SOME CHARACTERIZATIONS OF GENERALIZED S-PLATEAUED FUNCTIONS

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

BY

EMİRCAN ÇELİK

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER OF SCIENCE
IN
CRYPTOGRAPHY

SEPTEMBER 2017

Approval of the thesis:

SOME CHARACTERIZATIONS OF GENERALIZED S-PLATEAUED FUNCTIONS

submitted by **EMİRCAN ÇELİK** in partial fulfillment of the requirements for the degree of **Master of Science in Department of Cryptography, Middle East Technical University** by,

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

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

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

Examining Committee Members:

Assoc. Prof. Dr. Murat Cenk
Department of Cryptography, METU ______________

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

Assist. Prof. Dr. Burcu Gülmez Temür
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: EMİRCAN ÇELİK

Signature :

ABSTRACT

SOME CHARACTERIZATIONS OF GENERALIZED S-PLATEAUED FUNCTIONS

ÇELİK, Emircan
M.S., Department of Cryptography
Supervisor : Prof. Dr. Ferruh Özbudak

September 2017, 32 pages

Plateaued functions play important role in cryptography because of their various desirable cryptographic features. Due to this characteristics they have been widely studied in the literature. This studies include p-ary functions and some generalizations of the boolean functions. In this thesis, we present some of this important work and show that plateaued functions can be generalized much more general framework naturally. Characterizations of generalized plateaued functions using Walsh power moments are also given.

Keywords : Boolean functions, Plateaued functions, p-ary functions, Walsh transform

ÖZ

S-PLATEAUED FONKSİYONLARIN BAZI NİTELENDİRİLMELERİ

ÇELİK, Emircan
Yüksek Lisans, Kriptografi Bölümü
Tez Yöneticisi : Prof. Dr. Ferruh Özbudak

Eylül 2017, 32 sayfa

Plateaued fonksiyonlar çeşitli kriptografik özellikeri sebebiyle kriptografide önemli rol oynamaktadır. Bu karakteristikleri nedeniyle literatürde geniş çaplı çalışılmışlardır. Bu çalışmalar p-ary fonksiyonlar ve boole fonksiyonların bazı genellemelerini içermektedir. Bu tezde, bu önemli çalışmaların bazıları sunulmuş ve plateaued fonksiyonların çok daha genel bir çerçeveye doğal bir şekilde genişletilebileceği gösterilmiştir. Ayrıca plateaued fonksiyonların Walsh kuvvet anları kullanılarak karakterize edilişleri de verilmiştir.

Anahtar Kelimeler: Boole fonksiyonlar, plateaued fonksiyonlar, p-ary fonksiyonlar, Walsh dönüşümü

To My Mother and Father

ACKNOWLEDGMENTS

I would like express my sincere gratitude to my supervisor Prof. Dr. Ferruh Özbudak for his guidance and insight. His inspiration is difficult to state by means of words for me. Truly, this work would not be possible without him.

I also would like to thank to all my colleagues at the Assessment Selection and Placement Center for their constant support and advices throughout this thesis.

I am grateful to my best friends Onur and Gurur for their enthusiasm and support for not only during my studies, but over a decade. I feel fortunate to have such friends in my life.

And last but by no means least, I would like to thank to my family. They deserve more credit in this accomplishment I could ever give them.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

A Boolean function f in n variables defined as s-plateaued function if the absolute value of the Walsh transform of f belong to the set $\{0, 2^{\frac{n+s}{2}}\}$. Plateaued functions first introduced to the literature by Zheng and Zhang in 1999 in [26]. And Carlet and Prouff studied them further in [6], and they have been studied widely ever since. Plateaued functions draw attention of cryptographers due to their various cryptographic characteristics. As a result of their low Hadamard transform, plateaued functions bring safeguard against linear cryptanalysis and fast correlation attacks. In [26], authors showed that plateaued functions have nonlinear characteristics, namely high nonlinearity, high algebraic degree and resiliency. They satisfy propagation criteria. Plateaued functions defined over $\mathbb{F}_2^n$ include three most commonly known classes. First class is bent functions, i.e. $s = 0$ in the functions Walsh transform's amplitude. Second class is *near-bent* functions also known as *semi-bent* functions in odd dimension. Near-bent functions are 1-plateaued functions and they exists when dimension n is odd. Third class is *semi-bent* functions, whic are 2-plateaued functions. Bent functions and semi-bent functions exist when dimension n is even.

P-ary functions are generalization of the boolean functions in odd prime characteristic p.

This thesis organised as follows. In Preliminaries, basic concepts and definitions about boolean functions and functions that are defined over odd characteristic are given. Also generalizations of boolean functions and some characteristic of this generalizations are presented.

Chapter 3 is dedicated to p-ary functions. This Chapter only includes present studies about p-ary plateaued functions.

In Chapter 4 we generalize the concept of the plateaued functions defined over both even and odd dimension vector spaces. Characterizations of generalized plateaued functions are presented.

CHAPTER 2

PRELIMINARIES

Let $\mathbb{F}_2$ denote the Galois field with two elements. $\mathbb{C}$ denotes the set of complex numbers. For $z \in \mathbb{C}$, $\overline{z}$ denotes the conjugate of the number z. Len $\mathbb{F}_2^n$ denote the vector space of dimension n over $\mathbb{F}_2$. Number of non-zero components of the vector $x \in \mathbb{F}_2^n$ is called *Hamming weight* of x and denoted by $wt(x)$. Number of non-equal components of two vectors x and y is defined as *Hamming distance* and denoted by $d_H(x, y)$. For $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ in $\mathbb{F}_2^n$, standard scalar product of x and y on the vector space $\mathbb{F}_2^n$ is

$$x \cdot y = \sum_{i=1}^{n} x_i y_i$$

A mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is called *boolean function*. Set of boolean functions defined over $\mathbb{F}_2^n$ is denoted with $\mathcal{B}_n$. Hamming weight of the boolean function is defined as the size of the set $\{x \in \mathbb{F}_2^n | f(x) \neq 0\}$ and denoted by $wt(f)$. *Hamming distance* $d_H(f, g)$ of the functions f and g on $\mathbb{F}_2^n$ is the size of the set $\{x \in \mathbb{F}_2^n | f(x) \neq g(x)\}$.

The Walsh Transform of the boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is defined as;

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

for every $w \in \mathbb{F}_2^n$. The Walsh Transform is invertible, i.e. *Inverse Walsh Transform* of f is;

$$f(x) = 2^{-n} \sum_{w \in \mathbb{F}_2^n} \widehat{\chi_f}(w)(-1)^{w \cdot x}$$

Lemma 2.1. *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a boolean function and let $\widehat{\chi_f}$ be Walsh Transform of f. Then;*

$$\sum_{w \in \mathbb{F}_2^n} |\widehat{\chi}_f(w)|^2 = 2^{2n}$$

Proof.

$$\begin{aligned}
\sum_{w\in\mathbb{F}_2^n} |\widehat{\chi}_f(w)|^2 &= \sum_{w\in\mathbb{F}_2^n} \widehat{\chi}_f(w)\cdot\widehat{\chi}_f(w) \\
&= \sum_{w\in\mathbb{F}_2^n}\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)}(-1)^{w\cdot x}\sum_{a\in\mathbb{F}_2^n}(-1)^{f(a)}(-1)^{w\cdot a} \\
&= \sum_{w\in\mathbb{F}_2^n}\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)+f(a)}\sum_{a\in\mathbb{F}_2^n}(-1)^{w\cdot(x+a)} \\
&= \sum_{x,a\in\mathbb{F}_2^n}(-1)^{f(x)+f(a)}\sum_{w\in\mathbb{F}_2^n}(-1)^{w\cdot(x+a)} \qquad (2.1)
\end{aligned}$$

As

$$\sum_{w\in\mathbb{F}_2^n}(-1)^{w\cdot(x+a)} = \begin{cases} 0 & \text{, if } x\neq a \\ 2^n & \text{, if } x=a \end{cases}$$

(2.1) can be written as

$$\begin{aligned}
\sum_{w\in\mathbb{F}_2^n} |\widehat{\chi}_f(w)|^2 &= 2^n\sum_{x\in\mathbb{F}_2^n}(-1)^0 \\
&= 2^n\sum_{x\in\mathbb{F}_2^n} 1 \\
&= 2^{2n}
\end{aligned}$$

□

For $f\in\mathbb{B}_n$, f is defined as *bent* function if Walsh transform of f satisfies $|\widehat{\chi_f}(w)| = 2^{n/2}$ for every w in $\mathbb{F}_2^n$.

The *directional difference* (or simply first-order derivative) of the function $f:\mathbb{F}_2^n\to\mathbb{F}_2$ at the direction of $r\in\mathbb{F}_2^n$ is the map

$$\begin{aligned}
&D_af:\mathbb{F}_2^n\to\mathbb{F}_2 \\
&\quad x\mapsto D_af(x)=f(x+a)-f(x), \quad \forall x\in\mathbb{F}_2^n
\end{aligned}$$

And for $a,b\in\mathbb{F}_2^n$, the *second-order derivative* of the function $f:\mathbb{F}_2^n\to\mathbb{F}_2$, is the map

$$\begin{aligned}
&D_aD_bf:\mathbb{F}_2^n\to\mathbb{F}_2 \\
&\quad x\mapsto D_aD_bf(x)=f(x+a+b)-f(x+a)-f(x+b)+f(x), \quad \forall x\in\mathbb{F}_2^n
\end{aligned}$$

Let p be a odd prime number. Let $\zeta_p = e^{\frac{2\pi i}{p}}$ be a primitive p^{th} root of unity. Let $\mathbb{F}_p$ denote the Galois field with p elements and let $\mathbb{F}_p^n$ denote the vector space of dimension n over $\mathbb{F}_p$. The scalar product of two elements $x,y\in\mathbb{F}_p^n$ with $x\cdot y$.

