STUDIES ON NON-WEAKLY REGULAR BENT FUNCTIONS AND RELATED STRUCTURES

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

RUMI MELIH PELEN

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

JULY 2020

Approval of the thesis:

STUDIES ON NON-WEAKLY REGULAR BENT FUNCTIONS AND RELATED STRUCTURES

submitted by **RUMI MELIH PELEN** in partial fulfillment of the requirements for the degree of **Doctor of Philosophy in Mathematics Department, Middle East Technical University** by,

Prof. Dr. Halil Kalıpçılar
Dean, Graduate School of **Natural and Applied Sciences** _____

Prof. Dr. Yıldıray Ozan
Head of Department, **Mathematics** _____

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

Examining Committee Members:

Assoc. Prof. Dr. Ali Özgür Kişisel
Mathematics, METU _____

Prof. Dr. Ferruh Özbudak
Mathematics, METU _____

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

Assoc. Prof. Dr. Barış Bülent Kırlar
Mathematics, Süleyman Demirel University _____

Assist. Prof. Dr. Eda Tekin
Business Administration, Karabük University _____

Date:

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

Name, Surname: Rumi Melih Pelen

Signature :

ABSTRACT

STUDIES ON NON-WEAKLY REGULAR BENT FUNCTIONS AND RELATED STRUCTURES

Pelen, Rumi Melih
Ph.D., Department of Mathematics
Supervisor: Prof. Dr. Ferruh Özbudak

July 2020, 84 pages

Interest in bent functions over finite fields arises both from mathematical theory and practical applications. There has been lots of literature addressing various properties of bent functions. They have a number of applications consisting of coding theory, cryptography, and sequence designs. They're divided into four subclasses: regular bent functions that are contained within the class of weakly regular bent functions that are contained within the class of dual-bent functions. Additionally, there are *non-weakly regular bent* functions with no intersection with weakly regular, but an intersection with the class of dual-bent functions. The present thesis studies various combinatorial properties of non-weakly regular bent functions over finite fields.

The principal result in the thesis is the solution of the open problem "Is there any non-weakly regular bent function f for which the dual f^* is weakly regular?" which is proposed by Çeşmelioğlu, Meidl and Pott. We also generalize this result to plateaued functions.

For an arbitray non-weakly regular bent function f, we define the partition $B^+(f)$

and $B^-(f)$ of $\mathbb{F}_{p^n}$. Then, we show that, if the corresponding partition for a non-weakly regular bent function in the *GMMF* class gives a partial difference set then it is trivial. Moreover, we exhibit that these subsets associated with the two of the recognized sporadic examples of non-weakly regular bent functions correspond to non-trivial partial difference sets, therefore, correspond to non-trivial strongly regular graphs.

For the ternary non-weakly regular bent functions in a subclass of the *GMMF* class, we also represent a construction method of two infinite families of translation association schemes of classes 5 and 6 in odd and even dimensions respectively. Furthermore, fusing the first or last three non-trivial relations of those association schemes we obtain association schemes of classes 3 and 4.

Finally, for a non-weakly regular bent function f satisfying certain conditions, we construct three-weight linear codes on the subsets $B^+(f)$ and $B^-(f)$ by using one of the known conventional construction methods. Moreover, we determine the weight distribution of the corresponding three-weight linear codes in the case of f belongs to a subclass of the *GMMF* class. In addition to these, we prove that our construction yields minimal linear codes nearly in all cases.

Keywords: bent, non-weakly regular bent, partial difference set, strongly regular graph, association scheme, linear codes, minimal linear codes

ÖZ

ZAYIF DÜZENLİ OLMAYAN BENT FONKSİYONLAR VE ALAKALI YAPILAR ÜZERİNE ÇALIŞMALAR

Pelen, Rumi Melih
Doktora, Matematik Bölümü
Tez Yöneticisi: Prof. Dr. Ferruh Özbudak

Temmuz 2020 , 84 sayfa

Bent fonksiyonlara ilgi hem matematiksel teori hem de pratik uygulamalardan kaynaklanıyor. Şu ana kadar, bent fonksiyonların çeşitli özelliklerini ele alan birçok yazılı kaynak oldu. Kodlama teorisi, kriptografi ve dizi inşasını da içeren çeşitli uygulamaları var. Bent fonksiyonlar dört alt sınıfa ayrılıyor; düzenli bent fonksiyonlar zayıf düzenli bent fonksiyonların, zayıf düzenli bent fonksiyonlar dual bent fonksiyonların içinde kalıyor. Bunlara ek olarak bir de zayıf düzenli bent fonksiyonlarla kesişimi olmayıp dual bent fonksiyonlar sınıfı ile kesişimi olan zayıf düzenli olmayan bent fonksiyonlar var. Bu tez çalışması, sonlu cisimler üzerindeki zayıf düzenli olmayan bent fonksiyonların çeşitli kombinatoryal özelliklerini ele alıyor.

Bu tezdeki ana sonuç, Çeşmelioğlu, Meidl ve Pott tarafından ortaya atılan " Duali zayıf düzenli bent olup, kendisi zayıf düzenli olmayan bent bir fonksiyon var mıdır?" açık probleminin çözümüdür. Ayrıca bu sonucu plato fonksiyonlara da genelledik.

Herhangi zayıf düzenli olmayan bir f bent fonksiyonu için $\mathbb{F}_{p^n}$ nin $B^+(f)$ ve $B^-(f)$ parçalanmasını tanımladık. Daha sonra, *GMMF* sınıfındaki zayıf düzenli olmayan bir

bent fonksiyona karşılık gelen parçalanma bize bir kısmi fark kümesi verirse bunun önemsiz kısmi fark kümesi olduğunu gösterdik. Ayrıca, zayıf düzenli olmayan bent fonksiyonların bilinen iki nadir örneğine karşılık gelen alt kümelerin önemsiz olmayan kısmi fark kümelerine ve dolayısıyla önemsiz olmayan kuvvetli düzenli grafiklere karşılık geldiğini gösterdik.

GMMF sınıfının bir alt sınıfındaki zayıf düzenli olmayan üçlü bent fonksiyonlar için tek ve çift boyutlarda sırasıyla sınıfı 5 ve 6 olan 2 adet sonsuz öteleme bağlantı şeması inşa eden bir yöntem sunduk. Ayrıca bu bağlantı şemalarının önemsiz olmayan ilk veya son üç ilişkisinin füzyonuyla sınıfı 3 ve 4 olan bağlantı şemaları elde ettik.

Son olarak, belirli koşulları sağlayan zayıf düzenli olmayan bir f fonksiyonu için bilinen jenerik inşa yöntemlerinden birini kullanarak $B^+(f)$ ve $B^-(f)$ alt kümeleri üzerinde ağırlığı 3 olan doğrusal kodlar inşa ettik. Ayrıca, f'in *GMMF* sınıfının bir alt sınıfına dahil olduğu durumda bu kodların ağırlık dağılımlarını belirledik. Bunlara ek olarak, inşaatımızın hemen hemen her durumda en düşük doğrusal kodları verdiğini kanıtladık.

Anahtar Kelimeler: bent, zayıf düzenli olmayan bent, kısmi fark kümesi, kuvvetli düzenli grafik, bağlantı şeması, doğrusal kodlar, en düşük doğrusal kodlar

To My Son Abdullah Yusuf

ACKNOWLEDGMENTS

Firstly, I would like to state my honest gratitude to my advisor Prof. Ferruh Özbudak for the continuous assistance of my Ph.D. study and associated research, for his patience, motivation, and substantial knowledge. His coaching helped me in all the time of lookup and writing of this thesis. I may want to no longer have imagined having a better guide and mentor for my Ph.D. study.

Besides my advisor, I would like to thank Assoc. Prof. Ali Özgür Kişisel, Assoc. Prof. Murat Cenk, Assoc. Prof. Barış Bülent Kırlar and Assist. Prof. Eda Tekin for being committee members of my defense.

I appreciate my mother in law Mediha Aykır and father in law Halil Aykır as they help in the care of our children many times during my Ph.D. study.

I am grateful to my parents Alaettin and Meliha Pelen for their hosting and endless support during my Ph.D. education. I also would like to thank my brother Semih Pelen due to his help with transportation to university many times.

Also, I would like to thank my colleagues in the Middle Black Sea Development Agency due to their tolerance for my weekly academic leave during the last two years of my Ph.D. study.

At last, this thesis might not exist at all without the cherish and back of my family. I would like to thank my spouse Neslihan Nesliye Pelen made incalculable self-devotion so that I might center on my research. In spite of the fact that he was as well youthful, my son Abdullah Yusuf Pelen persevered my absence for three years whereas I was week by week traveling between Ankara and Samsun; for his extraordinary give up, I can never thank him sufficient. I moreover would like to thank my young twin ladies Ayşe Pelen and Zehra Pelen made my life much more clever and colorful within the final year of my Ph.D. study.

TABLE OF CONTENTS

LIST OF TABLES

TABLES

LIST OF ABBREVIATIONS

ABBREVIATIONS

$\mathbb{Z}$	The ring of integers.
$\mathbb{Z}^+$	The set of positive integers.
$\mathbb{Q}$	The field of rational numbers.
$\mathbb{Q}(\epsilon_p)$	p-th cyclotomic field.
$\mathbb{C}$	The field of complex numbers.
$\mathbb{C}[G]$	The group ring of a group G over the complex field.
$\mathbf{0}$	Zero vector in a vector space of dimension greater than 1.
$\bar{z}$	Complex conjugate of z.
Tr	Trace function.
$A^\star$	The non zero elements in a set A.
$\#A$	The cardinality of a set A.
$-A$	The set consists of inverse elements of the subset A in a group.
$U^\perp$	Orthogonal complement of a subspace U of a vector space with respect to usual inner product.

CHAPTER 1

INTRODUCTION

In this thesis, we study various properties of non-weakly regular bent functions and related structures over finite fields. We can divide the thesis into four main part with respect to the chronological order as follows

- The duals of non-weakly regular bent functions;
- The relation between non-weakly regular bent functions, cyclotomic cosets, partial difference sets, and strongly regular graphs;
- The construction of translation association schemes from ternary bent functions in a subclass of the *GMMF* class;
- The construction of three-weight linear codes from non-weakly regular bent functions, the determination of their weight distributions when f belongs to a subclass of the *GMMF* class and the mimimality of constructed codes.

1.1 Motivation and Problem Definition

In 1976, Rothaus defined the bent functions as Boolean functions having constant magnitude Walsh transform. They have various applications including coding theory, cryptography and sequence designs. In 1985, Kumar, Scholtz, and Welch [29] generalized bent functions to arbitrary characteristics. Unlike the binary case, not all bent functions are regular over finite fields of odd characteristic. They're divided into four subclasses: regular bent functions that are contained within the class of weakly regular bent functions that are contained within the class of dual-bent functions (which

means that bent functions whose dual functions are also bent). Additionally there are *non-weakly regular bent* functions with no intersection with weakly regular, but an intersection with the class of dual-bent functions. It is known that duals of Boolean bent functions are also bent. However, in odd characteristic, duals of bent functions are not necessarily bent [14]. There are infinitely many non-weakly regular bent functions having bent or non-bent duals [14, 15]. It is quoted in [14] that,"...The existence of non-weakly regular bent functions with the dual f^* is weakly regular is an open problem..." In this thesis, among other things, we solve this open problem. Furthermore we show that if $f : \mathbb{F}_p^n \to \mathbb{F}_p$ is a non-weakly regular bent function such that its dual f^* is bent, then $f^{**}(-x) = f(x)$ for all $x \in \mathbb{F}_p^n$.

Partial difference sets (see the Definition 3.1.1 in Chapter 3) have been studied extensively because of their relations with different combinatorial structures such as two-weight codes and strongly regular graphs. There are a number of constructions of partial difference sets in elementary abelian groups, for a short survey see [31]. It is known that *Cayley* graphs such that their connection sets as are regular partial difference sets are strongly regular graphs (see the Definition 3.1.4 in Chapter 3). One of the instruments to build partial difference sets are bent functions. In [41], the authors proved that pre-image sets of the ternary weakly regular even bent functions are partial difference sets. Shortly after, this result is generalized to arbitrary odd characteristics in [16]. As far as we know, no one introduced a relation between non-weakly regular bent functions and partial difference sets. In this thesis, we also study the two special subsets of a finite field of odd characteristic related with the non-weakly regular bent functions which are introduced by the authors in [38]. We observe that these two subsets associated with the two sporadic examples of ternary non-weakly regular bent functions which are introduced in [24, 25] are non-trivial partial difference sets and are the union of the cyclotomic cosets with certain parameters. As a consequence of this, they are 2-class fusion schemes of some cyclotomic association schemes (see the definitions in Chapter 3) with certain parameters. We also present a further construction giving non-trivial PDSs from certain p-ary functions which are not bent functions. Moreover, we prove that if the corresponding subsets of non-weakly regular even bent functions in the *GMMF* class are partial difference sets then they are trivial.

Association schemes had been introduced with the aid of R.C. Bose and T. Shimamoto [7], studied similarly by way of the Bose–Mesner algebra brought in [6], generalized and given the most essential motivation by P. Delsarte [19]. The first text dedicated to the concept is [5]. A textual content that develops the idea each quite normally and notably is [23]. Association schemes supply an appropriate framework for treating certain issues from a range of exclusive areas of algebraic combinatorics, for example, coding theory, design theory, algebraic graph theory, finite group theory, and finite geometry. One of the tools to construct association schemes are bent functions. It is proven that for any odd prime p the collection of the pre-image sets of a p-ary weakly regular bent function form a p-class translation association scheme [39]. As far as we know, no one introduced a relation between non-weakly regular bent functions and d-class association schemes for some $d \geq 3$. In this paper, we construct association schemes of classes 5 and 6 from ternary non-weakly regular dual-bent functions in the *GMMF* class by proving that if they satisfy certain conditions then the collection of the pre-image sets of the dual functions with respect to the subsets $B_{\pm}(F)$ form translation schemes of classes 5 and 6 in odd and even dimensions respectively. Furthermore, we also obtain association schemes of classes 3 and 4 by fusing the first or last 3 non-trivial relations of the association schemes of classes 5 and 6 respectively.

Linear codes with a few weights have practices in secret sharing [1, 12, 22, 44], authentication codes [20], association schemes [10], and strongly regular graphs [11]. They have been substantially studied in the literature via a massive range of researchers and employed with the aid of many engineers. Some fascinating two-weight and three-weight codes can be found in [32, 22, 18, 21, 43, 46, 33]. There are quite a few methods to build linear codes, one of which is primarily based on functions over finite fields. Two familiar constructions, which are referred to as the first and second conventional constructions, of linear codes from functions have been extraordinary from the others in the literature. Recently, Mesnager [32] has built a new family of three-weight linear codes from weakly regular bent functions in odd characteristic based totally on the first conventional construction. Within this framework, we aim to build linear codes from non-weakly regular dual-bent functions based totally on the first conventional construction. To do this, instead of the whole space we

use the subset $B_+(f)$ or $B_-(f)$ associated with a non-weakly regular bent function f. We additionaly determine the weight distributions of the constructed codes when the associated non-weakly regular bent functions belong to a certain subclass of bent functions. As a specific type of linear codes, minimal linear codes have essential practices in secret sharing and reliable two-party computation. Constructing minimal linear codes with new and acceptable parameters has been an interesting research subject matter in coding theory and cryptography. Minimal linear codes have fascinating implementations in secret sharing [12, 44, 34, 26] and secure two-party computation [3, 17], and ought to be decoded with a minimal distance decoding method [2]. In the closing section, we examine that all non-zero codewords of the built codes are minimal for nearly all cases.

1.2 Contributions and Novelties

The main contributions of the present thesis study are followings:

- We solve the open problem which is quoted in [14] by proving that if the dual of a non-weakly regular bent function is bent then it is also non-weakly regular.
- We suspect a relation between non-weakly regular bent functions and cyclotomic association schemes. For some known sporadic examples of ternary non-weakly regular bent functions, we observe that the corresponding sets $B_{\pm}(f)$ can be written as union of certain cyclotomic cosets. Moreover, we show that these sets are non-trivial regular partial different sets hence correspond to non-trivial strongly regular graphs. In addition to these, we also present a further construction that certain p-ary functions which are not bent also give non-trivial partial difference sets.
- For the first time in literature, we construct an infinite family of (translation) association schemes from non-weakly regular bent functions.
- For the first time in literature, we construct few weights linear codes from non-weakly regular bent functions. We determine the weight distributions of the constructed codes when the corresponding non-weakly regular bent functions

belongs to a subclass of the *GMMF* class. Moreover, we prove that our construction yields minimal linear codes for almost all cases.

1.3 The Outline of the Thesis

The thesis is organized as follows.

In Chapter 2, we study the value distribution of duals of the non-weakly regular bent functions whose duals are also bent. This gives us information about regularity of the dual function f^*. We obtain analogous results for the plateaued functions over the finite fields of odd characteristic. In Chapter 3, we prove that if the two special subsets associated with the non-weakly regular even bent functions in the *GMMF* class are partial difference sets then they are trivial. We analyze the corresponding subsets of the two sporadic examples of ternary non-weakly regular bent functions. Our further construction giving non-trivial PDSs from certain p-ary functions which are not bent functions is also given. In Chapter 4, we prove that if a non-weakly regular ternary bent function in the *GMMF* class satisfies certain conditions then the collection of the pre-image sets of the dual function F^* with respect to subsets $B_{\pm}(F)$ form a translation scheme of class 5 in odd dimension and class 6 in even dimension. Furthermore by fusing the first or last 3 non-trivial relations of the corresponding association schemes we obtain 3 and 4 classes fusion schemes. We also give numerical examples. In Chapter 5, we build three-weight linear p-ary codes on $B_+(f)$ and $B_-(f)$ from non-weakly regular bent functions based on the first conventional construction. Moreover, we determine the weight distributions of the built codes when the associated non-weakly regular bent functions belong to a certain subclass of the *GMMF* bent functions. We observe that all non-zero codewords of the built codes are minimal for nearly all cases. We conclude in Chapter 6.

CHAPTER 2

THE DUALS OF NON-WEAKLY REGULAR BENT FUNCTIONS

In this chapter, we study the value distribution of duals of the non-weakly regular bent functions whose duals are also bent. This gives us information about regularity of the dual function f^*. Hence we prove that if dual function of a non-weakly regular bent function is bent then it is also non-weakly regular bent. We obtain analogous results for the plateaued functions over the finite fields of odd characteristic.

2.1 Preliminaries

Let p be an odd prime and $\mathbb{F}_{p^n}$ be the finite field of order p^n. Since it is a vector space of dimension n over $\mathbb{F}_p$, we also use the notation $\mathbb{F}_p^n$ which consists of n-tuples of the prime field $\mathbb{F}_p$. Let f be a function from $\mathbb{F}_p^n$ to $\mathbb{F}_p$. The Walsh transform of f at $\alpha \in \mathbb{F}_p^n$ is defined as a complex valued function $\hat{f}$ on $\mathbb{F}_p^n$

$$\hat{f}(\alpha) = \sum_{x \in \mathbb{F}_p^n} \epsilon_p^{f(x)-\alpha.x}$$

where $\epsilon_p = e^{\frac{2\pi i}{p}}$ and $\alpha.x$ denotes the usual dot product in $\mathbb{F}_p^n$.

The function f is called bent function if $|\hat{f}(\alpha)| = p^{n/2}$ for all $\alpha \in \mathbb{F}_p^n$. The normalized Walsh coefficient of a bent function f at α is defined by $p^{-n/2}\hat{f}(\alpha)$. The normalized Walsh coefficients of a bent function f are characterized in [29] as follows

$$p^{-n/2}\hat{f}(\alpha) = \begin{cases} \pm\epsilon_p^{f^*(\alpha)} & \text{if } n \text{ even or } n \text{ odd and } p \equiv 1 \bmod 4, \\ \pm i\epsilon_p^{f^*(\alpha)} & \text{if } n \text{ odd and } p \equiv 3 \bmod 4, \end{cases}$$

where f^* is a function from $\mathbb{F}_p^n$ to $\mathbb{F}_p$, which is called the dual of f.

A bent function $f : \mathbb{F}_p^n \to \mathbb{F}_p$ is called *regular* if $\forall\ \alpha \in \mathbb{F}_p^n$, we have

$$p^{-n/2}\hat{f}(\alpha) = \epsilon_p^{f^*(\alpha)}$$

and is called *weakly regular* if $\forall\ \alpha \in \mathbb{F}_p^n$, we have

$$p^{-n/2}\hat{f}(\alpha) = \xi\epsilon_p^{f^*(\alpha)}$$

where $\xi \in \{\pm 1, \pm i\}$ is independent from α, otherwise it is called *non-weakly regular*.

It is known that weakly regular bent functions appear in pairs since their duals are also weakly regular. If f is non-weakly regular, then f^* may not be a bent function. There are infinitely many examples of non-weakly regular bent functions f such that the dual is bent (resp. not bent) [15].

Let a be a positive integer and p be an odd prime number. Let $a \equiv \tilde{a}\ (mod\ p)$. The *Legendre symbol* is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } \tilde{a} = 0; \\ 1 & \text{if } \sqrt{\tilde{a}} \in \mathbb{F}_p^\star; \\ -1 & \text{if } \sqrt{\tilde{a}} \notin \mathbb{F}_p^\star. \end{cases}$$

The *trace* of $\alpha \in \mathbb{F}_{p^n}$ over $\mathbb{F}_p$ is defined as $\mathrm{Tr}_n(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + \cdots + \alpha^{p^{n-1}}$.

2.2 Value Distributions of the Duals of Non-weakly Regular Bent Functions

Let $f : \mathbb{F}_p^n \to \mathbb{F}_p$ be a non-weakly regular bent function and f^* be its dual function. Let $B_+(f)$ and $B_-(f)$ be the partitions of $\mathbb{F}_p^n$ given by

$$B_+(f) := \{w : w \in \mathbb{F}_p^n \mid \hat{f}(w) = \xi p^{\frac{n}{2}} \epsilon_p^{f^*(w)}\}$$

$$B_-(f) := \{w : w \in \mathbb{F}_p^n \mid \hat{f}(w) = -\xi p^{\frac{n}{2}} \epsilon_p^{f^*(w)}\},$$

where $\xi = 1$ if n is even or n odd and $p \equiv 1 \pmod 4$, and $\xi = i$ if n is odd and $p \equiv 3 \pmod 4$. Note that these sets are non empty as f is a non-weakly regular bent function. For any $y \in \mathbb{F}_p^n$ and $u \in \mathbb{F}_p$ we further define the sums $S_0(f, y),\ S_1(f, y)$ of complex numbers and integers $c_f(y, u),\ d_f(y, u)$ and $e_f(y, u)$ as follows:

$$S_0(f, y) = \sum_{\alpha \in B_+(f)} \epsilon_p^{f^*(\alpha)+\alpha.y}, \qquad S_1(f, y) = \sum_{\alpha \in B_-(f)} \epsilon_p^{f^*(\alpha)+\alpha.y},$$

and $c_f(y,u) := \#\{\alpha : \alpha \in B_+(f) \mid f^*(\alpha) + \alpha.y = u\}$, $d_f(y,u) := \#\{\alpha : \alpha \in B_-(f) \mid f^*(\alpha) + \alpha.y = u\}$, $e_f(y,u) = c_f(y,u) - d_f(y,u)$. For an arbitrary bent function $g : \mathbb{F}_p^n \to \mathbb{F}_p$ we define the type of g as

$$g(x) \text{ is of type } (+) \text{ if } \hat{g}(0) = \xi p^{\frac{n}{2}} \epsilon_p^{g^*(0)} \text{ and of type } (-) \text{ if } \hat{g}(0) = -\xi p^{\frac{n}{2}} \epsilon_p^{g^*(0)}.$$

The following lemma is a generalization of the Lemma in [36, page 156].

Lemma 2.2.1 *Let k be an integer. For a prime p there is a unique solution $(A_1, A_2, \ldots, A_{p-1})$ consisting of integers with $A_i = \left(\frac{i}{p}\right) p^k$ for $1 \leq i \leq p-1$, to the equation*

$$A_1\epsilon_p + A_2\epsilon_p^2 + \cdots + A_{p-1}\epsilon_p^{p-1} = \begin{cases} \sqrt{p}p^k & \text{for } p \equiv 1 \pmod 4, \\ i\sqrt{p}p^k & \text{for } p \equiv 3 \pmod 4. \end{cases} \tag{21}$$

Proof. Let $\mathbb{Q}(\epsilon_p)$ be the p-th cylotomic field. By a well known result on Gauss sums we have $\xi\sqrt{p} \in \mathbb{Q}(\epsilon_p)$ [30, Theorem 5.15]. Hence $\xi\sqrt{p}p^k \in \mathbb{Q}(\epsilon_p)$ for all $k \in \mathbb{Z}$. Since $\epsilon_p, \epsilon_p^2, \ldots, \epsilon_p^{p-1}$ is a basis for $\mathbb{Q}(\epsilon_p)$ over $\mathbb{Q}$ [30, Theorem 2.47 (i)], there exist uniquely determined coefficients $A_i \in \mathbb{Q}$ satisfying equation (21). Moreover again using [30, Theorem 5.15] we obtain a solution $A_i = \left(\frac{i}{p}\right) p^k$ for $1 \leq k \leq p-1$. □

For an arbitrary function $g : \mathbb{F}_p^n \to \mathbb{F}_p$ and $i \in \mathbb{F}_p$, let $N_i(g)$ denote the cardinality $\#\{x \in \mathbb{F}_p^n | g(x) = i\}$. In the following two propositions we determine $N_i(g)$ for a bent function g, depending on the type of g explicitly when n is odd and n is even, respectively. We start with n odd as its proof is more involved.

Proposition 2.2.1 *Let $g : \mathbb{F}_p^n \to \mathbb{F}_p$ be a bent function and n is odd. For $g^*(0) = i_0$ we have*

$$N_{i_0}(g) = p^{n-1}, \quad N_{i_0+j}(g) = p^{n-1} \pm \left(\frac{j}{p}\right) p^{\frac{n-1}{2}}, \quad \text{for } 1 \leq j \leq p-1.$$

Here the sign is $+$ (respectively $-$) if and only if the type of g is $(+)$ (respectively $(-)$).

