüksek doğrusalsızlık, düşük otokorelasyon, esneklik, yayılma kriteri, dengelilik ve korelasyon dayanıklılığı gibi çeşitli istenen kriptografik özelliklere sahip olabilmektedir. Aslında bu fonksiyonlar esneklik derecesi ve doğrusalsızlık arasındaki mümkün olan en iyi sınırı sağlar. Bunun yanı sıra, bu fonksiyonlar düşük Walsh-Hadamard dönüşüm değerlerine sahip olmalarından dolayı doğrusal kriptanalize ve hızlı korelasyon saldırılarına karşı dayanıklıdır. Gerçekten de, kriptografik algoritmalar çoğunlukla doğrusal olmayan fonksiyonların uygun bileşkeleri ile tasarlanır, bu nedenle plato fonksiyonlar bu algoritmaların güvenliği üzerinde önemli bir etkiye sahiptir. Plato fonksiyonlar aynı zamanda, gizli paylaşım şemaları, kimlik doğrulama kodları, iletişim, veri depolama cihazları ve tüketici elektronikleri gibi birçok alanda uygulamaları olan ve kodlama teorisindeki en önemli kod sınıfını oluşturan doğrusal kodlarla yakından ilgilidir.

Bu tezin iki temel amacı vardır: kriptografik açıdan sonlu cisimler üzerindeki fonksiyonların platoluluk özelliğini veren karakterizasyonlarını detaylı çalışmak, ve kodlama teorisinde zayıf düzenli plato fonksiyonlardan doğrusal kodlar inşa etmektir.

Bu tezde, ilk olarak sonlu cisim $\mathbb{F}_p$, p asal sayı, üzerindeki plato (vektörel) fonksi-

yonların karakterizasyonlarını analiz ediyoruz. Açıkçası, bu fonksiyonların yapılarını anlamak ve inşaları hakkında bilgi edinmek için, Walsh kuvvet momentleri, türevleri ve otokorelasyon fonksiyonları bakımından çok sayıda karakterizasyonlarını elde ediyoruz. Özel olarak $\mathbb{F}_p$, p tek asal sayı, üzerinde homojen kübik bükük (ve bazı durumlarda homojen kübik plato) fonksiyonların olamayacağını gözlemliyoruz. Ayrıca, mutlak Walsh dönüşümü üç farklı değere (bir tanesi sıfır) sahip olan fonksiyon olamayacağını gösteriyoruz ve mutlak Walsh dönüşümü dört farklı değere (bir tanesi sıfır) sahip olan yeni fonksiyonlar sınıfı veriyoruz. Daha sonra, kısmi bükük ve plato fonksiyonlarını herhangi bir sonlu cisim $\mathbb{F}_q$, q asal kuvvet, üzerinde çalışıyor ve bu cisim üzerindeki davranışlarını anlamak için bazı karakterizasyonlarını veriyoruz.

Bunlara ek olarak, $\mathbb{F}_p$, p tek asal sayı, üzerinde zayıf düzenli (olmayan) plato fonksiyon kavramını ve bu fonksiyonların ikincil inşalarını veriyoruz. Sonra, zayıf düzenli p-li plato (sırayla, Boole plato) fonksiyonlardan üç ağırlıklı doğrusal p-li (sırayla, ikili) kodlar inşa ediyoruz ve bu kodların ağırlık dağılımlarını belirliyoruz. Son olarak da, inşa edilen doğrusal kodların "mükemmel" erişim yapılarına sahip gizli paylaşım şemaları üretmek için kullanılabileceğini gösteriyoruz. Bilgimiz dahilinde, $\mathbb{F}_p$, p tek asal sayı, üzerinde plato fonksiyonlardan doğrusal kodların inşası literatürde ilk kez bu tezde çalışılıyor.

Anahtar Kelimeler: Boole fonksiyonlar, vektörel fonksiyonlar, p-li fonksiyonlar, bükük, kısmi bükük, plato, zayıf düzenli (olmayan) plato, doğrusal kodlar, gizli paylaşım şemaları

To My Parents and My Fiancée Ebru

ACKNOWLEDGMENTS

"*Mathematics is the most beautiful and most powerful creation of the human spirit*".
Stefan Banach

First and foremost, I would like to extend my sincere thanks to my supervisor, Prof. Dr. Ferruh Özbudak, for his patient guidance, enthusiastic encouragement and valuable advices during the development and preparation of this thesis. I also gratefully appreciate his considerable assistance during this thesis in spite of his many other concerns.

My best regards and heartfelt thanks are due to my co-supervisor, Prof. Dr. Sihem Mesnager, for her great guidance, effective suggestions and substantial efforts to keep me motivated in my thesis years. I must say that I respect her for checking up on my progress even at the times when she seemed so busy. I am also indebted to her for inviting me as a guest researcher at Paris 8 University.

I would like to thank anonymous reviewers and the editors of the papers resulting from this thesis for their valuable comments and suggestions. It is also a great pleasure to thank Prof. Dr. Claude Carlet for our joint work in part of this thesis and his valuable papers which helped in obtaining some results of this thesis.

My thanks are also to Ali Doğanaksoy, Ersan Akyıldız, Sedat Akleylek and Burcu Gülmez Temur for being committee members of my defense. Especially, my heartfelt thanks are to Ersan Akyıldız and Sedat Akleylek for their valuable suggestions and directions throughout my graduate years, which helped me in establishing my academic way of life.

I wish to extend my profound thanks to Mehpare Bilhan, who taught me Finite Fields, for her generous teaching and warm attitude to all of her students.

I owe a debt of gratitude to Murat Cenk, Zülfükar Saygı and Oğuz Yayla for their enduring support and encouragement. Especially, I gratefully appreciate Oğuz Yayla for his considerable assistance in my graduate years.

I wish to record my deep sense of appreciation and thankfulness to the members of IAM family, especially to A. Sevtap Selçuk-Kestel, Nejla Erdoğdu (Nejla Sultan is the mother of IAM family), and Gerhard-Wilhelm Weber (Willi) for providing enjoyable atmosphere, motivation and a relaxed working environment during my IAM life. I am deeply grateful to my warm roommates: Ayşe, Büşra, Cansu, Derya, Meral,

Neşe, Önder, Özge, Sinem and Ziya for their patience and understanding, and for being close companions and sharing enjoyable moments in my Ofis life. Indeed, both Önder and Sinem deserve my special thanks due to their genuine friendship and continuous support. I am also grateful to all my colleagues in cryptography program, especially to Canan Çimen, Pınar Çomak, Murat Demircioğlu, Turgut Hanoymak, Kamil Otal, and Halil Kemal Taşkın (who shares his skills in MAGMA with me) for their close friendship and pleasant times in my Kripto life. Among my dear friends who deserve my thanks are Saffet Aykın, Serkan Demiröz, Cevher Durmuş, Ömer Ergüven, Muharrem Kayabel and Cafer Topal for helping with departmental chores. On a side note, I will never forget the many days I spent in the IAM building where I committed myself to this thesis until the first lights of the next day.

I would like to express my deep gratitude to the many other wonderful friends who have always been with me. Especially, I am deeply grateful to Fuat Bey (Fuat Erdem) for his intimate friendship during my ODTÜ life and proofreading the whole thesis with a great commitment of time and energy. I am also indebted to Fırat Batman and Yavuz Yazıcı for their genuine friendship over the years.

I gratefully acknowledge generous financial support from the Scientific and Technological Research Council of Turkey (TÜBİTAK) via Graduate Scholarship programs 2211 during my PhD years and 2214/A during my visit to Paris 8 University. I also acknowledge financial support from the Council of Higher Education (YÖK) via Öğretim Üyesi Yetiştirme Programı (ÖYP) during my PhD years.

Lastly and most importantly, I wish to express my deepest gratitude to my family for their endless support, and especially to my lovely nieces and nephews: Yiğit, Eymen, Miraç, Uğurcan, Cansu, İlayda, Umut, Berat, Hatice, Mıstık and Adnan, who are a great source of happiness in my life, for spending joyous moments together.

To conclude, I am so glad to have left fond memories that will long be cherished as I start the next chapter of my life.

I praise God for each and every bit of my life.

TABLE OF CONTENTS

LIST OF TABLES

TABLES

LIST OF ABBREVIATIONS

ABBRV	Abbreviation
$\mathbb{C}$	The set of complex numbers
$\mathbb{R}$	The set of real numbers
$\mathbb{Q}$	The set of rational numbers
$\mathbb{Z}$	The set of integers
$\mathbb{N}$	The set of natural numbers
p	A prime number
q	A power of a prime number
m, n, s	Positive integers with $0 \leq s \leq n$
$\mathbb{F}_p$	The prime finite field with p elements
$\mathbb{F}_{q^n}$	The finite field with q^n elements
$\mathbb{F}_q^n$	The vector space with dimension n over $\mathbb{F}_q$
$\mathrm{Tr}_{q^m}^{q^n}$	The relative trace function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_{q^m}$
ξ_p	A primitive p-th root of unity $\left(e^{\frac{2\pi i}{p}}\right)$
ξ_q	A primitive q-th root of unity $\left(e^{\frac{2\pi i}{q}}\right)$
χ	The canonical additive character of $\mathbb{F}_q$
$\widehat{G}$	The Fourier transform of a complex valued function G
$\widehat{\chi_f}$	The Walsh transform of a function f
$\deg f$	Algebraic degree of a function f
$\gcd(a, b)$	The greatest common divisor of integers a and b
" $*$ "	A usual product in $\mathbb{Z}$
" . "	An inner product in a vector space
$\#E$	The size of a set E
$E^\star = E \setminus \{0\}$	The set of the nonzero elements of a set E
$\lvert z \rvert$	The absolute value of a complex number z
$\overline{z}$	The conjugate of a complex number z
$\left(\frac{a}{p}\right)$	The Legendre symbol for $a \in \mathbb{F}_p^\star$
p^*	denotes $\left(\frac{-1}{p}\right) p$

CHAPTER 1

INTRODUCTION

1.1 Overview

The functions over a binary field are called *Boolean functions*, which play an important role in cryptography and coding theory. Bent functions over a binary field are maximally nonlinear Boolean functions. They have attracted considerable attention in the literature not only for being interesting combinatorial objects, but also for their relations to coding theory (e.g. the Reed-Muller codes, the Kerdock codes, etc.), combinatorics (e.g. difference sets), design theory, sequence theory, and applications in cryptography (design of stream ciphers and of substitution-boxes for block ciphers). Plateaued Boolean functions are generalization of Boolean bent functions. They also have a significant role in cryptography, coding theory, sequences for communications, and the related combinatorics and designs. Notably, they are applicable primitives used in coding theory to construct linear codes and symmetric cryptography to construct nonlinear functions. In addition to the desirable various cryptographic properties of bent functions such as high nonlinearity, low additive autocorrelation, resiliency and propagation criteria, plateaued functions can have balancedness and correlation immunity. In fact, the order of resiliency and the nonlinearity of Boolean functions is strongly bounded only by plateaued functions. Additionally, some plateaued functions provide resistance against linear cryptanalysis and fast correlation attacks due to their high nonlinearities and low Walsh-Hadamard transform values. The algorithms in symmetric cryptography (stream and block ciphers) are designed using an appropriate composition of nonlinear functions, and thereby plateaued functions have a great effect on the security of these algorithms (for in-

stance, the security of block ciphers highly depends on the substitution-boxes).

The notion of Boolean bent functions was introduced by Rothaus [72] in the 1970s and initially studied by Dillon as early as in 1974 [30]. They have been widely studied in the past forty years by a large number of researchers (see, a non-exhaustive list, [6, 11, 13, 14, 39, 49, 70]). In fact, a jubilee survey paper [19] and a book [57] have been devoted to bent functions (including generalizations, variations and applications). Because of unbalanced-ness of bent functions, Carlet (1993) introduced in [12] a super class of bent functions: the notion of *partially bent functions*, whose elements not only have high nonlinearity but also can be balanced. As an extension of this notion, Zheng and Zhang (1999) introduced in [78] the notion of *plateaued functions*, whose squared Walsh transform takes only one nonzero value (also possibly the value 0). Plateaued Boolean functions include four important classes of Boolean functions: 0-plateaued functions (called bent functions), 1-plateaued functions (called near-bent functions), 2-plateaued functions (called semi-bent functions) and partially bent functions. It is worth noting that, in characteristic 2, 0-plateaued and 2-plateaued functions exist only when n is even, while 1-plateaued functions exist only when n is odd. These Boolean functions have been extensively studied by a large number of researchers (see, e.g., [15, 21, 26, 45, 49, 54, 56, 79]). However, the other plateaued Boolean functions have not been studied much in a general framework when compared to their importance. In fact, a small amount of work have been done in [21, 69, 78]. Recently, Carlet [15] (2015) has deeply studied the constructions and characterizations of plateaued Boolean (vectorial) functions by means of their Walsh power moments, autocorrelation functions, first-order and second-order derivatives.

The notion of plateaued functions has been generalized to arbitrary characteristic: the so-called *p-ary plateaued functions* (see, e.g., [23, 55]). Indeed, in 2014, the first study of p-ary plateaued functions was done in [55] by Mesnager, who introduced new characterizations of p-ary plateaued by the constant of the ratio of two consecutive Walsh power moments of even order. A small number of researchers have studied and brought some results on these functions, especially on their characterizations and constructions in arbitrary characteristic (see, e.g., [23, 43, 55]). Because of the gap between the interest of the notion of these functions and our knowledge on it,

we aim in this thesis to continue bringing new results on the characterizations of p-ary plateaued (vectorial) functions and to provide new tools which allow us a better understanding of their structure and have a toolbox for future construction of these functions. To this end, we first push further the study initiated by Mesnager on p-ary plateaued (vectorial) functions (2014) and extend the ones done by Carlet (2015) in characteristic 2. We also obtain a number of new characterizations of these functions by using their Walsh power moments, derivatives and autocorrelation functions, with the aim of clarifying their structure.

In 1985, the notion of bent functions was generalized to any residue class ring $\mathbb{Z}_k$ by Kumar et al. [46] where k is any positive integer, and since then they have been exhaustively studied by a number of researchers (see, e.g., [18, 40, 41, 48, 67] for a positive integer k and see, e.g., [22, 23, 24, 36, 37, 38, 75] for a prime k). In 1991, the notion of perfect nonlinear functions over $\mathbb{Z}_k$, with k any positive integer, was introduced by Nyberg [67]. Nyberg established some properties of bent and perfect nonlinear functions over $\mathbb{Z}_k$. We emphasize that generalized bent and perfect nonlinear functions over $\mathbb{Z}_k$ are not equivalent for a positive integer k, in general. Nyberg, over $\mathbb{Z}_k$, showed that any perfect nonlinear function is a generalized bent function for any positive integer k, but the converse is true only if k is a prime number. In 1997, Coulter and Matthews [28] redefined bent functions over any finite field $\mathbb{F}_q$ with q a prime power, and discussed some of their properties and permutation behaviour. They showed that bent and perfect nonlinear functions are equivalent over $\mathbb{F}_q$, while they are not equivalent over $\mathbb{Z}_k$ for a composite number k. Additionally, Hou [41] (2004) come up with further results about bent functions over $\mathbb{F}_q$. Within this framework, the other purpose of this thesis is to study the notions of partially bent and plateaued functions over any finite field $\mathbb{F}_q$ and their various characterizations.

Error correcting codes are extensively studied in the literature by a large number of researchers and employed by many engineers. They have long been known to have applications in computer and communication systems, data storage devices (starting from the use of Reed Solomon codes in CDs) and consumer electronics. Considerable progress has been made on the constructions of linear codes with few weights. Such codes have many applications in secret sharing schemes [1, 17, 27, 35, 77], authentication codes [32], association schemes and strongly regular graphs [9]. There

are several methods to construct linear codes, one of which is based on functions over finite fields (see, a non-exhaustive list, [31, 34, 35, 58, 76, 80]). Two generic constructions (say, *first* and *second*) of linear codes from functions have been kept apart from the others in the literature. Recently, several constructions of linear codes based on the second generic construction were proposed, and plenty of linear codes with perfect parameters were constructed. In fact, Ding brought out an interesting survey [31] devoted to the construction of binary linear codes from Boolean functions based on the second generic construction. Commonly, bent functions (mostly, quadratic and weakly regular bent functions) have been used to construct linear codes with few weights. Recently, it was shown in a few papers (see, e.g., [35, 76, 80]) that they lead to the construction of interesting linear codes with few weights based on the second generic construction. Very recently, Mesnager [58] has constructed a new family of three-weight linear codes from weakly regular bent functions in odd characteristic based on the first generic construction. Within this framework, the next purpose of this thesis is to construct new classes of three-weight linear codes from weakly regular plateaued functions. This is the first time construction of linear codes from weakly regular plateaued functions in odd characteristic.

Secret sharing schemes were introduced in 1979 by Blakley [4] and Shamir [74]. They have been widely studied by a large number of researchers due to their diverse real-word applications in cryptographic protocols, electronic voting systems, banking systems and a controlling of nuclear weapons. There are several methods to construct secret sharing schemes, one of which is based on linear codes in coding theory. In fact, the connection between Shamir's secret sharing scheme and the Reed-Solomon codes was given in 1981 by McEliece and Sarwate [53] and since then, the construction of secret sharing schemes using linear codes has been extensively studied (see, e.g., [1, 17, 33, 35, 51, 53, 71, 77]). Every linear code can be used to construct secret sharing schemes and provides a pair of secret sharing schemes, based on itself and its dual code. We emphasize that the constructed linear codes in this thesis generate secret sharing schemes with "nice" access structures.

1.2 Motivation and Achievements

Although plateaued functions were first introduced more than a decade ago, our knowledge on them is actually not at a sufficient level corresponding to their importance. With their explicit characterizations we indeed aim to reduce to a degree the gap between the interest of these functions and what is known on them. The main contributions of this thesis are summarized as follows. We first study characterizations of bent and plateaued (vectorial) functions over $\mathbb{F}_p$, with p a prime number. More precisely, we obtain a large number of their characterizations in terms of their Walsh power moments, derivatives and autocorrelation functions, with the aim of not only clarifying their structure but also obtaining new tools which help their future construction. Actually, using one of these characterizations, we observe the non-existence of a homogeneous cubic bent function (and for some cases a (homogeneous) cubic plateaued function) over $\mathbb{F}_p$, with p an odd prime. We next study the notions of partially bent and plateaued functions over $\mathbb{F}_q$, with q a prime power, in order to understand their behaviour over $\mathbb{F}_q$. Moreover, we show the non-existence of a function whose absolute Walsh transform takes exactly three distinct values (one being zero), and then introduce a new class of functions whose absolute Walsh transform takes exactly four distinct values (one being zero) over $\mathbb{F}_2$ and $\mathbb{F}_3$. Furthermore, we introduce the notion of weakly regular plateaued functions, and construct three-weight linear codes from these functions over $\mathbb{F}_p$, with p an odd prime. We also determine the weight distributions of the constructed codes. Finally, we describe the access structures of the secret sharing schemes based on the dual codes of the constructed linear codes.

1.3 Outline

In this section, we describe how this thesis is organized.

- Chapter 2 sets main notations and collects necessary background in finite field theory, cryptography and coding theory. More precisely, we first give basic notions in the study of finite fields such as the Legendre symbol and cyclotomic field. Next we present the notions of significant cryptographic functions over

finite fields such as bent, partially bent and plateaued functions. Meanwhile, we give the Fourier transform and the Walsh transform of a function in terms of additive characters of a finite field. Finally, linear codes, secret sharing schemes and their connection are mentioned.

- Chapter 3 focuses on explicit characterizations for plateaued-ness of (vectorial) p-ary functions in arbitrary characteristic, with the aim of understanding their structure and getting more information about their construction. Section 3.1 characterizes p-ary bent functions by means of their Walsh power moments, derivatives and autocorrelation functions. Section 3.2 obtains a large number of characterizations of p-ary plateaued functions in terms of the value distribution of their second-order derivatives, even power moments of their Walsh transform and their autocorrelation functions, which allow us a better understanding of their structure and provide useful intuition for their future construction. In Section 3.3, we use the value distributions of the second-order (and also first-order) derivatives of vectorial functions in order to provide several characterizations of vectorial bent and plateaued p-ary functions. In Section 3.4, to characterize vectorial p-ary plateaued functions by means of the Walsh transform and autocorrelation function, we make use of the Walsh power moments and autocorrelation functions of their nonzero component functions. Section 3.5 explores a probably unexpected behavior of cubic functions in even and odd characteristics. Indeed, we observe the non-existence of a homogeneous cubic bent function (and for some cases a (homogeneous) cubic plateaued function) in odd characteristic.

- Chapter 4 is concerned with functions whose absolute Walsh transform takes exactly three and four distinct values. Section 4.1 shows the non-existence of a function whose absolute Walsh transform takes exactly three distinct values (one being zero) in arbitrary characteristic. Section 4.2 introduces a new class of functions whose absolute Walsh transform takes exactly four distinct values (one being zero) in characteristics 2 and 3.

- Chapter 5 investigates the notions of partially bent and plateaued functions over any finite field $\mathbb{F}_q$, with q a prime power. Section 5.1 redefines, over $\mathbb{F}_q$, the notions of partially bent and plateaued functions, which rely on the concept of

their Walsh transform in terms of canonical additive characters of $\mathbb{F}_q$. Indeed, we provide a concrete example of a 4-ary plateaued but not vectorial plateaued Boolean function. In Section 5.2, we obtain several characterizations of q-ary partially bent functions by means of their Walsh power moments, derivatives and autocorrelation functions. In Section 5.3 we extend to q-ary case some of characterizations of p-ary plateaued functions given in Section 3.3. Finally, in Section 5.4, we introduce the notion of a q-ary plateaued-type function associated with its Walsh-type transform.

- Chapter 6 focuses on the construction of linear codes with few weights from functions over finite fields and their application in secret sharing schemes. In Section 6.1, we first introduce the notion of (non)-weakly regular plateaued functions over finite fields of odd characteristic, which covers a non-trivial subclass of the class of plateaued functions. We next give the secondary and recursive constructions for the first constructions of these functions. Section 6.2 deals with the construction of linear codes involving special functions based on the first generic construction. In Section 6.3, we construct new classes of three-weight linear p-ary (resp. binary) codes from weakly regular p-ary plateaued (resp. plateaued Boolean) functions based on the first generic construction. We also determine the weight distributions of the constructed linear codes. Finally, in Section 6.4, we observe that all nonzero codewords of the constructed linear codes are minimal for almost all cases. This suggests that the constructed linear codes can be used to construct secret sharing schemes with "nice" access structures.

CHAPTER 2

PRELIMINARIES

In this chapter, we state main notations and recall some necessary definitions/results in finite field theory, cryptography and coding theory. For more details and further reading of the essential theory and concepts, the reader is referred to [44, 50, 66] for finite field theory, to [6, 13, 14, 57] for cryptography, and to [42] for coding theory.

2.1 Basic Background in Finite Field Theory

Let p be a prime number. The residue class ring $\mathbb{Z}_p := \mathbb{Z}/_{\langle p \rangle}$ forms a finite field, identified with the Galois field $\mathbb{F}_p$ with p elements. For a prime p and an integer $n \geq 1$, to construct a finite extension field with p^n elements over $\mathbb{F}_p$, one needs an irreducible polynomial of degree n over $\mathbb{F}_p$. In fact, the residue class ring

$$\mathbb{F}_p[x]/_{\langle g(x) \rangle} = \{a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} : a_i \in \mathbb{F}_p \text{ for } 0 \leq i \leq n-1\} \quad (2.1)$$

forms a finite field with p^n elements, where $g(x)$ is an irreducible polynomial of degree n in $\mathbb{F}_p[x]$. The finite field with p^n elements is unique up to isomorphism and is denoted by $\mathbb{F}_{p^n}$. Here, $\mathbb{F}_{p^n}^\star = \langle \zeta \rangle$ is a multiplicative cyclic group of order $p^n - 1$ with generator ζ, and $\mathbb{F}_p$ is the prime field contained in $\mathbb{F}_{p^n}$ (i.e., the characteristic of $\mathbb{F}_{p^n}$ is p).

Let α be a root of an irreducible polynomial $g(x)$ in $\mathbb{F}_{p^n}$. By choosing a basis $B = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\} \subseteq \mathbb{F}_{p^n}$ over $\mathbb{F}_p$, the extension field $\mathbb{F}_{p^n}$ can be viewed as an n-dimensional vector space over $\mathbb{F}_p$, denoted by

$$\mathbb{F}_p^n = \langle B \rangle = \{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} : a_i \in \mathbb{F}_p \text{ for } 0 \leq i \leq n-1\} \quad (2.2)$$

An element $a \in \mathbb{F}_{p^n}$ can be viewed as a vector $a = (a_0, a_1, \ldots, a_{n-1}) \in \mathbb{F}_p^n$ where $a_i \in \mathbb{F}_p$ for $0 \leq i \leq n-1$. This identification gives an isomorphism between the finite field $\mathbb{F}_{p^n}$ in (2.1) and the vector space $\mathbb{F}_p^n$ in (2.2). The dimension of the vector space $\mathbb{F}_p^n$ over $\mathbb{F}_p$ is the size of B, in symbols $\dim(\mathbb{F}_p^n) = n$. The size of the vector space $\mathbb{F}_p^n$ is equal to $p^{\dim(\mathbb{F}_p^n)}$, denoted by $\#\mathbb{F}_p^n = p^n$. We now recall the definition of the trace function.

Definition 2.1. Let n and k be two positive integers such that k divides n. Then the *relative trace function* $\mathrm{Tr}_{p^k}^{p^n}$ from the finite field $\mathbb{F}_{p^n}$ to its subfield $\mathbb{F}_{p^k}$ is defined by

$$\mathrm{Tr}_{p^k}^{p^n}(x) = \sum_{i=0}^{\frac{n}{k}-1} x^{p^{ki}} = x + x^{p^k} + \cdots + x^{p^{n-k}}.$$

The *absolute trace* of $x \in \mathbb{F}_{p^n}$ over $\mathbb{F}_p$ is defined by $\mathrm{Tr}_p^{p^n}(x) = x + x^p + \cdots + x^{p^{n-1}}$.

Proposition 2.1. *The trace function has the following significant properties:*

- *It is the surjective function:*
- *It is the linear function:* $\mathrm{Tr}_p^{p^n}(ax+by) = a\mathrm{Tr}_p^{p^n}(x)+b\mathrm{Tr}_p^{p^n}(y)$ *for all* $x, y \in \mathbb{F}_{p^n}$ *and* $a, b \in \mathbb{F}_p$.
- *It satisfies the transitivity property in a chain of extension fields, i.e., for all* $x \in \mathbb{F}_{p^n}$, $\mathrm{Tr}_p^{p^n}(x) = \mathrm{Tr}_p^{p^k}\left(\mathrm{Tr}_{p^k}^{p^n}(x)\right)$.
- $\mathrm{Tr}_p^{p^n}(x^p) = \mathrm{Tr}_p^{p^n}(x)$ *for all* $x \in \mathbb{F}_{p^n}$.

Two bases $B = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ and $B' = \{\alpha_1', \alpha_2', \ldots, \alpha_n'\}$ of $\mathbb{F}_p^n$ over $\mathbb{F}_p$ are said to be dual if for $1 \leq i, j \leq n$

$$\mathrm{Tr}_p^{p^n}(\alpha_i \alpha_j') = \begin{cases} 1 \text{ if } i = j, \\ 0 \text{ if } i \neq j. \end{cases}$$

For an $\mathbb{F}_p$-linear subspace W of $\mathbb{F}_p^n$, there exists a complementary subspace $\overline{W}$ of W such that $\mathbb{F}_p^n = W \oplus \overline{W}$ (namely, $\mathbb{F}_p^n = W + \overline{W}$ and $W \cap \overline{W} = \{0\}$), where $\oplus$ is the direct sum. Thus, an element $x \in \mathbb{F}_p^n$ can be uniquely written as $x = x_1 + x_2$ where $x_1 \in W$ and $x_2 \in \overline{W}$. Notice that $\dim(W) + \dim(\overline{W}) = n$.

In the following, we state the Legendre symbol and the cyclotomic field, which will be used in Chapter 6.

The Legendre Symbol. Let a be a positive integer and p be an odd prime number. Consider the following quadratic congruence:

$$x^2 \equiv a \pmod{p}. \tag{2.3}$$

We say that a is a quadratic residue modulo p if the congruence relation (2.3) has a solution in $\mathbb{F}_p^\star$, that is, $\sqrt{a} \in \mathbb{F}_p^\star$ and a is a quadratic non-residue modulo p if the congruence relation (2.3) has no solution in $\mathbb{F}_p^\star$, that is, $\sqrt{a} \notin \mathbb{F}_p^\star$. The *Legendre symbol* is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p|a, \\ 1 & \text{if } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p. \end{cases}$$

Lemma 2.1. *The Legendre symbol satisfies the congruence relation:*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}. \tag{2.4}$$

Proof. It is obvious that both sides are 0 modulo p when p divides a. Assume that p does not divide a. Let ζ be a generator of $\mathbb{F}_p^*$. Note that all quadratic residues are in the form ζ^{2i} for some i. If $a \equiv \zeta^{2i} \pmod{p}$ for $i \in \mathbb{N}$, then

$$a^{\frac{p-1}{2}} \equiv \zeta^{2i(\frac{p-1}{2})} \equiv \zeta^{i(p-1)} \equiv \left(\zeta^{p-1}\right)^i \equiv 1 \pmod{p}.$$

This shows that (2.4) holds.

For a non-quadratic residue $a \equiv \zeta^{2i+1} \pmod{p}$ for $i \in \mathbb{N}$, we have

$$a^{\frac{p-1}{2}} \equiv \zeta^{(2i+1)\frac{p-1}{2}} \equiv \zeta^{i(p-1)}\zeta^{\frac{p-1}{2}} \equiv \zeta^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

This shows (2.4) also holds in this case. The proof is complete. □

The Legendre symbol satisfies the following properties for positive integers a, b and odd primes p, q.

- The Legendre symbol has the multiplicative property: $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. By Lemma 2.1,

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \pmod{p} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \pmod{p} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

- If $p \nmid a$, then $\left(\frac{a^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{p}\right) = 1$. In particular, we have $\left(\frac{1}{p}\right) = 1$.
- If $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$, that is, $\left(\frac{a}{p}\right)$ depends only on $a \in \mathbb{F}_p$.
- We have the following:

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p} = \begin{cases} 1 & \iff p \equiv 1 \pmod{4} \\ -1 & \iff p \equiv 3 \pmod{4}. \end{cases} \tag{2.5}$$

Throughout this thesis, $\left(\frac{a}{p}\right)$ denotes the Legendre symbol for $a \in \mathbb{F}_p^\star$, and p^* denotes $\left(\frac{-1}{p}\right)p$, where p is an odd prime.

Cyclotomic Field $\mathbb{Q}(\xi_p)$. Let p be a prime and let $\mathbb{Q}$ denote the field of rational numbers. Let $\xi_p = e^{2\pi i/p}$ be *a primitive p-th root of unity* in $\mathbb{C}$ where $i = \sqrt{-1}$. A cyclotomic field $\mathbb{Q}(\xi_p)$ is obtained from the field $\mathbb{Q}$ by adjoining ξ_p. The ring of integers in $\mathbb{Q}(\xi_p)$ is defined as $\mathcal{O}_{\mathbb{Q}(\xi_p)} := \mathbb{Z}(\xi_p)$, where $\mathbb{Z}$ is the set of integers. An integral basis of $\mathcal{O}_{\mathbb{Q}(\xi_p)}$ is the set

$$\{\xi_p^i : 1 \leq i \leq p-1\}.$$

The field extension $\mathbb{Q}(\xi_p)/\mathbb{Q}$ is Galois of degree $p-1$, and the Galois group

$$Gal(\mathbb{Q}(\xi_p)/\mathbb{Q}) = \{\sigma_a : a \in \mathbb{F}_p^\star\},$$

where the automorphism σ_a of $\mathbb{Q}(\xi_p)$ is defined by $\sigma_a(\xi_p) = \xi_p^a$. The cyclotomic field $\mathbb{Q}(\xi_p)$ has a unique quadratic subfield $\mathbb{Q}(\sqrt{p^*})$, where $p^* = \left(\frac{-1}{p}\right)p$. For $a \in \mathbb{F}_p^\star$, we have $\sigma_a(\sqrt{p^*}) = \left(\frac{a}{p}\right)\sqrt{p^*}$. Hence, the Galois group $Gal(\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}) = \{1, \sigma_\gamma\}$ for any $\gamma \in \mathbb{F}_p$ such that $\sqrt{\gamma} \notin \mathbb{F}_p^\star$. The reader is referred to [44] for further reading on cyclotomic fields.

2.2 On the (Vectorial) Functions over Finite Fields

In this section, we consider the discrete functions between two vector spaces.

We mention the functions from $\mathbb{F}_p^n$ to $\mathbb{F}_p^m$, where p is a prime and m, n are positive integers. For any prime p, a function F from $\mathbb{F}_p^n$ to $\mathbb{F}_p^m$ is called *vectorial p-ary function* (or, (n,m)-p-ary function), and a function f from $\mathbb{F}_p^n$ to $\mathbb{F}_p$ is called *p-ary*

function (or, $(n,1)$-p-ary function) in n variables. For simplicity, in this thesis, a function F from $\mathbb{F}_p^n$ to $\mathbb{F}_p^m$ is denoted by $F : \mathbb{F}_p^n \to \mathbb{F}_p^m$ and a function f from $\mathbb{F}_p^n$ to $\mathbb{F}_p$ is denoted by $f : \mathbb{F}_p^n \to \mathbb{F}_p$.

Remark 2.1. The identification between the finite field $\mathbb{F}_{p^n}$ and n-dimensional vector space $\mathbb{F}_p^n$ over $\mathbb{F}_p$ allows us to define these functions over finite fields as well.

In the case of $p = 2$, a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ is called *vectorial Boolean function* (or, (n,m)-Boolean function), and a function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is called *Boolean function* in n variables.

Boolean Functions. The functions over a binary field are called *Boolean functions*. Boolean functions play a significant role in cryptography and coding theory. In both frameworks, n is rarely large in practice. In fact, cryptographic transformations (pseudo-random generators in stream ciphers, substitution boxes in block ciphers) can be designed by an appropriate composition of nonlinear Boolean functions. In coding theory, every code of length 2^n can be expressed as a set of Boolean functions, since every n-variable Boolean function can be represented by its truth table. Two of the most famous codes, the Reed–Muller and the Kerdock codes, are defined this way as sets of Boolean functions. For more details on Boolean functions, the reader is referred to [13, 14].

Representations of p-Ary Functions over $\mathbb{F}_p$. There exist several representations of p-ary functions, we now refer two ones that will be used in this thesis. We first explain the univariate form of a p-ary function f, which is an essential representation. Since an n-dimensional vector space $\mathbb{F}_p^n$ over $\mathbb{F}_p$ is identified with the Galois field $\mathbb{F}_{p^n}$ (see Remark 2.1), every p-ary function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ can be described in the so-called *univariate form*, which can be given in *trace form* as

$$f(x) = \mathrm{Tr}_p^{p^n}\left(\sum_{i=0}^{p^n-1} a_i x^i\right)$$

where $a_i \in \mathbb{F}_{p^n}$. It is worth noting that the univariate representation is not unique. Indeed, a unique univariate form of p-ary function f, called *trace representation*, is given by

$$f(x) = \sum_{i \in \Gamma_n} \mathrm{Tr}_p^{p^{\circ(i)}}(a_i x^i) + a_{p^n-1} x^{p^n-1},$$

where

- Γ_n is the set of integers obtained by choosing the smallest element in each cyclotomic coset modulo $p^n - 1$ (with respect to p);
- $\circ(i)$ is the size of the cyclotomic coset containing i;
- $a_i \in \mathbb{F}_{p^{\circ(i)}}$ and $a_{p^n-1} \in \mathbb{F}_p$.

The algebraic degree of f (denoted by $\deg f$) is equal to $\max\{w_p(i) : a_i \neq 0\}$, where $w_p(i)$ is the weight of the p-ary expansion of i. In particular, p-ary linear functions are exactly all functions of the form $\mathrm{Tr}_p^{p^n}(ax)$ for some $a \in \mathbb{F}_{p^n}$, namely, a function is called linear if its algebraic degree is one. On the other hand, a function is called quadratic if its algebraic degree is two.

If we do not identify the vector space $\mathbb{F}_p^n$ with the finite field $\mathbb{F}_{p^n}$, p-ary function has a representation as a unique multinomial in $x_1, x_2, \ldots, x_n$, where the variables x_i occur with exponent at most $p-1$. A p-ary function $f : \mathbb{F}_p^n \to \mathbb{F}_p$ is uniquely expressed by

$$f(x) = \sum_{\mathbf{u} \in \mathbb{F}_p^n} a_{\mathbf{u}} \mathbf{x}^{\mathbf{u}} = \sum_{\mathbf{u} \in \mathbb{F}_p^n} a_{\mathbf{u}} x_1^{u_1} x_2^{u_2} \cdots x_n^{u_n},$$

where $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_p^n$, $\mathbf{u} = (u_1, u_2, \ldots, u_n) \in \mathbb{F}_p^n$ and $a_{\mathbf{u}} \in \mathbb{F}_p$. This is called the *multivariate representation* or *algebraic normal form (ANF)*. The algebraic degree of a p-ary function is the global degree of its multivariate representation.

Representations of Vectorial p-Ary Functions. Recall that a function F from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ is said to be vectorial p-ary function.

If $m = n$, any vectorial function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ has a unique representation as a univariate polynomial over $\mathbb{F}_{p^n}$ of degree smaller than p^n

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

A function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is linear if $F(x) = \sum_{0 \leq i \leq n} a_i x^{p^i}$, where $a_i \in \mathbb{F}_{p^n}$, and F is affine if it is a sum of a linear function and a constant function.

In the case when m divides n, $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ can also admit a univariate polynomial

representation (since it can be seen as a function from $\mathbb{F}_{p^n}$ to itself): in the trace form

$$F(x) = \mathrm{Tr}_{p^m}^{p^n}\left(\sum_{i=0}^{p^n-1} a_i x^i\right), \quad a_i \in \mathbb{F}_{p^n}.$$

In this case, the vectorial function F can be viewed as a function f from $\mathbb{F}_{q^k}$ to $\mathbb{F}_q$ defined by

$$f(x) = \mathrm{Tr}_{q}^{q^k}\left(\sum_{i=0}^{q^k-1} a_i x^i\right), \quad a_i \in \mathbb{F}_{q^k},$$

where $q = p^m$ and $n = mk$ for a positive integer k. This function f is called *q-ary function* and denoted by $f : \mathbb{F}_{q^k} \to \mathbb{F}_q$, where q is a prime power.

On the other hand, in the case when m is not a divisor of n, the univariate representation of vectorial function F in the field is not proper. Hence, F should be viewed over the vector space, i.e., $F : \mathbb{F}_p^n \to \mathbb{F}_p^m$ and represented by its *algebraic normal form ANF*:

$$F(x) = \sum_{u \in \mathbb{F}_p^n} a_u \prod_{i=1}^{n} x_i^{u_i}, \quad a_u \in \mathbb{F}_p^m,$$

(this sum is in $\mathbb{F}_p^m$). The algebraic degree of F equals the degree of its ANF.

We now indicate the component functions of a vectorial $F : \mathbb{F}_p^n \to \mathbb{F}_p^m$. The nonzero component functions of F are $F_\lambda = \lambda \cdot F : \mathbb{F}_p^n \to \mathbb{F}_p$, $\lambda \in \mathbb{F}_p^m \setminus \{0\}$, defined as

$$F_\lambda(x) = \lambda \cdot F(x)$$

for every $x \in \mathbb{F}_p^n$, where "$\cdot$" denotes an inner product in $\mathbb{F}_p^m$. Since the vector spaces $\mathbb{F}_p^n$ and $\mathbb{F}_p^m$ can be identified with the Galois fields $\mathbb{F}_{p^n}$ and $\mathbb{F}_{p^m}$ of orders p^n and p^m, respectively (see Remark 2.1), then for every $\lambda \in \mathbb{F}_{p^m}^\star$, the component function F_λ is defined as

$$F_\lambda(x) = \mathrm{Tr}_p^{p^m}(\lambda F(x))$$

for every $x \in \mathbb{F}_{p^n}$.

2.3 The Fourier Transform and the Walsh Transform of Function

We start by giving the notion of additive characters of a finite field.

Let $\xi_p = e^{2\pi i/p}$ be *a primitive p-th root of unity* in $\mathbb{C}$, where $i = \sqrt{-1}$ and p is a prime number. It is obvious that the complex conjugation of ξ_p is its inverse, i.e., $\overline{\xi}_p = \xi_p^{-1}$. Then, the function χ from $\mathbb{F}_q$ to $\mathbb{C}$, defined as

$$\chi(x) = \xi_p^{\mathrm{Tr}_p^q(x)} \tag{2.6}$$

for all $x \in \mathbb{F}_q$, is called *the canonical additive character* of $\mathbb{F}_q$. Notice that for each $y \in \mathbb{F}_q$, the function $\chi_y(x) = \chi(yx)$ for all $x \in \mathbb{F}_q$ is an additive character of $\mathbb{F}_q$ and every additive character of $\mathbb{F}_q$ is obtained in this way. In particular, χ_0 is the *trivial* additive character of $\mathbb{F}_q$ defined as $\chi_0(x) = 1$ for all $x \in \mathbb{F}_q$. For each character χ of $\mathbb{F}_q$, there is associated the *conjugate* character $\overline{\chi}$ defined as $\overline{\chi}(x) := \overline{\chi(x)}$ for all $x \in \mathbb{F}_q$. Let χ and ψ be the canonical additive characters of $\mathbb{F}_q$ and $\mathbb{F}_q^n$, respectively. Then for all $\alpha \in \mathbb{F}_q^n$, they are connected by the identity $\chi(\mathrm{Tr}_q^{q^n}(\alpha)) = \psi(\alpha)$.

The following lemma gives some well known properties of additive characters of $\mathbb{F}_q$, which will be frequently used in the sequel.

Lemma 2.2. *Let $\chi : \mathbb{F}_q \to \mathbb{C}$ be an additive character as in (2.6). Then for all $x_1, x_2 \in \mathbb{F}_q$, we have $\chi(x_1 + x_2) = \chi(x_1)\chi(x_2)$ and $\overline{\chi}(x) = \chi(-x)$ for all $x \in \mathbb{F}_q$.*

Proof. For all $x_1, x_2 \in \mathbb{F}_q$, we have

$$\chi(x_1 + x_2) \ = \xi_p^{\mathrm{Tr}_p^q(x_1+x_2)} = \xi_p^{\mathrm{Tr}_p^q(x_1)+\mathrm{Tr}_p^q(x_2)} = \xi_p^{\mathrm{Tr}_p^q(x_1)} \xi_p^{\mathrm{Tr}_p^q(x_2)} = \chi(x_1)\chi(x_2)$$

where in the second equality we used the fact that Tr_p^q is linear. Next, for all $x \in \mathbb{F}_q$ we have

$$\overline{\chi}(x) = \overline{\xi_p^{\mathrm{Tr}_p^q(x)}} = \left(\overline{\xi}_p\right)^{\mathrm{Tr}_p^q(x)} = \left(\xi_p^{-1}\right)^{\mathrm{Tr}_p^q(x)} = \xi_p^{-\mathrm{Tr}_p^q(x)} = \xi_p^{\mathrm{Tr}_p^q(-x)} = \chi(-x)$$

where we used the fact that $\overline{\xi}_p = \xi_p^{-1}$ in the third equality, and that Tr_p^q is linear in the fifth equality. □

Below we give the definition of the Fourier transform of a complex valued function (see [66, Definition 10.1.3]).

Definition 2.2. Let G be a function from $\mathbb{F}_q^n$ to $\mathbb{C}$ and χ be an additive character of $\mathbb{F}_q$ as in (2.6). The Fourier transform of G is defined as

$$\begin{aligned} \widehat{G} : \ & \mathbb{F}_q^n \to \mathbb{C} \\ & \omega \longmapsto \widehat{G}(\omega) = \sum_{x \in \mathbb{F}_q^n} G(x)\overline{\chi}(\omega \cdot x). \end{aligned}$$

In the following, we define the Walsh transform of a function $f : \mathbb{F}_q^n \to \mathbb{F}_q$. Let $\chi : \mathbb{F}_q \to \mathbb{C}$ be an additive character as in (2.6). A composite function χ_f from $\mathbb{F}_q^n$ to $\mathbb{C}$ of χ and f can be defined as

$$\chi_f(x) := \chi(f(x)) = \xi_p^{\mathrm{Tr}_p^q(f(x))}.$$

Definition 2.3. Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. The *Walsh transform* of f at $\omega \in \mathbb{F}_q^n$ is the Fourier transform $\widehat{\chi_f}$ of χ_f defined as

$$\begin{aligned} \widehat{\chi_f} : \ & \mathbb{F}_q^n \to \mathbb{C} \\ & \omega \longmapsto \widehat{\chi_f}(\omega) = \sum_{x \in \mathbb{F}_q^n} \chi_f(x)\overline{\chi}(\omega \cdot x), \end{aligned} \tag{2.7}$$

where $\chi : \mathbb{F}_q \to \mathbb{C}$ is any non-trivial additive character of $\mathbb{F}_q$ in (2.6) and "$\cdot$" denotes an inner product (for instance, the usual inner product) over $\mathbb{F}_q^n$.

It is worth mentioning that (2.7) can also be given without the conjugate of χ. We should also remark that f is constant if and only if $\widehat{\chi_f}(\omega) = 0$ at any nonzero $\omega \in \mathbb{F}_{q^n}$ (see, e.g., [66]). If $\mathbb{F}_q^n$ is identified with $\mathbb{F}_{q^n}$, we can take $\omega \cdot x = \mathrm{Tr}_q^{q^n}(\omega x)$, and the *Walsh transform* of f at $\omega \in \mathbb{F}_{q^n}$ is

$$\widehat{\chi_f}(\omega) = \sum_{x \in \mathbb{F}_{q^n}} \xi_p^{\mathrm{Tr}_p^q(f(x)) - \mathrm{Tr}_p^{q^n}(\omega x)}.$$

The set of complex values $\widehat{\chi_f}(\omega)$, called the *Walsh coefficient* of f at point ω, for all $\omega \in \mathbb{F}_{q^n}$ is called the *Walsh spectrum* of f. The *Walsh support* of f is the set

$$\{\omega \in \mathbb{F}_{q^n} : \widehat{\chi_f}(\omega) \neq 0\},$$

denoted by $\mathrm{Supp}(\widehat{\chi_f})$ and $\mathcal{N}_{\widehat{\chi_f}} = \#\mathrm{Supp}(\widehat{\chi_f})$, and obviously, $\mathcal{N}_{\widehat{\chi_f}} \leq q^n$.

We now give some strong properties of the Fourier transform of a complex valued function from $\mathbb{F}_q^n$ to $\mathbb{C}$.

Lemma 2.3. *Let $G : \mathbb{F}_q^n \to \mathbb{C}$ be a function and let $\widehat{G} : \mathbb{F}_q^n \to \mathbb{C}$ be its Fourier transform. Then $\widehat{\widehat{G}}(u) = q^n G(-u)$ for all $u \in \mathbb{F}_q^n$.*

Proof. The Fourier transform $\widehat{\widehat{G}}$ of $\widehat{G}$ at $\alpha \in \mathbb{F}_q^n$ is obtained by

$$\begin{aligned} \widehat{\widehat{G}}(\alpha) &= \sum_{v \in \mathbb{F}_q^n} \widehat{G}(v)\chi(-v \cdot \alpha) = \sum_{v \in \mathbb{F}_q^n} \sum_{u \in \mathbb{F}_q^n} G(u)\chi(-v \cdot u)\chi(-v \cdot \alpha) \\ &= \sum_{u \in \mathbb{F}_q^n} G(u) \sum_{v \in \mathbb{F}_q^n} \chi(-v \cdot (u + \alpha)) = q^n G(-\alpha) \end{aligned}$$

since $\sum_{v\in\mathbb{F}_q^n}\xi_p^{\mathrm{Tr}_p^{q^n}(-v(u+\alpha))}=\begin{cases} q^n & \text{if } u=-\alpha,\\ 0 & \text{if } u\neq -\alpha.\end{cases}$ □

It easily follows from Lemma 2.3 that for all $u\in\mathbb{F}_q^n$

$$G(-u)=\frac{1}{q^n}\sum_{v\in\mathbb{F}_q^n}\widehat{G}(v)\overline{\chi}(v\cdot u).$$

This suggests that $G(u)=0$ for all $u\in\mathbb{F}_q^n$ if and only if $\widehat{G}(v)=0$ for all $v\in\mathbb{F}_q^n$. In the light of the above results, we have the following strong property of the Fourier transform.

Lemma 2.4. *Let $G_1, G_2:\mathbb{F}_q^n\to\mathbb{C}$ be two functions. Then*

$$G_1(u)=G_2(u),\ \forall u\in\mathbb{F}_q^n \Longleftrightarrow \widehat{G}_1(v)=\widehat{G}_2(v),\ \forall v\in\mathbb{F}_q^n.$$

Next we recall the convolution of two complex valued functions (see [66, Definition 10.1.18]).

Definition 2.4. Let G_1 and G_2 be two functions from $\mathbb{F}_q^n$ to $\mathbb{C}$. The convolution of G_1 and G_2 is the map from $\mathbb{F}_q^n$ to $\mathbb{C}$, at $a\in\mathbb{F}_q^n$, defined as

$$(G_1\otimes G_2)(a)=\sum_{x\in\mathbb{F}_q^n}G_1(a-x)G_2(x).$$

The convolution theorem of Fourier analysis states that the Fourier transform of a convolution of two functions is the ordinary product of their Fourier transforms (see [66, Theorem 10.1.19]).

Theorem 2.1. *Let G_1 and G_2 be two functions from $\mathbb{F}_q^n$ to $\mathbb{C}$. Then, we have $\widehat{G_1\otimes G_2}=\widehat{G_1}\widehat{G_2}$, and also $\widehat{G_1}\otimes\widehat{G_2}=q^n\widehat{G_1G_2}$.*

Proof. Applying the Fourier transform to the convolution of G_1 and G_2 at point $v\in\mathbb{F}_q^n$, we obtain

$$\begin{aligned}(\widehat{G_1\otimes G_2})(v) &= \sum_{u\in\mathbb{F}_q^n}(G_1\otimes G_2)(u)\chi(-v\cdot u)\\ &= \sum_{u\in\mathbb{F}_q^n}\sum_{t\in\mathbb{F}_q^n}G_1(t)G_2(u-t)\chi(-v\cdot u)\\ &= \sum_{t\in\mathbb{F}_q^n}G_1(t)\chi(-v\cdot t)\sum_{u\in\mathbb{F}_q^n}G_2(u-t)\chi(-v\cdot(u-t))\\ &= \widehat{G_1}(v)\widehat{G_2}(v),\end{aligned}$$

that is, $\widehat{G_1 \otimes G_2} = \widehat{G_1}\widehat{G_2}$. To show the next relation, apply the Fourier transform to $\widehat{G_1} \otimes \widehat{G_2}$. Then, by the first relation, for all $u \in \mathbb{F}_q^n$ we have

$$(\widehat{\widehat{G_1} \otimes \widehat{G_2}})(u) = \widehat{\widehat{G_1}}(u)\widehat{\widehat{G_2}}(u) = q^{2n}G_1(-u)G_2(-u),$$

where the second equality follows from Lemma 2.3. Next, applying again the Fourier transform to them, for all $u \in \mathbb{F}_q^n$ we obtain

$$q^{2n}\widehat{G_1G_2}(-u) = (\widehat{\widehat{G_1} \otimes \widehat{G_2}})(u) = q^n(\widehat{G_1} \otimes \widehat{G_2})(-u),$$

where the second equality follows from Lemma 2.3. Hence the proof is complete. □

2.4 Some Tools of a Function

In this section, we introduce some useful tools of a function such as its Walsh power moments, derivative, balanced-ness, linear translator and autocorrelation function, which will be frequently used in the sequel to characterize plateaued (vectorial) functions.

The Walsh Power Moments. The notion of even power moments of the Walsh transform (for simplicity, we call it as the Walsh power moments) of a p-ary function was introduced by Mesnager [55]. This notion can be also given for a q-ary function. For any nonnegative integer i, the Walsh power moment of a q-ary function f is defined as

$$S_i(f) = \sum_{\omega \in \mathbb{F}_q^n} |\widehat{\chi_f}(\omega)|^{2i}$$

with the convention that $S_0(f) = q^n$. It is a well known fact that $S_1(f) = q^{2n}$, which is known as *the Parseval identity*. We now make a preliminary but useful remark: for every nonnegative integers A and i, we have

$$\sum_{\omega \in \mathbb{F}_{q^n}} \left(|\widehat{\chi}_f(\omega)|^2 - A\right)^2 |\widehat{\chi}_f(\omega)|^{2i} \quad = S_{i+2}(f) - 2AS_{i+1}(f) + A^2S_i(f) \geq 0.$$

Derivative. The definition of derivative of a q-ary function is given as follows (see, e.g., [28, 57]).

Definition 2.5. Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. The derivative (first-order derivative) of f in the direction of $a \in \mathbb{F}_q^n$ is the map $\mathcal{D}_a f$ from $\mathbb{F}_q^n$ to $\mathbb{F}_q$ defined by

$$\mathcal{D}_a f(x) = f(x+a) - f(x).$$

The second-order derivative of f in the direction of $(a, b) \in \mathbb{F}_{q^n}^2$ is given as $\mathcal{D}_b\mathcal{D}_a f(x) = f(x+a+b)-f(x+a)-f(x+b)+f(x)$. By the definition of derivative, for $(a, b) \in \mathbb{F}_{q^n}^2$ we readily have that $\mathcal{D}_b\mathcal{D}_a f(x) = \mathcal{D}_a\mathcal{D}_b f(x)$ for every $x \in \mathbb{F}_{q^n}$.

For a vectorial function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$, the first-order derivative $\mathcal{D}_a F$ in the direction of $a \in \mathbb{F}_{p^n}$ is the map from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ defined as $\mathcal{D}_a F(x) = F(x + a) - F(x)$, and its second-order derivative in the direction of $(a, b) \in \mathbb{F}_{p^n}^2$ is given as

$$\mathcal{D}_b\mathcal{D}_a F(x) = F(x + a + b) - F(x + a) - F(x + b) + F(x).$$

By the definition of derivative, $\mathcal{D}_b\mathcal{D}_a F(x) = \mathcal{D}_a\mathcal{D}_b F(x)$ for all $x \in \mathbb{F}_{p^n}$.

Linear Translator. The notion of linear translator for a q-ary function is given as follows (see [47, 57]).

Definition 2.6. Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. A nonzero element $\alpha \in \mathbb{F}_q^n$ is called a *b-linear translator* for f if

$$f(x + u\alpha) - f(x) = ub$$

holds for all $x \in \mathbb{F}_q^n$, $u \in \mathbb{F}_q$ and a fixed $b \in \mathbb{F}_q$. In other words, f is said to have a *linear translator* if there exists a nonzero $\alpha \in \mathbb{F}_q^n$ such that $f(x + u\alpha) - f(x) = u(f(\alpha)-f(0))$ for all $x \in \mathbb{F}_q^n$ and $u \in \mathbb{F}_q$. The set of linear translators of f is denoted by $\mathcal{L}_f$.

In particular, when $q = 2$, $\alpha \in \mathbb{F}_2^n$ is said to be *b-linear structure* for the Boolean function f if $f(x + \alpha) + f(x) = b$ holds for all $x \in \mathbb{F}_2^n$ and a fixed $b \in \mathbb{F}_2$. Note that if α is b-linear structure of f, then necessarily $b = f(\alpha) - f(0)$. The notions of linear translators and derivatives are related. The linear kernel of f is the linear subspace of vectors b such that $\mathcal{D}_b f$ is a constant function. In fact, any element of the linear kernel of f is a linear translator of f.

Balanced-ness. Cryptographic functions should be balanced to avoid statistical dependence between the plain-text (input) and the cipher-text (output) in the stream

cipher and to prohibit cryptographic distinguishing attacks. However, cryptographic functions having maximum nonlinearity cannot be balanced (for instance, bent functions). A balanced Boolean function is the function whose output yields as many zeros as ones over its input set. For q-ary functions and vectorial functions, the balanced-ness can be given as follows.

Definition 2.7. [28] Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. Then f is said to be *balanced (or permutation polynomial)* over $\mathbb{F}_q$ if $\#\{x \in \mathbb{F}_q^n : f(x) = k\} = q^{n-1}$ for each $k \in \mathbb{F}_q$ i.e., f takes every element of $\mathbb{F}_q$ the same number q^{n-1} of pre-images.

Definition 2.8. [6] Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$. Then F is called *balanced* over $\mathbb{F}_{p^m}$ if F takes every element of $\mathbb{F}_{p^m}$ the same number p^{n-m} of pre-images.

It is easy to see that a vectorial function is balanced if and only if all of its nonzero component functions are balanced.

The Autocorrelation Function. The autocorrelation function of a q-ary function can be defined by its first-order derivative (see, e.g., [46]).

Definition 2.9. Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. Then, the autocorrelation function of a q-ary function f is the map from $\mathbb{F}_q^n$ to $\mathbb{C}$ defined as

$$\Delta_f(a) = \sum_{x \in \mathbb{F}_q^n} \chi(\mathcal{D}_a f(x))$$

for all $a \in \mathbb{F}_q^n$, where χ is a non-trivial additive character of $\mathbb{F}_q$ in (2.6).

We end this section by proving the following properties of the Walsh transform and the autocorrelation function, which will be used in the sequel. They can be easily obtained by using the properties of additive character of $\mathbb{F}_q$ (see Lemma 2.2).

Proposition 2.2. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. Then*

i.) *f is balanced if and only if $\widehat{\chi_f}(0) = 0$.*

ii.) *$\widehat{\overline{\chi_f}}(\omega) = \overline{\widehat{\chi_f}(-\omega)}$ for all $\omega \in \mathbb{F}_q^n$.*

iii.) *$\widehat{\chi_{\mathcal{D}_a f}}(0) = \Delta_f(a)$ for all $a \in \mathbb{F}_q^n$.*

iv.) *$\Delta_f(a) = \overline{\Delta_f}(-a)$ for all $a \in \mathbb{F}_q^n$.*

v.) $|\widehat{\chi_f}(\omega)|^2 = \widehat{\Delta_f}(\omega)$ *for all* $\omega \in \mathbb{F}_q^n$.

vi.) $|\widehat{\chi_f}(0)|^2 = \sum_{a\in\mathbb{F}_q^n} \Delta_f(a)$.

Proof. *i.)* A function f is balanced if and only if $\sum_{x\in\mathbb{F}_q^n} \xi_p^{\mathrm{Tr}_p^q(f(x))} = 0$, namely,

$$\widehat{\chi_f}(0) = \sum_{x\in\mathbb{F}_q^n} \chi(f(x)) = \sum_{x\in\mathbb{F}_q^n} \xi_p^{\mathrm{Tr}_p^q(f(x))} = 0.$$

ii.) For all $\omega \in \mathbb{F}_q^n$,

$$\widehat{\overline{\chi_f}}(\omega) = \sum_{x\in\mathbb{F}_q^n} \overline{\chi}(f(x))\overline{\chi}(\omega\cdot x) = \sum_{x\in\mathbb{F}_q^n} \overline{\chi\big(f(x)\big)\overline{\chi}(-\omega\cdot x)} = \overline{\widehat{\chi_f}(-\omega)}.$$

iii.) Clearly, for all $a \in \mathbb{F}_q^n$,

$$\widehat{\chi_{\mathcal{D}_a f}}(0) = \sum_{x\in\mathbb{F}_q^n} \chi(\mathcal{D}_a f(x))\overline{\chi}(0\cdot x) = \sum_{x\in\mathbb{F}_q^n} \chi(\mathcal{D}_a f(x)) = \Delta_f(a).$$

iv.) Clearly, for all $a \in \mathbb{F}_q^n$,

$$\Delta_f(a) = \sum_{x\in\mathbb{F}_q^n} \chi(f(x+a) - f(x)) = \sum_{x\in\mathbb{F}_q^n} \overline{\chi(f(x) - f(x+a))} = \overline{\Delta_f}(-a),$$

where in the last equality we used the (bijective) change of variable $x \mapsto x - a$.

v.) Since $|z|^2 = z\overline{z}$ for $z \in \mathbb{C}$, for all $\omega \in \mathbb{F}_q^n$, it easily follows that

$$\begin{aligned}
|\widehat{\chi_f}(\omega)|^2 &= \sum_{a\in\mathbb{F}_q^n} \chi(f(a) - \omega\cdot a) \sum_{b\in\mathbb{F}_q^n} \chi(-f(b) + \omega\cdot b) \\
&= \sum_{a,b\in\mathbb{F}_q^n} \chi(f(a) - f(b))\overline{\chi}(\omega\cdot(a-b)) \\
&= \sum_{a\in\mathbb{F}_q^n} \sum_{b\in\mathbb{F}_q^n} \chi(f(a+b) - f(b))\overline{\chi}(\omega\cdot a) \\
&= \sum_{a\in\mathbb{F}_q^n} \Delta_f(a)\overline{\chi}(\omega\cdot a) = \widehat{\Delta_f}(\omega),
\end{aligned}$$

where in the third equality we used the (bijective) change of variable $a \mapsto a+b$.

vi.) This follows from (*v*) by setting $\omega = 0$.