A function $f:\mathbb{F}_p^n\to\mathbb{F}_p$ is defined as *p-ary function*.

The Walsh transform of function $f: F_p^n \to F_p$ is defined as

$$\begin{aligned} \widehat{\chi_f} &: \mathbb{F}_p^n \to \mathbb{C} \\ w &\mapsto \widehat{\chi_f}(w) = \sum_{w \in \mathbb{F}_p^n} \zeta_p^{f(x)} \zeta_p^{w \cdot x} \end{aligned}$$

Inverse Walsh Transform of the function $f: \mathbb{F}_p^n \to \mathbb{F}_p$ is defined as

$$f(x) = p^{-n} \sum_{w \in \mathbb{F}_p^n} \widehat{\chi_f}(w) \zeta_p^{w \cdot x}$$

Lemma 2.2. *Let $f: \mathbb{F}_p^n \to \mathbb{F}_p$ be a p-ary function. Then, for all $w \in \mathbb{F}_p^n$*

$$\sum_{w \in \mathbb{F}_p^n} |\widehat{\chi_f}(w)|^2 = p^{2n}$$

Proof is very similar as proof of Lemma 2.1 therefore it is omitted.

Let $\rho \leq 1$ be an integer. Let $\mathbb{Z}$ denote the set of integers and let $\mathbb{Z}_\rho$ denote ring of integers modulo ρ. A function $f: \mathbb{F}_2^n \to \mathbb{Z}_\rho$ is defined as *generalized boolean* function. The set of all generalized boolean functions in n variables are denoted by $\mathcal{GB}_n^\rho$. Note that $\mathcal{GB}_n^\rho = \mathcal{B}_n$ when $\rho = 2$.

Let ζ be a primitive ρ^{th} root of unity. *The Walsh transform* of the generalized boolean function is defined as

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

Generalized boolean function $f \in \mathcal{GN}_n^\rho$ is called *generalized bent function* if and only if $|\widehat{\chi_f}(w)| = 1$ for all $w \in \mathbb{F}_2^n$. Notice that f is reduced to be bent when $\rho = 2$.

CHAPTER 3

P-ARY PLATEAUED FUNCTIONS

In this chapter nothing but existing studies are presented. In [5, 16, 17, 19], further information can be found.

Definition 3.1. Function $f : \mathbb{F}_p^n \to \mathbb{F}_p$ is called *s- plateaued* if $|\widehat{\chi_f}|^2 \in \{0, p^{n+s}\}$ holds for all $w \in \mathbb{F}_p^n$ where $0 \leq s \leq n$.

Lemma 3.1.

$$\sum_{w\in\mathbb{F}_p^n} |\widehat{\chi}_f(w)|^2 = p^{2n} \tag{3.1}$$

Proof. Since for a complex number z, $|z|^2 = z \cdot \overline{z}$, we can write

$$\begin{aligned}
\sum_{w\in\mathbb{F}_p^n} |\widehat{\chi}_f(w)|^2 &= \sum_{w\in\mathbb{F}_p^n} \widehat{\chi}_f(w) \cdot \overline{\widehat{\chi}_f(w)} \\
&= \sum_{w\in\mathbb{F}_p^n} \sum_{x\in\mathbb{F}_p^n} \zeta_p^{f(x)} \zeta_p^{w\cdot x} \sum_{y\in\mathbb{F}_p^n} \zeta_p^{-f(y)} \zeta_p^{-w\cdot y} \\
&= \sum_{w\in\mathbb{F}_p^n} \sum_{x\in\mathbb{F}_p^n} \zeta_p^{f(x)-f(y)} \sum_{y\in\mathbb{F}_p^n} \zeta_p^{w\cdot(x-y)} \\
&= \sum_{x,y\in\mathbb{F}_p^n} \zeta_p^{f(x)-f(y)} \sum_{w\in\mathbb{F}_p^n} \zeta_p^{w\cdot(x-y)} \qquad (3.2)
\end{aligned}$$

As

$$\sum_{w\in\mathbb{F}_p^n} \zeta_p^{w\cdot(x-y)} = \begin{cases} 0 & \text{, if } \ x \neq y \\ p^n & \text{, if } \ x = y \end{cases}$$

(3.2) can be written as

$$\begin{aligned}
\sum_{w\in\mathbb{F}_p^n} |\widehat{\chi}_f(w)|^2 &= p^n \sum_{x\in\mathbb{F}_p^n} \zeta_p^0 \\
&= p^n \sum_{x\in\mathbb{F}_p^n} 1 \\
&= p^{2n}
\end{aligned}$$

$\square$

Lemma 3.2. *Let $f : \mathbb{F}_p^n \to \mathbb{F}_p$ be an p-ary s-plateaued function. For $w \in \mathbb{F}_p^n$, $|\widehat{\chi_f}(w)|$ equals to $p^{\frac{n+s}{2}}$ for p^{n-s} times and 0 for $p^n - p^{n-s}$ times.*

Proof. Define the set $\mathcal{N}_f = \{w \in \mathbb{F}_p^n : |\widehat{\chi_f}(w)| = p^{\frac{n+s}{2}}\}$. Then,

$$\sum_{w\in\mathbb{F}_p^n} |\widehat{\chi_f}(w)|^2 = |\mathcal{N}_f| \cdot p^{n+s}$$

and from (3.1)

$$\sum_{w\in\mathbb{F}_p^n} |\widehat{\chi}_f(w)|^2 = p^{2n} = |\mathcal{N}_f| \cdot p^{n+s}$$

$$\Rightarrow |\mathcal{N}_f| = p^{n-s} \tag{3.3}$$

□

Thus the rest of the result follows.

Definition 3.2. For integer $i \geq 0$, *Walsh moment* of the Walsh transform of a *p-ary* function f is defined as

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

and define

$$T_i(f) = \frac{S_{i+1}(f)}{S_i(f)}$$

Note that for $i = 0$, $S_0(f) = p^n$ and for $i = 1$, $S_1(f) = p^{2n}$ according to (3.1) (and $T_0(f) = \frac{S_1(f)}{S_0(f)} = p^n$).
For any integer A and integer $i \geq 0$, following equation

$$\sum_{w\in\mathbb{F}_p^n} \left(|\widehat{\chi_f}(w)|^2 - A\right)^2 |\widehat{\chi_f}(w)|^{2i} = S_{i+2}(f) - 2AS_{i+1}(f) + A^2 S_i(f) \tag{3.4}$$

always holds.

Theorem 3.3. *For a p-ary function $f : \mathbb{F}_p^n \to \mathbb{F}_p$ and two positive integers n and k following are equivalent.*

1. *f is s-plateaued with $0 \leq s \leq n$.*
2. $T_{i+1}(f) = T_i(f)$

Proof. 1. Suppose that f is s-plateaued with $0 \leq s \leq n$, . Then, from Lemma 3.2

$$S_i(f) = \sum_{w\in\mathbb{F}_p^n} |\widehat{\chi_f}|^{2i} = p^{n-s} p^{i(n+s)}$$

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

And

$$S_{i+1}(f) = p^{n(i+2)+si}$$
$$S_{i+2}(=) = p^{n(i+3)+s(i+1)}$$

Hence we get,

$$T_i(f) = \frac{S_{i+1}(f)}{S_i(f)} = \frac{p^{(i+2)n+is}}{p^{(i+1)n+(i-1)s}} = p^{n+s}$$
$$T_{i+1}(f) = \frac{S_{i+2}(f)}{i+1} = \frac{p^{(i+3)n+(i+1)s}}{p^{(i+2)n+is}} = p^{n+s}$$

Proving that $T_i(f) = T_{i+1}(f)$.

2. Conversely assume that $T_i(f) = T_{i+1}(f)$. Then, $S_{i+2}(f) = T_i(f) \cdot S_{i+1}(f)$. Taking $A = T_i(f)$ in (3.4) we get

$$\begin{aligned}\sum_{w\in\mathbb{F}_p^n} \left(|\widehat{\chi_f}(w)|^2 - T_i(f)\right)^2 |\widehat{\chi_f}(w)|^{2i} &= S_{i+2}(f) - 2T_i(f)S_{i+1}(f) + (T_i(f))^2 S_i(f) \\ &= T_i(f)\cdot S_{i+1}(f) - 2T_i(f)S_{i+1}(f) + T_i(f)S_{i+1}(f) \\ &= 0\end{aligned}$$

meaning that $|\widehat{\chi_f}|^2 \in \{0, T_i(f)\}$ for all $w \in \mathbb{F}_p^n$. Now let $\mathcal{N}_T = \{w \in \mathbb{F}_p^n : |\widehat{\chi_f}|^2 = T_i(f)\}$. Then,

$$\sum_{w\in\mathbb{F}_p^n} |\widehat{\chi_f}|^2 = T_i(f)\cdot|\mathcal{N}_T| \tag{3.5}$$

from (3.1) we know that left hand side of the (3.5) equal to p^{2n}. Therefore $T_i(f)|p^{2n}$ which means $T_i(f) = p^\lambda$ for some positive integer λ. Thus we have that $|\mathcal{N}_T| = p^{2n-\lambda}$. Since there is p^n elements in $\mathbb{F}_p^n$, $|\mathcal{N}_T|$ is at most p^n, i.e. $p^{2n-\lambda} \le p^n$ implying that $\lambda \ge n$ which means $\lambda = n + s$ for some nonnegative integer s.