Proof. Since g is bent and n is odd we have

$$\hat{g}(0) = \sum_{i=0}^{p-1} N_i(g)\epsilon_p^i = \eta_0 \xi p^{\frac{n}{2}} \epsilon_p^{g^*(0)}$$

where $\eta_0 \in \{-1, 1\}$, $\xi = 1$ if $p \equiv 1 \pmod 4$ and $\xi = i$ if $p \equiv 3 \pmod 4$. Assume that g is of type $(+)$. Then $\eta_0 = 1$. Recall that $g^*(0) = i_0$. Then we have $\sum_{i=0}^{p-1} N_i(g)\epsilon_p^i = \xi\sqrt{p}p^{\frac{n-1}{2}}\epsilon_p^{i_0}$. Dividing by $\epsilon_p^{i_0}$ we get

$$\xi\sqrt{p}p^{\frac{n-1}{2}} = \sum_{i=0}^{p-1} N_i(g)\epsilon_p^{i-i_0} = N_{i_0}(g) + \sum_{j=1}^{p-1} N_{i_0+j}(g)\epsilon_p^j = \sum_{j=1}^{p-1}(N_{i_0+j}(g) - N_{i_0}(g))\epsilon_p^j.$$

Note that putting $A_j = N_{i_0+j}(g) - N_{i_0}(g)$ we obtain that $(A_1, A_2, \ldots, A_{p-1})$ is a solution of the equation $A_1\epsilon_p + A_2\epsilon_p^2 + \cdots + A_{p-1}\epsilon_p^{p-1} = \xi\sqrt{p}p^{\frac{n-1}{2}}$. Hence by Lemma 2.2.1 we obtain that

$$N_{i_0+j}(g) = N_{i_0}(g) + \left(\frac{j}{p}\right) p^{\frac{n-1}{2}}.$$

As $\sum_{j=1}^{p-1} N_{i_0+j}(g) + N_{i_0}(g) = p^n$ we get $N_{i_0}(g) = p^{n-1}$. Then $N_{i_0+j}(g) = p^{n-1} + \left(\frac{j}{p}\right) p^{\frac{n-1}{2}}$.

Assume that g is of type $(-)$. Then $\eta_0 = -1$. By similar arguments we obtain that

$$N_{i_0+j}(g) = N_{i_0}(g) - \left(\frac{j}{p}\right) p^{\frac{n-1}{2}} \text{ for } 1 \le j \le p-1, \text{ and } N_{i_0}(g) = p^{n-1}.$$

□

Proposition 2.2.2 *Let $g : \mathbb{F}_p^n \to \mathbb{F}_p$ be a bent function and n is even. For $g^*(0) = i_0$ we have*

$$N_{i_0}(g) = p^{n-1} \pm p^{\frac{n}{2}} \mp p^{\frac{n}{2}-1} \text{ and } N_i(g) = p^{n-1} \mp p^{\frac{n}{2}-1}, \text{ for } i \neq i_0 \in \mathbb{F}_p.$$

Here the sign is $+$ (respectively $-$) if and only if the type of g is $(+)$ (respectively $(-)$).

Proof. Since g is bent and n is even we have $\hat{g}(0) = \sum_{i=0}^{p-1} N_i(g)\epsilon_p^i = \pm p^{\frac{n}{2}}\epsilon_p^{g^*(0)}$. Recall that $g^*(0) = i_0$. Then

$$(N_{i_0}(g) \mp p^{\frac{n}{2}})\epsilon_p^{i_0} + \sum_{i \neq i_0} N_i(g)\epsilon_p^i = 0.$$

Dividing by $\epsilon_p^{i_0}$ and using the Lemma 2.2.1 as in Proposition 2.2.1 we complete the proof. □

Recall that $f : \mathbb{F}_p^n \to \mathbb{F}_p$ is a non-weakly regular bent function and $e_f(y, u)$ is an integer for $y \in \mathbb{F}_p^n$ and $u \in \mathbb{F}_p$ defined above. From now on, if n is even then we put $n = 2m$, and if n is odd then we put $n = 2m + 1$.

Lemma 2.2.2 *Let n be odd. There exists an integer k such that for every $y \in \mathbb{F}_p^n$ we have*

- *If $p \equiv 1 (mod\ 4)$ then, $e_f(y, u_0) = k$ and $e_f(y, u_0 + i) = k + \left(\frac{i}{p}\right) p^m$ for $1 \leq i \leq p-1$;*
- *If $p \equiv 3 (mod\ 4)$ then, $e_f(y, u_0) = k$ and $e_f(y, u_0 + i) = k - \left(\frac{i}{p}\right) p^m$ for $1 \leq i \leq p-1$;*

where $u_0 = f(y)$.

Proof. Consider first the case $p \equiv 1 \pmod 4$. By inverse Walsh transform we have

$$p^{2m+1} \epsilon_p^{f(y)} = \sum_{\alpha \in \mathbb{F}_p^{2m+1}} \epsilon_p^{\alpha.y} \hat{f}(\alpha).$$

As f is bent, for $\alpha \in \mathbb{F}_p^{2m+1}$, we have $\hat{f}(\alpha) = \xi_\alpha p^m \sqrt{p} \epsilon_p^{f^*(\alpha)}$, where $\xi_\alpha \in \{-1, 1\}$ depending on α. Therefore we get

$$p^m \sqrt{p} \epsilon_p^{u_0} = \sum_{\alpha \in \mathbb{F}_p^{2m+1}} \xi_\alpha \epsilon_p^{f^*(\alpha) + \alpha.y}.$$

Using the definition of $e_f(y, u)$, this implies that

$$p^m \sqrt{p} \epsilon_p^{u_0} = e_f(y, u_0) \epsilon_p^{u_0} + \sum_{u \in \mathbb{F}_p \setminus \{u_0\}} e_f(y, u) \epsilon_p^u.$$

Dividing by $\epsilon_p^{u_0}$ we have

$$p^m \sqrt{p} = e_f(y, u_0) + \sum_{u \in \mathbb{F}_p \setminus \{u_0\}} e_f(y, u) \epsilon_p^{u - u_0}.$$

Putting $e_f(y, u_0 + i) = b_i$ for $i \in \mathbb{F}_p$, we have

$$\sum_{i \in \mathbb{F}_p} b_i \epsilon_p^i = p^m \sqrt{p}.$$

Using Lemma 2.2.1 we conclude that there exists an integer k such that

$$e_f(y, u_0) = k \text{ and } e_f(y, u_0 + i) = k + \left(\frac{i}{p}\right) p^m \text{ for } 1 \leq i \leq p-1.$$

Next we consider the case $p \equiv 3 \pmod 4$. By inverse Walsh transform we have

$$-ip^m \sqrt{p} \epsilon_p^{u_0} = e_f(y, u_0) \epsilon_p^{u_0} + \sum_{u \in \mathbb{F}_p \setminus \{u_0\}} e_f(y, u) \epsilon_p^u.$$

Using similar arguments and putting $-e_f(y, u_0 + i) = b_i$ for $i \in \mathbb{F}_p$ we obtain

$$\sum_{i \in \mathbb{F}_p} b_i \epsilon_p^i = i p^m \sqrt{p}.$$

Again from Lemma 2.2.1 we conclude that there exists an integer k such that

$$e_f(y, u_0) = k \text{ and } e_f(y, u_0 + i) = k - \left(\frac{i}{p}\right) p^m \text{ for } 1 \leq i \leq p-1.$$

Now let us show that k does not depend on y. Observe that for any $y \in \mathbb{F}_p^{2m+1}$ and $j \in \mathbb{F}_p$ we have

$$c_f(y, j) = \frac{N_j(f^*(x) + x.y) + e_f(y, j)}{2} \text{ and } d_f(y, j) = \frac{N_j(f^*(x) + x.y) - e_f(y, j)}{2}.$$

On the other hand,

$$\#B_+(f) = \sum_{j=0}^{p-1} c_f(y, j) \text{ and } \#B_-(f) = \sum_{j=0}^{p-1} d_f(y, j).$$

Combining them with the identity $\sum_{j=0}^{p-1} N_j(f^*(x) + x.y) = p^{2m+1}$ we get,

$$\#B_+(f) = \frac{p^{2m+1} + pk}{2} \text{ and } \#B_-(f) = \frac{p^{2m+1} - pk}{2}.$$

As $\#B_+(f)$ and $\#B_-(f)$ are constants, we conclude that k is independent of y.

□

Lemma 2.2.3 *Let n be even. There exists an integer k such that for every $y \in \mathbb{F}_p^n$ we have*

$$e_f(y, u) = \begin{cases} k + p^m & \text{if } f(y) = u, \\ k & \text{otherwise}. \end{cases}$$

Proof. By inverse Walsh transform we have

$$p^m \epsilon_p^{f(y)} = \sum_{\alpha \in \mathbb{F}_p^{2m}} \epsilon_p^{\alpha.y} \hat{f}(\alpha).$$

As f is bent, for $\alpha \in \mathbb{F}_p^{2m}$, $\hat{f}(\alpha) = \xi_\alpha p^m \epsilon_p^{f^*(\alpha)}$, where $\xi_\alpha \in \{-1, 1\}$. Therefore we get

$$p^m \epsilon_p^{f(y)} = \sum_{\alpha \in \mathbb{F}_p^{2m}} \xi_\alpha \epsilon_p^{f^*(\alpha) + \alpha.y}.$$

Using the definition of $e_f(y,u)$ we get

$$p^m\epsilon_p^{u_0} = e_f(y,u_0)\epsilon_p^{u_0} + \sum_{u\in\mathbb{F}_p\setminus\{u_0\}} e_f(y,u)\epsilon_p^u.$$

Dividing by $\epsilon_p^{u_0}$ and applying Lemma 2.2.1 we complete the proof. Moreover uniqueness of k can be shown by using similar arguments as in the proof of Lemma 2.2.2. □

Remark 2.2.1 *In Lemmas 2.2.3 and 2.2.2, we do not determine k explicitly. In fact k is independent of y, it only depends on the cardinalities $\#B_+(f)$ and $\#B_-(f)$. Using Magma we determine k for the following sporadic examples of ternary non-weakly regular bent functions [14, page 429].*

Example 1 *$g_1 : \mathbb{F}_{3^6} \to \mathbb{F}_3$, $g_1(x) = Tr_6(\lambda^7 x^{98})$ is a non-weakly regular bent function. We have $\#B_+(g_1) = 504,\ \#B_-(g_1) = 225$ and $k = 84$.*

Example 2 *$g_2 : \mathbb{F}_{3^6} \to \mathbb{F}_3$, $g_2(x) = Tr_6(\lambda x^{20} + \lambda^{41}x^{92})$ is non-weakly regular bent. We have $\#B_+(g_2) = 648,\ \#B_-(g_2) = 81$ and $k = 180$.*

From now on we further assume that the dual function f^* of f is bent as well. For $y \in \mathbb{F}_p^n$, let $g_y : \mathbb{F}_p^n \to \mathbb{F}_p$ be the function

$$g_y(x) := f^*(x) + x.y,$$

which is a bent function affine equivalent to f^*. For $y, \alpha \in \mathbb{F}_{p^n}$, it follows from the definition that

$$\hat{g_y}(\alpha) = \hat{f}^*(\alpha - y). \tag{22}$$

As f^* is bent, it follows from the definitions that

$$S_0(f,y) + S_1(f,y) = \pm\xi p^{n/2}\epsilon_p^{i_y} \tag{23}$$

where $0 \le i_y \le p-1$ depends on y. In the following two lemmas we determine the sign and the value of i_y in (23) exactly.

Lemma 2.2.4 *Let n be odd. Under notation and assumptions as above we have*

$$\hat{f}^*(-y) = S_0(f,y) + S_1(f,y) = \begin{cases} \xi p^m \sqrt{p} \epsilon_p^{f(y)} & \text{if } g_y \text{ is of type } (+), \\ -\xi p^m \sqrt{p} \epsilon_p^{f(y)} & \text{if } g_y \text{ is of type } (-), \end{cases} \tag{24}$$

where $\xi \in \{1, i\}$ depending on p.

Proof. It follows from the definition that

$$\hat{g_y}(0) = S_0(f,y) + S_1(f,y). \tag{25}$$

Using (22) and (25) we obtain that $\hat{f}^*(-y) = S_0(f,y) + S_1(f,y)$. In the rest of this proof we show that the equality in the right hand side of (24) holds.

For $y \in \mathbb{F}_{p^{2m+1}} = \mathbb{F}_{p^n}$ let $u_0 = f(y)$ and $i_0 = g_y^*(0)$. For $u \in \mathbb{F}_p$ by definition we have

$$c_f(y,u) = \frac{N_u(g_y) + e_f(y,u)}{2} \quad \text{and} \quad d_f(y,u) = \frac{N_u(g_y) - e_f(y,u)}{2}. \tag{26}$$

Using the fact that $c_f(y,u)$ is an integer for $u \in \mathbb{F}_p$, we prove that $u_0 = i_0$. Our method of the proof of $u_0 = i_0$ is as follows: Assume the contrary that $u_0 \neq i_0$. Let $t_0 \in \mathbb{F}_p \setminus \{u_0, i_0\}$. There exists such $t_0 \in \mathbb{F}_p \setminus \{u_0, i_0\}$ as $p \geq 3$. We will show that the fact $c_f(y,i_0)$ is an integer implies that $e_f(y,u_0)$ is an even integer. We will also show that the fact $c_f(y,t_0)$ is an integer implies that $e_f(y,u_0)$ is an odd integer. Hence these arguments will imply to the contradiction on the parity of $e_f(y,u_0)$ and we will obtain that $u_0 = i_0$.

Now we explain the details of these arguments. By Proposition 2.2.1 the integer $N_{i_0}(g_y)$ is odd. As $c_f(y,i_0) = (N_{i_0}(g_y) + e_f(y,i_0))/2$ by (26) and $c_f(y,i_0)$ is an integer, we get that $e_f(y,i_0)$ is odd. Using Lemma 2.2.2 we have $e_f(y,i_0) = e_f(y,u_0) \pm \left(\frac{i_0-u_0}{p}\right) p^m$ as $i_0 \neq u_0$. As $e_f(y,i_0)$ is odd we obtain that $e_f(y,u_0)$ is even.

Similarly we consider $c_f(y,t_0)$. By Proposition 2.2.1 we have $N_{t_0} = p^{2m} \pm \left(\frac{t_0-i_0}{p}\right) p^m$ as $t_0 \neq i_0$. Hence the integer $N_{t_0}(g_y)$ is even. As $c_f(y,t_0) = (N_{t_0}(g_y) + e_f(y,t_0))/2$ by (26) and $c_f(y,t_0)$ is an integer, we get that $e_f(y,t_0)$ is even. Using Lemma 2.2.2 we have $e_f(y,t_0) = e_f(y,u_0) \pm \left(\frac{t_0-u_0}{p}\right) p^m$ as $t_0 \neq u_0$. As $e_f(y,t_0)$ is even we obtain that $e_f(y,u_0)$ is odd. These arguments complete the proof of the fact that $u_0 = i_0$.

The rest of the proof of the lemma is presented case by case. There are four cases to consider.

Case $p \equiv 1 \pmod 4$ and g_y is of type $(+)$:

Let $k = e_f(y, u_0)$. Using Proposition 2.2.1, Lemma 2.2.2, the fact $u_0 = i_0$ and (26) we obtain that

$$c_f(y,u) = \begin{cases} \frac{p^{2m}+k}{2}. & \text{if } u = u_0, \\ \frac{p^{2m}+k+2\left(\frac{u-u_0}{p}\right)p^m}{2} & \text{if } u \neq u_0, \end{cases} \quad d_f(y,u) = \begin{cases} \frac{p^{2m}-k}{2} & \text{if } u = u_0, \\ \frac{p^{2m}-k}{2} & \text{if } u \neq u_0. \end{cases}$$

By definition we have $S_0(f,y) = \sum_{j=0}^{p-1} c_f(y,j)\epsilon_p^j$. Putting the values of $c_f(y,u)$ in the definition of $S_0(f,y)$ we obtain that

$$\begin{aligned} S_0(f,y) &= \tfrac{p^{2m}+k}{2}\epsilon_p^{u_0} + \textstyle\sum_{u\in\mathbb{F}_p\setminus\{u_0\}} \frac{p^{2m}+k+2\left(\frac{u-u_0}{p}\right)p^m}{2}\epsilon_p^u \\ &= \tfrac{p^{2m}+k}{2}\textstyle\sum_{u=0}^{p-1}\epsilon_p^u + \sum_{u\in\mathbb{F}_p\setminus\{u_0\}}\left(\frac{u-u_0}{p}\right)p^m\epsilon_p^u \\ &= \textstyle\sum_{u\in\mathbb{F}_p\setminus\{u_0\}}\left(\frac{u-u_0}{p}\right)p^m\epsilon_p^u \qquad (\text{ as } \textstyle\sum_{u=0}^{p-1}\epsilon_p^u = 0\ ) \\ &= p^m\epsilon_p^{u_0}\textstyle\sum_{u\in\mathbb{F}_p\setminus\{u_0\}}\left(\frac{u-u_0}{p}\right)\epsilon_p^{u-u_0}. \end{aligned}$$

Put $A_{u-u_0} = \left(\frac{u-u_0}{p}\right)p^m$. Then by Lemma 2.2.1 we get $S_0(f,y) = \sqrt{p}p^m\epsilon_p^{u_0} = \sqrt{p}p^m\epsilon_p^{f(y)}$.

By definition we have $S_1(f,y) = \sum_{j=0}^{p-1} d_f(y,j)\epsilon_p^j$. Putting the values of $d_f(y,u)$ in the definition of $S_1(f,y)$ we obtain that

$$S_1(f,y) = \sum_{j=0}^{p-1}\frac{p^{2m}-k}{2}\epsilon_p^j = \frac{p^{2m}-k}{2}\sum_{j=0}^{p-1}\epsilon_p^j = 0.$$

Case $p \equiv 1 \pmod 4$ and g_y is of type $(-)$: By similar arguments we have,

$$c_f(y,u) = \begin{cases} \frac{p^{2m}+k}{2}. & \text{if } u = u_0, \\ \frac{p^{2m}+k}{2} & \text{if } u \neq u_0, \end{cases} \quad d_f(y,u) = \begin{cases} \frac{p^{2m}-k}{2} & \text{if } u = u_0, \\ \frac{p^{2m}-k-2\left(\frac{u-u_0}{p}\right)p^m}{2} & \text{if } u \neq u_0. \end{cases}$$

Applying similar arguments as in the previous case, we obtain that $S_0(f,y) = 0$ and $S_1(f,y) = -p^m\sqrt{p}\epsilon_p^{f(y)}$.

Case $p \equiv 3 \pmod 4$ and g_y is of type $(+)$: By similar arguments we have,

$$c_f(y,u) = \begin{cases} \frac{p^{2m}+k}{2}. & \text{if } u = u_0, \\ \frac{p^{2m}+k}{2} & \text{if } u \neq u_0, \end{cases} \quad d_f(y,u) = \begin{cases} \frac{p^{2m}-k}{2} & \text{if } u = u_0, \\ \frac{p^{2m}-k+2\left(\frac{u-u_0}{p}\right)p^m}{2} & \text{if } u \neq u_0. \end{cases}$$

Applying similar arguments as in the first case, we obtain that $S_0(f,y) = 0$ and $S_1(f,y) = ip^m\sqrt{p}\epsilon_p^{f(y)}$.

Case $p \equiv 3 \pmod 4$ and g_y is of type $(-)$: By similar arguments we have,

$$c_f(y,u) = \begin{cases} \frac{p^{2m}+k}{2}. & \text{if } u = u_0, \\ \frac{p^{2m}+k-2\left(\frac{u-u_0}{p}\right)p^m}{2} & \text{if } u \neq u_0, \end{cases} \quad d_f(y,u) = \begin{cases} \frac{p^{2m}-k}{2} & \text{if } u = u_0, \\ \frac{p^{2m}-k}{2} & \text{if } u \neq u_0. \end{cases}$$

Applying similar arguments as in the first case, we obtain that $S_0(f,y) = -ip^m\sqrt{p}\epsilon_p^{f(y)}$ and $S_1(f,y) = 0$. □

Lemma 2.2.5 *Let n be even. Under notation and assumptions as above we have*

$$\hat{f}^*(-y) = S_0(f,y) + S_1(f,y) = \begin{cases} p^m\epsilon_p^{f(y)} & \textit{if } g_y \textit{ is of type } (+), \\ -p^m\epsilon_p^{f(y)} & \textit{if } g_y \textit{ is of type } (-). \end{cases} \tag{27}$$

Proof. The proof is similar to the proof of Lemma 2.2.4. Using the same arguments we get $\hat{f}^*(-y) = S_0(f,y) + S_1(f,y)$. We show the equality in the right hand side of (27) below in this proof.

Again let $u_0 = f(y)$ and $i_0 = g_y^*(0)$. Note that (26) holds here as well. We prove that $u_0 = i_0$ similar to the proof of Lemma 2.2.4. The main differences are that we use Proposition 2.2.2 instead of Proposition 2.2.1 and we use Lemma 2.2.3 instead of Lemma 2.2.2. Assume that $u_0 \neq i_0$. Let $t_0 \in \mathbb{F}_p \setminus \{u_0, i_0\}$. First we consider the integer $c_f(y,i_0)$. By Proposition 2.2.2, the integer $N_{i_0}(g_y)$ is odd. As in the proof of Lemma 2.2.4, using (26) and the fact that $c_f(y,i_0)$ is an integer we obtain that $e_f(y,i_0)$ is an odd integer. Using Lemma 2.2.3 we have $e_f(y,i_0) = e_f(y,u_0) - p^m$ as $i_0 \neq u_0$. As $e_f(y,i_0)$ is odd, we conclude that $e_f(y,u_0)$ is an even integer.

Next we consider the integer $c_f(y,t_0)$. By Proposition 2.2.2, we have $N_{t_0}(g_y) = p^{2m-1} \mp p^{m-1}$ as $t_0 \neq i_0$. Hence the integer $N_{t_0}(g_y)$ is even. As in the proof of Lemma 2.2.4, using (26) and the fact that $c_f(y,t_0)$ is an integer we obtain that $e_f(y,t_0)$ is an

even integer. Using Lemma 2.2.3 we have $e_f(y,t_0) = e_f(y,u_0) - p^m$ as $t_0 \neq u_0$. As $e_f(y,t_0)$ is even, we conclude that $e_f(y,u_0)$ is an odd integer.

These arguments lead to the contradiction on the parity of the integer $e_f(y,u_0)$. Hence our assumption is wrong and we complete the proof of the fact that $u_0 = i_0$.

For arbitrary $t \in \mathbb{F}_p \setminus \{u_0\}$ let $k = e_f(y,t)$. Using Lemma 2.2.3 we note that k is independent from the choice of $t \in \mathbb{F}_p \setminus \{u_0\}$.

Assume that g_y is of type $(+)$. Using Proposition 2.2.2, Lemma 2.2.3, the fact $u_0 = i_0$ and (26) we obtain that

$$c_f(y,u) = \begin{cases} \frac{p^{2m-1}+2p^m-p^{m-1}+k}{2} & \text{if } u = u_0, \\ \frac{p^{2m-1}-p^{m-1}+k}{2} & \text{if } u \neq u_0, \end{cases} \quad d_f(y,u) = \begin{cases} \frac{p^{2m-1}-p^{m-1}-k}{2} & \text{if } u = u_0, \\ \frac{p^{2m-1}-p^{m-1}-k}{2} & \text{if } u \neq u_0. \end{cases}$$

Putting these values in the definitions we obtain that $S_0(f,y) = p^m \epsilon_p^{f(y)}$ and $S_1(f,y) = 0$.

The proof of the case g_y is of type $(-)$ is similar. □

Now we are ready to state our first theorem.

Theorem 2.2.1 *Let $f : \mathbb{F}_p^n \to \mathbb{F}_p$ be a non-weakly regular bent function whose dual function f^* is bent as well. Let $f^{**} : \mathbb{F}_p^n \to \mathbb{F}_p$ be the dual function of f^*. For $y \in \mathbb{F}_p^n$ we have*

$$f^{**}(y) = f(-y).$$

Proof. As f^* is bent we have

$$\hat{f^*}(-y) = \eta_{-y} \xi p^{\frac{n}{2}} \epsilon_p^{f^{**}(-y)}, \tag{28}$$

where $\eta_{-y} \in \{-1, 1\}$ depending on y. Combining Lemmas 2.2.4, 2.2.5 and (28) we complete the proof. □

As an immediate consequence of Theorem 2.2.1, we solve the quoted open problem of [14].

Corollary 2.2.1 *Let $f : \mathbb{F}_p^n \to \mathbb{F}_p$ be a non-weakly regular bent function whose dual function f^* is bent as well. Then f^* is also non-weakly regular.*

Proof. Assume that f^* is weakly regular. Then its dual f^{**} must also be weakly regular. However by Theorem 2.2.1 , f^{**} is equivalent to f and hence f^{**} is non-weakly regular. □

2.3 The Duals of Plateaued Functions

In this section we generalize our results in Section 2.2 to plateaued functions. We also generalize two results of Nyberg [36] on Hamming distance of bent functions to a nearest affine function in Corollary 2.3.1 below.

We define non-weakly regular plateaued functions using the notation in [33] for weakly regular plateaued functions.

Definition 2.3.1 *A function $f : \mathbb{F}_p^n \to \mathbb{F}_p$ is called s-plateaued if*

$$|\hat{f}(\alpha)| = p^{\frac{n+s}{2}} \text{ or } 0$$

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

The Walsh spectrum of s-plateaued functions is given as follows (see [27]).

Theorem 2.3.1 *Let $f : \mathbb{F}_p^n \to \mathbb{F}_p$ be an s-plateaued function then*

$$\hat{f}(\alpha) = \begin{cases} \pm p^{\frac{n+s}{2}} \epsilon_p^{f^*(\alpha)}, 0 & \text{if } n+s \text{ even or } n+s \text{ odd and } p \equiv 1 \bmod 4, \\ \pm i p^{\frac{n+s}{2}} \epsilon_p^{f^*(\alpha)}, 0 & \text{if } n+s \text{ odd and } p \equiv 3 \bmod 4, \end{cases}$$

where f^* is a function from support of $\hat{f}$ to $\mathbb{F}_p$.

Let us call f^* the dual of f. We denote support of $\hat{f}$ by $\mathrm{Supp}(\hat{f})$ and it is defined as

$$\mathrm{Supp}(\hat{f}) := \{\alpha : \alpha \in \mathbb{F}_p^n \mid \hat{f}(\alpha) \neq 0\}.$$

Observe that, if f is an s-plateaued function over $\mathbb{F}_p^n$, by Parseval identity we have $\#\mathrm{Supp}(\hat{f}) = p^{n-s}$. Observe that if $s \geq 1$ then f^* has restricted domain which is different from the case of bent functions. The following definition is given in [33].

Definition 2.3.2 *Let $f : \mathbb{F}_p^n \to \mathbb{F}_p$ be an s-plateaued function such that for all $\alpha \in \mathrm{Supp}(\hat{f})$*

$$\hat{f}(\alpha) = up^{\frac{n+s}{2}}\epsilon_p^{f^*(\alpha)}$$

where $u \in \{\pm 1, \pm i\}$ is independent from α. Then f is called a weakly regular s-plateaued function. When $u = 1$, f is called regular s-plateaued. If u changes with respect to α then f is called non-weakly regular s-plateaued.