□

2.5 Bent, Partially Bent and Plateaued Functions over Finite Fields

In this section, we give the notions of significant cryptographic functions, which have various useful cryptographic properties.

To begin with, we recall the notion of the Walsh transform of a p-ary function $f : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_p$. The Walsh transform of f at point $\omega \in \mathbb{F}_{p^n}$ is defined by:

$$\widehat{\chi_f}(\omega) = \sum_{x \in \mathbb{F}_{p^n}} \xi_p{}^{f(x) - \mathrm{Tr}_p^{p^n}(\omega x)}.$$

In the case of $p = 2$, the Walsh transform of a Boolean function f at point $\omega \in \mathbb{F}_{2^n}$ is given as

$$\widehat{\chi_f}(\omega) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x) + \mathrm{Tr}_2^{2^n}(\omega x)}.$$

Bent functions were introduced by Rothaus [72] in characteristic 2 and generalized to any residue class ring by Kumar et al. [46].

Definition 2.10. Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ and let n be an even integer. Then, f is called a *Boolean bent function* if for every $\omega \in \mathbb{F}_{2^n}$, we have $\widehat{\chi_f}(\omega) = \pm 2^{\frac{n}{2}}$.

We now give the definition of a generalized bent function over a finite field.

Definition 2.11. Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then, f is *p-ary bent* if for every $\omega \in \mathbb{F}_{p^n}$, we have $|\widehat{\chi_f}(\omega)|^2 = p^n$.

Remark 2.2. A function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is p-ary bent if and only if the derivative $\mathcal{D}_a f$ is balanced for all nonzero $a \in \mathbb{F}_{p^n}$.

Remark 2.3. A function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is *linear* if and only if $f(x+y) = f(x) + f(y)$ for all $x, y \in \mathbb{F}_{p^n}$. A function $g : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is *affine* if and only if $g = f + a$ where f is a linear function and a is a constant.

As an extension of bent functions, Carlet [12] introduced a superclass: the notion of *partially bent functions* whose elements are in the form $f(x, y) = g(x) + h(y)$ where g is a bent function on $\mathbb{F}_{2^k}$ and h is an affine function on $\mathbb{F}_{2^{n-k}}$. This notion has been generalized to arbitrary characteristic (see, e.g., [25]).

Definition 2.12. Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then, f is called *p-ary partially bent* if the derivative $\mathcal{D}_a f$ is either balanced or constant for all $a \in \mathbb{F}_{p^n}$.

Remark 2.4. Any p-ary bent and quadratic functions are p-ary partially bent functions.

As an extension of partially bent functions, Zheng and Zhang [78] introduced plateaued functions in characteristic 2.

Definition 2.13. Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ and s be an integer with $0 \leq s \leq n$. Then, f is called an *s-plateaued Boolean function* if $\widehat{\chi_f}(\omega) \in \{0, \pm 2^{(n+s)/2}\}$ for all $\omega \in \mathbb{F}_{2^n}$, where $n + s$ is an even integer.

Plateaued Boolean functions have been generalized to arbitrary characteristic and they are called *p-ary plateaued functions* (see, e.g., [23, 55]).

Definition 2.14. Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then, f is called *p-ary plateaued* if its absolute Walsh transform takes only one nonzero value μ (also possibly the value 0), which is called *the amplitude* of f.

For any n-variable p-ary plateaued function f of the amplitude μ, the Parseval identity implies that $p^{2n} = \mu^2 \mathcal{N}_{\widehat{\chi_f}}$ where

$$\mathcal{N}_{\widehat{\chi_f}} = \#\{\omega \in \mathbb{F}_{p^n} : |\widehat{\chi_f}(\omega)|^2 = \mu^2\}.$$

Since p is a prime and $\mathcal{N}_{\widehat{\chi_f}} \leq p^n$, we get $\mu^2 = p^t$ for $t \geq n$. Then, $1 \leq \mathcal{N}_{\widehat{\chi_f}} = p^{2n-t} \leq p^n$ gives $t = n + s$ for an integer s with $0 \leq s \leq n$. Namely, we have $\mu^2 = p^{n+s}$ with $0 \leq s \leq n$. In the light of these results, f is said to be a *p-ary s-plateaued function* if for every $\omega \in \mathbb{F}_{p^n}$, we have

$$|\widehat{\chi_f}(\omega)|^2 \in \{0, p^{n+s}\},$$

where s is an integer with $0 \leq s \leq n$. From now on, s is an integer with $0 \leq s \leq n$ for s-plateaued functions unless otherwise stated. We point out that a bent function is 0-plateaued and an affine function is n-plateaued.

The absolute Walsh distribution of plateaued functions follows from the Parseval identity (see, e.g., [55]).

Lemma 2.5. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be an s-plateaued function. Then for $\omega \in \mathbb{F}_{p^n}$, $|\widehat{\chi_f}(\omega)|^2$ takes p^{n-s} times the value p^{n+s} and $p^n - p^{n-s}$ times the value 0.*

In fact, in characteristic 2, the Walsh distribution of plateaued Boolean functions is given in the following lemma (see, e.g., [11] in the case of a quadratic Boolean function).

Lemma 2.6. *Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ be an s-plateaued Boolean function with $f(0) = 0$ and $n + s$ is an even integer. Then for $\omega \in \mathbb{F}_{2^n}$, the Walsh distribution of f is given by*

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

Proof. Let A and B denote the multiplicities of the values $2^{\frac{n+s}{2}}$ and $-2^{\frac{n+s}{2}}$ in the Walsh spectrum of f, respectively. By Lemma 2.5, we have that $A + B = 2^{n-s}$ and the multiplicity of the value 0 in its Walsh spectrum is equal to $2^n - 2^{n-s}$. On the other hand, since $\sum_{\omega \in \mathbb{F}_{2^n}} \widehat{\chi_f}(\omega) = 2^n$, we have $A - B = 2^{\frac{n-s}{2}}$. By solving the two equations obtained above, the proof is complete. □

We end this section by giving an upper bound for the degrees of p-ary plateaued functions (see, e.g., [43]).

Remark 2.5. Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be s-plateaued. Then we have

$$\deg f \leq (p-1)\frac{n-s}{2} + 1$$

provided that $p > 1 + \frac{2}{n+s}$ (i.e., except when $p = 3$ and $n = 1$).

2.6 Linear Codes in Coding Theory

Coding theory is concerned with improving reliability of communication over noisy channels. This is achieved by adding redundancy to the messages in order to detect or even correct the transmission errors. The most significant class of the codes in coding theory is the class of linear codes, which have been exhaustively studied due to their various applications. For further reading on coding theory, we send the reader to [42].

Linear Codes. Let p be a prime number and n be a positive integer. A linear code $\mathcal{C}$ of length n and dimension k over $\mathbb{F}_p$ is a k-dimensional linear subspace of $\mathbb{F}_p^n$, denoted by $[n,k]_p$. Indeed, a linear code $\mathcal{C}$ of length n and dimension k over $\mathbb{F}_p$ with minimum Hamming distance d is denoted by $[n,k,d]_p$. It is worth noting that the minimum Hamming distance d detects the error correcting capability of $\mathcal{C}$. The elements of the linear code are called *codewords*. The minimum Hamming distance of the code is the minimum Hamming weight of its nonzero codewords. The Hamming weight of a codeword $\tilde{a} = (a_0, \ldots, a_{n-1}) \in \mathbb{F}_p^n$, denoted by $wt(\tilde{a})$, is the size of its support defined as

$$\mathrm{supp}(\tilde{a}) := \{0 \leq i \leq n-1 : a_i \neq 0\}.$$

Let A_w denote the number of codewords with Hamming weight w in $\mathcal{C}$ of length n. Then, $(1, A_1, \ldots, A_n)$ is the *weight distribution* of $\mathcal{C}$ and the polynomial $1 + A_1 y + \cdots + A_n y^n$ is called the *weight enumerator* of $\mathcal{C}$. The code $\mathcal{C}$ is called a t-*weight code* if the number of nonzero A_w in the weight distribution is t. The weight distribution of linear codes attracts considerable attention and has been widely studied in coding theory since it contains significant information for estimating the probability of error detection and correction.

The *dual code* of a linear code $\mathcal{C}$ is the linear code of length n and dimension $n-k$ over $\mathbb{F}_p$ defined by

$$\mathcal{C}^\perp = \{\tilde{b} \in \mathbb{F}_p^n : \tilde{b} \cdot \tilde{a} = \tilde{0} \text{ for all } \tilde{a} \in \mathcal{C}\},$$

where " $\cdot$ " is an inner product (for instance, Euclidean inner product) on $\mathbb{F}_p^n$. The dual code $\mathcal{C}^\perp$ is denoted by $[n, n-k, d^\perp]_p$, where $d^\perp$ denotes the minimum Hamming distance of $\mathcal{C}^\perp$.

Since a linear code has a basis, any of its codeword can be written as a linear combination of the basis vectors. A *generator matrix* G of a linear code $\mathcal{C}$ is a $k \times n$ matrix whose rows form a basis for $\mathcal{C}$, that is, the row vectors of G generate the linear subspace $\mathcal{C}$. A *generator matrix* H of the dual code $\mathcal{C}^\perp$ is an $(n-k) \times n$ matrix whose rows form a basis for the dual code $\mathcal{C}^\perp$, namely, the row vectors of H generate the linear subspace $\mathcal{C}^\perp$.

We now state the covering problem of linear codes.

The Covering Problem of Linear Codes. Let $\mathcal{C}$ be a linear $[n, k, d]_p$ code over $\mathbb{F}_p$. We say that a codeword $\tilde{a}$ covers a codeword $\tilde{b}$ if $\mathrm{supp}(\tilde{b}) \subset \mathrm{supp}(\tilde{a})$. If a nonzero codeword $\tilde{a}$ of a linear code $\mathcal{C}$ does not cover any other nonzero codeword of $\mathcal{C}$, then $\tilde{a}$ is called a *minimal codeword* of $\mathcal{C}$.

Definition 2.15. The *covering problem* of a linear code $\mathcal{C}$ is to find all minimal codewords of $\mathcal{C}$.

The covering problem is extremely difficult for general linear codes, but is easy for some particular linear codes (it has been solved only for a few special linear codes).

From [2, 3], when the Hamming weights of the codewords of a linear code $\mathcal{C}$ are too close to each other, then all nonzero codewords of $\mathcal{C}$ are minimal.

Lemma 2.7. *[2, 3] Let $\mathcal{C}$ be a linear code over $\mathbb{F}_p$. Then, all nonzero codewords of $\mathcal{C}$ are minimal if*

$$\frac{p-1}{p} < \frac{w_{\min}}{w_{\max}},$$

where $w_{\min}$ and $w_{\max}$ denote the minimum and maximum nonzero weights in $\mathcal{C}$, respectively.

In view of Lemma 2.7, the question arises: how to construct a linear code whose all nonzero codewords are minimal?

2.7 Application of the Linear Codes in Secret Sharing Schemes

In this section, we first describe secret sharing scheme, and then investigate the application of linear codes in secret sharing schemes. The following results are mainly quoted from the papers [17, 33, 35].

2.7.1 Secret Sharing Schemes

A secret sharing scheme consists of

- a dealer D and a group $\mathcal{P} = \{P_1, P_2, \ldots, P_{n-1}\}$ of $(n-1)$ participants;

- a secret space S;
- $n-1$ share spaces $S_1, S_2, \ldots, S_{n-1}$;
- a share computing procedure; and
- a secret recovering procedure.

The dealer D chooses a secret s from S, and computes a share, which belongs to S_i, of s (with the sharing computing procedure) for each participant P_i and then gives the share to P_i, where $1 \leq i \leq n-1$. A proper subset of the participants may be able to recover the secret s from their shares by the secret recovering procedure. Any set covering a set of participants who can recover the secret s can also recover s. The sharing computing procedure and the secret s are known only by D, while the secret recovering procedure is known by all the participants in $\mathcal{P}$.

Definition 2.16. A set of participants who can recover the secret s from their shares is called *an access set*. The set of all access sets is called *the access structure* of a secret sharing scheme. An access set is called *a minimal access set* if any of its proper subsets cannot recover s from their shares. Notice that a proper subset has less participants than this set. Hence, we take only an interest in the set of all minimal access sets, which is said to be as *the "nice" access structure* of a secret sharing scheme.

Remark 2.6. A secret sharing scheme has the monotone access structure if any superset of any access set is also an access set. In such a secret sharing scheme, the access structure is fully characterized by its minimal access sets.

There are a number of methods to construct secret sharing schemes, one of which is based on linear codes in coding theory, which is now described in the following subsection.

2.7.2 A Construction of Secret Sharing Schemes from the Linear Codes

The connection between Shamir's secret sharing scheme and the Reed-Solomon codes was given in 1981 [53] and since then, the construction of the secret sharing schemes

from linear codes have been widely studied. In fact, every linear code $\mathcal{C}$ can be used to construct secret sharing scheme and generates a pair of secret sharing schemes, based on $\mathcal{C}$ and its dual code $\mathcal{C}^{\perp}$. But, the following two essential problems are unavoidable in the secret sharing scheme based on a linear code:

- How can one find the access structure of the secret sharing scheme based on a linear code?
- How can one construct a linear code such that the secret sharing scheme based on the dual code has a nice access structure, while minimizing information rate?

The first question is equivalent to the covering problem of the linear codes (see Remark 2.7). The second question depends on solutions to the first question, and turns out to be difficult in general.

There are several ways to use linear codes in the construction of secret sharing schemes. In 1993, Massey [51, 52] introduced the following construction of secret sharing schemes using linear error-correcting codes. Given a linear $[n, k, d]_p$ code $\mathcal{C}$, its $k \times n$ generator matrix G is denoted by

$$G = [\mathbf{g}_0, \mathbf{g}_1, \ldots, \mathbf{g}_{n-1}].$$

In the secret sharing scheme based on $\mathcal{C}$, the secret s is an element of $\mathbb{F}_p$. In order to compute the shares with respect to s, the dealer D chooses randomly a vector $\mathbf{u} = (u_0, u_1, \ldots, u_{k-1}) \in \mathbb{F}_p^k$ such that $s = \mathbf{u}\mathbf{g}_0$, which is an inner product of two vectors. Notice that there exist p^{k-1} such vectors $\mathbf{u} \in \mathbb{F}_p^k$. The dealer D computes the corresponding codeword as

$$\mathbf{t} = (t_0, t_1, \ldots, t_{n-1}) = \mathbf{u}G,$$

which is $(\mathbf{u}\mathbf{g}_0, \mathbf{u}\mathbf{g}_1, \ldots, \mathbf{u}\mathbf{g}_{n-1})$. The dealer D then assigns t_i to party P_i as share for all $1 \leq i \leq n-1$. Now we introduce the secret recovering procedure. Notice that the secret s is $t_0 = \mathbf{u}\mathbf{g}_0$. It is easy to see that a set of shares $\{t_{i_1}, t_{i_2}, \ldots, t_{i_m}\}$ recovers the secret s if and only if $\mathbf{g}_0$ is a linear combination of $\mathbf{g}_{i_1}, \mathbf{g}_{i_2}, \ldots, \mathbf{g}_{i_m}$.

Lemma 2.8. *[51] Let G be a generator matrix of a linear $[n, k, d]_p$ code $\mathcal{C}$. In the secret sharing scheme based on $\mathcal{C}$, a set of shares $\{t_{i_1}, t_{i_2}, \ldots, t_{i_m}\}$ determines the*

secret s if and only if there exists a codeword

$$(1, 0, \ldots, 0, c_{i_1}, 0, \ldots, 0, c_{i_m}, 0, \ldots, 0) \tag{2.8}$$

in the dual code $\mathcal{C}^\perp$, where $c_{i_j} \neq 0$ for at least one j, $1 \leq i_2 < \cdots < i_m \leq n-1$, and $1 \leq m \leq n-1$.

If there exists a codeword as in (2.8) in the dual code $\mathcal{C}^\perp$, then $\mathbf{g}_0$ is a linear combination of the elements $g_{i_1}, g_{i_2}, \ldots, g_{i_m}$, i.e., we have $\mathbf{g}_0 = \sum_{j=1}^{m} x_j g_{i_j}$. Hence, the secret s can be recovered as

$$s = \sum_{j=1}^{m} x_j t_{i_j}.$$

Remark 2.7. In the light of Lemma 2.8, clearly there is a one-to-one correspondence between the set of minimal access sets of the secret sharing scheme based on $\mathcal{C}$ and the set of minimal codewords of the dual code $\mathcal{C}^\perp$ whose first coordinate is 1. The other nonzero coordinates of these codewords correspond to the participants in the minimal access set.

In view of Remark 2.7, to find the access structure of the secret sharing scheme based on $\mathcal{C}$, it is enough to find all minimal codewords whose first coordinate is 1, i.e., a subset of the set of all minimal codewords of the dual code $\mathcal{C}^\perp$. Notice that in almost all cases we should in any case find the set of all minimal codewords of the dual code $\mathcal{C}^\perp$.

The access structure of the secret sharing scheme based on a linear code is complicated in general, however it can be easily found in certain cases. The following theorem (see [17, 33, 77]) gives the access structure of the secret sharing scheme based on a linear code.

Theorem 2.2. *Let $\mathcal{C}$ be a linear $[n, k, d]_p$ code over $\mathbb{F}_p$ with the generator matrix $G = [\mathbf{g}_0, \mathbf{g}_1, \ldots, \mathbf{g}_{n-1}]$. We denote by $d^\perp$ the minimum Hamming distance of its dual code $\mathcal{C}^\perp$. If all nonzero codewords of $\mathcal{C}$ are minimal, then in the secret sharing scheme based on the dual code $\mathcal{C}^\perp$, the number of participants is $n-1$, and there exist p^{k-1} minimal access sets.*

- *If $d^\perp = 2$, the access structure is given as follows.*

- *If* $\mathbf{g}_i$, $1 \leq i \leq n-1$, *is a multiple of* $\mathbf{g}_0$, *then* P_i *must be in all minimal access sets. Such* P_i *is called a dictatorial participant.*
- *If* $\mathbf{g}_i$, $1 \leq i \leq n-1$, *is not a multiple of* $\mathbf{g}_0$, *then* P_i *must be in* $(p-1)p^{k-2}$ *out of* p^{k-1} *minimal access sets.*

- *If* $d^\perp \geq 3$, *for any fixed* $1 \leq t \leq \min\{k-1, d^\perp - 2\}$, *every set of* t *participants is involved in* $(p-1)^t p^{k-(t+1)}$ *out of* p^{k-1} *minimal access sets.*

The minimum Hamming distance d of $\mathcal{C}$ gives the lower bound $d-1$ for the size of any minimal access set, while the minimum Hamming distance $d^\perp$ of $\mathcal{C}^\perp$ indicates the extent of democracy of the secret sharing scheme. But, there is a trade-off between them, i.e., $d + d^\perp \leq n + 2$, with an equality if and only if $\mathcal{C}$ is maximum-distance separable (MDS).

Remark 2.8. The shares for the participants depend on the choice of the generator matrix G of the code $\mathcal{C}$. However, the choice of G does not affect the access structures of the secret sharing schemes. Thus, we call it the secret sharing scheme based on $\mathcal{C}$ without mentioning G.

We finally remark that the general construction of the secret sharing scheme based on a linear code is described in this section. In Section 6.4, we consider the secret sharing schemes based on the dual codes of the constructed linear codes.

CHAPTER 3

EXPLICIT CHARACTERIZATIONS FOR PLATEAUED-NESS OF (VECTORIAL) FUNCTIONS OVER $\mathbb{F}_P$

Plateaued functions have appealed great interest since their introduction in the literature due to their various desirable cryptographic properties and applications in the sequence theory and coding theory. Several researchers obtained some important results about them and introduced new tools to better understand their structure and to design such functions. However, they have not yet been studied in detail in a general framework in view of their importance. Their structure is still more difficult to characterize and little is known about these functions already in characteristic 2 and still more in arbitrary characteristic. To fill a little the gap between the interest of the notion of these functions and our knowledge on it, we provide various tools to handle the plateaued-ness property of (vectorial) functions. In this chapter, we mainly make use of the value distribution of their derivatives, even power moments of their Walsh transform and their autocorrelation functions in order to characterize bent and plateaued (vectorial) functions.

The objective of this chapter is to obtain a large number of characterizations of bent and plateaued (vectorial) p-ary functions in terms of the value distribution of their second-order (also first-order) derivatives, Walsh power moments and autocorrelation functions of p-ary functions. The obtained characterizations may be related to each other, however they provide complementary information on these functions. We believe that they are rather useful to clarify the structure of plateaued functions for their future construction.

The presented results in this chapter appear in [20, 62, 63, 64].

We begin with the following applicable tools, which will be frequently used in the sequel. Let $f : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_p$ be a p-ary function. For any nonnegative integer i, even power moments of the Walsh transform of f is defined as

$$S_i(f) = \sum_{\omega \in \mathbb{F}_{p^n}} |\widehat{\chi_f}(\omega)|^{2i}$$

with $S_0(f) = p^n$. For every nonnegative integers A and i, we have

$$\sum_{\omega \in \mathbb{F}_{p^n}} \Big(|\widehat{\chi}_f(\omega)|^2 - A\Big)^2 |\widehat{\chi}_f(\omega)|^{2i} \ = S_{i+2}(f) - 2AS_{i+1}(f) + A^2 S_i(f) \geq 0. \quad (3.1)$$

For positive integers i and $A = p^{n+s}$ with an integer $1 \leq s \leq n$, the inequality (3.1) becomes an equality if and only if f is p-ary s-plateaued. For $i = 1$, f is p-ary s-plateaued if and only if $S_3(f) + p^{4n+2s} = 2p^{n+s}S_2(f)$. For every integer A and every nonnegative integers i and j, we have

$$\sum_{\omega \in \mathbb{F}_{p^n}} \Big(|\widehat{\chi_f}(\omega)|^2 - A\Big)^{2j} |\widehat{\chi_f}(\omega)|^{2i} \geq 0. \quad (3.2)$$

For $A = p^{n+s}$ with $1 \leq s \leq n$ and positive integers i and j, the inequality (3.2) becomes an equality if and only if f is s-plateaued. For $i = j = 1$, f is s-plateaued if and only if $S_3(f) + p^{4n+2s} = 2p^{n+s}S_2(f)$. For $i = 2$ and $j = 1$, f is s-plateaued if and only if

$$S_4(f) + p^{2n+2s}S_2(f) = 2p^{n+s}S_3(f).$$

The increment on i and/or j gives new relations between the next power moments of the Walsh transform of plateaued function. The autocorrelation function at $a \in \mathbb{F}_{p^n}$ of p-ary function f is defined as

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

For $G_1, G_2 : \mathbb{F}_{p^n} \to \mathbb{C}$, by Theorem 2.1, we have

$$\widehat{G_1} \otimes \widehat{G_2} = p^n \widehat{G_1 G_2}, \quad (3.3)$$

and by Lemma 2.4,

$$G_1(x) = G_2(x), \ \forall x \in \mathbb{F}_{p^n} \Longleftrightarrow \widehat{G}_1(\omega) = \widehat{G}_2(\omega), \ \forall \omega \in \mathbb{F}_{p^n}. \quad (3.4)$$

Here, for a p-ary function $f : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_p$ and a vectorial function $F : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^m}$, we introduce the following notations, which will be used in the sequel.

- $\mathrm{Supp}(\widehat{\chi_f}) = \{\omega \in \mathbb{F}_{p^n} \mid \widehat{\chi_f}(\omega) \neq 0\}$ and $\mathcal{N}_{\widehat{\chi_f}} = \#\mathrm{Supp}(\widehat{\chi_f})$.
- $\mathrm{Supp}(\Delta_f) = \{a \in \mathbb{F}_{p^n} \mid \Delta_f(a) \neq 0\}$ and $\mathcal{N}_{\Delta_f} = \#\mathrm{Supp}(\Delta_f)$.
- $\mathfrak{N}(f) = \#\{(a, b, x) \in \mathbb{F}_{p^n}^3 : \mathcal{D}_b\mathcal{D}_a f(x) = 0\}$.
- $\mathfrak{N}(F) = \#\{(a, b, x) \in \mathbb{F}_{p^n}^3 : \mathcal{D}_b\mathcal{D}_a F(x) = 0\}$.
- For $v \in \mathbb{F}_p$ and $x \in \mathbb{F}_{p^n}$, $\mathcal{N}_f(v; x) = \#\{(a, b) \in \mathbb{F}_{p^n}^2 : \mathcal{D}_b\mathcal{D}_a f(x) = v\}$.
- For $v \in \mathbb{F}_{p^m}$ and $x \in \mathbb{F}_{p^n}$, $\mathcal{N}_F(v; x) = \#\{(a, b) \in \mathbb{F}_{p^n}^2 : \mathcal{D}_b\mathcal{D}_a F(x) = v\}$.

We now state the well-known Hölder's Inequality, which will be frequently used in the sequel.

Theorem 3.1 (Hölder's Inequality)**.** *[73] Let $p_1, p_2 \in (1, \infty)$ with $\frac{1}{p_1} + \frac{1}{p_2} = 1$. Then, for all vectors $(x_1, x_2, \ldots, x_m), (y_1, y_2, \ldots, y_m) \in \mathbb{R}^m$ or $\mathbb{C}^m$, Hölder's Inequality states that*

$$\sum_{k=1}^{m} |x_k y_k| \leq \left(\sum_{k=1}^{m} |x_k|^{p_1} \right)^{\frac{1}{p_1}} \left(\sum_{k=1}^{m} |y_k|^{p_2} \right)^{\frac{1}{p_2}}.$$

The above inequality becomes an equality if and only if for every $k \in \{1, \ldots, m\}$

$$|x_k|^{p_1} = d|y_k|^{p_2}$$

for some $d \in \mathbb{R}^+$. In particular, if $p_1 = p_2 = 2$, then this is called the Cauchy-Schwarz Inequality.

In the following section, we characterize p-ary bent functions in terms of their Walsh power moments, second-order derivatives and autocorrelation functions.

3.1 Characterizations of p-Ary Bent Functions

We start by extending the following theorem for all even power moments of the Walsh transform of a p-ary function.

Theorem 3.2. *[55] Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then we have $p^{3n} \leq S_2(f)$, with an equality if and only if f is p-ary bent.*

A lower bound of even power moments of the Walsh transform of a function can be derived from Hölder's Inequality, whose equality case yields the following strong characterizations of bent functions.

Theorem 3.3. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then for every integer $i \geq 2$, we have*

$$p^{n(i+1)} \leq S_i(f),$$

where the equality holds for one (and hence for all) $i \geq 2$ if and only if f is p-ary bent.

Proof. By Theorem 3.1, putting $x_k = |\widehat{\chi_f}(\omega)|^2$ and $y_k = 1$ for all $\omega \in \mathbb{F}_{p^n}$, $1 \leq k \leq p^n$, with $p_1 = i$ and $p_2 = \frac{i}{i-1}$ where $i \geq 2$, we have

$$\sum_{\omega \in \mathbb{F}_{p^n}} |\widehat{\chi_f}(\omega)|^2 \leq \left(\sum_{\omega \in \mathbb{F}_{p^n}} |\widehat{\chi_f}(\omega)|^{2i} \right)^{\frac{1}{i}} \left(\sum_{\omega \in \mathbb{F}_{p^n}} 1 \right)^{\frac{i-1}{i}}, \tag{3.5}$$

that is, by the Parseval identity, $p^{2ni} \leq S_i(f) p^{n(i-1)}$ from which we conclude that $p^{n(i+1)} \leq S_i(f)$ for every integer $i \geq 2$.

By the equality case of Hölder's Inequality, for $i \geq 2$, the inequality (3.5) becomes an equality if and only if for every $\omega \in \mathbb{F}_{p^n}$, $|\widehat{\chi_f}(\omega)|^{2i} = d$, for some $d \in \mathbb{R}^+$, i.e., for every $\omega \in \mathbb{F}_{p^n}$, $|\widehat{\chi_f}(\omega)|^2$ is the same positive integer; equivalently, f is p-ary bent. □

Corollary 3.1. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then, f is p-ary bent if and only if $\mathcal{N}_{\Delta_f} = 1$; equivalently, $\max_{a \in \mathbb{F}_{p^n}^\star}(|\Delta_f(a)|) = 0$. Also, f is p-ary affine if and only if $\mathcal{N}_{\widehat{\chi_f}} = 1$.*

The sequence of the Walsh power moments of p-ary bent function is a simple geometric sequence.

Corollary 3.2. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be p-ary bent. Then for all positive integers i and j, we have $S_i(f) = p^{n(i+1)}$ and $S_i(f)S_j(f) = S_{i+1}(f)S_{j-1}(f)$.*

Proof. By the Walsh transform values of bent functions, we have

$$S_i(f) = \sum_{\omega \in \mathbb{F}_{p^n}} |\widehat{\chi_f}(\omega)|^{2i} = p^n(p^{ni}) = p^{n(i+1)}.$$

Then the following

$$\begin{aligned} S_i(f)S_j(f) &= p^{n(i+1)}p^{n(j+1)} = p^{n(i+j+2)}, \text{ and} \\ S_{i+1}(f)S_{j-1}(f) &= p^{n(i+2)}p^{nj} = p^{n(i+j+2)} \end{aligned}$$

are equal. Hence, the result clearly follows. □

The following link between the second-order derivative and the fourth power moment of the Walsh transform was given in [55] (in characteristic 2, see [13]).

Proposition 3.1. *[55] Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then,*

$$S_2(f) = p^n \sum_{a,b,x \in \mathbb{F}_{p^n}} \xi_p^{\mathcal{D}_a\mathcal{D}_b f(x)}.$$

The following is an immediate consequence of Theorem 3.2 and Proposition 3.1.

Corollary 3.3. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then we have*

$$p^{2n} \leq \sum_{a,b,x \in \mathbb{F}_{p^n}} \xi_p^{\mathcal{D}_a\mathcal{D}_b f(x)},$$

with an equality if and only if f is p-ary bent.

The following corollary can be readily given (see [46, Property 4]).

Corollary 3.4. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then*

$$p^{2n} \leq \sum_{a \in \mathbb{F}_{p^n}} |\Delta_f(a)|^2 \tag{3.6}$$

with an equality if and only if f is p-ary bent.

Proof. For any function f, $\Delta_f(0) = p^n$ and $|\Delta_f(a)| \geq 0$ for all $a \in \mathbb{F}_{p^n}^\star$. Hence, the bound in (3.6) holds for every function, and it is satisfied by p-ary bent functions because of the fact that f is p-ary bent if and only if $\Delta_f(a) = 0$ for all $a \in \mathbb{F}_{p^n}^\star$. □

We now give a link between the second-order derivative and autocorrelation function of a p-ary function.

Proposition 3.2. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then*

$$\sum_{a \in \mathbb{F}_{p^n}} |\Delta_f(a)|^2 = \sum_{a,b,x \in \mathbb{F}_{p^n}} \xi_p^{\mathcal{D}_a\mathcal{D}_b f(x)}.$$

Proof. Since $|z|^2 = z\overline{z}$ for $z \in \mathbb{C}$, clearly we have

$$\sum_{a\in\mathbb{F}_{p^n}} |\Delta_f(a)|^2 = \sum_{a\in\mathbb{F}_{p^n}} \left(\sum_{b\in\mathbb{F}_{p^n}} \xi_p^{\mathcal{D}_a f(b)} \sum_{x\in\mathbb{F}_{p^n}} \xi_p^{-\mathcal{D}_a f(x)} \right) = \sum_{a,b,x\in\mathbb{F}_{p^n}} \xi_p^{\mathcal{D}_a\mathcal{D}_b f(x)},$$

where in the second equality we used the bijective change of variable: $b \mapsto b+x$. □

In the light of Proposition 3.2, Corollaries 3.3 and 3.4 are equivalent. The next proposition is a direct consequence of Propositions 3.1 and 3.2.

Proposition 3.3. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then,*

$$S_2(f) = p^n \sum_{a\in\mathbb{F}_{p^n}} |\Delta_f(a)|^2.$$

The first characterization of Boolean bent functions in terms of their second-order derivatives was provided by Carlet and Prouff in [21]. Below, we give it with a different proof in arbitrary characteristic.

Theorem 3.4. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then we have for all $x \in \mathbb{F}_{p^n}$*

$$p^n \leq \sum_{a,b\in\mathbb{F}_{p^n}} \xi_p^{\mathcal{D}_a\mathcal{D}_b f(x)},$$

with an equality if and only if f is p-ary bent.

Proof. For all $x \in \mathbb{F}_{p^n}$, it is obvious that for $a = 0$, we have

$$\sum_{b\in\mathbb{F}_{p^n}} \xi_p^{\mathcal{D}_0\mathcal{D}_b f(x)} = p^n. \tag{3.7}$$

For all $x \in \mathbb{F}_{p^n}$, we have

$$\sum_{a\in\mathbb{F}_{p^n}^\star} \sum_{b\in\mathbb{F}_{p^n}} \xi_p^{\mathcal{D}_a\mathcal{D}_b f(x)} = \sum_{a\in\mathbb{F}_{p^n}^\star} \xi_p^{-\mathcal{D}_a f(x)} \sum_{b\in\mathbb{F}_{p^n}} \xi_p^{\mathcal{D}_a f(b)} \geq 0 \tag{3.8}$$

with an equality if and only if $\mathcal{D}_a f$ is balanced at $a \in \mathbb{F}_{p^n}^\star$, where we used the (bijective) change of variable: $b \mapsto b - x$. Combining (3.7) and (3.8), the proof is complete. □

The last aim of this section is to characterize bent functions in terms of the zeros of their second-order derivatives. To do this, we need the following results. For a

function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$, a corresponding function $f_\lambda := \lambda f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is defined as $x \mapsto \lambda f(x)$ for every $\lambda \in \mathbb{F}_p^\star$. Then for any $\lambda \in \mathbb{F}_p^\star$, we have $\mathcal{D}_b\mathcal{D}_a f_\lambda(x) = \lambda(\mathcal{D}_b\mathcal{D}_a f(x))$ at $(a, b) \in \mathbb{F}_{p^n}^2$ for every $x \in \mathbb{F}_{p^n}$.

Proposition 3.4. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ and let $\mathfrak{N}(f)$ be the size of the set $K = \{(a, b, x) \in \mathbb{F}_{p^n}^3 : \mathcal{D}_b\mathcal{D}_a f(x) = 0\}$. Then*

$$\sum_{\lambda \in \mathbb{F}_p^\star} S_2(\lambda f) = p^{n+1}\mathfrak{N}(f) - p^{4n}.$$

Proof. By Proposition 3.1, we have

$$\begin{aligned}\sum_{\lambda \in \mathbb{F}_p^\star} S_2(f_\lambda) &= \sum_{\lambda \in \mathbb{F}_p^\star} \Big(p^n \sum_{a,b,x \in \mathbb{F}_{p^n}} \xi_p^{\mathcal{D}_b\mathcal{D}_a f_\lambda(x)} \Big) \\ &= p^n \Big(\sum_{\lambda \in \mathbb{F}_p^\star} \sum_{(a,b,x) \in K} \xi_p^{\lambda\mathcal{D}_b\mathcal{D}_a f(x)} + \sum_{(a,b,x) \notin K} \sum_{\lambda \in \mathbb{F}_p^\star} \xi_p^{\lambda\mathcal{D}_b\mathcal{D}_a f(x)} \Big) \\ &= p^n \Big((p-1)\mathfrak{N}(f) - (p^{3n} - \mathfrak{N}(f)) \Big) = p^{n+1}\mathfrak{N}(f) - p^{4n},\end{aligned}$$

where in the third equality we used that $1 + \xi_p + \xi_p^2 + \cdots + \xi_p^{p-1} = 0$. □

From Theorem 3.2 and Proposition 3.4, we derive the following characterization of bent functions.

Theorem 3.5. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then, f is p-ary bent if and only if $\mathfrak{N}(f) = p^{2n} + p^{3n-1} - p^{2n-1}$.*

Proof. Clearly, f is p-ary bent if and only if f_λ is p-ary bent for every $\lambda \in \mathbb{F}_p^\star$. Hence, in view of Theorem 3.2, f is p-ary bent if and only if

$$\sum_{\lambda \in \mathbb{F}_p^\star} S_2(f_\lambda) = (p-1)p^{3n};$$

equivalently, by Proposition 3.4 we have $\mathfrak{N}(f) = p^{2n} + p^{3n-1} - p^{2n-1}$. □

3.2 Characterizations of p-Ary Plateaued Functions

This section provides many explicit characterizations of p-ary plateaued functions in terms of the value distribution of their second-order derivatives, even power moments of their Walsh transform and their autocorrelation functions. More precisely,

we extend the characterizations of plateaued Boolean functions given in [15, 21] to arbitrary characteristic and complete the given ones in [55]. We also obtain further new characterizations of plateaued functions in arbitrary characteristic.

3.2.1 Characterizations of p-Ary Plateaued Functions by their Derivatives

In this subsection, we make use of the value distribution of the second-order derivatives of p-ary functions in order to characterize p-ary plateaued functions.

The first characterization of plateaued Boolean functions in terms of their second-order derivatives was provided by Carlet and Prouff in [21]. We extend it to arbitrary characteristic in the next theorem with a different proof.

Theorem 3.6. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Set $\theta_f(x) = \sum_{a,b\in\mathbb{F}_{p^n}} \xi_p^{\mathcal{D}_b\mathcal{D}_a f(x)}$ for $x \in \mathbb{F}_{p^n}$. Then, f is p-ary s-plateaued if and only if for all $x \in \mathbb{F}_{p^n}$*

$$\theta_f(x) = p^{n+s}. \tag{3.9}$$

Proof. Put $\theta = p^{n+s}$. Then for all $x \in \mathbb{F}_{p^n}$, (3.9) holds if and only if

$$\sum_{a,b\in\mathbb{F}_{p^n}} \xi_p^{f(x+a+b)-f(x+a)-f(x+b)} = \theta\xi_p^{-f(x)}, \quad \forall x \in \mathbb{F}_{p^n}. \tag{3.10}$$

Put $a_1 = x + a$ and $b_1 = x + b$ for $a_1, b_1 \in \mathbb{F}_{p^n}$. Thus, (3.10) is equivalent to

$$\sum_{a_1,b_1\in\mathbb{F}_{p^n}} \xi_p^{f(a_1+b_1-x)-f(a_1)-f(b_1)} = \theta\xi_p^{-f(x)}, \quad \forall x \in \mathbb{F}_{p^n}. \tag{3.11}$$

Let the left-hand side of (3.11) be $G_1(x)$ and its right-hand side be $G_2(x)$ for all $x \in \mathbb{F}_{p^n}$, i.e., $G_1(x) = G_2(x)$ for all $x \in \mathbb{F}_{p^n}$. Then, their Fourier transforms at $\omega \in \mathbb{F}_{p^n}$ are

$$\begin{aligned}
\widehat{G}_1(\omega) &= \sum_{x\in\mathbb{F}_{p^n}} G_1(x)\xi_p^{-\mathrm{Tr}_p^{p^n}(\omega x)} = \sum_{x\in\mathbb{F}_{p^n}} \sum_{a_1,b_1\in\mathbb{F}_{p^n}} \xi_p^{f(a_1+b_1-x)-f(a_1)-f(b_1)}\xi_p^{-\mathrm{Tr}_p^{p^n}(\omega x)} \\
&= \sum_{a_1\in\mathbb{F}_{p^n}} \xi_p^{-f(a_1)-\mathrm{Tr}_p^{p^n}(\omega a_1)} \sum_{b_1\in\mathbb{F}_{p^n}} \xi_p^{-f(b_1)-\mathrm{Tr}_p^{p^n}(\omega b_1)} \\
&\sum_{x\in\mathbb{F}_{p^n}} \xi_p^{f(a_1+b_1-x)-\mathrm{Tr}_p^{p^n}(-\omega(a_1+b_1-x))} = (-\widehat{\chi_f})(\omega)(-\widehat{\chi_f})(\omega)\widehat{\chi_f}(-\omega),
\end{aligned}$$

and

$$\widehat{G}_2(\omega) = \sum_{x\in\mathbb{F}_{p^n}} G_2(x)\xi_p^{-\mathrm{Tr}_p^{p^n}(\omega x)} = \sum_{x\in\mathbb{F}_{p^n}} \theta\xi_p^{-f(x)-\mathrm{Tr}_p^{p^n}(\omega x)} = \theta(-\widehat{\chi_f})(\omega).$$

By Proposition 2.2, $(-\widehat{\chi_f})(\omega) = \overline{\widehat{\chi_f}(-\omega)}$ for all $\omega \in \mathbb{F}_{p^n}$. By (3.4), then (3.11) holds for all $x \in \mathbb{F}_{p^n}$ if and only if for all $\omega \in \mathbb{F}_{p^n}$

$$\widehat{\chi_f}(-\omega)\overline{\widehat{\chi_f}(-\omega)\widehat{\chi_f}(-\omega)} = \theta\overline{\widehat{\chi_f}(-\omega)}.$$

Therefore, (3.9) holds for all $x \in \mathbb{F}_{p^n}$ if and only if $|\widehat{\chi_f}(\omega)|^2 \in \{0, \theta\}$ for all $\omega \in \mathbb{F}_{p^n}$, where $\theta = p^{n+s}$, that is, f is p-ary s-plateaued. □

From Proposition 3.1 and Theorem 3.6, we have the following.

Corollary 3.5. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Set $\theta_f(x) = \sum_{a,b\in\mathbb{F}_{p^n}} \xi_p^{\mathcal{D}_b\mathcal{D}_a f(x)}$ for $x \in \mathbb{F}_{p^n}$. Then, f is p-ary plateaued if and only if $S_2(f) = p^{2n}\theta_f(x)$ for all $x \in \mathbb{F}_{p^n}$.*

Proof. Assume that f is p-ary plateaued. By Proposition 3.1,

$$S_2(f) = p^n \sum_{x\in\mathbb{F}_{p^n}} \theta_f(x).$$

Then by Theorem 3.6, $S_2(f) = p^n p^n \theta_f(x)$ for all $x \in \mathbb{F}_{p^n}$. Conversely, for all $x \in \mathbb{F}_{p^n}$ we have $\theta_f(x) = \theta$, where $\theta = p^{-2n}S_2(f)$. By Theorem 3.6, f is p-ary plateaued. □

Theorem 3.6 directly implies the following result.

Corollary 3.6. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. If f is s-plateaued, then*

$$\sum_{a,b,x\in\mathbb{F}_{p^n}} \xi_p^{\mathcal{D}_a\mathcal{D}_b f(x)} = p^{2n+s}. \tag{3.12}$$

The following is a direct consequnece of Theorem 3.2 and Proposition 3.1.

Corollary 3.7. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then, f is p-ary bent if and only if*

$$\sum_{a,b,x\in\mathbb{F}_{p^n}} \xi_p^{\mathcal{D}_a\mathcal{D}_b f(x)} = p^{2n}.$$

We now mention our mistake given in [57, 63].

Remark 3.1. The converse of Corollary 3.6 fails for integers $1 \leq s \leq n$, in general. In other words, the plateaued-ness of f cannot be checked only with the fourth power moment of its Walsh transform in general. Unfortunately, we had the wrong statement that the converse of Corollary 3.6 holds for integers $1 \leq s \leq n$ in [63, Corollary 4 and Theorem 4] (and hence, [57, Corollary 16.3.13 and Theorem 16.3.15]). We observed that it is wrong for integers $1 \leq s \leq n$, while it is correct for $s = 0$ as in Corollary 3.7. To see this, by MAGMA [5], we obtain a great number of examples, which satisfy (3.12) although they are not s-plateaued for $1 \leq s \leq n$. These examples motivate us to study further functions giving these counterexamples for the converse of Corollary 3.6 rather systematically, and we present our results in Chapter 4. Here we only give two such examples explicitly.

Example 3.1. *Let* $f(x) = \mathrm{Tr}_2^{2^5}(\zeta x^7 + \zeta^{13}x^{11} + \zeta^{18}x^{15})$*, where* $\mathbb{F}_{2^5}^\star = \langle\zeta\rangle$ *with* $\zeta^5 + \zeta^2 + 1 = 0$*. Then we have* $S_2(f) = 2^{16}$ *but* f *is not* 1*-plateaued function.*

Example 3.2. *Let* $f(x) = \mathrm{Tr}_3^{3^3}(\zeta x^4 + \zeta^3 x^5 + \zeta^{11}x^{11} + \zeta^{25}x^{13})$*, where* $\mathbb{F}_{3^3}^\star = \langle\zeta\rangle$ *with* $\zeta^3 + 2\zeta + 1 = 0$*. Then we have* $S_2(f) = 3^{10}$ *but* f *is not* 1*-plateaued function.*

For the next characterization of plateaued functions, we need the following lemma.

Lemma 3.1. *Let* $h : \mathbb{F}_{p^n} \times \mathbb{F}_{p^n} \to \mathbb{F}_p$ *and* s *be a nonnegative integer. For* $v \in \mathbb{F}_p$*, let* $\mathcal{N}_h(v)$ *be the size of the set* $\{(a, b) \in \mathbb{F}_{p^n}^2 : h(a, b) = v\}$*. Then, the following statements are equivalent:*

i.) $\displaystyle\sum_{a,b\in\mathbb{F}_{p^n}} \xi_p^{h(a,b)} = p^{n+s}$,

ii.) $\mathcal{N}_h(0) = p^{n+s} + p^{2n-1} - p^{n+s-1}$ *and* $\mathcal{N}_h(v) = p^{2n-1} - p^{n+s-1}$*, where* $v \in \mathbb{F}_p^\star$.

Proof. Assume that (*i*) holds. Then we have

$$\sum_{a,b\in\mathbb{F}_{p^n}} \xi_p^{h(a,b)} = \mathcal{N}_h(0) + \mathcal{N}_h(1)\xi_p + \mathcal{N}_h(2)\xi_p^2 + \cdots + \mathcal{N}_h(p-1)\xi_p^{p-1} = p^{n+s} \quad (3.13)$$

where $\mathcal{N}_h(v) = \#\{(a, b) \in \mathbb{F}_{p^n}^2 : h(a, b) = v\}$ for $v \in \mathbb{F}_p$. Recall that $1 + x + x^2 + \cdots + x^{p-1}$ is the minimal polynomial of ξ_p over the rational number field. It follows readily from (3.13) that there exists a nonnegative integer c such that $\mathcal{N}_h(0) = p^{n+s}+c$

and $\mathcal{N}_h(v) = c$, where $v \in \mathbb{F}_p^\star$ since

$$p^{n+s} + c(1 + \xi_p + \xi_p^2 + \cdots + \xi_p^{p-1}) = p^{n+s}.$$

Hence, since $\mathcal{N}_h(0) + \mathcal{N}_h(1) + \cdots + \mathcal{N}_h(p-1) = p^{2n}$, we have $c = p^{2n-1} - p^{n+s-1}$, that is, (*ii*) holds. Conversely, by (*ii*), clearly we get

$$\sum_{a,b \in \mathbb{F}_{p^n}} \xi_p^{h(a,b)} = p^{n+s} + (p^{2n-1} - p^{n+s-1})(1 + \xi_p + \cdots + \xi_p^{p-1}) = p^{n+s},$$

where we used that $1 + \xi_p + \xi_p^2 + \cdots + \xi_p^{p-1} = 0$. Thus, (*i*) holds. □

We deduce by Theorem 3.6 and Lemma 3.1 the following characterizations of plateaued functions via the value distribution of their second-order derivatives.

Theorem 3.7. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then, f is s-plateaued if and only if there exist two integers u_1 and u_2 such that $\mathcal{N}_f(0; x) = u_1$ and $\mathcal{N}_f(v; x) = u_2$ for every $v \in \mathbb{F}_p^\star$ and $x \in \mathbb{F}_{p^n}$.*

Proof. Assume that f is s-plateaued. Let x_0 be any chosen element of $\mathbb{F}_{p^n}$. Set $h(a,b) = \mathcal{D}_b\mathcal{D}_a f(x_0)$ for every $(a,b) \in \mathbb{F}_{p^n}^2$ and define $\mathcal{N}_f(v; x_0) = \#\{(a,b) \in \mathbb{F}_{p^n}^2 : h(a,b) = v\}$. By Theorem 3.6 and Lemma 3.1, we obtain $\mathcal{N}_f(0; x_0) = p^{n+s} + p^{2n-1} - p^{n+s-1}$ and $\mathcal{N}_f(v; x_0) = p^{2n-1} - p^{n+s-1}$ for $v \in \mathbb{F}_p^\star$. For each chosen element $x \in \mathbb{F}_{p^n}$, we can do the same process, and hence the assertion holds. Conversely, for every $x \in \mathbb{F}_{p^n}$ we have

$$\sum_{a,b \in \mathbb{F}_{p^n}} \xi_p^{\mathcal{D}_b\mathcal{D}_a f(x)} = \sum_{v \in \mathbb{F}_p} \mathcal{N}_f(v; x)\xi_p^v = u_1 + \sum_{v \in \mathbb{F}_p^\star} u_2 \xi_p^v = u_1 - u_2.$$

Put $\theta = u_1 - u_2$. Equivalently, for every $x \in \mathbb{F}_{p^n}$, by the (bijective) change of variables: $a \to a - x$ and $b \to b - x$,

$$\sum_{a,b \in \mathbb{F}_{p^n}} \xi_p^{f(a+b-x)-f(a)-f(b)} = \theta \xi_p^{-f(x)}. \tag{3.14}$$

We denote by $G_1(x)$ the left-hand side of (3.14) and by $G_2(x)$ its right-hand side, i.e., $G_1(x) = G_2(x)$ for every $x \in \mathbb{F}_{p^n}$. As in the proof of Theorem 3.6, their Fourier transforms are

$$\widehat{G}_1(\omega) = (-\widehat{\chi_f})(\omega)(-\widehat{\chi_f})(\omega)\widehat{\chi_f}(-\omega)$$

and $\widehat{G}_2(\omega) = \theta(-\widehat{\chi_f})(\omega)$ for every $\omega \in \mathbb{F}_{p^n}$. By Proposition 2.2, $(-\widehat{\chi_f})(\omega) = \overline{\widehat{\chi_f}(-\omega)}$ for every $\omega \in \mathbb{F}_{p^n}$. By (3.4), the equation (3.14) holds for every $x \in \mathbb{F}_{p^n}$ if and only if

$$\overline{\widehat{\chi_f}(\omega)}\ \overline{\widehat{\chi_f}(\omega)}\widehat{\chi_f}(\omega) = \theta\overline{\widehat{\chi_f}(\omega)},$$

that is, $|\widehat{\chi_f}(\omega)|^2 \in \{0, \theta\}$ for every $\omega \in \mathbb{F}_{p^n}$. Hence, by the Parseval identity, $\theta = p^{n+s}$, namely, f is s-plateaued with $0 \leq s \leq n$. □

This suggests a characterization of plateaued functions in terms of the number of the value distribution of their second-order derivatives.

Corollary 3.8. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then, f is s-plateaued if and only if for every $x \in \mathbb{F}_{p^n}$ and $v \in \mathbb{F}_p^\star$*

$$\mathcal{N}_f(v; x) = p^{2n-1} - p^{n+s-1}. \tag{3.15}$$

Proof. Assume that (3.15) holds. For any $x \in \mathbb{F}_{p^n}$, we have

$$\mathcal{N}_f(0; x) + \sum_{v \in \mathbb{F}_p^\star} \mathcal{N}_f(v; x) = p^{2n}.$$

Then, by (3.15) we have $\mathcal{N}_f(0; x) = p^{n+s} + p^{2n-1} - p^{n+s-1}$ for every $x \in \mathbb{F}_{p^n}$. Thus by Theorem 3.7, f is s-plateaued. The converse is clear from Theorem 3.6 and Lemma 3.1. □

In the light of Theorem 3.7, the following characterization of bent functions follows immediately from Theorem 3.5.

Corollary 3.9. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then, f is p-ary bent if and only if $\mathcal{N}_f(0; x) = p^n + p^{2n-1} - p^{n-1}$ for any $x \in \mathbb{F}_{p^n}$.*

Remark 3.2. Corollary 3.9 can be given for bent functions only although Theorem 3.6 and Corollary 3.8 are valid for any s-plateaued function with $0 \leq s \leq n$.

3.2.2 Characterizations of p-Ary Plateaued Functions by their Walsh Power Moments

This subsection, to characterize p-ary plateaued functions, makes use of even power moments of their Walsh transform. We construct several new characterizations of

plateaued functions in arbitrary characteristic and extend some characterizations of plateaued Boolean functions to arbitrary characteristic.

The sequence of the Walsh power moments of a p-ary plateaued function is a simple geometric sequence, which is an immediate consequence of Lemma 2.5.

Corollary 3.10. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. If f is s-plateaued, then for all $i \in \mathbb{Z}^+$*

$$S_i(f) = p^{(i+1)n+(i-1)s}.$$

Proof. By Lemma 2.5, for all integers $i \geq 1$, we have $S_i(f) = p^{n-s}(p^{n+s})^i + (p^n - p^{n-s})0 = p^{(i+1)n+(i-1)s}$. □

Theorem 3.8. *[55] Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then, f is plateaued if and only if $S_i(f)^2 = S_{i-1}(f)S_{i+1}(f)$ for all $i \in \mathbb{Z}^+$.*

The following seems to be more practical than Theorem 3.8 in some applications.

Corollary 3.11. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then, f is plateaued if and only if $S_i(f)S_j(f) = S_{i+1}(f)S_{j-1}(f)$ for all integers $i \geq 1$ and $j \geq 2$.*

Proof. Assume that f is plateaued. The assertion is clear from Corollary 3.10. The converse follows from Theorem 3.8 for $j = i$. □

In fact, Corollary 3.11 is equivalent to Theorem 3.8.

Proposition 3.5. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then the following are equivalent:*

i.) $S_i(f)^2 = S_{i+1}(f)S_{i-1}(f)$ *for all integers* $i \geq 2$.

ii.) $S_i(f)S_j(f) = S_{i+1}(f)S_{j-1}(f)$ *for all integers* $i \geq 1$ *and* $j \geq 2$.

Proof. Suppose that (*i*) holds. Without loss of generality, we may assume $i < j$. Fix $i \geq 2$. We proceed by induction on j. For $j = i + 1$ and $j = i + 2$, then (*ii*) trivially holds. Let $j = i + 3$. From (*i*), we get

$$\begin{aligned} S_{i+1}(f)S_{i+1}(f) &= S_{i+2}(f)S_i(f), \\ S_{i+2}(f)S_{i+2}(f) &= S_{i+3}(f)S_{i+1}(f). \end{aligned}$$

It follows that $S_i(f)S_{i+3}(f) = S_{i+1}(f)S_{i+2}(f)$. Then, (*ii*) holds for $j = i + 3$. For $j = i + k$, assume that (*ii*) holds. We then have

$$\begin{aligned} S_i(f)S_{i+k}(f) &= S_{i+1}(f)S_{i+k-1}(f), \\ S_{i+k-1}(f)S_{i+k+1}(f) &= S_{i+k}(f)S_{i+k}(f). \end{aligned}$$

It follows that $S_i(f)S_{i+k+1}(f) = S_{i+1}(f)S_{i+k}(f)$. Therefore, (*ii*) holds for $j = i + k + 1$. The converse is obvious for $j = i$. □

According to (3.1), for $i \geq 1$ and a nonnegative integer A, f is p-ary s-plateaued if and only if

$$S_i(f)A^2 - 2S_{i+1}(f)A + S_{i+2}(f) = 0, \tag{3.16}$$

where $A = p^{n+s} > 0$. Then, the reduced discriminant $S_{i+1}(f)^2 - S_{i+2}(f)S_i(f) \leq 0$ of the above equation cannot be positive, and it is zero if and only if f is p-ary plateaued. This proves the following.

Proposition 3.6. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then for all integers $i \geq 1$,*

$$S_{i+1}(f)^2 \leq S_{i+2}(f)S_i(f), \tag{3.17}$$

where the equality holds for one (and hence for all) $i \geq 1$ if and only if f is p-ary plateaued.

Proposition 3.6 can be also derived from the *Cauchy-Schwarz Inequality* (see Theorem 3.1). Notice that its equality case is equivalent to Theorem 3.8.

More precisely, from (3.16), for $i = 1$ and $A > 0$, f is p-ary plateaued if and only if

$$S_1(f)A^2 - 2S_2(f)A + S_3(f) = 0.$$

The reduced discriminant $S_2(f)^2 - S_3(f)S_1(f) \leq 0$ of the above equation cannot be positive and it is zero if and only if f is p-ary plateaued.

Corollary 3.12. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then $S_2(f)^2 \leq p^{2n}S_3(f)$, with an equality if and only if f is p-ary plateaued.*

Indeed, the plateaued-ness of a p-ary function can be checked by the values of the fourth and sixth power moments of its Walsh transform.

Theorem 3.9. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then, f is p-ary s-plateaued if and only if $S_2(f) = p^{3n+s}$ and $S_3(f) = p^{4n+2s}$.*

Proof. Assume that f is s-plateaued. Then, the assertion follows directly from Corollary 3.10. Conversely, by (3.1) with $A = p^{n+s}$ and $i = 1$, we have

$$\begin{aligned}\sum_{\omega\in\mathbb{F}_{p^n}} (|\widehat{\chi_f}(\omega)|^2 - p^{n+s})^2|\widehat{\chi_f}(\omega)|^2 &= S_3(f) - 2p^{n+s}S_2(f) + p^{2n+2s}S_1(f)\\ &= p^{4n+2s} - 2p^{n+s}p^{3n+s} + p^{2n+2s}p^{2n} = 0,\end{aligned}$$

where we used the Parseval identity in the last equality. Therefore, $|\widehat{\chi_f}(\omega)|^2 \in \{0, p^{n+s}\}$ for all $\omega \in \mathbb{F}_{p^n}$, namely, f is s-plateaued. □

We now use the Cauchy-Schwarz Inequality to obtain new characterizations of plateaued functions. In Theorem 3.1, applying the Cauchy-Schwarz Inequality, for $x_k = |\widehat{\chi_f}(\omega)|^2$ and $y_k = |\widehat{\chi_f}(\omega)|^{2i}$ for all $\omega \in \mathbb{F}_{p^n}$, $1 \le k \le p^n$, we have

$$\left(\sum_{\omega\in\mathbb{F}_{p^n}} |\widehat{\chi_f}(\omega)|^{2i+2}\right)^2 \le \sum_{\omega\in\mathbb{F}_{p^n}} |\widehat{\chi_f}(\omega)|^4 \sum_{\omega\in\mathbb{F}_{p^n}} |\widehat{\chi_f}(\omega)|^{4i},$$

that is, $S_{i+1}(f)^2 \le S_2(f)S_{2i}(f)$, where the equality holds for one (and hence for all) $i \ge 1$ if and only if for all $\omega \in \mathbb{F}_{p^n}$, $|\widehat{\chi_f}(\omega)|^2 = d\,|\widehat{\chi_f}(\omega)|^{2i}$ for some $d \in \mathbb{R}^+$; or equivalently, for all $\omega \in \mathbb{F}_{p^n}$, $|\widehat{\chi_f}(\omega)|^2$ is either the same positive integer or 0, namely, f is p-ary plateaued. This proves the following.

Proposition 3.7. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then for all integers $i \ge 1$, we have*

$$S_{i+1}(f)^2 \le S_2(f)S_{2i}(f),$$

where the equality holds for one (and hence for all) $i \ge 1$ if and only if f is p-ary plateaued.

In a similar way, by Theorem 3.1, for $x_k = |\widehat{\chi_f}(\omega)|$ and $y_k = |\widehat{\chi_f}(\omega)|^{2i+1}$ for all $\omega \in \mathbb{F}_{p^n}$, $1 \le k \le p^n$, we have $S_{i+1}(f)^2 \le S_1(f)S_{2i+1}(f)$, where the equality holds for one (and hence for all) $i \ge 1$ if and only if for all $\omega \in \mathbb{F}_{p^n}$, $|\widehat{\chi_f}(\omega)|^2$ is either the same positive integer or 0, that is, f is p-ary plateaued. Hence, by the Parseval identity, we have the following.

Theorem 3.10. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then for all integers $i \geq 1$, we have*

$$S_{i+1}(f)^2 \leq p^{2n} S_{2i+1}(f),$$

where the equality holds for one (and hence for all) $i \geq 1$ if and only if f is p-ary plateaued.

The following corollary follows readily from Corollary 3.10 and Theorem 3.10.

Corollary 3.13. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then f is p-ary s-plateaued if and only if for one (and hence for all) $i \geq 1$, $S_{i+1}(f) = p^{n(i+2)+si}$ and $S_{2i+1}(f) = p^{n(2i+2)+2si}$,*

Remark 3.3. In the following, the nonzero Walsh transform values of f correspond to the nonzero coordinates of the vector $(x_1, x_2, \ldots, x_{p^n}) \in \mathbb{R}^{p^n}$ in Theorem 3.1. And the nonzero coordinates of the corresponding vector $(y_1, y_2, \ldots, y_{p^n}) \in \mathbb{R}^{p^n}$ are all 1.