□

Theorem 3.4. *Let $f : \mathbb{F}_p^n \to \mathbb{F}_p$ be p-ary function. For an integer s with $0 \le s \le n$ and two positive integers i and j, below assertions are equivalent:*

1. *f is p-ary s-plateaued.*
2. *$S_i(f)S_j(f) = S_{i+1}(f)S_{j-1}(f)$ for all $i \ge 1$ and $j \ge 2$*

Proof. 1. Assume that f is *p-ary* s-plateaued function with $0 \le s \le n$. From Lemma 3.2 we know that,

$$S_i(f) = p^{n(i+1)+s(i-1)}$$
$$S_j f = p^{n(j+1)+s(j-1)}$$
$$S_{i+1}(f) = p^{n(i+2)+si}$$
$$S_{j-1}(f) = p^{nj+s(j-2)}$$

Therefore we have

$$S_i(f)S_j(f) = p^{n(i+j+2)+s(i+j-2)} = S_{i+1}(f)S_{j-1}(f)$$

2. Assume that $S_i(f)S_j(f) = S_{i+1}(f)S_{j-1}(f)$. Then, for $i = j$, we have $T_{i-1}(f) = T_i(f)$. Taking $A = T_{i-1}(f)$ in (3.4) we have that

$$\sum_{w\in\mathbb{F}_p^n} \left(|\widehat{\chi_f}(w)|^2 - T_{i-1}(f)\right)^2 |\widehat{\chi_f}(w)|^{2i} = S_{i+2}(f) - 2T_{i-1}(f)S_{i+1}(f) + (T_{i-1}(f))^2\, S_i(f)$$

And remaining proof deduced to proof of the Theorem 3.3.

□

Corollary 3.5. *Let $f : \mathbb{F}_p^n \to F_p$ be a p-ary function. If f is bent, then $\forall i \in \mathbb{N}$*

$$S_i(f) = p^{n(i+1)} \tag{3.6}$$

Proof. Since we assumed that f is bent, $|\widehat{\chi_f}(w)|^2 = p^n$ for all $w \in \mathbb{F}_p^n$. For $A = p^n$ and $i = 0$ in (3.4) we have

$$\begin{aligned}\sum_{w\in\mathbb{F}_p^n} \left(|\widehat{\chi_f}(w)|^2 - p^n\right)^2 =& S_2(f) - 2p^n S_1(f) + A^2 S_0(f)\\ \sum_{w\in\mathbb{F}_p^n} \left(|\widehat{\chi_f}(w)|^2 - p^n\right)^2 =& S_2(f) - p^{3n}\end{aligned} \tag{3.7}$$

Since f is bent, left hand side of the (3.7) is equal to 0. So $S_2(f) = p^{3n}$. By (3.1) $S_2(f) = p^{2n}$ and by Theorem 3.4, one gets

$$S_i(f) = \frac{S_{i-1}(f)^2}{S_{i-2}(f)} = p^{(i+1)n}$$

□

Next theorem characterizes s-plateaued functions by means of their *Walsh moments.*

Theorem 3.6. *Let $f : \mathbb{F}_p^n \to \mathbb{F}_p$ be a p-ary function and let s be an integer $1 \leq s \leq n$. Then f is s-plateaued iff*

$$S_2(f) = p^{3n+s} \text{ and } S_3(f) = p^{4n+s}.$$

Proof. Suppose f is *p-ary* s-plateaued. Taking $A = p^{n+s}$ and $i = 0$ in (3.4) we get

$$\sum_{w\in\mathbb{F}_p^n} \left(|\widehat{\chi_f}(w)|^2 - p^{n+s}\right)^2 = S_2(f) - 2p^{n+s}S_1(f) + p^{2n+2s}S_0(f)$$

From Lemma 3.2 we know that $\widehat{\chi_f}(w)$ takes $p^n - p^{n-s}$ times the value 0. Therefore we can write

$$\sum_{w\in\mathbb{F}_p^n} \left(|\widehat{\chi_f}(w)|^2 - p^{n+s}\right)^2 = S_2(f) - 2p^{n+s}S_1(f) + p^{2n+2s}S_0(f) \tag{3.8}$$
$$= \left(p^n - p^{n-s}\right)\left(-p^{n+s}\right)^2$$

From definition $S_0(f) = p^n$ and from (3.1), $S_1(f) = p^{2n}$. Putting this values in (3.8) we get

$$\begin{aligned} S_2(f) - 2p^{n+s}p^{2n} + p^{2n+2s}p^n &= \left(p^n - p^{n-s}\right)\left(-p^{n+s}\right)^2 \\ S_2(f) - 2p^{3n+s} + p^{3n+2s} &= p^{3n+2s} - p^{3n+s} \\ S_2(f) &= p^{3n+s} \end{aligned}$$

Also, from Theorem 3.4 for $i = j = 2$ we have $S_3(f) = \frac{(S_2(f))^2}{S_1(f} = \frac{p^{6n+2s}}{p^{2n}} = p^{4n+2s}$ □

Now assume that $S_2(f) = p^{3n+s}$ *and* $S_3(f) = p^{4n+s}$. Taking $A = p^{n+s}$ and $i = 1$ in (3.4) we have,

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

implying that $\widehat{\chi_f}(w) \in \{0, p^{n+s}\}$ for every $w \in \mathbb{F}_p^n$. This concludes the proof.

Corollary 3.7. *If p-ary function f is s-plateaued, for all positive integer i*

$$S_i(f) = p^{n(i+1)+s(i-1)} \tag{3.9}$$

Proof. From Theorem 3.6 we have that $S_2(f) = p^{3n+s}$ and $S_3(f) = p^{4n+2s}$. And by Theorem 3.3, recursively we have

$$S_i(f) = \frac{(S_{i-1}(f))^2}{S_{i-2}(f)} = p^{n(i+1)+s(i-1)}$$

$\forall i \geq 4$. Therefore, (3.9) holds for all positive integer i. □

Following theorem brings new characterizations of the plateaued functions in characteristic p.

Theorem 3.8. *Let $f : \mathbb{F}_p^n \to \mathbb{F}_p$ be p-ary function and define θ_f as*

$$\begin{aligned} \theta_f : &\mathbb{F}_p^n \to \mathbb{C} \\ &x \longrightarrow \theta_f(x) = \sum_{a\in\mathbb{F}_p^n}\sum_{b\in\mathbb{F}_p^n} \zeta_p^{D_aD_bf(x)} \end{aligned}$$

f is s-plateaued iff

$$\theta_f(x) = p^{n+s} \tag{3.10}$$

holds for all $x \in \mathbb{F}_p^n$ and integer s such that $0 \leq s \leq n$.

Following two propositions are useful for the proof of the Theorem 3.8.

Proposition 3.9. *Let $G_i : \mathbb{F}_p^n \to \mathbb{C}$, $i = 1, 2$ be two functions and define $\widehat{G_i} : \mathbb{F}_p^n \to \mathbb{C}$ as*

$$\widehat{G_i} = \sum_{x \in \mathbb{F}_p^n} G_i(x) \zeta_p^{-w \cdot x}$$

Then for all $w, v \in \mathbb{F}_p^n$

$$G_1(w) = G_2(w) \quad \text{if and only if} \quad \widehat{G_1}(v) = \widehat{G_2}(v)$$

Proof. Assume that $G_1(w) = G_2(w)$ for all $w \in \mathbb{F}_p^n$. Then from definition $\widehat{G_1}(v) = \widehat{G_2}(v)$ Now assume that $\widehat{G_1}(v) = \widehat{G_2}(v)$ for all $v \in \mathbb{F}_p^n$ and $G_1(w) \neq G_2(w)$ for some $w \in \mathbb{F}_p^n$. Since $\widehat{G_1}(v) = \widehat{G_2}(v)$ we can write

$$\widehat{G_1}(v) - \widehat{G_2}(v) = \sum_{x \in \mathbb{F}_p^n} (G_1(x) - G_2(x)) \zeta_p^{-v \cdot x}$$

Since left hand side of this equation is equal to 0, we have reached a contradiction. So $G_1(w) = G_2(w)$ for all $w \in \mathbb{F}_p^n$. This completes the proof of Proposition 3.9 $\square$

Let $f : \mathbb{F}_p^n \to \mathbb{F}_p$ be p-ary function. Define complex-valued functions F_1 and F_2 as

$$\begin{aligned} F_1 : \mathbb{F}_p^n &\to \mathbb{C} \\ x &\longrightarrow F_1(x) = \zeta_p^{-f(x)} \end{aligned}$$

$$\begin{aligned} F_2 : \mathbb{F}_p^n &\to \mathbb{C} \\ x &\longrightarrow F_2(x) = \zeta_p^{f(x)} \end{aligned}$$

Proposition 3.10. *For all $w \in \mathbb{F}_p^n$,* $\quad \overline{\widehat{F_1}(w)} = \widehat{F_2}(-w)$

Proof.

$$\begin{aligned} \overline{\widehat{F_1}(w)} &= \sum_{x \in \mathbb{F}_p^n} \overline{F_1(x) \zeta_p^{-w \cdot x}} \\ &= \sum_{x \in \mathbb{F}_p^n} \overline{\zeta_p^{-f(x)} \zeta_p^{-w \cdot x}} \\ &= \sum_{x \in \mathbb{F}_p^n} \zeta_p^{f(x)} \zeta_p^{w \cdot x} \\ &= \widehat{F_2}(-w) \end{aligned}$$