Definition 2.3.3 *Let S be a subset of $\mathbb{F}_p^n$ with cardinality N and f be a function from S to $\mathbb{F}_p$. If $\mid \hat{f}(\alpha) \mid = N^{1/2}$ for all $\alpha \in \mathbb{F}_p^n$, f is called bent relative to S where $\hat{f}(\alpha) = \sum_{x \in S} \epsilon_p^{f(x)-\alpha.x}$.*

Remark 2.3.1 *Observe that if $S = \mathbb{F}_p^n$, the notion is the same as for bent functions. Note that, we still continue to use the notation $\hat{f}$ even if $S \neq \mathbb{F}_p^n$ which can be viewed as a restricted Walsh transform over S. Moreover, if $N = p^m$ for some $m < n$, by using same techniques as in ([29]), one can derive that normalized Walsh coefficients of corresponding relative bent function belongs to the set $\{\pm 1, \pm i\}$ which changes with respect to p and parity of m, as in the case of bent functions.*

Proposition 2.3.1 *Let $f : \mathbb{F}_p^n \to \mathbb{F}_p$ be a weakly regular s-plateaued function then f^* is bent relative to $\mathrm{Supp}(\hat{f})$. Moreover we have*

$$\hat{f^*}(\alpha) = u^{-1}p^{\frac{n-s}{2}}\epsilon_p^{f(-\alpha)} \text{for all } \alpha \in \mathbb{F}_p^n$$

where $\hat{f}(\alpha) = up^{\frac{n+s}{2}}\epsilon_p^{f^*(\alpha)}$ for all $\alpha \in \mathrm{Supp}(\hat{f})$.

Proof. See, [33, Lemma 6]. □

Remark 2.3.2 *Under the notation of Proposition 2.3.1 we also get that $f^{**}(x)$ is weakly regular s-plateaued function over $\mathbb{F}_p^n$ and f^* is weakly regular bent function relative to $\mathrm{Supp}(\hat{f})$.*

The situation is different for non-weakly regular plateaued functions. As in the case of non-weakly regular bent functions, there are two possibilities for the dual of non-weakly regular plateaued functions: the dual may be bent relative to $\mathrm{Supp}(\hat{f})$ and the dual may not be bent relative to $\mathrm{Supp}(\hat{f})$. Both cases happen infinitely often.

Example 3 *Let $g : \mathbb{F}_p^r \to \mathbb{F}_p$ be a non-weakly regular bent whose dual is a bent (resp. not bent) function. There are infinitely many such functions [14, 15]. For $s \geq 1$ let $n = r + s$ and $f : \mathbb{F}_p^r \times \mathbb{F}_p^s \to \mathbb{F}_p$ be the function defined as $f(x, y) = g(x)$. Then f is an s-plateaued function which is non-weakly regular and also the dual f^* is bent (resp. not bent) relative to* $\mathrm{Supp}(f)$.

Example 4 *Note that the function f in Example 3 is partially bent. In fact there are also infinitely many non-weakly regular μ-plateaued functions f with $\mu \geq 1$ whose dual f^* is bent (resp. not bent) with respect to* $\mathrm{Supp}(f)$*, and f is not partially bent. These correspond to a different infinite class then the ones in Example 3. Let $g : \mathbb{F}_p^r \to \mathbb{F}_p$ be a regular μ-plateaued function with $\mu \geq 1$, which has no nonzero linear structure. Let $h : \mathbb{F}_p^t \to \mathbb{F}_p$ be be a non-weakly regular bent whose dual is a bent (resp. not bent) function. There are infinitely many such h functions [14, 15]. Let $n = r + t$ and $f : \mathbb{F}_p^r \times \mathbb{F}_p^t \to \mathbb{F}_p$ be the defined as $f(x, y) = g(x) + h(y)$. Then f has no nonzero linear structure $(\alpha, \beta) \in \mathbb{F}_p^r \times \mathbb{F}_p^t$. Indeed if $\alpha \neq 0$, then the map $(x, y) \mapsto g(x+\alpha)-g(x)+h(y+\beta)-h(y)$ cannot be constant on $\mathbb{F}_p^r \times \mathbb{F}_p^t$. Otherwise for a fixed $y_0 \in \mathbb{F}_p^t$ we obtain a constant map $x \mapsto g(x + \alpha) - g(x) + h(y_0 + \beta) - h(y_0)$ on $\mathbb{F}_p^r$, which is a contradiction as g has no nonzero linear structure. Recall that a bent function cannot have a nonzero linear structure. Hence if $\beta \neq 0$, then $(\alpha, \beta) \in \mathbb{F}_p^r \times \mathbb{F}_p^t$ cannot be a linear structure of f. These arguments show that f has no nonzero linear structure and f is not partially bent. As g is μ-plateaued with* $\mathrm{Supp}(g) \subsetneq \mathbb{F}_p^r$*, we get that f is μ-plateaued with* $\mathrm{Supp}(f) = \mathrm{Supp}(g) \times \mathbb{F}_p^t \subsetneq \mathbb{F}_p^r \times \mathbb{F}_p^t$*. If $(x, y) \in \mathrm{Supp}(f)$, then for the dual f^* we have $f^*(x, y) = g^*(x) + h^*(y)$, where g^* and h^* are the duals of g and h. As g is regular and h is non-weakly regular we obtain that f is non-weakly regular. Finally f^* is is bent (resp. not bent) with respect to* $\mathrm{Supp}(f)$ *as h is bent (resp. not bent). We give an explicit example of a regular μ-plateaued function with $\mu \geq 1$ which has no nonzero linear structure as follows: Let $g : \mathbb{F}_3^3 \to \mathbb{F}_3$ be the function given by $g(x, y, z) = z$ if $x = 0$, $g(x, y, z) = y$ if $x = 1$, and $g(x, y, z) = y + z$ if $x = 2$. Then g has no nonzero linear structure and $\hat{g}(\alpha, \beta, \gamma) \in \{0, 9\epsilon_3, 9\epsilon_3, 9\epsilon_3^2\}$.*

Let $f : \mathbb{F}_p^n \to \mathbb{F}_p$ be a non-weakly regular s-plateaued function such that its dual f^* is bent relative to $\mathrm{Supp}(\hat{f})$. By Theorem 2.3.1 we have $\hat{f}(\alpha) = \xi_\alpha p^{\frac{n+s}{2}} \epsilon_p^{f^*(\alpha)}$ for

all $\alpha \in \mathrm{Supp}(\hat{f})$ where $\xi_\alpha \in \{\pm 1, \pm i\}$. Let $B_+(f)$ and $B_-(f)$ be the partitions of $\mathrm{Supp}(\hat{f})$ given by

$$B_+(f) := \{w : w \in \mathrm{Supp}(\hat{f}) \mid \hat{f}(w) = \xi p^{\frac{n+s}{2}} \epsilon_p^{f^*(w)}\},$$

$$B_-(f) := \{w : w \in \mathrm{Supp}(\hat{f}) \mid \hat{f}(w) = -\xi p^{\frac{n+s}{2}} \epsilon_p^{f^*(w)}\},$$

where $\xi \in \{1, i\}$.

For an arbitrary non-weakly regular plateaued function $g : \mathbb{F}_p^n \to \mathbb{F}_p$ whose dual is bent relative to $\mathrm{Supp}(\hat{g})$, we define the type of g^* as follows

$$g^*(x) \text{ is of type } (+) \text{ if } \hat{g^*}(0) = \xi p^{\frac{n-s}{2}} \epsilon_p^{g^{**}(0)},$$

$$g^*(x) \text{ is of type } (+) \text{ if } \hat{g^*}(0) = -\xi p^{\frac{n-s}{2}} \epsilon_p^{g^{**}(0)}.$$

For any $y \in \mathbb{F}_p^n$ and $u \in \mathbb{F}_p$, the definitions of the sums $S_0(f, y),\ S_1(f, y)$ of complex numbers and integers $c_f(y, u),\ d_f(y, u)$ and $e_f(y, u)$ are exactly same as in Section 4.2. For an arbitrary s-plateaued function $g : \mathbb{F}_p^n \to \mathbb{F}_p$ we define the type of g as

- $g(x)$ is of type (0) if $\hat{g}(0) = 0$ (i.e. g is balanced).
- $g(x)$ is of type $(+)$ if $\hat{g}(0) = \xi p^{\frac{n+s}{2}} \epsilon_p^{g^*(0)}$.
- $g(x)$ is of type $(-)$ if $\hat{g}(0) = -\xi p^{\frac{n+s}{2}} \epsilon_p^{g^*(0)}$.

Next we generalize [36, Theorems 3.2 and 3.4] to plateaued functions. In rest of the section we skip the proofs if they are very similar to the ones in Section 4.2.

Proposition 2.3.2 *Let $g : \mathbb{F}_p^n \to \mathbb{F}_p$ be an unbalanced s-plateaued function. For $g^*(0) = i_0$ we have*

- $N_{i_0}(g) = p^{n-1},\ \ N_{i_0+j}(g) = p^{n-1} \pm \left(\frac{j}{p}\right) p^{\frac{n+s-1}{2}},$ *for* $1 \le j \le p-1,$ *for* $n+s$ *odd.*
- $N_{i_0}(g) = p^{n-1} \pm p^{\frac{n+s}{2}} \mp p^{\frac{n+s}{2}-1}$ *and* $N_i(g) = p^{n-1} \mp p^{\frac{n+s}{2}-1},$ *for* $i \neq i_0 \in F_p,$ *for* $n+s$ *even.*

Here the sign is $+$ (respectively $-$) if and only if the type of g is $(+)$ (respectively $(-)$).

The next corollary follows from Proposition 2.3.2. It generalizes [36, Theorems 3.3 and 3.5] to plateaued functions.

Corollary 2.3.1 *Let p be a prime. Then the Hamming distance of an s-plateaued function $g : \mathbb{F}_p^n \to \mathbb{F}_p$ to a nearest affine function is*

- $(p-1)p^{n-1} - p^{\frac{n+s-1}{2}}$, *for $n+s$ odd.*
- $(p-1)(p^{n-1} - p^{\frac{n+s}{2}-1})$, *for $n+s$ even and g is of type$(+)$.*
- $(p-1)p^{n-1} - p^{\frac{n+s}{2}-1}$, *for $n+s$ even and g is of type$(-)$.*

Proof. Let $h : \mathbb{F}_p^n \to \mathbb{F}_p$ be an affine function. Then the Hamming distance of g to h is $d(g,h) = \sum_{i \in \mathbb{F}_p \setminus \{0\}} N_i(g-h)$. It is minimized if we choose $N_0(g-h)$ maximal possible. Therefore by Proposition 2.3.2 we have

$$d(g,h) = \begin{cases} (p-1)p^{n-1} - p^{\frac{n+s-1}{2}} & \text{if } n+s \text{ odd}, \\ (p-1)(p^{n-1} - p^{\frac{n+s}{2}-1}) & \text{if } n+s \text{ even and } g \text{ is of type } +, \\ (p-1)p^{n-1} - p^{\frac{n+s}{2}-1} & \text{if } n+s \text{ even and } g \text{ is of type } -. \end{cases}$$

□

Recall that $f : \mathbb{F}_p^n \to \mathbb{F}_p$ is a non-weakly regular s-plateaued function and $e_f(y,u)$ is an integer for $y \in \mathbb{F}_p^n$ and $u \in \mathbb{F}_p$ defined above. For $y \in \mathbb{F}_p^n$ let $g_y : \mathbb{F}_p^n \to \mathbb{F}_p$ be the function

$$g_y(x) := f^*(x) + x.y,$$

which is a plateaued function affine equivalent to f^*.

We generalize Lemmas 2.2.2, 2.2.3, 2.2.4, 2.2.5, and Theorem 2.2.1, Corollary 2.2.1 in the following theorem.

Theorem 2.3.2 *Let $f : \mathbb{F}_p^n \to \mathbb{F}_p$ be a non-weakly regular s-plateaued function. Under notation and assumptions as above we have,*

- *Let $n+s$ be odd, there exists an integer k such that for every $y \in \mathbb{F}_p^n$ we have*

- *If* $p \equiv 1 (mod\ 4)$ *then,* $e_f(y, u_0) = k$ *and* $e_f(y, u_0 + i) = k + \left(\frac{i}{p}\right) p^{\frac{n-s-1}{2}}$ *for* $1 \leq i \leq p-1$;
- *If* $p \equiv 3 (mod\ 4)$ *then,* $e_f(y, u_0) = k$ *and* $e_f(y, u_0 + i) = k - \left(\frac{i}{p}\right) p^{\frac{n-s-1}{2}}$ *for* $1 \leq i \leq p-1$;

where $u_0 = f(y)$.

- *Let* $n + s$ *be even. There exists an integer* k *such that for every* $y \in \mathbb{F}_p^n$ *we have*

$$e_f(y, u) = \begin{cases} k + p^{\frac{n-s}{2}} & \text{if } f(y) = u, \\ k & \text{otherwise}. \end{cases}$$

If f^* *is bent relative to* $\mathrm{Supp}(\hat{f})$ *then we have*

- $$S_0(f, y) + S_1(f, y) = \begin{cases} \xi p^{\frac{n-s}{2}} \epsilon_p^{f(y)} & \text{if } g_y \text{ is of type } (+), \\ -\xi p^{\frac{n-s}{2}} \epsilon_p^{f(y)} & \text{if } g_y \text{ is of type } (-), \end{cases}$$

  where

$$\xi = \begin{cases} 1 & \text{if } n \text{ even or } n \text{ odd and } p \equiv 1 \ mod\ 4, \\ i & \text{if } n \text{ odd and } p \equiv 3 \ mod\ 4. \end{cases}$$

- f^* *is non-weakly regular bent relative to* $\mathrm{Supp}(\hat{f})$.
- *Let* $f^{**} : \mathbb{F}_p^n \to \mathbb{F}_p$ *be the dual function of* f^*. *For* $y \in \mathbb{F}_p^n$ *we have* $f^{**}(y) = f(-y)$.

CHAPTER 3

STRONGLY REGULAR GRAPHS ARISING FROM NON-WEAKLY REGULAR BENT FUNCTIONS

In this chapter, we prove that if the two special subsets associated with the non-weakly regular even bent functions in the *GMMF* class are partial difference sets then they are trivial. We prove that the corresponding subsets of the two sporadic examples of ternary non-weakly regular bent functions are non-trivial PDSs. We also show that special subsets associated with the two sporadic examples of ternary non-weakly regular bent functions are union of certain cyclotomic cosets. Our further construction giving non-trivial PDSs from certain p-ary functions which are not bent functions is also given.

3.1 Preliminaries

Let $f : \mathbb{F}_p^n \to \mathbb{F}_p$ be a function. For $v \in \mathbb{F}_p^n$ let $D_v f$ be the derivative function $D_v f(x) : \mathbb{F}_{p^n} \to \mathbb{F}_p$ given by $D_v f(x) = f(x+v) - f(x)$. A function $f : \mathbb{F}_p^n \to \mathbb{F}_p$ is called partially bent if the following property holds: For $v \in \mathbb{F}_{p^n}$, if the derivative function $D_v f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is not balanced then $D_v f$ is a constant function. Note that *partially bent* functions are special subclass of *plateaued* functions, and most of the known *plateaued* functions are *partially bent*. In the literature, only a few construction methods for *plateaued* but not *partially bent* functions are known, for example, see [45].

Definition 3.1.1 (Partial Difference Sets) *Let G be a group of order v and D be a subset of G with k elements. Then D is called a (v, k, λ, μ)- PDS in G if the expressions $g - h$, for g and h in D with $g \neq h$, represent each non-identity element*

in D exactly λ times and represent each non-identity element not in D exactly μ times.

Definition 3.1.2 (*Cayley Graph*) *Let G be a finite abelian group and D be a subset of G such that $0 \notin D$ and $D = -D$. Let E be the set defined as $\{(x, y)|x, y \in G,\ x - y \in D\}$. Then, (G, E) is called a Cayley graph, and denoted by $Cay(G, D)$.*

Here, D is called the connection set of (G, E). A PDS is called *regular* if $e \notin D$ and $D^{-1} = D$. A subset D of G is called *trivial* if either $D \cup \{e\}$ or $G/D \cup \{e\}$ is a subgroup of G. It is equivalent to saying that the Cayley graph generated by $D \setminus \{e\}$ is a union of complete graphs or its complement. Otherwise, D is called *non-trivial.*

Proposition 3.1.1 *([31, Propostion 1.5]) Let D be a regular $(v, k, \lambda, \mu)-$ PDS with $D \neq G \setminus \{e\}$. Then D is nontrivial if and only if $1 \leq \mu \leq k - 1$.*

Remark 3.1.1 *$\mu = 0$ implies that that $D \cup \{e\}$ is a subgroup of G. The other case $\mu = k$ implies that D is equal G/H for some subgroup H of G.*

Definition 3.1.3 (Strongly Regular Graphs) *A graph Γ with v vertices is said to be a $(v, k, \lambda, \mu)-$ strongly regular graph if*

1. *it is regular of valency k, i.e., each vertex is joined to exactly k other vertices;*
2. *any two adjacent vertices are both joined to exactly λ other vertices and two non-adjacent vertices are both joined to exactly μ other vertices.*

Proposition 3.1.2 *([31, Propostion 1.5]) A Cayley graph Γ , generated by a subset D of the regular automorphism group G, is a strongly regular graph if and only if D is a regular PDS in G.*

Definition 3.1.4 (*Association scheme*) *Let V be a finite set of vertices, and let $\{R_0, R_1, \ldots, R_d\}$ be binary relations on V with $R_0 := \{(x, x) : x \in V\}$. The configuration $(V; R_0, R_1, \ldots, R_d)$ is called an association scheme of class d on V if the following holds:*

1. *$V \times V = R_0 \cup R_1 \cup \cdots \cup R_d$ and $R_i \cap R_j = \emptyset$ for $i \neq j$.*

2. *$R_i^t = R_{i'}$ for some $i' \in \{0, 1, \ldots, d\}$, where $R_i^t := \{(x, y) | (y, x) \in R_i\}$. If $i' = i$, we call R_i is symmetric.*

3. *For $i, j, k \in \{0, 1, \ldots, d\}$ and for any pair $(x, y) \in R_k$, the number $\#\{z \in V | (x, z) \in R_i,$ and $(z, y) \in Rj\}$ is a constant, which is denoted by p_{ij}^k.*

Definition 3.1.5 (*Translation Scheme*) *Let $\Gamma_i := (G, E_i),\ 1 \leq i \leq d$, be Cayley graphs on an abelian group G, and D_i be connection sets of (G, E_i) with $D_0 := \{0\}$. Then, $(G, \{D_i\}_{i=0}^d)$ is called a translation scheme if $(G, \{\Gamma_i\}_{i=0}^d)$ is an association scheme.*

Given a d-class translation scheme $(X, \{R_i\}_{i=0}^d)$, we can take unions of classes to form graphs with larger edge sets which is called a *fusion*.

Remark 3.1.2 (Fusion Scheme) *Note that if the fusion gives a translation scheme again, it is called fusion scheme. However, it is not the case every time. We refer to [28] for further reading about fusion schemes.*

Definition 3.1.6 (*Cyclotomic Scheme*) *Let $\mathbb{F}_q$ be the finite field of order q, $\mathbb{F}_q^\star$ be the multiplicative group of $\mathbb{F}_q$, and S be a subgroup of $\mathbb{F}_q^\star$ s.t. $S = -S$. The partition $\mathbb{F}_q$ by $\{0\}$ and the multipicative cosets of S gives a translation scheme on $(\mathbb{F}_q, +)$, called a cyclotomic scheme.*

Each coset (called a *cyclotomic coset*) of $\mathbb{F}_q^\star \setminus S$ is expressed as

$$C_i = w^i \langle w^N \rangle, \quad 0 \leq i \leq N - 1,$$

where $N | q - 1$ is a positive integer and w is a fixed primitive element of $\mathbb{F}_q^\star$.

3.2 Partial Difference Sets Associated with Non-Weakly Regular *GMMF* Bent Functions are Trivial

Let p be an odd prime and $F : \mathbb{F}_p^n \times \mathbb{F}_p^s \to \mathbb{F}_p$ be the map $(x, y) \to f_y(x)$, where $f_y : \mathbb{F}_p^n \to \mathbb{F}_p$ is an *s-plateaued* function for each $y \in \mathbb{F}_p^s$ such that $\mathrm{Supp}(\hat{f}_i) \cap$

$\mathrm{Supp}(\hat{f_j}) = \emptyset$ for $i \neq j$, $i, j \in \mathbb{F}_p^s$. In [13], the authors showed that F is a bent function. They use *partially bent* functions with disjoint supports to obtain *plateaued* functions.

Remark 3.2.1 *In fact, it is not easy to find s-plateaued but not partially bent functions with disjoint supports. The plateaued functions f_a used in [13] can be obtained easily by adding a linear term to a bent function f, i.e. $f_a : \mathbb{F}_p^{n-s} \times \mathbb{F}_p^s \to \mathbb{F}_p$ such that $f_a(x, y) = f(x) + a.y$, where $f : \mathbb{F}_p^{n-s} \to \mathbb{F}_p$, $a \in \mathbb{F}_p^s$. Then $supp(\hat{f_i}) \cap supp(\hat{f_j})$ becomes the empty set for all $i, j \in \mathbb{F}_p^s$.*

The *bent* functions of the form $F(x, y) = f_y(x)$ are called the *GMMF* (Generalized Maiorana-McFarland) bent. The Walsh transform of F at (α, β) is given by

$$\begin{aligned} \hat{F}(\alpha, \beta) &= \sum_{x \in \mathbb{F}_p^n} \sum_{y \in \mathbb{F}_p^s} \epsilon_p^{F(x,y) - \alpha.x - \beta.y} \\ &= \sum_{x \in \mathbb{F}_p^n} \epsilon_p^{f_y(x) - \alpha.x} \sum_{y \in \mathbb{F}_p^s} \epsilon_p^{-y.\beta} \\ &= \widehat{f_{y_0}(x)}(\alpha) \epsilon_p^{-y_0.\beta}. \end{aligned}$$

where y_0 is the unique element of $\mathbb{F}_p^s$ such that $\alpha \in supp(\widehat{f_{y_0}})$. Then we have,

$$\hat{F}(\alpha, \beta) = \xi_{\alpha,\beta} p^{\frac{n+s}{2}} \epsilon_p^{(f_{y_0})^*(\alpha) - y_0.\beta} \tag{31}$$

which follows from $\widehat{f_{y_0}}(\alpha) = \xi_{\alpha,\beta} p^{\frac{n+s}{2}} \epsilon_p^{(f_{y_0})^*(\alpha)}$, where $\xi_{\alpha,\beta} \in \{\pm 1, \pm i\}$.
Observation: F is weakly regular if f_y is weakly regular *s-plateaued* with the same sign for all $y \in \mathbb{F}_p^s$ in their non-zero Walsh coefficients. F is non-weakly regular bent if f_y is weakly regular *s-plateaued* for all $y \in \mathbb{F}_p^s$ and there are $y_1, y_2 \in \mathbb{F}_p^s$ such that $f^{(y_1)}$ and $f^{(y_2)}$ have opposite signs in their non-zero Walsh coefficients or there exists $y \in \mathbb{F}_p^s$ such that f_y is non-weakly regular *s-plateaued*.

Let us partition weakly regular *s-plateaued* functions into two subclasses as f_y is in subclass $(+)$ if its non-zero Walsh coefficients are positive, and in subclass $(-)$ if its non-zero Walsh coefficients are negative. Let $F \in$ *GMMF* be a non-weakly regular bent function with $F(x) = F(-x)$. Next, we determine the structure of the sets $B_+(F)$ and $B_-(F)$ in two different cases.

Case 1 *[* $\mathbf{f_y}$ ***is weakly regular s-plateaued for all*** $\mathbf{y \in \mathbb{F}_p^s}$*]*

By the observation above, one can partition $\mathbb{F}_p^s$ into two subsets as $W^+(F) := \{y : y \in \mathbb{F}_p^s | f_y$ is in subclass $(+)\}$ and $W^-(F) := \{y : y \in \mathbb{F}_p^s | f_y$ is in subclass $(-)\}$, where $F : \mathbb{F}_p^n \times \mathbb{F}_p^s \to \mathbb{F}_p$ is given by $F(x, y) = f_y(x)$. Then by the equation (31) we deduce that

$$B_+(F) = \Big(\bigcup_{y \in W^+(F)} supp(\hat{f}_y) \Big) \times \mathbb{F}_p^s \text{ and } B_-(F) = \Big(\bigcup_{y \in W^-(F)} supp(\hat{f}_y) \Big) \times \mathbb{F}_p^s. \quad (32)$$

Case 2 *[$\mathbf{f_y}$ is non-weakly regular s-plateaued for some $\mathbf{y} \in \mathbb{F}_\mathbf{p}^\mathbf{s}$]*

Let $W^+(F), W^-(F)$ be as in the Case 1, and $W_0 := \{y : y \in \mathbb{F}_p^s | f_y$ is non-weakly regular s-plateaued$\}$. Again by the equation (31) we have

$$B_+(F) = \bigcup_{y \in W_0} \big(B_+(f_y) \times \mathbb{F}_p^s\big) \cup \Big(\bigcup_{y \in W^+(F)} supp(\hat{f}_y) \Big) \times \mathbb{F}_p^s \Big),$$

$$B_-(F) = \bigcup_{y \in W_0} \big(B_-(f_y) \times \mathbb{F}_p^s\big) \cup \Big(\bigcup_{y \in W^-(F)} supp(\hat{f}_y) \Big) \times \mathbb{F}_p^s \Big).$$

Remark 3.2.2 *In Cases 1 and 2; the sets $B_+(F)$ and $B_-(F)$ can be viewed as a union of some cosets of the subgroup $\{0\} \times \mathbb{F}_p^s$ in $\mathbb{F}_p^n \times \mathbb{F}_p^s$.*

Proposition 3.2.1 *Let H be a subgroup of $\mathbb{F}_{p^n}$ and K be one of its complement in $\mathbb{F}_{p^n}$, i.e. $H \cap K = \{0\}$ and $H \oplus K = \mathbb{F}_{p^n}$. Let L be a proper subset of K such that $0 \notin L$ and for each $v \in L$, $-v$ is also in L. Let $D = \bigcup_{v \in L}(H + v)$. If D is a PDS in $\mathbb{F}_{p^n}$, then it is trivial.*

Proof. Since $0 \notin L$, we have $0 \notin D$, and $H \subset \mathbb{F}_p^n \setminus D$. Since for $v \in L$, $-v$ is also in L, we have $D = -D$. Assume that D is a (p^n, kr, λ, μ) PDS where $\#H = k$, $\#L = r$. Since $H \subset \mathbb{F}_{p^n} \setminus D$, every non-zero elements in H can be represented as $x - y$ exactly μ times, for $x \neq y \in D$. Let $x \neq y$, $x, y \in D$. Let $x = h_1 + v_1$, $y = h_2 + v_2$, for some $h_1, h_2 \in H$ and $v_1, v_2 \in L$, then we get $x - y = (h_1 - h_2) + (v_1 - v_2)$. Clearly, if $v_1 \neq v_2$ then $x - y \notin H$. Hence $x - y \in H$ if and only if $x, y \in H + v_j$ for some $v_j \in L$. Let $x = h_1 + v_j$, $y = h_2 + v_j$. Then $x - y = h_1 - h_2 \in H$. Since H is a group, each non-zero $h \in H$ can be expressed exactly k times by the differences $h_1 - h_2$ for $h_1, h_2, \in H$. If $h \in H$; then for each $v_j \in L$, h can be represented exactly k times as $(h_1 + v_j) - (h_2 + v_j)$ for $h_1 \neq h_2 \in H$. Hence h can be expressed exactly

$\#H\#L = k.r$ times as the difference $x - y$ for $x \neq y \in D$. Therefore, $\mu = k.r$, and by Proposition 3.1.1, we have D is a trivial PDS in $\mathbb{F}_{p^n}$. □

Corollary 3.2.1 *Let $F \in$ GMMF such that $F(x) = F(-x)$. If $B_+(F)$(or equivalently $B_-(F)$) is a PDS, then it is trivial.*

Proof. The proof follows from the Cases 3,4 and Proposition 3.2.1. □

In the following example, we use a non-weakly regular ternary bent function (see [42]). In [13], the authors showed that it belongs to the *GMMF* class. By using *Magma*, we observe that the set $B_+(f_1)$ is a subgroup of $\mathbb{F}_{3^3}$. Hence, it is a trivial *PDS* in $\mathbb{F}_{3^3}$. Moreover, in [14], the authors claim that f_1 is self-dual bent. However, by *Magma* computations, we observe that the dual function f_1^* of f_1 is indeed equal to $-f_1$, and it is not self-dual.