By Theorem 3.1, for $x_k = |\widehat{\chi_f}(\omega)|^{2i}$ for all $\omega \in \mathrm{Supp}(\widehat{\chi_f})$ and $y_k = 1$ (notice that $x_j = y_j = 0$ for all j with $1 \leq j \neq k \leq p^n$), we have

$$\left(\sum_{\omega \in \mathrm{Supp}(\widehat{\chi_f})} |\widehat{\chi_f}(\omega)|^{2i} \right)^2 \leq \sum_{\omega \in \mathrm{Supp}(\widehat{\chi_f})} |\widehat{\chi_f}(\omega)|^{4i} \sum_{\omega \in \mathrm{Supp}(\widehat{\chi_f})} 1$$

that is, $S_i(f)^2 \leq S_{2i}(f) * \mathcal{N}_{\widehat{\chi_f}}$, with an equality for one (and hence for all) $i \geq 1$ if and only if for all $\omega \in \mathrm{Supp}(\widehat{\chi_f})$, $|\widehat{\chi_f}(\omega)|^{2i} = d$ for some $d \in \mathbb{R}^+$; equivalently, $|\widehat{\chi_f}(\omega)|^2$ is the same positive integer for all $\omega \in \mathrm{Supp}(\widehat{\chi_f})$, that is, f is p-ary plateaued. This proves the following theorem.

Theorem 3.11. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then for every integer $i \geq 1$, we have*

$$S_i(f)^2 \leq S_{2i}(f) * \mathcal{N}_{\widehat{\chi_f}}, \tag{3.18}$$

where the equality holds for one (and hence for all) $i \geq 1$ if and only if f is p-ary plateaued.

In the case of $i = 1$, Theorem 3.11 indicates a bound stating the trade-off between the size of the Walsh support and the value of the fourth power moments of the Walsh transform of p-ary functions, and this bound is satisfied by plateaued functions only. In view of the Parseval identity, we have the following.

Corollary 3.14. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then*

$$p^{4n} \leq S_2(f) * \mathcal{N}_{\widehat{\chi_f}},$$

with an equality if and only if f is p-ary plateaued.

The following is an immediate consequence of Proposition 3.1 and Corollary 3.14.

Corollary 3.15. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Set $\theta_f = \sum_{a,b,x \in \mathbb{F}_{p^n}} \xi_p^{\mathcal{D}_a \mathcal{D}_b f(x)}$. Then*

$$p^{3n} \leq \theta_f * \mathcal{N}_{\widehat{\chi_f}},$$

with an equality if and only if f is p-ary plateaued.

Proposition 3.2 and Corollary 3.15 directly bring the following result, which was first observed in [78], in characteristic 2.

Corollary 3.16. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Set $\mathcal{A}_{\Delta_f} = \sum_{a \in \mathbb{F}_{p^n}} |\Delta_f(a)|^2$. Then*

$$p^{3n} \leq \mathcal{A}_{\Delta_f} * \mathcal{N}_{\widehat{\chi_f}},$$

with an equality if and only if f is p-ary plateaued.

In Theorem 3.1, putting $x_k = |\widehat{\chi_f}(\omega)|^2$ for all $\omega \in \mathrm{Supp}(\widehat{\chi_f})$ and $y_k = 1$ (notice that $x_j = y_j = 0$ for all j with $1 \leq j \neq k \leq p^n$), with $p_1 = i$ and $p_2 = \frac{i}{i-1}$, we have

$$\sum_{\omega \in \mathrm{Supp}(\widehat{\chi_f})} |\widehat{\chi_f}(\omega)|^2 \leq \left(\sum_{\omega \in \mathrm{Supp}(\widehat{\chi_f})} |\widehat{\chi_f}(\omega)|^{2i} \right)^{\frac{1}{i}} \left(\sum_{\omega \in \mathrm{Supp}(\widehat{\chi_f})} 1 \right)^{\frac{i-1}{i}},$$

by the Parseval identity, $p^{2ni} \leq S_i(f) * \mathcal{N}_{\widehat{\chi_f}}^{(i-1)}$, where the equality holds for one (and hence for all) $i \geq 2$ if and only if for every $\omega \in \mathrm{Supp}(\widehat{\chi_f})$, $|\widehat{\chi_f}(\omega)|^2 = d$ for some $d \in \mathbb{R}^+$; equivalently, f is p-ary plateaued. This proves the following theorem.

Theorem 3.12. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then for every integer $i \geq 2$,*

$$p^{2ni} \leq S_i(f) * \mathcal{N}_{\widehat{\chi_f}}^{(i-1)},$$

where the equality holds for one (and hence for all) $i \geq 2$ if and only if f is p-ary plateaued.

The following was first observed in [78] in characteristic 2. We extend it to arbitrary characteristic with a different proof .

Proposition 3.8. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then*

$$p^{2n} \leq \max_{b\in\mathbb{F}_{p^n}}(|\widehat{\chi_f}(b)|^2) * \mathcal{N}_{\widehat{\chi_f}}, \tag{3.19}$$

with an equality if and only if f is p-ary plateaued.

Proof. By the definition of $\mathcal{N}_{\widehat{\chi_f}}$, we have

$$\sum_{\omega\in\mathbb{F}_p^n} |\widehat{\chi_f}(\omega)|^2 \leq \max_{b\in\mathbb{F}_{p^n}}(|\widehat{\chi_f}(b)|^2) * \mathcal{N}_{\widehat{\chi_f}}.$$

Hence, the first assertion follows directly from the Parseval identity.

Assume that the lower bound in (3.19) holds. By the Parseval identity, for all $\omega \in \mathrm{Supp}(\widehat{\chi_f})$, we have $|\widehat{\chi_f}(\omega)|^2 = \max_{b\in\mathbb{F}_{p^n}}(|\widehat{\chi_f}(b)|^2)$, that is, there exists an integer s such that $|\widehat{\chi_f}(\omega)|^2 = p^{n+s}$ for all $\omega \in \mathrm{Supp}(\widehat{\chi_f})$. Hence, f is s-plateaued. Conversely, assume that f is s-plateaued. By Lemma 2.5, we have $\mathcal{N}_{\widehat{\chi_f}} = p^{n-s}$ and $|\widehat{\chi_f}(\omega)|^2 = p^{n+s}$ for all $\omega \in \mathrm{Supp}(\widehat{\chi_f})$. Hence, the bound in (3.19) is satisfied. □

Theorem 3.13. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then,*

$$S_2(f) \leq p^{2n} \max_{b\in\mathbb{F}_{p^n}}(|\widehat{\chi_f}(b)|^2),$$

with an equality if and only if f is p-ary plateaued.

Proof. We have

$$\sum_{\omega\in\mathbb{F}_{p^n}} |\widehat{\chi_f}(\omega)|^4 = \sum_{\omega\in\mathbb{F}_{p^n}} |\widehat{\chi_f}(\omega)|^2|\widehat{\chi_f}(\omega)|^2 \leq \sum_{\omega\in\mathbb{F}_{p^n}} |\widehat{\chi_f}(\omega)|^2 \max_{b\in\mathbb{F}_{p^n}}(|\widehat{\chi_f}(b)|^2); \tag{3.20}$$

equivalently, $S_2(f) \leq S_1(f) \max_{b\in\mathbb{F}_{p^n}}(|\widehat{\chi_f}(b)|^2)$. In view of the Parseval identity, the first assertion holds.

For the equality case, assume that f is plateaued. By Corollary 3.10, $S_2(f) = p^{3n+s}$. Hence, the assertion is clear from the assumption. Conversely, by (3.20), for all $\omega \in \mathrm{Supp}(\widehat{\chi_f})$, $|\widehat{\chi_f}(\omega)|^2 = \max_{b\in\mathbb{F}_{p^n}}(|\widehat{\chi_f}(b)|^2)$, i.e., there exists an integer s such that $|\widehat{\chi_f}(\omega)|^2 = p^{n+s}$; equivalently, f is plateaued. □

In the light of Proposition 3.1, the following is a direct conclusion of Theorem 3.13.

Corollary 3.17. *Let $f : \mathbb{F}_p^n \to \mathbb{F}_p$. Set $\theta_f = \sum_{a,b,x\in\mathbb{F}_{p^n}} \xi_p^{\mathcal{D}_a\mathcal{D}_b f(x)}$. Then,*

$$\theta_f \leq p^n \max_{b\in\mathbb{F}_{p^n}}(|\widehat{\chi_f}(b)|^2),$$

with an equality if and only if f is p-ary plateaued.

The equality case of Corollary 3.17 was first observed in [10], in characteristic 2.

By Proposition 3.2, the following is an immediate consequence of Theorem 3.13.

Corollary 3.18. *Let $f : \mathbb{F}_p^n \to \mathbb{F}_p$. Set $\mathcal{A}_{\Delta_f} = \sum_{a\in\mathbb{F}_{p^n}} |\Delta_f(a)|^2$. Then,*

$$\mathcal{A}_{\Delta_f} \leq p^n \max_{b\in\mathbb{F}_{p^n}}(|\widehat{\chi_f}(b)|^2),$$

with an equality if and only if f is p-ary plateaued.

Remark 3.4. [13] A function from $\mathbb{F}_{p^n}$ to $\mathbb{C}$ is constant if and only if its Fourier transform vanishes at any nonzero input.

We now extend to arbitrary characteristic the characterizations of plateaued Boolean functions given in [15], considering Theorem 3.6 and Remark 3.4.

Theorem 3.14. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then f is p-ary plateaued if and only if for all $\alpha \in \mathbb{F}_{p^n}^\star$, we have*

$$\sum_{\omega\in\mathbb{F}_{p^n}} \widehat{\chi_f}(\alpha+\omega)\overline{\widehat{\chi_f}(\omega)}\ |\widehat{\chi_f}(\omega)|^2 = 0. \tag{3.21}$$

Proof. By the definition of $\widehat{\chi_f}$, for all $\alpha \in \mathbb{F}_{p^n}^\star$ (3.21) is equivalent to:

$$\sum_{\omega,x,y,z,t\in\mathbb{F}_{p^n}} \xi_p^{f(x)-(\alpha+\omega)\cdot x-f(y)+\omega\cdot y+f(z)-\omega\cdot z-f(t)+\omega\cdot t} = 0,$$

that is, to: $\sum_{\omega,x,y,z,t\in\mathbb{F}_{p^n}} \xi_p^{f(x)-f(y)+f(z)-f(t)-\omega\cdot(x-y+z-t)-\alpha\cdot x} = 0$, equivalently, to:

$$\sum_{x,y,z\in\mathbb{F}_{p^n}} \xi_p^{f(x)-f(y)+f(z)-f(x-y+z)-\alpha\cdot x} = 0$$

since $\sum_{\omega\in\mathbb{F}_{p^n}} \xi_p^{\omega\cdot(x-y+z-t)}$ is null if $x-y+z-t \neq 0$, that is, (by the bijective change of variables: $y = x+a$ and $z = x+a+b$) to:

$$\sum_{x,a,b\in\mathbb{F}_{p^n}} \xi_p^{\mathcal{D}_b\mathcal{D}_a f(x)-\alpha\cdot x} = 0, \tag{3.22}$$

which is the Fourier transform at $\alpha \in \mathbb{F}_{p^n}^\star$ of the function

$$x \mapsto \sum_{a,b \in \mathbb{F}_{p^n}} \xi_p^{\mathcal{D}_b \mathcal{D}_a f(x)}. \tag{3.23}$$

Owing to Remark 3.4, (3.22) holds for all $\alpha \in \mathbb{F}_{p^n}^\star$ if and only if the function in (3.23) is constant; equivalently by Theorem 3.6, f is p-ary plateaued. □

Corollary 3.19. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then f is p-ary plateaued if and only if for all $x \in \mathbb{F}_{p^n}$*

$$S_2(f) = p^n \sum_{\omega \in \mathbb{F}_{p^n}} \xi_p^{f(x)-\omega \cdot x} \overline{\widehat{\chi_f}(\omega)}\, |\widehat{\chi_f}(\omega)|^2. \tag{3.24}$$

Proof. Assume that f is p-ary s-plateaued. By Corollary 3.10, $S_2(f) = p^{3n+s}$. For all $x \in \mathbb{F}_{p^n}$, the right-hand side of (3.24) equals

$$p^{2n+s} \sum_{\omega \in \mathbb{F}_{p^n}} \xi_p^{f(x)-\omega \cdot x} \overline{\widehat{\chi_f}(\omega)} = p^{2n+s} \sum_{y \in \mathbb{F}_{p^n}} \xi_p^{f(x)-f(y)} \sum_{\omega \in \mathbb{F}_{p^n}} \xi_p^{\omega \cdot (y-x)} = p^{3n+s}.$$

Thus for all $x \in \mathbb{F}_{p^n}$, (3.24) holds. Conversely, assume that (3.24) holds for all $x \in \mathbb{F}_{p^n}$. That is, for all $x \in \mathbb{F}_{p^n}$, the function $G : \mathbb{F}_{p^n} \to \mathbb{C}$ defined by

$$x \mapsto G(x) = \sum_{\omega \in \mathbb{F}_{p^n}} \xi_p^{f(x)-\omega \cdot x} \overline{\widehat{\chi_f}(\omega)} |\widehat{\chi_f}(\omega)|^2$$

is constant. The Fourier transform of this constant function at $\alpha \in \mathbb{F}_{p^n}$ is given by

$$\begin{aligned} \widehat{G}(\alpha) &= \sum_{x \in \mathbb{F}_{p^n}} G(x) \xi_p^{-\alpha \cdot x} = \sum_{\omega \in \mathbb{F}_{p^n}} \sum_{x \in \mathbb{F}_{p^n}} \xi_p^{f(x)-x \cdot (\alpha+\omega)} \overline{\widehat{\chi_f}(\omega)}\, |\widehat{\chi_f}(\omega)|^2 \\ &= \sum_{\omega \in \mathbb{F}_{p^n}} \widehat{\chi_f}(\alpha+\omega) \overline{\widehat{\chi_f}(\omega)}\, |\widehat{\chi_f}(\omega)|^2, \end{aligned}$$

which is null at any $\alpha \in \mathbb{F}_{p^n}^\star$ by Remark 3.4. Hence, by Theorem 3.14, f is p-ary plateaued. □

The following gives a link between the Walsh transform and second-order derivative of a p-ary function.

Proposition 3.9. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then, for all $x \in \mathbb{F}_{p^n}$*

$$\sum_{\omega \in \mathbb{F}_{p^n}} \xi_p^{f(x)-\omega \cdot x} \overline{\widehat{\chi_f}(\omega)}\, |\widehat{\chi_f}(\omega)|^2 = p^n \sum_{a,b \in \mathbb{F}_{p^n}} \xi_p^{\mathcal{D}_a \mathcal{D}_b f(x)}. \tag{3.25}$$

Proof. By the definition of $\widehat{\chi_f}$, for all $x \in \mathbb{F}_{p^n}$, the left-hand side of (3.25) equals

$$\sum_{\omega,a,b,c\in\mathbb{F}_{p^n}} \xi_p^{f(x)-f(a)-f(b)+f(c)+\omega\cdot(a+b-c-x)} = p^n \sum_{a,b\in\mathbb{F}_{p^n}} \xi_p^{f(x)-f(a)-f(b)+f(a+b-x)}$$

since $\sum_{\omega\in\mathbb{F}_{p^n}} \xi_p^{-\omega\cdot(x-a-b+c)}$ is null if $c \neq a+b-x$. For all $x \in \mathbb{F}_{p^n}$, by the bijective change of variables: $a \mapsto a+x$ and $b \mapsto b+x$, it is equal to the right-hand side of (3.25). Hence, the proof is complete. □

In view of Proposition 3.9, the following follows readily from Theorem 3.6.

Corollary 3.20. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then, f is p-ary s-plateaued if and only if for all $x \in \mathbb{F}_{p^n}$*

$$\sum_{\omega\in\mathbb{F}_{p^n}} \xi_p^{f(x)-\omega\cdot x}\overline{\widehat{\chi_f}(\omega)}\ |\widehat{\chi_f}(\omega)|^2 = p^{2n+s}.$$

3.2.3 Characterizations of p-Ary Plateaued Functions by their Autocorrelation Functions

In this subsection, we extend the characterizations of plateaued Boolean functions to arbitrary characteristic, by means of their autocorrelation functions.

By Lemma 2.3, for all $a \in \mathbb{F}_{p^n}$, we have

$$\widehat{\widehat{\Delta_f}}(a) = p^n \Delta_f(-a). \tag{3.26}$$

By Proposition 2.2, for all $a \in \mathbb{F}_{p^n}$,

$$\overline{\Delta_f}(a) = \Delta_f(-a), \tag{3.27}$$

and for all $\omega \in \mathbb{F}_{p^n}$,

$$|\widehat{\chi_f}(\omega)|^2 = \widehat{\Delta_f}(\omega). \tag{3.28}$$

Combining (3.26), (3.27) and (3.28), we have $|\widehat{\widehat{\chi_f}(a)}|^2 = p^n\overline{\Delta_f}(a)$ for all $a \in \mathbb{F}_{p^n}$. Hence, the Fourier transform of $|\widehat{\chi_f}|^4$ is obtained as

$$|\widehat{\widehat{\chi_f}|^2|\widehat{\chi_f}}|^2 \ = p^{-n}\left(\widehat{|\widehat{\chi_f}|^2} \otimes \widehat{|\widehat{\chi_f}|^2}\right) = p^{-n}\left(p^n\overline{\Delta_f} \otimes p^n\overline{\Delta_f}\right) = p^n\left(\overline{\Delta_f} \otimes \overline{\Delta_f}\right) \tag{3.29}$$

where we used (3.3) in the first equality.

Now we characterize p-ary plateaued functions by considering the Fourier transforms of their absolute Walsh transforms. By the definition of p-ary plateaued, we can say that f is p-ary plateaued of the amplitude μ if and only if the two functions $|\widehat{\chi_f}|^4$ and $\mu^2|\widehat{\chi_f}|^2$ are equal; equivalently, by (3.4), their Fourier transforms are equal. This implies the following.

Theorem 3.15. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then, f is p-ary plateaued of the amplitude μ if and only if for all $x \in \mathbb{F}_{p^n}$*

$$\sum_{a\in\mathbb{F}_{p^n}} \Delta_f(a)\Delta_f(x-a) = \mu^2\Delta_f(x). \tag{3.30}$$

Proof. As stated above, f is p-ary plateaued of the amplitude μ if and only if the two functions $\overline{\Delta_f} \otimes \overline{\Delta_f}$ and $\mu^2\overline{\Delta_f}$ are equal; equivalently, $(\Delta_f \otimes \Delta_f)(x) = \mu^2\Delta_f(x)$ for all $x \in \mathbb{F}_{p^n}$ by (3.27). This completes the proof. □

The Fourier transform of $|\widehat{\chi_f}|^6$ can be given by

$$\widehat{|\widehat{\chi_f}|^2|\widehat{\chi_f}|^4} = p^{-n}\left(\widehat{|\widehat{\chi_f}|^2} \otimes \widehat{|\widehat{\chi_f}|^4}\right) = p^n\left(\overline{\Delta_f} \otimes \overline{\Delta_f} \otimes \overline{\Delta_f}\right)$$

where we used (3.3) in the first equality and used (3.29) in the second equality. We now give the next characterization of plateaued function.

Corollary 3.21. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then, f is p-ary plateaued of the amplitude μ if and only if for all $x \in \mathbb{F}_{p^n}$*

$$\sum_{a,b\in\mathbb{F}_{p^n}} \Delta_f(a)\Delta_f(b)\Delta_f(x-a-b) = \mu^2 \sum_{c\in\mathbb{F}_{p^n}} \Delta_f(c)\Delta_f(x-c).$$

Proof. As in the proof of Theorem 3.15, f is p-ary plateaued of the amplitude μ if and only if the two functions $|\widehat{\chi_f}|^6$ and $\mu^2|\widehat{\chi_f}|^4$ are equal; equivalently, by (3.4) their Fourier transforms are equal, that is, by (3.27) for all $x \in \mathbb{F}_{p^n}$ we have

$$(\Delta_f \otimes \Delta_f \otimes \Delta_f)(x) = \mu^2(\Delta_f \otimes \Delta_f)(x).$$

□

In order to characterize vectorial plateaued p-ary functions whose component functions may have different amplitudes, we need to eliminate the constant μ^2 in (3.30).

Then putting $x = 0$ in (3.30), we have

$$\sum_{a \in \mathbb{F}_{p^n}} |\Delta_f(a)|^2 = \mu^2 \Delta_f(0) = \mu^2 p^n$$

by (3.27) since $\Delta_f(0) = p^n$. Hence the following follows directly from Theorem 3.15.

Corollary 3.22. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then, f is p-ary plateaued if and only if for all $x \in \mathbb{F}_{p^n}$,*

$$p^n \sum_{a \in \mathbb{F}_{p^n}} \Delta_f(a)\Delta_f(x-a) = \sum_{a \in \mathbb{F}_{p^n}} |\Delta_f(a)|^2 \Delta_f(x).$$

We now give an example of quadratic plateaued functions.

Example 3.3. *Let p be an odd prime and $n \geq 2$ be an integer. Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be an arbitrary $\mathbb{F}_p$-quadratic form defined as*

$$f(x) = \mathrm{Tr}_p^{p^n}(a_0 x^2 + a_1 x^{p+1} + a_2 x^{p^2+1} + \cdots + a_{\lfloor \frac{n}{2} \rfloor} x^{p^{\lfloor \frac{n}{2} \rfloor}+1}).$$

The radical of f given by

$$\mathcal{W}_f = \{x \in \mathbb{F}_{p^n} : f(x+y) = f(x) + f(y), \forall y \in \mathbb{F}_{p^n}\}$$

is an $\mathbb{F}_p$-linear subspace of $\mathbb{F}_{p^n}$. Let $\dim_{\mathbb{F}_p}(\mathcal{W}_f) = s$. It follows from the proof of [8, Theorem 4.1] that for all $\omega \in \mathbb{F}_{p^n}$

$$|\widehat{\chi_f}(\omega)|^2 = 0 \quad or \quad p^{2s} \sum_{y_1,\ldots,y_{n-s} \in \mathbb{F}_p} \sum_{z_1,\ldots,z_{n-s} \in \mathbb{F}_p} \xi_p^{H(y_1,\ldots,y_{n-s}) - H(z_1,\ldots,z_{n-s})},$$

where $H(x_1, \ldots, x_{n-s}) = \frac{1}{2}(x_1^2 + \cdots + x_{n-s-1}^2 + d x_{n-s}^2)$ and $d \in \mathbb{F}_p^\star$. For each pair y_i and z_i, where $i = 1, \ldots, n-s$, as is readily seen,

$$\sum_{y_i, z_i \in \mathbb{F}_p} \xi_p^{\frac{1}{2}(y_i^2 - z_i^2)} = \sum_{t_{i1}, t_{i2} \in \mathbb{F}_p} \xi_p^{\frac{1}{2}(t_{i1} t_{i2})} = \sum_{t_{i2} \in \mathbb{F}_p} \left(\sum_{t_{i1} \in \mathbb{F}_p} \xi_p^{\frac{1}{2} t_{i1}} \right) = p.$$

Therefore, we conclude that $|\widehat{\chi_f}(\omega)|^2 \in \{0, p^{n+s}\}$ for all $\omega \in \mathbb{F}_{p^n}$. Moreover, [7, Proposition 5.8] gives an algorithm to construct such a quadratic form f with radical $\mathcal{W}_f$ of dimension s with $0 \leq s \leq n-1$. In fact, this algorithm holds for any finite field $\mathbb{F}_q$, where q is a prime power. Hence, for odd prime p, integers $n \geq 2$ and s with $0 \leq s \leq n-1$, there exists a quadratic p-ary s-plateaued f from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$. For example, for $p = 3$ and $n = 5$,

- $\mathrm{Tr}_3^{3^5}(x^2+x^4+2x^{10})$ *is the quadratic* 0*-plateaued function,*
- $\mathrm{Tr}_3^{3^5}(x^2+x^4+x^{10})$ *is the quadratic* 1*-plateaued function,*
- $\mathrm{Tr}_3^{3^5}(\zeta x^2+x^4+2x^{10})$ *is the quadratic* 2*-plateaued function,*
- $\mathrm{Tr}_3^{3^5}(\zeta^2 x^2+2x^4+\zeta^{28}x^{10})$ *is the quadratic* 3*-plateaued function and*
- $\mathrm{Tr}_3^{3^5}(x^2+2x^4+2x^{10})$ *is the quadratic* 4*-plateaued function,*

where ζ *is a primitive element of* $\mathbb{F}_{3^5}$ *with* $\zeta^5+2\zeta+1=0$.

3.3 Characterizations of Vectorial Bent and Plateaued p-Ary Functions

This section characterizes bent and plateaued vectorial functions in arbitrary characteristic. Firstly, the notion of vectorial Boolean plateaued functions is extended to arbitrary characteristic. We next give a number of characterizations of bent and plateaued vectorial p-ary functions by the value distribution of their second-order (and also first-order) derivatives. More precisely, we investigate plateaued-ness property of vectorial p-ary functions whose component functions are all unbalanced. We also deal with plateaued-ness property of power functions by their first-order derivatives. We finally extend the notion of strongly-plateaued Boolean functions to arbitrary characteristic.

The notion of vectorial bent p-ary functions was given as follows (see, e.g., [55]).

Definition 3.1. Let F be a vectorial function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ and let F_λ, $\lambda \in \mathbb{F}_{p^m}^\star$, be its component function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ defined by $F_\lambda(x) = \mathrm{Tr}_p^{p^m}(\lambda F(x))$ for every $x \in \mathbb{F}_{p^n}$. Then, F is called *vectorial p-ary bent* if F_λ, $\lambda \in \mathbb{F}_{p^m}^\star$, is p-ary bent function.

The notion of plateaued vectorial Boolean functions was first given by Carlet in [14], which can be given in arbitrary characteristic.

Definition 3.2. Let F be a vectorial function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ and let F_λ, $\lambda \in \mathbb{F}_{p^m}^\star$, be its component function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ defined by $F_\lambda(x) = \mathrm{Tr}_p^{p^m}(\lambda F(x))$ for every $x \in \mathbb{F}_{p^n}$. Then,

- F is called *vectorial p-ary partially bent* if F_λ, $\lambda \in \mathbb{F}_{p^m}^\star$, is p-ary partially bent.
- F is called *vectorial p-ary plateaued* if F_λ, $\lambda \in \mathbb{F}_{p^m}^\star$, is p-ary plateaued with possibly different amplitudes.
- F is called *vectorial p-ary plateaued with single amplitude* if F_λ, $\lambda \in \mathbb{F}_{p^m}^\star$, is p-ary plateaued of the same amplitude. In other words, there exists an integer s with $0 \leq s \leq n$ such that F is called *vectorial p-ary s-plateaued* if F_λ, $\lambda \in \mathbb{F}_{p^m}^\star$, is p-ary s-plateaued.

Remark 3.5. A vectorial p-ary function is plateaued if and only if all of its component functions are p-ary plateaued with possibly different amplitudes. More precisely, a vectorial p-ary function is plateaued with single amplitude if and only if all of its component functions are p-ary plateaued of the same amplitude. These facts will be frequently used in the sequel.

A vectorial p-ary bent is vectorial p-ary 0-plateaued. The following example shows that the notion of vectorial plateaued is strictly more general than the notion of vectorial s-plateaued for nonzero s.

Example 3.4. *Let p be a prime and n be a positive even integer. Let f_1 and f_2 be quadratic p-ary s_1-plateaued and s_2-plateaued functions from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ with $s_1 \neq s_2$, respectively. For any $\theta \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$, the function F given as*

$$F(x) = f_1(x) + \theta f_2(x)$$

is vectorial plateaued from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^2}$, but it is not vectorial s-plateaued function for any integer s.

3.3.1 Characterizations of Vectorial Bent p-Ary Functions

This subsection provides a new proof of the link between the balanced-ness of first-order derivatives and the number of zeros of second-order derivatives of vectorial functions.

In 1991, Nyberg characterized vectorial bent functions by the balanced-ness of their first-order derivatives.

Theorem 3.16. *[67, Theorem 2.3] Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$. Then F is vectorial p-ary bent if and only if the derivative $\mathcal{D}_a F$ is balanced for all $a \in \mathbb{F}_{p^n}^\star$.*

In 2014, Mesnager presented the following characterization of vectorial bent functions in terms of the zeros of their second-order derivatives.

Theorem 3.17. *[55, Theorem 6] Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$. Then F is vectorial p-ary bent if and only if*

$$\mathfrak{N}(F) = p^{3n-m} + p^{2n} - p^{2n-m}.$$

It would be interesting to prove directly that $\mathcal{D}_a F$ is balanced for all $a \in \mathbb{F}_{p^n}^\star$ if and only if $\mathfrak{N}(F) = p^{3n-m}+p^{2n}-p^{2n-m}$ without using the bent-ness of vectorial function F. Before proving it, we give the following well-known result, which can be easily proven using Theorem 3.1.

Lemma 3.2. *Let $x_1, x_2, \ldots, x_m$ be positive real numbers such that $x_1 + x_2 + \cdots + x_m = n$. We then have*

$$\frac{n^2}{m} \leq x_1^2 + x_2^2 + \cdots + x_m^2$$

with an equality if and only if $x_1 = x_2 = \cdots = x_m$.

The following lemma is similar to [16, Proposition 1], but is also valid in arbitrary characteristic.

Lemma 3.3. *Let G be a vectorial function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$. Then*

$$p^{2n-m} \leq \#\{(x_1, x_2) \in \mathbb{F}_{p^n}^2 : G(x_1) = G(x_2)\} \tag{3.31}$$

with an equality if and only if G is balanced.

Proof. Let $A_j = \{x \in \mathbb{F}_{p^n} : G(x) = y_j \in \mathbb{F}_{p^m}\}$ and $z_j = \#A_j$ for $j \in \{1, \ldots, p^m\}$. Then we have

$$\begin{aligned}\#\{(x_1, x_2) \in \mathbb{F}_{p^n}^2 : G(x_1) = G(x_2)\} &= \#\left(\bigcup_{j=1}^{p^m} \{(x_1, x_2) \in \mathbb{F}_{p^n}^2 : x_1, x_2 \in A_j\}\right) \\ &= \sum_{j=1}^{p^m} (\#A_j)^2 = \sum_{j=1}^{p^m} z_j^2.\end{aligned}$$

By Lemma 3.2, for $\sum_{j=1}^{p^m} z_j = p^n$ and $z_j \geq 0$, we get $\sum_{j=1}^{p^m} z_j^2 \geq p^{2n-m}$. Thus, (3.31) holds. Notice that G is balanced if and only if $z_1 = z_2 = \cdots = z_{p^m}$. Hence, the last assertion follows from Lemma 3.2. □

Theorem 3.18. *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$. Then*

$$\mathcal{D}_a F \text{ is balanced for all } a \in \mathbb{F}_{p^n}^\star \iff \mathfrak{N}(F) = p^{3n-m} + p^{2n} - p^{2n-m}. \quad (3.32)$$

Proof. For $(a, b, x) \in \mathbb{F}_{p^n}^3$, clearly we have that $\mathcal{D}_b\mathcal{D}_a F(x) = 0$ if and only if

$$\mathcal{D}_a F(x) = \mathcal{D}_a F(x + b). \quad (3.33)$$

First, for $n = m$, we prove that $\mathcal{D}_a F$ is balanced for all $a \in \mathbb{F}_{p^n}^\star$ if and only if $\mathfrak{N}(F) = 2p^{2n} - p^n$. For $a = 0$, it is easy to see that (3.33) holds for all $b, x \in \mathbb{F}_{p^n}$ since $\mathcal{D}_a F$ is the zero map. Then,

$$\#\{(0, b, x) \in \mathbb{F}_{p^n}^3 : \mathcal{D}_b\mathcal{D}_a F(x) = 0\} = p^{2n}.$$

For $a \neq 0$, by Lemma 3.3, the number of pairs $(b, x) \in \mathbb{F}_{p^n}^2$ satisfying (3.33) is p^n if and only if $\mathcal{D}_a F$ is balanced. Then, $\#\{(a, b, x) \in \mathbb{F}_{p^n}^3 : a \neq 0, \mathcal{D}_b\mathcal{D}_a F(x) = 0\} = p^{2n} - p^n$. Therefore, $\mathcal{D}_a F$ is balanced for all $a \in \mathbb{F}_{p^n}^\star$ if and only if $\mathfrak{N}(F) = 2p^{2n} - p^n$.

Now assume $n \neq m$. For $a = 0$, we get $\#\{(0, b, x) \in \mathbb{F}_{p^n}^3 : \mathcal{D}_b\mathcal{D}_a F(x) = 0\} = p^{2n}$. For $a \neq 0$, by Lemma 3.3, the number of pairs $(b, x) \in \mathbb{F}_{p^n}^2$ satisfying (3.33) is p^{2n-m} if and only if $\mathcal{D}_a F$ is balanced. Then

$$\#\{(a, b, x) \in \mathbb{F}_{p^n}^3 : a \neq 0, \mathcal{D}_b\mathcal{D}_a F(x) = 0\} = (p^n - 1)p^{2n-m}.$$

Thus, (3.32) holds. □

Corollary 3.23. *[55, Corollary 1] Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$. Then F is vectorial p-ary bent if and only if $\mathfrak{N}^\star(F) = (p^n - 1)(p^{2n-m} - p^n)$, where $\mathfrak{N}^\star(F) = \#\{(a, b, x) \in \mathbb{F}_{p^n}^\star \times \mathbb{F}_{p^n}^\star \times \mathbb{F}_{p^n} : \mathcal{D}_b\mathcal{D}_a F(x) = 0\}$.*

As in the proof of Theorem 3.18, the following corollary easily follows without using bent-ness.

Corollary 3.24. *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$. Then, $\mathcal{D}_a F$ is balanced for all $a \in \mathbb{F}_{p^n}^\star$ if and only if $\mathfrak{N}^\star(F) = (p^n - 1)(p^{2n-m} - p^n)$.*

3.3.2 Characterizations of Vectorial Plateaued p-Ary Functions by their Derivatives

This subsection extends to arbitrary characteristic the characterizations of plateaued vectorial Boolean functions in terms of their derivatives given in [15]. We also obtain new characterizations of vectorial plateaued functions in terms of the value distribution of their second-order derivatives in arbitrary characteristic. We finally extend the notion of strongly-plateaued functions to arbitrary characteristic.

We start by giving the following characterization of vectorial plateaued functions.

Theorem 3.19. *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$. Then*

i.) F is vectorial plateaued if and only if for every $v \in \mathbb{F}_{p^m}$, $\mathcal{N}_F(v; x)$ does not depend on $x \in \mathbb{F}_{p^n}$.

ii.) There exists an integer s with $0 \leq s \leq n$ such that F is vectorial s-plateaued if and only if for every $v \in \mathbb{F}_{p^m}$, $\mathcal{N}_F(v; x)$ does not depend on $x \in \mathbb{F}_{p^n}$ and $\mathcal{N}_F(v_1; x) = \mathcal{N}_F(v_2; x)$ for every $v_1, v_2 \in \mathbb{F}_{p^m}^\star$ and $x \in \mathbb{F}_{p^n}$.

Proof. For $x \in \mathbb{F}_{p^n}$ and $u \in \mathbb{F}_{p^m}$, let $G(u; x)$ be the complex valued function defined by

$$G(u; x) = \sum_{a,b \in \mathbb{F}_{p^n}} \xi_p^{\mathcal{D}_b \mathcal{D}_a \mathrm{Tr}^m(uF(x))}. \tag{3.34}$$

For $x \in \mathbb{F}_{p^n}$ and $v \in \mathbb{F}_{p^m}$, the Fourier transform $\widehat{G}$ of G is defined as

$$\widehat{G}(v; x) = \sum_{u \in \mathbb{F}_{p^m}} G(u; x) \xi_p^{-\mathrm{Tr}^m(uv)}.$$

Then for every $x \in \mathbb{F}_{p^n}$ and $v \in \mathbb{F}_{p^m}$, the Fourier transform $\widehat{G}(v; x)$ is given by

$$\begin{aligned} &\sum_{u \in \mathbb{F}_{p^m}} \sum_{a,b \in \mathbb{F}_{p^n}} \xi_p^{\mathcal{D}_b \mathcal{D}_a \mathrm{Tr}^m(uF(x)) - \mathrm{Tr}^m(uv)} = \sum_{a,b \in \mathbb{F}_{p^n}} \sum_{u \in \mathbb{F}_{p^m}} \xi_p^{\mathrm{Tr}^m(u(\mathcal{D}_b \mathcal{D}_a F(x) - v))} \\ &= p^m \#\{(a, b) \in \mathbb{F}_{p^n}^2 : \mathcal{D}_b \mathcal{D}_a F(x) = v\} = p^m \mathcal{N}_F(v; x). \end{aligned} \tag{3.35}$$

Then for every $v \in \mathbb{F}_{p^m}$, $\mathcal{N}_F(v; x)$ does not depend on $x \in \mathbb{F}_{p^n}$ if and only if the Fourier transform $\widehat{G}(v; x)$ does not depend on $x \in \mathbb{F}_{p^n}$. It follows from (3.4) that for $x_1, x_2 \in \mathbb{F}_{p^n}$, $\widehat{G}(v; x_1) = \widehat{G}(v; x_2)$ for every $v \in \mathbb{F}_{p^m}$ if and only if

$$G(u; x_1) = G(u; x_2)$$

for every $u \in \mathbb{F}_{p^m}$. By Theorem 3.6, $G(u;x)$ does not depend on $x \in \mathbb{F}_{p^n}$ for every $u \in \mathbb{F}_{p^m}$ if and only if F is vectorial plateaued. Hence, F is vectorial plateaued if and only if for every $v \in \mathbb{F}_{p^m}$, $\mathcal{N}_F(v;x)$ does not depend on $x \in \mathbb{F}_{p^n}$.

Next we prove (*ii*). Note that F is vectorial s-plateaued if and only if F is vectorial plateaued and for every $x \in \mathbb{F}_{p^n}$ we have $G(u_1;x) = G(u_2;x)$ for every $u_1, u_2 \in \mathbb{F}_{p^m}^\star$ given in (3.34). This also follows from Theorem 3.6. For any $x \in \mathbb{F}_{p^n}$, using the above arguments we obtain $G(u_1;x) = G(u_2;x)$ for every $u_1, u_2 \in \mathbb{F}_{p^m}^\star$ if and only if $\mathcal{N}_F(v_1;x) = \mathcal{N}_F(v_2;x)$ for every $v_1, v_2 \in \mathbb{F}_{p^m}^\star$. The proof follows from (*i*). □

We remark that Theorem 3.19 gives an alternative proof of the fact that any quadratic (vectorial) function is plateaued in arbitrary characteristic. The following theorem is related to Theorem 3.19. It yields the number of the value distribution of the second-order derivatives of these functions. To do this, by Lemma 2.3, for $G : \mathbb{F}_{p^n} \to \mathbb{C}$, we have

$$G(u) = \theta, \quad \forall u \in \mathbb{F}_{p^n}^\star \Longleftrightarrow \widehat{G}(v) = \theta', \quad \forall v \in \mathbb{F}_{p^n}^\star, \tag{3.36}$$

where θ and θ' are constants in $\mathbb{C}$. Notice that $G(0) = \theta + \theta'$ and $\widehat{G}(0) = p^n\theta + \theta'$.

Theorem 3.20. *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$. The following hold.*

i.) There exists an integer s with $0 \le s \le n$ such that F is vectorial s-plateaued if and only if $\mathcal{N}_F(v;x) = p^{2n-m} - p^{n+s-m}$ for every $v \in \mathbb{F}_{p^m}^\star$ and $x \in \mathbb{F}_{p^n}$. In this case, $\mathcal{N}_F(0;x) = p^{n+s} + p^{2n-m} - p^{n+s-m}$ for every $x \in \mathbb{F}_{p^n}$.

ii.) Assume that F is vectorial plateaued. For each $\lambda \in \mathbb{F}_{p^m}^\star$, let s_λ be an integer with $0 \le s_\lambda \le n$ such that component function F_λ is s_λ-plateaued. Then $\mathcal{N}_F(0;x) = p^{2n-m} + p^{n-m}\sum_{\lambda \in \mathbb{F}_{p^m}^\star} p^{s_\lambda}$ for every $x \in \mathbb{F}_{p^n}$.

Proof. i.) For $x \in \mathbb{F}_{p^n}$ and $\lambda \in \mathbb{F}_{p^m}$, let $G(\lambda;x)$ be the complex valued function defined by

$$G(\lambda;x) = \sum_{a,b \in \mathbb{F}_{p^n}} \xi_p^{\mathcal{D}_b\mathcal{D}_a \mathrm{Tr}^m(\lambda F(x))}.$$

Clearly, for $\lambda = 0$, we have $G(0;x) = p^{2n}$ for every $x \in \mathbb{F}_{p^n}$. By Theorem 3.6, F is vectorial s-plateaued if and only if for every $\lambda \in \mathbb{F}_{p^m}^\star$ we have $G(\lambda;x) = p^{n+s}$ for

every $x \in \mathbb{F}_{p^n}$; equivalently, by (3.36), for every $v \in \mathbb{F}_{p^m}^\star$ we obtain

$$\widehat{G}(v;x) = G(0;x) - G(\lambda;x) = p^{2n} - p^{n+s}$$

for every $x \in \mathbb{F}_{p^n}$, by (3.35), the first assertion holds.

For the second statement, notice that for every $x \in \mathbb{F}_{p^n}$, we have

$$\mathcal{N}_F(0;x) + \sum_{v \in \mathbb{F}_{p^m}^\star} \mathcal{N}_F(v;x) = p^{2n}.$$

Hence, with the above arguments, we get $\mathcal{N}_F(0;x) = p^{n+s} + p^{2n-m} - p^{n+s-m}$ for every $x \in \mathbb{F}_{p^n}$.

ii.) Assume that F is vectorial plateaued. As F_λ is s_λ-plateaued for every $\lambda \in \mathbb{F}_{p^m}^\star$, we have $G(0;x) = p^{2n}$ and $G(\lambda;x) = p^{n+s_\lambda}$ for every $\lambda \in \mathbb{F}_{p^m}^\star$ and $x \in \mathbb{F}_{p^n}$. Then, for every $x \in \mathbb{F}_{p^n}$ we obtain

$$\widehat{G}(0;x) = p^{2n} + \sum_{\lambda \in \mathbb{F}_{p^m}^\star} p^{n+s_\lambda}.$$

Thus, the assertion follows from (3.35). □

The following characterization of vectorial bent functions is derived readily from Theorems 3.17 and 3.19.

Corollary 3.25. *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$. Then, F is vectorial p-ary bent if and only if $\mathcal{N}_F(0;x) = p^n + p^{2n-m} - p^{n-m}$ for every $x \in \mathbb{F}_{p^n}$.*

The following proposition is helpful to distinguish vectorial plateaued functions.

Proposition 3.10. *Let $F, G : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ be two vectorial plateaued functions. If $\mathcal{N}_F(v;x) = N_G(v;x)$ for every $v \in \mathbb{F}_{p^m}^\star$, which means that F and G have the same distribution for $\mathcal{D}_b\mathcal{D}_aF(x)$ and $\mathcal{D}_b\mathcal{D}_aG(x)$, then the component functions F_λ and G_λ are s_λ-plateaued functions with the same amplitude for every $\lambda \in \mathbb{F}_{p^m}^\star$.*

Proof. By (3.4), it follows from (3.34) and (3.35) that if $\mathcal{N}_F(v;x) = N_G(v;x)$ for every $v \in \mathbb{F}_{p^m}^\star$ and $x \in \mathbb{F}_{p^n}$, then for every $\lambda \in \mathbb{F}_{p^m}^\star$ and $x \in \mathbb{F}_{p^n}$ we have

$$\sum_{a,b \in \mathbb{F}_{p^n}} \xi_p^{\mathcal{D}_b\mathcal{D}_a \mathrm{Tr}^m(\lambda F(x))} = \sum_{a,b \in \mathbb{F}_{p^n}} \xi_p^{\mathcal{D}_b\mathcal{D}_a \mathrm{Tr}^m(\lambda G(x))}. \tag{3.37}$$

By Theorem 3.6, there exists an integer s_λ with $0 \leq s_\lambda \leq n$ for every $\lambda \in \mathbb{F}_{p^m}^\star$ such that the functions in (3.37) are equal to p^{n+s_λ} for every $x \in \mathbb{F}_{p^n}$. Hence, F_λ and G_λ are s_λ-plateaued functions with the same s_λ for every $\lambda \in \mathbb{F}_{p^m}^\star$. □

The characterizations of plateaued (vectorial) functions in terms of their second-order derivatives can be also given by means of their first-order derivatives, which potentially makes easier the study of checking the plateaued-ness of (vectorial) functions in arbitrary characteristic.

Proposition 3.11. *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$. For $v \in \mathbb{F}_{p^m}$, we have $\mathcal{N}_F(v; x) = \#\{(a, b) \in \mathbb{F}_{p^n}^2 : \mathcal{D}_a F(b) - \mathcal{D}_a F(x) = v\}$ for every $x \in \mathbb{F}_{p^n}$.*

Proof. For $(a, b) \in \mathbb{F}_{p^n}^2$ and for every $x \in \mathbb{F}_{p^n}$, by the (bijective) change of variable $b \to b - x$, we have $\mathcal{D}_b\mathcal{D}_a F(x) = \mathcal{D}_{b-x}\mathcal{D}_a F(x) = F(b + a) - F(b) - F(x + a) + F(x) = \mathcal{D}_a F(b) - \mathcal{D}_a F(x)$. Hence, the value distribution of $\mathcal{D}_b\mathcal{D}_a F(x)$ when $(a, b) \in \mathbb{F}_{p^n}^2$ is equal to the value distribution of $\mathcal{D}_a F(b) - \mathcal{D}_a F(x)$. This completes the proof. □

Notice that for all $a, b, c \in \mathbb{F}_{p^n}$ we have $\mathcal{D}_a\mathcal{D}_b F_\lambda(c) = \lambda \cdot \mathcal{D}_a\mathcal{D}_b F(c)$, where $F_\lambda = \lambda \cdot F$ for $\lambda \in \mathbb{F}_{p^m}^\star$. By Proposition 3.1 and Corollary 3.5, F is p-ary plateaued if and only if for all $x \in \mathbb{F}_{p^n}$ and $\lambda \in \mathbb{F}_{p^m}^\star$

$$\sum_{a,b,c \in \mathbb{F}_{p^n}} \xi_p^{\lambda \cdot \mathcal{D}_a\mathcal{D}_b F(c)} = p^n \sum_{a,b \in \mathbb{F}_{p^n}} \xi_p^{\lambda \cdot \mathcal{D}_a\mathcal{D}_b F(x)},$$

equivalently, applying the Fourier transform, by (3.4) for all $x \in \mathbb{F}_{p^n}$ and $v \in \mathbb{F}_{p^m}$

$$\#\{(a, b, c) \in \mathbb{F}_{p^n}^3 : \mathcal{D}_a\mathcal{D}_b F(c) = v\} = p^n \#\{(a, b) \in \mathbb{F}_{p^n}^2 : \mathcal{D}_a\mathcal{D}_b F(x) = v\} \quad (3.38)$$

that is, for all $v \in \mathbb{F}_{p^m}$, $\#\{(a, b) \in \mathbb{F}_{p^n}^2 : \mathcal{D}_a\mathcal{D}_b F(x) = v\}$ is independent of $x \in \mathbb{F}_{p^n}$. Thus, Corollary 3.5 can be also derived from Theorem 3.19.

Remark 3.6. If we add an affine function to F, then plateaued-ness of F is preserved because it does not change the value of the second-order derivative of F. On the other hand, adding a quadratic function to F changes this value since the distribution of the second-order derivative of F is dependent on x in general. We indicate this in the following results.

Corollary 3.26. *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$. Then, F is p-ary plateaued if and only if for all $x \in \mathbb{F}_{p^n}$, there exists a permutation ϕ_x of $\mathbb{F}_{p^n}^2$ defined as $\phi_x(a,b) = (a_x, b_x)$ such that $\mathcal{D}_b\mathcal{D}_aF(x) = \mathcal{D}_{b_x}\mathcal{D}_{a_x}F(0)$; or equivalently, there exists a permutation ψ_x of $\mathbb{F}_{p^n}^2$ defined as $\psi_x(a,b) = (a'_x, b'_x)$ such that $\mathcal{D}_aF(b) - \mathcal{D}_aF(x) = \mathcal{D}_{a'_x}F(b'_x) - \mathcal{D}_{a'_x}F(0)$.*

Proof. For $v \in \mathbb{F}_{p^m}$ and $x \in \mathbb{F}_{p^n}$, we define the sets

$$\left\{(a,b) \in \mathbb{F}_{p^n}^2 : \mathcal{D}_b\mathcal{D}_aF(x) = v\right\} \text{ and } \left\{(a_x,b_x) \in \mathbb{F}_{p^n}^2 : \mathcal{D}_{b_x}\mathcal{D}_{a_x}F(0) = v\right\} \quad (3.39)$$

Assume that F is p-ary plateaued. By Theorem 3.19, for each $x \in \mathbb{F}_{p^n}$ the sizes of the sets in (3.39) are equal for all $v \in \mathbb{F}_{p^m}$. Then for all $x \in \mathbb{F}_{p^n}$ there exists a permutation ϕ_x of $\mathbb{F}_{p^n}^2$ from the first set (defined for some value of v and $x \neq 0$) to the second set (defined for the same value of v and for $x = 0$) in (3.39) defined as $\phi_x(a,b) = (a_x, b_x)$. Conversely, because of the permutation ϕ_x, for all $v \in \mathbb{F}_{p^m}$ and $x \in \mathbb{F}_{p^n}$, the sizes of the sets in (3.39) are equal. By Theorem 3.19, F is p-ary plateaued.

For the second statement, we consider the sets

$$\{(a,b) \in \mathbb{F}_{p^n}^2 : \mathcal{D}_aF(b) - \mathcal{D}_aF(x) = v\} \text{ and} \quad (3.40)$$

$$\{(a'_x,b'_x) \in \mathbb{F}_{p^n}^2 : \mathcal{D}_{a'_x}F(b'_x) - \mathcal{D}_{a'_x}F(0) = v\} \quad (3.41)$$

for $v \in \mathbb{F}_{p^m}$ and $x \in \mathbb{F}_{p^n}$. By Theorem 3.19, using the above arguments, F is p-ary plateaued if and only if for all $x \in \mathbb{F}_{p^n}$, there exists a permutation ψ_x of $\mathbb{F}_{p^n}^2$ from the set in (3.40) to the set in (3.41) defined as $\psi_x(a,b) = (a'_x, b'_x)$. □

Recall that $\mathcal{D}_aF(b) - \mathcal{D}_aF(x) = \mathcal{D}_a\mathcal{D}_{b-x}F(x)$ for all $a, b, x \in \mathbb{F}_{p^n}$. Hence we have $\psi_x(a,b) = \phi_x(a, b-x)$ since $\mathcal{D}_{a'_x}F(b'_x) - \mathcal{D}_{a'_x}F(0) = \mathcal{D}_aF(b) - \mathcal{D}_aF(x) = \mathcal{D}_a\mathcal{D}_{b-x}F(x) = \mathcal{D}_{a''_x}\mathcal{D}_{b''_x}F(0) = \mathcal{D}_{a''_x}F(b''_x) - \mathcal{D}_{a''_x}F(0)$ where $\psi_x(a,b) = (a'_x, b'_x)$ and $\phi_x(a, b-x)$ is denoted by (a''_x, b''_x).

Remark 3.7. Notice that the simple permutation $\phi_x(a,b) = (a,b)$ for all $a, b \in \mathbb{F}_{p^n}$ correlates with quadratic functions. Actually, F admits such an associated ϕ_x if and only if $\mathcal{D}_b\mathcal{D}_aF(c) = \mathcal{D}_b\mathcal{D}_aF(0)$ at $(a,b) \in \mathbb{F}_{p^n}^2$ for all $c \in \mathbb{F}_{p^n}$, that is, $\mathcal{D}_c\mathcal{D}_b\mathcal{D}_aF(0) = 0$ at $(a,b,c) \in \mathbb{F}_{p^n}^3$, which means that it is a quadratic function.

Corollary 3.27. *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ be p-ary plateaued, and for all $x \in \mathbb{F}_{p^n}$, let ϕ_x be a permutation defined by $\phi_x(a, b) = (a_x, b_x)$ as in Corollary 3.26. Let $G : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ be a function such that $\mathcal{D}_b\mathcal{D}_a G(x) = \mathcal{D}_{b_x}\mathcal{D}_{a_x} G(0)$ at $(a, b) \in \mathbb{F}_{p^n}^2$ for all $x \in \mathbb{F}_{p^n}$. Then, $F + G$ is p-ary plateaued.*

Proof. By Corollary 3.26, for all $x \in \mathbb{F}_{p^n}$, we have $\mathcal{D}_b\mathcal{D}_a F(x) = \mathcal{D}_{b_x}\mathcal{D}_{a_x} F(0)$, where $(a_x, b_x) = \phi_x(a, b)$. Then, for all $x \in \mathbb{F}_{p^n}$, $\mathcal{D}_b\mathcal{D}_a(F + G)(x) = \mathcal{D}_b\mathcal{D}_a F(x) + \mathcal{D}_b\mathcal{D}_a G(x) = \mathcal{D}_{b_x}\mathcal{D}_{a_x} F(0) + \mathcal{D}_{b_x}\mathcal{D}_{a_x} G(0) = \mathcal{D}_{b_x}\mathcal{D}_{a_x}(F + G)(0)$ where $(a_x, b_x) = \phi_x(a, b)$. Thus, $F + G$ is p-ary plateaued. □

Remark 3.8. We derive from the above results that in general $F + G$ may not be p-ary plateaued when F is p-ary plateaued and G is quadratic. For a quadratic function G, although we have $\mathcal{D}_b\mathcal{D}_a G(x) = \mathcal{D}_b\mathcal{D}_a G(0)$ (see Remark 3.7), $\mathcal{D}_b\mathcal{D}_a G(x)$ may not be equal to $\mathcal{D}_{b_x}\mathcal{D}_{a_x} G(0)$ for some $x \in \mathbb{F}_{p^n}$, where $(a_x, b_x) = \phi_x(a, b)$ for the associated permutation ϕ_x of F.

We now investigate power functions on $\mathbb{F}_{p^n}$ in terms of their first-order derivatives. Power functions are exhaustively studied due to their interesting algebraic and combinatorial properties, and their applications in sequence design, coding theory and cryptography.

Corollary 3.28. *Let F be a power function on $\mathbb{F}_{p^n}$ defined as $F(x) = x^d$. For $v, x \in \mathbb{F}_{p^n}$, let $\mathcal{N}_F(v; x)$ be the size of the set $\{(a, b) \in \mathbb{F}_{p^n}^2 : \mathcal{D}_a F(b) - \mathcal{D}_a F(x) = v\}$. Then for all $v, x, \gamma \in \mathbb{F}_{p^n}$ with $\gamma \neq 0$,*

$$\mathcal{N}_F(v; x) = \#\{(a, b) \in \mathbb{F}_{p^n}^2 : \mathcal{D}_a F(b) - \mathcal{D}_a F(x/\gamma) = v/\gamma^d\}. \tag{3.42}$$

In particular, for all $v \in \mathbb{F}_{p^n}$, $\mathcal{N}_F(v; 0) = \mathcal{N}_F(v/\gamma^d; 0)$ for any $\gamma \in \mathbb{F}_{p^n}^\star$. Moreover

i.) F is p-ary plateaued if and only if $\mathcal{N}_F(v; 1) = \mathcal{N}_F(v; 0)$ for all $v \in \mathbb{F}_{p^n}$.

ii.) F is p-ary plateaued with single amplitude if and only if $\mathcal{N}_F(0; 1) = \mathcal{N}_F(0; 0)$ and there exists an integer u such that $\mathcal{N}_F(v; 1) = \mathcal{N}_F(v; 0) = u$ for all $v \in \mathbb{F}_{p^n}^\star$.

If F is p-ary plateaued and $\gcd(d, p^n - 1) = 1$, then it has a single amplitude.

Proof. For all $\gamma \in \mathbb{F}_{p^n}$ with $\gamma \neq 0$, by the bijective change of variable $a \mapsto \gamma a$ and $b \mapsto \gamma b$, we have $\#\{(a,b) \in \mathbb{F}_{p^n}^2 : \mathcal{D}_a F(b) - \mathcal{D}_a F(x) = v\} = \#\{(a,b) \in \mathbb{F}_{p^n}^2 : \mathcal{D}_{\gamma a} F(\gamma b) - \mathcal{D}_{\gamma a} F(x) = v\}$. For all $a, b, x, \gamma \in \mathbb{F}_{p^n}$ with $\gamma \neq 0$, we can easily see $\mathcal{D}_{\gamma a} F(\gamma b) = (\gamma b + \gamma a)^d - (\gamma b)^d = \gamma^d \mathcal{D}_a F(b)$ and $\mathcal{D}_{\gamma a} F(x) = \gamma^d \mathcal{D}_a F(x/\gamma)$. Hence, (3.42) holds for all $v, x, \gamma \in \mathbb{F}_{p^n}$ with $\gamma \neq 0$.

In particular, for $x = 0$ in (3.42), we have $\#\{(a,b) \in \mathbb{F}_{p^n}^2 : \mathcal{D}_a F(b) - \mathcal{D}_a F(0) = v\} = \#\{(a,b) \in \mathbb{F}_{p^n}^2 : \mathcal{D}_a F(b) - \mathcal{D}_a F(0) = v/\gamma^d\}$, that is, $\mathcal{N}_F(v;0) = \mathcal{N}_F(v/\gamma^d;0)$ for all $v, \gamma \in \mathbb{F}_{p^n}$ with $\gamma \neq 0$.

We now prove (*i*). By (3.42), for all $v \in \mathbb{F}_{p^n}$ we have (by taking $\gamma = x$ for $x \neq 0$)

$$\mathcal{N}_F(v;x) = \#\{(a,b) \in \mathbb{F}_{p^n}^2 : \mathcal{D}_a F(b) - \mathcal{D}_a F(1) = v/x^d\}. \tag{3.43}$$

Assume that $\mathcal{N}_F(v;1) = \mathcal{N}_F(v;0)$ for all $v \in \mathbb{F}_{p^n}$. Then we have $\#\{(a,b) \in \mathbb{F}_{p^n}^2 : \mathcal{D}_a F(b) - \mathcal{D}_a F(1) = v/x^d\} = \#\{(a,b) \in \mathbb{F}_{p^n}^2 : \mathcal{D}_a F(b) - \mathcal{D}_a F(0) = v/x^d\}$, which equals $\#\{(a,b) \in \mathbb{F}_{p^n}^2 : \mathcal{D}_a F(b) - \mathcal{D}_a F(0) = v\}$ from the second statement. Then, for all $v \in \mathbb{F}_{p^n}$, $\mathcal{N}_F(v;x) = \mathcal{N}_F(v;0)$ for all $x \in \mathbb{F}_{p^n}^\star$ by (3.43). Hence, F is p-ary plateaued by Theorem 3.19. The other direction is clear from Theorem 3.19.

Next we prove (*ii*). Theorem 3.19 says that F is p-ary plateaued with single amplitude if and only if there exist two integers u_1 and u_2 such that $\mathcal{N}_F(0;x) = u_1$ and $\mathcal{N}_F(v;x) = u_2$ for all $x \in \mathbb{F}_{p^n}$ and $v \in \mathbb{F}_{p^n}^\star$. Assume that $\mathcal{N}_F(0;1) = \mathcal{N}_F(0;0)$ and there exists an integer u such that $\mathcal{N}_F(v;1) = \mathcal{N}_F(v;0) = u$ for all $v \in \mathbb{F}_{p^n}^\star$. From the proof of (*i*), we have

$$\mathcal{N}_F(v;x) = \mathcal{N}_F(v;0)$$

for all $v, x \in \mathbb{F}_{p^n}$ with $x \neq 0$. Combining them, we conclude that $\mathcal{N}_F(v;x) = u$ for all $v, x \in \mathbb{F}_{p^n}$ with $v \neq 0$ and $\mathcal{N}_F(0;x)$ is independent of $x \in \mathbb{F}_{p^n}$. Hence, by Theorem 3.19, F is p-ary plateaued with single amplitude. The other direction follows from Theorem 3.19.