$\square$

Proof of Theorem 3.8 . Since $D_aD_bf(x) = f(x+a+b) - f(x+a) - f(x+b) + f(x)$, we can write $\theta_f(x)$ as

$$\theta_f(x) = \sum_{a\in\mathbb{F}_p^n}\sum_{b\in\mathbb{F}_p^n} \zeta_p^{f(x+a+b)-f(x+a)-f(x+b)+f(x)}$$

Put $x + a = a_1$ and $x + b = b_1$, then $x + a + b = a_1 + b_1 - x$.
For $i = 1, 2$, define $G_i : \mathbb{F}_p^n \to \mathbb{C}$ as

$$G_1(x) = \sum_{a_1\in\mathbb{F}_p^n}\sum_{b_1\in\mathbb{F}_p^n} \zeta_p^{f(a_1+b_1-x)-f(a_1)-f(b_1)}$$

and

$$G_2(x) = p^{n+s}\zeta_p^{-f(x)}$$

Then for all $x \in \mathbb{F}_p^n$, (3.10) holds if and only if $G_1(x) = G_2(x)$ holds for all $x \in \mathbb{F}_p^n$. We continue by computing $\widehat{G_1}$ and $\widehat{G_2}$.

$$\begin{aligned}
\widehat{G_1}(w) &= \sum_{x\in\mathbb{F}_p^n}\sum_{a_1\in\mathbb{F}_p^n}\sum_{b_1\in\mathbb{F}_p^n} \zeta_p^{f(a_1+b_1-x)-f(a_1)-f(b_1)}\zeta_p^{-w\cdot x} \\
&= \sum_{a_1\in\mathbb{F}_p^n} \zeta_p^{-f(a_1)}\zeta_p^{-w\cdot a_1} \sum_{s_1\in\mathbb{F}_p^n} \zeta_p^{-f(b_1)}\zeta_p^{-w\cdot b_1} \sum_{x\in\mathbb{F}_p^n} \zeta_p^{f(a_1+b_1-x)}\zeta_p^{w\cdot(a_1+b_1-x)} \\
&= \widehat{F_1}(w)\cdot\widehat{F_1}(w)\cdot\widehat{F_2}(-w)
\end{aligned}$$

And

$$\begin{aligned}
\widehat{G_2}(w) &= \sum_{x\in\mathbb{F}_p^n} p^{n+s}\zeta_p^{-f(x)}\zeta_p^{-w\cdot x} \\
&= p^{n+s}\sum_{x\in\mathbb{F}_p^n} \zeta_p^{-f(x)}\zeta_p^{-w\cdot x} \\
&= p^{n+s}\sum_{x\in\mathbb{F}_p^n} F_1(x)\zeta_p^{-w\cdot x} \\
&= p^{n+s}\cdot\widehat{F_1}(w)
\end{aligned}$$

By Proposition 3.9, $G_1(x) = G_2(x)$ iff $\widehat{G_1}(w) = \widehat{G_2}(w)$. Therefore (3.10) holds if and only if

$$\widehat{F_1}(w)\cdot\widehat{F_1}(w)\cdot\widehat{F_2}(-w) = p^{n+s}\cdot\widehat{F_1}(w), \quad \forall w \in \mathbb{F}_p^n \tag{3.11}$$

holds . And by Proposition 3.10, (3.11) holds for all $x \in \mathbb{F}_p^n$ if and only if

$$\widehat{F_1}(w)\cdot\widehat{F_1}(w)\cdot\overline{\widehat{F_1}(w)} = p^{n+s}\cdot\widehat{F_1}(w), \quad \forall w \in \mathbb{F}_p^n$$

which is equivalent to

$$\widehat{F_1}(w)\left(\left|\widehat{F_1}(w)\right|^2 - p^{n+s}\right) = 0, \quad \forall w \in \mathbb{F}_p^n \tag{3.12}$$

Therefore, (3.12) holds and only if

$$\left|\widehat{F_1}(w)\right|^2 \in \{0, p^{n+s}\}$$

holds for all $w \in \mathbb{F}_p^n$.
This completes the proof of Theorem 3.8. We can rewrite Theorem 3.8 as following.

Corollary 3.11. *P-ary function $f : \mathbb{F}_p^n \to F_p$ s s-plateaued iff*

$$\sum_{x\in\mathbb{F}_p^n} \theta_f(x) = p^{2n+s} \tag{3.13}$$

□

Proposition 3.12. *For a positive integer n and a p-ary function f;*

$$S_2(f) = \sum_{w\in\mathbb{F}_p^n} |\widehat{\chi_f}(w)|^4 = p^n \sum_{x\in\mathbb{F}_p^n} \theta_f(x)$$

Proof. Since $|z|^4 = z^2\overline{z}^2$ and $\overline{\zeta_p} = \zeta_p^{-1}$ we can write

$$\begin{aligned} S_2(f) = \sum_{w\in\mathbb{F}_p^n} |\widehat{\chi_f}(w)|^4 &= \sum_{w\in\mathbb{F}_p^n} \sum_{a_{1,2,3,4}\in\mathbb{F}_p^n} \zeta_p^{f(a_1)+f(a_2)-f(a_3)-f(a_4)} \cdot \zeta_p^{w\cdot(a_1+a_2-a_3-a_4)} \\ &= \sum_{a_1,a_2,a_3,a_4\in\mathbb{F}_p^n} \zeta_p^{f(a_1)+f(a_2)-f(a_3)-f(a_4)} \sum_{w\in\mathbb{F}_p^n} \zeta_p^{w\cdot(a_1+a_2-a_3-a_4)} \end{aligned}$$

Since

$$\sum_{w\in\mathbb{F}_p^n} \zeta_p^{w\cdot(a_1+a_2a_3-a_4)} = \begin{cases} p^n & \text{if } a_1+a_2-a_3-a_4=0 \\ 0 & \text{otherwise} \end{cases}$$

Hence,

$$\sum_{w\in\mathbb{F}_p^n} |\widehat{\chi_f}(w)|^4 = p^n \sum_{a_1,a_2,a_3,a_4\in\mathbb{F}_p^n} \zeta_p^{f(a_1)+f(a_2)-f(a_3)-f(a_4)}$$

For $a, b \in \mathbb{F}_p^n$ put $a_1 = x$, $a_2 = x+a+b$, $a_3 = x+a$, and $a_4 = x+b$ we get

$$\begin{aligned} \sum_{a_1,a_2,a_3,a_4\in\mathbb{F}_p^n} \zeta_p^{f(a_1)+f(a_2)-f(a_3)-f(a_4)} &= \sum_{x\in\mathbb{F}_p^n} \sum_{a\in\mathbb{F}_p^n} \sum_{a\in\mathbb{F}_p^n} \zeta_p^{f(x+a+b)-f(x+a)-f(x+b)+f(x)} \\ &= \sum_{x\in\mathbb{F}_p^n} \sum_{a\in\mathbb{F}_p^n} \sum_{b\in\mathbb{F}_p^n} \zeta_p^{D_aD_bf(x)} \\ &= \sum_{x\in\mathbb{F}_p^n} \theta_f(x) \end{aligned}$$

Therefore,

$$S_2(f) = \sum_{w\in\mathbb{F}_p^n} |\widehat{\chi_f}(w)|^4 = p^n \sum_{x\in\mathbb{F}_p^n} \theta_f(x)$$

□

From Proposition 3.12 and Corollary 3.11 we can derive a new characterization of the plateaued functions by the means of *Walsh moments*.

Theorem 3.13. *For an integer s with $0 \leq s \leq n$, p-ary function f is s-plateaued iff*

$$S_2(f) = p^{3n+s}$$

Proof. From Proposition 3.12 and Corollary 3.11 we can deduce that f is s-plateaued iff

$$S_2(f) = p^n \sum_{x \in \mathbb{F}_p^n} \theta_f(x) = p^{3n+s}$$

□

CHAPTER 4

GENERALIZED PLATEAUED AND P-ARY GENERALIZED PLATEAUED FUNCTIONS

4.1 Generalizations of the Plateaued Functions

Let $\rho \geq 2$ be any integer, and let complex number $\zeta = e^{\frac{2\pi i}{\rho}}$ be primitive ρ^{th} root of unity. In this section, we generalize plateaued functions and characterize them by the means of their second-order derivatives. The cases of even and odd characteristics are given separately.

4.1.1 Even Characteristic

Definition 4.1. Generalized boolean function. $f : \mathbb{F}_2^n \to \mathbb{Z}_\rho$ defined to be *generalized s-plateaued function* if

$$\left| \sum_{w \in \mathbb{F}_2^n} \widehat{\chi}_f(w) \right|^2 \in \{0, 2^{n+s}\}$$

holds for all $w \in \mathbb{F}_2^n$ and integer s such that $0 \leq s \leq n$.