Example 5 *$f_1 : \mathbb{F}_{3^3} \to \mathbb{F}_3$, $f_1(x) = Tr_3(x^{22} + x^8)$ is non-weakly regular of Type (+).*

- *$B_+^\star(f_1)$ is a $(27, 8, 7, 0)$-PDS in $\mathbb{F}_{3^3}$.*
- *$B_-(f_1)$ is a $(27, 18, 9, 18)$-PDS in $\mathbb{F}_{3^3}$.*

Remark 3.2.3 *By the Corollary 3.2.1 it follows that if neither $\bigcup_{y \in W^+(F)} supp(\hat{f}_y)$ nor $\bigcup_{y \in W^-(F)} supp(\hat{f}_y)$ is a subgroup of $\mathbb{F}_{p^n}$, then neither $B^+(F)$ nor $B^-(F)$ is a PDS in $\mathbb{F}_p^n \times \mathbb{F}_p^s$. Hence, we conclude that not all non-weakly regular bent functions of the form $f(x) = f(-x)$ have the property that $B^+(f)$ or $B^-(f)$ is a partial difference set. It is interesting to determine certain conditions on those sets, so that they become non-trivial PDSs. To do this, in the following section we analyze the sets $B^+(f)$ and $B^-(f)$ associated with two of the known sporadic examples of ternary non-weakly regular bent functions.*

3.3 Non-Trivial PDSs From Ternary Non-Weakly Regular Bent Functions

It is known that one of the tools to construct partial difference sets are bent functions. In [41], the authors proved that pre-image sets of the ternary weakly regular even bent

functions are partial difference sets.

Let $f : \mathbb{F}_{p^m} \to \mathbb{F}_p$ be a p-ary function, and $D_i := \{x : x \in \mathbb{F}_{p^m} | f(x) = i\}$. The following is due to [41]

Theorem 3.3.1 *Let $f : \mathbb{F}_{3^{2m}} \to \mathbb{F}_3$ be ternary function satisfying $f(x) = f(-x)$, and $f(0) = 0$. Then f is weakly regular bent if and only if D_1 and D_2 are both*

$$(3^{2m}, 3^{2m-1} + \epsilon 3^{m-1}, 3^{2m-2}, 3^{2m-2} + \epsilon 3^{m-1}) - PDSs,$$

where $\epsilon = \pm 1$. Moreover, $D_0 \setminus \{0\}$ is a

$$(3^{2m}, 3^{2m-1} - 1 - 2\epsilon 3^{m-1}, 3^{2m-2} - 2 - 2\epsilon 3^{m-1}, 3^{2m-2} - \epsilon 3^{m-1}) - PDSs.$$

Later this result is generalized to arbitrary odd characteristic in [16] for the weakly regular bent functions from $\mathbb{F}_{p^{2m}}$ to $\mathbb{F}_p$ satisfying certain conditions. Namely, for a weakly regular bent function f the following subsets

$$\begin{aligned} D &:= \{x : x \in \mathbb{F}_{p^{2m}} \setminus \{0\} | f(x) = 0\}, \\ D_S &:= \{x : x \in \mathbb{F}_{p^{2m}} \setminus \{0\} | f(x) \text{ is square}\}, \\ D'_S &:= \{x : x \in \mathbb{F}_{p^{2m}} \setminus \{0\} | f(x) \text{ is non-zero square}\}, \\ D_N &:= \{x : x \in \mathbb{F}_{p^{2m}} \setminus \{0\} | f(x) \text{ is non-square}\} \end{aligned}$$

are regular partial difference sets.

As far as we know, no one introduced a relation between non-weakly regular bent functions and partial difference sets. In this section, we examine to a relation between the set $B_+(f)$ (or equivalently $B_-(f)$) and cyclotomic schemes by analyzing two known sporadic examples of non-weakly regular bent functions over $\mathbb{F}_{3^6}$ (see[24, 25]). We observe that the sets $B_+(f)$ (or equivalently $B_-(f)$) corresponding to these sporadic examples are non-trivial partial difference sets and they are fusion scheme of some cyclotomic schemes for certain parameters. Hence, this is a different relation from the previous ones in the sense of while the pre-image sets of some weakly regular bent functions give PDSs, the partition of $\mathbb{F}_{p^{2m}}$ with respect to the sign of the Walsh transformation of some non-weakly regular bent functions also gives PDSs. For the following examples we have $q = 729$, and $N = 13$. Let w be a fixed primitive element of $\mathbb{F}_{3^6}$. Let C_0 be the multiplicative subgroup of $\mathbb{F}_{3^6}$ generated

by w^{13}. For $1 \leq i \leq 12$, C_i denotes the i-th cyclotomic coset of C_0, and defined by $C_i = w^i C_0$.

Example 6 *$f_2 : \mathbb{F}_{3^6} \to \mathbb{F}_3$, $f_2(x) = Tr_6(w^7 x^{98})$ is non-weakly regular of Type $(-)$. The dual of f_2 is not bent and corresponding partial difference sets and strongly regular graphs are non-trivial.*

- *$B_+(f_2)$ is a $(729, 504, 351, 342)$-PDS in $\mathbb{F}_{3^6}$*
- *$B^\star_-(f_2)$ is a $(729, 224, 62, 71)$-PDS in $\mathbb{F}_{3^6}$*

By using Magma, we compute $B_+(f_2)$ and $B_-(f_2)$. We observe that $B_+(f_2) = \bigcup_{i\in\{0,3,5,6,7,8,9,11,12\}} C_i$ and $B_-(f_2) = \bigcup_{i\in\{1,2,4,10\}} C_i$. Hence $B_+(f_2)$ and $B^\star_-(f_2)$ are 2-class fusion schemes and correspond to non-trivial strongly regular graphs.

Example 7 *$f_3 : \mathbb{F}_{3^6} \to \mathbb{F}_3$, $f_3(x) = Tr_6(w^7 x^{14} + w^{35} x^{70})$ is non-weakly regular of Type $(-)$. The dual of f_3 is not bent. Corresponding partial difference sets are non-trivial.*

- *$B_+(f_3)$ is a $(729, 504, 351, 342)$- regular PDS in $\mathbb{F}_{3^6}$.*
- *$B^\star_-(f_3)$ is a $(729, 224, 62, 71)$- regular PDS in $\mathbb{F}_{3^6}$.*

Again by Magma computations we have, $B_+(f_3) = \bigcup_{i\in\{0,1,2,4,5,6,9,11,12\}} C_i$ and $B_-(f_3) = \bigcup_{i\in\{3,7,8,10\}} C_i$. Hence $B_+(f_3)$ and $B^\star_-(f_3)$ are 2-class fusion schemes and correspond to non-trivial strongly regular graphs.

Remark 3.3.1 *Non-trivial strongly regular graphs correspond to f_2 and f_3 are from a unital: projective $9-ary$ $[28, 3]$ code with weights $24, 27$; $VO^-(6, 3)$ affine polar graph (See, [9]).*

In fact, these are not the only examples giving non-trivial strongly regular graph. We easily obtain different non-trivial partial difference sets on $\mathbb{F}_{3^6}$ by preserving the images of the functions f_2 and f_3 on C_0. For example the functions; $h_1(x) =$

$Tr_6(w^{7k}x^{154})$ and $h_2(x) = Tr_6(w^{7k}x^{658})$ are non-weakly regular bent for any odd integer k. The corresponding subsets $B_-(h_1)\backslash\{0\}$ and $B_-(h_2)\backslash\{0\}$) are $(729, 224, 62, 71)$-PDSs in $\mathbb{F}_{3^6}$. On the other hand if we take k even the Walsh transform of the corresponding functions h_1 and h_2 have the form;

$$\widehat{h_i}(\alpha) = \begin{cases} 27\epsilon_3^{f^*(\alpha)}, \\ 0, \\ -54, \end{cases}$$

as α runs through $\mathbb{F}_{3^6}^\star$.

Let k be even, $D := \{\alpha : \alpha \in \mathbb{F}_{3^6} | \widehat{h_i}(\alpha) = 0\}$. We observe that D is a $(729, 252, 81, 90)$-PDS in $\mathbb{F}_{3^6}$. The parameters of D are different than the parameters of Examples 2 and 3. Moreover as k is even h_i is not a bent function. This gives a construction of non-trivial strongly regular graphs from certain p-ary functions which are not bent functions.

It is an interesting problem to determine fusion schemes of an N-class cyclotomic scheme on $\mathbb{F}_q$. There are a lot of research papers devoted to this problem, for example, see [4, 40, 28, 35]. Moreover, another interesting problem is to find an explicit relation between non-weakly regular bent functions and 2-class fusion schemes of cyclotomic schemes.

CHAPTER 4

ASSOCIATIONS SCHEMES OF CLASSES 5 AND 6 ARISING FROM TERNARY NON-WEAKLY REGULAR BENT FUNCTIONS

In this chapter we give a construction method of association schemes of class 5 and class 6 in odd and even dimensions respectively by using ternary non-weakly regular bent functions in *GMMF* class.

4.1 Preliminaries

Remember that any bent function $g : \mathbb{F}_p^n \to \mathbb{F}_p$ is of two types (see Chapter 2)).

$$\text{Type } (+) \text{ if } \hat{f}(0) = \epsilon p^{\frac{n}{2}} \epsilon_p^{f^*(0)},\ \epsilon \in \{1, i\}. \tag{41}$$

$$\text{Type } (-) \text{ if } \hat{f}(0) = \epsilon p^{\frac{n}{2}} \epsilon_p^{f^*(0)},\ \epsilon \in \{-1, -i\}. \tag{42}$$

Remark 4.1.1 *It is recognised that weakly regular bent functions show up in pairs and given a weakly regular bent function $f : \mathbb{F}_p^n \to \mathbb{F}_p$ we have (see [24])*

$$\widehat{f^*}(\alpha) = \xi^{-1} p^{\frac{n}{2}} \epsilon_p^{f(-\alpha)} \tag{43}$$

where $\widehat{f}(\alpha) = \xi p^{\frac{n}{2}} \epsilon_p^{f^*(\alpha)}$. It is easy to see that for $p^n \equiv 1$ (mod 4) the types of f and f^* are same, for $p^n \equiv 3$ (mod 4) they are of different types.

Let $f : \mathbb{F}_p^n \to \mathbb{F}_p$ be a non-weakly regular bent function. For any $y \in \mathbb{F}_p^n$ we have

$$\xi^{-1}p^{\frac{n}{2}}\epsilon_p^{f(y)} = S_0(f,y) - S_1(f,y). \tag{44}$$

By Equation 44 we have

$$S_0(f,y) - S_1(f,y) = \begin{cases} p^{\frac{n}{2}}\epsilon_p^{f(y)} & \text{if } n \text{ even or } n \text{ odd and } p \equiv 1 \bmod 4; \\ -ip^{\frac{n}{2}}\epsilon_p^{f(y)} & \text{if } n \text{ odd and } p \equiv 3 \bmod 4. \end{cases}$$

In Chapter 2, we prove that if f^* is bent then it is non-weakly regular. So, if f^* is bent then the subsets $B_+(f^*)$ and $B_-(f^*)$ are well defined. Let $H_i(f) := \{x : x \in \mathbb{F}_p^n | f(x) = i\}$, $C_i(f) := \{x : x \in B_+(f) | f^*(x) = i\}$ and $D_i(f) := \{x : x \in B_-(f) | f^*(x) = i\}$ for $0 \leq \forall i \leq p-1$. We further define the subsets $H_i^+(f) := B_+(f^*) \cap H_i(f)$ and $H_i^-(f) := B_-(f^*) \cap H_i(f)$, for $0 \leq \forall i \leq p-1$.

From now on, all the plateaued functions we consider are partially bent. It is known that all partially bent functions can be written as sum of a bent function and an affine function. Let $f^{(a)} : \mathbb{F}_p^n \to \mathbb{F}_p$ be bent for all $a \in \mathbb{F}_{p^s}$ and $f_a : \mathbb{F}_p^n \times \mathbb{F}_p^s \to \mathbb{F}_p$ be the map $(x,y) \to f^{(a)}(x) + a.y$. Then the function $F : \mathbb{F}_p^n \times \mathbb{F}_p^s \times \mathbb{F}_p^s \to \mathbb{F}_p$ defined by

$$F(x,y,z) = f_z(x,y) = f^z(x) + z.y \tag{45}$$

belongs to GMMF class. The Walsh transform of F at (α,β,γ) is given by

$$\begin{aligned} \widehat{F}(\alpha,\beta,\gamma) &= \textstyle\sum_{x\in\mathbb{F}_p^m}\sum_{y\in\mathbb{F}_p^s}\sum_{z\in\mathbb{F}_p^s}\epsilon_p^{F(x,y,z)-\alpha.x-\beta.y-\gamma.z} \\ &= \textstyle\sum_{x\in\mathbb{F}_p^m}\epsilon_p^{f^{(z)}(x)-\alpha.x}\sum_{y\in\mathbb{F}_p^s}\epsilon_p^{y.(z-\beta)}\sum_{z\in\mathbb{F}_p^s}\epsilon_p^{-\gamma.z} \\ &= p^s\epsilon_p^{-\gamma.\beta}\widehat{f^{(\beta)}}(\alpha). \end{aligned} \tag{46}$$

Then we have,

$$\widehat{F}(\alpha,\beta,\gamma) = \xi_{\alpha,\beta}p^{\frac{n+s}{2}}\epsilon_p^{f^{(\beta)^*}(\alpha)-\gamma.\beta} \tag{47}$$

which follows from $\widehat{f^{(\beta)}}(\alpha) = \xi_{\alpha,\beta}p^{\frac{n}{2}}\epsilon_p^{f^{(\beta)^*}(\alpha)}$, where $\xi_{\alpha,\beta} \in \{\pm 1, \pm i\}$. Hence we have

$$F^*(x,y,z) = f^{(y)^*}(x) - y.z. \tag{48}$$

Observe that F is weakly regular if $f^{(z)}$ is weakly regular bent of the same type for

all $z \in \mathbb{F}_p^s$. F is non-weakly regular bent if $f^{(z)}$ is weakly regular bent for all $z \in \mathbb{F}_p^s$ and there are $z_1, z_2 \in \mathbb{F}_p^s$ such that $f^{(z_1)}$ and $f^{(z_2)}$ are of different types or there exists $z \in \mathbb{F}_p^s$ such that $f^{(z)}$ is non-weakly regular bent.

Let $F \in$ *GMMF* be a non-weakly regular bent function. Next, we determine the structure of the sets $B_+(F)$ and $B_-(F)$ in the case of $f^{(z)}$ is weakly regular bent for all $z \in \mathbb{F}_p^s$. Note that this is a specific case of the general version for which we determine the structure of the sets $B_+(F)$ and $B_-(F)$ in Chapter 3. By the observation above, one can partition $\mathbb{F}_p^s$ into two subsets as $W^+(F) := \{z : z \in \mathbb{F}_p^s | f^{(z)} \text{ is of type } (+)\}$ and $W^-(F) := \{z : z \in \mathbb{F}_p^s | f^{(z)} \text{ is of type } (-)\}$, where $F : \mathbb{F}_p^n \times \mathbb{F}_p^s \times \mathbb{F}_p^s \to \mathbb{F}_p$ is given by $F(x, y, z) = f_z(x, y)$. Then by the equation (47) we deduce that

$$B_+(F) = \mathbb{F}_p^n \times W^+(F) \times \mathbb{F}_p^s \text{ and } B_-(F) = \mathbb{F}_p^n \times W^-(F) \times \mathbb{F}_p^s. \tag{49}$$

Remark 4.1.2 *Note that Equation (48) implies F^* is also bent and belongs to the GMMF class.*

The Walsh transform of F^* at (α, β, γ) is given by

$$\begin{aligned} \widehat{F^*}(\alpha, \beta, \gamma) &= \sum_{x \in \mathbb{F}_p^m} \sum_{y \in \mathbb{F}_p^s} \sum_{z \in \mathbb{F}_p^s} \epsilon_p^{F^*(x,y,z) - \alpha.x - \beta.y - \gamma.z} \\ &= \sum_{x \in \mathbb{F}_p^m} \epsilon_p^{f^{(y)^*}(x) - \alpha.x} \sum_{y \in \mathbb{F}_p^s} \epsilon_p^{-y.\beta} \sum_{z \in \mathbb{F}_p^s} \epsilon_p^{-z.(\gamma+y)} \\ &= p^s \epsilon_p^{\gamma.\beta} \widehat{f^{(-\gamma)^*}}(\alpha). \end{aligned} \tag{410}$$

Hence, we have

$$\begin{aligned} F^{**}(x, y, z) &= f^{(-z)^{**}}(x) + y.z \\ &= f^{(-z)}(-x) + y.z, \end{aligned} \tag{411}$$

where the second equality follows from Equation (43).

Definition 4.1.1 *A character of a group G is a homomorphism from G to $\mathbb{C}^\star$, where $\mathbb{C}^\star$ denotes the multiplicative group of the field of complex numbers. Moreover, a character is called trivial if it maps the all group elements to* 1.

Remark 4.1.3 *Note that fields have two kinds of characters as they have two different group structures, namely, additive and multiplicative.*

4.2 Associations Schemes Related with Ternary Non-Weakly Regular Bent Functions in GMMF Class

In this section we give a construction method of association schemes of class 5 and class 6 in odd and even dimensions respectively by using ternary non-weakly regular bent functions in *GMMF* class.

The functions $\chi_j : \mathbb{F}_p^n \to \mathbb{C}^\star, \;\; j \in \mathbb{F}_p^n$, defined by

$$\chi_j(x) = \epsilon_p^{j.x}$$

are all additive characters of $\mathbb{F}_p^n$. Let $\widehat{G}$ denotes the character group of an finite abelian group G and χ_0 be the trivial character. We assign a subset A of G with the group ring element $\sum_{x\in A} x$, which will also be denoted by means of A. By linearity, we extend each character $\chi \in G$ to a homomorphism from $\mathbb{C}[G]$ to $\mathbb{C}$, and we nevertheless denote this homomorphism by χ. Let $A_0 = \{0\}, A_1, \ldots, A_d$ be an inversed-closed partition of G. This partition induces a partition $S_0 = \{\chi_0\}, S_1, S_2, \ldots, S_e$, of $\widehat{G}$: $\Psi, \Phi \in \widehat{G} \setminus \{\chi_0\}$ are in the same S_j iff $\Psi(A_i) = \Phi(A_i) \;\; for\; 1 \leq \forall i \leq d$.

The following theorem is given in [8].

Theorem 4.2.1 (Bridges-Mena, 1982) *It holds that $d \leq e$. In particular $(G, \{A_i\}_{i=0}^d)$ forms a translation scheme iff $d = e$.*

	A_0	A_1	A_2	A_3	$\ldots$	A_d
$\Psi_0 \in S_0$	1	$\#A_1$	$\#A_2$	$\#A_3$	$\ldots$	$\#A_d$
$\Psi \in S_1$	1	a_{11}	a_{12}	a_{13}	$\ldots$	a_{1d}
$\Psi^{'} \in S_2$	1	a_{21}	a_{22}	a_{23}	$\ldots$	a_{2d}
$\Psi^{''} \in S_3$	1	a_{31}	a_{32}	a_{33}	$\ldots$	a_{3d}
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\Psi^{(e)} \in S_e$	1	a_{e1}	a_{e2}	a_{e3}	$\ldots$	a_{ed}

If $d = e$ then the d by d matrix $P = [a_{ij}]$ is called the principal part of the first eigenmatrix of the translation scheme $(G, \{A_i\}_{i=0}^d)$.

4.2.1 Construction in Even Dimension

From now on we further assume that $s \in \mathbb{Z}^+$ and $F : \mathbb{F}_3^2 \times \mathbb{F}_3^s \times \mathbb{F}_3^s \to \mathbb{F}_3$ be a non-weakly regular bent function defined by the Equation (45) such that $f^{(z)}$ is weakly regular bent for all $z \in \mathbb{F}_3^s$.

Condition 1 *$f^{(0)}$ is of type $(-)$ and $f^{(z)}$ is of type $(+)$ for all nonzero $z \in \mathbb{F}_3^s$; $f^{(0)}(0) = 0$ and $f^{(z)} = f^{(-z)}$ for all $z \in \mathbb{F}_3^s$; $f^{(z)}(x) = f^{(z)}(-x)$ for all $x \in \mathbb{F}_{3^2}$.*

It is easy to see that if F satisfies the Condition 1 then $F(x, y, z) = F(-x, -y, -z)$ and $\widehat{F}(\alpha, \beta, \gamma) = \widehat{F}(-\alpha, -\beta, -\gamma)$ so that $F^*(x, y, z) = F^*(-x, -y, -z)$. Denote $G_1 = \mathbb{F}_3^2 \times \mathbb{F}_3^s \times \mathbb{F}_3^s$.

Theorem 4.2.2 *Let F satisfies the Condition 1. Let $A_0 = \{\mathbf{0}\}$, $A_i = C_i(F)$ for $1 \leq \forall i \leq 3$, $A_4 = D_0^\star(F)$, $A_j = D_{j-4}(F)$ for $5 \leq \forall j \leq 6$. Let $\Gamma_i := (G_1, E_i)$, $0 \leq i \leq 6$ be Cayley graphs on G_1 with connection sets $\{A_i\}_{i=0}^6$, then $(G_1, \{\Gamma_i\}_{i=0}^6)$ is an association scheme of class 6.*

Proof. By Equation (44) we have

$$3^{s+1}\epsilon_3^{F(\theta)} = \sum_{i=0}^{2} \chi_\theta(C_i(F))\epsilon_3^i - \sum_{i=0}^{2} \chi_\theta(D_i(F))\epsilon_3^i. \tag{412}$$

Since $F^*(x, y, z) = F^*(-x, -y, -z)$ then $C_i(F) = -C_i(F)$ and $D_i(F) = -D_i(F)$ for all $i \in \mathbb{F}_3$. Since $\epsilon_3 + \bar{\epsilon_3} = -1$, $\chi_\theta(C_i(F))$ and $\chi_\theta(D_i(F))$ are integers for all $i \in \mathbb{F}_3$ and $\theta \in \mathbb{F}_3^2 \times \mathbb{F}_3^s \times \mathbb{F}_3^s$. The assumptions $f^{(0)}$ is of type $(-)$, $f^{(z)}$ is of type $(+)$ for all nonzero $z \in \mathbb{F}_{3^s}$ and Equation (49) imply that $B^-(F) = \mathbb{F}_3^2 \times \{\mathbf{0}\} \times \mathbb{F}_3^s$. Since $B^-(F)$ is a subgroup of G_1 every character of $B^-(F)$ can be represented by the restriction of a character of G_1 into $B^-(F)$. Then by character theory of finite abelian groups we have

$$\chi_\theta(B_-(F)) = \begin{cases} 3^{s+2} & \text{if } \theta \in B_-(F)^\perp, \\ 0 & \text{otherwise.} \end{cases} \tag{413}$$

Since F^* is bent (see Remark 4.1.2)by Remarks 4.1.1, 4.1.2 and Equation (411) we have $B_+(F^*) = \mathbb{F}_3^2 \times \mathbb{F}_3^s \times \mathbb{F}_3^{s\star}$ and $B_-(F^*) = \mathbb{F}_3^2 \times \mathbb{F}_3^s \times \{\mathbf{0}\}$. It is clear that $B_-(F)^\perp =$

$\{\mathbf{0}\} \times \mathbb{F}_3^s \times \{\mathbf{0}\}$ and for any element $(\mathbf{0}, y, \mathbf{0}) \in B_-(F)^\perp$ we have $F(\mathbf{0}, y, \mathbf{0}) = f^{(\mathbf{0})}(\mathbf{0}) = 0$ implying $B_-(F)^\perp \subset H_0(F)$. Moreover, since $B_-(F)^\perp \subset B_-(F^*)$ we have $B_-(F)^\perp \subset H_0^-(F)$. Now we will prove that $B_-(F)^\perp = H_0^-(F)$. Since F^* is bent we have $F^{**}(x) = F(x)$ by Theorem 2.2.1. By definition we have $C_i(F^*) = \{x \in B_+(F^*) : F(x) = i\}$ and $D_i(F^*) = \{x \in B_-(F^*) : F(x) = i\}$ for $i \in \mathbb{F}_3$. Let us denote $\theta = (\alpha, \beta, \gamma) \in G_1$ and $v = (x, y, z) \in G_1$. By inverse Walsh transform we have

$$\begin{aligned} 3^{s+1}\epsilon_3^{F^*(\theta)} &= \textstyle\sum_{v \in B_+(F^*)} \epsilon_3^{F(v)+v.\theta} - \sum_{v \in B_-(F^*)} \epsilon_3^{F(v)+v.\theta} \\ &= \textstyle\sum_{i=0}^{2} \chi_\theta(C_i(F^*))\epsilon_3^i - \sum_{i=0}^{2} \chi_\theta(D_i(F^*))\epsilon_3^i. \end{aligned}$$

Observe that $H_i^+(F) = C_i(F^*)$ and $H_i^-(F) = D_i(F^*)$ for all $i \in \mathbb{F}_3$. Put $\theta = \mathbf{0}$. Since F is of type $(-)$ by Lemma 2.2.5 we have

$$-3^{s+1}\epsilon_3^{F^*(\mathbf{0})} = -3^{s+1} = \#D_0(F^*) + \#D_1(F^*)\epsilon_3 + \#D_2(F^*)\epsilon_3^2. \tag{414}$$

Since $\{\epsilon_3, \epsilon_3^2\}$ is a basis for $\mathbb{Q}(\epsilon_3)$ over $\mathbb{Q}$ [30, Theorem 2.47 (i)], there exist uniquely determined coefficients in $\mathbb{Q}$ satisfying the equation

$$-(3^{s+1} + \#D_0(F^*)) = \#D_1(F^*)\epsilon_3 + \#D_2(F^*)\epsilon_3^2. \tag{415}$$

Then $\epsilon_3 + \bar{\epsilon_3} = -1$ implies $\#D_1(F^*) = \#D_2(F^*) = \#D_0(F^*) + 3^{s+1}$. Since $\#D_0(F^*) + \#D_1(F^*) + \#D_2(F^*) = \#B_-(F^*)$ and $B_-(F^*) = \mathbb{F}_3^2 \times \mathbb{F}_3^s \times \{0\}$, we have $\#D_0(F^*) = 3^s$. On the other hand we have $\#B_-(F)^\perp = 3^s$. Combining $B_-(F)^\perp \subset H_0^-(F)$ and $H_0^-(F) = D_0(F^*)$ we deduce that $B_-(F)^\perp = H_0^-(F)$.