Finally we prove the last assertion. Assume that F is p-ary plateaued. By (*i*), $\mathcal{N}_F(v;1) = \mathcal{N}_F(v;0)$ for all $v \in \mathbb{F}_{p^n}$. From the second assertion, $\mathcal{N}_F(v;0) = \mathcal{N}_F(v/\gamma^d;0)$ for all $v, \gamma \in \mathbb{F}_{p^n}$ with $\gamma \neq 0$. Then,

$$\mathcal{N}_F(v;1) = \mathcal{N}_F(v/\gamma^d;0)$$

for all $v, \gamma \in \mathbb{F}_{p^n}$ with $\gamma \neq 0$. For $v = 0$, it is obvious that $\mathcal{N}_F(0;1) = \mathcal{N}_F(0;0)$. For $v \in \mathbb{F}_{p^n}^\star$, if we set $v = 1$ and using the fact $\gcd(d, p^n - 1) = 1$, then $\gamma \mapsto 1/\gamma^d$ is a permutation of $\mathbb{F}_{p^n}^\star$. Then we get $\mathcal{N}_F(1,1) = \mathcal{N}_F(v,0)$ for all $v \in \mathbb{F}_{p^n}^\star$, that is, $\mathcal{N}_F(v,0) = \mathcal{N}_F(v;1)$ does not depend on $v \in \mathbb{F}_{p^n}^\star$. Hence, plateaued function F has single amplitude by (*ii*). □

Remark 3.9. With the above notations, for the power function $F(x) = x^d$, in general we have $\mathcal{N}_F(v;1) \neq \mathcal{N}_F(v/\gamma^d;1)$ for $v, \gamma \in \mathbb{F}_{p^n}$ with $\gamma \neq 0$. However, the equality case is necessary for plateaued-ness.

Below, we consider plateaued-ness property of vectorial p-ary functions whose component functions are all unbalanced.

Remark 3.10. A function is balanced if and only if its Walsh transform vanishes at the zero input.

Theorem 3.21. *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$, and let the functions F_λ, $\lambda \in \mathbb{F}_{p^m}^\star$, be unbalanced. Then, F is p-ary plateaued if and only if for all $v \in \mathbb{F}_{p^m}$ and $x \in \mathbb{F}_{p^n}$*

$$\mathcal{N}_F(v;x) = \#\{(a,b) \in \mathbb{F}_{p^n}^2 : F(a) - F(b) = v\}. \tag{3.44}$$

In particular, F is p-ary plateaued with single amplitude if and only if for all $v \in \mathbb{F}_{p^m}$ and $x \in \mathbb{F}_{p^n}$ (3.44) holds and is independent of $v \in \mathbb{F}_{p^m}^\star$.

Proof. Assume that F is p-ary plateaued. Since $F_\lambda = \lambda \cdot F$, $\lambda \in \mathbb{F}_{p^m}^\star$, are all unbalanced p-ary plateaued of the amplitude μ_λ, we have $\widehat{\chi_{F_\lambda}}(0) \neq 0$ for all $\lambda \in \mathbb{F}_{p^m}^\star$ (and also for $\lambda = 0$), and hence $\mu_\lambda^2 = |\widehat{\chi_{F_\lambda}}(0)|^2$. For $\lambda \in \mathbb{F}_{p^m}$, since $|z|^2 = z\overline{z}$ for $z \in \mathbb{C}$, we can easily see

$$|\widehat{\chi_{F_\lambda}}(0)|^2 = \sum_{a,b \in \mathbb{F}_{p^n}} \xi_p^{\lambda \cdot (F(a) - F(b))}. \tag{3.45}$$

Recall that $\mathcal{D}_a\mathcal{D}_b F_\lambda(x) = \lambda \cdot (\mathcal{D}_a\mathcal{D}_b F(x))$ for all $a, b, x \in \mathbb{F}_{p^n}$ and $\lambda \in \mathbb{F}_{p^m}$. Then, by Theorem 3.6, for all $x \in \mathbb{F}_{p^n}$ and $\lambda \in \mathbb{F}_{p^m}$ we have

$$G(\lambda; x) = \sum_{a,b \in \mathbb{F}_{p^n}} \xi_p^{\lambda \cdot \mathcal{D}_a\mathcal{D}_b F(x)} = \sum_{a,b \in \mathbb{F}_{p^n}} \xi_p^{\lambda \cdot (F(a) - F(b))}, \tag{3.46}$$

where the second equality follows from (3.45). By (3.4), for all $x \in \mathbb{F}_{p^n}$ and $v \in \mathbb{F}_{p^m}$, the Fourier transforms of the equal functions in (3.46) are equal:

$$\widehat{G}(v;x) = \sum_{\lambda \in \mathbb{F}_{p^m}} \sum_{a,b \in \mathbb{F}_{p^n}} \xi_p^{\lambda \cdot (\mathcal{D}_a\mathcal{D}_b F(x) - v)} = \sum_{\lambda \in \mathbb{F}_{p^m}} \sum_{a,b \in \mathbb{F}_{p^n}} \xi_p^{\lambda \cdot (F(a) - F(b) - v)}, \tag{3.47}$$

equivalently, $\widehat{G}(v;x) = p^m\#\{(a,b) \in \mathbb{F}_{p^n}^2 : \mathcal{D}_a\mathcal{D}_bF(x) = v\} = p^m\#\{(a,b) \in \mathbb{F}_{p^n}^2 : F(a) - F(b) = v\}$. Hence, the assertion holds. Conversely, assume that for all $x \in \mathbb{F}_{p^n}$ and $v \in \mathbb{F}_{p^m}$ (3.44) holds, that is, (3.47) holds. By (3.4), for all $x \in \mathbb{F}_{p^n}$ and $\lambda \in \mathbb{F}_{p^m}$, (3.46) holds, equivalently by (3.45), $G(\lambda;x) = |\widehat{\chi_{F_\lambda}}(0)|^2$, which is nonzero since F_λ, $\lambda \in \mathbb{F}_{p^m}^\star$, are all unbalanced. Then, for all $\lambda \in \mathbb{F}_{p^m}^\star$, $G(\lambda;x)$ does not depend on $x \in \mathbb{F}_{p^n}$. By Theorem 3.6, F_λ, $\lambda \in \mathbb{F}_{p^m}^\star$, is p-ary plateaued, and hence, F is p-ary plateaued.

We prove the last assertion. Theorem 3.6 says that F is p-ary plateaued with single amplitude if and only if $G(\lambda;x)$ in (3.46) does not depend on $x \in \mathbb{F}_{p^n}$ nor λ for $\lambda \neq 0$; equivalently by (3.4), $\widehat{G}(v;x)$ in (3.47) does not depend on $x \in \mathbb{F}_{p^n}$ nor on v for $v \neq 0$. Hence, using the above arguments, the proof is complete. □

In view of Theorem 3.21, the following corollary is derived directly from Corollary 3.25 and Theorem 3.20.

Corollary 3.29. *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ be a function such that all of whose component functions are unbalanced. Then F is vectorial p-ary s-plateaued if and only if for all $v \in \mathbb{F}_{p^m}^\star$*

$$\#\{(a,b) \in \mathbb{F}_{p^n}^2 : F(a) - F(b) = v\} = p^{2n-m} - p^{n+s-m}.$$

In this case, we also have $\#\{(a,b) \in \mathbb{F}_{p^n}^2 : F(a) = F(b)\} = p^{2n-m} + p^{n+s} - p^{n+s-m}$. In particular, F is vectorial p-ary bent if and only if

$$\#\{(a,b) \in \mathbb{F}_{p^n}^2 : F(a) = F(b)\} = p^{2n-m} + p^n - p^{n-m}.$$

3.3.3 p-Ary Strongly-Plateaued Functions over $\mathbb{F}_p$

In this subsection, we study a particular case of p-ary plateaued (vectorial) functions: when the value distribution of $b \mapsto \mathcal{D}_a\mathcal{D}_bF(x)$ is independent of $x \in \mathbb{F}_{p^n}$ for each fixed value of a although the value distribution of $\mathcal{D}_b\mathcal{D}_aF(x)$ when $(a,b) \in \mathbb{F}_{p^n}^2$ is independent of $x \in \mathbb{F}_{p^n}$ in Theorem 3.19.

Definition 3.3. Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$. Then, F is called *vectorial p-ary strongly-plateaued* if for all $a \in \mathbb{F}_{p^n}$ and $v \in \mathbb{F}_{p^m}$, the size of the set $\{b \in \mathbb{F}_{p^n} : \mathcal{D}_a\mathcal{D}_bF(x) =$

$v\}$ is independent of $x \in \mathbb{F}_{p^n}$. In particular, $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is called *p-ary strongly-plateaued* if for all $a \in \mathbb{F}_{p^n}$ and $v \in \mathbb{F}_p$, the size of the set $\{b \in \mathbb{F}_{p^n} : \mathcal{D}_a\mathcal{D}_b f(x) = v\}$ is independent of $x \in \mathbb{F}_{p^n}$.

Remark 3.11. By Theorem 3.19, any p-ary strongly-plateaued function is the p-ary plateaued function. Moreover, a vectorial p-ary function is strongly-plateaued if and only if its component functions are p-ary strongly-plateaued.

Proposition 3.12. *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$. For all $a, x \in \mathbb{F}_{p^n}$ and $v \in \mathbb{F}_{p^m}$ we have $\#\{b \in \mathbb{F}_{p^n} : \mathcal{D}_a\mathcal{D}_b F(x) = v\} = \#\{b \in \mathbb{F}_{p^n} : \mathcal{D}_a F(b) - \mathcal{D}_a F(x) = v\}$.*

Proof. For all $a, b, x \in \mathbb{F}_{p^n}$, (by the bijective change of variable $b \mapsto b - x$), we have $\mathcal{D}_a\mathcal{D}_b F(x) = \mathcal{D}_a\mathcal{D}_{b-x}F(x) = F(a + b) - F(x + a) - F(b) + F(x) = \mathcal{D}_a F(b) - \mathcal{D}_a F(x)$. This completes the proof. □

The notion of p-ary strongly-plateaued is closely connected to p-ary partially-bent.

Proposition 3.13. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Then f is p-ary strongly-plateaued if and only if f is p-ary partially-bent.*

Proof. By Definition 2.12, f is p-ary partially-bent if and only if the derivative $\mathcal{D}_a f$ is either balanced or constant for all $a \in \mathbb{F}_{p^n}$; equivalently, for all $v \in \mathbb{F}_{p^m}$ and $a \in \mathbb{F}_{p^n}$, $\#\{b \in \mathbb{F}_{p^n} : \mathcal{D}_a f(b) = \mathcal{D}_a f(x) + v\}$ is independent of $x \in \mathbb{F}_{p^n}$, that is, f is p-ary strongly-plateaued by Proposition 3.12. □

Proposition 3.14. *A vectorial p-ary function is strongly-plateaued if and only if all of its component functions are p-ary partially-bent. In particular, p-ary bent and quadratic (vectorial) functions are p-ary strongly-plateaued (vectorial) functions.*

Proof. The first assertion follows from Remark 3.11 and Proposition 3.13. By Remark 2.4, the last assertion follows from the first assertion. □

3.4 Characterizations of Vectorial Plateaued p-Ary Functions

This section, in order to characterize plateaued vectorial p-ary functions, makes use of the Walsh power moments and autocorrelation functions of their component func-

tions. We first characterize plateaued vectorial functions by using Walsh power moments of their component functions in arbitrary characteristic.

We can extract from Theorem 3.9 the following characterization of vectorial plateaued functions.

Theorem 3.22. *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ and let F_λ, $\lambda \in \mathbb{F}_{p^m}^\star$, be the component functions of F. Then, F is vectorial s-plateaued if and only if*

$$\sum_{\lambda \in \mathbb{F}_{p^m}^\star} S_2(F_\lambda) = p^{3n+s}(p^m - 1) \text{ and } \sum_{\lambda \in \mathbb{F}_{p^m}^\star} S_3(F_\lambda) = p^{4n+2s}(p^m - 1). \tag{3.48}$$

Proof. Assume that F is vectorial s-plateaued, that is, F_λ, $\lambda \in \mathbb{F}_{p^m}^\star$, is s-plateaued. By Theorem 3.9, we conclude that (3.48) holds. Conversely, suppose that (3.48) holds. By (3.1) with $A = p^{n+s}$ and $i = 1$, for all $\lambda \in \mathbb{F}_{p^m}^\star$ we have

$$D_\lambda = \sum_{\omega \in \mathbb{F}_{p^n}} (|\widehat{\chi_{F_\lambda}}(\omega)|^2 - p^{n+s})^2 |\widehat{\chi_{F_\lambda}}(\omega)|^2 = S_3(F_\lambda) - 2p^{n+s} S_2(F_\lambda) + p^{2(n+s)} S_1(F_\lambda).$$

By (3.48) and using the Parseval identity, we have

$$\sum_{\lambda \in \mathbb{F}_{p^m}^\star} D_\lambda = p^{4n+2s}(p^m - 1) - 2p^{n+s} p^{3n+s}(p^m - 1) + p^{2n+2s} p^{2n}(p^m - 1) = 0.$$

Then, since $D_\lambda \geq 0$ and $\sum_{\lambda \in \mathbb{F}_{p^m}^\star} D_\lambda = 0$, we get $D_\lambda = 0$ for every $\lambda \in \mathbb{F}_{p^m}^\star$. Hence, for every $\lambda \in \mathbb{F}_{p^m}^\star$, $|\widehat{\chi_{F_\lambda}}(\omega)|^2 \in \{0, p^{n+s}\}$ for all $\omega \in \mathbb{F}_{p^n}$, namely, F_λ, $\lambda \in \mathbb{F}_{p^m}^\star$, is s-plateaued. Hence, F is vectorial s-plateaued. □

To give the next characterization of vectorial s-plateaued functions, we recall the following result.

Proposition 3.15. *[55] Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ and let F_λ, $\lambda \in \mathbb{F}_{p^m}^\star$, be its component functions. Then*

$$\sum_{\lambda \in \mathbb{F}_{p^m}^\star} S_2(F_\lambda) = p^{n+m} \mathfrak{N}(F) - p^{4n}.$$

Theorem 3.23. *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ and let F_λ, $\lambda \in \mathbb{F}_{p^m}^\star$, be its component functions. Then, F is vectorial s-plateaued if and only if $S_3(F_\lambda) = p^{4n+2s}$ for all $\lambda \in \mathbb{F}_{p^m}^\star$ and*

$$\mathfrak{N}(F) = p^{3n-m} + p^{2n+s} - p^{2n+s-m}.$$

Proof. Assume that F is vectorial s-plateaued. By Theorem 3.9, we have $S_2(F_\lambda) = p^{3n+s}$ and $S_3(F_\lambda) = p^{4n+2s}$ for all $\lambda \in \mathbb{F}_{p^m}^\star$. By Proposition 3.15, we get

$$p^{3n+s}(p^m - 1) = p^{n+m}\mathfrak{N}(F) - p^{4n}.$$

Thus, the assertion holds. Conversely, we have $\sum_{\lambda \in \mathbb{F}_{p^m}^\star} S_3(F_\lambda) = p^{4n+2s}(p^m - 1)$, and by Proposition 3.15, we get

$$\sum_{\lambda \in \mathbb{F}_{p^m}^\star} S_2(F_\lambda) = p^{n+m}(p^{3n-m} + p^{2n+s} - p^{2n+s-m}) - p^{4n} = p^{3n+s}(p^m - 1).$$

By Theorem 3.22, F is vectorial s-plateaued. □

In view of Proposition 3.6, we can deduce the following.

Theorem 3.24. *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ and let F_λ, $\lambda \in \mathbb{F}_{p^m}^\star$, be its component functions. Then for all integers $i \geq 1$, we have*

$$\sum_{\lambda \in \mathbb{F}_{p^m}^\star} S_{i+1}(F_\lambda)^2 \leq \sum_{\lambda \in \mathbb{F}_{p^m}^\star} S_{i+2}(F_\lambda) S_i(F_\lambda), \tag{3.49}$$

equivalently,

$$\sum_{\lambda \in \mathbb{F}_{p^m}^\star} S_{i+1}(F_\lambda) \leq \sum_{\lambda \in \mathbb{F}_{p^m}^\star} \sqrt{S_{i+2}(F_\lambda) S_i(F_\lambda)}, \tag{3.50}$$

with an equality if and only if F is p-ary plateaued.

Proof. The inequalities (3.49) and (3.50) follows easily from (3.17). To prove equality cases, notice that by (3.17) we have

$$S_{i+2}(F_\lambda) S_i(F_\lambda) - S_{i+1}(F_\lambda)^2 \geq 0$$

for all $\lambda \in \mathbb{F}_{p^m}^\star$. Thanks to the well known fact that a sum of nonnegative terms is zero if and only if each term is zero, the inequality (3.49) (equivalently, (3.50)) becomes an equality if and only if F_λ, $\lambda \in \mathbb{F}_{p^m}^\star$, are all p-ary plateaued by (3.17); equivalently, F is p-ary plateaued. □

Theorem 3.24, in the case of $i = 1$, suggests the following corollary.

Corollary 3.30. *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ and let F_λ, $\lambda \in \mathbb{F}_{p^m}^\star$, be the component functions of F. Then we have*

$$\sum_{\lambda \in \mathbb{F}_{p^m}^\star} S_2(F_\lambda)^2 \leq p^{2n} \sum_{\lambda \in \mathbb{F}_{p^m}^\star} S_3(F_\lambda),$$

equivalently, $\sum_{\lambda \in \mathbb{F}_{p^m}^\star} S_2(F_\lambda) \leq p^n \sum_{\lambda \in \mathbb{F}_{p^m}^\star} \sqrt{S_3(F_\lambda)}$, with an equality if and only if F is p-ary plateaued.

In the light of Remark 3.5, clearly we have the following corollaries.

Corollary 3.31. *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$, and let F_λ, $\lambda \in \mathbb{F}_{p^m}^\star$, be the component functions of F. Then F is p-ary plateaued if and only if for each $\lambda \in \mathbb{F}_{p^m}^\star$,*

$$S_2(F_\lambda) = p^{2n} \theta_{F_\lambda}(x)$$

for all $x \in \mathbb{F}_{p^n}$. In particular, F is p-ary plateaued with single amplitude if and only if, additionally, $S_2(F_\lambda)$ does not depend on λ for $\lambda \neq 0$.

Proof. By Remark 3.5, the first assertion is a direct consequence of Corollary 3.5. The second assertion follows from Theorems 3.6 and 3.19. □

Corollary 3.32. *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ and let F_λ, $\lambda \in \mathbb{F}_{p^m}^\star$, be the component functions of F. Then, F is p-ary plateaued if and only if*

$$\sum_{\omega \in \mathbb{F}_{p^n}} \widehat{\chi_{F_\lambda}}(\alpha + \omega) \overline{\widehat{\chi_{F_\lambda}}(\omega)} \, |\widehat{\chi_{F_\lambda}}(\omega)|^2 \; = 0$$

for all $\alpha \in \mathbb{F}_{p^n}^\star$ and $\lambda \in \mathbb{F}_{p^m}^\star$. In particular, F is p-ary plateaued with single amplitude if and only if, additionally, $S_2(F_\lambda)$ does not depend on λ for $\lambda \neq 0$.

Proof. By Remark 3.5, the first assertion is a direct consequence of Theorem 3.14. The second assertion follows from Theorems 3.6 and 3.19. □

Corollary 3.33. *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$, and let F_λ, $\lambda \in \mathbb{F}_{p^m}^\star$, be the component functions of F. Then F is p-ary plateaued if and only if for all $x \in \mathbb{F}_{p^n}$ and $\lambda \in \mathbb{F}_{p^m}^\star$*

$$\sum_{\omega \in \mathbb{F}_{p^n}} |\widehat{\chi_{F_\lambda}}(\omega)|^4 = p^n \sum_{\omega \in \mathbb{F}_{p^n}} \xi_p^{F_\lambda(x) - \omega \cdot x} \overline{\widehat{\chi_{F_\lambda}}(\omega)} |\widehat{\chi_{F_\lambda}}(\omega)|^2. \tag{3.51}$$

In particular, F is p-ary plateaued with single amplitude if and only if for all $x \in \mathbb{F}_{p^n}$ and $\lambda \in \mathbb{F}_{p^m}^\star$ (3.51) holds and is independent of $\lambda \neq 0$.

Proof. By Remark 3.5, the first statement is a direct consequence of Corollary 3.20. The second assertion follows from Theorems 3.6 and 3.19. □

Considering $F_\lambda = \lambda \cdot F$ for $\lambda \in \mathbb{F}_{p^m}^\star$, for all $x \in \mathbb{F}_{p^n}$ and $\lambda \in \mathbb{F}_{p^m}^\star$ the equality (3.51) is equivalent to:

$$\sum_{\omega,a,b,c,d \in \mathbb{F}_{p^n}} \xi_p^{\lambda\cdot(F(a)-F(b)+F(c)-F(d))-\omega\cdot(a-b+c-d)} = p^n \sum_{\omega,a,b,c \in \mathbb{F}_{p^n}} \xi_p^{\lambda\cdot(F(x)-F(a)+F(b)-F(c))-\omega\cdot(x-a+b-c)},$$

equivalently,

$$\sum_{a,b,c \in \mathbb{F}_{p^n}} \xi_p^{\lambda\cdot(F(a)-F(b)+F(c)-F(a-b+c))} = p^n \sum_{a,b \in \mathbb{F}_{p^n}} \xi_p^{\lambda\cdot(F(x)-F(a)+F(b)-F(x-a+b))},$$

that is, (by the bijective change of variables: $a \mapsto a+b+c$ and $b \mapsto b+c$ in the left-hand side, and $a \mapsto a+x$ and $b \mapsto a+b+x$ in the right-hand side) we have

$$\sum_{a,b,c \in \mathbb{F}_{p^n}} \xi_p^{\lambda\cdot(\mathcal{D}_b\mathcal{D}_a F(c))} = p^n \sum_{a,b \in \mathbb{F}_{p^n}} \xi_p^{\lambda\cdot(\mathcal{D}_b\mathcal{D}_a F(x))},$$

which is equivalent to (3.38). Namely, the characterizations given by Corollaries 3.20 and 3.5 are equivalent.

In the following, we extend to arbitrary characteristic the characterizations of plateaued vectorial Boolean functions in terms of autocorrelation functions of their component functions.

We can derive from Remark 3.5 and Theorem 3.15 the following.

Corollary 3.34. *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ and let F_λ, $\lambda \in \mathbb{F}_{p^m}^\star$, be the component functions of F. Then, F is p-ary plateaued with single amplitude μ if and only if for all $x \in \mathbb{F}_{p^n}$ and $\lambda \in \mathbb{F}_{p^m}^\star$, we have*

$$\sum_{a \in \mathbb{F}_{p^n}} \Delta_{F_\lambda}(a)\Delta_{F_\lambda}(x-a) = \mu^2 \Delta_{F_\lambda}(x).$$

In the light of Remark 3.5 and Corollary 3.21, obviously we have the following.

Corollary 3.35. *Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ and let F_λ, $\lambda \in \mathbb{F}_{p^m}^\star$, be the component functions of F. Then, F is p-ary plateaued with single amplitude μ if and only if for all $x \in \mathbb{F}_{p^n}$*

and $\lambda \in \mathbb{F}_{p^m}^\star$,

$$\sum_{a,b\in\mathbb{F}_{p^n}} \Delta_{F_\lambda}(a)\Delta_{F_\lambda}(b)\Delta_{F_\lambda}(x-a-b) = \mu^2 \sum_{c\in\mathbb{F}_{p^n}} \Delta_{F_\lambda}(c)\Delta_{F_\lambda}(x-c).$$

In a similar way, considering Remark 3.5 and Corollary 3.22, we have the following.

Corollary 3.36. *Let* $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$*, and* F_λ*,* $\lambda \in \mathbb{F}_{p^m}^\star$*, be the component functions of* F*. Then,* F *is* p*-ary plateaued if and only if for all* $x \in \mathbb{F}_{p^n}$ *and* $\lambda \in \mathbb{F}_{p^m}^\star$*,*

$$p^n \sum_{a\in\mathbb{F}_{p^n}} \Delta_{F_\lambda}(a)\Delta_{F_\lambda}(x-a) = \sum_{a\in\mathbb{F}_{p^n}} |\Delta_{F_\lambda}(a)|^2\Delta_{F_\lambda}(x).$$

We can rewrite Corollary 3.36 as follows. A p-ary function f is plateaued if and only if for all $x \in \mathbb{F}_{p^n}$ (by the bijective change of variable $a \mapsto a-b$)

$$\begin{aligned} & p^n \sum_{a,b,c\in\mathbb{F}_{p^n}} \xi_p^{-f(a)+f(b)+f(c)-f(-a+b+c+x)} \\ &= \sum_{a,b,c,d\in\mathbb{F}_{p^n}} \xi_p^{-f(a)+f(b)+f(c)-f(-a+b+c)+f(d)-f(d+x)}. \end{aligned}$$

For vectorial $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$, we can write this by considering $f = \lambda \cdot F$ for $\lambda \in \mathbb{F}_{p^m}^\star$. Applying the Fourier transform, by (3.4) their Fourier transforms are equal, and hence we deduce (see the proof of Theorem 3.19) the following.

Corollary 3.37. *A vectorial function* F *is plateaued if and only if for all* $x \in \mathbb{F}_{p^n}$ *and* $v \in \mathbb{F}_{p^m}$ $p^n\#\{(a,b,c) \in \mathbb{F}_{p^n}^3 : -F(a)+F(b)+F(c)-F(-a+b+c+x) = v\} = \#\{(a,b,c,d) \in \mathbb{F}_{p^n}^4 : -F(a)+F(b)+F(c)-F(-a+b+c)+F(d)-F(d+x) = v\}$.

We end this section with the following result, which follows directly from Remark 3.5 and Corollary 3.4.

Corollary 3.38. *Let* $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$*, and let* F_λ*,* $\lambda \in \mathbb{F}_{p^m}^\star$*, be the component functions of* F*. Then* F *is vectorial* p*-ary bent if and only if* $\sum_{a\in\mathbb{F}_{p^n}} |\Delta_{F_\lambda}(a)|^2 = p^{2n}$ *for all* $\lambda \in \mathbb{F}_{p^m}^\star$*.*

Remark 3.12. It is worth noting that all characterizations of plateaued p-ary functions can be given for vectorial plateaued p-ary functions by the component functions in the light of Remark 3.5.

3.5 Cubic (Homogeneous) Bent and Plateaued p-Ary Functions

This section studies (homogeneous) cubic functions. In this section, the characterization of bent and plateaued functions in terms of their second-order derivatives is devoted especially to (homogeneous) cubic functions. This reveals the non-existence of a homogeneous cubic bent function (and a (homogeneous) cubic plateaued function for some cases) in odd characteristic. Moreover, we use a rank notion which generalizes the rank notion of quadratic function in arbitrary characteristic and we give a simple algorithm to determine it. This rank notion discovers new results about (homogeneous) cubic plateaued functions.

3.5.1 Cubic (Homogeneous) Bent p-Ary Functions

In this subsection, we provide new results on (homogeneous) cubic bent functions in arbitrary characteristic. Indeed, we observe that there does not exist homogeneous cubic bent functions in odd characteristic (see Corollary 3.39). On the other hand, by Remark 3.16 and Example 3.6 we point out that it is not the case for even characteristic. We give a concrete example of homogeneous cubic s-plateaued functions in odd characteristic when $s > 0$ to show their existence.

We begin with the notion of cubic functions in arbitrary characteristic. Let f be a cubic function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$. Then, f can be written as

$$f(x) = \mathrm{Tr}_p^{p^n}(xD(x)) + \mathrm{Tr}_p^{p^n}(xA(x)) + \alpha(x). \tag{3.52}$$

Hence, D is a quadratic polynomial given by

$$D(x) = \sum_{0 \le i < j \le n-1} d_{ij} x^{2^i+2^j} \text{ with } d_{ij} \in \mathbb{F}_{2^n} \quad \text{if } p = 2$$

and

$$D(x) = \sum_{0 \le i \le j \le n-1} d_{ij} x^{p^i+p^j} \text{ with } d_{ij} \in \mathbb{F}_{p^n} \quad \text{if } p \neq 2. \tag{3.53}$$

Moreover, here A is a linearized polynomial given by

$$A(x) = \sum_{0 \le i \le n-1} a_i x^{p^i} \text{ with } a_i \in \mathbb{F}_{p^n} \tag{3.54}$$

and $\alpha(x)$ is an affine polynomial for $x \in \mathbb{F}_{p^n}$. Notice that $\mathcal{D}_a\mathcal{D}_b\alpha(x)$ is equal to zero for every $a, b, x \in \mathbb{F}_{p^n}$. Then by Theorem 3.6, a cubic function f as in (3.52) is plateaued if and only if $\mathrm{Tr}_p^{p^n}(xD(x)) + \mathrm{Tr}_p^{p^n}(xA(x))$ is plateaued. Therefore, without loss of generality we assume that $f(x) = \mathrm{Tr}_p^{p^n}(xD(x)) + \mathrm{Tr}_p^{p^n}(xA(x))$, i.e., $\alpha(x) = 0$ throughout this section.

Definition 3.4. We say that a cubic function f as in (3.52) is homogeneous if the linearized polynomial A in (3.54) is the zero polynomial.

Remark 3.13. Choosing a basis $\{w_1, w_2, \ldots, w_n\}$ of $\mathbb{F}_2^n$ and considering $x = x_1w_1 + \cdots + x_nw_n$ with $x_i \in \mathbb{F}_2$, any function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ can be represented as an element of $\mathbb{F}_2[x_1, \ldots, x_n]/\langle x_1^2 - x_1, \ldots, x_n^2 - x_n\rangle$. This representation is called algebraic normal form or multivariate form. In the literature a Boolean cubic function is called homogeneous if it has only cubic terms in algebraic normal form. The notions of algebraic normal form (multivariate form) and homogeneous function in this sense also exist in odd characteristic (see, e.g., [57, Section 1.3]). It is well known that a Boolean homogeneous cubic function becomes Boolean cubic containing (multivariate) quadratic terms or linear terms under a linear isomorphism. However, this is not the case for homogeneous cubic functions if $p > 3$. Moreover if $p = 3$, then a homogeneous cubic function becomes a cubic function containing linear terms (but not quadratic terms). Therefore, using Definition 3.4 the notions of homogeneous cubic functions and algebraic normal form are the same for $p > 3$. Moreover they can be considered to be the same for plateaued functions without loss of generality if $p = 3$ as they may differ only by linear terms. However, for $p = 2$ and $n = 6$, there is an important difference for cubic bent functions in the notions of homogeneous functions in the sense of Definition 3.4 and in the sense of this remark using algebraic normal form (see Remark 3.17 below).

Let $B : \mathbb{F}_{p^n} \times \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be the quadratic map depending on D defined as

$$B(x, y) = D(x + y) - D(x) - D(y) \tag{3.55}$$

for $x, y \in \mathbb{F}_{p^n}$. For $a, b \in \mathbb{F}_{p^n}$, let $L_{a,b,B}$ be the linear map from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ defined as

$$L_{a,b,B}(x) = \mathrm{Tr}_p^{p^n}(xB(a, b) + aB(x, b) + bB(x, a)) \tag{3.56}$$

for every $x \in \mathbb{F}_{p^n}$. For $a, b \in \mathbb{F}_{p^n}$, let $C_{a,b,D}$ and $C_{a,b,A}$ be the constant functions from

$\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ defined as

$$\begin{aligned} C_{a,b,D} &= \mathrm{Tr}_p^{p^n}(aB(a,b) + bB(b,a) + aD(b) + bD(a)), \\ C_{a,b,A} &= \mathrm{Tr}_p^{p^n}(aA(b) + bA(a)). \end{aligned} \tag{3.57}$$

From now on, we keep the above notations in this section.

Lemma 3.4. *Let f be a cubic function as in (3.52). Then the second-order derivative of f at $(a,b) \in \mathbb{F}_{p^n}^2$ is the affine function defined as $\mathcal{D}_a\mathcal{D}_b f(x) = L_{a,b,B}(x) + C_{a,b,D} + C_{a,b,A}$ for $x \in \mathbb{F}_{p^n}$.*

Proof. Recall that $f(x) = \mathrm{Tr}_p^{p^n}(xD(x) + xA(x))$ for $x \in \mathbb{F}_{p^n}$. The first-order derivative $\mathcal{D}_b\mathrm{Tr}_p^{p^n}(xD(x))$ at $b \in \mathbb{F}_{p^n}$ is given as

$$\mathrm{Tr}_p^{p^n}(xB(x,b) + bB(x,b) + xD(b) + bD(x) + bD(b))$$

and $\mathcal{D}_b\mathrm{Tr}_p^{p^n}(xA(x)) = \mathrm{Tr}_p^{p^n}(xA(b) + bA(x) + bA(b))$ for every $x \in \mathbb{F}_{p^n}$. The second-order derivatives at $(a,b) \in \mathbb{F}_{p^n}^2$ are obtained as

$$\begin{aligned} \mathcal{D}_a\mathcal{D}_b\mathrm{Tr}_p^{p^n}(xD(x)) &= \mathrm{Tr}_p^{p^n}(xB(a,b) + aB(x,b) + bB(x,a) + \\ &\quad aB(a,b) + bB(b,a) + aD(b) + bD(a)), \end{aligned}$$

which is equal to $L_{a,b,B}(x) + C_{a,b,D}$ for every $x \in \mathbb{F}_{p^n}$, and

$$\mathcal{D}_a\mathcal{D}_b\mathrm{Tr}_p^{p^n}(xA(x)) = \mathrm{Tr}_p^{p^n}(aA(b) + bA(a)),$$

which is equal to $C_{a,b,A}$. This completes the proof. □

Let $S \subseteq \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$ be the subset

$$S = \{(a,b) \in \mathbb{F}_{p^n}^2 : L_{a,b,B}(x) = 0,\ \forall x \in \mathbb{F}_{p^n}\}. \tag{3.58}$$

Note that S is not a linear subspace of $\mathbb{F}_{p^n}^2$ in general. For $a \in \mathbb{F}_{p^n}$, let $S_a \subseteq \mathbb{F}_{p^n}$ be the subset $S_a = \{b \in \mathbb{F}_{p^n} : L_{a,b,B}(x) = 0,\ \forall x \in \mathbb{F}_{p^n}\} = \{b \in \mathbb{F}_{p^n} : (a,b) \in S\}$. Hence for every $a \in \mathbb{F}_{p^n}$, S_a is an $\mathbb{F}_p$-linear subspace of $\mathbb{F}_{p^n}$. In particular, if $a = 0$, then $S_0 = \mathbb{F}_{p^n}$. It is worth noting that $S = \bigcup_{a \in \mathbb{F}_{p^n}} \{(a,b) \in \mathbb{F}_{p^n}^2 : b \in S_a\}$. Now we can give the following.

Proposition 3.16. *Let p be an arbitrary prime and let f be a cubic function as in (3.52). If f is p-ary s-plateaued, then*

$$\sum_{a \in \mathbb{F}_{p^n}^\star} \sum_{b \in S_a} \xi_p^{C_{a,b,D} + C_{a,b,A}} = p^n(p^s - 1). \tag{3.59}$$

Conversely, if the above sum is zero, then f is p-ary bent.

Proof. Assume that f is s-plateaued. By Corollary 3.6, we have

$$\sum_{(a,b)\notin S}\sum_{x\in\mathbb{F}_{p^n}}\xi_p^{\mathcal{D}_a\mathcal{D}_bf(x)}+\sum_{(a,b)\in S}\sum_{x\in\mathbb{F}_{p^n}}\xi_p^{\mathcal{D}_a\mathcal{D}_bf(x)}=p^{2n+s}. \tag{3.60}$$

Recall that by Lemma 3.4, $\mathcal{D}_a\mathcal{D}_bf(x)=L_{a,b,B}(x)+C_{a,b,D}+C_{a,b,A}$ is the affine function for $x\in\mathbb{F}_{p^n}$. For $(a,b)\notin S$, the first sum in (3.60) is zero since an affine function is balanced. By (3.58), if $(a,b)\in S$, then we have $L_{a,b,B}(x)=0$ for every $x\in\mathbb{F}_{p^n}$. Then, (3.60) is equivalent to:

$$\sum_{(a,b)\in S}\xi_p^{C_{a,b,D}+C_{a,b,A}}=p^{n+s}.$$

Notice that $(a,b)\in S$ if and only if $b\in S_a$ for $a\in\mathbb{F}_{p^n}$. Recall that if $a=0$, then $S_0=\mathbb{F}_{p^n}$. If $a=0$, then we can easily see by (3.57) that $C_{a,b,D}=0$ and $C_{a,b,A}=0$. Thus we have

$$\sum_{b\in\mathbb{F}_{p^n}}\xi_p^0+\sum_{(a,b)\in S,a\neq 0}\xi_p^{C_{a,b,D}+C_{a,b,A}}=p^{n+s},$$

that is, (3.59) holds. Conversely, using the above arguments we have

$$\begin{aligned}\sum_{x,a,b\in\mathbb{F}_{p^n}}\xi_p^{\mathcal{D}_a\mathcal{D}_bf(x)}&=\sum_{x\in\mathbb{F}_{p^n}}\sum_{(a,b)\in S}\xi_p^{C_{a,b,D}+C_{a,b,A}}\\&=\sum_{x\in\mathbb{F}_{p^n}}\left(\sum_{b\in\mathbb{F}_{p^n}}\xi_p^0+\sum_{a\in\mathbb{F}_{p^n}^\star}\sum_{b\in S_a}\xi_p^{C_{a,b,D}+C_{a,b,A}}\right)=p^{2n}.\end{aligned}$$

Hence, by Corollary 3.7, f is p-ary bent. □

Remark 3.14. In Subsection 3.2.2, we indicate that the converse of Proposition 3.16 does not hold, in general when $s>0$. Namely, (3.59) does not determine whether f is s-plateaued or not when $s>0$.

The following fact can be given in odd characteristic.

Lemma 3.5. *Let B be the quadratic map as in (3.55). Assume that p is an odd prime. Then, for every $b\in\mathbb{F}_{p^n}$ we have*

$$B(b,b)=2D(b). \tag{3.61}$$

Proof. By (3.55), we have $B(b,b)=D(b+b)-D(b)-D(b)=D(2b)-2D(b)$ for every $b\in\mathbb{F}_{p^n}$. From the definition of D as in (3.53), for $0\leq i\leq j\leq n-1$

we have $(2b)^{p^i+p^j} = 2^{p^i+p^j} b^{p^i+p^j} = 2^{p^i} 2^{p^j} b^{p^i+p^j} = 4b^{p^i+p^j}$, where in the last equality we used that $2^{p^i} = 2$ in $\mathbb{F}_{p^n}$ for $0 \leq i \leq n-1$ in odd characteristic. In other words, $D(2b) = 4D(b)$ for every $b \in \mathbb{F}_{p^n}$ since $2 \in \mathbb{F}_p^\star$ in odd characteristic. This completes the proof. □

In the light of the above results, we have further simplifications.

Lemma 3.6. *Assume that p is an odd prime. Let $S \subseteq \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$ be the subset as in (3.58) and $C_{a,b,D}$ be a constant function as in (3.57). For every $(a,b) \in S$, we have $C_{a,b,D} = 0$.*

Proof. Recall the definition of linear function $L_{a,b,B}$ in (3.56), and put $x = a$,

$$L_{a,b,B}(a) = \mathrm{Tr}_p^{p^n}(bB(a,a)) + 2\mathrm{Tr}_p^{p^n}(aB(a,b)). \tag{3.62}$$

Similarly, by symmetry on $a \leftrightarrow b$, we have

$$L_{a,b,B}(b) = \mathrm{Tr}_p^{p^n}(aB(b,b)) + 2\mathrm{Tr}_p^{p^n}(bB(b,a)). \tag{3.63}$$

By (3.58), if $(a,b) \in S$, then $L_{a,b,B}(x) = 0$ for every $x \in \mathbb{F}_{p^n}$. Then for every $(a,b) \in S$,

$$L_{a,b,B}(a) = 0 \text{ and } L_{a,b,B}(b) = 0. \tag{3.64}$$

Combining (3.61), (3.62) and (3.63), we have $L_{a,b,B}(a) + L_{a,b,B}(b) = 2C_{a,b,D}$. Hence, by (3.64), $C_{a,b,D} = 0$ for every $(a,b) \in S$. □

Remark 3.15. In the case when $p = 2$, Lemma 3.6 does not hold. The following example shows that Lemma 3.6 fails in characteristic 2.

Example 3.5. *Let $f(x) = \mathrm{Tr}_2^{2^3}(\zeta^2 x^2 + \zeta^3 x^3 + \zeta x^6)$ be the Boolean function, where $\mathbb{F}_{2^3}^\star = \langle \zeta \rangle$ with $\zeta^3 + \zeta + 1 = 0$. Then, in characteristic 2, there exist $a = \zeta^3$ and $b = \zeta^5$ such that $(\zeta^3, \zeta^5) \in S$ but $C_{a,b,D} = 1$. On the other hand, there exist $a = \zeta^6$ and $b = \zeta^5$ such that $(\zeta^6, \zeta^5) \in S$ and $C_{a,b,D} = 0$.*

To state the next result, we define the following linear function. For $a \in \mathbb{F}_{p^n}$, let $\psi_{a,A}$ be the linear function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ defined as

$$\psi_{a,A}(x) = \mathrm{Tr}_p^{p^n}(aA(x) + xA(a)). \tag{3.65}$$

Notice that the kernel of $\psi_{a,A}$ is defined as $\ker(\psi_{a,A}) = \{b \in \mathbb{F}_{p^n} : \psi_{a,A}(b) = 0\}$, which is an $\mathbb{F}_p$-linear subspace of $\mathbb{F}_{p^n}$. The following result improves Proposition 3.16 when p is an odd prime.

Proposition 3.17. *Let p be an odd prime, and let f be a cubic function as in (3.52). If f is s-plateaued, then the following equivalent statements hold:*

$$\textit{i.)} \sum_{a\in\mathbb{F}_{p^n}^\star} \sum_{b\in S_a} \xi_p^{C_{a,b,A}} = p^n(p^s-1),$$

$$\textit{ii.)} \sum_{a\in\mathbb{F}_{p^n}^\star, S_a\subseteq\ker(\psi_{a,A})} p^{\dim(S_a)} = p^n(p^s-1).$$

Conversely, if one of the above summations is zero, then f is p-ary bent.

Proof. Assume that f is s-plateaued. By Proposition 3.16 and Lemma 3.6, it is obvious that (*i*) holds. We now prove (*ii*). Recall the definition of the linear function $\psi_{a,A}$ in (3.65), and put $x = b$. Then we have $\psi_{a,A}(b) = \mathrm{Tr}_p^{p^n}(aA(b) + bA(a))$, that is, $C_{a,b,A}$. Note that if $S_a \subseteq \ker(\psi_{a,A})$, then $C_{a,b,A} = 0$ for every $b \in S_a$; otherwise, $C_{a,b,A}$ is the linear function. Thus, we have

$$\begin{aligned}\sum_{a\in\mathbb{F}_{p^n}^\star} \sum_{b\in S_a} \xi_p^{C_{a,b,A}} &= \sum_{a\in\mathbb{F}_{p^n}^\star} \sum_{b\in S_a\subseteq\ker(\psi_{a,A})} \xi_p^0 + \sum_{a\in\mathbb{F}_{p^n}^\star} \sum_{b\in S_a\not\subseteq\ker(\psi_{a,A})} \xi_p^{C_{a,b,A}} \\ &= \sum_{a\in\mathbb{F}_{p^n}^\star,\, S_a\subseteq\ker(\psi_{a,A})} \#S_a.\end{aligned}$$

If f is s-plateaued, then the assertion follows from (*i*). Conversely, by Proposition 3.16 and using the above arguments we have

$$\begin{aligned}\sum_{x,a,b\in\mathbb{F}_{p^n}} \xi_p^{\mathcal{D}_a\mathcal{D}_b f(x)} &= \sum_{x\in\mathbb{F}_{p^n}} \sum_{(a,b)\in S} \xi_p^{C_{a,b,A}} \\ &= \sum_{x\in\mathbb{F}_{p^n}} \left(\sum_{b\in\mathbb{F}_{p^n}} \xi_p^0 + \sum_{a\in\mathbb{F}_{p^n}^\star} \sum_{b\in S_a} \xi_p^{C_{a,b,A}} \right) = p^{2n}.\end{aligned}$$

By Corollary 3.7, we conclude that f is p-ary bent. □

The following corollary explains a probably unexpected behavior of homogeneous cubic functions in even and odd characteristics (see also Remark 3.16).

Corollary 3.39. *Let p be an odd prime and f be homogeneous cubic as in Definition 3.4. Then, f is not bent.*

Proof. By Proposition 3.17, f is bent if and only if

$$\sum_{a\in\mathbb{F}_{p^n}^\star}\sum_{b\in S_a}\xi_p^{C_{a,b,A}}=0. \tag{3.66}$$

Assume that f is a homogeneous cubic function. Then $A(x)=0$ and here $C_{a,b,A}=0$ for every $a\in\mathbb{F}_{p^n}^\star$ and $b\in S_a$. It is worth noting that S_a is an $\mathbb{F}_p$-linear subspace of $\mathbb{F}_{p^n}$ for every $a\in\mathbb{F}_{p^n}$. Thus we have

$$\sum_{a\in\mathbb{F}_{p^n}^\star}\sum_{b\in S_a}\xi_p^{C_{a,b,A}}=\sum_{a\in\mathbb{F}_{p^n}^\star}\#S_a\geq p^n-1,$$

which contradicts (3.66). Hence, f is not bent. □

Remark 3.16. For $p=2$, Corollary 3.39 does not hold. The following example shows that Corollary 3.39 fails in characteristic 2.

Example 3.6. *The homogeneous cubic function* $\mathrm{Tr}_2^{2^6}(\zeta^{11}x^7+\zeta^6x^{11}+\zeta x^{13})$*, where* $\mathbb{F}_{2^6}^\star=\langle\zeta\rangle$ *with* $\zeta^6+\zeta^4+\zeta^3+\zeta+1=0$*, is bent in characteristic* 2*.*

Remark 3.17. Under the notation of Example 3.6, let $\{1,\alpha,\alpha^2,\ldots,\alpha^5\}$ be a basis of $\mathbb{F}_{2^6}$. Putting $x=x_1+x_2\alpha+x_3\alpha^2+\cdots+x_6\alpha^5$ we obtain a multivariate form representation in $\mathbb{F}_2[x_1,\cdots,x_6]/\langle x_1^2-x_1,\ldots,x_6^2-x_6\rangle$ of the function f in Example 3.6. We denote this multivariate form representation again as $f=f(x_1,\ldots,x_6)$ for simplicity of notation. The degree 3 part of this form is $f_3(x_1,\ldots,x_6)=x_1x_2x_3+x_1x_2x_6+x_1x_3x_4+x_1x_4x_5+x_1x_4x_6+x_1x_5x_6+x_2x_3x_6+x_2x_4x_6+x_3x_4x_5$. Recall $\mathrm{rank}_3(f_3)=\mathrm{rank}_3(f)$ is an affine invariant defined in [39]. By a simple and useful matrix computation explained in [39, Section 3] we obtain that $\mathrm{rank}_3(f_3)=6$. Recall that there are exactly 3 distinct cubic bent functions R_1,R_2,R_3 up to extended affine equivalence for $q=2$ and $n=6$ such that $\mathrm{rank}_3(R_1)=3$, $\mathrm{rank}_3(R_2)=5$ and $\mathrm{rank}_3(R_3)=6$ (see [72]). This shows that the function in Example 3.6 is extended affine equivalent to R_3. Moreover for $p=2$ and $n=6$ there are exactly 30 distinct homogeneous cubic bent functions in the sense of multivariate form and they all are extended affine equivalent to R_1 (see [70]). Therefore it is impossible to obtain a homogeneous cubic bent function in the sense of multivariate form starting from the function in Example 3.6, choosing a basis and making an affine change of variables. This shows the important difference for $p=2$ and $n=6$ mentioned at the end of Remark 3.13.

There exists a homogeneous cubic s-plateaued function in odd characteristic when $s > 0$.

Example 3.7. *In characteristic* 3*, the homogeneous cubic function* $\mathrm{Tr}_3^{3^3}(\zeta^4 x^5 + \zeta^2 x^{11} + \zeta x^{13})$ *is* 1*-plateaued where* $\mathbb{F}_{3^3}^\star = \langle \zeta \rangle$ *with* $\zeta^3 + 2\zeta + 1 = 0$.

Recall that the radical of a quadratic function $Q : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is defined as

$$\mathcal{W}_Q := \{y \in \mathbb{F}_{p^n} : Q(x+y) = Q(x) + Q(y),\ \forall x \in \mathbb{F}_{p^n}\},$$

which is an $\mathbb{F}_p$-linear subspace of $\mathbb{F}_{p^n}$. If $\dim(\mathcal{W}_Q) = 0$, that is, $\mathcal{W}_Q = \{0\}$, then Q is said to be non-degenerate; otherwise, Q is said to be degenerate.

Corollary 3.40. *Let p be an odd prime and f be a cubic function as in (3.52). If f is bent, then the homogeneous quadratic function $Q(x) = \mathrm{Tr}_p^{p^n}(xA(x))$ is non-degenerate.*

Proof. Assume that $Q(x) = \mathrm{Tr}_p^{p^n}(xA(x))$ is degenerate. Then, there exists $u \in \mathbb{F}_{p^n}^\star$ such that $Q(x+u) = Q(x) + Q(u)$ for every $x \in \mathbb{F}_{p^n}$. As

$$\mathrm{Tr}_p^{p^n}((x+u)A(x+u)) = Q(x) + \mathrm{Tr}_p^{p^n}(xA(u) + uA(x)) + Q(u),$$

there exists $u \in \mathbb{F}_{p^n}^\star$ such that $\mathrm{Tr}_p^{p^n}(xA(u) + uA(x)) = 0$ for every $x \in \mathbb{F}_{p^n}$. Recall the definition of the linear function $\psi_{u,A}$ defined as $\psi_{u,A}(x) = \mathrm{Tr}_p^{p^n}(xA(u) + uA(x))$ in (3.65). Then, there exists $u \in \mathbb{F}_{p^n}^\star$ such that $\ker(\psi_{u,A}) = \mathbb{F}_{p^n}$. Assume also that f is bent. By Proposition 3.17, we obtain

$$\sum_{a \in \mathbb{F}_{p^n}^\star, S_a \subseteq \ker(\psi_{a,A})} p^{\dim(S_a)} = 0. \tag{3.67}$$

As $u \in \mathbb{F}_{p^n}^\star$ and $\ker(\psi_{u,A}) = \mathbb{F}_{p^n}$, we have $S_u \subseteq \ker(\psi_{u,A})$, $\dim(S_u) \geq 0$ and $p^{\dim(S_u)} \geq 1$. Hence for $u \in \mathbb{F}_{p^n}^\star$, the left-hand side of (3.67) is positive, which is a contradiction. □

Example 3.8. *Let* $\mathrm{Tr}_3^{3^3}(2x^4 + 2x^5 + x^{11})$ *be the cubic bent function. Then, its homogeneous quadratic part* $\mathrm{Tr}_3^{3^3}(2x^4)$ *is non-degenerate.*

A linearized polynomial $C(x) = c_0 x + c_1 x^p + \cdots + c_{n-1} x^{p^{n-1}} \in \mathbb{F}_{p^n}[x]$ is called a permutation polynomial if the map $x \mapsto C(x)$ is a bijection on $\mathbb{F}_{p^n}$, which means that

C has no nonzero root in $\mathbb{F}_{p^n}$. Using a well-known characterization of non-degenerate quadratic forms in odd characteristic we obtain the following.

Corollary 3.41. *Let p be an odd prime and f be a cubic function as in (3.52). Let $a \in \mathbb{F}_p^\star$ be a quadratic non-residue. If f is bent, then there exists a linearized permutation polynomial $C(x) \in \mathbb{F}_{p^n}[x]$ such that $f(C(x)) = \mathrm{Tr}_p^{p^n}(x\tilde{D}(x)) + \mathrm{Tr}_p^{p^n}(\eta x^2)$ where $\eta \in \{1, a\}$ and*

$$\tilde{D}(x) = \sum_{0 \le i \le j \le n-1} \tilde{d}_{ij} x^{p^i + p^j} \text{ with } \tilde{d}_{ij} \in \mathbb{F}_{p^n} \tag{3.68}$$

satisfying $\mathrm{Tr}_p^{p^n}(x\tilde{D}(x)) = \mathrm{Tr}_p^{p^n}(C(xD(x)))$ for every $x \in \mathbb{F}_{p^n}$.

Proof. By Corollary 3.40, the quadratic function $\mathrm{Tr}_p^{p^n}(xA(x))$ is non-degenerate. Using the arguments in the proof of [68, Proposition 3.1], we obtain that any non-degenerate quadratic function is equivalent to exactly one of the quadratic functions $x \mapsto \mathrm{Tr}_p^{p^n}(\eta x^2)$ with $\eta \in \{1, a\}$. Then we consider the quadratic functions $\mathrm{Tr}_p^{p^n}(\eta x^2)$ with $\eta \in \{1, a\}$. Hence, there exists a linearized permutation polynomial $C(x) \in \mathbb{F}_{p^n}[x]$ such that $\mathrm{Tr}_p^{p^n}(C(xA(x))) = \mathrm{Tr}_p^{p^n}(\eta x^2)$ with $\eta \in \{1, a\}$. Moreover, there exists $\tilde{D}(x)$ as in (3.68) such that $\mathrm{Tr}_p^{p^n}(C(xD(x))) = \mathrm{Tr}_p^{p^n}(x\tilde{D}(x))$ since C is a linearized permutation polynomial over $\mathbb{F}_{p^n}$. Combining the arguments above, the proof is complete. □

3.5.2 Cubic (Homogeneous) Plateaued p-Ary Functions Without Full Rank

In this subsection, we first consider a notion of the rank of a function in arbitrary characteristic, and then give a method, which can be straightforwardly obtained from the definition, to determine it. By MAGMA [5], we obtain several cubic plateaued functions without full rank in characteristic 3. By considering the rank of plateaued functions, we characterize these functions in terms of their second-order derivatives, and hence it reveals the non-existence of a (homogeneous) cubic plateaued function in odd characteristic in many cases.

Definition 3.5. Let f be a function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$. The rank of f is defined as the smallest nonnegative integer r such that there exists an $\mathbb{F}_p$-linear subspace $W \subseteq \mathbb{F}_{p^n}$

and its complement $\overline{W} \subseteq \mathbb{F}_{p^n}$ of dimension $n-r$ satisfying

$$f(x_1+x_2) = f(x_1)$$

for every $x_1 \in W$ and $x_2 \in \overline{W}$. We write $\mathrm{rank}(f) = r$.

It is worth noting that if f is a quadratic function, then the notion of the rank of f in Definition 3.5 coincides with the usual rank of quadratic functions (see, e.g., [7]).

Remark 3.18. We remark that the notion of the rank in Definition 3.5 is invariant under affine transformations. Indeed, let $\psi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be an $\mathbb{F}_p$-linear isomorphism and $\alpha \in \mathbb{F}_{p^n}$. Let $g(x) = f(\psi(x))$ and $h(x) = f(x+\alpha)$. It is enough to show that the ranks of f, g and h are the same in the sense of Definition 3.5. Assume that $\mathrm{rank}(f) = r$ and $W, \overline{W}$ are $\mathbb{F}_p$-linear subspaces of $\mathbb{F}_{p^n}$ with $\dim(W) = r$, $\dim(\overline{W}) = n-r$ and $W \cap \overline{W} = \{0\}$. Moreover, we assume that $f(x_1+x_2) = f(x_1)$ for all $x_1 \in W$ and $x_2 \in \overline{W}$. Then it is not difficult to observe that $g(y_1+y_2) = g(y_1)$ for all $y_1 \in \psi^{-1}(W)$ and $y_2 \in \psi^{-1}(\overline{W})$. Moreover, $\dim(\psi^{-1}(W)) = r$, $\dim(\psi^{-1}(\overline{W})) = n-r$ and $\psi^{-1}(W) \cap \psi^{-1}(\overline{W}) = \{0\}$. Also we observe that $h(x_1+x_2) = h(x_1)$ for all $x_1 \in W$ and $x_2 \in \overline{W}$. These arguments show that the rank in Definition 3.5 is invariant under affine transformations.

Recall that the cubic function f is defined as

$$f(x) = \mathrm{Tr}_p^{p^n}(xD(x)) + \mathrm{Tr}_p^{p^n}(xA(x))$$

for $x \in \mathbb{F}_{p^n}$ without loss of generality. Assume that $\mathrm{rank}(f) = r$. Let W be a corresponding r-dimensional $\mathbb{F}_p$-linear subspace of $\mathbb{F}_{p^n}$. Indeed, there may be many different r-dimensional subspaces corresponding to rank r. By Definition 3.5, f can be written as $f(x_1) = \mathrm{Tr}_p^{p^n}(x_1D(x_1)) + \mathrm{Tr}_p^{p^n}(x_1A(x_1))$ for $x_1 \in W$. We keep the above notations in the sequel. The following is a direct generalization of Lemma 3.4.

Lemma 3.7. *Let f be a cubic function as in (3.52), and let W be an $\mathbb{F}_p$-linear subspace of dimension $\mathrm{rank}(f)$ for the rank of f in Definition 3.5. For $a, b, x \in \mathbb{F}_{p^n}$, let $a_1, b_1, x_1 \in W$ and $a_2, b_2, x_2 \in \overline{W}$ such that $a = a_1 + a_2$, $b = b_1 + b_2$ and $x = x_1 + x_2$. Then, the second-order derivative of f at $(a, b) \in \mathbb{F}_{p^n}^2$ for $x \in \mathbb{F}_{p^n}$ is the affine function defined as $\mathcal{D}_a\mathcal{D}_b f(x) = L_{a_1,b_1,B}(x_1) + C_{a_1,b_1,D} + C_{a_1,b_1,A}$, where $a_1, b_1, x_1 \in W$.*

Proof. The second-order derivative of f at $(a,b) \in \mathbb{F}_{p^n}^2$ for $x \in \mathbb{F}_{p^n}$ is given as

$$\begin{aligned}
&\mathcal{D}_a\mathcal{D}_b f(x) = f(x+a+b) - f(x+a) - f(x+b) + f(x) = \\
&f(x_1+x_2+a_1+a_2+b_1+b_2) - f(x_1+x_2+a_1+a_2) - f(x_1+x_2+b_1+b_2) \\
&+f(x_1+x_2) = f(x_1+a_1+b_1) - f(x_1+a_1) - f(x_1+b_1) + f(x_1) \\
&= \mathcal{D}_{a_1}\mathcal{D}_{b_1} f(x_1),
\end{aligned}$$

where we use the fact that W is an $\mathbb{F}_p$-linear subspace of dimension $\mathrm{rank}(f)$. By Lemma 3.4, and using the notation we have

$$\mathcal{D}_{a_1}\mathcal{D}_{b_1} f(x_1) = L_{a_1,b_1,B}(x_1) + C_{a_1,b_1,D} + C_{a_1,b_1,A}.$$

This completes the proof. □

The following is a direct but practical generalization of Theorem 3.6.

Theorem 3.25. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. Let r be the rank of f and let W be a corresponding r-dimensional $\mathbb{F}_p$-linear subspace of $\mathbb{F}_{p^n}$. Then, f is s-plateaued if and only if for every $x_1 \in W$*

$$\sum_{a_1,b_1 \in W} \xi_p^{\mathcal{D}_{a_1}\mathcal{D}_{b_1} f(x_1)} = p^{2r+s-n}.$$

Proof. Let $\overline{W}$ be a corresponding $n-r$ dimensional $\mathbb{F}_p$-linear subspace of $\mathbb{F}_{p^n}$. Then $a, b, x \in \mathbb{F}_{p^n}$ are uniquely determined as $a = a_1 + a_2, b = b_1 + b_2$ and $x = x_1 + x_2$, where $a_1, b_1, x_1 \in W$ and $a_2, b_2, x_2 \in \overline{W}$. By Lemma 3.7, we have $\mathcal{D}_a\mathcal{D}_b f(x) = \mathcal{D}_{a_1}\mathcal{D}_{b_1} f(x_1)$. Then by Theorem 3.6, f is s-plateaued if and only if for every $x_1 \in W, x_2 \in \overline{W}$

$$\sum_{a_1 \in W} \sum_{a_2 \in \overline{W}} \sum_{b_1 \in W} \sum_{b_2 \in \overline{W}} \xi_p^{\mathcal{D}_{a_1}\mathcal{D}_{b_1} f(x_1)} = p^{n+s},$$

that is, $p^{n-r}p^{n-r} \sum_{a_1 \in W} \sum_{b_1 \in W} \xi_p^{\mathcal{D}_{a_1}\mathcal{D}_{b_1} f(x_1)} = p^{n+s}$ for every $x_1 \in W$. □

As a generalization of the sets S and S_a given before Proposition 3.16, we now define the sets T and T_{a_1} as follows. Let $T \subseteq W \times W$ be the subset $T = \{(a_1, b_1) \in W^2 : L_{a_1,b_1,B}(x_1) = 0, \forall x_1 \in W\}$. For $a_1 \in W$, let $T_{a_1} \subseteq W$ be the subset

$$T_{a_1} = \{b_1 \in W : L_{a_1,b_1,B}(x_1) = 0, \forall x_1 \in W\} = \{b_1 \in W : (a_1, b_1) \in T\}.$$

Note that for every $a_1 \in W$, T_{a_1} is an $\mathbb{F}_p$-linear subspace of W. Clearly, if $a_1 = 0$, then $T_0 = W$.