Definition 4.2. The directional difference(derivative) of f at the direction $a \in \mathbb{F}_2^n$ is the map $D_a f$ from $\mathbb{F}_2^n$ to $\mathbb{Z}_\rho$ defined as

$$D_a f(x) = f(x+a) - f(x), \quad \forall x \in \mathbb{F}_2^n$$

In same analogy, we can define second-order derivative of f as

$$D_b D_a(f) = f(x+a+b) - f(x+a) - f(x+b) + f(x)$$

for all $a, b \in \mathbb{F}_2^n$

Lemma 4.1. *Let f be generalized s-plateaued function and let $\widehat{\chi_f}$ be Walsh transform of f. Then;*

$$\sum_{w \in \mathbb{F}_2^n} |\widehat{\chi}_f(w)|^2 = 2^{2n}$$

Proof. Since

$$|\widehat{\chi}_f(w)|^2 = \widehat{\chi}_f(w) \cdot \overline{\widehat{\chi}_f(w)}$$

we can write

$$\begin{aligned}\sum_{w\in\mathbb{F}_2^n}\sum_{x\in\mathbb{F}_2^n}\zeta^{f(x)}(-1)^{w\cdot x}\sum_{y\in\mathbb{F}_2^n}\zeta^{-f(y)}(-1)^{w\cdot y} &= \sum_{w\in\mathbb{F}_2^n}\sum_{x\in\mathbb{F}_2^n}\zeta^{f(x)-f(y)}\sum_{y\in\mathbb{F}_2^n}(-1)^{w\cdot(x+y)}\\ &= \sum_{x,y\in\mathbb{F}_2^n}\zeta^{f(x)-f(y)}\sum_{w\in\mathbb{F}_2^n}(-1)^{w\cdot(x+y)} \quad (4.1)\end{aligned}$$

As

$$\sum_{w\in\mathbb{F}_2^n}(-1)^{w\cdot(x+y)} = \begin{cases} 0 & \text{, if } \ x \neq y \\ 2^n & \text{, if } \ x = y \end{cases}$$

we can rewrite (4.1) as

$$2^n \sum_{x\in\mathbb{F}_2^n}(-1)^0 = 2^n \sum_{x\in\mathbb{F}_2^n} 1 = 2^{2n}$$

□

Later theorem is very useful characterization of the generalized plateaued boolean functions.

Theorem 4.2. *For a function $f : \mathbb{F}_2^n \to \mathbb{Z}_\rho$ define θ_f as*

$$\begin{aligned}\theta_f : &\mathbb{F}_2^n \to \mathbb{C}\\ &x \longrightarrow \theta_f(x) = \sum_{a\in\mathbb{F}_2^n}\sum_{b\in\mathbb{F}_2^n}\zeta^{D_aD_bf(x)}\end{aligned}$$

f is generalized s-plateaued function iff

$$\theta_f(x) = 2^{n+s} \quad (4.2)$$

holds for all $x \in \mathbb{F}_2^n$ and integer s such that $0 \leq s \leq n$.

Before starting to proof, we will show some propositions that will be helpful to prove Theorem (4.2).

Proposition 4.3. *Let $G_i : \mathbb{F}_2^n \to \mathbb{C}$, $i = 1, 2$ be functions and define $\widehat{G_i} : \mathbb{F}_2^n \to \mathbb{C}$ as*

$$\widehat{G_i} = \sum_{x\in\mathbb{F}_2^n} G_i(x)\zeta^{-w\cdot x}$$

Then for all $w, v \in \mathbb{F}_2^n$

$$G_1(w) = G_2(w) \ \text{ if and only if } \ \widehat{G_1}(v) = \widehat{G_2}(v)$$

Proof. Assume that $G_1(w) = G_2(w)$ for all $w \in \mathbb{F}_2^n$. Then

$$\widehat{G_1}(v) = \sum_{x \in \mathbb{F}_2^n} G_1(x)\zeta^{-v \cdot x} = \sum_{x \in \mathbb{F}_2^n} G_2(x)\zeta^{-v \cdot x} = \widehat{G_2}(v)$$

Now assume that $\widehat{G_1}(v) = \widehat{G_2}(v)$ for all $v \in \mathbb{F}_2^n$ and $G_1(w) \neq G_2(w)$ for some $w \in \mathbb{F}_2^n$. Since $\widehat{G_1}(v) = \widehat{G_2}(v)$ we can write

$$\widehat{G_1}(v) - \widehat{G_2}(v) = \sum_{x \in \mathbb{F}_2^n} (G_1(x) - G_2(x))\zeta^{-v \cdot x} \tag{4.3}$$

From our assumption, (4.3) is equal to 0, therefore we have reached a contradiction. So $G_1(w) = G_2(w)$ for all $w \in \mathbb{F}_2^n$.

□

Let $f \in \mathcal{GB}_n^\rho$. Define complex-valued functions F_1 and F_2 as

$$\begin{aligned} F_1 : \mathbb{F}_2^n &\to \mathbb{C} \\ w &\longrightarrow F_1(w) = \zeta^{-f(w)} \end{aligned}$$

$$\begin{aligned} F_2 : \mathbb{F}_2^n &\to \mathbb{C} \\ w &\longrightarrow F_2(w) = \zeta^{f(w)} \end{aligned}$$

Proposition 4.4. *For all* $x \in \mathbb{F}_2^n$, $\quad \overline{\widehat{F_1}(x)} = \widehat{F_2}(-x)$

Proof.

$$\begin{aligned} \overline{\widehat{F_1}(x)} &= \sum_{w \in \mathbb{F}_2^n} \overline{F_1(w)\zeta^{-x \cdot w}} \\ &= \sum_{w \in \mathbb{F}_2^n} \overline{\zeta^{-f(w)}\zeta^{-x \cdot w}} \\ &= \sum_{w \in \mathbb{F}_2^n} \zeta^{f(w)}\zeta^{x \cdot w} \\ &= \widehat{F_2}(-x) \end{aligned}$$

□

Next, we prove Theorem4.2

Proof of Theorem 4.2 . Since $D_aD_bf(x) = f(x+a+b) - f(x+a) - f(x+b) + f(x)$, we rewrite $\theta_f(x)$ as

$$\theta_f(x) = \sum_{a\in\mathbb{F}_2^n}\sum_{b\in\mathbb{F}_2^n} \zeta^{f(x+a+b)-f(x+a)-f(x+b)+f(x)}$$

Put $x + b = b_1$ and $x + a = a_1$, then $x + a + b = a_1 + b_1 - x$.
For $i = 1, 2$; define $G_i : \mathbb{F}_2^n \to \mathbb{C}$ as

$$G_1(x) = \sum_{a_1\in\mathbb{F}_2^n}\sum_{b_1\in\mathbb{F}_2^n} \zeta^{f(a_1+b_1-x)-f(a_1)-f(b_1)}$$

and

$$G_2(x) = 2^{n+s}\zeta^{-f(x)}$$

With this definitions, (4.2) holds iff $G_1(x) = G_2(x)$ holds for all $x \in \mathbb{F}_2^n$. We continue by computing $\widehat{G_1}$ and $\widehat{G_2}$.

$$\begin{aligned}
\widehat{G_1}(w) &= \sum_{x\in\mathbb{F}_2^n}\sum_{a_1\in\mathbb{F}_2^n}\sum_{b_1\in\mathbb{F}_2^n} \zeta^{f(a_1+b_1-x)-f(a_1)-f(b_1)}\zeta^{-w\cdot x} \\
&= \sum_{a_1\in\mathbb{F}_2^n} \zeta^{-f(a_1)}\zeta^{-w\cdot a_1} \sum_{b_1\in\mathbb{F}_2^n} \zeta^{-f(b_1)}\zeta^{-w\cdot b_1} \sum_{x\in\mathbb{F}_2^n} \zeta^{f(a_1+b_1-x)}\zeta^{w\cdot(a_1+b_1-x)} \\
&= \widehat{F_1}(w)\cdot\widehat{F_1}(w)\cdot\widehat{F_2}(-w)
\end{aligned}$$

And

$$\begin{aligned}
\widehat{G_2}(w) &= \sum_{x\in\mathbb{F}_2^n} 2^{n+s}\zeta^{-f(x)}\zeta^{-w\cdot x} \\
&= 2^{n+s}\sum_{x\in\mathbb{F}_2^n} \zeta^{-f(x)}\zeta^{-w\cdot x} \\
&= 2^{n+s}\sum_{x\in\mathbb{F}_2^n} F_1(x)\zeta^{-w\cdot x} \\
&= 2^{n+s}\cdot\widehat{F_1}(w)
\end{aligned}$$

By Proposition 4.3, $G_1(x) = G_2(x)$ iff $\widehat{G_1}(w) = \widehat{G_2}(w)$. Therefore (4.2) holds if and only if

$$\widehat{F_1}(w)\cdot\widehat{F_1}(w)\cdot\widehat{F_2}(-w) = 2^{n+s}\cdot\widehat{F_1}(w), \quad \forall w \in \mathbb{F}_2^n \tag{4.4}$$

holds . And by Proposition 4.4, (4.4) holds for all $x \in \mathbb{F}_2^n$ if and only if

$$\widehat{F_1}(w)\cdot\widehat{F_1}(w)\cdot\overline{\widehat{F_1}(w)} = 2^{n+s}\cdot\widehat{F_1}(w), \quad \forall w \in \mathbb{F}_2^n$$

which is equivalent to

$$\widehat{F_1}(w)\left(\left|\widehat{F_1}(w)\right|^2 - 2^{n+s}\right) = 0, \quad \forall w \in \mathbb{F}_2^n \tag{4.5}$$

Therefore, (4.5) holds and only if

$$\left|\widehat{F_1}(w)\right|^2 \in \{0, 2^{n+s}\}$$

holds for all for all $w \in \mathbb{F}_2^n$.
This completes the proof of Theorem 4.2. $\square$

4.1.2 Odd Characteristic

In this section, we will define *p-ary generalized plateaued* functions for some odd prime number p. From now on, $\zeta = p^{\frac{2\pi i}{\rho}}$ will denote primitive ρ^{th} root of unity.