Case 3 ($\theta \in H_i^+(F)$) *By Lemma 2.2.5 we have $S_1(F, \theta) = 0$ and $3^{s+1}\epsilon_3^{F(\theta)} = \sum_{i=0}^{2} \chi_\theta(C_i(F))\epsilon_3^i$. Then we have*

$$0 = (\chi_\theta(C_i(F)) - 3^{s+1})\epsilon_3^i + \sum_{j \neq i \in F_3} \chi_\theta(C_j(F))\epsilon_3^j. \tag{416}$$

$$0 = \sum_{j \in \mathbb{F}_3} \chi_\theta(D_j(F))\epsilon_3^j. \tag{417}$$

By similar arguments above, there exist uniquely determined coefficients in $\mathbb{Q}$ satisfying Equations (416 and 417). It is clear that for all $i \in \mathbb{F}_3$ we have $\chi_\theta(D_0(F)) = \chi_\theta(D_1(F)) = \chi_\theta(D_2(F))$. Since $\theta \notin H_0^-(F) = B_-(F)^\perp$, by Equation (413) we have

$\chi_\theta(D_0(F)) = \chi_\theta(D_1(F)) = \chi_\theta(D_2(F)) = 0$ *for all* $i \in \mathbb{F}_3$. *By character theory of finite abelian groups we have*

$$\sum_{i\in\mathbb{F}_3} \chi_\theta(C_i(F) + D_i(F)) = 0 \tag{418}$$

for $\theta \neq \mathbf{0}$. *Hence we have*

$$\chi_\theta(C_0(F)) + \chi_\theta(C_1(F)) + \chi_\theta(C_2(F)) = 0. \tag{419}$$

On the other hand, Equation (416) implies

$$(\chi_\theta(C_i(F)) - 3^{s+1}) = \chi_\theta(C_{i+1}(F)) = \chi_\theta(C_{i+2}(F)) \tag{420}$$

for $i \in \mathbb{F}_3$. *Combining Equations (419) and (420) we have* $\chi_\theta(C_i(F)) = 3^{s+1} - 3^s$ *and* $\chi_\theta(C_{i+1}(F)) = \chi_\theta(C_{i+2}(F)) = -3^s$, *for* $i \in \mathbb{F}_3$.

Case 4 ($\theta \in H_i^-(F)$**)** *By Lemma 2.2.5 we have* $S_0(F,\theta) = 0$ *and* $-3^{s+1}\epsilon_3^{F(\theta)} = \sum_{i=0}^{2} \chi_\theta(D_i(F))\epsilon_3^i$. *Then we have*

$$0 = (\chi_\theta(D_i(F)) + 3^{s+1})\epsilon_3^i + \sum_{j\neq i\in F_3} \chi_\theta(D_j(F))\epsilon_3^j. \tag{421}$$

$$0 = \sum_{j\in\mathbb{F}_3} \chi_\theta(C_j(F))\epsilon_3^j. \tag{422}$$

By similar arguments above we have

$$\chi_\theta(D_i(F)) + 3^{s+1} = \chi_\theta(D_{i+1}(F)) = \chi_\theta(D_{i+2}(F)) \tag{423}$$

for $i \in \mathbb{F}_3$. *Let* $\theta \in H_0^-(F) = B_-(F)^\perp$. *Then by Equation (413) we have*

$$\chi_\theta(D_0(F)) + \chi_\theta(D_1(F)) + \chi_\theta(D_2(F)) = 3^{s+2}. \tag{424}$$

Combining Equations (424) and (423) we get $\chi_\theta(D_0(F)) = 3^s$ *and* $\chi_\theta(D_1(F)) = \chi_\theta(D_2(F)) = 3^{s+1} + 3^s$. *Since* $\mathbf{0} \in H_0^-(F)$ *and* $\chi_{\mathbf{0}}(D_i(F)) = \#D_i(F)$ *for* $i \in \mathbb{F}_3$, *we have* $\#D_0(F) = 3^s$ *and* $\#D_1(F) = \#D_2(F) = 3^{s+1} + 3^s$. *It is clear that Equation (422) implies*

$$\chi_\theta(C_0(F)) = \chi_\theta(C_1(F)) = \chi_\theta(C_2(F)). \tag{425}$$

Hence we have $\chi_{\mathbf{0}}(C_i(F)) = \#C_i(F) = 3^{2s+1} - 3^{s+1}$ *for* $i \in \mathbb{F}_3$. *If* $\theta \neq \mathbf{0}$ *then by Equation (418) we have* $\chi_\theta(C_0(F)) = \chi_\theta(C_1(F)) = \chi_\theta(C_2(F)) = -3^{s+1}$. *Let* $\theta \in H_i^-(F)$ *for* $i \in \{1,2\}$. *Since* $\theta \notin B_-(F)^\perp$ *by Equation (413) we have*

$$\chi_\theta(D_0(F)) + \chi_\theta(D_1(F)) + \chi_\theta(D_2(F)) = 0 \tag{426}$$

Then by Equations (418), (426) and (425) we have $\chi_\theta(C_0(F)) = \chi_\theta(C_1(F)) = \chi_\theta(C_2(F)) = 0$. *Combining Equations (423) and (426) we get* $\chi_\theta(D_i(F)) = 3^s - 3^{s+1}$ *and* $\chi_\theta(D_{i+1}(F)) = \chi_\theta(D_{i+2}(F)) = 3^s$ *for* $i \in \{1,2\}$.

Let $S_0 := \{\chi_0\}$, $S_i := \{\chi_y : y \in H_{i-1}^+(F)\}$ for $1 \leq \forall i \leq 3$ and $S_4 := \{\chi_y : 0 \neq y \in H_0^-(F)\}$, $S_j := \{\chi_y : y \in H_{j-4}^-(F)\}$ for $5 \leq \forall j \leq 6$. Then by Theorem 4.2.1 $(G, \{A_i\}_{i=0}^6)$ forms a translation scheme. □

Hence for any positive integer s we have translation scheme of class 6 with following first eigenmatrix;

$$\begin{bmatrix}
1 & 3^{2s+1}-3^{s+1} & 3^{2s+1}-3^{s+1} & 3^{2s+1}-3^{s+1} & 3^s-1 & 3^{s+1}+3^s & 3^{s+1}+3^s \\
1 & 3^{s+1}-3^s & -3^s & -3^s & -1 & 0 & 0 \\
1 & -3^s & 3^{s+1}-3^s & -3^s & -1 & 0 & 0 \\
1 & -3^s & -3^s & 3^{s+1}-3^s & -1 & 0 & 0 \\
1 & -3^{s+1} & -3^{s+1} & -3^{s+1} & 3^s-1 & 3^{s+1}+3^s & 3^{s+1}+3^s \\
1 & 0 & 0 & 0 & 3^s-1 & 3^s-3^{s+1} & 3^s \\
1 & 0 & 0 & 0 & 3^s-1 & 3^s & 3^s-3^{s+1}
\end{bmatrix}$$

Moreover fusing the first three non-trivial classes of the those translation schemes we obtain fusion schemes of class 4.

$$\begin{bmatrix}
1 & 3^{2s+2}-3^{s+2} & 3^s-1 & 3^{s+1}+3^s & 3^{s+1}+3^s \\
1 & 0 & -1 & 0 & 0 \\
1 & -3^{s+2} & 3^s-1 & 3^{s+1}+3^s & 3^{s+1}+3^s \\
1 & 0 & 3^s-1 & 3^s-3^{s+1} & 3^s \\
1 & 0 & 3^s-1 & 3^s & 3^s-3^{s+1}
\end{bmatrix}$$

4.2.2 Construction in Odd Dimension

From now on we further assume that $s \in \mathbb{Z}^+$ and $F : \mathbb{F}_3 \times \mathbb{F}_3^s \times \mathbb{F}_3^s \to \mathbb{F}_3$ be a non-weakly regular bent function defined by the Equation (45) such that $f^{(z)}$ is weakly regular bent for all $z \in \mathbb{F}_{3^s}$.

Condition 2 *$f^{(0)}$ is of type $(-)$ and $f^{(z)}$ is of type $(+)$ for all nonzero $z \in \mathbb{F}_3^s$; $f^{(0)}(0) = 0$ and $f^{(z)} = f^{(-z)}$ for all $z \in \mathbb{F}_3^s$; $f^{(z)}(x) = f^{(z)}(-x)$ for all $x \in \mathbb{F}_3$.*

Condition 3 *$f^{(0)}$ is of type $(+)$ and $f^{(z)}$ is of type $(-)$ for all nonzero $z \in \mathbb{F}_3^s$; $f^{(0)}(0) = 0$ and $f^{(z)} = f^{(-z)}$ for all $z \in \mathbb{F}_3^s$; $f^{(z)}(x) = f^{(z)}(-x)$ for all $x \in \mathbb{F}_3$.*

It is easy to see that if F satisfies the Condition 2 or 3 then $F(x, y, z) = F(-x, -y, -z)$ and $\widehat{F}(\alpha, \beta, \gamma) = \widehat{F}(-\alpha, -\beta, -\gamma)$ so that $F^*(x, y, z) = F^*(-x, -y, -z)$. Denote $G_2 = \mathbb{F}_3 \times \mathbb{F}_3^s \times \mathbb{F}_3^s$.

Proposition 4.2.1 *If F satisfies the Condition 2 then $D_2(F)$ is empty set; if F satisfies the Condition 3 then $C_1(F)$ is empty set.*

Proof 1 *Let us assume that F satisfies the Condition 2. By Equation (47) we have $\widehat{F}(\mathbf{0}) = \xi_{\mathbf{0}}\sqrt{3}3^s\epsilon_3^{f^{(0)^*}(0)}$. Since $f^{(0)}$ is of type $(-)$ then by Equation (42) F is of type $(-)$. Then F^* is of type $(+)$ (see Remark 4.1.2). By Equation (44) we have*

$$-i\sqrt{3}3^s\epsilon_3^{F(\theta)} = \sum_{v \in B_+(F)} \epsilon_3^{F^*(v)+v.\theta} - \sum_{v \in B_-(F)} \epsilon_3^{F^*(v)+v.\theta} \tag{427}$$

Put $\theta = \mathbf{0}$. Since F^* is of type $(+)$ then by Lemma 2.2.4 we have $S_0(F, \mathbf{0}) = 0$ and

$$i\sqrt{3}3^s\epsilon_3^{F^*(\mathbf{0})} = \sum_{i=0}^{2} \chi_\theta(D_i(F))\epsilon_3^i. \tag{428}$$

By Equation (45) $F(\mathbf{0}) = 0$ then we have $i\sqrt{3}3^s = \sum_{i=0}^{2} \chi_{\mathbf{0}}(D_i(F))\epsilon_3^i$. Moreover it is well known that $i\sqrt{3} = \sum_{j \in \mathbb{F}_3^\star}(\frac{j}{3})\epsilon_3^j$. Hence we have

$$\#D_0(F) + (\#D_1(F) - (\frac{1}{3})3^s)\epsilon_3 + (\#D_2(F) - (\frac{2}{3})3^s)\epsilon_3^2 = 0 \tag{429}$$

On the other hand

$$\#D_0(F) + \#D_1(F) + \#D_2(F) = \#B^-(F) = \#\mathbb{F}_3 \times \{\mathbf{0}\} \times \mathbb{F}_3^s = 3^{s+1}. \tag{430}$$

Combining Equations (429) and (430) we have $\#D_0(F) = 3^s$, $\#D_1(F) = 3^{s+1} - 3^s$ *and* $\#D_2(F) = 0$. *We conclude that* $D_2(F)$ *is the empty set.*
Let us assume that F *satisfies the Condition 3. Since* $f^{(0)}$ *is of type* $(+)$ *then by Equation (41)* F *is of type* $(+)$. *Then* F^* *is of type* $(-)$ *(see Remark 4.1.2). Put* $\theta = \mathbf{0}$. *Since* F^* *is of type* $(-)$ *then by Lemma 2.2.4 we have* $S_1(F, \mathbf{0}) = 0$ *and*

$$-i\sqrt{3}3^s\epsilon_3^{F^*(\mathbf{0})} = \sum_{i=0}^{2} \chi_\theta(C_i(F))\epsilon_3^i. \tag{431}$$

By Equation (45) $F(\mathbf{0}) = 0$ *then we have* $-i\sqrt{3}3^s = \sum_{i=0}^{2} \chi_{\mathbf{0}}(C_i(F))\epsilon_3^i$. *Hence we have*

$$\#C_0(F) + (\#C_1(F) + (\frac{1}{3})3^s)\epsilon_3 + (\#C_2(F) + (\frac{2}{3})3^s)\epsilon_3^2 = 0 \tag{432}$$

On the other hand

$$\#C_0(F) + \#C_1(F) + \#C_2(F) = \#B^+(F) = \#\mathbb{F}_3 \times \{\mathbf{0}\} \times \mathbb{F}_3^s = 3^{s+1}. \tag{433}$$

Combining Equations (432) and (433) we have $\#C_0(F) = 3^s$, $\#C_1(F) = 0$ *and* $\#C_2(F) = 3^{s+1} - 3^s$. *We conclude that* $C_1(F)$ *is the empty set.*

Proposition 4.2.2 *If* F *satisfies the Condition 2 (resp. Condition 3) then* F^* *satisfies the Condition 3 (resp. Condition 2).*

Proof 2 *The proof follows from the Equations (43) and (48) (see Remarks 4.1.1 and 4.1.2).*

Corollary 4.2.1 *If* F *satisfies the Condition 2 then* $H_1^+(F)$ *is empty set; if* F *satisfies the Condition 3 then* $H_2^-(F)$ *is empty set.*

Proof. It is clear that for $i \in \mathbb{F}_3$ we have $C_i(F^*)$=$H_i^+(F)$ and $D_i(F^*)$=$H_i^-(F)$ by definition. Hence the proof follows from the Propositions 4.2.1 and 4.2.2. □

Theorem 4.2.3 *Let* $F : G_2 \to \mathbb{F}_3$ *be a non-weakly regular bent function satisfying the Condition 2. Let* $A_0 = \{\mathbf{0}\}$, $A_i = C_i(F)$ *for* $1 \leq \forall i \leq 3$, $A_4 = D_0^\star(F)$ *and* $A_5 = D_1(F)$. *Let* $\Gamma_i := (G_2, E_i)$, $0 \leq i \leq 5$ *be Cayley graphs on* G_2 *with connection sets* $\{A_i\}_{i=0}^5$, *then* $(G_2, \{\Gamma_i\}_{i=0}^5)$ *is an association scheme of class* 5.

Proof. By similar arguments in Theorem 4.2.2 we have $C_i(F) = -C_i(F)$ and $D_i(F) = -D_i(F)$ for all $i \in \mathbb{F}_3$; $\chi_\theta(C_i(F))$ and $\chi_\theta(D_i(F))$ are integers for all $i \in \mathbb{F}_3$ and $\theta \in \mathbb{F}_3 \times \mathbb{F}_3^s \times \mathbb{F}_3^s$.

Assume that F satisfies the Condition 2 . Then the Equation (49) implies that $B_-(F) = \mathbb{F}_3 \times \{\mathbf{0}\} \times \mathbb{F}_3^s$. Then by character theory of finite abelian groups we have

$$\chi_\theta(B_-(F)) = \begin{cases} 3^{s+1} & \text{if } \theta \in B_-(F)^\perp, \\ 0 & \text{otherwise.} \end{cases} \tag{434}$$

By Remarks 4.1.1, 4.1.2 and Equation (411) we have $B_+(F^*) = \mathbb{F}_3 \times \mathbb{F}_3^s \times \{\mathbf{0}\}$ and $B_-(F^*) = \mathbb{F}_3^2 \times \mathbb{F}_3^s \times \mathbb{F}_3^{s\star}$. It is clear that $B_-(F)^\perp = \{0\} \times \mathbb{F}_3^s \times \{\mathbf{0}\}$ and for any element $(0, y, \mathbf{0}) \in B_-(F)^\perp$ we have $F(0, y, \mathbf{0}) = f^{(\mathbf{0})}(0) = 0$ implying $B_-(F)^\perp \subset H_0(F)$. Moreover, since $B_-(F)^\perp \subset B_+(F^*)$ we have $B_-(F)^\perp \subset H_0^+(F)$. Now we will prove that $B_-(F)^\perp = H_0^+(F)$. Since F^* is bent we have $F^{**}(x) = F(x)$ by Theorem 2.2.1. Let us denote $\theta := (\alpha, \beta, \gamma) \in G_2$ and $v := (x, y, z) \in G_2$. By inverse Walsh transform we have

$$\begin{aligned} -i\sqrt{3}3^s\epsilon_3^{F^*(\theta)} &= \textstyle\sum_{v \in B_+(F^*)} \epsilon_3^{F(v)+v.\theta} - \sum_{v \in B_-(F^*)} \epsilon_3^{F(v)+v.\theta} \\ &= \textstyle\sum_{i=0}^{2} \chi_\theta(C_i(F^*))\epsilon_3^i - \sum_{i=0}^{2} \chi_\theta(D_i(F^*))\epsilon_3^i. \end{aligned}$$

Put $\theta = \mathbf{0}$. Since F is of type $(-)$ then by Lemma 2.2.4 we have

$$-i\sqrt{3}3^s\epsilon_3^{F^*(\mathbf{0})} = -i\sqrt{3}3^s = \#C_0(F^*) + \#C_1(F^*)\epsilon_3 + \#C_2(F^*)\epsilon_3^2. \tag{435}$$

By previous arguments we have

$$\#C_0(F^*) = \#C_1(F^*) + \left(\frac{1}{3}\right)3^s = \#C_2(F^*) + \left(\frac{2}{3}\right)3^s. \tag{436}$$

Since $\#C_0(F^*) + \#C_1(F^*) + \#C_2(F^*) = \#B_+(F^*)$ and $B_+(F^*) = \mathbb{F}_3 \times \mathbb{F}_3^s \times \{\mathbf{0}\}$ combining with Equation (436) we have $\#C_0(F^*) = 3^s$. On the other hand we have $\#B_-(F)^\perp = 3^s$. Combining $B_-(F)^\perp \subset H_0^+(F)$ and $H_0^+(F) = C_0(F^*)$ we deduce that $B_-(F)^\perp = H_0^+(F)$.

Case 5 ($\theta \in H_i^+(F)$) *By Lemma 2.2.4 and Proposition 4.2.1 we have $S_0(F, \theta) = 0$ and $i\sqrt{3}3^s\epsilon_3^{F(\theta)} = \chi_\theta(D_0(F)) + \chi_\theta(D_1(F))\epsilon_3$. Then we have*

$$0 = \chi_\theta(D_0(F)) + \chi_\theta(D_1(F))\epsilon_3 - \left(\frac{1}{3}\right)3^s\epsilon_3^{i+1} - \left(\frac{2}{3}\right)3^s\epsilon_3^{i+2}. \tag{437}$$

$$0 = \sum_{j \in \mathbb{F}_3} \chi_\theta(C_j(F))\epsilon_3^j. \tag{438}$$

By Corollary 4.2.1 $i \in \{0, 2\}$. *If* $i = 0$ *then by Equation 437 we have* $\chi_\theta(D_0(F)) + (\chi_\theta(D_1(F)) - \left(\frac{1}{3}\right) 3^s)\epsilon_3 - \left(\frac{2}{3}\right) 3^s\epsilon_3^2 = 0$. *Then by previous arguments we have* $\chi_\theta(D_0(F)) = 3^s$ *and* $\chi_\theta(D_1(F)) = 3^{s+1} - 3^s$. *On the other hand if* $\theta \neq \mathbf{0}$, *the Equations (418) and (438) imply that* $\chi_\theta(C_j(F)) = -3^s$ *for all* $j \in \mathbb{F}_3$. *In particular since* $\mathbf{0} \in H_0^+$ *we have* $\chi_{\mathbf{0}}(D_0(F)) = \#D_0(F) = 3^s$ *and* $\chi_{\mathbf{0}}(D_1(F)) = \#D_1(F) = 3^{s+1} - 3^s$. *Then Equation (438) implies that* $\#C_j(F) = 3^{2s} - 3^s$ *for all* $j \in \mathbb{F}_3$.

If $i = 2$ *then by Equation 437 we have* $\chi_\theta(D_0(F)) - \left(\frac{1}{3}\right) 3^s + (\chi_\theta(D_1(F)) - \left(\frac{2}{3}\right) 3^s)\epsilon_3 = 0$. *Then by similar arguments we have* $\chi_\theta(D_0(F)) = 3^s$ *and* $\chi_\theta(D_1(F)) = -3^s$. *Then by Equations (418) and (438) we have* $\chi_\theta(C_j(F)) = 0$ *for all* $j \in \mathbb{F}_3$.

Case 6 ($\theta \in H_i^-(F)$**)** *By Lemma 2.2.4 and Proposition 4.2.1 we have* $S_1(F, \theta) = 0$ *and* $-i\sqrt{3}3^s\epsilon_3^{F(\theta)} = \sum_{j=0}^{2} \chi_\theta(C_j)\epsilon_3^j$. *Then we have*

$$\begin{aligned} 0 \;\; = \;\; & \chi_\theta(C_i(F))\epsilon_3^i + (\chi_\theta(C_{i+1}(F)) + \left(\tfrac{1}{3}\right) 3^s)\epsilon_3^{i+1} \\ & + (\chi_\theta(C_{i+2}(F)) + \left(\tfrac{2}{3}\right) 3^s)\epsilon_3^{i+2}. \end{aligned} \tag{439}$$

$$0 = \sum_{j \in \{0,1\}} \chi_\theta(D_j(F))\epsilon_3^j. \tag{440}$$

Since 1 *and* ϵ_3 *are linearly independent over* $\mathbb{F}_3$, *Equation (440) implies that* $\chi_\theta(D_0(F)) = \chi_\theta(D_1(F)) = 0$ *for all* $i \in \mathbb{F}_3$. *By previous arguments we have*

$$\chi_\theta(C_i(F)) = (\chi_\theta(C_{i+1}(F)) + \left(\frac{1}{3}\right) 3^s) = (\chi_\theta(C_{i+2}(F)) + \left(\frac{2}{3}\right) 3^s) \tag{441}$$

Combining Equations (418),(440), and (441) we have $\chi_\theta(C_i(F)) = 0$, $\chi_\theta(C_{i+1}(F)) = -3^s$ *and* $\chi_\theta(C_{i+2}(F)) = 3^s$ *for* $i \in \mathbb{F}_3$.

Let $S_0 := \{\chi_0\}$, $S_1 := \{\chi_y : 0 \neq y \in H_0^+(F)\}$, $S_2 := \{\chi_y : y \in H_2^+(F)\}$, and $S_j := \{\chi_y : y \in H_{j-3}^-(F)\}$ for $3 \leq \forall j \leq 5$. Then by Theorem 4.2.1 $(G_2, \{A_i\}_{i=0}^5)$ forms a translation scheme. □

Hence for any positive integer s we have translation scheme of class 5 with following first eigenmatrix;

$$\begin{bmatrix} 1 & 3^{2s}-3^s & 3^{2s}-3^s & 3^{2s}-3^s & 3^s-1 & 3^{s+1}-3^s \\ 1 & -3^s & -3^s & -3^s & 3^s-1 & 3^{s+1}-3^s \\ 1 & 0 & 0 & 0 & 3^s-1 & -3^s \\ 1 & 0 & -3^s & 3^s & -1 & 0 \\ 1 & 3^s & 0 & -3^s & -1 & 0 \\ 1 & -3^s & 3^s & 0 & -1 & 0 \end{bmatrix}$$

Moreover fusing the first three non-trivial classes of the those translation schemes we obtain fusion schemes of class 3.

$$\begin{bmatrix} 1 & 3^{2s+1}-3^{s+1} & 3^s-1 & 3^{s+1}-3^s \\ 1 & -3^{s+1} & 3^s-1 & 3^{s+1}-3^s \\ 1 & 0 & 3^s-1 & -3^s \\ 1 & 0 & -1 & 0 \end{bmatrix}$$

Theorem 4.2.4 *Let $F : G_2 \to \mathbb{F}_3$ be a non-weakly regular bent function satisfying Condition 3. Let $A_0 = \{\mathbf{0}\}$, $A_1 = C_0^\star(F)$, and $A_2 = C_2(F)$, $A_j = D_{j-3}(F)$ for $3 \leq \forall j \leq 5$. Let $\Gamma_i := (G_2, E_i)$, $0 \leq i \leq 5$ be Cayley graphs on G_2 with connection sets $\{A_i\}_{i=0}^5$, then $(G_2, \{\Gamma_i\}_{i=0}^5)$ is an association scheme of class 5.*

Proof. By previous arguments we have $C_i(F) = -C_i(F)$ and $D_i(F) = -D_i(F)$ for all $i \in \mathbb{F}_3$; $\chi_\theta(C_i(F))$ and $\chi_\theta(D_i(F))$ are integers for all $i \in \mathbb{F}_3$ and $\theta \in \mathbb{F}_3 \times \mathbb{F}_3^s \times \mathbb{F}_3^s$.

Assume that F satisfies Condition 3. Then Equation (49) implies that $B_+(F) = \mathbb{F}_3 \times \{\mathbf{0}\} \times \mathbb{F}_3^s$. Then by character theory of finite abelian groups we have

$$\chi_\theta(B_+(F)) = \begin{cases} 3^{s+1} & \text{if } \theta \in B_+(F)^\perp, \\ 0 & \text{otherwise.} \end{cases} \tag{442}$$

By Remarks 4.1.1, 4.1.2 and Equation (411) we have $B_-(F^*) = \mathbb{F}_3 \times \mathbb{F}_3^s \times \{\mathbf{0}\}$ and $B_+(F^*) = \mathbb{F}_3 \times \mathbb{F}_3^s \times \mathbb{F}_3^{s\star}$. It is clear that $B_+(F)^\perp = \{0\} \times \mathbb{F}_3^s \times \{\mathbf{0}\}$ and for any element $(0, y, \mathbf{0}) \in B_+(F)^\perp$ we have $F(0, y, \mathbf{0}) = f^{(\mathbf{0})}(0) = 0$ implying $B_+(F)^\perp \subset$

$H_0(F)$. Moreover, since $B_+(F)^\perp \subset B_-(F^*)$ we have $B_+(F)^\perp \subset H_0^-(F)$. Now we will prove that $B_+(F)^\perp = H_0^-(F)$.