Let $\tilde{\psi}_{a_1,A} : W \to \mathbb{F}_p$ be a generalization of the linear function $\psi_{a,A}$ given in (3.65). Namely, for $a_1 \in W$, let $\tilde{\psi}_{a_1,A}(x_1) = \mathrm{Tr}_p^{p^n}(a_1 A(x_1)) + \mathrm{Tr}_p^{p^n} x_1 A(a_1))$ for $x_1 \in W$. Notice that the kernel of $\tilde{\psi}_{a_1,A}$ is defined as $\ker(\tilde{\psi}_{a_1,A}) = \{b_1 \in W : \tilde{\psi}_{a_1,A}(b_1) = 0\}$, which is an $\mathbb{F}_p$-linear subspace of W.

Now we are ready to give a generalization of Proposition 3.17.

Proposition 3.18. *Let p be an odd prime and let f be a cubic function as in (3.52). Assume that $\mathrm{rank}(f) = r$ in Definition 3.5. Let W be a corresponding r-dimensional $\mathbb{F}_p$-linear subspace of $\mathbb{F}_{p^n}$. If f is s-plateaued, then the following equivalent statements hold:*

i.) $$\sum_{0 \neq a_1 \in W} \sum_{b_1 \in T_{a_1}} \xi_p^{C_{a_1,b_1,A}} = p^r(p^{r+s-n} - 1),$$

ii.) $$\sum_{0 \neq a_1 \in W,\ T_{a_1} \subseteq \ker(\tilde{\psi}_{a_1,A})} p^{\dim(T_{a_1})} = p^r(p^{r+s-n} - 1).$$

Proof. By Lemma 3.7, the second-order derivative of f at $(a_1, b_1) \in W^2$ is the affine function given as $\mathcal{D}_{a_1}\mathcal{D}_{b_1} f(x_1) = L_{a_1,b_1,B}(x_1) + C_{a_1,b_1,D} + C_{a_1,b_1,A}$ for $x_1 \in W$. Assume that f is s-plateaued. By Theorem 3.25, we have

$$\sum_{(a_1,b_1) \notin T} \sum_{x_1 \in W} \xi_p^{\mathcal{D}_{a_1}\mathcal{D}_{b_1} f(x_1)} + \sum_{(a_1,b_1) \in T} \sum_{x_1 \in W} \xi_p^{\mathcal{D}_{a_1}\mathcal{D}_{b_1} f(x_1)} = p^{3r+s-n}.$$

For $(a_1, b_1) \notin T$, the first sum is zero since an affine function is balanced. For $(a_1, b_1) \in T$ we have $L_{a_1,b_1,B}(x_1) = 0$ for every $x_1 \in W$. Then, we have

$$\sum_{(a_1,b_1) \in T} \xi_p^{C_{a_1,b_1,D} + C_{a_1,b_1,A}} = p^{2r+s-n}.$$

Notice that $(a_1, b_1) \in T$ if and only if $b_1 \in T_{a_1}$ for $a_1 \in W$. Recall that if $a_1 = 0$, then $T_0 = W$. If $a_1 = 0$, we have $C_{a_1,b_1,D} = 0$ and $C_{a_1,b_1,A} = 0$. By Lemmas 3.6 and 3.7, $C_{a_1,b_1,D} = 0$ for every $(a_1, b_1) \in T$. Thus we have

$$\sum_{b_1 \in W} \xi_p^0 + \sum_{(a_1,b_1) \in T, a_1 \neq 0} \xi_p^{C_{a_1,b_1,A}} = p^{2r+s-n},$$

that is, (*i*) holds.

We next prove (*ii*). From the definition of $\tilde{\psi}_{a_1,A}$, putting $x_1 = b_1$, we have

$$\tilde{\psi}_{a_1,A}(b_1) = \mathrm{Tr}_p^{p^n}(a_1 A(b_1)) + \mathrm{Tr}_p^{p^n}(b_1 A(a_1)),$$

which is equal to $C_{a_1,b_1,A}$. Hence, if $T_{a_1} \subseteq \ker(\tilde{\psi}_{a_1,A})$, then $C_{a_1,b_1,A} = 0$ for every $b_1 \in T_{a_1}$; otherwise, $C_{a_1,b_1,A}$ is the linear function. Then we have

$$\begin{aligned}\sum_{0\neq a_1\in W}\sum_{b_1\in T_{a_1}} \xi_p^{C_{a_1,b_1,A}} &= \sum_{0\neq a_1\in W}\sum_{b_1\in T_{a_1}\subseteq\ker(\tilde{\psi}_{a_1,A})} \xi_p^0 + \\ \sum_{0\neq a_1\in W}\sum_{b_1\in T_{a_1}\not\subseteq\ker(\tilde{\psi}_{a_1,A})} \xi_p^{C_{a_1,b_1,A}} &= \sum_{0\neq a_1\in W,\, T_{a_1}\subseteq\ker(\tilde{\psi}_{a_1,A})} \#T_{a_1}.\end{aligned}$$

Hence, the proof follows from (*i*). □

We derive from Proposition 3.18 the following result.

Corollary 3.42. *Let p be an odd prime and f be a cubic function as in (3.52) with $\mathrm{rank}(f) = r$. If $r + s < n$, then f is not s-plateaued.*

Proof. Let W be a corresponding r-dimensional $\mathbb{F}_p$-linear subspace of $\mathbb{F}_{p^n}$ for the rank of f in Definition 3.5. Assume that f is s-plateaued. By Proposition 3.18, we have

$$\sum_{0\neq a_1\in W,\, T_{a_1}\subseteq\ker(\tilde{\psi}_{a_1,A})} p^{\dim(T_{a_1})} = p^r(p^{r+s-n} - 1). \tag{3.69}$$

Note that the left-hand side of (3.69) is nonnegative. However, since $r + s < n$, we have $p^{r+s-n} - 1 < 0$ and hence the right-hand side of (3.69) is negative, which is a contradiction. □

In the case of $r + s = n$, we obtain the following result, which is a generalization of Corollary 3.39. We assume that f is non-constant without loss of generality, that is, the rank of f cannot be zero.

Corollary 3.43. *Let p be an odd prime and f be homogeneous cubic as in Definition 3.4 with $\mathrm{rank}(f) = r \geq 1$. If $r + s = n$, then f is not s-plateaued.*

Proof. Let W be a corresponding r-dimensional $\mathbb{F}_p$-linear subspace of $\mathbb{F}_{p^n}$ for the rank of f in Definition 3.5. Assume that f is s-plateaued and $r+s=n$. By Proposition 3.18, we have

$$\sum_{0\neq a_1\in W}\sum_{b_1\in T_{a_1}}\xi_p^{C_{a_1,b_1,A}}=p^r(p^{r+s-n}-1)=0, \tag{3.70}$$

since $p^{r+s-n}=1$. Moreover, since f is a homogeneous cubic function, $A(x)=0$ for every $x\in\mathbb{F}_{p^n}$ and hence $C_{a_1,b_1,A}=0$ for every $0\neq a_1\in W$ and $b_1\in T_{a_1}$. Note that T_{a_1} is an $\mathbb{F}_p$-linear subspace of W for every $a_1\in W$. Hence, as in the proof of Corollary 3.39, we have

$$\sum_{0\neq a_1\in W}\sum_{b_1\in T_{a_1}}\xi_p^{C_{a_1,b_1,A}}=\sum_{0\neq a_1\in W}\#T_{a_1}\geq p^r-1. \tag{3.71}$$

Since $r\geq 1$, combining (3.70) and (3.71) we get a contradiction. □

The following result can be considered as a generalization of Corollary 3.40.

Corollary 3.44. *Let p be an odd prime and f be a cubic function as in (3.52) with $\mathrm{rank}(f)=r\geq 1$. Assume that f is s-plateaued and $r+s=n$. Let W be a corresponding r-dimensional $\mathbb{F}_p$-linear subspace of $\mathbb{F}_{p^n}$ for the rank of f in Definition 3.5. Let $Q_W:W\to\mathbb{F}_p$ be the restriction of the corresponding homogeneous quadratic function such that $Q_W(x)=\mathrm{Tr}^n(xA(x))$ for $x\in W$. Then Q_W is non-degenerate.*

Proof. As in the proof of Corollary 3.43, since f is s-plateaued and $r+s=n$, we have

$$\sum_{0\neq a_1\in W,\ T_{a_1}\subseteq\ker(\tilde{\psi}_{a_1,A})}p^{\dim(T_{a_1})}=p^r(p^{r+s-n}-1)=0. \tag{3.72}$$

Next we use an argument in the proof of Corollary 3.40. Assume that Q_W is degenerate. Then, there exists $a_1\in W\setminus\{0\}$ such that $\mathrm{Tr}_p^{p^n}(xA(a_1))+\mathrm{Tr}_p^{p^n}(a_1A(x))=0$ for every $x\in W$. This implies $\ker(\tilde{\psi}_{a_1,A})=W$ and hence the right-hand side of (3.72) is at least $p^{\dim(T_{a_1})}\geq 1$. This gives a contradiction. Hence, Q_W is non-degenerate. □

As a generalization of Corollary 3.41, we give the next result. Recall that if W is an $\mathbb{F}_p$-linear subspace of $\mathbb{F}_{p^n}$ of dimension $\mathrm{rank}(f)$ and if $\overline{W}\subseteq\mathbb{F}_{p^n}$ is its complement as in Definition 3.5, then $f(x_1+x_2)=f(x_1)$ for $x_1\in W$ and $x_2\in\overline{W}$.

Corollary 3.45. *Let p be an odd prime and f be a cubic function as in (3.52) with* $\mathrm{rank}(f) = r \geq 1$. *Assume that f is s-plateaued and $r + s = n$. Let $\eta \in \mathbb{F}_{p^n}^\star$ be a quadratic non-residue. Let W be a corresponding r-dimensional $\mathbb{F}_p$-linear subspace of $\mathbb{F}_{p^n}$ for the rank of f in Definition 3.5. Then there exists an $\mathbb{F}_p$-linear isomorphism $L : W \to \mathbb{F}_{p^r}$ and $\mu \in \{1, \eta\}$ such that*

$$f(L(y_1)) = \mathrm{Tr}_p^{p^n}(L(y_1)D(L(y_1))) + \mathrm{Tr}^r(\mu y_1^2)$$

for every $y_1 \in \mathbb{F}_{p^r}$.

Proof. By the help of the proof of Corollary 3.41, we are able to prove this corollary. Let $Q_W : W \to \mathbb{F}_p$ be a homogeneous quadratic function defined as $Q_W(x_1) = \mathrm{Tr}^n(x_1 A(x_1))$ for $x_1 \in W$. By Corollary 3.44, Q_W is non-degenerate. As in the proof of Corollary 3.41 we obtain an $\mathbb{F}_p$-linear isomorphism $L : W \to \mathbb{F}_{p^r}$ and $\mu \in \{1, \eta\}$ such that

$$\mathrm{Tr}_p^{p^n}(L(y_1)A(L(y_1))) = \mathrm{Tr}^r(\mu y_1^2)$$

for every $y_1 \in \mathbb{F}_{p^r}$. Using the fact that $f(x_1) = \mathrm{Tr}_p^{p^n}(x_1 D(x_1)) + \mathrm{Tr}_p^{p^n}(x_1 A(x_1))$ for every $x_1 \in W$, the result follows. □

In this section we consider mainly arbitrary cubic functions as in (3.52). It is worth noting that if $p = 2$, then there exists a different and natural notion of ranks for Boolean functions (see [39]). For example if f is a Boolean cubic function in n variables in algebraic normal form (multivariate form), then $\mathrm{rank}_3(f)$ is the smallest number of linearly independent combinations of $x_1, \ldots, x_n$ needed in the degree 3 part of $f = f(x_1, \ldots, x_n)$. Then $\mathrm{rank}_2(f)$ is also defined. Moreover, [39] gives a very nice algorithm to determine these ranks. The notion of rank in Definition 3.5 is different from these notions in [39]. Finally in this subsection, we give a rather direct method, the consequence of the definition, to determine the rank of a cubic (and actually an arbitrary) function in arbitrary characteristic in the sense of Definition 3.5.

A method to determine $\mathrm{rank}(f)$**:** Let $f : \mathbb{F}_p^n \to \mathbb{F}_p$. Recall that the rank of f is the smallest nonnegative integer r such that there exists an $\mathbb{F}_p$-linear subspace $W \subseteq \mathbb{F}_p^n$ and its complement $\overline{W} \subseteq \mathbb{F}_p^n$ of dimension $n - r$ satisfying $f(x_1 + x_2) = f(x_1)$ for every $x_1 \in W$ and $x_2 \in \overline{W}$, where $x_1 + x_2 = x \in \mathbb{F}_p^n$. Let $B_W = \{\alpha_1, \alpha_2, \ldots, \alpha_r\}$ be

a basis of W over $\mathbb{F}_p$ and $B_{\overline{W}} = \{\alpha_{r+1}, \alpha_{r+2}, \ldots, \alpha_n\}$ be a basis of $\overline{W}$ over $\mathbb{F}_p$ where $B = \{\alpha_1, \alpha_2, \ldots, \alpha_r, \alpha_{r+1}, \ldots, \alpha_n\}$ is a basis of $\mathbb{F}_p^n$. Let $B'_W = \{\alpha'_1, \alpha'_2, \ldots, \alpha'_r\}$ and $B'_{\overline{W}} = \{\alpha'_{r+1}, \alpha'_{r+2}, \ldots, \alpha'_n\}$ be the dual bases of B_W and $B_{\overline{W}}$, respectively where $B' = \{\alpha'_1, \alpha'_2, \ldots, \alpha'_r, \alpha'_{r+1}, \ldots, \alpha'_n\}$ is a basis of $\mathbb{F}_p^n$. Notice that $\mathbb{F}_p^n = \langle B \rangle = \langle B' \rangle$, where B and B' are the dual bases of $\mathbb{F}_p^n$ over $\mathbb{F}_p$. Hence, x_1 and x_2 can be written as

$$\begin{aligned} x_1 &= \alpha_1 \mathrm{Tr}_p^{p^n}(\alpha'_1 x) + \alpha_2 \mathrm{Tr}_p^{p^n}(\alpha'_2 x) + \cdots + \alpha_r \mathrm{Tr}_p^{p^n}(\alpha'_r x) \\ &\text{and} \\ x_2 &= \alpha_{r+1} \mathrm{Tr}_p^{p^n}(\alpha'_{r+1} x) + \alpha_{r+2} \mathrm{Tr}_p^{p^n}(\alpha'_{r+2} x) + \cdots + \alpha_n \mathrm{Tr}_p^{p^n}(\alpha'_n x). \end{aligned}$$

Using the dual bases B and B', we can determine r and provide a corresponding $\mathbb{F}_p$-linear subspace $W = \langle B_W \rangle$ using Algorithm 1.

Algorithm 1 Find $\mathrm{rank}(f) = r$

Require: $n, f, B = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}, B' = \{\alpha'_1, \alpha'_2, \ldots, \alpha'_n\}, \mathbb{F}_p^n$.

Ensure: r.

```
for r := 1 to n − 1 do
    for x in F_p^n do
        Compute x_1 = α_1 Tr_p^{p^n}(α'_1 x) + α_2 Tr_p^{p^n}(α'_2 x) + ··· + α_r Tr_p^{p^n}(α'_r x)
        Compute x_2 = α_{r+1} Tr_p^{p^n}(α'_{r+1} x) + α_{r+2} Tr_p^{p^n}(α'_{r+2} x) + ··· + α_n Tr_p^{p^n}(α'_n x)
        if f(x_1 + x_2)! = f(x_1) then
            goto next r
        end if
    end for
    return r
end for
return n
```

In the following example we give a cubic plateaued function f with $\mathrm{rank}(f) < n$ and a corresponding $\mathbb{F}_p$-linear subspace W of dimension $\mathrm{rank}(f)$ when p is an odd prime.

Example 3.9. *Let* $f(x) = \mathrm{Tr}_3^{3^3}(\zeta x^2 + \zeta x^3 + \zeta^{22} x^4 + \zeta^{22} x^{13})$*, where* $\mathbb{F}_{3^3}^\star = \langle \zeta \rangle$ *with* $\zeta^3 + 2\zeta + 1 = 0$*. Then,* f *is* 1*-plateaued with* $\mathrm{rank}(f) = 2$ *and* $W = \langle \{\zeta, \zeta^2\} \rangle$.

CHAPTER 4

ON THE FUNCTIONS WITH FOUR-VALUED ABSOLUTE WALSH SPECTRUM

The main motivation of this chapter is about the converse of Corollary 3.6 in Subsection 3.2.2. As this shows a drastic change for $s = 0$ and an integer $s \geq 1$ cases, by MAGMA [5] we found a great number of concrete examples which show the failure of the converse of Corollary 3.6 for $s \geq 1$ (notice that its converse is true for $s = 0$). Then, we tried to study these examples in a systematic way. As a plateaued (but not bent) function has exactly two distinct values (one being zero) in its absolute Walsh spectrum, then it is natural to try such examples first with three distinct values (one being zero). We observe that it is impossible for many cases to find a such example with exactly three distinct values (one being zero) in its absolute Walsh spectrum. Finally we search a such example with exactly four distinct values (one being zero), and find several examples in characteristics 2 and 3. The results presented in this chapter appear in [64].

4.1 Non-Existence of Functions with Three-valued Absolute Walsh Spectrum

This section shows the non-existence of a function f such that $S_2(f) = p^{3n+s}$ with $1 \leq s \leq n$ and its absolute Walsh transform takes exactly three distinct values, which are in $\{0, c_1 p^n, c_2 p^n\}$ with $0 < c_1 < p^s < c_2$ positive integers. In the case of $s = 0$, the non-existence of a such function follows readily from Theorem 3.2.

We first need the following lemma. Recall that $S_0(f) = p^n$ and $S_1(f) = p^{2n}$ for any function f. The even moments $S_i(f)$ for $i = 0, 1, 2$ allow us to compute the

multiplicity of each value of the absolute Walsh transforms of f.

Lemma 4.1. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ and s be an integer with $1 \leq s \leq n$. Assume that there exists a function f such that $|\widehat{\chi_f}(\omega)|^2 \in \{0, c_1 p^n, c_2 p^n\}$ for every $\omega \in \mathbb{F}_{p^n}$, all of three appear and c_1, c_2 are positive integers with $0 < c_1 < p^s < c_2$, and also $S_2(f) = p^{3n+s}$. Then $|\widehat{\chi_f}(\omega)|^2$ takes a_0 times the value 0, a_1 times the value $c_1 p^n$ and a_2 times the value $c_2 p^n$, where the values $a_0 = p^n - a_1 - a_2$,*

$$a_1 = \frac{p^n(p^s - c_2)}{c_1(c_1 - c_2)} \text{ and } a_2 = \frac{p^n(p^s - c_1)}{c_2(c_2 - c_1)} \tag{4.1}$$

are positive integers with $0 < c_1 < p^s < c_2$.

Proof. As $S_0(f) = p^n$, $S_1(f) = p^{2n}$ and $S_2(f) = p^{3n+s}$, we have the following equations, respectively:

$$\begin{aligned} a_0 + a_1 + a_2 &= p^n, \\ a_1 c_1 + a_2 c_2 &= p^n, \\ a_1 c_1^2 + a_2 c_2^2 &= p^{n+s}. \end{aligned}$$

Then, by solving the above linear equation system, we obtain the desired positive integers in (4.1). □

Recall that for a prime p, the p-adic valuation of a positive integer c is the highest power v such that p^v divides c, which is denoted by $v_p(c) = v$.

Theorem 4.1. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ and s be an integer with $1 \leq s \leq n$. There does not exist a function f such that*

$$|\widehat{\chi_f}(\omega)|^2 \in \{0, c_1 p^n, c_2 p^n\}$$

for every $\omega \in \mathbb{F}_{p^n}$, all of three appear and c_1, c_2 are positive integers with $0 < c_1 < p^s < c_2$, and also $S_2(f) = p^{3n+s}$.

Proof. Assume that there exists a such function f. By Lemma 4.1, the values

$$a_1 = \frac{p^n(p^s - c_2)}{c_1(c_1 - c_2)} \text{ and } a_2 = \frac{p^n(p^s - c_1)}{c_2(c_2 - c_1)}$$

are two positive integers with $0 < c_1 < p^s < c_2$. Let v_p be p-adic valuation. It is obvious that $v_p(c_2) \geq 0$ and $v_p(c_1) \geq 0$. Assume that there exists an integer i with $0 \leq i \leq s-1$ such that $v_p(c_1) \geq i$ and $v_p(c_2) \geq i$. We now show

$$\begin{aligned} v_p(c_2) &\geq i+1, \\ v_p(c_1) &\geq i+1. \end{aligned} \tag{4.2}$$

Assume that $v_p(c_2) = i$. The positive integer a_2 can be rewritten as

$$a_2 = \frac{p^n \left(\frac{p^s - c_1}{p^i}\right)}{\left(\frac{c_2}{p^i}\right)(c_2 - c_1)}$$

since $v_p(p^s - c_1) \geq i$ and $v_p(c_2) = i$. As both $\frac{c_2}{p^i}$ and $\frac{p^s-c_1}{p^i}$ are integers and $\gcd(p, \frac{c_2}{p^i}) = 1$, we have $\frac{c_2}{p^i} \mid \frac{p^s-c_1}{p^i}$. Then, $c_2 \mid (p^s - c_1)$ and it implies $c_2 \leq p^s - c_1$, which is a contradiction with $0 < c_1 < p^s < c_2$. Hence, $v_p(c_2) \geq i+1$.

To prove the second inequality in (4.2), assume that $v_p(c_1) = i$. We have $v_p(c_2 - c_1) = \min\{v_p(c_2), v_p(c_1)\} = i$, which implies

$$\gcd\left(\frac{c_2 - c_1}{p^i}, p\right) = 1. \tag{4.3}$$

Notice that $v_p(p^s - c_1) \geq i$ by assumption. Then the positive integer a_2 can be rewritten as

$$a_2 = \frac{p^n \left(\frac{p^s - c_1}{p^i}\right)}{c_2 \left(\frac{c_2 - c_1}{p^i}\right)}.$$

Thus, $\frac{c_2-c_1}{p^i} \mid \frac{p^s-c_1}{p^i}$ by (4.3). We conclude $c_2 - c_1 \leq p^s - c_1$, that is, $c_2 \leq p^s$, which is a contradiction with $0 < c_1 < p^s < c_2$. Hence, $v_p(c_1) \geq i+1$. By using (4.2), we have $v_p(c_2) \geq s$ and $v_p(c_1) \geq s$, which is a contradiction with $0 < c_1 < p^s < c_2$. Thus, we conclude the non-existence of a such function f. □

4.2 A new Class of Functions with Four-valued Absolute Walsh Spectrum

This section is concerned with a function f such that $S_2(f) = p^{3n+s}$ with $1 \leq s \leq n$ and its absolute Walsh transform takes exactly four distinct values, which are in $\{0, c_1 p^n, c_2 p^n, c_3 p^n\}$ with $0 < c_1 < c_2 < c_3$. We present some experimental results about such functions by MAGMA [5] in characteristics 2 and 3.

We start by introducing the notion of WT 4-valued with type-s Boolean functions for a nonempty class of such functions in characteristic 2.

Definition 4.1. Let f be a Boolean function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$, and both n and s be odd (or even) integers with $1 \leq s \leq n-4$. Then, f is called *WT 4-valued with type-s* if $|\widehat{\chi_f}(\omega)|^2$ has exactly four values, which are in $\{0, 2^{n+s-2}, 4*2^{n+s-2}, 9*2^{n+s-2}\}$ for every $\omega \in \mathbb{F}_{2^n}$.

The following theorem allows us to obtain an infinite class of WT 4-valued with type-s functions in the sense of Definition 4.1 starting from one such function with a smaller type parameter.

Theorem 4.2. *Let f be a WT 4-valued with type-s Boolean function on $\mathbb{F}_{2^n}$ and both n and s be integers with $1 \leq s \leq n$. Let m be a positive integer. There exists a Boolean function h on $\mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$ defined as $h(x,y) = f(x)$ for $x \in \mathbb{F}_{2^n}$ and $y \in \mathbb{F}_{2^m}$. Then, h is WT 4-valued with type-s' Boolean on $\mathbb{F}_{2^{n+m}}$, where $s' = m + s$.*

Proof. For $(\omega, v) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$, the Walsh transform $\widehat{\chi_h}(\omega, v)$ of h from $\mathbb{F}_{2^{n+m}}$ to $\mathbb{F}_2$ is given by

$$\begin{aligned}\widehat{\chi_h}(\omega, v) &= \sum_{x \in \mathbb{F}_{2^n}} \sum_{y \in \mathbb{F}_{2^m}} \xi_2^{h(x,y) - \mathrm{Tr}_2^{2^n}(\omega x) - \mathrm{Tr}_2^{2^m}(vy)} \\ &= \sum_{x \in \mathbb{F}_{2^n}} \xi_2^{f(x) - \mathrm{Tr}_2^{2^n}(\omega x)} \sum_{y \in \mathbb{F}_{2^m}} \xi_2^{-\mathrm{Tr}_2^{2^m}(vy)} = 2^m \widehat{\chi_f}(\omega),\end{aligned}$$

where in the second equality we used $h(x,y) = f(x)$ for $x \in \mathbb{F}_{2^n}$ and $y \in \mathbb{F}_{2^m}$. Hence, the proof is complete. □

We now make a preliminary but useful remark, which can be used to characterize the WT 4-valued with type-s functions. For every integers A_1, A_2, A_3 and every nonnegative integers u_1, u_2, u_3, u_4, we have

$$\sum_{\omega \in \mathbb{F}_{p^n}} \left(|\widehat{\chi_f}(\omega)|^2 - A_1\right)^{2u_1} \left(|\widehat{\chi_f}(\omega)|^2 - A_2\right)^{2u_2} \left(|\widehat{\chi_f}(\omega)|^2 - A_3\right)^{2u_3} |\widehat{\chi_f}(\omega)|^{2u_4} \geq 0.$$

In particular, for any integers A_1, A_2, A_3, the following equation holds

$$\sum_{\omega \in \mathbb{F}_{p^n}} \left(|\widehat{\chi_f}(\omega)|^2 - A_1\right) \left(|\widehat{\chi_f}(\omega)|^2 - A_2\right) \left(|\widehat{\chi_f}(\omega)|^2 - A_3\right) |\widehat{\chi_f}(\omega)|^2 =$$
$$S_4(f) - S_3(f)(A_1 + A_2 + A_3) + S_2(f)(A_1A_2 + A_2A_3 + A_1A_3) - S_1(f)A_1A_2A_3.$$

Theorem 4.3. *Let $f : F_{2^n} \to \mathbb{F}_2$ be a Boolean function such that $S_2(f) = 2^{3n+1}$ and $S_3(f) = 2^{4n-5}173$. Then f is WT 4-valued with type-1 if and only if $S_4(f) = 2^{5n-5}571$.*

Proof. For $A_1 = 2^{n-1}, A_2 = 4 * 2^{n-1}, A_3 = 9 * 2^{n-1}$, and by substituting the $S_i(f)$ values into above equation, we get

$$\sum_{\omega \in \mathbb{F}_{p^n}} \left(|\widehat{\chi_f}(\omega)|^2 - 2^{n-1}\right) \left(|\widehat{\chi_f}(\omega)|^2 - 4 * 2^{n-1}\right) \left(|\widehat{\chi_f}(\omega)|^2 - 9 * 2^{n-1}\right) |\widehat{\chi_f}(\omega)|^2$$
$$= 2^{5n-5}571 - 2^{5n-6}173 * 14 + 2^{5n-1}49 - 2^{5n-3}36 = 0,$$

that is, $|\widehat{\chi_f}(\omega)|^2 \in \{0, 2^{n-1}, 4*2^{n-1}, 9*2^{n-1}\}$ for every $\omega \in \mathbb{F}_{2^n}$. It is clear that all of these values appear. Indeed, otherwise, modifying the argument above in this proof we obtain the contradiction that $S_4(f) \neq 2^{5n-5}571$. This completes the proof. □

By MAGMA [5], we obtain several concrete examples of a WT 4-valued with type-1 Boolean function f such that $S_2(f) = 2^{3n+1}$ and $S_3(f) = 2^{4n-5}173$, where $n = 5$ and $s = 1$.

Example 4.1. *The function f given in Example 3.1 is WT 4-valued with type-1, i.e., $|\widehat{\chi_f}(\omega)|^2 \in \{0, 16, 64, 144\}$ for every $\omega \in \mathbb{F}_{2^5}$. Moreover it satisfies $S_2(f) = 2^{16}$ and $S_3(f) = 2^{15}173$.*

Recall that $S_0(f) = p^n$ and $S_1(f) = p^{2n}$ for any function f. Assume that f is a WT 4-valued with type-1 Boolean function such that $S_2(f) = 2^{3n+1}$ and $S_3(f) = 2^{4n-5}173$. Then, the even moments $S_i(f)$ for $i = 0, 1, 2, 3$ of f allow us to compute the multiplicity of each value of the absolute Walsh transform of f.

Lemma 4.2. *Let f be a WT 4-valued with type-1 Boolean function on $\mathbb{F}_{2^n}$, where n is an odd integer. Assume that $S_2(f) = 2^{3n+1}$ and $S_3(f) = 2^{4n-5}173$. Then, $|\widehat{\chi_f}(\omega)|^2$ takes a_0 times the value 0, a_1 times the value 2^{n-1}, a_2 times the value $4 * 2^{n-1}$ and a_3 times the value $9 * 2^{n-1}$, where $a_0 = 2^n - 26 * 2^{n-5}$, $a_1 = 15 * 2^{n-5}$, $a_2 = 10 * 2^{n-5}$, and $a_3 = 2^{n-5}$ are positive integers.*

Proof. As $S_0(f) = 2^n$, $S_1(f) = 2^{2n}$, $S_2(f) = 2^{3n+1}$ and $S_3(f) = 2^{4n-5}173$, we have

the following four equations, respectively:

$$\begin{aligned} a_0 + a_1 + a_2 + a_3 &= 2^n, \\ a_1 + 4a_2 + 9a_3 &= 2^{n+1}, \\ a_1 + 16a_2 + 81a_3 &= 2^{n+3}, \\ a_1 + 64a_2 + 729a_3 &= 2^{n-2}173. \end{aligned}$$

Thus, solving the above linear equation system, we get the desired positive integers.

□

The sequence of the Walsh power moments of a WT 4-valued with type-1 Boolean function follows from Lemma 4.2.

Corollary 4.1. *Let f be a WT 4-valued with type-1 Boolean function on $\mathbb{F}_{2^n}$. Assume that $S_2(f) = 2^{3n+1}$ and $S_3(f) = 2^{4n-5}173$. Then for every integer $i \geq 2$, we get*

$$S_i(f) = \sum_{\omega \in \mathbb{F}_{2^n}} |\widehat{\chi_f}(\omega)|^{2i} = 2^{n(i+1)+i-4}(2^{-2i-1}(15 + 9^i) + 5).$$

Proof. By Lemma 4.2, for every integer $i \geq 2$, we get

$$\begin{aligned} S_i(f) &= \sum_{\omega \in \mathbb{F}_{2^n}} |\widehat{\chi_f}(\omega)|^{2i} = (2^n - 26 * 2^{n-5}) * 0 \\ &+15 * 2^{n-5} * 2^{i(n-1)} + 10 * 2^{n-5} * 4^i * 2^{i(n-1)} + 2^{n-5} * 9^i * 2^{i(n-1)} \\ &= 2^{i(n-1)}(15 * 2^{n-5} + 10 * 2^{n-5} * 4^i + 2^{n-5} * 9^i) \\ &= 2^{n(i+1)+i-4}(2^{-2i-1}(15 + 9^i) + 5). \end{aligned}$$

The proof is complete. □

Remark 4.1. Let f be a WT 4-valued with type-1 Boolean function on $\mathbb{F}_{2^n}$. Assume that $S_2(f) = 2^{3n+1}$ and $S_3(f) = 2^{4n-5}173$. For $n = 5, 7$, the Walsh power moments $S_i(f)$ are given in

$$2^{n(i+1)+i-1} < S_i(f) < 2^{n(i+1)+2(i-1)}$$

for $i = 4, \ldots, 17$ and in $2^{n(i+1)+2(i-1)} < S_i(f) < 2^{n(i+1)+3(i-1)}$ for $i = 18, \ldots, 100000$.

By MAGMA [5], we obtain several concrete examples of a WT 4-valued with type-2 Boolean function f such that $S_2(f) = 2^{3n+2}$ and $S_3(f) = 2^{4n-2}109$, where n is an even integer for $s = 2$.

Example 4.2. *Let* $f(x) = \mathrm{Tr}_2^{2^6}(\zeta x^{23} + \zeta^{18}x^{27})$*, where* $\mathbb{F}_{2^6}^\star = \langle\zeta\rangle$ *with* $\zeta^6 + \zeta^4 + \zeta^3 + \zeta + 1 = 0$*. Then* f *is WT* 4*-valued with type-*2*, i.e.,* $|\widehat{\chi_f}(\omega)|^2 \in \{0, 64, 256, 576\}$ *for every* $\omega \in \mathbb{F}_{2^6}$*. Moreover it satisfies* $S_2(f) = 2^{20}$ *and* $S_3(f) = 2^{22}109$.

Assume that f is a WT 4-valued with type-2 Boolean function such that $S_2(f) = 2^{3n+2}$ and $S_3(f) = 2^{4n-2}109$. Then, the even moments $S_i(f)$ for $i = 0, 1, 2, 3$ of f allow us to compute the multiplicity of each value of the absolute Walsh transform of f.

Lemma 4.3. *Let* f *be a WT* 4*-valued with type-*2 *Boolean function on* $\mathbb{F}_{2^n}$*, where* n *is an even integer. Assume that* $S_2(f) = 2^{3n+2}$ *and* $S_3(f) = 2^{4n-2}109$*. Then,* $|\widehat{\chi_f}(\omega)|^2$ *takes* a_0 *times the value* 0*,* a_1 *times the value* 2^n*,* a_2 *times the value* $4 * 2^n$ *and* a_3 *times the value* $9 * 2^n$*, where* $a_0 = 2^n - 18 * 2^{n-5},\ a_1 = 15 * 2^{n-5},\ a_2 = 2 * 2^{n-5}$ *and* $a_3 = 2^{n-5}$ *are positive integers.*

Proof. Notice that we have $S_0(f) = 2^n$, $S_1(f) = 2^{2n}$, $S_2(f) = 2^{3n+2}$ and $S_3(f) = 2^{4n-2}109$. Then we have the following four equations, respectively:

$$\begin{aligned} a_0+ \quad & a_1 + a_2 + a_3 && = 2^n, \\ & a_1 + 4a_2 + 9a_3 && = 2^n, \\ & a_1 + 16a_2 + 81a_3 && = 2^{n+2}, \\ & a_1 + 64a_2 + 729a_3 && = 2^{n-2}109. \end{aligned}$$

Thus, solving the above linear equation system, we obtain these integers. □

The sequence of the Walsh power moments of a WT 4-valued with type-2 Boolean function follows from Lemma 4.3.

Corollary 4.2. *Let* f *be a WT* 4*-valued with type-*2 *Boolean function on* $\mathbb{F}_{2^n}$*. Assume that* $S_2(f) = 2^{3n+2}$ *and* $S_3(f) = 2^{4n-2}109$*. Then for every integer* $i \geq 2$*, we get*

$$S_i(f) = \sum_{\omega\in\mathbb{F}_{2^n}} |\widehat{\chi_f}(\omega)|^{2i} = 2^{n(i+1)+2i-4}(2^{-2i-1}(15 + 9^i) + 1).$$

Proof. By Lemma 4.3, for every integer $i \geq 2$, we have

$$\begin{aligned} S_i(f) &= \sum_{\omega \in \mathbb{F}_{2^n}} |\widehat{\chi_f}(\omega)|^{2i} = (2^n - 18 * 2^{n-5}) * 0 \\ &+15 * 2^{n-5} * 2^{in} + 2 * 2^{n-5} * 4^i * 2^{ni} + 2^{n-5} * 9^i * 2^{in} \\ &= 2^{n(i+1)+2i-4}(2^{-2i-1}(15 + 9^i) + 1). \end{aligned}$$

The proof is complete. □

Below we introduce the notion of WT 4-valued with type-s functions in odd characteristic, which is a non-empty class of such functions.

Definition 4.2. Let f be a function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$, and both n and s be integers with $1 \leq s \leq n-2$, where $p = 3$. Then, f is called *WT 4-valued with type-s* if $|\widehat{\chi_f}(\omega)|^2$ has exactly four values, which are in $\{0, p^{n+s-1}, 4p^{n+s-1}, 7p^{n+s-1}\}$ for every $\omega \in \mathbb{F}_{p^n}$.

By MAGMA [5], we obtain several concrete examples of a WT 4-valued with type-1 function f such that $S_2(f) = p^{3n+1}$ and $S_3(f) = 47p^{4n-1}$, where $p = 3$.

Example 4.3. *The function f given in Example 3.2 is the WT 4-valued with type-1, i.e., $|\widehat{\chi_f}(\omega)|^2 \in \{0, 27, 108, 189\}$ for every $\omega \in \mathbb{F}_{3^3}$. Moreover it satisfies $S_2(f) = 3^{10}$ and $S_3(f) = 3^{11}47$.*

Assume that f is a WT 4-valued with type-1 function such that $S_2(f) = p^{3n+1}$ and $S_3(f) = 47p^{4n-1}$, where $p = 3$. The even moments $S_i(f)$ for $i = 0, 1, 2, 3$ of f allow us to compute the multiplicity of each value of its absolute Walsh transform.

Lemma 4.4. *Let f be a WT 4-valued with type-1 function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$, where $p = 3$. Assume that $S_2(f) = p^{3n+1}$ and $S_3(f) = p^{4n-1}47$. Then $|\widehat{\chi_f}(\omega)|^2$ takes a_0 times the value 0, a_1 times the value p^n, a_2 times the value $4p^n$ and a_3 times the value $7p^n$, where $a_0 = p^n - 18p^{n-3}$, $a_1 = 16p^{n-3}$, $a_2 = p^{n-3}$ and $a_3 = p^{n-3}$ are positive integers.*

Proof. As $S_0(f) = p^n$, $S_1(f) = p^{2n}$, $S_2(f) = p^{3n+1}$ and $S_3(f) = 47p^{4n-1}$, we have

the following four equations, respectively:

$$\begin{aligned} a_0+ \quad & a_1 + a_2 + a_3 && = p^n, \\ & a_1 + 4a_2 + 7a_3 && = p^n, \\ & a_1 + 16a_2 + 49a_3 && = p^{n+1}, \\ & a_1 + 64a_2 + 343a_3 && = 47p^{n-1}. \end{aligned}$$

Then solving the above linear equation system, we get these integers. □

The sequence of the Walsh power moments of a WT 4-valued with type-1 function follows from Lemma 4.4.

Corollary 4.3. *Let f be a WT 4-valued with type-1 function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$, where $p = 3$. Assume that $S_2(f) = p^{3n+1}$ and $S_3(f) = p^{4n-1}47$. Then for every integer $i \geq 2$,*

$$S_i(f) = \sum_{\omega \in \mathbb{F}_{p^n}} |\widehat{\chi_f}(\omega)|^{2i} = p^{n(i+1)-3}(16 + 4^i + 7^i).$$

Proof. By Lemma 4.4, for every integer $i \geq 2$,

$$\begin{aligned} S_i(f) \quad &= \sum_{\omega \in \mathbb{F}_{2^n}} |\widehat{\chi_f}(\omega)|^{2i} = (p^n - 18p^{n-3})0 + 16p^{n-3}p^{ni} + p^{n-3}4^i p^{ni} + p^{n-3}7^i p^{ni} \\ &= p^{n(i+1)-3}(16 + 4^i + 7^i). \end{aligned}$$

□

Remark 4.2. Let f be a WT 4-valued with type-1 function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$. Assume that $S_2(f) = p^{3n+1}$ and $S_3(f) = p^{4n-1}47$. For $p = 3$ and $n = 3$, we have $p^{n(i+1)+i-1} < S_i(f) < p^{n(i+1)+2i-2}$ for $i = 3, \ldots, 100000$.

This chapter showed the non-existence of a function whose absolute Walsh transform has exactly three distinct values (one being zero). Additionally, we introduced the notion of WT 4-valued with type-s functions and presented explicit examples in characteristics 2 and 3.

CHAPTER 5

PARTIALLY BENT AND PLATEAUED FUNCTIONS OVER $\mathbb{F}_Q$ AND THEIR CHARACTERIZATIONS

Bent functions over $\mathbb{Z}_2$ were introduced by Rothaus [72] in the 1970s and then were extended to the residue class ring $\mathbb{Z}_k$ for any positive integer k by Kumar et.al. (1985) [46]. In 1991, perfect nonlinear functions over the residue class ring $\mathbb{Z}_k$ for any positive integer k were introduced by Nyberg [67]. It is worth mentioning that generalized bent and perfect nonlinear functions over $\mathbb{Z}_k$ are not equivalent for a positive integer k, in general. Nyberg [67], over $\mathbb{Z}_k$, showed that any perfect nonlinear function is a generalized bent function for any positive integer k, but the converse is true only if k is a prime number. In 1993, Carlet [12] introduced partially bent functions over $\mathbb{Z}_2$, and then they were extended in [25] to the finite field $\mathbb{Z}_p$ for any prime number p. As an extension of partially bent, Zheng and Zhang (1999) introduced in [78] plateaued functions over $\mathbb{Z}_2$, and then they were extended to the finite field $\mathbb{Z}_p$ and studied in [23, 55]. In 1997, Coulter and Matthews redefined in [28] bent functions over any finite field $\mathbb{F}_q$, with q a prime power.

The aim of this chapter is to study partially bent and plateaued functions over any finite field $\mathbb{F}_q$, with q a prime power. We first redefine partially bent and plateaued functions over $\mathbb{F}_q$, which rely on the concept of the Walsh transform in terms of canonical additive characters of $\mathbb{F}_q$. We give an explicit example of a 4-ary plateaued, but not vectorial plateaued Boolean function. We next provide a large number of characterizations of q-ary partially bent and q-ary plateaued functions by means of their Walsh power moments, derivatives and autocorrelation functions. Furthermore, we emphasize that q-ary bent and q-ary partially bent are q-ary plateaued. We finally

introduce the notion of a q-ary plateaued-type function associated with its Walsh-type transform.

The presented results in this chapter appear in [59, 65].

5.1 q-Ary Partially Bent and q-Ary Plateaued Functions over $\mathbb{F}_q$

This section revisits the notions of partially bent and plateaued functions over $\mathbb{F}_q$, where $q = p^m$ for a prime p and an integer $m > 1$.

The notions of generalized bent and perfect nonlinear functions over $\mathbb{Z}_k$ were redefined in [28] over any finite field $\mathbb{F}_q$. These notions rely on the concept of the Walsh transform in terms of canonical additive character of $\mathbb{F}_q$ given in (2.7).

Definition 5.1. [28] Let f be a function from $\mathbb{F}_q^n$ to $\mathbb{F}_q$. Then f is called *q-ary bent* if $|\widehat{\chi_f}(\omega)|^2 = q^n$ for all $\omega \in \mathbb{F}_q^n$, and f is called *perfect nonlinear* if the derivative $\mathcal{D}_a f$ (see Definition 2.7) is balanced for all nonzero $a \in \mathbb{F}_q^n$.

We can redefine partially bent and plateaued functions over $\mathbb{F}_q$, which rely on the concept of the Walsh transform in terms of canonical additive character of $\mathbb{F}_q$ given in (2.7).

Definition 5.2. Let f be a function from $\mathbb{F}_q^n$ to $\mathbb{F}_q$. Then

- f is called *q-ary partially bent* if the derivative $\mathcal{D}_a f$ is either balanced or constant for all $a \in \mathbb{F}_q^n$.
- f is called *q-ary plateaued* if its absolute Walsh transform takes only one nonzero value μ (also possibly the value 0), where μ is called *the amplitude* of plateaued f.

For any n-variable q-ary plateaued function, there exists a nonzero value μ such that $\mu^2 = q^r$, where $r \geq n$, since $\mathcal{N}_{\widehat{\chi_f}} \leq q^n$. Then the squared absolute Walsh transform of q-ary plateaued is divisible by q^n, and hence there exists an integer s with $0 \leq s \leq n$ such that $\mu^2 = q^{n+s}$. In the light of the above arguments, f is said to be *q-ary s-plateaued* if

$$|\widehat{\chi_f}(\omega)|^2 \in \{0, q^{n+s}\}$$

for all $\omega \in \mathbb{F}_q^n$. From now on, s is an integer with $0 \leq s \leq n$ in this chapter unless otherwise stated.

The multiplicity of the absolute Walsh coefficient of a q-ary plateaued function follows from the Parseval identity (see [55] for the p-ary case).

Lemma 5.1. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$ be s-plateaued. Then for $\omega \in \mathbb{F}_q^n$, $|\widehat{\chi_f}(\omega)|^2$ takes q^{n-s} times the value q^{n+s} and $q^n - q^{n-s}$ times the value 0.*

Proof. Recall that $\mathcal{N}_{\widehat{\chi_f}} = \#\{\omega \in \mathbb{F}_q^n : |\widehat{\chi_f}(\omega)|^2 = q^{n+s}\}$ for s-plateaued f. Then,

$$\sum_{\omega \in \mathbb{F}_q^n} |\widehat{\chi_f}(\omega)|^2 = q^{n+s}\mathcal{N}_{\widehat{\chi_f}}$$

and hence, $\mathcal{N}_{\widehat{\chi_f}} = q^{n-s}$ by the Parseval identity. Since $\#\mathbb{F}_q^n = q^n$, then we have $\#\{\omega \in \mathbb{F}_q^n : |\widehat{\chi_f}(\omega)|^2 = 0\} = q^n - q^{n-s}$. Hence, the result follows. □

By MAGMA [5], we obtain several q-ary plateaued functions, which show their existence.

Example 5.1. *Let $q = 4$ and $n = 3$. The function $f_1(x) = \mathrm{Tr}_4^{4^3}(\xi^2 x + \xi x^3)$ is the 4-ary 0-plateaued function and $f_2(x) = \mathrm{Tr}_4^{4^3}(\xi^3 x^3)$ is the 4-ary 1-plateaued function, where $\mathbb{F}_{4^3}^\star = \langle \xi \rangle$ with $\xi^3 + \xi^2 + \xi + \zeta^2 = 0$ for $\mathbb{F}_{2^2}^\star = \langle \zeta \rangle$.*

Remark 5.1. It is worth noting that, over $\mathbb{F}_q$, any perfect nonlinear function is q-ary partially bent. Moreover, the following theorem shows that, over $\mathbb{F}_q$, the notion of q-ary bent functions and the notion of perfect nonlinear functions are equivalent.

Theorem 5.1. *([28, Theorem 2.3]) Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. Then f is q-ary bent if and only if f is perfect nonlinear. Namely, f is q-ary bent if and only if the derivative $\mathcal{D}_a f$ is balanced for all nonzero $a \in \mathbb{F}_q^n$.*

The following follows readily from Theorem 5.1.

Corollary 5.1. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. Then f is q-ary bent if and only if $\Delta_f(a) = 0$ for all nonzero $a \in \mathbb{F}_q^n$.*

Proof. By Theorem 5.1, f is q-ary bent if and only if the derivative $\mathcal{D}_a f$ is balanced; equivalently, $\Delta_f(a) = 0$ for all nonzero $a \in \mathbb{F}_q^n$. □

In [28], by choosing an m-dimensional basis of $\mathbb{F}_q$ with $q = p^m$, we have that a q-ary bent function from $\mathbb{F}_q^n$ to $\mathbb{F}_q$ is equivalent to a vectorial p-ary bent function from $\mathbb{F}_p^{mn}$ to $\mathbb{F}_p^m$.

The following example shows that there exists a 4-ary plateaued function from $\mathbb{F}_4^3$ to $\mathbb{F}_4$, which is not vectorial plateaued from $\mathbb{F}_2^6$ to $\mathbb{F}_2^2$.

Example 5.2. *Let $q = 4$ and $n = 3$ where $q = p^m$ for $p = 2$ and $m = 2$. The function $f(x) = \mathrm{Tr}_4^{4^3}(\xi^4 x^{11} + \xi^4 x^7 + \xi^5 x^5)$ is 4-ary 1-plateaued where $\mathbb{F}_{4^3}^\star = \langle \xi \rangle$ with $\xi^3 + \xi^2 + \xi + \gamma^2 = 0$ for $\mathbb{F}_{2^2}^\star = \langle \gamma \rangle$. Then, its component function $f_1(x) = \mathrm{Tr}_2^4(f(x))$ is 2-plateaued Boolean function from $\mathbb{F}_2^6$ to $\mathbb{F}_2$. However, the other component functions $f_\gamma(x) = \mathrm{Tr}_2^4(\gamma f(x))$ and $f_{\gamma^2}(x) = \mathrm{Tr}_2^4(\gamma^2 f(x))$ are not plateaued Boolean functions from $\mathbb{F}_2^6$ to $\mathbb{F}_2$ since $|\widehat{\chi_{f_\gamma}}(\omega)|^2$ and $|\widehat{\chi_{f_{\gamma^2}}}(\omega)|^2$ have exactly four values, which are in $\{0, 64, 256, 576\}$ for every $\omega \in \mathbb{F}_{2^6}$. Hence, f is not vectorial plateaued Boolean function from $\mathbb{F}_2^6$ to $\mathbb{F}_2^2$.*

In view of Example 5.2, we can say that a q-ary plateaued function from $\mathbb{F}_q^n$ to $\mathbb{F}_q$ with its Walsh transform may not correspond to vectorial p-ary plateaued function from $\mathbb{F}_p^{mn}$ to $\mathbb{F}_p^m$ with the Walsh transform of its component functions for some cases, where $q = p^m$ for a prime p and an integer $m > 1$.

Remark 5.2. The notion of q-ary plateaued functions is not equivalent to the notion of vectorial p-ary plateaued functions in general, where $q = p^m$ for a prime p and an integer $m > 1$. This is the main reason for dealing with the notion of q-ary plateaued functions in this chapter.

We should remark that the characterizations of q-ary partially bent and q-ary plateaued functions given in Section 5.2 and Section 5.3, respectively, may not be given for vectorial p-ary functions, where $q = p^m$ for a prime p and an integer $m > 1$.

5.2 Characterizations of q-Ary Partially Bent Functions over $\mathbb{F}_q$

In this section, we characterize q-ary partially bent functions by means of their Walsh power moments, derivatives and autocorrelation functions. Several characterizations of these functions are presented, although some of them are interrelated, since they

can provide useful information about the structure of these functions. We also highlight that q-ary bent and q-ary partially bent functions are q-ary plateaued functions.

We begin with the significant properties of linear translator of a q-ary function (see Definition 2.6).

Lemma 5.2. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$ and let $\mathcal{L}_f$ be the set of linear translators of f. Let $\alpha \in \mathcal{L}_f$. Then we have the following.*

i.) $f(x + u\alpha) = f(x) + f(u\alpha) - f(0)$ *for all* $x \in \mathbb{F}_q^n$ *and* $u \in \mathbb{F}_q$.

ii.) $\mathcal{L}_f$ *is a linear subspace of* $\mathbb{F}_q^n$ *and it is called a linear space of* f.

iii.) $l(x) := f(x) - f(0)$ *is a linear function on* $\mathcal{L}_f$.

Proof. i.) For two values of x (one of which is 0), by Definition 2.6, obviously we have $f(x + u\alpha) - f(x) = f(u\alpha) - f(0)$ for all $x \in \mathbb{F}_q^n$ and $u \in \mathbb{F}_q$.

ii.) Firstly, the all-zero vector 0 is a linear translator of any function f, that is, $0 \in \mathcal{L}_f$. Next, let $\alpha_1 \in \mathcal{L}_f$ and $c \in \mathbb{F}_q$. For all $u \in \mathbb{F}_q$, by (*i*)

$$\begin{aligned}
&f(x + u(c\alpha_1)) - f(x) = \\
&f(x + u\alpha_1 + u(c-1)\alpha_1) - f(x + u\alpha_1) + f(x + u\alpha_1) - f(x) = \\
&f(u(c-1)\alpha_1) - f(0) + f(u\alpha_1) - f(0)
\end{aligned}$$

does not depend on $x \in \mathbb{F}_q^n$, that is, $c\alpha_1 \in \mathcal{L}_f$ where in the last equality we used that $f(x+u\alpha_1+u(c-1)\alpha_1) - f(x+u\alpha_1) = f(u(c-1)\alpha_1) - f(0)$ by setting $x = x+u\alpha_1$ and $u = u(c-1)$ in (*i*). Lastly, let $\alpha_1, \alpha_2 \in \mathcal{L}_f$. For all $x \in \mathbb{F}_q^n$ and $u \in \mathbb{F}_q$,

$$\begin{aligned}
f(x + u(\alpha_1 + \alpha_2)) &= f(x + u\alpha_1) + f(u\alpha_2) - f(0) \\
&= f(x) + f(u\alpha_1) - f(0) + f(u\alpha_2) - f(0) \\
&= f(x) + f(u(\alpha_1 + \alpha_2)) - f(0),
\end{aligned} \tag{5.1}$$

where in the last equality we used that $f(u\alpha_1 + u\alpha_2) = f(u\alpha_1) + f(u\alpha_2) - f(0)$ by setting $x = u\alpha_1$ by (*i*). Hence, $\alpha_1 + \alpha_2 \in \mathcal{L}_f$.

iii.) Let $\alpha_1, \alpha_2 \in \mathcal{L}_f$. By (5.1), for all $u \in \mathbb{F}_q$, we have

$$f(u(\alpha_1 + \alpha_2)) - f(0) = f(u\alpha_1) - f(0) + f(u\alpha_2) - f(0),$$

that is, $l(u(\alpha_1 + \alpha_2)) = l(u\alpha_1) + l(u\alpha_2)$. The proof is complete. □

Remark 5.3. The notion of q-ary partially bent functions can be revisited as follows. A function f with linear space $\mathcal{L}_f$ is called q-ary partially bent if the derivative $\mathcal{D}_a f$ is balanced for all $a \in \mathbb{F}_q^n \setminus \mathcal{L}_f$. It is obvious that the derivative $\mathcal{D}_a f$ is constant for all $a \in \mathcal{L}_f$ by Definition 2.6.

Remark 5.4. Any q-ary bent is the q-ary partially bent with $\mathcal{L}_f = \{0\}$ since q-ary bent functions have balanced derivatives $\mathcal{D}_a f$ for all nonzero $a \in \mathbb{F}_q^n$ (see Theorem 5.1).

Proposition 5.1. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$ with linear space $\mathcal{L}_f$ and let $\dim(\mathcal{L}_f) = s$. If f is q-ary partially bent, then $|\widehat{\chi_f}(\omega)|^2 \in \{0, q^{n+s}\}$ for all $\omega \in \mathbb{F}_q^n$.*

Proof. Assume that f is q-ary partially bent, that is, the derivative $\mathcal{D}_a f$ is balanced for all $a \in \mathbb{F}_q^n \setminus \mathcal{L}_f$. By Proposition 2.2 (*v*), for all $\omega \in \mathbb{F}_q^n$

$$\begin{aligned} |\widehat{\chi_f}(\omega)|^2 &= \widehat{\Delta_f}(\omega) = \sum_{a \in \mathbb{F}_q^n} \Delta_f(a) \overline{\chi}(\omega \cdot a) \\ &= \sum_{a \in \mathcal{L}_f} \sum_{x \in \mathbb{F}_q^n} \chi(\mathcal{D}_a f(x)) \overline{\chi}(\omega \cdot a) + \sum_{a \notin \mathcal{L}_f} \sum_{x \in \mathbb{F}_q^n} \chi(\mathcal{D}_a f(x)) \overline{\chi}(\omega \cdot a) \end{aligned}$$

where the latter is zero since $\mathcal{D}_a f$ is balanced for all $a \in \mathbb{F}_q^n \setminus \mathcal{L}_f$. By Lemma 5.2 (*i*), if $a \in \mathcal{L}_f$, then $f(x+a) - f(x) = f(a) - f(0)$ for all $x \in \mathbb{F}_q^n$. Then, for all $\omega \in \mathbb{F}_q^n$

$$\begin{aligned} |\widehat{\chi_f}(\omega)|^2 &= \sum_{a \in \mathcal{L}_f} \sum_{x \in \mathbb{F}_q^n} \chi(f(a) - f(0) - \omega \cdot a) \\ &= q^n \sum_{a \in \mathcal{L}_f} \chi(f(a) - f(0) - \omega \cdot a) \\ &= \begin{cases} q^{n+s}, & \text{if } f(a) - \omega \cdot a = f(0) \text{ on } \mathcal{L}_f, \\ 0, & \text{otherwise} \end{cases} \end{aligned}$$

where we used that $f(a) - f(0) - \omega \cdot a$ is linear on $\mathcal{L}_f$. Hence, $|\widehat{\chi_f}(\omega)|^2 \in \{0, q^{n+s}\}$ for all $\omega \in \mathbb{F}_q^n$. □

The identity involving the fourth power moment of the Walsh transform and the second-order derivative of a function was constituted for Boolean and p-ary functions (see, e.g., [13, 55]), which can also be given for q-ary functions.

Proposition 5.2. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. Then*

$$S_2(f) = q^n \sum_{a,b,x \in \mathbb{F}_q^n} \chi(\mathcal{D}_a \mathcal{D}_b f(x)). \tag{5.2}$$

Proof. Recall that $|z|^4 = z^2\overline{z}^2$ for $z \in \mathbb{C}$. Then the left hand-side of (5.2) is

$$\begin{aligned} & \sum_{x,a,b,c \in \mathbb{F}_q^n} \chi(f(x) - f(a) + f(b) - f(c)) \sum_{\omega \in \mathbb{F}_q^n} \overline{\chi}(\omega \cdot (x - a + b - c)) \\ = \; & q^n \sum_{a,b,x \in \mathbb{F}_q^n} \chi(f(x) - f(a) + f(b) - f(x - a + b)) \end{aligned}$$

since $\sum_{\omega \in \mathbb{F}_q^n} \xi_p^{\mathrm{Tr}_p^{q^n}(-\omega(x-a+b-c))} = \begin{cases} q^n \text{ if } c = x - a + b, \\ 0 \text{ otherwise.} \end{cases}$

Hence, since $(a, b, x) \mapsto (x + a, x + a + b, x)$ is a permutation of $(\mathbb{F}_q^n)^3$, then (5.2) holds. □

Obviously, the link given in Proposition 3.2 can be extended to a q-ary function as follows.

Proposition 5.3. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. Then,*

$$\sum_{a \in \mathbb{F}_q^n} |\Delta_f(a)|^2 = \sum_{a,b,x \in \mathbb{F}_q^n} \chi(\mathcal{D}_a \mathcal{D}_b f(x)). \tag{5.3}$$

Proof. Since $|z|^2 = z\overline{z}$ for $z \in \mathbb{C}$, the left hand side of (5.3) is

$$\begin{aligned} \sum_{a \in \mathbb{F}_q^n} \sum_{b \in \mathbb{F}_q^n} \chi(\mathcal{D}_a f(b)) \sum_{x \in \mathbb{F}_q^n} \overline{\chi}(\mathcal{D}_a f(x)) &= \sum_{a,b,x \in \mathbb{F}_q^n} \chi(\mathcal{D}_a f(b) - \mathcal{D}_a f(x)) \\ &= \sum_{a,b,x \in \mathbb{F}_q^n} \chi(\mathcal{D}_a \mathcal{D}_b f(x)), \end{aligned}$$

where in the last equality we used the (bijective) change of variable $b \mapsto b + x$. □

The following is a direct consequence of Propositions 5.2 and 5.3.

Proposition 5.4. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. Then*

$$S_2(f) = q^n \sum_{a \in \mathbb{F}_q^n} |\Delta_f(a)|^2.$$

The q-ary partially bent functions can be characterized in terms of the fourth power moment of its Walsh transform only.

Theorem 5.2. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$ with linear space $\mathcal{L}_f$ and let $\dim(\mathcal{L}_f) = s$. Then, f is q-ary partially bent if and only if $S_2(f) = q^{3n+s}$.*

Proof. Assume that $S_2(f) = q^{3n+s}$. Then by Proposition 5.4, we have

$$\sum_{a \in \mathbb{F}_q^n} |\Delta_f(a)|^2 = q^{2n+s}. \tag{5.4}$$

By the definition of $\mathcal{L}_f$, the derivative $\mathcal{D}_a f$ at point $a \in \mathcal{L}_f$ is constant. Then, since $|z|^2 = z\overline{z}$ for $z \in \mathbb{C}$, we have

$$\sum_{a \in \mathcal{L}_f} |\Delta_f(a)|^2 = \sum_{a \in \mathcal{L}_f} \sum_{x,y \in \mathbb{F}_q^n} \chi(\mathcal{D}_a f(x) - \mathcal{D}_a f(y)) = \sum_{a \in \mathcal{L}_f} q^{2n} = q^{2n+s}. \tag{5.5}$$

Combining (5.4) and (5.5), we have $\sum_{a \notin \mathcal{L}_f} |\Delta_f(a)|^2 = 0$, equivalently, $\Delta_f(a) = 0$, that is, $\mathcal{D}_a f$ is balanced for all $a \notin \mathcal{L}_f$. Hence, f is q-ary partially bent. The other direction follows from Proposition 5.1. □

We are ready to give the following natural consequence over $\mathbb{F}_q$.