Definition 4.3. $f : \mathbb{F}_p^n \to \mathbb{Z}_\rho$ is called *p-ary generalized plateaued* function if

$$\left| \sum_{w \in \mathbb{F}_p^n} \widehat{\chi}_f(w) \right|^2 \in \{0, p^{n+s}\}$$

holds for all $w \in \mathbb{F}_p^n$.

Definition 4.4. *The Walsh transform* of the p-ary generalized function f is defined as

$$\widehat{\chi_f}(w) = \sum_{w \in \mathbb{F}_p^n} \zeta^{f(x)} (\zeta)^{w \cdot x}$$

Definition 4.5. Directional difference or derivative of f at the direction of $a \in \mathbb{F}_p^n$ is the map $D_a f$ from $\mathbb{F}_p^n$ to $\mathbb{Z}_\rho$ defined as

$$D_a f(x) = f(x + a) - f(x), \quad \forall x \in \mathbb{F}_p^n$$

Second derivative of f is defined similarly as;

$$D_b D_a(f) = f(x + a + b) - f(x + a) - f(x + b) + f(x)$$

for all $a, b \in \mathbb{F}_p^n$

Following lemma known as Parseval identity holds for p-ary generalized plateaued functions.

Lemma 4.5. *Let f be p-ary generalized plateaued function and let $\widehat{\chi_f}$ be it's Walsh-Hadamard Transform. Then;*

$$\sum_{w \in \mathbb{F}_p^n} |\widehat{\chi}_f(w)|^2 = p^{2n}$$

Proof. Since

$$|\widehat{\chi}_f(w)|^2 = \widehat{\chi}_f(w) \cdot \overline{\widehat{\chi}_f(w)}$$

we can write

$$\begin{aligned} \sum_{w \in \mathbb{F}_p^n} \sum_{x \in \mathbb{F}_p^n} \zeta^{f(x)} \zeta^{w \cdot x} \sum_{y \in \mathbb{F}_p^n} \zeta^{-f(y)} \zeta^{-w \cdot y} &= \sum_{w \in \mathbb{F}_p^n} \sum_{x \in \mathbb{F}_p^n} \zeta^{f(x) - f(y)} \sum_{y \in \mathbb{F}_p^n} \zeta^{w \cdot (x - y)} \\ &= \sum_{x, y \in \mathbb{F}_p^n} \zeta^{f(x) - f(y)} \sum_{w \in \mathbb{F}_p^n} \zeta^{w \cdot (x - y)} \qquad (4.6) \end{aligned}$$

As

$$\sum_{w\in\mathbb{F}_p^n}\zeta^{w\cdot(x-y)} = \begin{cases} 0 & \text{, if } \ x\neq y \\ \\ p^n & \text{, if } \ x = y \end{cases}$$

(4.6) can be written as

$$p^n\sum_{x\in\mathbb{F}_p^n}\zeta^0 = p^n\sum_{x\in\mathbb{F}_p^n}1 = p^{2n} \tag{4.7}$$

□

Next we extend Theorem 4.2 for p-ary generalized plateaued functions.

Theorem 4.6. *For a p-ary generalized function $f:\mathbb{F}_p^n\to\mathbb{Z}_\rho$ define θ_f as*

$$\begin{aligned} \theta_f :\ & \mathbb{F}_p^n \to \mathbb{C} \\ & x \longrightarrow \theta_f(x) = \sum_{a\in\mathbb{F}_p^n}\sum_{b\in\mathbb{F}_p^n}\zeta^{D_aD_bf(x)} \end{aligned}$$

f is p-ary generalized s-plateaued iff

$$\theta_f(x) = p^{n+s} \tag{4.8}$$

holds for all $x\in\mathbb{F}_p^n$ and integer s such that $0\leq s\leq n$.

Before starting to proof the Theorem 4.6, let us extend Proposition 4.3 and Proposition 4.4 to odd prime p.

Proposition 4.7. *Let $G_i:\mathbb{F}_p^n\to\mathbb{C}$, $i=1,2$ be functions and define $\widehat{G_i}:\mathbb{F}_2^n\to\mathbb{C}$ as*

$$\widehat{G_i} = \sum_{x\in\mathbb{F}_2^n}G_i(x)\zeta^{-w\cdot x}$$

Then for all $w,v\in\mathbb{F}_p^n$

$$G_1(w) = G_2(w) \ \ \text{if and only if} \ \ \widehat{G_1}(v) = \widehat{G_2}(v)$$

Proof. Assume that $G_1(w) = G_2(w)$ for all $w\in\mathbb{F}_p^n$. Then clearly $\widehat{G_1}(v) = \widehat{G_2}(v)$ Now assume that $\widehat{G_1}(v) = \widehat{G_2}(v)$ for all $v\in\mathbb{F}_p^n$ and $G_1(w)\neq G_2(w)$ for some $w\in\mathbb{F}_p^n$. Since $\widehat{G_1}(v) = \widehat{G_2}(v)$ we can write

$$\widehat{G_1}(v) - \widehat{G_2}(v) = \sum_{x\in\mathbb{F}_p^n}(G_1(x) - G_2(x))\zeta^{-v\cdot x}$$

As this equation is equal to 0, we have reached a contradiction. So $G_1(w) = G_2(w)$ for all $w\in\mathbb{F}_p^n$. □

Let $f : \mathbb{F}_p^n \to \mathbb{Z}_\rho$ be a generalized p-ary function. Define complex-valued functions F_1 and F_2 as

$$\begin{aligned} F_1 : \mathbb{F}_p^n &\to \mathbb{C} \\ w &\longrightarrow F_1(w) = \zeta^{-f(w)} \end{aligned}$$

$$\begin{aligned} F_2 : \mathbb{F}_p^n &\to \mathbb{C} \\ w &\longrightarrow F_2(w) = \zeta^{f(w)} \end{aligned}$$

Proposition 4.8. *For all $x \in \mathbb{F}_p^n$,* $\quad \overline{\widehat{F_1}(x)} = \widehat{F_2}(-x)$

Proof.

$$\begin{aligned} \overline{\widehat{F_1}(x)} &= \sum_{w \in \mathbb{F}_p^n} \overline{F_1(w)\zeta^{-x\cdot w}} \\ &= \sum_{w \in \mathbb{F}_p^n} \overline{\zeta^{-f(w)}\zeta^{-x\cdot w}} \\ &= \sum_{w \in \mathbb{F}_p^n} \zeta^{f(w)}\zeta^{x\cdot w} \\ &= \widehat{F_2}(-x) \end{aligned}$$

□

Next we prove Theorem 4.6

Proof of Theorem 4.6. Since $D_a D_b f(x) = f(x+a+b) - f(x+a) - f(x+b) + f(x)$, we rewrite $\theta_f(x)$ as

$$\theta_f(x) = \sum_{a \in \mathbb{F}_p^n} \sum_{b \in \mathbb{F}_p^n} \zeta^{f(x+a+b)-f(x+a)-f(x+b)+f(x)}$$

Put $x + b = b_1$ and $x + a = a_1$, then $x + a + b = a_1 + b_1 - x$.
For $i = 1, 2$, define $G_i : \mathbb{F}_p^n \to \mathbb{C}$ as

$$G_1(x) = \sum_{a_1 \in \mathbb{F}_p^n} \sum_{b_1 \in \mathbb{F}_p^n} \zeta^{f(a_1+b_1-x)-f(a_1)-f(b_1)}$$

and

$$G_2(x) = p^{n+s}\zeta^{-f(x)}$$

Then for all $x \in \mathbb{F}_p^n$, (4.8) holds iff $G_1(x) = G_2(x)$ holds for all $x \in \mathbb{F}_p^n$. We continue by computing $\widehat{G_1}$ and $\widehat{G_2}$.

$$\begin{aligned}
\widehat{G_1}(w) &= \sum_{x\in\mathbb{F}_p^n}\sum_{a_1\in\mathbb{F}_p^n}\sum_{b_1\in\mathbb{F}_p^n}\zeta^{f(a_1+b_1-x)-f(a_1)-f(b_1)}\zeta^{-w\cdot x} \\
&= \sum_{a_1\in\mathbb{F}_p^n}\zeta^{-f(a_1)}\zeta^{-w\cdot a_1}\sum_{b_1\in\mathbb{F}_p^n}\zeta^{-f(b_1)}\zeta^{-w\cdot b_1}\sum_{x\in\mathbb{F}_p^n}\zeta^{f(a_1+b_1-x)}\zeta^{w\cdot(a_1+b_1-x)} \\
&= \widehat{F_1}(w)\cdot\widehat{F_1}(w)\cdot\widehat{F_2}(-w)
\end{aligned}$$

And

$$\begin{aligned}
\widehat{G_2}(w) &= \sum_{x\in\mathbb{F}_p^n} p^{n+s}\zeta^{-f(x)}\zeta^{-w\cdot x} \\
&= p^{n+s}\sum_{x\in\mathbb{F}_p^n}\zeta^{-f(x)}\zeta^{-w\cdot x} \\
&= p^{n+s}\sum_{x\in\mathbb{F}_p^n}F_1(x)\zeta^{-w\cdot x} \\
&= p^{n+s}\cdot\widehat{F_1}(w)
\end{aligned}$$

By Proposition 4.7, $G_1(x) = G_2(x)$ iff $\widehat{G_1}(w) = \widehat{G_2}(w)$. Therefore (4.8) holds if and only if

$$\widehat{F_1}(w)\cdot\widehat{F_1}(w)\cdot\widehat{F_2}(-w) = p^{n+s}\cdot\widehat{F_1}(w), \quad \forall w \in \mathbb{F}_p^n \tag{4.9}$$

holds . And by Proposition 4.8, (4.9) holds for all $x \in \mathbb{F}_p^n$ if and only if

$$\widehat{F_1}(w)\cdot\widehat{F_1}(w)\cdot\overline{\widehat{F_1}(w)} = p^{n+s}\cdot\widehat{F_1}(w), \quad \forall w \in \mathbb{F}_p^n$$

which is equivalent to

$$\widehat{F_1}(w)\left(\left|\widehat{F_1}(w)\right|^2 - p^{n+s}\right) = 0, \quad \forall w \in \mathbb{F}_p^n \tag{4.10}$$

Therefore, (4.10) holds and only if

$$\left|\widehat{F_1}(w)\right|^2 \in \{0, p^{n+s}\}$$

holds for all for all $w \in \mathbb{F}_p^n$.