By previous arguments we have $F^{**}(x) = F(x)$. Put $\theta = \mathbf{0}$. Since F is of type $(+)$ then by Lemma 2.2.4 we have

$$i\sqrt{3}3^s\epsilon_3^{F^*(\mathbf{0})} = i\sqrt{3}3^s = \#D_0(F^*) + \#D_1(F^*)\epsilon_3 + \#D_2(F^*)\epsilon_3^2. \tag{443}$$

By previous arguments we have

$$\#D_0(F^*) = \#D_1(F^*) - \left(\frac{1}{3}\right)3^s = \#D_2(F^*) - \left(\frac{2}{3}\right)3^s. \tag{444}$$

Since $\#D_0(F^*)+\#D_1(F^*)+\#D_2(F^*) = \#B_-(F^*)$ and $B_-(F^*) = \mathbb{F}_3 \times \mathbb{F}_3^s \times \{\mathbf{0}\}$ combining with Equation (444) we have $\#D_0(F^*) = 3^s$. On the other hand we have $\#B_+(F)^\perp = 3^s$. Combining $B_+(F)^\perp \subset H_0^-(F)$ and $H_0^-(F) = D_0(F^*)$ we deduce that $B_+(F)^\perp = H_0^-(F)$.

Case 7 ($\theta \in H_i^+(F)$) *By Lemma 2.2.4 and Proposition 4.2.1 we have $S_0(F,\theta) = 0$ and $i\sqrt{3}3^s\epsilon_3^{F(\theta)} = \sum_{j=0}^2 \chi_\theta(D_j)\epsilon_3^j$. Then we have*

$$\begin{aligned} 0 \;=\; & \chi_\theta(D_i(F))\epsilon_3^i + (\chi_\theta(D_{i+1}(F)) - \left(\tfrac{1}{3}\right)3^s)\epsilon_3^{i+1} \\ & -(\chi_\theta(D_{i+2}(F)) + \left(\tfrac{2}{3}\right)3^s)\epsilon_3^{i+2}. \end{aligned} \tag{445}$$

$$0 = \sum_{j\in\{0,2\}} \chi_\theta(C_j(F))\epsilon_3^j. \tag{446}$$

By similar arguments above, Equation (446) implies that $\chi_\theta(C_0(F)) = \chi_\theta(C_2(F)) = 0$ for all $i \in \mathbb{F}_3$.

By previous arguments we have

$$\chi_\theta(D_i(F)) = (\chi_\theta(D_{i+1}(F)) - \left(\frac{1}{3}\right)3^s) = (\chi_\theta(D_{i+2}(F)) - \left(\frac{2}{3}\right)3^s). \tag{447}$$

Combining Equations (418),(446) and (447) we have $\chi_\theta(D_i(F)) = 0$, $\chi_\theta(D_{i+1}(F)) = 3^s$ and $\chi_\theta(D_{i+2}(F)) = -3^s$ for $i \in \mathbb{F}_3$.

Case 8 ($\theta \in H_i^-(F)$) *By Lemma 2.2.4 and Proposition 4.2.1 we have $S_1(F,\theta) = 0$ and $-i\sqrt{3}3^s\epsilon_3^{F(\theta)} = \chi_\theta(C_0(F)) + \chi_\theta(C_2(F))\epsilon_3^2$. Then we have*

$$0 = \chi_\theta(C_0(F)) + \chi_\theta(C_2(F))\epsilon_3^2 + \left(\frac{1}{3}\right)3^s\epsilon_3^{i+1} + \left(\frac{2}{3}\right)3^s\epsilon_3^{i+2}. \tag{448}$$

$$0 = \sum_{j \in \mathbb{F}_3} \chi_\theta(D_j(F))\epsilon_3^j. \tag{449}$$

By Corollary 4.2.1 $i \in \{0, 1\}$. *If* $i = 0$ *then by Equation 448 we have* $\chi_\theta(C_0(F)) + (\chi_\theta(C_2(F)) + \left(\frac{2}{3}\right) 3^s)\epsilon_3^2 + \left(\frac{1}{3}\right) 3^s\epsilon_3 = 0$. *Then by previous arguments we have* $\chi_\theta(C_0(F)) = 3^s$ *and* $\chi_\theta(C_2(F)) = 3^{s+1} - 3^s$. *On the other hand if* $\theta \neq \mathbf{0}$, *Equations (418) and (449) imply that* $\chi_\theta(D_j(F)) = -3^s$ *for all* $j \in \mathbb{F}_3$. *In particular since* $\mathbf{0} \in H_0^-(F)$ *we have* $\chi_{\mathbf{0}}(C_0(F)) = \#C_0(F) = 3^s$ *and* $\chi_{\mathbf{0}}(C_2(F)) = \#C_2(F) = 3^{s+1} - 3^s$. *Then Equation (449) implies that* $\#D_j(F) = 3^{2s} - 3^s$ *for all* $j \in \mathbb{F}_3$.

If $i = 1$ *then by Equation 448 we have* $\chi_\theta(C_0(F)) + \left(\frac{2}{3}\right) 3^s + (\chi_\theta(C_2(F) + \left(\frac{1}{3}\right) 3^s)\epsilon_3 = 0$. *Then by similar arguments we have* $\chi_\theta(C_0(F)) = 3^s$ *and* $\chi_\theta(C_2(F)) = -3^s$. *Then by Equations (418) and (449) we have* $\chi_\theta(D_j(F)) = 0$ *for all* $j \in \mathbb{F}_3$.

Let $S_0 := \{\chi_0\}$, $S_i := \{\chi_y : y \in H_{i-1}^+(F)\}$ for $1 \leq \forall i \leq 3$, and $S_4 := \{\chi_y : 0 \neq y \in H_0^-(F)\}$, $S_5 := \{\chi_y : y \in H_1^-(F)\}$. Then by Theorem 4.2.1 $(G_2, \{A_i\}_{i=0}^5)$ forms a translation scheme. □

Hence for any positive integer s we have translation scheme of class 5 with following first eigenmatrix;

$$\begin{bmatrix} 1 & 3^s - 1 & 3^{s+1} - 3^s & 3^{2s} - 3^s & 3^{2s} - 3^s & 3^{2s} - 3^s \\ 1 & -1 & 0 & 0 & 3^s & -3^s \\ 1 & -1 & 0 & -3^s & 0 & 3^s \\ 1 & -1 & 0 & 3^s & -3^s & 0 \\ 1 & 3^s - 1 & 3^{s+1} - 3^s & -3^s & -3^s & -3^s \\ 1 & 3^s - 1 & -3^s & 0 & 0 & 0 \end{bmatrix}$$

Moreover fusing the last three non-trivial classes of the those translation schemes we obtain fusion schemes of class 3.

$$\begin{bmatrix} 1 & 3^s - 1 & 3^{s+1} - 3^s & 3^{2s+1} - 3^{s+1} \\ 1 & -1 & 0 & 0 \\ 1 & 3^s - 1 & 3^{s+1} - 3^s & -3^{s+1} \\ 1 & 3^s - 1 & -3^s & 0 \end{bmatrix}$$

Remark 4.2.1 *We observe that the first eigenmatrices of the translation schemes associated with Theorems 4.2.3 and 4.2.4 can be obtained from each other by multiplying one with a permutation matrix. Hence corresponding association schemes are isometric. Therefore we should think as Theorems 4.2.3 and 4.2.4 are equivalent.*

4.3 Numerical Examples

In the examples below, we evaluate the first eigenmatrices of the four different translation schemes by using the *Magma Computational Algebra System*.

Example 8 *Let* $s = 1$, $f : \mathbb{F}_3^4 \to \mathbb{F}_3$, $f(x_1, x_2, x_3, x_4) = x_2^2x_4^2 + x_1^2 + x_2^2 + x_3x_4$ *be a non-weakly regular bent function in the GMMF class satisfying Condition 1. Then the first eigenmatrix of the corresponding translation scheme is*

$$\begin{bmatrix} 1 & 18 & 18 & 18 & 2 & 12 & 12 \\ 1 & 6 & -3 & -3 & -1 & 0 & 0 \\ 1 & -3 & 6 & -3 & -1 & 0 & 0 \\ 1 & -3 & -3 & 6 & -1 & 0 & 0 \\ 1 & -9 & -9 & -9 & 2 & 12 & 12 \\ 1 & 0 & 0 & 0 & 2 & -6 & 3 \\ 1 & 0 & 0 & 0 & 2 & 3 & -6 \end{bmatrix}$$

By fusing the first 3 non-trivial classes in the first eigenmatrix, we obtain the first eigenmatrix of the fusing scheme of class 4.

$$\begin{bmatrix} 1 & 54 & 2 & 12 & 12 \\ 1 & 0 & -1 & 0 & 0 \\ 1 & -27 & 2 & 12 & 12 \\ 1 & 0 & 2 & -6 & 3 \\ 1 & 0 & 2 & 3 & -6 \end{bmatrix}$$

Example 9 *Let* $s = 2$, $f : \mathbb{F}_3^6 \to \mathbb{F}_3$, $f(x_1, x_2, x_3, x_4, x_5, x_6) = x_1^2x_5^2x_6^2 + 2x_1^2x_5x_6 + x_1^2x_6^2 + x_1^2 + x_2^2x_5^2x_6^2 + x_2^2x_5^2 + x_2^2x_5x_6 + x_2^2 + x_3x_5 + x_4x_6$ *be a non-weakly regular bent function in the GMMF class satisfying Condition 1. Then the first eigenmatrix*

of the corresponding translation scheme is

$$\begin{bmatrix} 1 & 216 & 216 & 216 & 8 & 36 & 36 \\ 1 & 18 & -9 & -9 & -1 & 0 & 0 \\ 1 & -9 & 18 & -9 & -1 & 0 & 0 \\ 1 & -9 & -9 & 18 & -1 & 0 & 0 \\ 1 & -27 & -27 & -27 & 8 & 36 & 36 \\ 1 & 0 & 0 & 0 & 8 & -18 & 9 \\ 1 & 0 & 0 & 0 & 8 & 9 & -18 \end{bmatrix}$$

By fusing the first 3 non-trivial classes in the first eigenmatrix, we obtain the first eigenmatrix of the fusing scheme of class 4.

$$\begin{bmatrix} 1 & 648 & 8 & 36 & 36 \\ 1 & 0 & -1 & 0 & 0 \\ 1 & -81 & 8 & 36 & 36 \\ 1 & 0 & 8 & -18 & 9 \\ 1 & 0 & 8 & 9 & -18 \end{bmatrix}$$

Example 10 *Let $s = 1$, $f : \mathbb{F}_3^3 \to \mathbb{F}_3$, $f(x_1, x_2, x_3) = 2x_1^2x_3^2 + 2x_1^2 + x_2x_3$ be a non-weakly regular bent function in the GMMF class satisfying Condition 2. Then the first eigenmatrix of the corresponding translation scheme is*

$$\begin{bmatrix} 1 & 6 & 6 & 6 & 2 & 6 \\ 1 & -3 & -3 & -3 & 2 & 6 \\ 1 & 0 & 0 & 0 & 2 & -3 \\ 1 & 0 & -3 & 3 & -1 & 0 \\ 1 & 3 & 0 & -3 & -1 & 0 \\ 1 & -3 & 3 & 0 & -1 & 0 \end{bmatrix}$$

By fusing the first 3 non-trivial classes in the first eigenmatrix, we obtain the first eigenmatrix of the fusing scheme of class 3.

$$\begin{bmatrix} 1 & 18 & 2 & 6 \\ 1 & -9 & 2 & 6 \\ 1 & 0 & 2 & -3 \\ 1 & 0 & -1 & 0 \end{bmatrix}$$

Example 11 *Let* $s = 2$*,* $f : \mathbb{F}_3^5 \to \mathbb{F}_3$*,* $f(x_1, x_2, x_3, x_4, x_5) = 2x_1^2x_4^2x_5^2 + x_1^2x_4^2 + x_1^2x_5^2 + x_1^2 + x_1x_4 + x_3x_5$ *be a non-weakly regular bent function in the GMMF class satisfying Condition 3. Then the first eigenmatrix of the corresponding translation scheme is*

$$\begin{bmatrix} 1 & 8 & 18 & 72 & 72 & 72 \\ 1 & -1 & 0 & 0 & 9 & -9 \\ 1 & -1 & 0 & -9 & 0 & 9 \\ 1 & -1 & 0 & 9 & -9 & 0 \\ 1 & 8 & 18 & -9 & -9 & -9 \\ 1 & 8 & -9 & 0 & 0 & 0 \end{bmatrix}$$

By fusing the last 3 non-trivial classes in the first eigenmatrix, we obtain the first eigenmatrix of the fusing scheme of class 3.

$$\begin{bmatrix} 1 & 8 & 18 & 72 \\ 1 & -1 & 0 & 0 \\ 1 & 8 & 18 & -27 \\ 1 & 8 & -9 & 0 \end{bmatrix}$$

CHAPTER 5

THREE WEIGHT LINEAR CODES FROM NON-WEAKLY REGULAR BENT FUNCTIONS

In this chapter, we build the classes of three-weight linear p-ary codes on $B_+(f)$ and $B_-(f)$ from non-weakly regular dual-bent functions based on the first conventional construction. Moreover, we determine the weight distributions of the built codes when the associated non-weakly regular bent functions belong to a certain subclass of the *GMMF* bent functions. We examine that all non-zero codewords of the constructed codes are minimal for nearly all cases.

5.1 Preliminaries

5.1.1 Cyclotomic Fields

Let p be an odd prime. A cyclotomic field $\mathbb{Q}(\epsilon_p)$ is obtained from the field $\mathbb{Q}$ by adjoining ϵ_p. The ring of integers in $\mathbb{Q}(\epsilon_p)$ is defined as $\mathcal{O}_{\mathbb{Q}(\epsilon_p)} := \mathbb{Z}(\epsilon_p)$. An integral basis of $\mathcal{O}_{\mathbb{Q}(\epsilon_p)}$ is the set $\{\epsilon_p^i : 1 \leq i \leq p-1\}$.
Let p be an odd prime number. The quadratic Gauss sum is defined as

$$\sum_{i \in \mathbb{F}_p^\star} \left(\frac{i}{p}\right) \epsilon_p^i = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \ (mod\ 4); \\ i\sqrt{p} & \text{if } p \equiv 3 \ (mod\ 4). \end{cases} \tag{51}$$

5.1.2 Linear Codes.

Let p be a prime number and n, k be positive integers. 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

$[n, k]_p$. The elements of $\mathcal{C}$ are referred to as *codewords*. A linear code $\mathcal{C}$ of length n and dimension k over $\mathbb{F}_p$ with minimum Hamming distance d is denoted by $[n, k, d]_p$. Note that the minimum Hamming distance d determine the error-correcting capability of $\mathcal{C}$. It is effortless to see that the minimum Hamming distance of $\mathcal{C}$ is the minimal Hamming weight of its nonzero codewords. The Hamming weight of a vector $v = (v_0, \ldots, a_{n-1}) \in \mathbb{F}_p^n$, denoted by $wt(v)$, is the size of its support described as

$$\mathrm{supp}(v) = \{0 \leq i \leq n-1 : v_i \neq 0\}.$$

Let E_a be indicating the number of codewords with Hamming weight a in $\mathcal{C}$ of length n. Then, $(1, E_1, \ldots, E_n)$ is the *weight distribution* of $\mathcal{C}$ and the polynomial $1+E_1y+\cdots+E_ny^n$ is reffered to as the *weight enumerator* of $\mathcal{C}$. The code $\mathcal{C}$ is reffered to as a t-*weight code* if the number of nonzero E_a in the weight distribution is t.

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 v covers a codeword u if $\mathrm{supp}(u) \subset \mathrm{supp}(v)$. If a nonzero codeword v of $\mathcal{C}$ does not cover any other nonzero codeword of $\mathcal{C}$, then v is referred to as a *minimal codeword* of $\mathcal{C}$. A linear code $\mathcal{C}$ is said to be *minimal* if each nonzero codeword of $\mathcal{C}$ is minimal. The *covering problem* of $\mathcal{C}$ is to locate all minimal codewords of $\mathcal{C}$.

In [2], the authors give a simple criteria to determine whether a given linear code is minimal.

Lemma 5.1.1 *(Ashikhmin-Barg) Let $\mathcal{C}$ be a linear code over $\mathbb{F}_p$. Then, all nonzero codewords of $\mathcal{C}$ are minimal if*

$$\frac{p-1}{p} < \frac{a_{\min}}{a_{\max}}, \tag{52}$$

where $a_{\min}$ and $a_{\max}$ indicate the minimum and maximum weights of nonzero codewords of $\mathcal{C}$, respectively.

5.2 Non-Weakly Regular Bent Functions and GMMF Class

Proposition 5.2.1 *Let $f : \mathbb{F}_p^n \to \mathbb{F}_p$ be a non-weakly regular bent function and its dual function f^* is also bent. If n even or n odd and $p \equiv 1$ mod 4, then we have*

$$S_0(f,y) = \begin{cases} p^{\frac{n}{2}}\epsilon_p^{f(y)} & \text{if } f^*(x)+x.y \text{ is of type } (+); \\ 0 & \text{if } f^*(x)+x.y \text{ is of type } (-); \end{cases}$$

$$S_1(f,y) = \begin{cases} -p^{\frac{n}{2}}\epsilon_p^{f(y)} & \text{if } f^*(x)+x.y \text{ is of type } (-); \\ 0 & \text{if } f^*(x)+x.y \text{ is of type } (+). \end{cases}$$

If n odd and $p \equiv 3$ mod 4, then we have

$$S_0(f,y) = \begin{cases} -ip^{\frac{n-1}{2}}\sqrt{p}\epsilon_p^{f(y)} & \text{if } f^*(x)+x.y \text{ is of type } (-); \\ 0 & \text{if } f^*(x)+x.y \text{ is of type } (+); \end{cases}$$

$$S_1(f,y) = \begin{cases} ip^{\frac{n-1}{2}}\sqrt{p}\epsilon_p^{f(y)} & \text{if } f^*(x)+x.y \text{ is of type } (+); \\ 0 & \text{if } f^*(x)+x.y \text{ is of type } (-). \end{cases}$$

Proof. The proof follows from Lemmas 2.2.4 and 2.2.5. □

Proposition 5.2.2 *Let $f : \mathbb{F}_p^n \to \mathbb{F}_p$ be a bent function such that $f(0) = 0$ and $f(x) = f(-x)$. Then $f^*(x) = f^*(-x)$ and $f^*(0) = 0$.*

Proof. For all $\alpha \in \mathbb{F}_p^n$, we have

$$\begin{aligned} \hat{f}(-\alpha) &= \xi_{-\alpha}p^{\frac{n}{2}}\epsilon_p^{f^*(-\alpha)} = \textstyle\sum_{x\in\mathbb{F}_p^n}\epsilon_p^{f(x)+\alpha.x} = \sum_{x\in\mathbb{F}_p^n}\epsilon_p^{f(-x)-\alpha.(-x)} = \hat{f}(\alpha) \\ &= \xi_\alpha p^{\frac{n}{2}}\epsilon_p^{f^*(\alpha)}. \end{aligned}$$

Hence, we prove $f^*(x) = f^*(-x)$. Put $f^*(0) = i_0$. If n is odd (resp. even), by Proposition 2.2.1 (resp. 2.2.2), we have $N_{i_0}(f)$ is an odd integer. Since $f(x) = f(-x)$, it is possible if and only if $i_0 = 0$. □

Let F be a non-weakly regular bent function defined by Equation 45 and $f^{(z)}$ is weakly regular bent for all $z \in F_p^s$. Then by Remarks 4.1.1, 4.1.2 and Equation (410), we have

$$B_{\pm}(F^*) = \begin{cases} \mathbb{F}_p^m \times \mathbb{F}_p^s \times W^{\pm}(F) & \text{if } p^n \equiv 1 \bmod 4; \\ \mathbb{F}_p^m \times \mathbb{F}_p^s \times W^{\mp}(F) & \text{if } p^n \equiv 3 \bmod 4. \end{cases} \tag{53}$$

Remark 5.2.1 *Let $f^{(z)} = f^{(-z)}$ and $f^{(z)}(x) = f^{(z)}(-x)$ for all $z \in \mathbb{F}_p^s,\ x \in \mathbb{F}_p^m$. Since $F(-x,-y,-z) = f^{(-z)}(-x)+y.z$, then we have $F(x,y,z) = F(-x,-y,-z)$. Moreover, Equation (49) enables us to set $B_+(F)$ or $B_-(F)$ as a vector space of any dimension k with $m+s \leq k < m+2s$.*

In the following two sections, inspiring from the work of Mesnager in [32], we construct three-weight linear codes based on the first conventional construction. Although the regular concept of the building technique employed is a classical one, but we are going to for the first time making use of non-weakly regular bent functions to construct linear codes over subspaces of finite fields of odd characteristic.

5.3 Three-Weight Linear Codes on $B_+(f)$

For any $\alpha \in \mathbb{F}_p,\ \beta \in \mathbb{F}_p^n$, we define a function

$$\begin{array}{rccl} h_{\alpha,\beta} & : & \mathbb{F}_p^n & \longrightarrow & \mathbb{F}_p, \\ & & x & \longmapsto & h_{\alpha,\beta}(x) := \alpha\Psi(x) + \beta.x, \end{array}$$

where Ψ is a mapping from $\mathbb{F}_p^n$ to $\mathbb{F}_p$ such that $\Psi(\mathbf{0}) = 0$.

Let $f : \mathbb{F}_p^n \to \mathbb{F}_p$ be a non-weakly regular bent function such that $f(x) = f(-x)$, $f(\mathbf{0}) = 0$, and f^* is bent. Then, for any $y \in \mathbb{F}_p^n$ and $u \in \mathbb{F}_p$, we have $c_{f^*}(y,u) = \#\{\alpha : \alpha \in B_+(f^*) \mid f(\alpha) + \alpha.y = u\}$, $d_{f^*}(y,u) = \#\{\alpha : \alpha \in B_-(f^*) \mid f(\alpha) + \alpha.y = u\}$. Let $B_+(f)$ be an $\mathbb{F}_p$-vector space with $\dim(B_+(f)) \geq \lfloor \frac{n}{2} \rfloor + 1$. Put $\dim(B_+(f)) = r$ and take $\Psi(x) = f^*(x)$. Then we also define a linear code $\mathcal{C}_\Psi$ over $\mathbb{F}_p$ as

$$\mathcal{C}_\Psi = \{c_{\alpha,\beta} = (h_{\alpha,\beta}(\zeta_1), h_{\alpha,\beta}(\zeta_2), \ldots, h_{\alpha,\beta}(\zeta_{p^r-1})) : \alpha \in \mathbb{F}_p, \beta \in \mathbb{F}_{p^n}\}, \tag{54}$$

where $\zeta_1, \ldots, \zeta_{p^r-1}$ are the elements of $B_+(f)^\star$ and $c_{\alpha,\beta}$ denotes a codeword of $\mathcal{C}_\Psi$. The length of the linear code $\mathcal{C}_\Psi$ is $p^r - 1$.

Remark 5.3.1 *Note that there are infinitely many non-weakly regular bent functions such that* $f(x) = f(-x)$*,* $B_+(f)$ *is a vector space and* $\dim(B_+(f)) \geq \lfloor \frac{n}{2} \rfloor + 1$ *(see, Remark 5.2.1).*

Proposition 5.3.1 *The linear code* $\mathcal{C}_\psi$ *of length* $p^r - 1$ *over* $\mathbb{F}_p$ *defined by* (54) *is a* k*-dimensional subspace of* $\mathbb{F}_p^n$*, where* $k = r + 1$ *and denoted by* $[p^r - 1, r + 1]_p$*.*

Proof. Let $\theta : \mathbb{F}_p \times \mathbb{F}_p^n \to \mathbb{F}_p^{p^r-1}$ such that $(\alpha, \beta) \to (h_{\alpha,\beta}(\zeta_1), h_{\alpha,\beta}(\zeta_2), \ldots, h_{\alpha,\beta}(\zeta_{p^r-1}))$, where $\zeta_1, \ldots, \zeta_{p^r-1}$ are the elements of $B_+(f)^\star$. Then $\mathrm{Ker}\ (\theta) := \{(\alpha, \beta) \in \mathbb{F}_p \times \mathbb{F}_p^n \mid \alpha f^*(x) = -\beta.x \quad \text{for all } x \in B_+(f)^\star\}$. If $\alpha \neq 0$, then $f^*(x) = -\alpha^{-1}(\beta.x)$ for all $x \in B_+(f)$. Since $f^*(x)$ is bent and $r \geq \lfloor \frac{n}{2} \rfloor + 1$, it is not possible. If $\alpha = 0$, then $\beta.x = 0$ for all $x \in B_+(f)$, which implies that $\beta \in \big(B_+(f)\big)^\perp$. Hence, by the isomorphism $\bar{\theta} : (\mathbb{F}_p \times \mathbb{F}_p^n)/\mathrm{Ker}\ (\theta) \to \mathrm{Im}(\theta)$, we have $\#\mathcal{C}_\Psi = \frac{p^{n+1}}{p^{n-r}} = p^{r+1}$. □

Let D be a subset of $\mathbb{F}_p^n$. Any function $f : D \longrightarrow \mathbb{F}_p$ is said to be *balanced* over $\mathbb{F}_p$ if f takes each and every value of $\mathbb{F}_p$ the equal range of times. If D is a subspace of $\mathbb{F}_p^n$ and $j \notin D^\perp$, then it is well-known that $j.x$ is balanced over $\mathbb{F}_p$. From now on we keep the above arguments and evaluate the weight of codewords in two cases. For $c_{\alpha,\beta} \in \mathcal{C}_{f^*}$, we have the following.