Proposition 5.5. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$ with linear space $\mathcal{L}_f$ and let $\dim(\mathcal{L}_f) = s$ where s is an integer with $0 \leq s \leq n$. Then, f is q-ary partially bent if and only if f is q-ary s-plateaued. In particular, f is q-ary bent if and only if f is q-ary 0-plateaued.*

Proof. Assume that f is q-ary s-plateaued. Then by Lemma 5.1, we have $S_2(f) = q^{3n+s}$ and hence, by Theorem 5.2, f is q-ary partially bent. The other direction follows readily from Proposition 5.1. In particular, by Remark 5.4, the second statement follows from the first statement. □

Remark 5.5. Notice that the second statement of Proposition 5.5 follows also from the Parseval identity, which implies that q-ary plateaued is q-ary bent if and only if its absolute Walsh transform never takes the value 0.

Remark 5.6. By Proposition 5.5, characterizations of a q-ary plateaued function are valid for any q-ary bent and q-ary partially bent.

In the light of Propositions 5.1 and 5.5, the following can be identified.

Remark 5.7. Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$ with linear space $\mathcal{L}_f$ and let $\dim(\mathcal{L}_f) = s$. Then, f is q-ary partially bent if and only if $|\widehat{\chi_f}(\omega)|^2 \in \{0, q^{n+s}\}$ for all $\omega \in \mathbb{F}_q^n$. Here, we can say that f is q-ary s-partially bent.

The multiplicity of the absolute Walsh coefficient of a q-ary partially bent function is as follows (see Lemma 5.1).

Lemma 5.3. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$ be a q-ary partially bent function with linear space $\mathcal{L}_f$ and let $\dim(\mathcal{L}_f) = s$. Then for $\omega \in \mathbb{F}_q^n$, $|\widehat{\chi_f}(\omega)|^2$ takes q^{n-s} times the value q^{n+s} and $q^n - q^{n-s}$ times the value 0.*

Remark 5.8. The set of q-ary bent functions is a proper subset of the set of q-ary partially bent functions. Namely, a q-ary partially bent function with nonzero linear translators is not a q-ary bent function. Similarly, the set of q-ary partially bent functions is a proper subset of the set of q-ary plateaued functions. Namely, q-ary s-plateaued functions with $\dim(\mathcal{L}_f) < s$ are not q-ary partially bent functions.

The sequence of the Walsh power moments of a q-ary partially bent function is a simple geometric sequence, which follows directly from Lemma 5.3.

Corollary 5.2. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$ be q-ary partially bent with linear space $\mathcal{L}_f$ and let $\dim(\mathcal{L}_f) = s$. Then for every positive integer i, we have $S_i(f) = q^{n(i+1)+s(i-1)}$ and for all integers $i \geq 1$ and $j \geq 2$, $S_i(f)S_j(f) = S_{i+1}(f)S_{j-1}(f)$.*

Proof. By Lemma 5.3, for all positive integers i, we have $S_i(f) = q^{n-s}(q^{n+s})^i = q^{n(i+1)+s(i-1)}$. Clearly, the following

$$\begin{aligned} S_i(f)S_j(f) &= q^{n(i+1)+s(i-1)}q^{n(j+1)+s(j-1)} = q^{n(i+j+2)+s(i+j-2)} \text{ and} \\ S_{i+1}(f)S_{j-1}(f) &= q^{n(i+2)+si}q^{nj+s(j-2)} = q^{n(i+j+2)+s(i+j-2)} \end{aligned}$$

are equal for all $i \geq 1$ and $j \geq 2$. Hence, the result follows. □

We now give a bound stating the trade-off between the number of the nonzero values of the autocorrelation function and the size of the Walsh support of q-ary functions. Carlet [12] gave this bound for every Boolean function, and it is satisfied by Boolean partially bent functions (for the p-ary case, see [25]). Recall that $\mathrm{Supp}(\widehat{\chi_f}) = \{\omega \in \mathbb{F}_q^n \mid \widehat{\chi_f}(\omega) \neq 0\}$ and $\mathcal{N}_{\widehat{\chi_f}} = \#\mathrm{Supp}(\widehat{\chi_f})$. We denote by $\mathrm{Supp}(\Delta_f)$ the set of elements $a \in \mathbb{F}_q^n$ such that $\mathcal{D}_a f$ is unbalanced, i.e., the autocorrelation of f at point a is nonzero:

$$\mathrm{Supp}(\Delta_f) := \{a \in \mathbb{F}_q^n \mid \Delta_f(a) \neq 0\}. \tag{5.6}$$

Denote by $\mathcal{N}_{\Delta_f}$ the size of $\mathrm{Supp}(\Delta_f)$.

Theorem 5.3. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. Then*

$$q^n \le \mathcal{N}_{\Delta_f} * \mathcal{N}_{\widehat{\chi_f}}, \tag{5.7}$$

with an equality if and only if for all $b \in \mathbb{F}_q^n$, the derivative $D_b f$ is either balanced or constant, that is, f is q-ary partially bent.

Proof. By Proposition 2.2 (*vi*), $|\widehat{\chi_f}(0)|^2 = \sum_{a \in \mathbb{F}_q^n} \Delta_f(a)$. Then by (5.6), we have $|\widehat{\chi_f}(0)|^2 \le q^n \mathcal{N}_{\Delta_f}$. Notice that $\mathcal{N}_{\Delta_f}$ is invariant if $f(x)$ is replaced with $f(x) - \omega \cdot x$ for all $\omega \in \mathbb{F}_q^n$, and hence,

$$|\widehat{\chi_f}(\omega)|^2 \le q^n \mathcal{N}_{\Delta_f}. \tag{5.8}$$

Then, since $\sum_{\omega \in \mathbb{F}_q^n} |\widehat{\chi_f}(\omega)|^2 \le \max_{b \in \mathbb{F}_q^n}(|\widehat{\chi_f}(b)|^2)\mathcal{N}_{\widehat{\chi_f}}$, by (5.8) and using the Parseval identity, we have

$$q^{2n} \le \max_{b \in \mathbb{F}_q^n}(|\widehat{\chi_f}(b)|^2)\mathcal{N}_{\widehat{\chi_f}} \le q^n \mathcal{N}_{\Delta_f} * \mathcal{N}_{\widehat{\chi_f}}. \tag{5.9}$$

This completes the proof of the first assertion.

For the equality case, assume that the bound (5.7) holds. Then (5.9) implies that $\max_{b \in \mathbb{F}_q^n}(|\widehat{\chi_f}(b)|^2)\mathcal{N}_{\widehat{\chi_f}} = q^{2n}$. By the Parseval identity, for all $\omega \in \mathrm{Supp}(\widehat{\chi_f})$ we have $|\widehat{\chi_f}(\omega)|^2 = \max_{b \in \mathbb{F}_q^n}(|\widehat{\chi_f}(b)|^2)$, that is, there exists an integer s such that $|\widehat{\chi_f}(\omega)|^2 = q^{n+s}$ for all $\omega \in \mathrm{Supp}(\widehat{\chi_f})$, i.e., f is s-plateaued. By Lemma 5.1, $\mathcal{N}_{\widehat{\chi_f}} = q^{n-s}$, and hence, $\mathcal{N}_{\Delta_f} = q^s$ by (5.7). For all $\omega \in \mathrm{Supp}(\widehat{\chi_f})$, by Proposition 2.2 (*v*), we have

$$\begin{aligned} |\widehat{\chi_f}(\omega)|^2 &= \sum_{a \in \mathbb{F}_q^n} \Delta_f(a)\overline{\chi}(\omega \cdot a) \\ &= \sum_{a \in \mathrm{Supp}(\Delta_f)} \Delta_f(a)\overline{\chi}(\omega \cdot a) + \sum_{a \notin \mathrm{Supp}(\Delta_f)} \Delta_f(a)\overline{\chi}(\omega \cdot a), \end{aligned}$$

where the latter is zero by (5.6). Hence, for all $\omega \in \mathrm{Supp}(\widehat{\chi_f})$,

$$\sum_{a \in \mathrm{Supp}(\Delta_f)} \sum_{x \in \mathbb{F}_q^n} \chi(\mathcal{D}_a f(x) - \omega \cdot a) = q^{n+s}.$$

Then for all $a \in \mathrm{Supp}(\Delta_f)$, we have $\sum_{x \in \mathbb{F}_q^n} \chi(\mathcal{D}_a f(x) - \omega \cdot a) = q^n$ for all $\omega \in \mathrm{Supp}(\widehat{\chi_f})$, that is, $\mathcal{D}_a f(x) = \omega \cdot a$ for all $x \in \mathbb{F}_q^n$, i.e., $\mathcal{D}_a f$ is constant. Notice that $\mathcal{D}_a f$ is balanced for all $a \notin \mathrm{Supp}(\Delta_f)$ by (5.6). Hence, f is q-ary partially bent. Conversely, assume that f is q-ary partially bent. Then, $\mathrm{Supp}(\Delta_f)$ is the set of linear

translators of f and there exists an integer s such that $\mathcal{N}_{\Delta_f} = q^s$, that is, the dimension of linear space of f is equal to s. By Lemma 5.3, we have $\mathcal{N}_{\widehat{\chi_f}} = q^{n-s}$. Hence, the bound (5.7) holds. □

Remark 5.9. A function f is q-ary partially bent if and only if $|\Delta_f(a)| \in \{0, q^n\}$ for all $a \in \mathbb{F}_q^n$.

We now give a powerful characterization of q-ary partially bent functions by means of their second-order derivatives (see [21] for a Boolean bent function).

Theorem 5.4. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$ with linear space $\mathcal{L}_f$ and let $\dim(\mathcal{L}_f) = s$. Set*

$$\theta_f(x) = \sum_{a,b \in \mathbb{F}_q^n} \chi(\mathcal{D}_b \mathcal{D}_a f(x))$$

for all $x \in \mathbb{F}_{p^n}$. Then, f is q-ary partially bent if and only if $\theta_f(x) = q^{n+s}$ for all $x \in \mathbb{F}_q^n$.

Proof. Put $\theta = q^{n+s}$. For all $x \in \mathbb{F}_q^n$, $\theta_f(x) = \theta$ if and only if for all $x \in \mathbb{F}_q^n$,

$$\sum_{a,b \in \mathbb{F}_q^n} \chi(f(a+b-x) - f(a) - f(b)) = \theta \chi(-f(x))$$

(by the (bijective) change of variables: $a \mapsto a - x$ and $b \mapsto b - x$); equivalently, for all $x \in \mathbb{F}_q^n$

$$\sum_{a,b \in \mathbb{F}_q^n} \overline{\chi_f}(a) \overline{\chi_f}(b) \chi_g(x - a - b) = \theta \overline{\chi_f}(x),$$

where we defined $g(y) := f(-y)$ for all $y \in \mathbb{F}_q^n$. Equivalently, using the convolution product (see Definition 2.4), for all $x \in \mathbb{F}_q^n$

$$\left(\overline{\chi_f} \otimes \overline{\chi_f} \otimes \chi_g\right)(x) = \theta \overline{\chi_f}(x). \tag{5.10}$$

By Theorem 2.1, the Fourier transform of left-hand side of (5.10) is $\widehat{\overline{\chi_f}}(\omega)\ \widehat{\overline{\chi_f}}(\omega)\widehat{\chi_g}(\omega)$ for all $\omega \in \mathbb{F}_q^n$. Notice that for all $\omega \in \mathbb{F}_q^n$, $\widehat{\overline{\chi_f}}(\omega) = \overline{\widehat{\chi_f}}(-\omega)$ by Proposition 2.2 and $\widehat{\chi_g}(\omega) = \widehat{\chi_f}(-\omega)$ since $g(y) = f(-y)$ for all $y \in \mathbb{F}_q^n$. By Lemma 2.4, for all $x \in \mathbb{F}_q^n$, (5.10) holds if and only if for all $\omega \in \mathbb{F}_q^n$

$$\overline{\widehat{\chi_f}}(\omega)\ \overline{\widehat{\chi_f}}(\omega)\widehat{\chi_f}(\omega) = \theta \overline{\widehat{\chi_f}}(\omega).$$

Therefore, for $\theta_f = q^{n+s}$, $\theta_f(x) = \theta$ for all $x \in \mathbb{F}_q^n$ if and only if $|\widehat{\chi_f}(\omega)|^2 \in \{0, \theta\}$ for all $\omega \in \mathbb{F}_q^n$, that is, f is q-ary partially bent. □

It is worth noting that Theorem 5.4 approves that any q-ary quadratic function is a q-ary partially bent function since the second-order derivative of quadratic function is constant.

The following seems to be more practical than Theorem 5.4.

Theorem 5.5. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$ with linear space $\mathcal{L}_f$ and let $\dim(\mathcal{L}_f) = s$. Then, we have*

$$q^{2n+s} \leq \sum_{a,b,x \in \mathbb{F}_q^n} \chi(\mathcal{D}_b \mathcal{D}_a f(x))$$

with an equality if and only if f is q-ary partially bent.

Proof. Because of the fact that $\mathcal{D}_a f$ is constant for all $a \in \mathcal{L}_f$, we have

$$\sum_{a \in \mathcal{L}_f} \sum_{b,x \in \mathbb{F}_q^n} \chi(\mathcal{D}_b \mathcal{D}_a f(x)) = q^{2n+s}. \tag{5.11}$$

Meanwhile,

$$\sum_{a \notin \mathcal{L}_f} \sum_{b,x \in \mathbb{F}_q^n} \chi(\mathcal{D}_b \mathcal{D}_a f(x)) \geq 0 \tag{5.12}$$

with an equality if and only if $\mathcal{D}_a f$ is balanced for all $a \notin \mathcal{L}_f$. Combining (5.11) and (5.12), the proof is complete. □

Corollary 5.3. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$ with linear space $\mathcal{L}_f$ and let $\dim(\mathcal{L}_f) = s$. Then, we have*

$$q^{2n+s} \leq \sum_{a \in \mathbb{F}_q^n} |\Delta_f(a)|^2$$

with an equality if and only if f is q-ary partially bent.

Proof. For all $a \in \mathcal{L}_f$, because $\mathcal{D}_a f$ is constant, $|\Delta_f(a)|^2 = q^{2n}$. As in the proof of Theorem 5.5, we have

$$\sum_{a \in \mathcal{L}_f} |\Delta_f(a)|^2 = q^{2n+s}, \tag{5.13}$$

$$\sum_{a \notin \mathcal{L}_f} |\Delta_f(a)|^2 \geq 0 \tag{5.14}$$

with an equality if and only if $\Delta_f(a) = 0$; i.e., $\mathcal{D}_a f$ is balanced for all $a \notin \mathcal{L}_f$. Combining (5.13) and (5.14), the proof is complete. □

In view of Proposition 5.3, Theorem 5.5 and Corollary 5.3 are equivalent. The following is an immediate consequence of Proposition 5.4 and Corollary 5.3.

Corollary 5.4. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$ with linear space $\mathcal{L}_f$ and let $\dim(\mathcal{L}_f) = s$. Then*

$$q^{3n+s} \leq S_2(f),$$

with an equality if and only if f is q-ary partially bent.

The link given in Proposition 3.9 can be extended to q-ary case.

Proposition 5.6. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. Then for all $x \in \mathbb{F}_q^n$,*

$$\sum_{\omega \in \mathbb{F}_q^n} \chi(f(x) - \omega \cdot x)\overline{\widehat{\chi_f}(\omega)}\, |\widehat{\chi_f}(\omega)|^2 = q^n \sum_{a,b \in \mathbb{F}_q^n} \chi(\mathcal{D}_a\mathcal{D}_b f(x)). \tag{5.15}$$

Proof. By the definition of $\widehat{\chi_f}$, for all $x \in \mathbb{F}_q^n$, the left-hand side of (5.15) is

$$\begin{aligned}
&\sum_{a,b,c \in \mathbb{F}_q^n} \chi(f(x) - f(a) - f(b) + f(c)) \sum_{\omega \in \mathbb{F}_q^n} \chi(\omega \cdot (a + b - c - x)) \\
&= q^n \sum_{a,b \in \mathbb{F}_q^n} \chi(f(x) - f(a) - f(b) + f(a + b - x)) \\
&= q^n \sum_{a,b \in \mathbb{F}_q^n} \chi(\mathcal{D}_a\mathcal{D}_b f(x)),
\end{aligned}$$

where we used that $\sum_{\omega \in \mathbb{F}_q^n} \overline{\chi}(\omega \cdot (x - a - b + c))$ is null if $c \neq a + b - x$ in the first equality, and $(a, b, x) \mapsto (a + x, b + x, x)$ is a permutation of $(\mathbb{F}_q^n)^3$ in the second equality. The result now follows. □

The following corollary is a direct consequence of Theorem 5.4 and Proposition 5.6.

Corollary 5.5. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$ with linear space $\mathcal{L}_f$ and let $\dim(\mathcal{L}_f) = s$. Then, we have for all $x \in \mathbb{F}_q^n$*

$$q^{2n+s} \leq \sum_{\omega \in \mathbb{F}_q^n} \chi(f(x) - \omega \cdot x)\overline{\widehat{\chi_f}(\omega)}\, |\widehat{\chi_f}(\omega)|^2,$$

with an equality if and only if f is q-ary partially bent.

We now give an example of q-ary partially bent functions.

Example 5.3. *Let p be an odd prime, $m \geq 2$ and $n \geq 2$ be integers and $q = p^m$. Let f be an arbitrary $\mathbb{F}_q$-quadratic form from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ given by*

$$f(x) = \mathrm{Tr}_q^{q^n}(a_0x^2 + a_1x^{q+1} + a_2x^{q^2+1} + \cdots + a_{\lfloor \frac{n}{2} \rfloor}x^{q^{\lfloor \frac{n}{2} \rfloor}+1}).$$

As in Example 3.3, by [7, 8], we have an algorithm to construct f with radical

$$\mathcal{W}_f = \{x \in \mathbb{F}_{q^n} : f(x+y) = f(x) + f(y), \forall y \in \mathbb{F}_{q^n}\} \tag{5.16}$$

of prescribed dimension s over $\mathbb{F}_q$ for each given integer s with $0 \leq s \leq n-1$. For $\lambda \in \mathbb{F}_{p^m}^\star$, the component function f_λ from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ given by $f_\lambda(x) = \mathrm{Tr}_p^{p^m}(\lambda f(x))$ is an $\mathbb{F}_p$-quadratic form with radical

$$\mathcal{W}_{f_\lambda} = \{x \in \mathbb{F}_{p^n} : f_\lambda(x+y) = f_\lambda(x) + f_\lambda(y), \forall y \in \mathbb{F}_{p^n}\}. \tag{5.17}$$

For a $\mathbb{F}_q$-quadratic form f on $\mathbb{F}_{q^n}$ and $\lambda \in \mathbb{F}_q^\star$, the radical $\mathcal{W}_f$ in (5.16) is the set of the roots of the equation

$$a_0x + a_1x^q + (a_1x)^{q^{-1}} + a_2x^{q^2} + (a_2x)^{q^{-2}} + \cdots + a_{\lfloor \frac{n}{2} \rfloor}x^{q^{\lfloor \frac{n}{2} \rfloor}} + \left(a_{\lfloor \frac{n}{2} \rfloor}x\right)^{q^{-\lfloor \frac{n}{2} \rfloor}} \tag{5.18}$$

in $\mathbb{F}_{q^n}$ and $\mathcal{W}_{f_\lambda}$ in (5.17) is the set of the roots of the equation

$$\lambda a_0x + \lambda a_1x^q + (\lambda a_1x)^{q^{-1}} + \lambda a_2x^{q^2} + \cdots + \lambda a_{\lfloor \frac{n}{2} \rfloor}x^{q^{\lfloor \frac{n}{2} \rfloor}} + \left(\lambda a_{\lfloor \frac{n}{2} \rfloor}x\right)^{q^{-\lfloor \frac{n}{2} \rfloor}} \tag{5.19}$$

(see e.g., [7, Lemma 2.1]). As $\lambda \in \mathbb{F}_q^\star$, it is easy to observe from (5.18) and (5.19) that $\mathcal{W}_f = \mathcal{W}_{f_\lambda}$. Therefore, we obtain vectorial s-plateaued function F from $\mathbb{F}_{p^{mn}}$ to $\mathbb{F}_{p^m}$ (notice that $F(x) = f(x)$ for all $x \in \mathbb{F}_{p^n}$). This shows existence of an algorithm to construct vectorial s-plateaued functions F for any integer s with $0 \leq s \leq n-1$.

5.3 Characterizations of q-Ary Plateaued Functions over $\mathbb{F}_q$

This section gives an extension of some characterizations of p-ary plateaued functions given in Chapter 3 to q-ary case. We provide many characterizations of q-ary plateaued functions by means of their derivatives, Walsh power moments and autocorrelation functions. We believe that they provide useful information about the structure of q-ary plateaued.

We make a preliminary but useful remarks. For every nonnegative integers i and A, we have

$$\sum_{\omega\in\mathbb{F}_q^n}\Big(|\widehat{\chi_f}(\omega)|^2-A\Big)^2|\widehat{\chi_f}(\omega)|^{2i} \quad = S_{i+2}(f)-2AS_{i+1}(f)+A^2S_i(f)\geq 0. \tag{5.20}$$

For any positive integer i, there exists a positive integer A such that

$$S_i(f)A^2-2S_{i+1}(f)A+S_{i+2}(f)=0 \tag{5.21}$$

if and only if f is q-ary s-plateaued, where $A=q^{n+s}$. To exhibit a link between the Walsh power moments of q-ary plateaued functions, we shall consider some particular values of i in (5.20). More precisely, for $A=q^{n+s}$, where s is an integer with $1\leq s\leq n$, and

- for $i=1$, f is q-ary s-plateaued if and only if $S_3(f)=2q^{n+s}S_2(f)-q^{4n+2s}$,
- for $i=2$, then f is q-ary s-plateaued if and only if $S_4(f)=2q^{n+s}S_3(f)-q^{2n+2s}S_2(f)$,
- for $i=3$, then f is q-ary s-plateaued if and only if $S_5(f)=2q^{n+s}S_4(f)-q^{2n+2s}S_3(f)$.

If $S_2(f)\geq q^{3n+s}$, then $S_3(f)\geq q^{4n+2s}$. More precisely, if $S_2(f)=q^{3n+s}$, then $S_4(f)\geq q^{5n+3s}$.

More generally, for every nonnegative integers A, i and j,

$$\sum_{\omega\in\mathbb{F}_q^n}\Big(|\widehat{\chi_f}(\omega)|^2-A\Big)^{2j}|\widehat{\chi_f}(\omega)|^{2i}\geq 0. \tag{5.22}$$

We consider some particular values of A, i and j in (5.22). For $A=q^n$, $i=0$ and $j\geq 1$, f is q-ary bent if and only if the inequality (5.22) is an equality. Indeed, for $s\geq 1$, $A=q^{n+s}$, $i\geq 1$ and $j\geq 1$, f is q-ary s-plateaued if and only if the inequality (5.22) becomes an equality.

Clearly, Lemma 5.1 suggests that the sequence of the Walsh power moments of q-ary plateaued function is a simple geometric sequence (see the proof of Corollary 5.2).

Corollary 5.6. *Let $f:\mathbb{F}_q^n\to\mathbb{F}_q$ be q-ary s-plateaued. Then for every integer $i\geq 1$, $S_i(f)=q^{n(i+1)+s(i-1)}$.*

The Cauchy-Schwarz Inequality gives the following inequality, and its equality case yields characterizations of q-ary plateaued functions.

Theorem 5.6. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. Then for every integer $i \geq 1$, $S_{i+1}(f)^2 \leq S_{i+2}(f)S_i(f)$, where the equality holds for one (and hence for all) $i \geq 1$ if and only if f is q-ary plateaued.*

Proof. By Theorem 3.1, for $p_1 = p_2 = 2$, put $x_k = |\widehat{\chi_f}(\omega)|^i$ and $y_k = |\widehat{\chi_f}(\omega)|^{i+2}$ for all $\omega \in \mathbb{F}_q^n$, then we have

$$\left(\sum_{\omega\in\mathbb{F}_q^n} |\widehat{\chi_f}(\omega)|^{2i+2}\right)^2 \leq \sum_{\omega\in\mathbb{F}_q^n} |\widehat{\chi_f}(\omega)|^{2i} \sum_{\omega\in\mathbb{F}_q^n} |\widehat{\chi_f}(\omega)|^{2i+4},$$

that is, $S_{i+1}(f)^2 \leq S_i(f)S_{i+2}(f)$, where the equality holds for one (and hence for all) $i \geq 1$ if and only if for all $\omega \in \mathbb{F}_q^n$, $|\widehat{\chi_f}(\omega)|^{2i} = d\,|\widehat{\chi_f}(\omega)|^{2i+4}$ for some $d \in \mathbb{R}^+$; equivalently, for all $\omega \in \mathbb{F}_{p^n}$, $|\widehat{\chi_f}(\omega)|^2$ is either the same positive integer or 0, i.e., f is q-ary plateaued. □

Remark 5.10. Notice that Theorem 5.6 can be also derived from (5.21). The reduced discriminant of (5.21), $S_{i+1}(f)^2 - S_{i+2}(f)S_i(f) \leq 0$, with an equality if and only if f is q-ary plateaued.

The plateaued-ness of a q-ary function can be checked only by using the fourth and sixth power moments of its Walsh transform.

Theorem 5.7. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. Then, f is q-ary s-plateaued if and only if $S_2(f) = q^{3n+s}$ and $S_3(f) = q^{4n+2s}$. In fact, f is q-ary plateaued if and only if $S_2(f)^2 = q^{2n}S_3(f)$.*

Proof. Assume that f is q-ary s-plateaued. Then, the assertion directly follows from Corollary 5.6. Conversely, by (5.20) with $A = q^{n+s}$ at $i = 1$, we have

$$\sum_{\omega\in\mathbb{F}_q^n} \left(|\widehat{\chi_f}(\omega)|^2 - q^{n+s}\right)^2 |\widehat{\chi_f}(\omega)|^2 \;= S_3(f) - 2q^{n+s}S_2(f) + q^{2n+2s}S_1(f) = 0,$$

where in the second equality we used the Parseval identity. Hence, $|\widehat{\chi_f}(\omega)|^2 \in \{0, q^{n+s}\}$ for all $\omega \in \mathbb{F}_q^n$, that is, f is q-ary s-plateaued.
The second statement follows from Theorem 5.6, in the case of $i = 1$, and using the Parseval identity. □

More precisely, as in the proof of Theorem 5.6, applying the Cauchy-Schwarz Inequality for $x_k = |\widehat{\chi_f}(\omega)|$ and $y_k = |\widehat{\chi_f}(\omega)|^{2i+1}$ for all $\omega \in \mathbb{F}_q^n$, we have $S_{i+1}(f)^2 \leq S_1(f)S_{2i+1}(f)$ for $i \geq 1$, where the equality holds for one (and hence for all) $i \geq 1$ if and only if for all $\omega \in \mathbb{F}_q^n$, $|\widehat{\chi_f}(\omega)|^2 = d\,|\widehat{\chi_f}(\omega)|^{4i+2}$ for some $d \in \mathbb{R}^+$; equivalently, for all $\omega \in \mathbb{F}_{p^n}$, $|\widehat{\chi_f}(\omega)|^2$ is either the same positive integer or 0, i.e., f is q-ary plateaued. Hence this implies the following theorem in view of the Parseval identity.

Corollary 5.7. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. Then for every integer $i \geq 1$, we have*

$$S_{i+1}(f)^2 \leq q^{2n} S_{2i+1}(f),$$

where the equality holds for one (and hence for all) $i \geq 1$ if and only if f is q-ary plateaued.

The following corollary follows from Corollaries 5.6 and 5.7.

Corollary 5.8. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. Then f is q-ary s-plateaued if and only if $S_{i+1}(f) = q^{n(i+2)+si}$ and $S_{2i+1}(f) = q^{n(2i+2)+2is}$ for one (and hence for all) positive integer i.*

We now give a strong characterization of q-ary plateaued functions in terms of their second-order derivatives. To do this, we extend Theorem 5.4 (see Section 5.2) for any integer s with $0 \leq s \leq n$ as follows. For the proof of Theorem 5.8, the reader is referred to the proof of Theorem 5.4. It can be also proven without using the convolution product (see the proof of Theorem 3.6 for the p-ary case).

Theorem 5.8. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. Then, f is q-ary s-plateaued if and only if for all $x \in \mathbb{F}_q^n$,*

$$\sum_{a,b \in \mathbb{F}_q^n} \chi(\mathcal{D}_b\mathcal{D}_a f(x)) = q^{n+s}.$$

Clearly, Theorem 5.8 suggests the following result.

Corollary 5.9. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$ be q-ary s-plateaued. Then*

$$\sum_{a,b,x \in \mathbb{F}_q^n} \chi(\mathcal{D}_b\mathcal{D}_a f(x)) = q^{2n+s}.$$

The following is a direct consequence of Corollary 5.6 and Theorem 5.8.

Corollary 5.10. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. Set $\theta_f(x) = \sum_{a,b\in\mathbb{F}_q^n} \chi(\mathcal{D}_b\mathcal{D}_a f(x))$ for all $x \in \mathbb{F}_q^n$. Then, f is q-ary plateaued if and only if for all $x \in \mathbb{F}_q^n$,*

$$S_2(f) = q^{2n}\theta_f(x). \tag{5.23}$$

Proof. Assume that f is q-ary s-plateaued. Then, we have $S_2(f) = q^{3n+s}$ by Corollary 5.6, and $\theta_f(x) = q^{n+s}$ for all $x \in \mathbb{F}_q^n$ by Theorem 5.8. Hence, (5.23) holds for all $x \in \mathbb{F}_q^n$. Conversely, assume that (5.23) holds for all $x \in \mathbb{F}_q^n$, that is, $\theta_f(x) = \theta$ is constant for all $x \in \mathbb{F}_q^n$, where $\theta = q^{-2n}S_2(f)$. Thus, by Theorem 5.8, f is q-ary plateaued. □

Remark 5.11. Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. For all $x \in \mathbb{F}_q^n$, at point $(a, b) \in (\mathbb{F}_q^n)^2$, we have $\mathcal{D}_b\mathcal{D}_a f(x) = \mathcal{D}_a f(b) - \mathcal{D}_a f(x)$ because of the (bijective) change of variable $b \mapsto b - x$. Hence, the characterizations of q-ary plateaued functions by their second-order derivatives can be given by their first-order derivatives, which makes easier the check of the plateaued-ness of q-ary functions.

Theorem 5.8 has a crucial role in proving the following characterizations of q-ary plateaued functions.

Theorem 5.9. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. Then f is q-ary plateaued if and only if for all $\alpha \in \mathbb{F}_q^n \setminus \{0\}$,*

$$\sum_{\omega\in\mathbb{F}_q^n} \widehat{\chi_f}(\alpha+\omega)\overline{\widehat{\chi_f}(\omega)}\ |\widehat{\chi_f}(\omega)|^2 \ = 0. \tag{5.24}$$

Proof. For all $\alpha \in \mathbb{F}_q^n \setminus \{0\}$, the left-hand side of (5.24) is

$$\begin{aligned}
&\sum_{x,a,b,c\in\mathbb{F}_q^n} \chi(f(x) - f(a) + f(b) - f(c) - \alpha\cdot x) \sum_{\omega\in\mathbb{F}_q^n} \overline{\chi}(\omega\cdot(x-a+b-c)) \\
&= q^n \sum_{x,a,b\in\mathbb{F}_q^n} \chi(f(x) - f(a) + f(b) - f(x-a+b) - \alpha\cdot x),
\end{aligned}$$

where we used that $\sum_{\omega\in\mathbb{F}_q^n} \xi_p^{\mathrm{Tr}_p^{q^n}(-\omega(x-a+b-c))} = \begin{cases} q^n \text{ if } c = x-a+b, \\ 0 \text{ otherwise.} \end{cases}$

Hence, since $(x, a, b) \mapsto (x, x + a, x + a + b)$ is a permutation of $(\mathbb{F}_q^n)^3$, it is equal to

$$q^n \sum_{x\in\mathbb{F}_q^n} \sum_{a,b\in\mathbb{F}_q^n} \chi(\mathcal{D}_b\mathcal{D}_a f(x))\overline{\chi}(\alpha\cdot x),$$

which is the Fourier transform at $\alpha \in \mathbb{F}_q^n \setminus \{0\}$ of the function $G : \mathbb{F}_q^n \to \mathbb{C}$ defined as $G(x) := q^n \sum_{a,b \in \mathbb{F}_q^n} \chi(\mathcal{D}_b \mathcal{D}_a f(x))$ for $x \in \mathbb{F}_q^n$. By Remark 3.4, (5.24) holds for all $\alpha \in \mathbb{F}_q^n \setminus \{0\}$ if and only if G is constant; equivalently by Theorem 5.8, f is q-ary plateaued. □

Corollary 5.11. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. Then, f is q-ary plateaued if and only if for all $x \in \mathbb{F}_q^n$*

$$S_2(f) = q^n \sum_{\omega \in \mathbb{F}_q^n} \chi(f(x) - \omega \cdot x) \overline{\widehat{\chi_f}(\omega)} \, |\widehat{\chi_f}(\omega)|^2. \tag{5.25}$$

Proof. Assume that f is q-ary s-plateaued. By Corollary 5.6, $S_2(f) = q^{3n+s}$. On the other hand, for all $x \in \mathbb{F}_q^n$,

$$\begin{aligned}
&\sum_{\omega \in \mathbb{F}_q^n} \chi(f(x) - \omega \cdot x) \overline{\widehat{\chi_f}(\omega)} \, |\widehat{\chi_f}(\omega)|^2 = q^{n+s} \sum_{\omega \in \mathbb{F}_q^n} \chi(f(x) - \omega \cdot x) \overline{\widehat{\chi_f}(\omega)} \\
&= q^{n+s} \sum_{y \in \mathbb{F}_q^n} \chi(f(x) - f(y)) \sum_{\omega \in \mathbb{F}_q^n} \chi(\omega \cdot (y - x)) = q^{2n+s}
\end{aligned}$$

since $\sum_{\omega \in \mathbb{F}_q^n} \xi_p^{\mathrm{Tr}_p^{q^n}(\omega(y-x))}$ is null if $y - x \neq 0$. Hence, the assertion holds. Conversely, assume that (5.25) holds for all $x \in \mathbb{F}_q^n$, that is, the function $G : \mathbb{F}_q^n \to \mathbb{C}$ defined as

$$G(x) := \sum_{\omega \in \mathbb{F}_q^n} \chi(f(x) - \omega \cdot x) \overline{\widehat{\chi_f}(\omega)} |\widehat{\chi_f}(\omega)|^2$$

is constant for all $x \in \mathbb{F}_q^n$. The Fourier transform of G at $\alpha \in \mathbb{F}_q^n$ is given as

$$\begin{aligned}
\widehat{G}(\alpha) &= \sum_{\omega \in \mathbb{F}_q^n} \sum_{x \in \mathbb{F}_q^n} \chi(f(x) - x \cdot (\alpha + \omega)) \overline{\widehat{\chi_f}(\omega)} \, |\widehat{\chi_f}(\omega)|^2 \\
&= \sum_{\omega \in \mathbb{F}_q^n} \widehat{\chi_f}(\alpha + \omega) \overline{\widehat{\chi_f}(\omega)} \, |\widehat{\chi_f}(\omega)|^2.
\end{aligned}$$

Notice that by Remark 3.4, $\widehat{G}(\alpha) = 0$ for any $\alpha \in \mathbb{F}_q^n \setminus \{0\}$. Hence, by Theorem 5.9, f is q-ary plateaued. □

In the light of Proposition 5.6, the characterizations given in Corollaries 5.10 and 5.11 are equivalent.

The following is an immediate consequence of Theorem 5.8 and Proposition 5.6.

Corollary 5.12. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. Then, f is q-ary s-plateaued if and only if for all $x \in \mathbb{F}_q^n$*

$$\sum_{\omega \in \mathbb{F}_q^n} \chi(f(x) - \omega \cdot x)\overline{\widehat{\chi_f}(\omega)}\ |\widehat{\chi_f}(\omega)|^2 = q^{2n+s}.$$

We end this section by characterizing q-ary plateaued functions in terms of their autocorrelation functions. According to the definition of plateaued functions, f is q-ary plateaued of the amplitude μ if and only if the two functions $|\widehat{\chi_f}|^4$ and $\mu^2|\widehat{\chi_f}|^2$ are equal; equivalently, their Fourier transforms are equal by Lemma 2.4.

The Fourier transform of the function $|\widehat{\chi_f}(b)|^2 = \sum_{x,y \in \mathbb{F}_q^n} \chi(f(x) - f(y) - b \cdot (x-y))$ is given by

$$\begin{aligned} \widehat{|\widehat{\chi_f}(a)|^2} &= \sum_{b \in \mathbb{F}_q^n} |\widehat{\chi_f}(b)|^2 \overline{\chi}(b \cdot a) \\ &= \sum_{x \in \mathbb{F}_q^n} \sum_{y \in \mathbb{F}_q^n} \chi(f(x) - f(y)) \sum_{b \in \mathbb{F}_q^n} \overline{\chi}(b \cdot (x + a - y)) = q^n \overline{\Delta_f}(a) \end{aligned}$$

where in the last equality we used that $\sum_{b \in \mathbb{F}_q^n} \overline{\chi}(b \cdot (x + a - y))$ is null if $y \neq x + a$. Hence, the Fourier transform of $|\widehat{\chi_f}|^4$ is

$$\widehat{|\widehat{\chi_f}|^2|\widehat{\chi_f}|^2} = q^{-n}\left(\widehat{|\widehat{\chi_f}|^2} \otimes \widehat{|\widehat{\chi_f}|^2}\right) = q^{-n}\left(q^n\overline{\Delta_f} \otimes q^n\overline{\Delta_f}\right) = q^n\left(\overline{\Delta_f} \otimes \overline{\Delta_f}\right) \quad (5.26)$$

where in the first equality we used Theorem 2.1. Then we conclude the following.

Theorem 5.10. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. Then, f is q-ary plateaued of the amplitude μ if and only if for all $x \in \mathbb{F}_q^n$*

$$\sum_{a \in \mathbb{F}_q^n} \Delta_f(a)\Delta_f(x - a) = \mu^2 \Delta_f(x). \quad (5.27)$$

Proof. As we said above, f is q-ary plateaued of the amplitude μ if and only if $|\widehat{\chi_f}|^4$ and $\mu^2|\widehat{\chi_f}|^2$ are equal; equivalently by Lemma 2.4, $\overline{\Delta_f} \otimes \overline{\Delta_f} = \mu^2\overline{\Delta_f}$; equivalently by Proposition 2.2 (*iv*), $(\Delta_f \otimes \Delta_f)(x) = \mu^2\Delta_f(x)$ for all $x \in \mathbb{F}_q^n$. The proof follows from Definition 2.4. □

The Fourier transform of $|\widehat{\chi_f}|^6$ is given by

$$\widehat{|\widehat{\chi_f}|^2|\widehat{\chi_f}|^4} = q^{-n}\left(\widehat{|\widehat{\chi_f}|^2} \otimes \widehat{|\widehat{\chi_f}|^4}\right) = q^n\left(\overline{\Delta_f} \otimes \overline{\Delta_f} \otimes \overline{\Delta_f}\right),$$

where we used Theorem 2.1 in the first equality and (5.26) in the last equality. Then, we say that f is plateaued of the amplitude μ if and only if $|\widehat{\chi_f}|^6$ and $\mu^2|\widehat{\chi_f}|^4$ are equal, by Lemma 2.4 their Fourier transforms are equal, that is, $\Delta_f \otimes \Delta_f \otimes \Delta_f = \mu^2 \Delta_f \otimes \Delta_f$. This proves the following.

Corollary 5.13. *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. Then, f is q-ary plateaued of the amplitude μ if and only if for all $x \in \mathbb{F}_q^n$*

$$\sum_{a,b \in \mathbb{F}_q^n} \Delta_f(a)\Delta_f(b)\Delta_f(x-a-b) = \mu^2 \sum_{c \in \mathbb{F}_q^n} \Delta_f(c)\Delta_f(x-c).$$

5.4 q-Ary Plateaued-type Functions over $\mathbb{F}_q$

In this section, we define a Walsh type transform of a q-ary function f from $\mathbb{F}_q^n$ to $\mathbb{F}_q$ by using a primitive q-th root of unity instead of a primitive p-th root of unity. We introduce the notion of q-ary plateaued type functions with respect to its Walsh type transform.

Let $\mathbb{F}_q$ be the finite field with q elements and ζ be a generator of $\mathbb{F}_q^\star$, i.e., $\mathbb{F}_q^\star = \langle \zeta \rangle$, where $q = p^m$. Then we have $\mathbb{F}_q = \{0, \zeta, \zeta^2, \ldots, \zeta^{q-1}\}$. Let $\xi_q = e^{\frac{2\pi\sqrt{-1}}{q}}$ be *a primitive q-th root of unity* in $\mathbb{C}$. Let ψ be the map from $\mathbb{F}_q$ to $\mathbb{C}$ (depending on the choice of ζ and ξ_q) given by

$$\psi(a) = \xi_q^a := \begin{cases} 1 & \text{if} \quad a = 0, \\ \xi_q^r & \text{if} \quad a = \zeta^r \quad \text{where} \quad 1 \le r \le q-1. \end{cases}$$

This map defines the a-th power of ξ_q in $\mathbb{C}$ for $a \in \mathbb{F}_q$. For example, let $\zeta \in \mathbb{F}_4$ be a generator of $\mathbb{F}_4^\star$. Then it is a root of primitive polynomial $x^2 + x + 1$ over $\mathbb{F}_2$. We have $\mathbb{F}_4 = \{0, 1, \zeta, \zeta + 1\}$ and $\mathbb{F}_4^\star = \langle \zeta \rangle = \{\zeta, \zeta^2, \zeta^3\}$. For $a \in \mathbb{F}_4$, the a-th powers of ξ_4 in $\mathbb{C}$ are given by

$$\xi_4^0 = 1, \quad \xi_4^1 = \xi_4^3, \quad \xi_4^\zeta = \xi_4^1 \quad \text{and} \quad \xi_4^{\zeta+1} = \xi_4^2.$$

Thus, we can define a Walsh type transform of a q-ary function $f : \mathbb{F}_q^n \to \mathbb{F}_q$ by using ξ_q instead of ξ_p. We denote by χ_f the complex valued function from $\mathbb{F}_q^n$ to $\mathbb{C}$ of f defined as $\chi_f(x) = \xi_q^{f(x)}$ for all $x \in \mathbb{F}_q^n$. A *Walsh type transform* of f at $\omega \in \mathbb{F}_q^n$ with

respect to ξ_q is defined by

$$\begin{aligned}\widehat{\chi_f} :&\mathbb{F}_q^n \to \mathbb{C}\\ &\omega \longmapsto \widehat{\chi_f}(\omega) = \sum_{x\in\mathbb{F}_q^n} \chi_f(x)\xi_q^{-\omega\cdot x},\end{aligned}$$

where " $\cdot$ " denotes an inner product in $\mathbb{F}_q^n$ over $\mathbb{F}_q$. Therefore, we have a Walsh type transform of f with ξ_q instead of ξ_p. This approach allows us to define the notion of q-ary plateaued type functions over $\mathbb{F}_q$ depending on ξ_q. A vectorial p-ary plateaued function f from $\mathbb{F}_{p^{mn}}$ to $\mathbb{F}_{p^m}$ with the Walsh transform of its component functions does not correspond to q-ary plateaued f from $\mathbb{F}_q^n$ to $\mathbb{F}_q$ with its Walsh type transform. Thus, we can introduce a such function f, called *q-ary plateaued type function*, with respect to the Walsh type transform.

Definition 5.3. Let f be a function from $\mathbb{F}_q^n$ to $\mathbb{F}_q$ and s be an integer with $0 \leq s \leq n$. Then, f is called *q-ary plateaued type* if its absolute Walsh transform takes only one nonzero value (also possibly the value 0). In other words, f is said to be *q-ary s-plateaued type* if $|\widehat{\chi_f}(\omega)|^2 \in \{0, q^{n+s}\}$ for all $\omega \in \mathbb{F}_q^n$, and f is said to be *q-ary bent type* if $|\widehat{\chi_f}(\omega)|^2 = q^n$ for all $\omega \in \mathbb{F}_q^n$.

CHAPTER 6

LINEAR CODES FROM WEAKLY REGULAR PLATEAUED FUNCTIONS AND THEIR SECRET SHARING SCHEMES

Linear error correcting codes have many applications in consumer electronics, secret sharing schemes, authentication codes, communication, data storage system, association schemes, and strongly regular graphs. The construction of these codes has been widely studied by a large number of researchers. There are several methods to construct linear codes, one of which is based on functions over finite fields. For example, bent functions (mostly, quadratic and weakly regular bent functions) have been extensively used to construct these codes. Very recently, Mesnager [58] has constructed a new family of three-weight linear codes from weakly regular bent functions in arbitrary characteristic based on the first generic construction. Within this framework, the main purpose of this chapter is to construct linear codes with few weights from plateaued functions and to analyze the constructed codes for the secret sharing schemes in arbitrary characteristic.

In this chapter, we first introduce the notion of (non)-weakly regular plateaued functions and then provide the first secondary constructions of these functions in odd characteristic. We next construct new classes of three-weight linear p-ary (resp. binary) codes from weakly regular p-ary plateaued (resp. plateaued Boolean) functions based on the first generic construction. We also determine the weight distributions of the constructed linear codes. We finally investigate the access structures of the secret sharing schemes based on the dual codes of the constructed linear codes.

The results of this chapter appear in [60, 61].

6.1 On the (Non)-Weakly Regular Plateaued Functions over Finite Fields of Odd Characteristic

In this section, we first introduce the notion of (non)-weakly regular plateaued functions over finite fields of odd characteristic, and then give the first secondary constructions of these functions.

6.1.1 The Notion of (Non)-Weakly Regular Plateaued p-Ary Functions

After introducing the notion of (non)-weakly regular plateaued functions, we give some concrete examples and properties of these functions.

We begin by recalling the notion of (non)-weakly regular bent functions in odd characteristic (see, e.g., [36]). A function $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is p-ary bent if $|\widehat{\chi_f}(\omega)|^2 = p^n$ for every $\omega \in \mathbb{F}_{p^n}$. A p-ary bent function f is called *regular* if $\widehat{\chi_f}(\omega) = p^{\frac{n}{2}} \xi_p^{f^*(\omega)}$ for every $\omega \in \mathbb{F}_{p^n}$, and called *weakly regular* if there exists a complex number u having unit magnitude (in fact, $|u| = 1$ and u does not depend on ω) such that $\widehat{\chi_f}(\omega) = up^{\frac{n}{2}} \xi_p^{f^*(\omega)}$ for every $\omega \in \mathbb{F}_{p^n}$, where f^* is the dual of f; otherwise, f is called *non-weakly regular* bent. It is worth noting that, for a weakly regular bent function, the constant u (defined above) can only be equal to ± 1 or $\pm i$. By [36, 37], a weakly regular bent function f satisfies

$$\widehat{\chi_f}(\omega) = \epsilon \sqrt{p^*}^n \xi_p^{f^*(\omega)},$$

where $\epsilon = \pm 1$ is the sign of $\widehat{\chi_f}$, p^* denotes $\left(\frac{-1}{p}\right) p$ and f^* is the dual of f. In fact, the Walsh transform coefficients of bent f satisfy

$$\widehat{\chi_f}(\omega) = \begin{cases} \pm p^{\frac{n}{2}} \xi_p^{f^*(\omega)}, & \text{if } n \text{ is even or } n \text{ is odd and } p \equiv 1 \pmod 4, \\ \pm i p^{\frac{n}{2}} \xi_p^{f^*(\omega)}, & \text{if } n \text{ is odd and } p \equiv 3 \pmod 4, \end{cases}$$

where i is a complex primitive 4-th root of unity and f^* is the dual of f. Hence, the regular bent functions can only be found for even n and for odd n with $p \equiv 1 \pmod 4$. Table 6.1 lists all known weakly regular bent functions over $\mathbb{F}_{p^n}$.

Below we introduce the notion of (non)-weakly regular plateaued functions in odd characteristic. We first recall that f is said to be p-ary s-plateaued if $|\widehat{\chi_f}(\omega)|^2 \in \{0, p^{n+s}\}$ for every $\omega \in \mathbb{F}_{p^n}$, where s is an integer with $0 \leq s \leq n$. The Walsh support

Weakly regular bent functions	n	p
$\sum_{i=0}^{\lfloor n/2 \rfloor} \mathrm{Tr}_p^{p^n}(a_i x^{p^{i+1}})$	arbitrary	arbitrary
$\sum_{i=0}^{p^k-1} \mathrm{Tr}_p^{p^n}(a_i x^{i(p^k-1)}) + \mathrm{Tr}_p^{p^n}(\delta x^{\frac{p^n-1}{e}}), e\|p^k+1$	$n=2k$	arbitrary
$\mathrm{Tr}_p^{p^n}(ax^{\frac{3^n-1}{4}+3^k+1})$	$n=2k$	$p=3$
$\mathrm{Tr}_p^{p^n}(x^{p^{3k}+p^{2k}-p^k+1}+x^2)$	$n=4k$	arbitrary
$\mathrm{Tr}_p^{p^n}(ax^{\frac{3^i+1}{2}})$; i odd, $\gcd(i,n)=1$	arbitrary	$p=3$

Table 6.1: Known weakly regular bent functions over $\mathbb{F}_{p^n}$, p is odd

of p-ary s-plateaued f is defined by $\mathrm{Supp}(\widehat{\chi_f}) = \{\omega \in \mathbb{F}_{p^n} : |\widehat{\chi_f}(\omega)|^2 = p^{n+s}\}$. In 2016, Hyun et al. [43] have shown that the Walsh transform coefficients of p-ary s-plateaued f satisfy

$$\widehat{\chi_f}(\omega) = \begin{cases} \pm p^{\frac{n+s}{2}} \xi_p^{g(\omega)}, 0 & \text{if } n+s \text{ is even or} \\ & n+s \text{ is odd and } p \equiv 1 \pmod 4, \\ \pm i p^{\frac{n+s}{2}} \xi_p^{g(\omega)}, 0 & \text{if } n+s \text{ is odd and } p \equiv 3 \pmod 4, \end{cases} \tag{6.1}$$

where i is a complex primitive 4-th root of unity and g is a p-ary function over $\mathbb{F}_{p^n}$ with $g(\omega) = 0$ for all $\omega \notin \mathrm{Supp}(\widehat{\chi_f})$. It is worth noting that by the definition of $g : \mathbb{F}_{p^n} \to \mathbb{F}_p$, it can be regarded as a mapping from $\mathrm{Supp}(\widehat{\chi_f})$ to $\mathbb{F}_p$ such that $g(\omega) = 0$ for all $\omega \notin \mathrm{Supp}(\widehat{\chi_f})$. Clearly, for all $\omega \in \mathrm{Supp}(\widehat{\chi_f})$,

$$\widehat{\chi_f}(\omega) \in \left\{ \pm p^{\frac{n+s}{2}} \xi_p^{g(\omega)}, \pm i p^{\frac{n+s}{2}} \xi_p^{g(\omega)} \right\}.$$

We now introduce the notion of (non)-weakly regular plateaued functions in odd characteristic, which covers a non-trivial subclass of the class of plateaued functions.

Definition 6.1. Let p be an odd prime and $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be a p-ary s-plateaued function, where s is an integer with $0 \le s \le n$. Then, f is called *weakly regular p-ary s-plateaued* if there exists a complex number u having unit magnitude (in fact, $|u| = 1$ and u does not depend on ω) such that

$$\widehat{\chi_f}(\omega) \in \left\{ 0, u p^{\frac{n+s}{2}} \xi_p^{g(\omega)} \right\} \tag{6.2}$$

for all $\omega \in \mathbb{F}_{p^n}$, where g is a p-ary function over $\mathbb{F}_{p^n}$ with $g(\omega) = 0$ for all $\omega \notin \mathrm{Supp}(\widehat{\chi_f})$; otherwise, f is called *non-weakly regular p-ary s-plateaued*. In particular, weakly regular p-ary s-plateaued f is called *regular p-ary s-plateaued* if $u = 1$ in (6.2).

Since $\widehat{\chi_f}(\omega) = 0$ for $\omega \notin \mathrm{Supp}(\widehat{\chi_f})$, it is safe to say that f is regular s-plateaued if $\widehat{\chi_f}(\omega) = p^{\frac{n+s}{2}}\xi_p^{g(\omega)}$ for all $\omega \in \mathrm{Supp}(\widehat{\chi_f})$, and f is weakly regular s-plateaued if there exists a complex number u having unit magnitude (in fact, u can only be equal to ± 1 or $\pm i$ and u does not depend on ω) such that

$$\widehat{\chi_f}(\omega) = up^{\frac{n+s}{2}}\xi_p^{g(\omega)} \tag{6.3}$$

for all $\omega \in \mathrm{Supp}(\widehat{\chi_f})$, where g is a p-ary function over $\mathrm{Supp}(\widehat{\chi_f})$. By (6.1), regular s-plateaued functions can only exist for even $n+s$ and for odd $n+s$ with $p \equiv 1 \pmod 4$.

We can derive from (6.3) the following lemma, which has a significant role in finding the Hamming weights of the codewords of a linear code (see Section 6.3).

Lemma 6.1. *Let p be an odd prime and let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be weakly regular s-plateaued. For all $\omega \in \mathrm{Supp}(\widehat{\chi_f})$,*

$$\widehat{\chi_f}(\omega) = \epsilon\sqrt{p^*}^{n+s}\xi_p^{g(\omega)},$$

where $\epsilon = \pm 1$ is the sign of $\widehat{\chi_f}$, p^* denotes $\left(\frac{-1}{p}\right)p$ and g is a p-ary function over $\mathrm{Supp}(\widehat{\chi_f})$.

Proof. The critical point of this proof is the fact that u does not depend on $\omega \in \mathrm{Supp}(\widehat{\chi_f})$ in (6.3). In view of (6.1), there are two cases:

- Assume $n+s$ is even or $n+s$ is odd and $p \equiv 1 \pmod 4$. Clearly by (2.5), we have $\left(\frac{-1}{p}\right)^{n+s} = 1$ and by (6.1), we have $u = \pm 1$ in (6.3). Hence, $\epsilon\sqrt{p^*}^{n+s} = \epsilon\sqrt{1}\sqrt{p}^{n+s} = u\sqrt{p}^{n+s}$, where $\epsilon = \pm 1$.
- Assume $n+s$ is odd and $p \equiv 3 \pmod 4$. Clearly by (2.5), we have $\left(\frac{-1}{p}\right) = -1$ and by (6.1), we have $u = \epsilon i$ in (6.3), where $\epsilon = \pm 1$. Hence,

$$\epsilon\sqrt{p^*}^{n+s} = \epsilon\sqrt{-1}^{n+s}\sqrt{p}^{n+s} = \epsilon i^{n+s}\sqrt{p}^{n+s} = u\sqrt{p}^{n+s}.$$

The assertion follows from (6.3). □

Lemma 6.2. *Let p be an odd prime and let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. The notion of weakly regular 0-plateaued functions coincides with the notion of weakly regular bent functions.*

Proof. Assume that f is weakly regular 0-plateaued. Then, there exists a complex number u with $|u| = 1$ such that for all $\omega \in \mathbb{F}_{p^n}$, $\widehat{\chi_f}(\omega) \in \{0, up^{\frac{n}{2}}\xi_p^{g(\omega)}\}$, where g is a p-ary function over $\mathbb{F}_{p^n}$ and u does not depend on ω. By the Parseval identity, since $|z|^2 = z\overline{z}$ for $z \in \mathbb{C}$, we have

$$\begin{aligned} p^{2n} &= \sum_{\omega\in\mathbb{F}_{p^n}} |\widehat{\chi}_f(\omega)|^2 = \sum_{\omega\in \mathrm{Supp}(\widehat{\chi_f})} |up^{\frac{n}{2}}\xi_p^{g(\omega)}|^2 = \sum_{\omega\in \mathrm{Supp}(\widehat{\chi_f})} p^n|u|^2\xi_p^{g(\omega)}\overline{\xi_p^{g(\omega)}} \\ &= \sum_{\omega\in \mathrm{Supp}(\widehat{\chi_f})} p^n\xi_p^0 = \sum_{\omega\in \mathrm{Supp}(\widehat{\chi_f})} p^n, \end{aligned}$$

which implies $\#\mathrm{Supp}(\widehat{\chi_f}) = p^n$. Hence, $\widehat{\chi_f}(\omega) = up^{\frac{n}{2}}\xi_p^{g(\omega)}$ for all $\omega \in \mathbb{F}_{p^n}$, where $|u| = 1$ and g is a p-ary function over $\mathbb{F}_{p^n}$, i.e., f is weakly regular bent. □

By MAGMA in [5], we obtain several concrete examples of a regular plateaued function.

Example 6.1. *The function* $f(x) = \mathrm{Tr}_3^{3^3}(\zeta^5x^{11} + \zeta^{20}x^5 + \zeta^{11}x^4 + \zeta^2x^3 + \zeta x^2)$*, where* $\mathbb{F}_{3^3}^\star = \langle\zeta\rangle$ *with* $\zeta^3+2\zeta+1 = 0$*, is regular* 3*-ary* 1*-plateaued with* $\widehat{\chi_f}(\omega) \in \{0, 9\xi_3^{g(\omega)}\}$ *for all* $\omega \in \mathbb{F}_{3^3}$*, where* g *is an unbalanced* 3*-ary function. Indeed, it is easily seen that* $\mathrm{Supp}(\widehat{\chi_f}) = \{0, \zeta^4, \zeta^6, \zeta^9, \zeta^{16}, \zeta^{17}, \zeta^{21}, \zeta^{24}, \zeta^{25}\}$ *and*

$$\begin{aligned}
\widehat{\chi_f}(0) &= 9\xi_3^{g(0)} = 9 && \textit{where} \quad g(0) &= 0,\\
\widehat{\chi_f}(\zeta^4) &= 9\xi_3^{g(\zeta^4)} = 9 && \textit{where} \quad g(\zeta^4) &= 0,\\
\widehat{\chi_f}(\zeta^6) &= 9\xi_3^{g(\zeta^6)} = 9\xi_3 && \textit{where} \quad g(\zeta^6) &= 1,\\
\widehat{\chi_f}(\zeta^9) &= 9\xi_3^{g(\zeta^9)} = 9\xi_3 && \textit{where} \quad g(\zeta^9) &= 1,\\
\widehat{\chi_f}(\zeta^{16}) &= 9\xi_3^{g(\zeta^{16})} = 9 && \textit{where} \quad g(\zeta^{16}) &= 0,\\
\widehat{\chi_f}(\zeta^{17}) &= 9\xi_3^{g(\zeta^{17})} = 9 && \textit{where} \quad g(\zeta^{17}) &= 0,\\
\widehat{\chi_f}(\zeta^{21}) &= 9\xi_3^{g(\zeta^{21})} = 9 && \textit{where} \quad g(\zeta^{21}) &= 0,\\
\widehat{\chi_f}(\zeta^{24}) &= 9\xi_3^{g(\zeta^{24})} = -9\xi_3 - 9 && \textit{where} \quad g(\zeta^{24}) &= 2,\\
\widehat{\chi_f}(\zeta^{25}) &= 9\xi_3^{g(\zeta^{25})} = -9\xi_3 - 9 && \textit{where} \quad g(\zeta^{25}) &= 2.
\end{aligned}$$

By MAGMA in [5], we obtain several concrete examples of a weakly regular plateaued function.