□

Proposition 4.9. *For p-ary generalized function $f : \mathbb{F}_p^n \to \mathbb{Z}_\rho$ and a positive integer n*

$$\sum_{w\in\mathbb{F}_p^n}|\widehat{\chi_f}(w)|^4 = p^n\sum_{x\in\mathbb{F}_p^n}\theta_f(x)$$

Proof. Since $|z|^4 = z^2\overline{z}^2$ and $\overline{\zeta} = \zeta^{-1}$ we can write

$$\sum_{w\in\mathbb{F}_p^n} |\widehat{\chi_f}(w)|^4 = \sum_{w\in\mathbb{F}_p^n} \sum_{x_1,x_2,x_3,x_4\in\mathbb{F}_p^n} \zeta^{f(x_1)+f(x_2)-f(x_3)-f(x_4)} \cdot \zeta^{w\cdot(x_1+x_2-x_3-x_4)}$$
$$= \sum_{x_1,x_2,x_3,x_4\in\mathbb{F}_p^n} \zeta^{f(x_1)+f(x_2)-f(x_3)-f(x_4)} \sum_{w\in\mathbb{F}_p^n} \zeta^{w\cdot(x_1+x_2-x_3-x_4)}$$

Since

$$\sum_{w\in\mathbb{F}_p^n} \zeta^{w\cdot(x_1+x_2-x_3-x_4)} = \begin{cases} p^n & \text{if } x_1+x_2-x_3-x_4=0 \\ 0 & \text{otherwise} \end{cases}$$

Hence,

$$\sum_{w\in\mathbb{F}_p^n} |\widehat{\chi_f}(w)|^4 = p^n \sum_{x_1,x_2,x_3,x_4\in\mathbb{F}_p^n} \zeta^{f(x_1)+f(x_2)-f(x_3)-f(x_4)}$$

For $a, b \in \mathbb{F}_p^n$ put $x_1 = x$, $x_2 = x+a+b$, $x_3 = x+a$, and $x_4 = x+b$ we get

$$\sum_{x_1,x_2,x_3,x_4\in\mathbb{F}_p^n} \zeta^{f(x_1)+f(x_2)-f(x_3)-f(x_4)} = \sum_{x\in\mathbb{F}_p^n} \sum_{a\in\mathbb{F}_p^n} \sum_{a\in\mathbb{F}_p^n} \zeta^{f(x+a+b)-f(x+a)-f(x+b)+f(x)}$$
$$= \sum_{x\in\mathbb{F}_p^n} \sum_{a\in\mathbb{F}_p^n} \sum_{b\in\mathbb{F}_p^n} \zeta^{D_aD_bf(x)}$$
$$= \sum_{x\in\mathbb{F}_p^n} \theta_f(x)$$

Therefore,

$$\sum_{w\in\mathbb{F}_p^n} |\widehat{\chi_f}(w)|^4 = p^n \sum_{x\in\mathbb{F}_p^n} \theta_f(x)$$

□

4.2 Characterizations of P-ary Generalized Plateaued Functions

Herein this section we characterize p-ary generalized plateaued functions with *Walsh moments*.

Definition 4.6. For an integer $i \geq 0$, the *Walsh moment* of p-ary generalized plateaued function f is

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

with the convention $S_0(f) = p^n$. Note that $S_1(f) = p^{2n}$ by *Parseval identity*.

Lemma 4.10. *Let $f : \mathbb{F}_p^n \to \mathbb{Z}_\rho$ be p-ary generalized s-plateaued function with $0 \leq s \leq n$. Then for $w \in \mathbb{F}_p^n$, for p^{n-s} times $|\widehat{\chi_f}(w)|^2$ takes the value p^{n+s} and for $p^n - p^{n-s}$ times $|\widehat{\chi_f}(w)|^2$ takes the value 0.*

Proof. Let $\mathcal{N}_S$ denote the size of the set $\{w \in \mathbb{F}_p^n : |\widehat{\chi_f}(w)|^2 = p^{n+s}\}$. Then,

$$\sum_{w\in\mathbb{F}_p^n} |\widehat{\chi_f}(w)|^2 = \mathcal{N}_S \cdot p^{n+s}$$

hence, by Parseval identity,

$$\begin{aligned} p^{2n} &= \mathcal{N}_S \cdot p^{n+s} \\ \mathcal{N}_S &= p^{n-s} \end{aligned}$$

And since $\#\mathbb{F}_p^n = p^n$, we have $\#\{w \in \mathbb{F}_p^n : |\widehat{\chi_f}(w)|^2 = 0\} = p^n - p^{n-s}$ □

Let f be p-ary generalized plateaued function. For any integer A and $i\ geq 0$, equation

$$\sum_{w\in\mathbb{F}_p^n} \left(|\widehat{\chi_f}(w)|^2 - A\right)^2 |\widehat{\chi_f}(w)|^{2i} = S_{i+2}(f) - 2AS_{i+1}(f) + A^2 S_i(f) \tag{4.11}$$

holds.

Theorem 4.11. *For integer s with $0 \leq s \leq n$ and a p-ary generalized s-plateaued function f;*

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

holds for all integers $i \geq 1$. Also we have $S_i(f)S_j(f) = S_{i+1}(f)S_{j-1}(f)$ for all integers $i \geq 1,\ j \geq 2$.

Proof. From Lemma 4.10, for a positive integer i, we have that

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

Therefore the following two equations

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

are equal for all $i \geq 1$ and $j \geq 2$. □

Theorem 4.12. *Let $f : \mathbb{F}_p^n \to \mathbb{Z}_\rho$ be a generalized p-ary function. f is s-plateaued iff*

$$S_2(f) = p^{3n+s}\, and\, S_3(f) = p^{4n+2s}$$

where s is an integer such that $1 \leq s \leq n$.

Proof. Let f be p-ary generalized s-plateaued function. Then by Theorem 4.11 $S_2(f) = p^{3n+s}\, and\, S_3(f) = p^{4n+2s}$. Conversely assume that $S_2(f) = p^{3n+s}\, and\, S_3(f) = p^{4n+2s}$. By (4.11) with $A = p^{n+s}$ and $i = 1$ we have,

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

Hence, $|\widehat{\chi_f}(w)|^2 \in \{0, p^{n+s}\}$ holds for all $w \in \mathbb{F}_p^n$, i.e. f is p-ary generalized s-plateaued function. $\square$

Proposition 4.13. *For a p-ary generalized function $f : \mathbb{F}_p^n \to \mathbb{Z}_\rho$ and a positive integer n*

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

Proof. Since $|z|^4 = z^2 \overline{z}^2$ and $\overline{\zeta} = \zeta^{-1}$ we can write

$$\begin{aligned} S_2(f) = \sum_{w \in \mathbb{F}_p^n} |\widehat{\chi_f}(w)|^4 &= \sum_{w \in \mathbb{F}_p^n} \sum_{x_1, x_2, x_3, x_4 \in \mathbb{F}_p^n} \zeta^{f(x_1)+f(x_2)-f(x_3)-f(x_4)} \cdot \zeta^{w \cdot (x_1+x_2-x_3-x_4)} \\ &= \sum_{x_1, x_2, x_3, x_4 \in \mathbb{F}_p^n} \zeta^{f(x_1)+f(x_2)-f(x_3)-f(x_4)} \sum_{w \in \mathbb{F}_p^n} \zeta^{w \cdot (x_1+x_2-x_3-x_4)} \end{aligned}$$

Since

$$\sum_{w \in \mathbb{F}_p^n} \zeta^{w \cdot (x_1+x_2-x_3-x_4)} = \begin{cases} p^n & \text{if } x_1 + x_2 - x_3 - x_4 = 0 \\ 0 & \text{otherwise} \end{cases}$$

Hence,

$$\sum_{w \in \mathbb{F}_p^n} |\widehat{\chi_f}(w)|^4 = p^n \sum_{x_1, x_2, x_3, x_4 \in \mathbb{F}_p^n} \zeta^{f(x_1)+f(x_2)-f(x_3)-f(x_4)}$$

For $a, b \in \mathbb{F}_p^n$ put $x_1 = x$, $x_2 = x + a + b$, $x_3 = x + a$, and $x_4 = x + b$ we get

$$\begin{aligned} \sum_{x_1, x_2, x_3, x_4 \in \mathbb{F}_p^n} \zeta^{f(x_1)+f(x_2)-f(x_3)-f(x_4)} &= \sum_{x \in \mathbb{F}_p^n} \sum_{a \in \mathbb{F}_p^n} \sum_{a \in \mathbb{F}_p^n} \zeta^{f(x+a+b)-f(x+a)-f(x+b)+f(x)} \\ &= \sum_{x \in \mathbb{F}_p^n} \sum_{a \in \mathbb{F}_p^n} \sum_{b \in \mathbb{F}_p^n} \zeta^{D_a D_b f(x)} \\ &= \sum_{x \in \mathbb{F}_p^n} \theta_f(x) \end{aligned}$$

Therefore,

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

$\square$

Using Theorem 4.12 and Proposition 4.13, we can get much more general case as stated below.