Case 9 n *is even.*

- $\alpha = 0$

  $wt(c_{0,\beta}) = wt((\beta.\zeta_1, \beta.\zeta_2, \ldots, \beta.\zeta_{p^r-1})$ *for all* $\beta \in \mathbb{F}_p^n$*. If* $\beta \in \big(B_+(f)\big)^\perp$*, then* $wt(c_{0,\beta}) = 0$*. If* $\beta \notin \big(B_+(f)\big)^\perp$*, then* $wt(c_{0,\beta}) = (p-1)p^{r-1}$ *by balancedness.*

- $\alpha \neq 0$

  $wt(c_{\alpha,\beta}) = wt((\alpha f^*(\zeta_1) + \beta.\zeta_1, \alpha f^*(\zeta_2) + \beta.\zeta_2, \ldots, \alpha f^*(\zeta_{p^r-1}) + \beta.\zeta_{p^r-1})$ *for all* $\alpha \in \mathbb{F}_p$, $\beta \in \mathbb{F}_p^n$*. It is clear that* $wt(c_{\alpha,\beta}) = wt(c_{1,\alpha^{-1}\beta})$*, where* α^{-1} *is the multiplicative inverse of* $\alpha \in \mathbb{F}_p^\star$*.*

  If $\alpha^{-1}\beta \in B_-(f^*)$*, by Proposition 5.2.1, we have*

$$\sum_{u=0}^{p-1} c_f(\alpha^{-1}\beta, u)\epsilon_p^u = \sum_{\zeta \in B_+(f)} \epsilon_p^{f^*(\zeta)+\zeta.(\alpha^{-1}\beta)} = 0,$$

which implies $-c_f(\alpha^{-1}\beta, 0) = \sum_{u=1}^{p-1} c_f(\alpha^{-1}\beta, u)\epsilon_p^u$. *As the set* $\{\epsilon_p^i : 1 \leq i \leq p-1\}$ *is an integral basis of* $\mathcal{O}_{\mathbb{Q}(\epsilon_p)}$ *and* $\sum_{i=1}^{p-1} \epsilon_p^i = -1$, *we have* $c_f(\alpha^{-1}\beta, 0) = c_f(\alpha^{-1}\beta, u)$ *for all* $u \in \mathbb{F}_p^\star$. *Hence* $f^*(\zeta) + \zeta.(\alpha^{-1}\beta)$ *is balanced over* $B_+(f)$. *Since* $f^*(\mathbf{0}) = 0$, *we have* $wt(c_{1,\alpha^{-1}\beta}) = (p-1)p^{r-1}$. *If* $\alpha^{-1}\beta \in B_+(f^*)$, *by Proposition 5.2.1, we have* $p^{\frac{n}{2}}\epsilon_p^{f(\alpha^{-1}\beta)} = \sum_{\zeta \in B_+(f)} \epsilon_p^{f^*(\zeta)+\zeta.(\alpha^{-1}\beta)}$. *For* $f(\alpha^{-1}\beta) = 0$, *we have*

$$\sum_{u=0}^{p-1} c_f(\alpha^{-1}\beta, u)\epsilon_p^u = p^{\frac{n}{2}}.$$

Then $c_f(\alpha^{-1}\beta, 0) - p^{\frac{n}{2}} + \sum_{u=1}^{p-1} c_f(\alpha^{-1}\beta, u)\epsilon_p^u = 0$. *Since the set* $\{\epsilon_p^i : 1 \leq i \leq p-1\}$ *is an integral basis of* $\mathcal{O}_{\mathbb{Q}(\epsilon_p)}$, *there exists a unique integer* a *such that* $c_f(\alpha^{-1}\beta, 0) = a + p^{\frac{n}{2}}$ *and* $c_f(\alpha^{-1}\beta, u) = a$ *for all* $u \neq 0 \in \mathbb{F}_p$. *On the other hand, we have* $\sum_{u=0}^{p-1} c_f(\alpha^{-1}\beta, u) = p^r$. *Therefore,* $a = p^{r-1} - p^{\frac{n}{2}-1}$ *and* $wt(c_{1,\alpha^{-1}\beta}) = \sum_{u=1}^{p-1} c_f(\alpha^{-1}\beta, u) = (p-1)(p^{r-1} - p^{\frac{n}{2}-1})$.

When $f(\alpha^{-1}\beta) \neq 0$, *by similar arguments above, we have*

$$wt(c_{1,\alpha^{-1}\beta}) = (p-1)(p^{r-1} - p^{\frac{n}{2}-1}) + p^{\frac{n}{2}}.$$

As a result of Case 9, we conclude even case with the following theorem.

Theorem 5.3.1 *Let* n *be an even integer, and* $f : \mathbb{F}_p^n \to \mathbb{F}_p$ *be a non-weakly regular bent function such that* $f(\mathbf{0}) = 0$, $f(x) = f(-x)$ *and* f^* *is bent. Let* $B_+(f)$ *be an* r*-dimensional* $\mathbb{F}_p$*-vector space with* $r \geq \frac{n}{2} + 1$. *Then the codewords* $c_{\alpha,\beta}$ *of the linear code* $\mathcal{C}_{f^*}$ *defined by equation (54) has zero-weight if* $\alpha = 0$ *and* $\beta \in \big(B_+(f)\big)^\perp$ *i.e.,* $(\alpha, \beta) \in \mathrm{Ker}\,(\theta)$. *The non-zero weight codewords are as follows.*

$$wt(c_{\alpha,\beta}) = \begin{cases} (p-1)p^{r-1} & \text{if } \alpha = 0 \text{ and } \beta \notin \big(B_+(f)\big)^\perp \text{ or } \alpha \neq 0 \text{ and } \alpha^{-1}\beta \in B_-(f^*); \\ (p-1)(p^{r-1} - p^{\frac{n}{2}-1}) & \text{if } \alpha \neq 0 \text{ and } \alpha^{-1}\beta \in B_+(f^*) \text{ and } f(\alpha^{-1}\beta) = 0\,; \\ (p-1)(p^{r-1} - p^{\frac{n}{2}-1}) + p^{\frac{n}{2}} & \text{if } \alpha \neq 0 \text{ and } \alpha^{-1}\beta \in B_+(f^*) \text{ and } f(\alpha^{-1}\beta) \neq 0\,. \end{cases}$$

Proposition 5.3.2 *Let* $n = m + 2s$ *and denote* $\mathbb{F}_p^m \times \mathbb{F}_p^s \times \mathbb{F}_p^s$ *by* $\mathbb{F}_p^n$. *Let* $F : \mathbb{F}_p^n \to \mathbb{F}_p$ *be a non-weakly regular bent function defined by Equation (45) such that* $f^{(z)}$ *is weakly regular bent for each* $z \in \mathbb{F}_p^s$. *Let* F *satisfies the conditions of Theorem 5.3.1. With the above notations, the weight distribution of* $\mathcal{C}_{F^*}$ *is as in Table 5.1.*

Table 5.1: The weight distribution of $\mathcal{C}_{F^*}$ over $B_+(F)$ when n is even.

Hamming weight a	Multiplicity E_a
0	1
$(p-1)p^{r-1}$	$p^r - 1 + (p-1)(p^r - p^{2r-n})$
$(p-1)(p^{r-1} - p^{\frac{n}{2}-1})$	$(p-1)(p^{r-\frac{n}{2}} + p^{2r-1-n} - p^{r-\frac{n}{2}-1})$
$(p-1)(p^{r-1} - p^{\frac{n}{2}-1}) + p^{\frac{n}{2}}$	$(p-1)^2(p^{2r-1-n} - p^{r-\frac{n}{2}-1})$

Proof. $B_+(F)$ being an r-dimensional $\mathbb{F}_p$-vector space implies that $W^+(F)$ is an $r-m-s$ dimensional subspace of $\mathbb{F}_p^s$.

(i) $wt(c_{\alpha,\beta}) = (p-1)p^{r-1}$ i.e., $\alpha = 0$ and $\beta \notin \big(B_+(F)\big)^\perp$ or $\alpha \neq 0$ and $\alpha^{-1}\beta \in B_-(F^*)$.

Since $\#\big(B_+(F)\big)^\perp = p^{n-r}$, then $\#\{(0,\beta) : \beta \notin \big(B_+(F)\big)^\perp\} = p^n - p^{n-r}$. By Equation (53), we have $B_+(F^*) = \mathbb{F}_p^m \times \mathbb{F}_p^s \times W^+(F)$ and so it is an r- dimensional vector space. Therefore, $\alpha^{-1}\beta \in B_-(F^*)$ implies that $\beta \in B_-(F^*)$. Hence, $\#\{(\alpha,\beta) : \alpha \in \mathbb{F}_p^\star,\ \beta \in \big(B_-(F^*)\big)\} = (p-1)(p^n - p^r)$. Therefore, we have $\#\{(\alpha,\beta) : (\alpha,\beta) \in \mathbb{F}_p \times \mathbb{F}_p^n | wt(c_{\alpha,\beta}) = (p-1)p^{r-1}\} = p^n - p^{n-r} + (p-1)(p^n - p^r)$. Since $\mathrm{Ker}\,(\theta)$ has size p^{n-r}, dividing the quantity $p^n - p^{n-r} + (p-1)(p^n - p^r)$ by p^{n-r}, we obtain $E_a = p^r - 1 + (p-1)(p^r - p^{2r-n})$ for $a = (p-1)p^{r-1}$.

(ii) $wt(c_{\alpha,\beta}) = (p-1)(p^{r-1} - p^{\frac{n}{2}-1})$ i.e., $\alpha \neq 0$ and $\alpha^{-1}\beta \in B_+(F^*)$, and $F(\alpha^{-1}\beta) = 0$.

Since $B_+(F^*) = \mathbb{F}_p^m \times \mathbb{F}_p^s \times W^+(F)$, by similar arguments above $\alpha^{-1}\beta \in B_+(F^*)$ implies that $\beta \in B_+(F^*)$. For any $\alpha \in \mathbb{F}_p^\star$, the map from $B_+(F^*)$ to itself defined by $x \to \alpha^{-1}x$ is one-to-one. Hence, for any $\alpha \in \mathbb{F}_p^\star$, we have $\#\{\beta : \beta \in B_+(F^*) | F(\alpha^{-1}\beta) = 0\} = \#\{\beta : \beta \in B_+(F^*) | F(\beta) = 0\}$. Remember that $F^{**} = F$ and observe that $\mathbf{0} \in B_+(F)$. Then by Proposition 5.2.1, we have $S_0(F^*, \mathbf{0}) = \sum_{u \in \mathbb{F}_p} c_{F^*}(\mathbf{0}, u)\epsilon_p^u = \sum_{\alpha \in B_+(F^*)} \epsilon_p^{F(\alpha)} = p^{\frac{n}{2}}$. Then $c_{F^*}(\mathbf{0},0) - p^{\frac{n}{2}} + \sum_{u=1}^{p-1} c_{F^*}(\mathbf{0},u)\epsilon_p^u = 0$. Since the set $\{\epsilon_p^i : 1 \leq i \leq p-1\}$ is an integral basis of $\mathcal{O}_{\mathbb{Q}(\epsilon_p)}$, there exists a unique integer k such that $c_{F^*}(\mathbf{0},0) = k + p^{\frac{n}{2}}$ and $c_{F^*}(\mathbf{0},u) = k$ for all $u \neq 0 \in \mathbb{F}_p$.

On the other hand, we have $\sum_{u=0}^{p-1} c_{F^*}(\mathbf{0}, u) = p^r$. Therefore, $k = p^{r-1} - p^{\frac{n}{2}-1}$ and $c_{F^*}(\mathbf{0}, 0) = p^{r-1} - p^{\frac{n}{2}-1} + p^{\frac{n}{2}}$. Hence, we have $\#\{(\alpha, \beta) : (\alpha, \beta) \in \mathbb{F}_p \times \mathbb{F}_p^n | wt(c_{\alpha,\beta}) = (p-1)(p^{r-1} - p^{\frac{n}{2}-1})\} = (p-1)(p^{r-1} - p^{\frac{n}{2}-1} + p^{\frac{n}{2}})$. Dividing the quantity $(p-1)(p^{r-1} - p^{\frac{n}{2}-1} + p^{\frac{n}{2}})$ by p^{n-r}, we obtain $E_a = (p-1)(p^{2r-1-n} - p^{r-\frac{n}{2}-1} + p^{r-\frac{n}{2}})$ for $a = (p-1)(p^{r-1} - p^{\frac{n}{2}-1})$.

(iii) $wt(c_{\alpha,\beta}) = (p-1)(p^{r-1} - p^{\frac{n}{2}-1}) + p^{\frac{n}{2}}$ i.e., $\alpha \neq 0$ and $\alpha^{-1}\beta \in B_+(F^*)$, and $F(\alpha^{-1}\beta) \neq 0$.

From part (ii), we have $c_{F^*}(\mathbf{0}, u) = k$ for all $u \neq 0 \in \mathbb{F}_p$ and $k = p^{r-1} - p^{\frac{n}{2}-1}$. Therefore, we have $E_a = (p-1)^2(p^{2r-1-n} - p^{r-\frac{n}{2}-1})$ for $a = (p-1)(p^{r-1} - p^{\frac{n}{2}-1}) + p^{\frac{n}{2}}$. □

Lemma 5.3.1 *Let n be odd, and $f : \mathbb{F}_p^n \to \mathbb{F}_p$ be a non-weakly regular bent function such that f^* is bent. Put $f(\alpha^{-1}\beta) = u_0$. Then there exists an integer k depending on f such that*

- *$p \equiv 1$ (mod 4) and $f^*(x) + (\alpha^{-1}\beta).x$ is of type $(-)$ or $p \equiv 3$ (mod 4) and $f^*(x) + (\alpha^{-1}\beta).x$ is of type $(+)$:*

$$c_f(\alpha^{-1}\beta, u) = \begin{cases} \frac{p^{n-1}+k}{2} & \text{if } u = u_0; \\ \frac{p^{n-1}+k}{2} & \text{if } u \neq u_0. \end{cases}$$

- *$p \equiv 1$ (mod 4) and $f^*(x) + (\alpha^{-1}\beta).x$ is of type $(+)$:*

$$c_f(\alpha^{-1}\beta, u) = \begin{cases} \frac{p^{n-1}+k}{2} & \text{if } u = u_0; \\ \frac{p^{n-1}+k+2\left(\frac{u-u_0}{p}\right)p^{\frac{n-1}{2}}}{2} & \text{if } u \neq u_0. \end{cases}$$

- *$p \equiv 3$ (mod 4) and $f^*(x) + (\alpha^{-1}\beta).x$ is of type $(-)$:*

$$c_f(\alpha^{-1}\beta, u) = \begin{cases} \frac{p^{n-1}+k}{2} & \text{if } u = u_0; \\ \frac{p^{n-1}+k-2\left(\frac{u-u_0}{p}\right)p^{\frac{n-1}{2}}}{2} & \text{if } u \neq u_0. \end{cases}$$

Proof.

The proof follows from Lemma 2.2.4. □

Remark 5.3.2 *For all $\beta \in \mathbb{F}_p^n$, we have $\#B_+(f) = \sum_{u=0}^{p-1} c_f(\beta, u)$. On the other hand, we have $\#B_+(f) = p^r$. Hence, by Lemma 5.3.1, we have*

$$p^r = \frac{p^n + pk}{2},$$

which implies that $k = 2p^{r-1} - p^{n-1}$.

Case 10 *n is odd.*

- $\alpha = 0$

  We have $wt(c_{0,\beta}) = wt((\beta.\zeta_1, \beta.\zeta_2, \ldots, \beta.\zeta_{p^r-1})$ for all $\beta \in \mathbb{F}_p^n$. If $\beta \in \big(B_+(f)\big)^\perp$, then we have $wt(c_{0,\beta}) = 0$. If $\beta \notin \big(B_+(f)\big)^\perp$, then $wt(c_{0,\beta}) = (p-1)p^{r-1}$ by balancedness.

- $\alpha \neq 0$

  If $p \equiv 1$ (mod 4) and $f^*(x) + (\alpha^{-1}\beta).x$ is of type $(-)$ or $p \equiv 3$ (mod 4) and $f^*(x) + (\alpha^{-1}\beta).x$ is of type $(+)$, then by Lemma 5.3.1 and Remark 5.3.2, we have

  $$wt(c_{1,\alpha^{-1}\beta}) = \sum_{u=1}^{p-1} c_f(\alpha^{-1}\beta, u) = (p-1)\frac{p^{n-1}+k}{2} = (p-1)p^{r-1}.$$

  If $p \equiv 1$ (mod 4) and $f^*(x) + (\alpha^{-1}\beta).x$ is of type $(+)$, and $f(\alpha^{-1}\beta) = 0$, then by Lemma 5.3.1 and Remark 5.3.2, we have

  $$\begin{aligned} wt(c_{1,\alpha^{-1}\beta}) &= \textstyle\sum_{u=1}^{p-1} c_f(\alpha^{-1}\beta, u) \\ &= \textstyle\sum_{u=1}^{p-1} \frac{p^{n-1}+k+2\left(\frac{u}{p}\right)p^{\frac{n-1}{2}}}{2} \\ &= (p-1)\tfrac{p^{n-1}+k}{2} = (p-1)p^{r-1}. \end{aligned}$$

  If $p \equiv 1$ (mod 4) and $f^*(x) + (\alpha^{-1}\beta).x$ is of type $(+)$, and $f(\alpha^{-1}\beta) = u_0$, where u_0 is a square in $\mathbb{F}_p^\star$. Then by Lemma 5.3.1 and Remark 5.3.2, we have

  $$\begin{aligned} wt(c_{1,\alpha^{-1}\beta}) &= \textstyle\sum_{u \neq -u_0} c_f(\alpha^{-1}\beta, u) \\ &= \tfrac{p^{n-1}+k}{2} + \tfrac{p-1}{2}\tfrac{p^{n-1}+k-2p^{\frac{n-1}{2}}}{2} + \tfrac{p-3}{2}\tfrac{p^{n-1}+k+2p^{\frac{n-1}{2}}}{2} \\ &= (p-1)\tfrac{p^{n-1}+k}{2} - p^{\frac{n-1}{2}} \\ &= (p-1)p^{r-1} - p^{\frac{n-1}{2}}. \end{aligned}$$

If $p \equiv 1$ (mod 4) and $f^*(x) + (\alpha^{-1}\beta).x$ is of type (+), and $f(\alpha^{-1}\beta) = u_0$, where u_0 is a non-square in $\mathbb{F}_p^\star$. Then by Lemma 5.3.1 and Remark 5.3.2, we have

$$\begin{aligned} wt(c_{1,\alpha^{-1}\beta}) &= \textstyle\sum_{u\neq -u_0} c_f(\alpha^{-1}\beta, u) \\ &= \frac{p^{n-1}+k}{2} + \frac{p-3}{2}\frac{p^{n-1}+k-2p^{\frac{n-1}{2}}}{2} + \frac{p-1}{2}\frac{p^{n-1}+k+2p^{\frac{n-1}{2}}}{2} \\ &= (p-1)\frac{p^{n-1}+k}{2} + p^{\frac{n-1}{2}} \\ &= (p-1)p^{r-1} + p^{\frac{n-1}{2}}. \end{aligned}$$

If $p \equiv 3$ (mod 4) and $f^*(x) + (\alpha^{-1}\beta).x$ is of type (−), and $f(\alpha^{-1}\beta) = 0$, then by Lemma 5.3.1 and Remark 5.3.2, we have

$$\begin{aligned} wt(c_{1,\alpha^{-1}\beta}) &= \textstyle\sum_{u=1}^{p-1} c_f(\alpha^{-1}\beta, u) \\ &= \textstyle\sum_{u=1}^{p-1} \frac{p^{n-1}+k-2\left(\frac{u}{p}\right)p^{\frac{n-1}{2}}}{2} \\ &= (p-1)\frac{p^{n-1}+k}{2} = (p-1)p^{r-1}. \end{aligned}$$

If $p \equiv 3$ (mod 4) and $f^*(x) + (\alpha^{-1}\beta).x$ is of type (−), and $f(\alpha^{-1}\beta) = u_0$, where u_0 is a square in $\mathbb{F}_p^\star$. Then by Lemma 5.3.1 and Remark 5.3.2, we have

$$\begin{aligned} wt(c_{1,\alpha^{-1}\beta}) &= \textstyle\sum_{u\neq -u_0} c_f(\alpha^{-1}\beta, u) \\ &= \frac{p^{n-1}+k}{2} + \frac{p-3}{2}\frac{p^{n-1}+k+2p^{\frac{n-1}{2}}}{2} + \frac{p-1}{2}\frac{p^{n-1}+k-2p^{\frac{n-1}{2}}}{2} \\ &= (p-1)\frac{p^{n-1}+k}{2} - p^{\frac{n-1}{2}} \\ &= (p-1)p^{r-1} - p^{\frac{n-1}{2}}. \end{aligned}$$

If $p \equiv 3$ (mod 4) and $f^*(x) + (\alpha^{-1}\beta).x$ is of type (−), and $f(\alpha^{-1}\beta) = u_0$, where u_0 is a non-square in $\mathbb{F}_p^\star$. Then by Lemma 5.3.1 and Remark 5.3.2, we have

$$\begin{aligned} wt(c_{1,\alpha^{-1}\beta}) &= \textstyle\sum_{u\neq -u_0} c_f(\alpha^{-1}\beta, u) \\ &= \frac{p^{n-1}+k}{2} + \frac{p-1}{2}\frac{p^{n-1}+k+2p^{\frac{n-1}{2}}}{2} + \frac{p-3}{2}\frac{p^{n-1}+k-2p^{\frac{n-1}{2}}}{2} \\ &= (p-1)\frac{p^{n-1}+k}{2} + p^{\frac{n-1}{2}} \\ &= (p-1)p^{r-1} + p^{\frac{n-1}{2}}. \end{aligned}$$

As a result of Case 10, we conclude the odd case with the following theorem.

Theorem 5.3.2 *Let n be an odd integer, and $f : \mathbb{F}_p^n \to \mathbb{F}_p$ be a non-weakly regular bent function such that $f(\mathbf{0}) = 0$, $f(x) = f(-x)$ and f^* is bent. Let $B_+(f)$ be an*

r-dimensional $\mathbb{F}_p$-vector space with $r \geq \frac{n+1}{2}$. Then, the codewords $c_{\alpha,\beta}$ of the linear code $\mathcal{C}_{f^*}$ defined by Equation (54) has zero-weight if $\alpha = 0$ and $\beta \in \big(B_+(f)\big)^{\perp}$. If $p \equiv 1 \pmod 4$, then the non-zero weight codewords are as follows.

$$wt(c_{\alpha,\beta}) =$$
$$\begin{cases} (p-1)p^{r-1} & \text{if } \alpha = 0 \text{ and } \beta \notin \big(B_+(f)\big)^{\perp} \text{ or } \alpha \neq 0 \text{ and } \alpha^{-1}\beta \in B_-(f^*) \text{ or } \alpha^{-1}\beta \in B_+(f^*) \text{ and } f(\alpha^{-1}\beta) = 0; \\ (p-1)(p^{r-1}) + p^{\frac{n-1}{2}} & \text{if } \alpha \neq 0 \text{ and } \alpha^{-1}\beta \in B_+(f^*) \text{ and } f(\alpha^{-1}\beta) = u_0 \text{ where } u_0 \text{ is a non-square in } \mathbb{F}_p^{\star}; \\ (p-1)(p^{r-1}) - p^{\frac{n-1}{2}} & \text{if } \alpha \neq 0 \text{ and } \alpha^{-1}\beta \in B_+(f^*) \text{ and } f(\alpha^{-1}\beta) = u_0 \text{ where } u_0 \text{ is a square in } \mathbb{F}_p^{\star}. \end{cases}$$

If $p \equiv 3 \pmod 4$, then the non-zero weight codewords are as follows.

$$wt(c_{\alpha,\beta}) =$$
$$\begin{cases} (p-1)p^{r-1} & \text{if } \alpha = 0 \text{ and } \beta \notin \big(B_+(f)\big)^{\perp} \text{ or } \alpha \neq 0, \text{and } \alpha^{-1}\beta \in B_+(f^*), \text{ or } \alpha^{-1}\beta \in B_-(f^*) \text{ and } f(\alpha^{-1}\beta) = 0; \\ (p-1)(p^{r-1}) + p^{\frac{n-1}{2}} & \text{if } \alpha \neq 0 \text{ and } \alpha^{-1}\beta \in B_-(f^*) \text{ and } f(\alpha^{-1}\beta) = u_0 \text{ where } u_0 \text{ is a non-square in } \mathbb{F}_p^{\star}; \\ (p-1)(p^{r-1}) - p^{\frac{n-1}{2}} & \text{if } \alpha \neq 0 \text{ and } \alpha^{-1}\beta \in B_-(f^*) \text{ and } f(\alpha^{-1}\beta) = u_0 \text{ where } u_0 \text{ is a square in } \mathbb{F}_p^{\star}. \end{cases}$$

Proposition 5.3.3 *Let $n = m + 2s$ and denote $\mathbb{F}_p^m \times \mathbb{F}_p^s \times \mathbb{F}_p^s$ by $\mathbb{F}_p^n$. Let $F : \mathbb{F}_p^n \to \mathbb{F}_p$ be a non-weakly regular bent function defined by Equation (45) such that $f^{(z)}$ is weakly regular bent for all $z \in \mathbb{F}_p^s$. Let F satisfies the conditions of Theorem 5.3.2. With the above notations, the weight distribution of $\mathcal{C}_{F^*}$ are as in Table 5.2.*

Table 5.2: The weight distribution of $\mathcal{C}_{F^*}$ over $B_+(F)$ when n is odd.

Hamming weight a	Multiplicity E_a
0	1
$(p-1)p^{r-1}$	$p^r - 1 + (p-1)(p^r - p^{2r-n} + p^{2r-1-n})$
$(p-1)p^{r-1} + p^{\frac{n-1}{2}}$	$\frac{(p-1)^2}{2}(p^{2r-1-n} - p^{r-\frac{n+1}{2}})$
$(p-1)p^{r-1} - p^{\frac{n-1}{2}}$	$\frac{(p-1)^2}{2}(p^{2r-1-n} + p^{r-\frac{n+1}{2}})$

Proof. $B_+(F)$ being an r-dimensional $\mathbb{F}_p$-vector space implies that $W^+(F)$ is an $r - m - s$ dimensional subspace of $\mathbb{F}_p^s$.