Example 6.2. *The function* $f(x) = \mathrm{Tr}_3^{3^3}(\zeta x^{13} + \zeta^7x^4 + \zeta^7x^3 + \zeta x^2)$*, where* $\mathbb{F}_{3^3}^\star = \langle\zeta\rangle$ *with* $\zeta^3 + 2\zeta + 1 = 0$*, is weakly regular* 3*-ary* 1*-plateaued with* $\widehat{\chi_f}(\omega) \in \{0, -9\xi_3^{g(\omega)}\}$ *for all* $\omega \in \mathbb{F}_{3^3}$*, where* g *is an unbalanced* 3*-ary function. We have* $\mathrm{Supp}(\widehat{\chi_f}) =$

$\{0, \zeta^6, \zeta^{10}, \zeta^{11}, 2, \zeta^{19}, \zeta^{23}, \zeta^{24}, 1\}$ *and*

$$\begin{array}{llllll}
\widehat{\chi_f}(0) & = -9\xi_3 & \textit{where} & g(0) & = 1, \\
\widehat{\chi_f}(\zeta^6) & = -9\xi_3 & \textit{where} & g(\zeta^6) & = 1, \\
\widehat{\chi_f}(\zeta^{10}) & = -9\xi_3 & \textit{where} & g(\zeta^{10}) & = 1, \\
\widehat{\chi_f}(\zeta^{11}) & = -9 & \textit{where} & g(\zeta^{11}) & = 0, \\
\widehat{\chi_f}(2) & = 9\xi_3 + 9 & \textit{where} & g(2) & = 2, \\
\widehat{\chi_f}(\zeta^{19}) & = 9\xi_3 + 9 & \textit{where} & g(\zeta^{19}) & = 2, \\
\widehat{\chi_f}(\zeta^{23}) & = 9\xi_3 + 9 & \textit{where} & g(\zeta^{23}) & = 2, \\
\widehat{\chi_f}(\zeta^{24}) & = -9\xi_3 & \textit{where} & g(\zeta^{24}) & = 1, \\
\widehat{\chi_f}(1) & = 9\xi_3 + 9 & \textit{where} & g(1) & = 2.
\end{array}$$

The following lemma has a crucial role in determining the weight distributions of the constructed linear codes (see Section 6.3). Recall that the inverse Walsh transform of f is defined by:

$$\xi_p^{f(x)} = \frac{1}{p^n} \sum_{\omega \in \mathbb{F}_{p^n}} \widehat{\chi_f}(\omega) \xi_p^{\mathrm{Tr}_p^{p^n}(\omega x)}. \tag{6.4}$$

Lemma 6.3. *Let p be an odd prime and $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be weakly regular s-plateaued. Then for $x \in \mathbb{F}_{p^n}$,*

$$\sum_{\omega \in \mathrm{Supp}(\widehat{\chi_f})} \xi_p^{g(\omega) + \mathrm{Tr}_p^{p^n}(\omega x)} = u^{-1} p^{\frac{n-s}{2}} \xi_p^{f(x)},$$

where $|u| = 1$ and g is a p-ary function over $\mathbb{F}_{p^n}$ with $g(\omega) = 0$ for all $\omega \in \mathbb{F}_{p^n} \setminus \mathrm{Supp}(\widehat{\chi_f})$.

Proof. Since f is weakly regular s-plateaued, for all $\omega \in \mathrm{Supp}(\widehat{\chi_f})$ we have $\widehat{\chi_f}(\omega) = up^{\frac{n+s}{2}} \xi_p^{g(\omega)}$, where $|u| = 1$ and g is a p-ary function over $\mathbb{F}_{p^n}$ with $g(\omega) = 0$ for all $\omega \in \mathbb{F}_{p^n} \setminus \mathrm{Supp}(\widehat{\chi_f})$. By the inverse Walsh transform in (6.4), we have

$$\begin{aligned}
u^{-1} p^{\frac{n+s}{2}} \xi_p^{f(x)} &= u^{-1} p^{\frac{n+s}{2}} \frac{1}{p^n} \sum_{\omega \in \mathbb{F}_{p^n}} \widehat{\chi_f}(\omega) \xi_p^{\mathrm{Tr}_p^{p^n}(\omega x)} \\
&= u^{-1} p^{\frac{n+s}{2}} \frac{1}{p^n} \sum_{\omega \in \mathrm{Supp}(\widehat{\chi_f})} up^{\frac{n+s}{2}} \xi_p^{g(\omega)} \xi_p^{\mathrm{Tr}_p^{p^n}(\omega x)} \\
&= p^s \sum_{\omega \in \mathrm{Supp}(\widehat{\chi_f})} \xi_p^{g(\omega) + \mathrm{Tr}_p^{p^n}(\omega x)},
\end{aligned}$$

where we used in the second equality that $\widehat{\chi_f}(\omega) = 0$ for all $\omega \in \mathbb{F}_{p^n} \setminus \mathrm{Supp}(\widehat{\chi_f})$. □

Recall that constructions from "scratch" are called primary. On the contrary, *secondary constructions* use already constructed functions to build new ones.

6.1.2 Secondary Constructions of (Non)-Weakly Regular Plateaued p-Ary Functions

This section presents the first secondary constructions of plateaued p-ary functions. We shall construct new (non)-weakly regular plateaued functions over finite fields of odd characteristic.

Direct Sum of Plateaued p-Ary Functions. The direct sum construction is the first secondary construction for Boolean bent functions given by Dillon [30] and Rothaus [72]. Such a construction has been extended first by Tan et al. [75] for p-ary bent functions and then by Carlet [15] for Boolean plateaued functions.

In the following, we give the concept of the so-called direct sum of p-ary functions.

Definition 6.2. Let p be an odd prime and both m and n be positive integers. Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ and $g : \mathbb{F}_{p^m} \to \mathbb{F}_p$. Then the direct sum of f and g is the map h from $\mathbb{F}_{p^n} \times \mathbb{F}_{p^m}$ to $\mathbb{F}_p$ defined as $h(x, y) = f(x) + g(y)$ for $x \in \mathbb{F}_{p^n}$ and $y \in \mathbb{F}_{p^m}$.

Now, we shall use the direct sum to construct new (non)-weakly regular plateaued p-ary functions over a larger field from two given ones over smaller fields. But above, we emphasize that the Walsh transform of a function derived from the direct sum can be easily expressed. Indeed, for $(a, b) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^m}$, it can be directly seen that

$$\begin{aligned} \widehat{\chi_h}(a,b) &= \sum_{x\in\mathbb{F}_{p^n}, y\in\mathbb{F}_{p^m}} {\xi_p}^{h(x,y)-a\cdot x-b\cdot y} = \sum_{x\in\mathbb{F}_{p^n}} {\xi_p}^{f(x)-a\cdot x} \sum_{y\in\mathbb{F}_{p^n}} {\xi_p}^{f(y)-b\cdot y} \\ &= \widehat{\chi_f}(a)\widehat{\chi_g}(b), \end{aligned} \tag{6.5}$$

where an inner product $(a, b) \cdot (x, y)$ in $\mathbb{F}_{p^n} \times \mathbb{F}_{p^m}$ is defined as the sum of the inner products $a \cdot x$ in $\mathbb{F}_{p^n}$ and $b \cdot y$ in $\mathbb{F}_{p^m}$.

Theorem 6.1. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be s_1-plateaued and $g : \mathbb{F}_{p^m} \to \mathbb{F}_p$ be s_2-plateaued, where $0 \le s_1 \le n$ and $0 \le s_2 \le m$. Let h be the direct sum of f and g from $\mathbb{F}_{p^{n+m}}$ to $\mathbb{F}_p$. Then, h is $(s_1 + s_2)$-plateaued.*

Proof. We first make a preliminary observation. It can be easily checked that we have $\mathrm{Supp}(\widehat{\chi_h}) = \mathrm{Supp}(\widehat{\chi_f}) \times \mathrm{Supp}(\widehat{\chi_g})$. Namely, for $(a,b) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^m}$, we have that $(a,b) \in \mathrm{Supp}(\widehat{\chi_h})$ if and only if $a \in \mathrm{Supp}(\widehat{\chi_f})$ and $b \in \mathrm{Supp}(\widehat{\chi_g})$. Now for all $(a,b) \in \mathrm{Supp}(\widehat{\chi_h})$, we have $a \in \mathrm{Supp}(\widehat{\chi_f})$ and $b \in \mathrm{Supp}(\widehat{\chi_g})$, and hence by (6.5),

$$|\widehat{\chi_h}(a,b)|^2 = |\widehat{\chi_f}(a)\widehat{\chi_g}(b)|^2 = |\widehat{\chi_f}(a)|^2|\widehat{\chi_g}(b)|^2 = p^{n+m+s_1+s_2},$$

which completes the proof. □

Remark 6.1. Note that in this subsection we use the notation f' to denote a p-ary function g over $\mathrm{Supp}(\widehat{\chi_f})$ in (6.3) in the Walsh spectrum of plateaued f.

The following proposition shows that the direct sum of a non-weakly regular plateaued function and a weakly regular plateaued function is non-weakly regular plateaued.

Proposition 6.1. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be non-weakly regular s_1-plateaued and $g : \mathbb{F}_{p^m} \to \mathbb{F}_p$ be weakly regular s_2-plateaued. Then, $h : \mathbb{F}_{p^{n+m}} \to \mathbb{F}_p$ is non-weakly regular (s_1+s_2)-plateaued.*

Proof. Since f is non-weakly regular s_1-plateaued, for all $a \in \mathrm{Supp}(\widehat{\chi_f})$, we have $\widehat{\chi_f}(a) = u_a p^{\frac{n+s_1}{2}} \xi_p^{f'(a)}$ where $|u_a| = 1$ and f' is a p-ary function over $\mathrm{Supp}(\widehat{\chi_f})$. Since g is weakly regular s_2-plateaued, for all $b \in \mathrm{Supp}(\widehat{\chi_g})$, we have $\widehat{\chi_g}(b) = up^{\frac{m+s_2}{2}} \xi_p^{g'(b)}$ where $|u| = 1$ and g' is a p-ary function over $\mathrm{Supp}(\widehat{\chi_g})$. Hence, by (6.5) and the above discussion, for all $(a,b) \in \mathrm{Supp}(\widehat{\chi_h})$, we have

$$\widehat{\chi_h}(a,b) = \widehat{\chi_f}(a)\widehat{\chi_g}(b) = u_{a,b} p^{\frac{n+m+s_1+s_2}{2}} \xi_p^{h'(a,b)}$$

where $u_{a,b} = u_a u$ (in fact, $|u_{a,b}| = 1$ and $u_{a,b}$ depends on $(a,b) \in \mathrm{Supp}(\widehat{\chi_h})$) and $h'(a,b) = f'(a) + g'(b)$ is a p-ary function over $\mathrm{Supp}(\widehat{\chi_h})$. Hence, h is a non-weakly regular (s_1+s_2)-plateaued function over $\mathbb{F}_{p^{n+m}}$. □

The following proposition shows that the direct sum of a (weakly) regular function and a weakly regular (but not regular) function is weakly regular (but not regular).

Proposition 6.2. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be (weakly) regular s_1-plateaued and $g : \mathbb{F}_{p^m} \to \mathbb{F}_p$ be weakly regular (but not regular) s_2-plateaued. Then, $h : \mathbb{F}_{p^{n+m}} \to \mathbb{F}_p$ is a weakly regular (s_1+s_2)-plateaued (but not regular) function.*

Proof. As in the proof of Proposition 6.1, for all $(a,b) \in \mathrm{Supp}(\widehat{\chi_h})$, we have

$$\widehat{\chi_h}(a,b) = up^{\frac{n+m+s_1+s_2}{2}} \xi_p^{h'(a,b)}$$

where $|u| = 1$, (in fact, $u \in \{-1, \pm i\}$ does not depend on $(a,b) \in \mathrm{Supp}(\widehat{\chi_h})$) and $h'(a,b) = f'(a)+g'(b)$ is a p-ary function over $\mathrm{Supp}(\widehat{\chi_h})$. The proof is complete. □

As observed in Propositions 6.1 and 6.2, one can construct new (non)-weakly regular plateaued functions over a larger field from given ones over smaller fields.

Semi-Direct Sum of Plateaued p-Ary Functions. As an extension of the direct sum construction, the semi-direct sum construction was proposed for bent functions in [24]. This is the following.

Definition 6.3. [24] Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$, $g : \mathbb{F}_{p^m} \to \mathbb{F}_p$ and $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ be functions. Then, the semi-direct sum $h : \mathbb{F}_{p^n} \times \mathbb{F}_{p^m} \to \mathbb{F}_p$ of f and g is defined as $h(x,y) = f(x) + g(y + F(x))$.

Below, we present the expression of the Walsh transform of the semi-direct sum of two p-ary functions.

Proposition 6.3. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$, $g : \mathbb{F}_{p^m} \to \mathbb{F}_p$ and $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ be functions. Then for $(a,b) \in \mathbb{F}_{p^{n+m}}$, the Walsh transform of the semi-direct sum $h : \mathbb{F}_{p^n} \times \mathbb{F}_{p^m} \to \mathbb{F}_p$ of f and g defined as $h(x,y) = f(x) + g(y + F(x))$ is given by*

$$\widehat{\chi_h}(a,b) = \widehat{\chi_{F_b}}(a)\widehat{\chi_g}(b),$$

where F_b is the map from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$ defined as $F_b(x) = f(x) + b \cdot F(x)$ for all $b \in \mathrm{Supp}(\widehat{\chi_g})$ and F_b is the zero function for all $b \notin \mathrm{Supp}(\widehat{\chi_g})$.

Remark 6.2. We have that $(a,b) \in \mathrm{Supp}(\widehat{\chi_h})$ if and only if $a \in \mathrm{Supp}(\widehat{\chi_{F_b}})$ and $b \in \mathrm{Supp}(\widehat{\chi_g})$.

In the following, we show that the semi-direct sum construction can be used to design plateaued functions in arbitrary characteristic.

Theorem 6.2. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be s_1-plateaued and let $g : \mathbb{F}_{p^m} \to \mathbb{F}_p$ be s_2-plateaued. Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ and let h be the semi-direct sum of f and g. Let F_b be as in Proposition 6.3. Then, h is $(s_1 + s_2)$-plateaued if and only if F_b is s_1-plateaued for all $b \in \mathrm{Supp}(\widehat{\chi_g})$.*

Proof. Since g is s_2-plateaued, we have $|\widehat{\chi_g}(b)|^2 = p^{m+s_2}$ for all $b \in \mathrm{Supp}(\widehat{\chi_g})$. Then by Proposition 6.3, $|\widehat{\chi_{F_b}}(a)|^2 = p^{n+s_1}$ for all $a \in \mathrm{Supp}(\widehat{\chi_{F_b}})$, i.e., F_b is s_1-plateaued for all $b \in \mathrm{Supp}(\widehat{\chi_g})$ if and only if

$$|\widehat{\chi_h}(a,b)|^2 = |\widehat{\chi_{F_b}}(a)\widehat{\chi_g}(b)|^2 = |\widehat{\chi_{F_b}}(a)|^2|\widehat{\chi_g}(b)|^2 = p^{n+m+s_1+s_2}$$

for all $(a,b) \in \mathrm{Supp}(\widehat{\chi_h})$, i.e., h is (s_1+s_2)-plateaued over $\mathbb{F}_{p^{n+m}}$. The proof is complete. □

Below, we construct new (non)-weakly regular plateaued functions over a larger field from given ones over smaller fields.

Corollary 6.1. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be weakly regular s_1-plateaued and let $g : \mathbb{F}_{p^m} \to \mathbb{F}_p$ be weakly regular s_2-plateaued. Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ and let h be the semi-direct sum of f and g. Let F_b be as in Proposition 6.3. Then, h is non-weakly regular (s_1+s_2)-plateaued if and only if F_b is (non)-weakly regular s_1-plateaued for all $b \in \mathrm{Supp}(\widehat{\chi_g})$.*

Proof. Since g is weakly regular s_2-plateaued, for all $b \in \mathrm{Supp}(\widehat{\chi_g})$, we have $\widehat{\chi_g}(b) = up^{\frac{m+s_2}{2}}\xi_p^{g'(b)}$ where $|u| = 1$, (in fact, u does not depend on b) and g' is a p-ary function over $\mathrm{Supp}(\widehat{\chi_g})$. Assume F_b is (non)-weakly regular s_1-plateaued for all $b \in \mathrm{Supp}(\widehat{\chi_g})$. Then, for all $a \in \mathrm{Supp}(\widehat{\chi_{F_b}})$, we have $\widehat{\chi_{F_b}}(a) = u_{a,b}p^{\frac{n+s_1}{2}}\xi_p^{F_b'(a)}$ where $|u_{a,b}| = 1$ (in fact, it depends on $b \in \mathrm{Supp}(\widehat{\chi_g})$ and possibly on $a \in \mathrm{Supp}(\widehat{\chi_{F_b}})$) and F_b' is a p-ary function over $\mathrm{Supp}(\widehat{\chi_{F_b}})$. Hence, in view of Proposition 6.3 and Remark 6.2, for all $(a,b) \in \mathrm{Supp}(\widehat{\chi_h})$, we have

$$\widehat{\chi_h}(a,b) = \widehat{\chi_{F_b}}(a)\widehat{\chi_g}(b) = v_{a,b}p^{\frac{n+m+s_1+s_2}{2}}\xi_p^{h'(a,b)}$$

where $|v_{a,b}| = 1$, (in fact, $v_{a,b} = uu_{a,b}$ and $v_{a,b}$ depends on $(a,b) \in \mathrm{Supp}(\widehat{\chi_h})$) and $h'(a,b) = F_b'(a) + g'(b)$ is a p-ary function over $\mathrm{Supp}(\widehat{\chi_h})$. Hence, h is a non-weakly regular (s_1+s_2)-plateaued function over $\mathbb{F}_{p^{n+m}}$. The other direction follows from the above arguments. □

We now propose new secondary construction of p-ary plateaued functions, as an extension of the semi-direct sum construction given in Definition 6.3. Our construction is as follows. Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$, $g : \mathbb{F}_{p^m} \to \mathbb{F}_p$, let $F : \mathbb{F}_{p^m} \to \mathbb{F}_{p^n}$ and

$G : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ be functions. We define a function $h : \mathbb{F}_{p^n} \times \mathbb{F}_{p^m} \to \mathbb{F}_p$ by

$$h(x, y) = f(x + F(y)) + g(y + G(x)). \tag{6.6}$$

We start by giving the expression of the Wash transform of h.

Proposition 6.4. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ and $g : \mathbb{F}_{p^m} \to \mathbb{F}_p$, let $F : \mathbb{F}_{p^m} \to \mathbb{F}_{p^n}$ and $G : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ be functions. Then, for $(a, b) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^m}$, the Walsh transform of the function $h : \mathbb{F}_{p^n} \times \mathbb{F}_{p^m} \to \mathbb{F}_p$ defined by (6.6) is given by*

$$\widehat{\chi_h}(a, b) = \widehat{\chi_{F_b}}(a)\widehat{\chi_{G_a}}(b),$$

where $F_b : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is defined as $F_b(x) = f(x) + b \cdot G(x)$ for all $b \in \mathrm{Supp}(\widehat{\chi_{G_a}})$ and it is the zero function for all $b \notin \mathrm{Supp}(\widehat{\chi_{G_a}})$, and $G_a : \mathbb{F}_{p^m} \to \mathbb{F}_p$ is defined as $G_a(y) = g(y) + a \cdot F(y)$ for all $a \in \mathrm{Supp}(\widehat{\chi_{F_b}})$ and it is the zero function for all $a \notin \mathrm{Supp}(\widehat{\chi_{F_b}})$.

Proof. For all $(a, b) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^m}$, we have

$$\begin{aligned}
\widehat{\chi_h}(a, b) &= \sum_{(x,y)\in\mathbb{F}_{p^n}\times\mathbb{F}_{p^m}} \xi_p^{h(x,y)-(a,b)\cdot(x,y)} = \sum_{x\in\mathbb{F}_{p^n}, y\in\mathbb{F}_{p^m}} \xi_p^{f(x+F(y))-a\cdot x+g(y+G(x))-b\cdot y} \\
&= \sum_{x\in\mathbb{F}_{p^n}} \xi_p^{f(x)+b\cdot G(x)-a\cdot x} \sum_{y\in\mathbb{F}_{p^m}} \xi_p^{g(y)+a\cdot F(y)-b\cdot y} \\
&= \sum_{x\in\mathbb{F}_{p^n}} \xi_p^{F_b(x)-a\cdot x} \sum_{y\in\mathbb{F}_{p^m}} \xi_p^{G_a(y)-b\cdot y} = \widehat{\chi_{F_b}}(a)\widehat{\chi_{G_a}}(b),
\end{aligned}$$

where in the third equality we used the bijective change of variables: $x \mapsto x - F(y)$ and $y \mapsto y - G(x)$. This completes the proof. □

Remark 6.3. If F and G are the zero functions, then this construction reduces to the direct sum construction. If F or G is the zero function, then this construction reduces to the semi-direct sum construction.

Remark 6.4. Notice that $(a, b) \in \mathrm{Supp}(\widehat{\chi_h})$ if and only if $a \in \mathrm{Supp}(\widehat{\chi_{F_b}})$ and $b \in \mathrm{Supp}(\widehat{\chi_{G_a}})$.

The following constructions of (non)-weakly regular bent and plateaued functions follow from Proposition 6.4 and Remark 6.4.

Proposition 6.5. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ and $g : \mathbb{F}_{p^m} \to \mathbb{F}_p$ be bent, and let $F : \mathbb{F}_{p^m} \to \mathbb{F}_{p^n}$ and $G : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$ be functions. If F_b and G_a are bent functions where $F_b : \mathbb{F}_{p^n} \to$*

$\mathbb{F}_p$ *is defined as* $F_b(x) = f(x) + b \cdot G(x)$ *for all* $b \in \mathbb{F}_{p^n}$ *and* $G_a : \mathbb{F}_{p^m} \to \mathbb{F}_p$ *is defined as* $G_a(y) = g(y) + a \cdot F(y)$ *for all* $a \in \mathbb{F}_{p^m}$*, then* h *is bent over* $\mathbb{F}_{p^{n+m}}$.

Theorem 6.3. *Let* $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ *and* $g : \mathbb{F}_{p^m} \to \mathbb{F}_p$ *be plateaued functions. Let* F_b*,* G_a *and* h *be as in Proposition 6.4. If* F_b *and* G_a *are plateaued functions for all* $b \in \mathrm{Supp}(\widehat{\chi_{G_a}})$ *and* $a \in \mathrm{Supp}(\widehat{\chi_{F_b}})$*, respectively, then* h *is plateaued over* $\mathbb{F}_{p^{n+m}}$.

The following proposition provides the construction of a non-weakly regular plateaued function from given a non-weakly regular plateaued function and a (weakly) regular plateaued function.

Proposition 6.6. *Let* $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ *be* s_1*-plateaued and* $g : \mathbb{F}_{p^m} \to \mathbb{F}_p$ *be* s_2*-plateaued. Let* F_b*,* G_a *and* h *be as in Proposition 6.4. Assume that* F_b *is non-weakly regular* s_1*-plateaued for all* $b \in \mathrm{Supp}(\widehat{\chi_{G_a}})$ *and* G_a *is (weakly) regular* s_2*-plateaued for all* $a \in \mathrm{Supp}(\widehat{\chi_{F_b}})$*. Then,* h *is non-weakly regular* $(s_1 + s_2)$*-plateaued over* $\mathbb{F}_{p^{n+m}}$.

Recursive Constructions of (Non)-Weakly Regular Plateaued p-Ary Functions. In this part, we construct (non)-weakly regular plateaued p-ary functions from given ones. In 2009, a construction method of binary bent functions from given near-bent functions was given in [49], and then in 2012, this method was generalized in [22] to arbitrary characteristic by obtaining p-ary bent functions from given p-ary near-bent functions. This is as follows.

Let $f_i : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be functions for all $i \in \{0, \ldots, p-1\}$ such that for $0 \leq j \neq k \leq p-1$,

$$\mathrm{Supp}(\widehat{\chi_{f_j}}) \cap \mathrm{Supp}(\widehat{\chi_{f_k}}) = \emptyset.$$

We define $F : \mathbb{F}_{p^n} \times \mathbb{F}_p \to \mathbb{F}_p$ by

$$h(x, y) = (p-1) \sum_{i=0}^{p-1} \frac{y(y-1)\ldots(y-(p-1))}{y-i} f_i(x). \tag{6.7}$$

The Walsh transform of h at $(a, b) \in \mathbb{F}_{p^n} \times \mathbb{F}_p$ was computed in [22]:

$$\widehat{\chi_h}(a, b) = \sum_{y \in \mathbb{F}_p} \xi_p^{-by} \widehat{\chi_{f_y}}(a).$$

We now use the construction presented above to produce the first construction of (non)-weakly regular plateaued p-ary functions from p given (non)-weakly regular plateaued p-ary functions with pairwise disjoint Walsh supports.

Let $f_i : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be s-plateaued functions for all $i \in \{0, \ldots, p-1\}$ such that $\mathrm{Supp}(\widehat{\chi_{f_j}}) \cap \mathrm{Supp}(\widehat{\chi_{f_k}}) = \emptyset$ for $0 \leq j \neq k \leq p-1$, where s is an integer with $1 \leq s \leq n$. Notice that $\mathrm{Supp}(\widehat{\chi_{f_i}}) = \{a \in \mathbb{F}_{p^n} : \widehat{\chi_{f_i}}(a) \neq 0\}$ and $\#\mathrm{Supp}(\widehat{\chi_{f_i}}) = p^{n-s}$ for all $i \in \{0, \ldots, p-1\}$. Hence, we have

$$\# \left(\bigcup_{i=0}^{p-1} \mathrm{Supp}(\widehat{\chi_{f_i}}) \right) = \sum_{i=0}^{p-1} \#\mathrm{Supp}(\widehat{\chi_{f_i}}) = p^{n+1-s},$$

and the set $\bigcup_{i=0}^{p-1} \mathrm{Supp}(\widehat{\chi_{f_i}})$ is the proper subset of $\mathbb{F}_{p^n}$ for an integer $s > 1$. Then, the Walsh support of $h : \mathbb{F}_{p^n} \times \mathbb{F}_p \to \mathbb{F}_p$ is given by

$$\begin{aligned} \mathrm{Supp}(\widehat{\chi_h}) &= \left\{ (a,b) \in \mathbb{F}_{p^n} \times \mathbb{F}_p : \ a \in \bigcup_{i=0}^{p-1} \mathrm{Supp}(\widehat{\chi_{f_i}}) \text{ and } b \in \mathbb{F}_p \right\} \\ &= \bigcup_{i=0}^{p-1} \mathrm{Supp}(\widehat{\chi_{f_i}}) \times \mathbb{F}_p, \end{aligned}$$

and $\#\mathrm{Supp}(\widehat{\chi_h}) = p^{n+1-(s-1)}$. It is worth noting that the Walsh spectrum of h is given by

$$spec(h) = \bigcup_{i=0}^{p-1} \bigcup_{b \in \mathbb{F}_p} \xi_p^{-bi} spec(f_i).$$

Remark 6.5. Note that $(a,b) \in \mathrm{Supp}(\widehat{\chi_h})$ if and only if $a \in \mathrm{Supp}(\widehat{\chi_{f_i}})$ for exactly one $i \in \mathbb{F}_p$ and $b \in \mathbb{F}_p$.

We can construct an $(s-1)$-plateaued function over $\mathbb{F}_{p^{n+1}}$ from p given s-plateaued functions over $\mathbb{F}_{p^n}$, where s is an integer with $1 \leq s \leq n$.

Theorem 6.4. *Let $f_i : \mathbb{F}_{p^n} \to \mathbb{F}_p$ for all $i \in \{0, \ldots, p-1\}$ and $h : \mathbb{F}_{p^n} \times \mathbb{F}_p \to \mathbb{F}_p$ defined by (6.7). If f_i is s-plateaued for all $i \in \{0, \ldots, p-1\}$, then h is $(s-1)$-plateaued.*

Proof. Using the expression of the Wash transform of h and by Remark 6.5, for all $(a,b) \in \mathrm{Supp}(\widehat{\chi_h})$, since each a belongs to $\mathrm{Supp}(\widehat{\chi_{f_y}})$ for exactly one $y \in \{0, \ldots, p-1\}$, for this y we have

$$\widehat{\chi_h}(a,b) = \xi_p^{-by} \widehat{\chi_{f_y}}(a),$$

and hence, $|\widehat{\chi_h}(a,b)|^2 = |\xi_p^{-by} \widehat{\chi_{f_y}}(a)|^2 = p^{n+s} = p^{n+1+(s-1)}$. Hence, h is $(s-1)$-plateaued over $\mathbb{F}_{p^{n+1}}$. □

We can construct a non-weakly regular plateaued function from some given weakly regular plateaued functions.

Corollary 6.2. *Let $f_i : \mathbb{F}_{p^n} \to \mathbb{F}_p$ for all $i \in \{0, \ldots, p-1\}$ and $h : \mathbb{F}_{p^n} \times \mathbb{F}_p \to \mathbb{F}_p$ defined by (6.7). Let s be an integer with $1 \leq s \leq n$. If f_i is weakly regular s-plateaued for all $i \in \{0, \ldots, p-1\}$, then h is non-weakly regular $(s-1)$-plateaued.*

Proof. As in the proof of Theorem 6.4, for all $(a, b) \in \mathrm{Supp}(\widehat{\chi_h})$,

$$\widehat{\chi_h}(a,b) = \xi_p^{-by}\widehat{\chi_{f_y}}(a) = \xi_p^{-by} u_y p^{\frac{n+s}{2}} \xi_p^{f'_y(a)} = u_y p^{\frac{(n+1)+(s-1)}{2}} \xi_p^{f'_y(a)-by}$$

where $|u_y| = 1$, (in fact, u_y depends on $(a, b) \in \mathrm{Supp}(\widehat{\chi_h})$) and $h'(a, b) = f'_y(a) - by$ is a p-ary function over $\mathrm{Supp}(\widehat{\chi_h})$. Hence, h is non-weakly regular $(s-1)$-plateaued over $\mathbb{F}_{p^{n+1}}$. □

Remark 6.6. In Corollary 6.2, if f_i is non-weakly regular s-plateaued for all $i \in \{0, \ldots, p-1\}$, then h is non-weakly regular $(s-1)$-plateaued.

The following construction given in [22, 24] combines n variable p bent functions to construct an $(n+2)$ variable one bent function. Let $f_i : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be functions for all $i \in \{0, \ldots, p-1\}$. Let $h : \mathbb{F}_{p^n} \times \mathbb{F}_{p^2} \to \mathbb{F}_p$ be the function defined as

$$h(x, y) = f_{y_2}(x) + y_1 y_2 \tag{6.8}$$

where $x \in \mathbb{F}_{p^n}$ and $y = (y_1, y_2) \in \mathbb{F}_{p^2}$. For $(a, b) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^2}$, the Walsh transform of h is

$$\widehat{\chi_h}(a,b) = p\xi_p^{-b_1 b_2}\widehat{\chi_{f_{b_1}}}(a), \tag{6.9}$$

where $b = (b_1, b_2) \in \mathbb{F}_{p^2}$.

Remark 6.7. Notice that $(a, b) \in \mathrm{Supp}(\widehat{\chi_h})$ if and only if $a \in \mathrm{Supp}(\widehat{\chi_{f_{b_1}}})$ where $b = (b_1, b_2) \in \mathbb{F}_{p^2}$.

Below, we consider this construction for plateaued functions.

Theorem 6.5. *Let $f_i : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be functions for all $i \in \{0, \ldots, p-1\}$ and let $h : \mathbb{F}_{p^n} \times \mathbb{F}_{p^2} \to \mathbb{F}_p$ defined by (6.8). Then, h is s-plateaued if and only if f_i is s-plateaued for all $i \in \{0, \ldots, p-1\}$.*

Proof. For all $(a,b) \in \mathrm{Supp}(\widehat{\chi_h})$, we have $\widehat{\chi_h}(a,b) = p\xi_p^{-b_1b_2}\widehat{\chi_{f_{b_1}}}(a)$, and hence,

$$|\widehat{\chi_h}(a,b)|^2 = |p\xi_p^{-b_1b_2}\widehat{\chi_{f_{b_1}}}(a)|^2 = p^2|\widehat{\chi_{f_{b_1}}}(a)|^2.$$

Hence, h is $(n+2)$ variable s-plateaued if and only if f_{b_1} is n variable s-plateaued for all $b_1 \in \{0,\ldots,p-1\}$. □

We can construct a non-weakly regular plateaued function from given weakly regular plateaued functions based on the above construction.

Proposition 6.7. *Let $f_i : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be functions for all $i \in \{0,\ldots,p-1\}$ and let $h : \mathbb{F}_{p^n} \times \mathbb{F}_{p^2} \to \mathbb{F}_p$ defined by (6.8). If f_i is weakly regular s-plateaued for all $i \in \{0,\ldots,p-1\}$, then h is a non-weakly regular s-plateaued function. In particular, f_i is weakly regular s-plateaued with the same complex number u (see Definition 6.1) for all $i \in \{0,\ldots,p-1\}$ if and only if h is weakly regular s-plateaued.*

Proof. Assume that f_i is weakly regular s-plateaued for all $i \in \{0,\ldots,p-1\}$. Then for all $a \in \mathrm{Supp}(\widehat{\chi_{f_i}})$, we have

$$\widehat{\chi_{f_i}}(a) = u_i p^{\frac{n+s}{2}} \xi_p^{f_i'(a)},$$

where $|u_i| = 1$, (in fact, u_i does not depend on $a \in \mathbb{F}_{p^n}$) and f_i' is a p-ary function over $\mathrm{Supp}(\widehat{\chi_{f_i}})$. For all $(a,b) \in \mathrm{Supp}(\widehat{\chi_h})$, by (6.9) we have

$$\widehat{\chi_h}(a,b) = p\xi_p^{-b_1b_2}\widehat{\chi_{f_{b_1}}}(a) = p\xi_p^{-b_1b_2}u_{b_1}p^{\frac{n+s}{2}}\xi_p^{f_{b_1}'(a)} = u_{b_1}p^{\frac{n+2+s}{2}}\xi_p^{f_{b_1}'(a)-b_1b_2}$$

where $|u_{b_1}| = 1$, (in fact, u_{b_1} depends on $(a,b) \in \mathrm{Supp}(\widehat{\chi_h})$) and $h'(a,b) = f_{b_1}'(a) - b_1b_2$ is a p-ary function over $\mathrm{Supp}(\widehat{\chi_h})$; equivalently, h is non-weakly regular s-plateaued over $\mathbb{F}_{p^{n+2}}$. In particular, the second statement follows from (6.9) and the first statement. □

Given n variable p plateaued functions, the following new construction produces $(n+4)$ variable one plateaued function. Let $f_i : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be functions for all $i \in \{0,\ldots,p-1\}$. Let $h : \mathbb{F}_{p^n} \times \mathbb{F}_{p^4} \to \mathbb{F}_p$ be the function defined as

$$h(x,y) = f_{y_4}(x) + y_1y_2 + y_3y_4, \tag{6.10}$$

where $y = (y_1,y_2,y_3,y_4) \in \mathbb{F}_p^4$.

Now we present further possibilities of constructions of (non)-weakly regular bent and plateaued functions based on the above construction.

Theorem 6.6. *Let $f_i : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be functions for all $i \in \{0, \ldots, p-1\}$ and let $h : \mathbb{F}_{p^n} \times \mathbb{F}_{p^4} \to \mathbb{F}_p$ defined by (6.10). Then, h is s-plateaued if and only if f_i is s-plateaued for all $i \in \{0, \ldots, p-1\}$.*

Proof. For $(a, b) \in \mathbb{F}_{p^n} \times \mathbb{F}_{p^4}$, the Walsh transform $\widehat{\chi_h}(a, b)$ of h is equal to

$$\begin{aligned}
&\sum_{x,y \in \mathbb{F}_{p^n}} \xi_p^{h(x,y)-(a,b)\cdot(x,y)} = \sum_{x \in \mathbb{F}_{p^n}} \xi_p^{f_{y_4}(x)-a\cdot x} \sum_{y_1,y_2,y_3,y_4 \in \mathbb{F}_p} \xi_p^{y_1y_2+y_3y_4-b_1y_1-b_2y_2-b_3y_3-b_4y_4} \\
&= \sum_{x \in \mathbb{F}_{p^n}} \xi_p^{-a\cdot x} \left(\sum_{y_2 \in \mathbb{F}_p} \xi_p^{-b_2y_2} \sum_{y_1 \in \mathbb{F}_p} \xi_p^{y_1(y_2-b_1)} \right) \left(\sum_{y_4 \in \mathbb{F}_p} \xi_p^{f_{y_4}(x)-b_4y_4} \sum_{y_3 \in \mathbb{F}_p} \xi_p^{y_3(y_4-b_3)} \right) \\
&= \sum_{x \in \mathbb{F}_{p^n}} \xi_p^{f_{b_3}(x)-a\cdot x} \left(p\xi_p^{-b_1b_2}\right) \left(p\xi_p^{-b_3b_4}\right) = p^2\xi_p^{-b_1b_2-b_3b_4}\widehat{\chi_{f_{b_3}}}(a).
\end{aligned}$$

Notice that $(a, b) \in \mathrm{Supp}(\widehat{\chi_h})$ if and only if $a \in \mathrm{Supp}(\widehat{\chi_{f_{b_3}}})$ where $b = (b_1, b_2, b_3, b_4) \in \mathbb{F}_p^4$. Hence, the result follows as in the proof of Theorem 6.5. □

Corollary 6.3. *Let $f_i : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be functions for all $i \in \{0, \ldots, p-1\}$ and let $h : \mathbb{F}_{p^n} \times \mathbb{F}_{p^4} \to \mathbb{F}_p$ be defined by (6.10). Then, h is bent if and only if f_i is bent for all $i \in \{0, \ldots, p-1\}$.*

We can derive a non-weakly regular plateaued function from given weakly regular plateaued functions based on the above construction. The following can be easily proven as in the proof of Proposition 6.7.

Proposition 6.8. *Let $f_i : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be functions for all $i \in \{0, \ldots, p-1\}$ and let $h : \mathbb{F}_{p^n} \times \mathbb{F}_{p^4} \to \mathbb{F}_p$ be defined by (6.10). If f_i is weakly regular s-plateaued for all $i \in \{0, \ldots, p-1\}$, then h is a non-weakly regular s-plateaued function. In particular, f_i is weakly regular s-plateaued with the same complex number u (see Definition 6.1) for all $i \in \{0, \ldots, p-1\}$ if and only if h is weakly regular s-plateaued.*

6.2 On the First Generic Construction of Linear Codes from Functions over $\mathbb{F}_p$

In this section, we review the construction of linear codes involving special functions over finite fields based on the first generic construction.

In the literature, there are mainly two generic constructions (say, *first* and *second*) of linear codes from functions over finite fields (see [31]). We now recall the first

generic construction, which is obtained by considering a code $\mathcal{C}(h)$ over $\mathbb{F}_p$ involving a polynomial h from $\mathbb{F}_q$ to $\mathbb{F}_q$ (where $q = p^m$) defined by

$$\mathcal{C}(h) = \{\mathbf{c} = (\mathrm{Tr}_p^q(ah(x) + bx))_{x \in \mathbb{F}_q^*} : a \in \mathbb{F}_q, b \in \mathbb{F}_q\}.$$

The resulting code $\mathcal{C}(h)$ from h is a linear code of length $q-1$ and its dimension is upper bounded by $2m$ which is reached in many cases. This is the following. It is worth mentioning that the importance of the first generic construction is supported by Delsarte's Theorem [29].

For any $\alpha, \beta \in \mathbb{F}_{q^n}$ (where $q = p^m$), we define a function

$$\begin{array}{rccl} f_{\alpha,\beta} & : & \mathbb{F}_{q^n} & \longrightarrow & \mathbb{F}_q \\ & & x & \longmapsto & f_{\alpha,\beta}(x) := \mathrm{Tr}_q^{q^n}(\alpha\Psi(x) - \beta x), \end{array}$$

where Ψ is a polynomial from $\mathbb{F}_{q^n}$ to $\mathbb{F}_{q^n}$ such that $\Psi(0) = 0$. Then we also define a linear code $\mathcal{C}_\Psi$ over $\mathbb{F}_q$ as:

$$\mathcal{C}_\Psi := \{\tilde{c}_{\alpha,\beta} = (f_{\alpha,\beta}(\zeta_1), f_{\alpha,\beta}(\zeta_2), \ldots, f_{\alpha,\beta}(\zeta_{q^n-1})) \ : \ \alpha, \beta \in \mathbb{F}_{q^n}\},$$

where $\zeta_1, \ldots, \zeta_{q^n-1}$ are the elements of $\mathbb{F}_{q^n}^\star$ and $\tilde{c}_{\alpha,\beta}$ denotes a codeword of $\mathcal{C}_\Psi$.

Very recently, Mesnager [58] has proposed an approach for constructing linear codes with special types of functions based on the first generic construction. With this approach, we will construct linear codes from plateaued functions in arbitrary characteristic in the next section. We first recall this approach based on the first generic construction.

Remark 6.8. Clearly, the length of the linear code $\mathcal{C}_\Psi$ is $q^n - 1$.

Proposition 6.9. *If the polynomial $\Psi : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ has no linear component, then $\mathcal{C}_\Psi$ has dimension $2n$ over $\mathbb{F}_q$.*

Proof. We observe that $\tilde{c}_{\alpha,\beta} = 0$ if and only if for all $i \in \{1, \ldots, q^n - 1\}$,

$$\begin{aligned} \mathrm{Tr}_q^{q^n}(\alpha\Psi(\zeta_i) - \beta\zeta_i) = 0 &\Longleftrightarrow \mathrm{Tr}_q^{q^n}(\alpha\Psi(x) - \beta x) = 0, \text{ for all } x \in \mathbb{F}_{q^n}^\star \\ &\Rightarrow \mathrm{Tr}_p^{q^n}(\alpha\Psi(x) - \beta x) = 0, \text{ for all } x \in \mathbb{F}_{q^n} \\ &\Rightarrow \mathrm{Tr}_p^{q^n}(\alpha\Psi(x)) = \mathrm{Tr}_p^{q^n}(\beta x), \text{ for all } x \in \mathbb{F}_{q^n}. \end{aligned}$$

Hence, $\tilde{c}_{\alpha,\beta} = 0$ implies that the component of Ψ associated with $\alpha \neq 0$ is linear or null and coincides with $x \mapsto \mathrm{Tr}_p^{q^n}(\beta x)$. Hence, to ensure that the zero codeword

appears only once (when $\alpha = \beta = 0$), it is enough to show that no component function of Ψ is identically 0 or linear. Then this implies that all codewords $\tilde{c}_{\alpha,\beta}$ are pairwise distinct. Hence, the dimension of $\mathcal{C}_\Psi$ is $2n$. □

The Hamming weights of the codewords of $\mathcal{C}_\Psi$ of length $q^n - 1$ can be expressed by the Walsh transform of trace functions involving the map Ψ. We keep the above notations in the following proposition.

Proposition 6.10. *Let ψ_a be a function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_p$ defined by*

$$\psi_a(x) = \mathrm{Tr}_p^{q^n}(a\Psi(x)),$$

where $a \in \mathbb{F}_{q^n}$ and $\Psi : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ with $\Psi(0) = 0$. For all $\alpha, \beta \in \mathbb{F}_{q^n}$,

$$wt(\tilde{c}_{\alpha,\beta}) = q^n - \frac{1}{q} \sum_{\omega \in \mathbb{F}_q} \widehat{\chi_{\psi_{\omega\alpha}}}(\omega\beta).$$

Proof. Obviously, $f_{\alpha,\beta}(0) = 0$ since $\Psi(0) = 0$. For all $\alpha, \beta \in \mathbb{F}_{q^n}$, we have

$$\begin{aligned} wt(\tilde{c}_{\alpha,\beta}) &= \#\{x \in \mathbb{F}_{q^n}^\star : f_{\alpha,\beta}(x) \neq 0\} \\ &= \#\{x \in \mathbb{F}_{q^n} : f_{\alpha,\beta}(x) \neq 0\} \\ &= q^n - \#\{x \in \mathbb{F}_{q^n} : f_{\alpha,\beta}(x) = 0\} \\ &= q^n - \sum_{x \in \mathbb{F}_{q^n}} \frac{1}{q} \sum_{\omega \in \mathbb{F}_q} \xi_p{}^{\mathrm{Tr}_p^q(\omega f_{\alpha,\beta}(x))}, \end{aligned}$$

where the last equality follows from the fact that the sum of characters is q if $f_{\alpha,\beta}(x) = 0$, and 0 otherwise. Meanwhile, we have

$$\sum_{x \in \mathbb{F}_{q^n}} \sum_{\omega \in \mathbb{F}_q} \xi_p{}^{\mathrm{Tr}_p^q(\omega f_{\alpha,\beta}(x))} = \sum_{\omega \in \mathbb{F}_q} \sum_{x \in \mathbb{F}_{q^n}} \xi_p{}^{\mathrm{Tr}_p^q(\omega \mathrm{Tr}_q^{q^n}(\alpha\Psi(x) - \beta x))} =$$

$$\sum_{\omega \in \mathbb{F}_q} \sum_{x \in \mathbb{F}_{q^n}} \xi_p{}^{\mathrm{Tr}_p^{q^n}(\omega\alpha\Psi(x) - \omega\beta x)} = \sum_{\omega \in \mathbb{F}_q} \sum_{x \in \mathbb{F}_{q^n}} \xi_p{}^{\psi_{\omega\alpha}(x) - \mathrm{Tr}_p^{q^n}(\omega\beta x)} = \sum_{\omega \in \mathbb{F}_q} \widehat{\chi_{\psi_{\omega\alpha}}}(\omega\beta),$$

where we used the transitivity and the linearity of the trace function $\mathrm{Tr}_p^{q^n}$. This completes the proof. □

We consider a subclass of the class of the linear codes $\mathcal{C}_\Psi$. We assume $m = 1$ (i.e., $q = p$) and $\alpha \in \mathbb{F}_p$. Let $\psi_1(x) = \mathrm{Tr}_p^{p^n}(\Psi(x))$ be a p-ary function such that a polynomial $\Psi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ with $\Psi(0) = 0$ has no linear component. Then, we have

$$f_{\alpha,\beta}(x) = \alpha\psi_1(x) - \mathrm{Tr}_p^{p^n}(\beta x)$$

and define a subcode $\mathcal{C}_{\psi_1}$ of $\mathcal{C}_\Psi$ as follows:

$$\mathcal{C}_{\psi_1} := \{\tilde{c}_{\alpha,\beta} = (f_{\alpha,\beta}(\zeta_1), f_{\alpha,\beta}(\zeta_2), \ldots, f_{\alpha,\beta}(\zeta_{p^n-1})) \,:\, \alpha \in \mathbb{F}_p, \beta \in \mathbb{F}_{p^n}\}, \quad (6.11)$$

where $\zeta_1, \ldots, \zeta_{p^n-1}$ are the elements of $\mathbb{F}_{p^n}^\star$. The linear code $\mathcal{C}_{\psi_1}$ of length $p^n - 1$ over $\mathbb{F}_p$ defined by (6.11) is a k-dimensional subspace of $\mathbb{F}_p^n$, where $k = n + 1$, and denoted by $[p^n - 1, n + 1]_p$. In view of Proposition 6.10, the Hamming weights of the codewords of $\mathcal{C}_{\psi_1}$ are given as follows. We keep the above arguments in the following proposition.

Proposition 6.11. *For $\tilde{c}_{\alpha,\beta} \in \mathcal{C}_{\psi_1}$,*

- *if $\alpha = 0$, we have $wt(\tilde{c}_{0,0}) = 0$ and $wt(\tilde{c}_{0,\beta}) = p^n - p^{n-1}$ for all $\beta \in \mathbb{F}_{p^n}^\star$,*
- *if $\alpha \in \mathbb{F}_p^\star$, we have for all $\beta \in \mathbb{F}_{p^n}$*

$$wt(\tilde{c}_{\alpha,\beta}) = p^n - p^{n-1} - \frac{1}{p} \sum_{\omega \in \mathbb{F}_p^\star} \sigma_\omega \left(\sigma_\alpha(\widehat{\chi_{\psi_1}}(\alpha^{-1}\beta)) \right),$$

where α^{-1} is the multiplicative inverse of $\alpha \in \mathbb{F}_p^\star$ and σ_a is the automorphism of the cyclotomic field $\mathbb{Q}(\xi_p)$ for $a \in \mathbb{F}_p^\star$.

Proof. By Proposition 6.10, for all $\alpha \in \mathbb{F}_p$ and $\beta \in \mathbb{F}_{p^n}$, we have

$$wt(\tilde{c}_{\alpha,\beta}) = p^n - \frac{1}{p} \sum_{\omega \in \mathbb{F}_p} \widehat{\chi_{\psi_{\omega\alpha}}}(\omega\beta).$$

Clearly, the Walsh transform of the zero function (denoted by $\mathbf{0}$) at a point $b \in \mathbb{F}_{p^n}$ is

$$\widehat{\chi_{\mathbf{0}}}(b) = \sum_{x \in \mathbb{F}_{p^n}} \xi_p^{-bx} = p^n \delta_{0,b},$$

where $\delta_{i,j}$ denotes the Dirac symbol defined by $\delta_{i,j} = 1$ if $i = j$, and 0 otherwise. Then obviously $\widehat{\chi_{\mathbf{0}}}(0) = p^n$. Meanwhile, we have

$$\begin{aligned}\sum_{\omega \in \mathbb{F}_p} \widehat{\chi_{\psi_{\omega\alpha}}}(\omega\beta) &= p^n + \sum_{\omega \in \mathbb{F}_p^\star} \widehat{\chi_{\psi_{\omega\alpha}}}(\omega\beta) = p^n + \sum_{\omega \in \mathbb{F}_p^\star} \sum_{x \in \mathbb{F}_{p^n}} \xi_p^{\mathrm{Tr}_p^{p^n}(\omega\alpha\Psi(x) - \omega\beta x)} \\ &= p^n + \sum_{\omega \in \mathbb{F}_p^\star} \sum_{x \in \mathbb{F}_{p^n}} \xi_p^{\omega \mathrm{Tr}_p^{p^n}(\alpha\Psi(x) - \beta x)} = p^n + \sum_{\omega \in \mathbb{F}_p^\star} \sigma_\omega(\widehat{\chi_{\psi_\alpha}}(\beta)).\end{aligned}$$

If $\alpha = 0$, then

$$wt(\tilde{c}_{0,\beta}) = p^n - p^{n-1} - \frac{1}{p} \sum_{\omega \in \mathbb{F}_p^\star} \sigma_\omega(\widehat{\chi_{\mathbf{0}}}(\beta)) = p^n - p^{n-1} - p^{n-1}(p-1)\delta_{0,\beta}.$$

Hence, we obtain $wt(\tilde{c}_{0,0}) = 0$ and for $\beta \neq 0$, $wt(\tilde{c}_{0,\beta}) = p^n - p^{n-1}$.
For $\alpha \neq 0$, we have

$$\sigma_\alpha(\widehat{\chi_{\psi_1}}(\alpha^{-1}\beta)) = \sigma_\alpha\left(\sum_{x\in\mathbb{F}_{p^n}} \xi_p^{\psi_1(x)-\mathrm{Tr}_p^{p^n}(\alpha^{-1}\beta x)}\right) = \sum_{x\in\mathbb{F}_{p^n}} \xi_p^{\alpha\psi_1(x)-\mathrm{Tr}_p^{p^n}(\beta x)}$$
$$= \widehat{\chi_{\alpha\psi_1}}(\beta) = \widehat{\chi_{\psi_\alpha}}(\beta).$$

Hence, for all $\alpha \in \mathbb{F}_p^\star$ and $\beta \in \mathbb{F}_{p^n}$, we have

$$wt(\tilde{c}_{\alpha,\beta}) = p^n - p^{n-1} - \frac{1}{p}\sum_{\omega\in\mathbb{F}_p^\star} \sigma_\omega\left(\sigma_\alpha\left(\widehat{\chi_{\psi_1}}(\alpha^{-1}\beta)\right)\right).$$

□

In the following section, we use the above construction method based on the first generic construction to construct linear codes from plateaued functions.

6.3 New Classes of Three-Weight Linear Codes From Plateaued Functions

We construct new classes of linear codes with few weights from plateaued functions in arbitrary characteristic and determine their weight distributions. We shall analyze separately the binary case in Subsection 6.3.1 and the odd case in Subsection 6.3.2.

6.3.1 A New Class of Binary Three-Weight Linear Codes from Plateaued Boolean Functions

This subsection provides a new class of binary linear codes with few weights from plateaued Boolean functions with their weight distributions.

Let $p = 2$ and let Ψ be a polynomial over $\mathbb{F}_{2^n}$ with $\Psi(0) = 0$. Assume that

$$\psi_1(x) = \mathrm{Tr}_2^{2^n}(\Psi(x))$$

is an s-plateaued Boolean function, where $n+s$ is an even integer with $0 \leq s \leq n-2$ for $n \geq 2$. We consider the linear code $\mathcal{C}_{\psi_1}$ defined by (6.11). For $\alpha \in \mathbb{F}_2$ and $\beta \in \mathbb{F}_{2^n}$, we compute the Hamming weights of the codewords and the weight distribution of $\mathcal{C}_{\psi_1}$. By Proposition 6.11, clearly

- if $\alpha = 0$, we have $wt(\tilde{c}_{0,0}) = 0$ and $wt(\tilde{c}_{0,\beta}) = 2^{n-1}$ for $\beta \neq 0$,
- if $\alpha = 1$ and $\beta \in \mathbb{F}_{2^n}$, we have $wt(\tilde{c}_{1,\beta}) = 2^{n-1} - \frac{1}{2}\widehat{\chi_{\psi_1}}(\beta)$.

Hence, by Lemma 2.6 we have for all $\beta \in \mathbb{F}_{2^n}$,

$$wt(\tilde{c}_{1,\beta}) = \begin{cases} 2^{n-1} - 2^{\frac{n+s-2}{2}}, & 2^{n-s-1} + 2^{\frac{n-s-2}{2}} \text{ times}, \\ 2^{n-1}, & 2^n - 2^{n-s} \text{ times}, \\ 2^{n-1} + 2^{\frac{n+s-2}{2}}, & 2^{n-s-1} - 2^{\frac{n-s-2}{2}} \text{ times}. \end{cases}$$

The following theorem formalizes the Hamming weights of the codewords and the weight distribution of $\mathcal{C}_{\psi_1}$.

Theorem 6.7. *Let $p = 2$ and let $\mathcal{C}_{\psi_1}$ be the binary linear $[2^n - 1, n + 1]$ code defined by (6.11). Assume that ψ_1 is an s-plateaued Boolean function, where $n + s$ is an even integer with $0 \leq s \leq n - 2$ for $n \geq 2$. Then, the Hamming weights of the codewords and the weight distribution of $\mathcal{C}_{\psi_1}$ are as in Table 6.2.*

Hamming weight w	Multiplicity A_w
0	1
2^{n-1}	$2^{n+1} - 2^{n-s} - 1$
$2^{n-1} - 2^{\frac{n+s-2}{2}}$	$2^{n-s-1} + 2^{\frac{n-s-2}{2}}$
$2^{n-1} + 2^{\frac{n+s-2}{2}}$	$2^{n-s-1} - 2^{\frac{n-s-2}{2}}$

Table 6.2: The Hamming weights of the codewords and the weight distribution of $\mathcal{C}_{\psi_1}$ when $p = 2$ and $n + s$ is even.

Below, we give a 3-plateaued Boolean function and a corresponding binary linear code.

Example 6.3. *Let $\Psi(x) = \zeta^{18}x^5 + \zeta^2 x^3$ be the polynomial over $\mathbb{F}_{2^5}$, where $\mathbb{F}_{2^5}^\star = \langle \zeta \rangle$ with $\zeta^5 + \zeta^2 + 1 = 0$. Then, $\psi_1(x) = \mathrm{Tr}_2^{2^5}(\Psi(x))$ is the 3-plateaued Boolean function, and so the set $\mathcal{C}_{\psi_1}$ in (6.11) is the binary three-weight linear code with parameters $[31, 6, 8]$, weight enumerator $1+3y^8+59y^{16}+y^{24}$ and weight distribution $(1, 3, 59, 1)$. Hence, the Hamming weights of the codewords and the weight distribution of $\mathcal{C}_{\psi_1}$ are as in Table 6.3.*

We now consider the case when p is an odd prime. In odd characteristic, not every p-ary plateaued function can be used in this construction method because of their Walsh

Hamming weight w	Multiplicity A_w
0	1
16	59
8	3
24	1

Table 6.3: The Hamming weights of the codewords and the weight distribution of $\mathcal{C}_{\psi_1}$ when $p = 2$, $n = 5$ and $s = 3$.

transform values. Thereby, we should use the super subclass of the class of plateaued functions, which is the class of weakly regular plateaued functions.

6.3.2 New Classes of Three-Weight Linear p-Ary Codes from Weakly Regular Plateaued Functions

In this subsection, we construct new classes of linear p-ary codes with few weights from weakly regular plateaued p-ary functions and determine their weight distributions.

From now on, we assume that p is an odd prime and a p-ary function

$$\psi_1(x) = \mathrm{Tr}_p^{p^n}(\Psi(x)) \tag{6.12}$$

is weakly regular s-plateaued, where s is an integer with $0 \leq s \leq n-2$ for $n \geq 2$ and Ψ is a polynomial over $\mathbb{F}_{p^n}$ with $\Psi(0) = 0$. We consider the linear code $\mathcal{C}_{\psi_1}$ defined by (6.11).

We first compute the Hamming weights of $\tilde{c}_{\alpha,\beta}$ for all $\alpha \in \mathbb{F}_p$ and $\beta \in \mathbb{F}_{p^n}$, and then determine the weight distribution of $\mathcal{C}_{\psi_1}$. In view of Proposition 6.11, if $\alpha = 0$, we have $wt(\tilde{c}_{0,0}) = 0$ and $wt(\tilde{c}_{0,\beta}) = p^n - p^{n-1}$ for $\beta \in \mathbb{F}_{p^n}^\star$. And for all $\alpha \in \mathbb{F}_p^\star$ and $\beta \in \mathbb{F}_{p^n}$, we have

$$wt(\tilde{c}_{\alpha,\beta}) = p^n - p^{n-1} - \frac{1}{p} \sum_{\omega \in \mathbb{F}_p^\star} \sigma_\omega \left(\sigma_\alpha(\widehat{\chi_{\psi_1}}(\alpha^{-1}\beta)) \right). \tag{6.13}$$

To compute this, we first need the following lemma.

Lemma 6.4. *Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be s-plateaued. Define the sets $\mathcal{Z}(\widehat{\chi_f}) := \{(\alpha, \beta) \in$*

$\mathbb{F}_p^\star \times \mathbb{F}_{p^n} : \widehat{\chi_f}(\alpha^{-1}\beta) = 0\}$ *and*

$$\mathcal{S}(\widehat{\chi_f}) := \{(\alpha, \beta) \in \mathbb{F}_p^\star \times \mathbb{F}_{p^n} : \widehat{\chi_f}(\alpha^{-1}\beta) \neq 0\},$$

where α^{-1} *is the multiplicative inverse of* $\alpha \in \mathbb{F}_p^\star$*. Then, the sizes of* $\mathcal{Z}(\widehat{\chi_f})$ *and* $\mathcal{S}(\widehat{\chi_f})$ *are equal respectively to* $(p-1)(p^n - p^{n-s})$ *and* $(p-1)p^{n-s}$.

Proof. By Lemma 2.5, we have $\#\{\beta \in \mathbb{F}_{p^n} : \widehat{\chi_f}(\beta) = 0\} = p^n - p^{n-s}$ and $\#\mathrm{Supp}(\widehat{\chi_f}) = p^{n-s}$, where $\mathrm{Supp}(\widehat{\chi_f}) = \{\beta \in \mathbb{F}_{p^n} : \widehat{\chi_f}(\beta) \neq 0\}$. Notice that for each $\alpha \in \mathbb{F}_p^\star$, the element $\beta \in \mathbb{F}_{p^n}$ can be viewed as $\alpha^{-1}\beta$, that is, $\mathbb{F}_{p^n} = \{\alpha^{-1}\beta : \beta \in \mathbb{F}_{p^n}\}$. Hence, we have $\#\mathcal{Z}(\widehat{\chi_f}) = (p-1)(p^n - p^{n-s})$ and $\#\mathcal{S}(\widehat{\chi_f}) = (p-1)p^{n-s}$. The proof is complete. □

We should now consider two cases: the Walsh transform value of plateaued ψ_1 is either zero or nonzero. For all $\alpha \in \mathbb{F}_p^\star$ and $\beta \in \mathbb{F}_{p^n}$, we have the following.
If $\widehat{\chi_{\psi_1}}(\alpha^{-1}\beta) = 0$, i.e., $(\alpha, \beta) \in \mathcal{Z}(\widehat{\chi_{\psi_1}})$, then we have $wt(\tilde{c}_{\alpha,\beta}) = p^n - p^{n-1}$, that is, the number of codewords with Hamming weight $p^n - p^{n-1}$ is the size of $\mathcal{Z}(\widehat{\chi_{\psi_1}})$ by Lemma 6.4.
If $\widehat{\chi_{\psi_1}}(\alpha^{-1}\beta) \neq 0$, i.e., $(\alpha, \beta) \in \mathcal{S}(\widehat{\chi_{\psi_1}})$; equivalently, $\alpha^{-1}\beta \in \mathrm{Supp}(\widehat{\chi_{\psi_1}})$, then by Lemma 6.1,

$$\widehat{\chi_{\psi_1}}(\alpha^{-1}\beta) = \epsilon\sqrt{p^*}^{n+s}\xi_p^{g(\alpha^{-1}\beta)}, \tag{6.14}$$

where $\epsilon = \pm 1$, p^* denotes $\left(\frac{-1}{p}\right)p$ and g is a p-ary function over $\mathrm{Supp}(\widehat{\chi_{\psi_1}})$. Notice that we have

$$\sigma_\alpha(\sqrt{p^*}^{n+s}) = \sigma_\alpha(\sqrt{p}^*)^{n+s} = \left(\frac{\alpha}{p}\right)^{n+s}\sqrt{p^*}^{n+s}.$$

Then we get

$$\sigma_\omega\left(\sigma_\alpha(\widehat{\chi_{\psi_1}}(\alpha^{-1}\beta))\right) = \sigma_\omega\left(\epsilon\left(\frac{\alpha}{p}\right)^{n+s}\sqrt{p^*}^{n+s}\xi_p^{\alpha g(\alpha^{-1}\beta)}\right) =$$

$$\epsilon\left(\frac{\alpha}{p}\right)^{n+s}\sigma_\omega(\sqrt{p^*}^{n+s})\xi_p^{\omega\alpha g(\alpha^{-1}\beta)} = \epsilon\left(\frac{\alpha}{p}\right)^{n+s}\left(\frac{\omega}{p}\right)^{n+s}\sqrt{p^*}^{n+s}\xi_p^{\omega\alpha g(\alpha^{-1}\beta)}.$$

Note that $\left(\frac{a}{p}\right)^{n+s} = 1$ and $\sqrt{p^*}^{n+s} = \sqrt{p}^{n+s}$ if $n+s$ is even; otherwise, $\left(\frac{a}{p}\right)^{n+s} = \left(\frac{a}{p}\right)$ for $a \in \mathbb{F}_p^\star$. Hence, by (6.13) we have

$$wt(\tilde{c}_{\alpha,\beta}) = \begin{cases} p^n - p^{n-1} - \epsilon\frac{1}{p}\left(\frac{\alpha}{p}\right)\sqrt{p^*}^{n+s}\sum_{\omega\in\mathbb{F}_p^\star}\left(\frac{\omega}{p}\right)\xi_p^{\omega\alpha g(\alpha^{-1}\beta)}, & \text{if } n+s \text{ odd,} \\ p^n - p^{n-1} - \epsilon p^{\frac{n+s}{2}-1}\sum_{\omega\in\mathbb{F}_p^\star}\xi_p^{\omega\alpha g(\alpha^{-1}\beta)}, & \text{if } n+s \text{ even.} \end{cases}$$

We now investigate two cases.