Corollary 4.14. *Let $f : \mathbb{F}_p^n \to \mathbb{Z}_\rho$ be a p-ary generalized s-plateaued function. Then,*

$$S_i(f) = p^{n(i-1)+s(i-2)} \sum_{x \in \mathbb{F}_p^n} \theta_f(x)$$

where s is an integer with $0 \leq s \leq n$.

For another characterization plateaued functions, we recall two important inequalities.

Theorem 4.15 (Hölder's inequality)**.** *Let p_1, $p_2 \in (1,\infty)$ with $\frac{1}{p_1}+\frac{1}{p_2}=1$. Then for all $(x_1,x_2,\ldots,x_m)$, $(y_1,y_2,\ldots,y_m)\in\mathbb{C}^m$,*

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

and the equality holds if and only if, there exists a nonnegative constant c such that, for $k \in \{1,2,\ldots m\}$,

$$|x_k|^{p_1} = c\,|y_k|^{p_2}$$

holds. If $p_i = 2$ for $i = 1,2$, then the above inequality is reduced to the Chauchy-Schwarz Inequality.

Theorem 4.16. *Let $f:\mathbb{F}_p^n \to \mathbb{Z}_\rho$ be generalized p-ary boolean function. Then for all integers $i \geq 1$*

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

and the equality holds for at least one i, iff, f is p-ary generalized plateaued function.

Proof. Let $x_k,\ y_k$ in the theorem (above) be $x_k = |\widehat{\chi_f}(w)|^i$ and $y_k = |\widehat{\chi_f}(w)|^{i+2}$. Then, for all $w\in\mathbb{F}_p^n$ we have,

$$\left(\sum_{w\in\mathbb{F}_p^n}|\widehat{\chi_f}(w)|^{2i+2}\right)^2 \leq \sum_{w\in\mathbb{F}_p^n}|\widehat{\chi_f}(w)|^{2i}\sum_{w\in\mathbb{F}_p^n}|\widehat{\chi_f}(w)|^{2i+4}$$

that is,

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

for $i \geq 1$. Now suppose that f is *p-ary generalized plateaued* function. Then above equality holds for at least one $i\geq 1$ if and only if

$$|\widehat{\chi_f}(w)|^{2i} = c\,|\widehat{\chi_f}(w)|^{2i+4} \tag{4.12}$$

holds for all $w\in\mathbb{F}_p^n$ and for some nonnegative constant c. If $|\widehat{\chi_f}(w)|=0$, then (4.12) holds for all nonnegative c. If $|\widehat{\chi_f}(w)| = p^{n+s}$ for some s with $0\leq s\leq n$, one can simply take $c = |\widehat{\chi_f}(w)|^{-4}$. In both cases (4.12) holds, proving that equality above holds if and only if f is *p-ary generalized plateaued*.

□

CHAPTER 5

CONCLUSION

Plateaued functions, posses desirable cryptographic properties such as maximal nonlinearity amid balanced plateaued functions, low autocorrelation. Also, alongside of being practical in cryptography, plateaued functions also have use in coding theory and secret sharing schemes.
In this thesis we first introduced the mathematical background and basic concepts about generalized boolean, generalized p-ary functions and plateaued functions.
In Chapter 3, we present the studies about p-ary plateaued functions and their various characterizations using both second-order derivatives and Walsh moments.
In Chapter 4, the notation of Generalized plateaued functions are presented. We characterized generalized s-plateaued and p-ary generalized plateaued functions using their second-order derivatives and Walsh moments.

REFERENCES

[1] C. Carlet, Partially-bent functions, Designs, Codes and Cryptography, 3(2), pp. 135–145, May 1993, ISSN 1573-7586.

[2] C. Carlet, Vectorial boolean functions for cryptography, Boolean models and methods in mathematics, computer science, and engineering, 134, pp. 398–469, 2010.

[3] C. Carlet, Boolean and vectorial plateaued functions and apn functions, IEEE Transactions on Information Theory, 61(11), pp. 6272–6289, Nov 2015, ISSN 0018-9448.

[4] C. Carlet and S. Mesnager, On semibent boolean functions, IEEE Transactions on Information Theory, 58(5), pp. 3287–3292, May 2012, ISSN 0018-9448.

[5] C. Carlet, S. Mesnager, F. Özbudak, and A. Sinak, Explicit characterizations for plateaued-ness of p-ary (vectorial) functions, in *Codes, Cryptology and Information Security - Second International Conference, C2SI 2017, Rabat, Morocco, April 10-12, 2017, Proceedings - In Honor of Claude Carlet*, pp. 328–345, 2017.

[6] C. Carlet and E. Prouff, *On Plateaued Functions and Their Constructions*, pp. 54–73, Springer Berlin Heidelberg, Berlin, Heidelberg, 2003, ISBN 978-3-540-39887-5.

[7] A. Çeşmelioğlu and W. Meidl, A construction of bent functions from plateaued functions, Designs, Codes and Cryptography, 66(1), pp. 231–242, Jan 2013, ISSN 1573-7586.

[8] T. Cusick and P. Stănică, *Cryptographic Boolean Functions and Applications*, Academic Press/Elsevier, 2009, ISBN 9780123748904.

[9] S. Gangopadhyay, E. Pasalic, and P. Stanica, A note on generalized bent criteria for boolean functions, IEEE Trans. Information Theory, 59(5), pp. 3233–3236, 2013.

[10] T. Helleseth and A. Kholosha, *On the Dual of Monomial Quadratic p-ary Bent Functions*, pp. 50–61, Springer Berlin Heidelberg, Berlin, Heidelberg, 2007, ISBN 978-3-540-77404-4.

[11] J. Y. Hyun, J. Lee, and Y. Lee, Explicit criteria for construction of plateaued functions, IEEE Trans. Information Theory, 62(12), pp. 7555–7565, 2016.

[12] 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), pp. 279–295, Feb 2006, ISSN 1573-7586.

[13] P. Kumar, R. Scholtz, and L. Welch, Generalized bent functions and their properties, Journal of Combinatorial Theory, Series A, 40(1), pp. 90 – 107, 1985, ISSN 0097-3165.

[14] R. Lidl and H. Niederreiter, *Finite Fields*, number 20. c.,1. böl. in EBL-Schweitzer, Cambridge University Press, 1997, ISBN 9780521392310.

[15] S. Mesnager, Semibent functions from dillon and niho exponents, kloosterman sums, and dickson polynomials, IEEE Transactions on Information Theory, 57(11), pp. 7443–7458, Nov 2011, ISSN 0018-9448.

[16] S. Mesnager, Characterizations of plateaued and bent functions in characteristic p, in *Sequences and Their Applications - SETA 2014 - 8th International Conference, Melbourne, VIC, Australia, November 24-28, 2014, Proceedings*, pp. 72–82, 2014.

[17] S. Mesnager, *Bent Functions - Fundamentals and Results*, Springer, 2016, ISBN 978-3-319-32593-4.

[18] S. Mesnager, F. Özbudak, and E. Çelik, Some characterizations of generalized s-plateaued functions, Preprint.

[19] S. Mesnager, F. Özbudak, and A. Sinak, Results on characterizations of plateaued functions in arbitrary characteristic, in *Cryptography and Information Security in the Balkans - Second International Conference, BalkanCryptSec 2015, Koper, Slovenia, September 3-4, 2015, Revised Selected Papers*, pp. 17–30, 2015.

[20] S. Mesnager, F. Özbudak, and A. Sinak, A new class of three-weight linear codes from weakly regular plateaued functions, CoRR, abs/1703.08362, 2017.

[21] S. Mesnager, C. Tang, and Y. Qi, Generalized plateaued functions and admissible (plateaued) functions, IEEE Transactions on Information Theory, 2017.

[22] G. Mullen and D. Panario, *Handbook of Finite Fields*, Discrete Mathematics and Its Applications, CRC Press, 2013, ISBN 9781439873823.

[23] K. Nyberg, *Perfect nonlinear S-boxes*, pp. 378–386, Springer Berlin Heidelberg, Berlin, Heidelberg, 1991, ISBN 978-3-540-46416-7.

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

[25] W. Rudin, *Principles of mathematical analysis*, McGraw-Hill Book Co., New York, third edition, 1976, ISBN 0-07-085613-3, international Series in Pure and Applied Mathematics.

[26] Y. Zheng and X.-M. Zhang, *Plateaued Functions*, pp. 284–300, Springer Berlin Heidelberg, Berlin, Heidelberg, 1999, ISBN 978-3-540-47942-0.

[27] Y. Zheng and X.-M. Zhang, *Relationships between Bent Functions and Complementary Plateaued Functions*, pp. 60–75, Springer Berlin Heidelberg, Berlin, Heidelberg, 2000, ISBN 978-3-540-45568-4.