- Assume $n+s$ odd. If $g(\alpha^{-1}\beta)=0$, then

$$wt(\tilde{c}_{\alpha,\beta}) = p^n - p^{n-1} - \epsilon\tfrac{1}{p}\left(\tfrac{\alpha}{p}\right)\sqrt{p^*}^{n+s}\sum_{\omega\in\mathbb{F}_p^\star}\left(\frac{\omega}{p}\right) = p^n - p^{n-1},$$

where we used $\sum_{\omega\in\mathbb{F}_p^\star}\left(\frac{\omega}{p}\right)=0$. If $g(\alpha^{-1}\beta)\neq 0$, then we have

$$\begin{aligned}\sum_{\omega\in\mathbb{F}_p^\star}\left(\frac{\omega}{p}\right)(\xi_p^\omega)^{\alpha g(\alpha^{-1}\beta)} &= \sigma_{\alpha g(\alpha^{-1}\beta)}\left(\sum_{\omega\in\mathbb{F}_p^\star}\left(\frac{\omega}{p}\right)\xi_p^\omega\right) = \sigma_{\alpha g(\alpha^{-1}\beta)}(\sqrt{p^*})\\ &= \left(\frac{\alpha g(\alpha^{-1}\beta)}{p}\right)\sqrt{p^*},\end{aligned}$$

where we used $\sum_{\omega\in\mathbb{F}_p^\star}(\frac{\omega}{p})\xi_p^\omega=\sqrt{p^*}$. Hence,

$$\begin{aligned}wt(\tilde{c}_{\alpha,\beta}) &= p^n - p^{n-1} - \epsilon\tfrac{1}{p}\sqrt{p^*}^{n+s+1}\left(\tfrac{\alpha^2}{p}\right)\left(\tfrac{g(\alpha^{-1}\beta)}{p}\right)\\ &= p^n - p^{n-1} - \epsilon\left(\tfrac{-1}{p}\right)^{\frac{n+s+1}{2}}p^{\frac{n+s-1}{2}}\left(\tfrac{g(\alpha^{-1}\beta)}{p}\right),\end{aligned}$$

where we used the fact that $\left(\frac{\alpha}{p}\right)\left(\frac{\alpha}{p}\right)=\left(\frac{\alpha^2}{p}\right)$ in the first equality, and $p^*=\left(\frac{-1}{p}\right)p$ and $\left(\frac{\alpha^2}{p}\right)=1$ in the second equality.

- Assume $n+s$ even. If $g(\alpha^{-1}\beta)=0$, then we have

$$wt(\tilde{c}_{\alpha,\beta}) = p^n - p^{n-1} - \epsilon p^{\frac{n+s-2}{2}}(p-1).$$

If $g(\alpha^{-1}\beta)\neq 0$, we have $\sum_{\omega\in\mathbb{F}_p^\star}\xi_p^{\alpha\omega g(\alpha^{-1}\beta)}=-1$ since $\sum_{j=0}^{p-1}x^j$ is the minimal polynomial of ξ_p over $\mathbb{Q}$. Hence, we have $wt(\tilde{c}_{\alpha,\beta})=p^n-p^{n-1}+\epsilon p^{\frac{n+s-2}{2}}$.

The following theorem collects the Hamming weights of the codewords of $\mathcal{C}_{\psi_1}$.

Theorem 6.8. *Let $\mathcal{C}_{\psi_1}$ be the linear p-ary code defined by* (6.11). *Assume that ψ_1 in (6.12) is weakly regular p-ary s-plateaued with $0\le s\le n-2$ for $n\ge 2$. Then, for all $\alpha\in\mathbb{F}_p$ and $\beta\in\mathbb{F}_{p^n}$, the Hamming weights of $\tilde{c}_{\alpha,\beta}$ are given as follows.*

For $\alpha=0$, we have $wt(\tilde{c}_{0,0})=0$ and $wt(\tilde{c}_{0,\beta})=p^n-p^{n-1}$ for $\beta\neq 0$.
For $\alpha\in\mathbb{F}_p^\star$ and $\beta\in\mathbb{F}_{p^n}$,
if $(\alpha,\beta)\in\mathcal{Z}(\widehat{\chi_{\psi_1}})$, i.e., $\alpha^{-1}\beta\notin\mathrm{Supp}(\widehat{\chi_{\psi_1}})$, then we get $wt(\tilde{c}_{\alpha,\beta})=p^n-p^{n-1}$,
if $(\alpha,\beta)\in\mathcal{S}(\widehat{\chi_{\psi_1}})$, i.e., $\alpha^{-1}\beta\in\mathrm{Supp}(\widehat{\chi_{\psi_1}})$, then

- *when $n+s$ is odd,*

$$wt(\tilde{c}_{\alpha,\beta}) = \begin{cases} p^n - p^{n-1}, & \text{if } g(\alpha^{-1}\beta)=0,\\ p^n - p^{n-1} - \epsilon\left(\tfrac{-1}{p}\right)^{\frac{n+s+1}{2}}p^{\frac{n+s-1}{2}}\left(\tfrac{g(\alpha^{-1}\beta)}{p}\right), & \text{if } g(\alpha^{-1}\beta)\in\mathbb{F}_p^\star,\end{cases}$$

- *when $n+s$ is even,*

$$wt(\tilde{c}_{\alpha,\beta}) = \begin{cases} p^n - p^{n-1} - \epsilon(p-1)p^{\frac{n+s-2}{2}}, & \text{if } g(\alpha^{-1}\beta) = 0, \\ p^n - p^{n-1} + \epsilon p^{\frac{n+s-2}{2}}, & \text{if } g(\alpha^{-1}\beta) \in \mathbb{F}_p^\star, \end{cases}$$

where $\epsilon = \pm 1$ and g is a p-ary function over $\mathrm{Supp}(\widehat{\chi_{\psi_1}})$ by (6.14) and α^{-1} is the multiplicative inverse of $\alpha \in \mathbb{F}_p^\star$.

Our next aim is to determine the weight distributions of the constructed code $\mathcal{C}_{\psi_1}$ given in Theorem 6.8. To do this, we need to compute the number of $\omega \in \mathrm{Supp}(\widehat{\chi_{\psi_1}})$ such that $g(\omega) = j$ for all $j \in \mathbb{F}_p$. Set

$$\mathcal{N}_g(j) := \#\{\omega \in \mathrm{Supp}(\widehat{\chi_{\psi_1}}) : g(\omega) = j\}. \tag{6.15}$$

Since $\#\mathrm{Supp}(\widehat{\chi_{\psi_1}}) = p^{n-s}$, we have

$$\sum_{j=0}^{p-1} \mathcal{N}_g(j) = p^{n-s}. \tag{6.16}$$

Remark 6.9. If g is balanced over $\mathrm{Supp}(\widehat{\chi_{\psi_1}})$, $\mathcal{N}_g(j) = p^{n-s-1}$ for all $j \in \mathbb{F}_p$.

If g is unbalanced over $\mathrm{Supp}(\widehat{\chi_{\psi_1}})$, the following proposition allows us to compute the $\mathcal{N}_g(j)$ for all $j \in \mathbb{F}_p$. By Lemma 6.3, we have

$$\sum_{\omega \in \mathrm{Supp}(\widehat{\chi_{\psi_1}})} \xi_p^{g(\omega)+\mathrm{Tr}_p^{p^n}(\omega x)} = \epsilon v p^{\frac{n-s}{2}} \xi_p^{\psi_1(x)}, \tag{6.17}$$

where $\epsilon = \pm 1$ denotes the sign of $\widehat{\chi_{\psi_1}}$ and $v \in \{1, i\}$ in $\mathbb{C}$.

Proposition 6.12. *Under the above notations and the assumption that g is unbalanced over $\mathrm{Supp}(\widehat{\chi_{\psi_1}})$, we have the following. If $n-s$ is even, then*

$$\mathcal{N}_g(j) = \begin{cases} p^{n-s-1} + \epsilon p^{\frac{n-s-2}{2}}(p-1), & j = 0, \\ p^{n-s-1} - \epsilon p^{\frac{n-s-2}{2}}, & j \in \mathbb{F}_p^\star. \end{cases}$$

If $n-s$ is odd, then

$$\mathcal{N}_g(j) = \begin{cases} p^{n-s-1}, & j = 0, \\ p^{n-s-1} + \epsilon p^{\frac{n-s-1}{2}} \left(\frac{j}{p}\right), & j \in \mathbb{F}_p^\star, \end{cases}$$

where $\epsilon = \pm 1$ is the sign of $\widehat{\chi_{\psi_1}}$.

Proof. By (6.17), for $x = 0$ we have

$$\sum_{\omega \in \mathrm{Supp}(\widehat{\chi_{\psi_1}})} \xi_p^{g(\omega)} = \epsilon v p^{\frac{n-s}{2}} \xi_p^{\psi_1(0)},$$

equivalently,

$$\sum_{j=0}^{p-1} \mathcal{N}_g(j) \xi_p^j = \epsilon v p^{\frac{n-s}{2}},$$

where we used $\psi_1(0) = 0$. Hence, we have

$$\sum_{j=0}^{p-1} \mathcal{N}_g(j) \xi_p^j - \epsilon v p^{\frac{n-s}{2}} = 0. \tag{6.18}$$

If $n-s$ is even, then $v = 1$ by (6.1). Because $\sum_{j=0}^{p-1} x^j$ is the minimal polynomial of ξ_p over $\mathbb{Q}$, then for all $j \in \mathbb{F}_p^\star$ we have

$$\mathcal{N}_g(j) = a, \text{ and } \mathcal{N}_g(0) = a + \epsilon p^{\frac{n-s}{2}}$$

for some constant a. By (6.16), we get $a + \epsilon p^{\frac{n-s}{2}} + (p-1)a = p^{n-s}$ from which we deduce that $a = p^{n-s-1} - \epsilon p^{\frac{n-s}{2}-1}$.

If $n-s$ is odd, then $v = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 4, \\ i, & \text{if } p \equiv 3 \pmod 4. \end{cases}$

Recall the well-known identity: (see, e.g., [50])

$$\sum_{j=0}^{p-1} \left(\frac{j}{p}\right) \xi_p^j = \begin{cases} \sqrt{p}; & \text{if } p \equiv 1 \pmod 4, \\ i\sqrt{p}, & \text{if } p \equiv 3 \pmod 4, \end{cases}$$

that is, $\sum_{j=0}^{p-1} \left(\frac{j}{p}\right) \xi_p^j = v\sqrt{p}$. Thus, (6.18) can be rewritten as

$$\sum_{j=0}^{p-1} \mathcal{N}_g(j) \xi_p^j - \epsilon p^{\frac{n-s-1}{2}} \sum_{j=0}^{p-1} \left(\frac{j}{p}\right) \xi_p^j = 0;$$

equivalently,

$$\sum_{j=0}^{p-1} \xi_p^j \left(\mathcal{N}_g(j) - \epsilon p^{\frac{n-s-1}{2}} \left(\frac{j}{p}\right) \right) = 0.$$

Then for all $j \in \mathbb{F}_p^\star$, we have $\mathcal{N}_g(j) = \mathcal{N}_g(0) + \epsilon p^{\frac{n-s-1}{2}} \left(\frac{j}{p}\right)$. By (6.16), we obtain

$$\sum_{j=0}^{p-1} \mathcal{N}_g(j) = p\mathcal{N}_g(0) + \epsilon p^{\frac{n-s-1}{2}} \sum_{j=0}^{p-1} \left(\frac{j}{p}\right) = p^{n-s}.$$

Thus, since $\sum_{j=0}^{p-1} \left(\frac{j}{p}\right) = 0$, we get $\mathcal{N}_g(0) = p^{n-s-1}$. Hence, the proof is complete. □

In the light of Remark 6.9 and Proposition 6.12, we can determine the weight distributions of the constructed linear code given in Theorem 6.8. We investigate separately the case $n+s$ is an even integer and the case $n+s$ is an odd integer.

Theorem 6.9. *Let $\mathcal{C}_{\psi_1}$ be the linear p-ary code defined by* (6.11). *Assume that ψ_1 in (6.12) is a weakly regular p-ary s-plateaued, where $n+s$ is an even integer with $0 \le s \le n-2$ for $n \ge 2$. Then, the Hamming weights of the codewords and the weight distributions of the linear $[p^n-1, n+1]_p$ code $\mathcal{C}_{\psi_1}$ are as in Tables 6.4 and 6.5 if g is unbalanced and balanced over* $\mathrm{Supp}(\widehat{\chi_{\psi_1}})$, *respectively, where $\epsilon = \pm 1$ is the sign of $\widehat{\chi_{\psi_1}}$.*

Hamming weight w	Multiplicity A_w
0	1
$p^n - p^{n-1}$	$p^{n+1} - p^{n-s}(p-1) - 1$
$p^n - p^{n-1} - \epsilon(p-1)p^{\frac{n+s-2}{2}}$	$p^{n-s-1}(p-1) + \epsilon p^{\frac{n-s-2}{2}}(p-1)^2$
$p^n - p^{n-1} + \epsilon p^{\frac{n+s-2}{2}}$	$(p^{n-s} - p^{n-s-1})(p-1) - \epsilon p^{\frac{n-s-2}{2}}(p-1)^2$

Table 6.4: The Hamming weights of the codewords and the weight distribution of $\mathcal{C}_{\psi_1}$ when p is odd and $n+s$ is even for unbalanced g

Hamming weight w	Multiplicity A_w
0	1
$p^n - p^{n-1}$	$p^{n+1} - p^{n-s}(p-1) - 1$
$p^n - p^{n-1} - \epsilon(p-1)p^{\frac{n+s-2}{2}}$	$p^{n-s-1}(p-1)$
$p^n - p^{n-1} + \epsilon p^{\frac{n+s-2}{2}}$	$(p^{n-s} - p^{n-s-1})(p-1)$

Table 6.5: The Hamming weights of the codewords and the weight distribution of $\mathcal{C}_{\psi_1}$ when p is odd and $n+s$ is even for balanced g

Proof. By Theorem 6.8, the numbers of codewords with Hamming weight 0 and of Hamming weight $p^n - p^{n-1}$ are equal respectively to 1 and $p^n - 1 + \#\mathcal{Z}(\widehat{\chi_{\psi_1}}) = p^{n+1} + p^{n-s} - p^{n-s+1} - 1$. We now determine the weight distribution of $\mathcal{C}_{\psi_1}$ for

$(\alpha,\beta) \in \mathcal{S}(\widehat{\chi_{\psi_1}})$, i.e., $\alpha^{-1}\beta \in \mathrm{Supp}(\widehat{\chi_{\psi_1}})$. Set

$$\begin{aligned} \mathcal{Z}(g) &:= \{(\alpha,\beta) \in \mathcal{S}(\widehat{\chi_{\psi_1}}) : g(\alpha^{-1}\beta) = 0\}, \\ \mathcal{S}(g) &:= \{(\alpha,\beta) \in \mathcal{S}(\widehat{\chi_{\psi_1}}) : g(\alpha^{-1}\beta) \neq 0\}. \end{aligned} \tag{6.19}$$

By Lemma 6.4, we have $\#\mathcal{Z}(g) = (p-1)\mathcal{N}_g(0)$ and $\#\mathcal{S}(g) = (p-1)p^{n-s} - \#\mathcal{Z}(g)$. Assume that g is unbalanced over $\mathrm{Supp}(\widehat{\chi_{\psi_1}})$. Then, since $\mathcal{N}_g(0) = p^{n-s-1} + \epsilon p^{(n-s-2)/2}(p-1)$ by Proposition 6.12, we have

$$\#\mathcal{Z}(g) = p^{n-s-1}(p-1) + \epsilon p^{\frac{n-s-2}{2}}(p-1)^2,$$

and $\#\mathcal{S}(g) = (p^{n-s} - p^{n-s-1})(p-1) - \epsilon p^{(n-s-2)/2}(p-1)^2$. Hence, by Theorem 6.8, the numbers of codewords with Hamming weight $p^n - p^{n-1} - \epsilon(p-1)p^{(n+s-2)/2}$ and with Hamming weight $p^n - p^{n-1} + \epsilon p^{(n+s-2)/2}$ are equal to $\#\mathcal{Z}(g)$ and $\#\mathcal{S}(g)$, respectively. Hence, the proof of the first assertion is complete.

Assume that g is balanced over $\mathrm{Supp}(\widehat{\chi_{\psi_1}})$. By Remark 6.9, $\mathcal{N}_g(0) = p^{n-s-1}$, and so we have $\#\mathcal{Z}(g) = p^{n-s-1}(p-1)$ and $\#\mathcal{S}(g) = (p^{n-s} - p^{n-s-1})(p-1)$. Hence, as in the first case, the second assertion follows. □

Remark 6.10. In Theorem 6.9, the minimum Hamming distance of $\mathcal{C}_{\psi_1}$ is given by

$$d = \begin{cases} p^n - p^{n-1} - (p-1)p^{\frac{n+s-2}{2}}, & \text{if } \epsilon = 1, \\ p^n - p^{n-1} - p^{\frac{n+s-2}{2}}, & \text{if } \epsilon = -1. \end{cases}$$

We now give a weakly regular 3-ary 1-plateaued function and a corresponding linear 3-ary code for $p = 3$ and $n = 3$.

Example 6.4. *Let $\Psi : \mathbb{F}_{3^3} \to \mathbb{F}_{3^3}$ be the map defined by $\Psi(x) = \zeta^{22}x^{13} + \zeta^7 x^4 + \zeta x^2$, where $\mathbb{F}_{3^3}^\star = \langle\zeta\rangle$ with $\zeta^3 + 2\zeta + 1 = 0$. The function $\psi_1(x) = \mathrm{Tr}_3^{3^3}(\Psi(x))$ is the weakly regular 3-ary 1-plateaued with*

$$\widehat{\chi_{\psi_1}}(\omega) \in \{0, -9\xi_3^{g(\omega)}\}$$

for all $\omega \in \mathbb{F}_{3^3}$, where g is the unbalanced 3-ary function. Then, the set $\mathcal{C}_{\psi_1}$ in (6.11) is the three-weight linear 3-ary code with parameters $[26, 4, 15]_3$, weight enumerator $1 + 16y^{15} + 62y^{18} + 2y^{24}$ and weight distribution $(1, 16, 62, 2)$. Hence, the Hamming weights of the codewords and the weight distribution of $\mathcal{C}_{\psi_1}$ are as in Table 6.6.

Hamming weight w	Multiplicity A_w
0	1
18	62
24	2
15	16

Table 6.6: The Hamming weights of the codewords and the weight distribution of $\mathcal{C}_{\psi_1}$ when $p = 3$, $n = 3$ and $s = 1$.

The following theorem determines the weight distributions of the constructed linear code given in Theorem 6.8 when $n + s$ is an odd integer.

Theorem 6.10. *Let $\mathcal{C}_{\psi_1}$ be the linear p-ary code defined by* (6.11). *Assume that ψ_1 in (6.12) is a weakly regular p-ary s-plateaued, where $n + s$ is an odd integer with $0 \leq s \leq n - 1$. Then, the Hamming weights of the codewords and the weight distributions of $[p^n - 1, n+1]_p$ code $\mathcal{C}_{\psi_1}$ are as in Tables 6.7 and 6.8 if g is unbalanced and balanced over* $\mathrm{Supp}(\widehat{\chi_{\psi_1}})$, *respectively, where $\epsilon = \pm 1$ is the sign of $\widehat{\chi_{\psi_1}}$ and $\eta = \left(\frac{-1}{p}\right)^{\frac{n+s+1}{2}} = \pm 1$.*

Hamming weight w	Multiplicity A_w
0	1
$p^n - p^{n-1}$	$p^{n+1} - p^{n-s-1}(p-1)^2 - 1$
$p^n - p^{n-1} - \epsilon\eta p^{\frac{n+s-1}{2}}$	$\frac{1}{2}(p^{n-s-1} + \epsilon p^{\frac{n-s-1}{2}})(p-1)^2$
$p^n - p^{n-1} + \epsilon\eta p^{\frac{n+s-1}{2}}$	$\frac{1}{2}(p^{n-s-1} - \epsilon p^{\frac{n-s-1}{2}})(p-1)^2$

Table 6.7: The Hamming weights of the codewords and the weight distribution of $\mathcal{C}_{\psi_1}$ when p and $n + s$ are odd for unbalanced g

Hamming weight w	Multiplicity A_w
0	1
$p^n - p^{n-1}$	$p^{n+1} - p^{n-s-1}(p-1)^2 - 1$
$p^n - p^{n-1} - \epsilon\eta p^{\frac{n+s-1}{2}}$	$\frac{1}{2}p^{n-s-1}(p-1)^2$
$p^n - p^{n-1} + \epsilon\eta p^{\frac{n+s-1}{2}}$	$\frac{1}{2}p^{n-s-1}(p-1)^2$

Table 6.8: The Hamming weights of the codewords and the weight distribution of $\mathcal{C}_{\psi_1}$ when p and $n + s$ are odd for balanced g

Proof. Recall that the set $\mathcal{Z}(g)$ and the value $\mathcal{N}_g(j)$ were defined in (6.19) and (6.15),

respectively. By Lemma 6.4, we have $\#\mathcal{Z}(g) = (p-1)\mathcal{N}_g(0)$, where $\mathcal{N}_g(0) = p^{n-s-1}$ (see Remark 6.9 and Proposition 6.12). Hence by Theorem 6.8, the number of codewords with Hamming weight $p^n - p^{n-1}$ is

$$p^n - 1 + \#\mathcal{Z}(\widehat{\chi_{\psi_1}}) + \#\mathcal{Z}(g) = p^{n+1} + 2p^{n-s} - p^{n-s+1} - p^{n-s-1} - 1.$$

Moreover, the number of codewords with Hamming weight $p^n - p^{n-1} - \epsilon\eta p^{(n+s-1)/2}$ and of Hamming weight $p^n - p^{n-1} + \epsilon\eta p^{(n+s-1)/2}$ is equal respectively to

$$\sum_{j\in\{1,\ldots,p-1\},\left(\frac{j}{p}\right)=1} (p-1)\mathcal{N}_g(j)$$

and

$$\sum_{j\in\{1,\ldots,p-1\},\left(\frac{j}{p}\right)=-1} (p-1)\mathcal{N}_g(j).$$

If g is unbalanced, then by Proposition 6.12, respectively to:

$$\sum_{j\in\{1,\ldots,p-1\},\left(\frac{j}{p}\right)=1} (p-1)(p^{n-s-1} + \epsilon p^{\frac{n-s-1}{2}}) = \frac{(p-1)^2}{2}(p^{n-s-1} + \epsilon p^{\frac{n-s-1}{2}})$$

and

$$\sum_{j\in\{1,\ldots,p-1\},\left(\frac{j}{p}\right)=-1} (p-1)(p^{n-s-1} - \epsilon p^{\frac{n-s-1}{2}}) = \frac{(p-1)^2}{2}(p^{n-s-1} - \epsilon p^{\frac{n-s-1}{2}}).$$

If g is balanced, then by Remark 6.9, respectively to: $\frac{(p-1)^2}{2}p^{n-s-1}$ and $\frac{(p-1)^2}{2}p^{n-s-1}$. The proof is complete. □

Remark 6.11. In Theorem 6.10, the minimum Hamming distance of $\mathcal{C}_{\psi_1}$ is given by $d = p^n - p^{n-1} - p^{\frac{n+s-1}{2}}$. Its multiplicity depends on the values $\epsilon = \pm 1$ and $\eta = \pm 1$ in the case of unbalanced g.

Remark 6.12. If we assume only the weakly regular bent-ness in this section, then we can obviously recover the results given in [58] by Mesnager. Therefore, this section can be viewed as an extension of [58] to the notion of weakly regular plateaued functions.

6.4 Secret Sharing Schemes from the Constructed Linear Codes

In this section, we investigate the access structures of the secret sharing schemes based on the dual codes of the constructed linear codes from plateaued functions.

Remark 6.13. In the light of the results given in Section 2.7.2, the construction of linear codes all of whose nonzero codewords are minimal has a significant importance. Such linear codes generate secret sharing schemes with "nice" access structures.

Below, we first show that all nonzero codewords of the constructed linear codes are minimal for almost all cases (in the light of Lemma 2.7) and then describe the access structures of the secret sharing schemes based on the dual codes (in the light of Theorem 2.2). We consider separately the linear codes $\mathcal{C}_{\psi_1}$ given in Theorems 6.7, 6.9 and 6.10.

The Constructed Binary Linear Code in Theorem 6.7. The following theorem shows that all nonzero codewords of the constructed binary linear code from plateaued Boolean function are minimal for almost all cases.

Theorem 6.11. *Let $\mathcal{C}_{\psi_1}$ be the binary linear $[2^n-1, n+1, 2^{n-1}-2^{(n+s-2)/2}]$ code given in Theorem 6.7. Then, all nonzero codewords of $\mathcal{C}_{\psi_1}$ are minimal for $n \geq 4$ and $0 \leq s \leq n-4$.*

Proof. From Table 6.2, we have $w_{\min} = 2^{n-1} - 2^{(n+s-2)/2}$ and $w_{\max} = 2^{n-1} + 2^{(n+s-2)/2}$. For $0 \leq s \leq n-4$ and $n \geq 4$, we get

$$\frac{1}{2} < \frac{w_{\min}}{w_{\max}} = \frac{2^{n-1} - 2^{(n+s-2)/2}}{2^{n-1} + 2^{(n+s-2)/2}}$$

since $3 \cdot 2^{(n+s)/2} < 2^n$. Hence, by Lemma 2.7, all nonzero codewords of $\mathcal{C}_{\psi_1}$ are minimal for $n \geq 4$ and $0 \leq s \leq n-4$. □

The following corollary identifies the access structure of the secret sharing scheme based on the dual code of the constructed binary linear code.

Corollary 6.4. *Let $\mathcal{C}_{\psi_1}$ be the binary linear $[2^n-1, n+1, 2^{n-1}-2^{(n+s-2)/2}]$ code given in Theorem 6.7 and let $G = [\mathbf{g}_0, \mathbf{g}_1, \ldots, \mathbf{g}_{2^n-2}]$ be its generator matrix. Let $\mathcal{C}_{\psi_1}^{\perp}$ be its dual $[2^n-1, 2^n-n-2, d^{\perp}]$ code, where $d^{\perp}$ denotes the minimum Hamming distance of $\mathcal{C}_{\psi_1}^{\perp}$. Assume $n \geq 4$ and $0 \leq s \leq n-4$. In the secret sharing scheme based on $\mathcal{C}_{\psi_1}^{\perp}$:*

- *The number of participants is 2^n-2, and there exist 2^n minimal access sets.*

- *If $d^{\perp} = 2$, the access structure is given as follows: If $\mathbf{g}_i$, $1 \leq i \leq 2^n - 2$, is a multiple of $\mathbf{g}_0$, then P_i must be in all minimal access sets; otherwise, P_i must be in 2^{n-1} out of 2^n minimal access sets.*

- *If $d^{\perp} \geq 3$, for any fixed $1 \leq t \leq \min\{n, d^{\perp} - 2\}$, every set of t participants is involved in 2^{n-t} out of 2^n minimal access sets.*

Proof. By Theorem 6.11, every nonzero codeword of $\mathcal{C}_{\psi_1}$ is minimal for $n \geq 4$ and $0 \leq s \leq n-4$. Hence, the desired results follow directly from Theorem 2.2. □

The Constructed Linear p-Ary Code in Theorem 6.9. We now prove that all nonzero codewords of the constructed linear p-ary codes from weakly regular plateaued functions are minimal for almost all cases. There are two cases: $\epsilon = 1$ and $\epsilon = -1$.

Theorem 6.12. *Let $\mathcal{C}_{\psi_1}$ be the linear $[p^n - 1, n+1, p^n - p^{n-1} - (p-1)p^{(n+s-2)/2}]_p$ p-ary code given in Theorem 6.9 for $\epsilon = 1$. Then all nonzero codewords of $\mathcal{C}_{\psi_1}$ are minimal for $n \geq 4$ and $0 \leq s \leq n-4$.*

Proof. For $\epsilon = 1$, we have $w_{\min} = p^n - p^{n-1} - (p-1)p^{(n+s-2)/2}$ and $w_{\max} = p^n - p^{n-1} + p^{(n+s-2)/2}$. The inequality

$$\frac{p-1}{p} < \frac{w_{\min}}{w_{\max}} = \frac{p^n - p^{n-1} - (p-1)p^{(n+s-2)/2}}{p^n - p^{n-1} + p^{(n+s-2)/2}}$$

can be reduced to $(p+1)p^{(n+s)/2} < p^n$. If $n \geq 4$ and $0 \leq s \leq n-4$, clearly we have $(p+1)p^{(n+s)/2} < p^n$ for an odd prime p. By Lemma 2.7, all nonzero codewords of $\mathcal{C}_{\psi_1}$ are minimal for $n \geq 4$ and $0 \leq s \leq n-4$. □

We describe the access structure of the secret sharing scheme based on the dual code of the constructed linear p-ary code.

Corollary 6.5. *Let $\mathcal{C}_{\psi_1}$ be the linear $[p^n - 1, n+1, p^n - p^{n-1} - (p-1)p^{(n+s-2)/2}]_p$ p-ary code given in Theorem 6.9, and let $G = [\mathbf{g}_0, \mathbf{g}_1, \ldots, \mathbf{g}_{p^n-2}]$ be its generator matrix. Let $\mathcal{C}_{\psi_1}^{\perp}$ be its dual $[p^n - 1, p^n - n - 2, d^{\perp}]_p$ code, where $d^{\perp}$ denotes the minimum Hamming distance of $\mathcal{C}_{\psi_1}^{\perp}$. Assume $n \geq 4$ and $0 \leq s \leq n-4$. In the secret sharing scheme based on $\mathcal{C}_{\psi_1}^{\perp}$:*

- *The number of participants is $p^n - 2$, and there exist p^n minimal access sets.*
- *If $d^\perp = 2$, the access structure is given as follows: If $\mathbf{g}_i$, $1 \le i \le p^n - 2$, is a multiple of $\mathbf{g}_0$, then P_i must be in all minimal access sets; otherwise, P_i must be in $(p-1)p^{n-1}$ out of p^n minimal access sets.*
- *If $d^\perp \ge 3$, for any fixed $1 \le t \le \min\{n, d^\perp - 2\}$, every set of t participants is involved in $(p-1)^t p^{n-t}$ out of p^n minimal access sets.*

Proof. By Theorem 6.12, every nonzero codeword of $\mathcal{C}_{\psi_1}$ is minimal for $n \ge 4$ and $0 \le s \le n-4$. Hence, the desired results follow directly from Theorem 2.2. □

Theorem 6.13. *Let $\mathcal{C}_{\psi_1}$ be the linear $[p^n-1, n+1, p^n-p^{n-1}-p^{(n+s-2)/2}]_p$ p-ary code given in Theorem 6.9 for $\epsilon = -1$. Then all nonzero codewords of $\mathcal{C}_{\psi_1}$ are minimal for $n \ge 4$ and $0 \le s \le n-4$.*

Proof. For $\epsilon = -1$, we have $w_{\min} = p^n - p^{n-1} - p^{(n+s-2)/2}$ and $w_{\max} = p^n - p^{n-1} + (p-1)p^{(n+s-2)/2}$. As in the proof of Theorem 6.12, for $n \ge 4$ and $0 \le s \le n-4$, we have

$$\frac{p-1}{p} < \frac{w_{\min}}{w_{\max}} = \frac{p^n - p^{n-1} - p^{(n+s-2)/2}}{p^n - p^{n-1} + (p-1)p^{(n+s-2)/2}}$$

since $(p^2-p+1)p^{(n+s)/2} < p^n(p-1)$. Hence, by Lemma 2.7, all nonzero codewords of $\mathcal{C}_{\psi_1}$ are minimal for $n \ge 4$ and $0 \le s \le n-4$. □

Similarly, the following corollary describes the corresponding access structure.

Corollary 6.6. *Let $\mathcal{C}_{\psi_1}$ be the linear $[p^n - 1, n+1, p^n - p^{n-1} - p^{(n+s-2)/2}]_p$ p-ary code given in Theorem 6.9, and let $G = [\mathbf{g}_0, \mathbf{g}_1, \ldots, \mathbf{g}_{p^n-2}]$ be its generator matrix. Let $\mathcal{C}_{\psi_1}^\perp$ be its dual $[p^n - 1, p^n - n - 2, d^\perp]_p$ code, where $d^\perp$ denotes the minimum Hamming distance of $\mathcal{C}_{\psi_1}^\perp$. Assume $n \ge 4$ and $0 \le s \le n-4$. In the secret sharing scheme based on $\mathcal{C}_{\psi_1}^\perp$:*

- *The number of participants is $p^n - 2$, and there exist p^n minimal access sets.*
- *If $d^\perp = 2$, the access structure is given as follows: If $\mathbf{g}_i$, $1 \le i \le p^n - 2$, is a multiple of $\mathbf{g}_0$, then P_i must be in all minimal access sets; otherwise, P_i must be in $(p-1)p^{n-1}$ out of p^n minimal access sets.*

- *If $d^{\perp} \geq 3$, for any fixed $1 \leq t \leq \min\{n, d^{\perp} - 2\}$, every set of t participants is involved in $(p-1)^t p^{n-t}$ out of p^n minimal access sets.*

Proof. By Theorem 6.13, every nonzero codeword of $\mathcal{C}_{\psi_1}$ is minimal for $n \geq 4$ and $0 \leq s \leq n-4$. Hence, the desired results follow directly from Theorem 2.2. □

The Constructed Linear p-Ary Code in Theorem 6.10. The following theorem proves that all nonzero codewords of the constructed linear p-ary code from weakly regular plateaued function are minimal for almost all cases.

Theorem 6.14. *Let $\mathcal{C}_{\psi_1}$ be the linear $[p^n-1, n+1, p^n-p^{n-1}-p^{(n+s-1)/2}]_p$ p-ary code given in Theorem 6.10. Then all nonzero codewords of $\mathcal{C}_{\psi_1}$ are minimal for $n \geq 3$ and $0 \leq s \leq n-3$.*

Proof. There are two cases: $\epsilon = \eta$ and $\epsilon = -\eta$. For both values of $\epsilon\eta = \pm 1$, we have that $w_{\min} = p^n - p^{n-1} - p^{(n+s-1)/2}$ and $w_{\max} = p^n - p^{n-1} + p^{(n+s-1)/2}$. Then the inequality

$$\frac{p-1}{p} < \frac{w_{\min}}{w_{\max}} = \frac{p^n - p^{n-1} - p^{(n+s-1)/2}}{p^n - p^{n-1} + p^{(n+s-1)/2}},$$

can be reduced to $(2p-1)p^{(n+s+1)/2} < p^n(p-1)$. If $n \geq 3$ and $0 \leq s \leq n-3$, we can easily show this inequality for an odd prime p. Hence, by Lemma 2.7, all nonzero codewords of $\mathcal{C}_{\psi_1}$ are minimal for $n \geq 3$ and $0 \leq s \leq n-3$. □

The following corollary describes the access structure of the secret sharing scheme based on the dual code of the linear p-ary code.

Corollary 6.7. *Let $\mathcal{C}_{\psi_1}$ be the linear $[p^n-1, n+1, p^n-p^{n-1}-p^{(n+s-1)/2}]_p$ p-ary code given in Theorem 6.10, and let $G = [\mathbf{g}_0, \mathbf{g}_1, \ldots, \mathbf{g}_{p^n-2}]$ be its generator matrix. Let $\mathcal{C}_{\psi_1}^{\perp}$ be its dual $[p^n-1, p^n-n-2, d^{\perp}]_p$ code, where $d^{\perp}$ denotes the minimum Hamming distance of $\mathcal{C}_{\psi_1}^{\perp}$. Assume $n \geq 3$ and $0 \leq s \leq n-3$. In the secret sharing scheme based on $\mathcal{C}_{\psi_1}^{\perp}$:*

- *The number of participants is $p^n - 2$, and there exist p^n minimal access sets.*

- *If $d^{\perp} = 2$, the access structure is given as follows: If $\mathbf{g}_i$, $1 \leq i \leq p^n - 2$, is a multiple of $\mathbf{g}_0$, then P_i must be in all minimal access sets; otherwise, P_i must be in $(p-1)p^{n-1}$ out of p^n minimal access sets.*
- *If $d^{\perp} \geq 3$, for any fixed $1 \leq t \leq \min\{n, d^{\perp} - 2\}$, every set of t participants is involved in $(p-1)^t p^{n-t}$ out of p^n minimal access sets.*

Proof. By Theorem 6.14, every nonzero codeword of $\mathcal{C}_{\psi_1}$ is minimal for $n \geq 3$ and $0 \leq s \leq n-3$. Hence, the desired results follow directly from Theorem 2.2. □

Remark 6.14. Consequently we obtained linear codes $\mathcal{C}_{\psi_1}$ all of whose nonzero codewords are minimal if $n \geq 4$ and $0 \leq s \leq n-4$. Hence, the secret sharing schemes based on the dual codes $\mathcal{C}_{\psi_1}^{\perp}$ have "nice" access structures given in Theorem 2.2.

CHAPTER 7

CONCLUSION

Bent and plateaued functions have attracted attention since their introduction in the literature due to their role in diverse domains of Boolean and vectorial functions for sequences and cryptography like correlation immune functions and orthogonal arrays (since the order of resiliency and nonlinearity is strongly bounded only by plateaued functions), APN functions and substitution-boxes (since plateaued APN functions in odd dimension are almost bent), and because, like partially-bent functions, they represent a natural class for generalizing at the same time bent functions and quadratic functions, but they form a larger class than partially-bent functions, also including all semi-bent and near-bent functions. However, their structure is still complicated to characterize and, little is known about these functions already in characteristic 2 and still more in arbitrary characteristic. In view of given their importance, it is worth noting that they have not been studied in detail in a general framework. In this thesis, we brought out further new results on plateaued functions in arbitrary characteristic, with the aim of handling the plateaued-ness property of functions and getting various tools for their future construction.

The main objectives of this thesis are to bring further results on the characterization of plateaued (vectorial) functions, and to construct linear codes from weakly regular plateaued functions, in arbitrary characteristic. We hope that this thesis has reduced to a degree the gap between the interest of the notion of plateaued function and what is known on it.

To sum up, the contributions of this thesis are explicitly given as follows.

In Chapter 3, we obtained a large number of characterizations of bent and plateaued functions in terms of their Walsh power moments, second-order derivatives and autocorrelation functions. We next provided several characterizations of vectorial bent and plateaued functions by using the value distributions of their derivatives, and Walsh power moments and autocorrelation functions of their nonzero component functions. We believe that these characterizations are considerably useful to understand the structure of these functions and to design such functions in arbitrary characteristic. We hope that these characterizations will pave the way to construct new plateaued functions. Actually, using one of these characterizations, we observed the non-existence of a homogeneous cubic bent function (and a (homogeneous) cubic plateaued function for some cases) in odd characteristic.

In Chapter 4, we first showed the non-existence of a function whose absolute Walsh transform takes exactly three distinct values (one being is zero), and next introduced a new class of functions whose absolute Walsh transform takes exactly four distinct values (one being is zero).

In Chapter 5, we first redefined the notions of partially bent and plateaued functions over $\mathbb{F}_q$, with q a prime power. Next we gave a concrete example of a 4-ary plateaued, but not vectorial plateaued Boolean function. Moreover, we provided a large number of characterizations of q-ary partially bent and q-ary plateaued functions in terms of their derivatives, Walsh power moments and autocorrelation functions.

In Chapter 6, we obtained a new class of three-weight binary linear codes from plateaued Boolean functions with their weight distributions. In odd characteristic, we introduced the notion of (non)-weakly regular plateaued functions, and then provide the secondary and recursive constructions of these functions. Next, we made use of weakly regular plateaued functions to construct three-weight linear codes and then determined the weight distributions of the constructed linear codes. This is the first time construction of linear codes from weakly regular plateaued functions in odd characteristic. They are inequivalent to the known ones (since there is no linear code with obtained parameters) in the literature as far as we know. We finally analyzed the constructed linear codes for secret sharing schemes, and thereby described the access structures of the secret sharing schemes based on the dual codes of these codes.

REFERENCES

[1] R. Anderson, C. Ding, T. Helleseth, and T. Klove. How to build robust shared control systems. *Designs, Codes and Cryptography*, 15(2):111–124, 1998.

[2] A. Ashikhmin and A. Barg. Minimal vectors in linear codes. *IEEE Transactions on Information Theory*, 44(5):2010–2017, 1998.

[3] A. Ashikhmin, A. Barg, G. Cohen, and L. Huguet. Variations on minimal codewords in linear codes. *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, pages 96–105, 1995.

[4] G. R. Blakley. Safeguarding cryptographic keys. In *Proceedings of the national computer conference*, volume 48, pages 313–317, 1979.

[5] W. Bosma, J. Cannon, and C. Playoust. The magma algebra system i: The user language. *Journal of Symbolic Computation*, 24(3):235–265, 1997.

[6] L. Budaghyan. *Construction and Analysis of Cryptographic Functions*. Springer, 2015.

[7] E. Çakçak and F. Özbudak. Some artin–schreier type function fields over finite fields with prescribed genus and number of rational places. *Journal of Pure and Applied Algebra*, 210(1):113–135, 2007.

[8] E. Çakçak and F. Özbudak. Curves related to coulter's maximal curves. *Finite Fields and Their Applications*, 14(1):209–220, 2008.

[9] R. Calderbank and W. Kantor. The geometry of two-weight codes. *Bulletin of the London Mathematical Society*, 18(2):97–122, 1986.

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

[11] A. Canteaut, P. Charpin, and G. M. Kyureghyan. A new class of monomial bent functions. *Finite Fields and Their Applications*, 14(1):221–241, 2008.

[12] C. Carlet. Partially-bent functions. *Designs, Codes and Cryptography*, 3(2):135–145, 1993.

[13] C. Carlet. Boolean functions for cryptography and error correcting codes. *Boolean models and methods in mathematics, computer science, and engineering*, 2:257–397, 2010.

[14] C. Carlet. Vectorial boolean functions for cryptography. *Boolean models and methods in mathematics, computer science, and engineering*, 134:398–469, 2010.

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

[16] C. Carlet and C. Ding. Nonlinearities of s-boxes. *Finite fields and their applications*, 13(1):121–135, 2007.

[17] C. Carlet, C. Ding, and J. Yuan. Linear codes from perfect nonlinear mappings and their secret sharing schemes. *IEEE Transactions on Information Theory*, 51(6):2089–2102, 2005.

[18] C. Carlet and S. Dubuc. On generalized bent and q-ary perfect nonlinear functions. In *Finite Fields and Applications*, pages 81–94. Springer, 2001.

[19] C. Carlet and S. Mesnager. Four decades of research on bent functions. *Designs, Codes and Cryptography*, 78(1):5–50, 2016.

[20] C. Carlet, S. Mesnager, F. Özbudak, and A. Sınak. Explicit characterizations for plateaued-ness of p-ary (vectorial) functions. In *Second International Conference on Codes, Cryptology and Information Security (C2SI-2017), In Honor of Claude Carlet*, pages 328–345. Springer, 2017.

[21] C. Carlet and E. Prouff. On plateaued functions and their constructions. In *FSE*, pages 54–73. Springer, 2003.

[22] A. Çesmelioglu, G. McGuire, and W. Meidl. A construction of weakly and non-weakly regular bent functions. *J. Comb. Theory, Ser. A*, 119(2):420–429, 2012.

[23] A. Çeşmelioğlu and W. Meidl. A construction of bent functions from plateaued functions. *Designs, codes and cryptography*, pages 1–12, 2013.

[24] A. Çesmelioglu, W. Meidl, and A. Pott. There are infinitely many bent functions for which the dual is not bent. *IEEE Trans. Information Theory*, 62(9):5204–5208, 2016.

[25] A. Çesmelioglu, W. Meidl, and A. Topuzoglu. Partially bent functions and their properties. Applied Algebra and Number Theory, 2014.

[26] G. Cohen and S. Mesnager. On constructions of semi-bent functions from bent functions. *Journal Contemporary Mathematics*, 625:141–154, 2014.

[27] G. D. Cohen, S. Mesnager, and A. Patey. On minimal and quasi-minimal linear codes. In *IMA International Conference on Cryptography and Coding*, pages 85–98. Springer, 2013.

[28] R. S. Coulter and R. W. Matthews. Bent polynomials over finite fields. *Bulletin of the Australian Mathematical Society*, 56(3):429–437, 1997.

[29] B. Courteau and J. Wolfmann. On triple-sum-sets and two or three weights codes. *Discrete Mathematics*, 50:179–191, 1984.

[30] J. F. Dillon. *Elementary Hadamard difference sets*. PhD thesis, 1974.

[31] C. Ding. A construction of binary linear codes from boolean functions. *Discrete mathematics*, 339(9):2288–2303, 2016.

[32] C. Ding and X. Wang. A coding theory construction of new systematic authentication codes. *Theoretical computer science*, 330(1):81–99, 2005.

[33] C. Ding and J. Yuan. Covering and secret sharing with linear codes. *DMTCS*, 2731:11–25, 2003.

[34] K. Ding and C. Ding. Binary linear codes with three weights. *IEEE Communications Letters*, 18(11):1879–1882, 2014.

[35] K. Ding and C. Ding. A class of two-weight and three-weight codes and their applications in secret sharing. *IEEE Transactions on Information Theory*, 61(11):5835–5842, 2015.

[36] T. Helleseth and A. Kholosha. Monomial and quadratic bent functions over the finite fields of odd characteristic. *IEEE Transactions on Information Theory*, 52(5):2018–2032, 2006.

[37] T. Helleseth and A. Kholosha. New binomial bent functions over the finite fields of odd characteristic. In *Information Theory Proceedings (ISIT), 2010 IEEE International Symposium on*, pages 1277–1281. IEEE, 2010.

[38] T. Helleseth and A. Kholosha. Bent functions and their connections to combinatorics. Chapter of Surveys in Combinatorics 2013, pages 91-126, 2013.

[39] X.-D. Hou. Cubic bent functions. *Discrete Mathematics*, 189(1-3):149–161, 1998.

[40] X.-D. Hou. q-ary bent functions constructed from chain rings. *Finite Fields and Their Applications*, 4(1):55–61, 1998.

[41] X.-D. Hou. p-ary and q-ary versions of certain results about bent functions and resilient functions. *Finite Fields and Their Applications*, 10(4):566–582, 2004.

[42] W. C. Huffman and V. Pless. *Fundamentals of error-correcting codes*. Cambridge university press, 2010.

[43] J. Y. Hyun, J. Lee, and Y. Lee. Explicit criteria for construction of plateaued functions. *IEEE Transactions on Information Theory*, 62(12):7555–7565, 2016.

[44] K. Ireland and M. Rosen. *A classical introduction to modern number theory*, volume 84. Springer Science & Business Media, 2013.

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

[46] P. V. Kumar, R. A. Scholtz, and L. R. Welch. Generalized bent functions and their properties. *Journal of Combinatorial Theory, Series A*, 40(1):90–107, 1985.

[47] X. Lai. Additive and linear structures of cryptographic functions. In *International Workshop on Fast Software Encryption*, pages 75–85. Springer, 1994.

[48] P. Langevin. On generalized bent functions. In *Eurocode'92*, pages 147–152. Springer, 1993.

[49] G. Leander and G. McGuire. Construction of bent functions from near-bent functions. *Journal of Combinatorial Theory, Series A*, 116(4):960–970, 2009.

[50] R. Lidl and H. Niederreiter. *Finite fields*, volume 20. Cambridge university press, 1997.

[51] J. L. Massey. Minimal codewords and secret sharing. In *Proceedings of the 6th joint Swedish-Russian international workshop on information theory*, pages 276–279, 1993.

[52] J. L. Massey. Some applications of coding theory in cryptography. *Codes and Ciphers: Cryptography and Coding IV*, pages 33–47, 1995.

[53] R. J. McEliece and D. V. Sarwate. On sharing secrets and reed-solomon codes. *Communications of the ACM*, 24(9):583–584, 1981.

[54] S. Mesnager. Semibent functions from dillon and niho exponents, kloosterman sums, and dickson polynomials. *IEEE Transactions on Information Theory*, 57(11):7443–7458, 2011.

[55] S. Mesnager. Characterizations of plateaued and bent functions in characteristic p. In *International Conference on Sequences and Their Applications*, pages 72–82. Springer, 2014.

[56] S. Mesnager. On semi-bent functions and related plateaued functions over the galois field. In *Open Problems in Mathematics and Computational Science*, pages 243–273. Springer, 2014.

[57] S. Mesnager. *Bent functions*. Springer, 2016.

[58] S. Mesnager. Linear codes with few weights from weakly regular bent functions based on a generic construction. *Cryptography and Communications*, 9(1):71–84, 2017.

[59] S. Mesnager, F. Özbudak, and A. Sınak. Characterizations of partially bent and plateaued functions over finite fields.

[60] S. Mesnager, F. Özbudak, and A. Sınak. A new class of three-weight linear codes from weakly regular plateaued functions. In *Proceedings of Extended Abstract of the tenth International Workshop on Coding and Cryptography (WCC)-2017, its full paper will be submitted to Designs, Codes and Cryptography.*

[61] S. Mesnager, F. Özbudak, and A. Sınak. Secondary constructions of (non)-weakly regular plateaued p-ary functions.

[62] S. Mesnager, F. Özbudak, and A. Sınak. Characterizations of plateaued functions in arbitrary characteristic. In *Proceedings of Abstract Book of the International Conference on Coding theory and Cryptography (ICCC)-2015*, 2015.

[63] S. Mesnager, F. Özbudak, and A. Sınak. Results on characterizations of plateaued functions in arbitrary characteristic. In *International Conference on Cryptography and Information Security in the Balkans*, pages 17–30. Springer, 2015.

[64] S. Mesnager, F. Özbudak, and A. Sınak. On the p-ary (cubic) bent and plateaued (vectorial) functions. *Designs, Codes and Cryptography*, pages 1–28, 2017.

[65] S. Mesnager, F. Özbudak, A. Sınak, and G. D. Cohen. On the q-ary plateaued functions and their explicit characterizations. *European Journal of Combinatorics*, 2017.

[66] G. L. Mullen and D. Panario. *Handbook of finite fields*. CRC Press, 2013.

[67] K. Nyberg. Perfect nonlinear s-boxes. In *Advances in Cryptology—EUROCRYPT'91*, pages 378–386. Springer, 1991.

[68] F. Özbudak and A. Pott. Non-extendable f_q-quadratic perfect nonlinear maps. In *Open Problems in Mathematics and Computational Science*, pages 91–110. Springer, 2014.

[69] E. Pasalic, N. Cepak, and Y. Wei. Infinite classes of vectorial plateaued functions, permutations and complete permutations. *Discrete Applied Mathematics*, 215:177–184, 2016.

[70] C. Qu, J. Seberry, and J. Pieprzyk. Homogeneous bent functions. *Discrete Applied Mathematics*, 102(1):133–139, 2000.

[71] A. Renvall and C. Ding. The access structure of some secret-sharing schemes. In *Information Security and Privacy*, pages 67–78. Springer, 1996.

[72] O. S. Rothaus. On "bent" functions. *Journal of Combinatorial Theory, Series A*, 20(3):300–305, 1976.

[73] W. Rudin et al. *Principles of mathematical analysis*, volume 3. McGraw-hill New York, 1964.

[74] A. Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.

[75] Y. Tan, J. Yang, and X. Zhang. A recursive construction of p-ary bent functions which are not weakly regular. In *Information Theory and Information Security (ICITIS), 2010 IEEE International Conference on*, pages 156–159. IEEE, 2010.

[76] 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):1166–1176, 2016.

[77] J. Yuan and C. Ding. Secret sharing schemes from three classes of linear codes. *IEEE Transactions on Information Theory*, 52(1):206–212, 2006.

[78] Y. Zheng and X.-M. Zhang. Plateaued functions. In *ICICS*, volume 99, pages 284–300. Springer, 1999.

[79] Y. Zheng and X.-M. Zhang. Relationships between bent functions and complementary plateaued functions. In *International Conference on Information Security and Cryptology*, pages 60–75. Springer, 1999.

[80] Z. Zhou, N. Li, C. Fan, and T. Helleseth. Linear codes with two or three weights from quadratic bent functions. *Designs, Codes and Cryptography*, 81(2):283–295, 2016.

CURRICULUM VITAE

PERSONAL INFORMATION

Surname, Name: Sınak, Ahmet
Nationality: Turkish
Date and Place of Birth: 05.07.1984, Manavgat
Marital Status: Single
Phone: +90 312 210 29 87
Fax: +90 312 210 29 85

EDUCATION

Degree	Institution	Year of Graduation
M.S., Cryptography	Middle East Technical University	2012
B.S., Economics	Anadolu University	2015
B.S., Mathematics	Muğla Sıtkı Koçman University	2009
High School	Serik Anatolian High School	2004

PROFESSIONAL EXPERIENCE

Year	Place	Enrollment
27.02.2012-going on	Middle East Technical University	Research Assistant
25.08.2011-24.02.2012	Necmettin Erbakan University	Research Assistant
20.12.2010-14.08.2011	Artvin Çoruh University	Research Assistant

PUBLICATIONS

International Journal Publications

- Mesnager, S., Özbudak, F., Sınak, A., Cohen, G.: On the q-ary Plateaued Functions over $\mathbb{F}_q$ and their Explicit Characterizations. European Journal of Combinatorics (EJC), Elsevier, in press, December 2017.

- Mesnager, S., Özbudak, F., Sınak, A.: On the p-ary (Cubic) Bent and Plateaued (Vectorial) Functions. Designs, Codes and Cryptography (DCC), Springer, doi: 10.1007/s10623-017-0427-4, Vol.85, pp.1-28, October 2017.

- Akyıldız, E., Harold, N.Y., Sınak, A.: Free storage basis conversion over finite field. Turk J Math, 41, 96-109, doi:10.3906/mat-1503-84, January 2017.

- Sınak, A., Özkan, S., Yıldırım, H., Kiraz, M.S.: End-2-End Verifiable Internet Voting Protocol Based on Homomorphic Encryption. International Journal of Information Security Science, Vol.3, No.2, pp.165-181, June 2014.

International Book Publications

- Akyıldız, E., Cenk, M., Sınak, A.: Algorithms and Complexity in Cryptography, Handbook of Codes and Sequences with Applications in Communication, Computing and Information Security, Editors: S. Boztas ve U. Parampalli, CRC Press Taylor & Francis Group, in press, April 2018.

- Mesnager S., Özbudak F., Sınak A.: Results on Characterizations of Plateaued Functions in Arbitrary Characteristic. Cryptography and Information Security in the Balkans, Second International Conference, BalkanCryptSec 2015, Revised Selected Papers, Eds: Enes Pasalic and Lars R. Knudsen, LNCS 9540, Springer, ISBN: 978-3-319-29171-0, pp: 17-30, 2016.

- Özbudak F., Sınak A., Yayla O.: On Verification of Restricted Extended Affine Equivalence for Vectorial Boolean Functions. Arithmetic of Finite Fields, WAIFI 2014, Revised Selected Papers, Eds. Ç. K. Koç, S. Mesnager and E. Savaş, LNCS 9061, Springer, ISBN 978-3-319-16276-8, pp:137-154, 2015.

International Conference Publications

- Mesnager, S., Özbudak, F., Sınak, A.: A new class of three-weight linear codes from weakly regular plateaued functions, Proceedings of Extended Abstract of the tenth International Workshop on Coding and Cryptography (WCC)-2017, September 18-22, 2017, Saint-Petersburg, Russia.

- Carlet, C., Mesnager, S., Özbudak, F., Sınak, A.: Explicit Characterizations for Plateaued-ness of p-ary (Vectorial) Functions. Second International Conference on Codes, Cryptology and Information Security (C2SI-2017), Editors: S. El Hajji, A. Nitaj, E. M. Souidi. In Honor of Claude Carlet. Proceedings, LNCS 10194, Springer, pp:328-345, 9 March 2017, April 10-12, 2017, Rabat, Morocco.

- Mesnager, S., Özbudak, F., Sınak, A.: Characterizations of plateaued functions in arbitrary characteristic. Proceedings of Abstract Book of The International Conference on Coding theory and Cryptography ICCC-2015, 2-5 November 2015, Alger, Algeria.

- Mesnager, S., Özbudak, F., Sınak, A.: Results on characterizations of plateaued functions in arbitrary characteristic. Pre-Proceedings of BalkanCryptSec 2015, Eds: Enes Pasalic and Lars R. Knudsen, 3-4 September 2015, Koper, Slovenia.

- Özbudak, F., Sınak, A., Yayla, O.: On Verification of Restricted Extended Affine Equivalence for Vectorial Boolean Functions. Pre-Proceedings of Arithmetic of Finite Fields, WAIFI 2014, September 26-28, 2014, Gebze, Turkey.

- Sınak, A., Kiraz, M.S., Özkan, S., Yıldırım, H.: A Secure Internet Voting Protocol Based on Homomorphic Encryption. ISCTURKEY 2013, Proceedings of 6th International Conference on Information Security and Cryptology, pp.142-148, September 20-21, 2013, Ankara, Turkey.

Poster Presentations

- Mesnager, S., Özbudak, F., Sınak, A.: A new class of three-weight linear codes from weakly regular plateaued functions, 15th Anniversary of the Foundation

of the Institute of Applied Mathematics, METU, 9 October, 2017, Ankara, Turkey.

- Sınak, A., Kiraz, M.S.: Security Requirements of Electronic Voting and Cryptographic Measures. International Symposium on Digital Forensics, 30 May-1 June 2014, Ankara, Turkey.
- Sınak, A., Cenk, M.: Modular Multiplication Algorithms For Finite Field Multiplication in GF(p). Antalya Algebra Days XVI, May 9-13 2014, ANTALYA, Turkey.
- Sınak, A., Kiraz, M.S., Özkan, S., Yıldırım, H.: An Efficient and Secure Internet Voting Protocol Based on Homomorphic Encryption. CryptoDays 2013, 14-15 Haziran 2013, Tübitak, Gebze, Turkey.

Submissions/Preprints

- Mesnager, S., Özbudak, F., Sınak, A.: Linear codes from weakly regular plateaued functions and their secret sharing schemes. Designs, Codes and Cryptography (DCC), Springer, December 2017.
- Mesnager, S., Özbudak, F., Sınak, A.: Characterizations of Partially Bent and Plateaued Functions over Finite Fields.
- Mesnager, S., Özbudak, F., Sınak, A.: Secondary Constructions of (Non)-Weakly Regular Plateaued p-ary Functions.

Projects

- METU BAP, Boole Fonksiyonları, Cebirsel Eğriler ve Ağ Kodlaması, BAP-07-05-2014-002, Researcher, 01.01.2014-31.12.2014
- METU BAP, Boole Fonksiyonları, Kodlama Teorisi ve Kriptografi, BAP-07-05-2015-007, Researcher, 01.01.2015-31.12.2015
- METU BAP, Yan Kanal Analizi, Aritmetik Karmaşıklık, Alt Uzay Kodlar, Diziler ve Boole Fonksiyonlar, BAP-07-05-2016-005, Researcher, 01.01.2016-31.12.2016

- METU BAP, Arc İnşaaları ve Weierstass Noktalarının Kodlama Teorisine ve Kriptografiye Uygulamaları, BAP-07-05-2017-007, Researcher, 01.01.2017-31.12.2017