Case 11 $p \equiv 1 \pmod 4$

(i) $wt(c_{\alpha,\beta}) = (p-1)p^{r-1}$ *i.e.,* $\alpha = 0$ *and* $\beta \notin \big(B_+(F)\big)^\perp$ *or* $\alpha \neq 0$ *and* $\alpha^{-1}\beta \in B_-(F^*)$ *or* $\alpha^{-1}\beta \in B_+(F^*)$ *and* $f(\alpha^{-1}\beta) = 0$*. Since* $\#\big(B_+(F)\big)^\perp = p^{n-r}$*, then we have* $\#\{(0,\beta) : \beta \notin \big(B_+(F)\big)^\perp\} = p^n - p^{n-r}$*. By Equation (53), we have* $B_+(F^*) = \mathbb{F}_p^m \times \mathbb{F}_p^s \times W^+(F)$ *and so it is an* r*- dimensional vector space. Therefore,* $\alpha^{-1}\beta \in B_-(F^*)$ *implies that* $\beta \in B_-(F^*)$*. Hence,* $\#\{(\alpha,\beta) : \alpha \in \mathbb{F}_p^\star,\ \beta \in \big(B_-(F^*)\big)\} = (p-1)(p^n - p^r)$*. Similarly,* $\alpha^{-1}\beta \in B_+(F^*)$ *implies that* $\beta \in B_+(F^*)$*. By similar arguments as in the proof of Proposition 5.3.2, for any* $\alpha \in \mathbb{F}_p^\star$*, we have* $\#\{\beta : \beta \in B_+(F^*)|F(\alpha^{-1}\beta) = 0\} = \#\{\beta : \beta \in B_+(F^*)|F(\beta) = 0\}$*. By Proposition 5.2.2, we have* $F^*(\mathbf{0}) = 0$*. Since* $F^{**} = F$ *and* $\mathbf{0} \in B_+(F)$*, by Proposition 5.2.1, we have* $S_0(F^*, \mathbf{0}) = \sum_{u\in\mathbb{F}_p} c_{F^*}(\mathbf{0}, u)\epsilon_p^u = \sum_{\alpha\in B_+(F^*)} \epsilon_p^{F(\alpha)} = p^{\frac{n}{2}}$*. Then by Equation (51), we have* $\sum_{u\in\mathbb{F}_p} c_{F^*}(\mathbf{0}, u)\epsilon_p^u = p^{\frac{n-1}{2}} \sum_{i\in\mathbb{F}_p^\star} \left(\frac{i}{p}\right)\epsilon_p^i$*. Then* $\sum_{u\in\mathbb{F}_p^\star}(c_{F^*}(\mathbf{0}, u) - \left(\frac{u}{p}\right)p^{\frac{n-1}{2}})\epsilon_p^u + c_{F^*}(\mathbf{0}, 0) = 0$*. Using similar arguments as in the proof of Proposition 5.3.2, we get* $c_{F^*}(\mathbf{0}, 0) = p^{r-1}$*. Hence, we arrive at* $\#\{(\alpha,\beta) : (\alpha,\beta) \in \mathbb{F}_p^\star \times \mathbb{F}_p^n | wt(c_{\alpha,\beta}) = (p-1)p^{r-1}\} = p^n - p^{n-r} + (p-1)(p^n - p^r + p^{r-1})$*. Therefore, we have* $E_a = p^r - 1 + (p-1)(p^r - p^{2r-n} + p^{2r-n-1})$ *for* $a = (p-1)p^{r-1}$*.*

(ii) $wt(c_{\alpha,\beta}) = (p-1)(p^{r-1}) + p^{\frac{n-1}{2}}$ *i.e.,* $\alpha \neq 0$ *and* $\alpha^{-1}\beta \in B_+(F^*)$*, and* $F(\alpha^{-1}\beta) = u_0$*, where* u_0 *is a non-square in* $\mathbb{F}_p^\star$*. If* u_0 *is a non-square in* $\mathbb{F}_p^\star$*, from the equation* $\sum_{u\in\mathbb{F}_p^\star}(c_{F^*}(\mathbf{0}, u) - \left(\frac{u}{p}\right)p^{\frac{n-1}{2}})\epsilon_p^u + c_{F^*}(\mathbf{0}, 0) = 0$*, we obtain* $c_{F^*}(\mathbf{0}, u_0) = p^{r-1} - p^{\frac{n-1}{2}}$*. Moreover, there exist* $\frac{p-1}{2}$ *non-square elements in* $\mathbb{F}_p^\star$*. Hence, by previous arguments, we have* $\#\{(\alpha,\beta) : (\alpha,\beta) \in \mathbb{F}_p^\star \times \mathbb{F}_p^n | wt(c_{\alpha,\beta}) = (p-1)(p^{r-1}) + p^{\frac{n-1}{2}} = \frac{(p-1)^2}{2}(p^{r-1} - p^{\frac{n-1}{2}})$*. Therefore, we have* $E_a = \frac{(p-1)^2}{2}(p^{2r-n-1} - p^{r-\frac{n+1}{2}})$ *for* $a = (p-1)(p^{r-1}) + p^{\frac{n-1}{2}}$*.*

(iii) $wt(c_{\alpha,\beta}) = (p-1)(p^{r-1}) - p^{\frac{n-1}{2}}$ *i.e.* $\alpha \neq 0$ *and* $\alpha^{-1}\beta \in B_+(F^*)$*, and* $F(\alpha^{-1}\beta) = u_0$*, where* u_0 *is a square in* $\mathbb{F}_p^\star$*. If* u_0 *is a square in* $\mathbb{F}_p^\star$*, from the equation* $\sum_{u\in\mathbb{F}_p^\star}(c_{F^*}(0, u) - \left(\frac{u}{p}\right)p^{\frac{n-1}{2}})\epsilon_p^u + c_{F^*}(\mathbf{0}, 0) = 0$*, we obtain* $c_{F^*}(\mathbf{0}, u_0) = p^{r-1} + p^{\frac{n-1}{2}}$*. By similar arguments above, we have* $E_a = \frac{(p-1)^2}{2}(p^{2r-n-1} + p^{r-\frac{n+1}{2}})$ *for* $a = (p-1)(p^{r-1}) - p^{\frac{n-1}{2}}$*.*

Case 12 $p \equiv 3$ *(mod* 4*)*

(i) $wt(c_{\alpha,\beta}) = (p-1)p^{r-1}$ *i.e.,* $\alpha = 0$ *and* $\beta \notin \big(B_+(F)\big)^\perp$ *or* $\alpha \neq 0$ *and* $\alpha^{-1}\beta \in B_+(F^*)$ *or* $\alpha^{-1}\beta \in B_-(F^*)$ *and* $F(\alpha^{-1}\beta) = 0$*. Since* $\#\big(B_+(F)\big)^\perp = p^{n-r}$*,*

then we have $\#\{(0,\beta) : \beta \notin \big(B_+(F)\big)^\perp\} = p^n - p^{n-r}$. *By Equation (53), we have* $B_-(F^*) = \mathbb{F}_p^m \times \mathbb{F}_p^s \times W^+(F)$ *and so it is an* r*- dimensional vector space. Therefore,* $\alpha^{-1}\beta \in B_+(F^*)$ *implies that* $\beta \in B_+(F^*)$. *Hence,* $\#\{(\alpha,\beta) : \alpha \in \mathbb{F}_p^\star,\ \beta \in \big(B_+(F^*)\big)\} = (p-1)(p^n - p^r)$. *Similarly,* $\alpha^{-1}\beta \in B_-(F^*)$ *implies that* $\beta \in B_-(F^*)$. *By similar arguments above, for any* $\alpha \in \mathbb{F}_p^\star$, *we have* $\#\{\beta : \beta \in B_-(F^*)|F(\alpha^{-1}\beta) = 0\} = \#\{\beta : \beta \in B_-(F^*)|F(\beta) = 0\}$. *By Proposition 5.2.2, we have* $F^*(\mathbf{0}) = 0$. *Since* $F^{**} = F$ *and* $\mathbf{0} \in B_+(F)$, *by Proposition 5.2.1, we have* $S_1(F^*, \mathbf{0}) = \sum_{u\in\mathbb{F}_p} d_{F^*}(\mathbf{0}, u)\epsilon_p^u = \sum_{\alpha\in B_-(F^*)} \epsilon_p^{F(\alpha)} = ip^{\frac{n}{2}}$. *Then by Equation (51), we have* $\sum_{u\in\mathbb{F}_p} d_{F^*}(\mathbf{0}, u)\epsilon_p^u = p^{\frac{n-1}{2}} \sum_{j\in\mathbb{F}_p^\star} \left(\frac{j}{p}\right) \epsilon_p^j$ *and* $\sum_{u\in\mathbb{F}_p^\star}(d_{F^*}(\mathbf{0}, u) - \left(\frac{u}{p}\right) p^{\frac{n-1}{2}})\epsilon_p^u + d_{F^*}(\mathbf{0}, 0) = 0$. *Using previous arguments, we get* $d_{F^*}(\mathbf{0}, 0) = p^{r-1}$. *Hence, we obtain* $\#\{(\alpha,\beta) : (\alpha,\beta) \in \mathbb{F}_p^\star \times \mathbb{F}_p^n | wt(c_{\alpha,\beta}) = (p-1)p^{r-1}\} = p^n - p^{n-r} + (p-1)(p^n - p^r + p^{r-1})$. *Therefore, we have* $E_a = p^r - 1 + (p-1)(p^r - p^{2r-n} + p^{2r-n-1})$ *for* $a = (p-1)p^{r-1}$.

(ii) $wt(c_{\alpha,\beta}) = (p-1)(p^{r-1}) + p^{\frac{n-1}{2}}$ *i.e.,* $\alpha \neq 0$ *and* $\alpha^{-1}\beta \in B_-(F^*)$, *and* $F(\alpha^{-1}\beta) = u_0$, *where* u_0 *is a non-square in* $\mathbb{F}_p^\star$. *If* u_0 *is a non-square in* $\mathbb{F}_p^\star$, *from the equation* $\sum_{u\in\mathbb{F}_p^\star}(d_{F^*}(\mathbf{0}, u) - \left(\frac{u}{p}\right) p^{\frac{n-1}{2}})\epsilon_p^u + d_{F^*}(\mathbf{0}, 0) = 0$, *we have* $d_{F^*}(\mathbf{0}, u_0) = p^{r-1} - p^{\frac{n-1}{2}}$. *Moreover, there exist* $\frac{p-1}{2}$ *non-square elements in* $\mathbb{F}_p^\star$. *Hence, by previous arguments, we have* $\#\{(\alpha,\beta) : (\alpha,\beta) \in \mathbb{F}_p^\star \times \mathbb{F}_p^n | wt(c_{\alpha,\beta}) = (p-1)(p^{r-1}) + p^{\frac{n-1}{2}}\} = \frac{(p-1)^2}{2}(p^{r-1} - p^{\frac{n-1}{2}})$. *Therefore, we have* $E_a = \frac{(p-1)^2}{2}(p^{2r-n-1} - p^{r-\frac{n+1}{2}})$ *for* $a = (p-1)(p^{r-1}) + p^{\frac{n-1}{2}}$.

(iii) $wt(c_{\alpha,\beta}) = (p-1)(p^{r-1}) - p^{\frac{n-1}{2}}$ *i.e.,* $\alpha \neq 0$ *and* $\alpha^{-1}\beta \in B_-(F^*)$, *and* $F(\alpha^{-1}\beta) = u_0$, *where* u_0 *is a square in* $\mathbb{F}_p^\star$. *If* u_0 *is a square in* $\mathbb{F}_p^\star$, *from the equation* $\sum_{u\in\mathbb{F}_p^\star}(d_{F^*}(\mathbf{0}, u) - \left(\frac{u}{p}\right) p^{\frac{n-1}{2}})\epsilon_p^u + d_{F^*}(\mathbf{0}, 0) = 0$, *we obtain* $d_{F^*}(\mathbf{0}, u_0) = p^{r-1} + p^{\frac{n-1}{2}}$. *By similar arguments above, we have* $E_a = \frac{(p-1)^2}{2}(p^{2r-n-1} + p^{r-\frac{n+1}{2}})$ *for* $a = (p-1)(p^{r-1}) - p^{\frac{n-1}{2}}$.

□

Next, we verify Theorem 5.3.2 by MAGMA program for the following ternary non-weakly regular bent function (see,[42]).

Example 12 $f : \mathbb{F}_{3^3} \to \mathbb{F}_3$, $f(x) = Tr_3(x^{22} + x^8)$ *is non-weakly regular of Type (+).*

- $f(0) = 0$, $f(x) = f(-x)$ *and* $f^*(x) = -f(x)$ *is bent;*
- $B_+(f)$ *is a* 2*-dimenisonal subspace of* $\mathbb{F}_{3^3}$*;*
- *The set* $\mathcal{C}_{f^*}$ *is a two-weight ternary linear code with parameters* $[8, 3, 3]_3$*, weight enumerator* $1 + 4y^3 + 22y^6$ *and weight distribution* $(1, 4, 22)$.

Remark 5.3.3 *By Magma computation we observe that for any* $\alpha \neq 0$*, there is no* $\alpha^{-1}\beta \in B_-(f^*)$ *such that* $f(\alpha^{-1}\beta) = u_0$*, where* u_0 *is a non-square in* $\mathbb{F}_3^\star$*. Hence, the linear code in Example 12 is two-weight. Therefore, we can say that our construction gives at most three-weight linear codes.*

5.4 Three-Weight Linear Codes on $B_-(f)$

Let $f : \mathbb{F}_p^n \to \mathbb{F}_p$ be a non-weakly regular bent function such that $f(x) = f(-x)$, $f(\mathbf{0}) = 0$, and f^* is bent. Let $B_-(f)$ be an $\mathbb{F}_p$-vector space with $\dim(B_-(f)) \geq \lfloor \frac{n}{2} \rfloor + 1$. Put $\dim(B_-(f)) = r$. Then we also define a linear code $\mathcal{C}_{f^*}$ over $\mathbb{F}_p$ as:

$$\mathcal{C}_{f^*} = \{c_{\alpha,\beta} = (\alpha f^*(\zeta_1) + \beta.\zeta_1, \alpha f^*(\zeta_2) + \beta.\zeta_2, \ldots, \alpha f^*(\zeta_{p^r-1}) + \beta.\zeta_{p^r-1})) \ : \ \alpha \in \mathbb{F}_p, \beta \in \mathbb{F}_{p^n}\}, \tag{55}$$

where $\zeta_1, \ldots, \zeta_{p^r-1}$ are the elements of $B_-(f)^\star$ and $c_{\alpha,\beta}$ denotes a codeword of $\mathcal{C}_{f^*}$. The length of the linear code $\mathcal{C}_{f^*}$ is $p^r - 1$.

Proposition 5.4.1 *The linear code* $\mathcal{C}_{f^*}$ *of length* $p^r - 1$ *over* $\mathbb{F}_p$ *defined by (55) is a* k*-dimensional subspace of* $\mathbb{F}_p^n$*, where* $k = r + 1$ *and denoted by* $[p^r - 1, r + 1]_p$*.*

Proof. Similar to proof of Proposition 5.3.1. □

From now on we keep the above arguments and evaluate the weight of codewords in two cases. For $c_{\alpha,\beta} \in \mathcal{C}_{f^*}$, we have the following.

Case 13 n *is even.*

- $\alpha = 0$

  $wt(c_{0,\beta}) = wt((\beta.\zeta_1, \beta.\zeta_2, \ldots, \beta.\zeta_{p^r-1})$ *for all* $\beta \in \mathbb{F}_p^n$*. If* $\beta \in \big(B_-(f)\big)^\perp$*, then* $wt(c_{0,\beta}) = 0$*. If* $\beta \notin \big(B_-(f)\big)^\perp$*, then* $wt(c_{0,\beta}) = (p-1)p^{r-1}$ *by balancedness.*

- $\alpha \neq 0$

  $wt(c_{\alpha,\beta}) = wt((f^*(\zeta_1) + \beta.\zeta_1, f^*(\zeta_2) + \beta.\zeta_2, \ldots, f^*(\zeta_{p^r-1}) + \beta.\zeta_{p^r-1})$ *for all* $\beta \in \mathbb{F}_p^n$*, where* α^{-1} *is the multiplicative inverse of* $\alpha \in \mathbb{F}_p^\star$*. Then we have* $wt(c_{\alpha,\beta}) = wt(c_{1,\alpha^{-1}\beta})$.

  If $\alpha^{-1}\beta \in B_+(f^*)$*, by Proposition 5.2.1, we have*

  $$\sum_{u=0}^{p-1} d_f(\alpha^{-1}\beta, u)\epsilon_p^u = \sum_{\zeta \in B_-(f)} \epsilon_p^{f^*(\zeta)+\zeta.(\alpha^{-1}\beta)} = 0,$$

  which implies that $-d_f(\alpha^{-1}\beta, 0) = \sum_{u=1}^{p-1} d_f(\alpha^{-1}\beta, u)\epsilon_p^u$*. As the set* $\{\epsilon_p^i : 1 \leq i \leq p-1\}$ *is an inetgral basis of* $\mathcal{O}_{\mathbb{Q}(\epsilon_p)}$ *and* $\sum_{i=1}^{p-1} \epsilon_p^i = -1$*, we have* $d_f(\alpha^{-1}\beta, 0) = d_f(\alpha^{-1}\beta, u)$ *for all* $u \in \mathbb{F}_p^\star$*. Hence,* $f^*(\zeta) + \zeta.(\alpha^{-1}\beta)$ *is balanced over* $B_-(f)$*. Since* $f^*(\mathbf{0}) = 0$*, we have* $wt(c_{1,\alpha^{-1}\beta}) = (p-1)p^{r-1}$.

  If $\alpha^{-1}\beta \in B_-(f^*)$*, by Proposition 5.2.1, we have*

  $$-p^{\frac{n}{2}}\epsilon_p^{f(\alpha^{-1}\beta)} = \sum_{\zeta \in B_-(f)} \epsilon_p^{f^*(\zeta)+\zeta.(\alpha^{-1}\beta)}.$$

  For $f(\alpha^{-1}\beta) = 0$*, we have*

  $$\sum_{u=0}^{p-1} c_f(\alpha^{-1}\beta, u)\epsilon_p^u = -p^{\frac{n}{2}}.$$

  Then $d_f(\alpha^{-1}\beta, 0) + p^{\frac{n}{2}} + \sum_{u=1}^{p-1} d_f(\alpha^{-1}\beta, u)\epsilon_p^u = 0$*. Since the set* $\{\epsilon_p^i : 1 \leq i \leq p-1\}$ *is an inetgral basis of* $\mathcal{O}_{\mathbb{Q}(\epsilon_p)}$*, there exist an unique integer* a *such that* $d_f(\alpha^{-1}\beta, 0) = a - p^{\frac{n}{2}}$ *and* $d_f(\alpha^{-1}\beta, u) = a$ *for all* $u \neq 0 \in \mathbb{F}_p$*. On the other hand, we have* $\sum_{u=0}^{p-1} d_f(\alpha^{-1}\beta, u) = p^r$*. Therefore* $a = p^{r-1} + p^{\frac{n}{2}-1}$*, and* $wt(c_{1,\alpha^{-1}\beta}) = \sum_{u=1}^{p-1} d_f(\alpha^{-1}\beta, u) = (p-1)(p^{r-1} + p^{\frac{n}{2}-1})$.

  If $f(\alpha^{-1}\beta) \neq 0$*, by similar arguments above, we have*

  $$wt(c_{1,\alpha^{-1}\beta}) = (p-1)(p^{r-1} + p^{\frac{n}{2}-1}) - p^{\frac{n}{2}}.$$

As a result of Case 13 we conclude even case with the following theorem.

Theorem 5.4.1 *Let* n *be an even integer,* $f : \mathbb{F}_p^n \to \mathbb{F}_p$ *be a non-weakly regular bent function such that* $f(\mathbf{0}) = 0$*,* $f(x) = f(-x)$ *and* f^* *is bent. Let* $B_-(f)$ *be an* r*-dimensional* $\mathbb{F}_p$*-vector space with* $r \geq \frac{n}{2} + 1$*. Then the codewords* $c_{\alpha,\beta}$ *of the linear*

code $\mathcal{C}_{f^*}$ defined by Equation (55) has zero-weight if $\alpha = 0$ and $\beta \in \big(B_-(f) \cup \{0\}\big)^{\perp}$. The non-zero weight codewords are as follows.

$$wt(c_{\alpha,\beta}) = \begin{cases} (p-1)p^{r-1} & \text{if } \alpha = 0 \text{ and } \beta \notin \big(B_-(f)\big)^{\perp} \text{ or } \alpha \neq 0 \text{ and } \alpha^{-1}\beta \in B_+(f^*); \\ (p-1)(p^{r-1} + p^{\frac{n}{2}-1}) & \text{if } \alpha \neq 0 \text{ and } \alpha^{-1}\beta \in B_-(f^*) \text{ and } f(\alpha^{-1}\beta) = 0\,; \\ (p-1)(p^{r-1} + p^{\frac{n}{2}-1}) - p^{\frac{n}{2}} & \text{if } \alpha \neq 0 \text{ and } \alpha^{-1}\beta \in B_-(f^*) \text{ and } f(\alpha^{-1}\beta) \neq 0\,. \end{cases}$$

Proposition 5.4.2 *Let $n = m + 2s$ and denote $\mathbb{F}_p^m \times \mathbb{F}_p^s \times \mathbb{F}_p^s$ by $\mathbb{F}_p^n$. Let $F : \mathbb{F}_p^n \to \mathbb{F}_p$ be a non-weakly regular bent function defined by Equation (45)such that $f^{(z)}$ is weakly regular bent for all $z \in \mathbb{F}_p^s$. Let F satisfies the conditions of Theorem 5.4.1. With the above notations, the weight distribution of $\mathcal{C}_{F^*}$ are as in Table 5.3.*

Table 5.3: The weight distribution of $\mathcal{C}_{F^*}$ over $B_-(F)$ when n is even.

Hamming weight a	Multiplicity E_a
0	1
$(p-1)p^{r-1}$	$p^r - 1 + (p-1)(p^r - p^{2r-n})$
$(p-1)(p^{r-1} + p^{\frac{n}{2}-1})$	$(p-1)(-p^{r-\frac{n}{2}} + p^{2r-1-n} + p^{r-\frac{n}{2}-1})$
$(p-1)(p^{r-1} + p^{\frac{n}{2}-1}) - p^{\frac{n}{2}}$	$(p-1)^2(p^{2r-1-n} + p^{r-\frac{n}{2}-1})$

Proof. Similar to the proof of Proposition 5.3.2. □

Next, we verify Theorem 5.4.1 by MAGMA program for the following ternary non-weakly regular bent function (see,[25]).

Example 13 *$f : \mathbb{F}_{3^6} \to \mathbb{F}_3$, λ is a primitive element of $\mathbb{F}_{3^6}$ and $f(x) = Tr_6(\lambda x^{20} + \lambda^{41}x^{92})$ is non-weakly regular bent of Type $(-)$.*

- *$f(0) = 0$, $f(x) = f(-x)$ and $f^*(x)$ is bent;*
- *$B_-(f)$ is an 4-dimensional subspace of $\mathbb{F}_{3^6}$;*

- *The set $\mathcal{C}_{f^*}$ is a three weight ternary linear code with parameters $[80, 5, 45]_3$, weight enumerator $1+16y^{45}+224y^{54}+2y^{72}$ and weight distribution $(1, 16, 224, 2)$, which is verified by MAGMA.*

Lemma 5.4.1 *Let n be odd, and $f : \mathbb{F}_p^n \to \mathbb{F}_p$ be a non-weakly regular bent function such that its dual function f^* is also bent. Put $f(\alpha^{-1}\beta) = u_0$. Then there exists an integer k depending on f such that*

- *$p \equiv 1 \pmod 4$ and $f^*(x) + (\alpha^{-1}\beta).x$ is of type $(+)$ or $p \equiv 3 \pmod 4$ and $f^*(x) + (\alpha^{-1}\beta).x$ is of type $(-)$:*

$$d_f(\alpha^{-1}\beta, u) = \begin{cases} \frac{p^{n-1}-k}{2} & \text{if } u = u_0; \\ \frac{p^{n-1}-k}{2} & \text{if } u \neq u_0. \end{cases}$$

- *$p \equiv 1 \pmod 4$ and $f^*(x) + (\alpha^{-1}\beta).x$ is of type $(-)$:*

$$d_f(\alpha^{-1}\beta, u) = \begin{cases} \frac{p^{n-1}-k}{2} & \text{if } u = u_0; \\ \frac{p^{n-1}-k-2\left(\frac{u-u_0}{p}\right)p^{\frac{n-1}{2}}}{2} & \text{if } u \neq u_0. \end{cases}$$

- *$p \equiv 3 \pmod 4$ and $f^*(x) + (\alpha^{-1}\beta).x$ is of type $(+)$:*

$$d_f(\alpha^{-1}\beta, u) = \begin{cases} \frac{p^{n-1}-k}{2} & \text{if } u = u_0; \\ \frac{p^{n-1}-k+2\left(\frac{u-u_0}{p}\right)p^{\frac{n-1}{2}}}{2} & \text{if } u \neq u_0. \end{cases}$$

Proof.

The proof follows from [38, Lemma 3.4]. □

Remark 5.4.1 *Clearly for all $\beta \in \mathbb{F}_p^n$, we have $\#B_-(f) = \sum_{u=0}^{p-1} d_f(\beta, u)$. On the other hand, we have $\#B_-(f) = p^r$. Hence, by Lemma 5.4.1, we have*

$$p^r = \frac{p^n - pk}{2},$$

which implies that $k = p^{n-1} - 2p^{r-1}$.

Case 14 *n is odd*

- $\alpha = 0$

  We have $wt(c_{0,\beta}) = wt((\beta.\zeta_1, \beta.\zeta_2, \ldots, \beta.\zeta_{p^r-1})$ *for all* $\beta \in \mathbb{F}_p^n$. *If* $\beta \in \big(B_-(f)\big)^\perp$, *then* $wt(c_{0,\beta}) = 0$. *If* $\beta \notin \big(B_-(f)\big)^\perp$, *then* $wt(c_{0,\beta}) = (p-1)p^{r-1}$ *by balancedness.*

- $\alpha \neq 0$

  If $p \equiv 1$ *(mod* 4*) and* $\alpha^{-1}\beta \in B_+(f^*)$ *or* $p \equiv 3$ *(mod* 4*) and* $\alpha^{-1}\beta \in B_-(f^*)$, *then by Lemma 5.4.1 and Remark 5.4.1, we have*

$$wt(c_{1,\alpha^{-1}\beta}) = \sum_{u=1}^{p-1} d_f(\alpha^{-1}\beta, u) = (p-1)\frac{p^{n-1}-k}{2} = (p-1)p^{r-1}.$$

  If $p \equiv 1$ *(mod* 4*) and* $f^*(x) + (\alpha^{-1}\beta).x$ *is of type* $(-)$, *and* $f(\alpha^{-1}\beta) = 0$, *then by Lemma 5.4.1 and Remark 5.4.1, we have*

$$\begin{aligned} wt(c_{1,\alpha^{-1}\beta}) &= \textstyle\sum_{u=1}^{p-1} d_f(\alpha^{-1}\beta, u) \\ &= \textstyle\sum_{u=1}^{p-1} \frac{p^{n-1}-k-2\left(\frac{u}{p}\right)p^{\frac{n-1}{2}}}{2} \\ &= (p-1)\frac{p^{n-1}-k}{2} = (p-1)p^{r-1}. \end{aligned}$$

  If $p \equiv 1$ *(mod* 4*) and* $f^*(x) + (\alpha^{-1}\beta).x$ *is of type* $(-)$, *and* $f(\alpha^{-1}\beta) = u_0$, *where* u_0 *is a square in* $\mathbb{F}_p^\star$. *Then by Lemma 5.4.1 and Remark 5.4.1, we have*

$$\begin{aligned} wt(c_{1,\alpha^{-1}\beta}) &= \textstyle\sum_{u \neq -u_0} d_f(\alpha^{-1}\beta, u) \\ &= \frac{p^{n-1}-k}{2} + \frac{p-1}{2}\frac{p^{n-1}-k+2p^{\frac{n-1}{2}}}{2} + \frac{p-3}{2}\frac{p^{n-1}-k-2p^{\frac{n-1}{2}}}{2} \\ &= (p-1)\frac{p^{n-1}-k}{2} + p^{\frac{n-1}{2}} \\ &= (p-1)p^{r-1} + p^{\frac{n-1}{2}}. \end{aligned}$$

  If $p \equiv 1$ *(mod* 4*) and* $f^*(x) + (\alpha^{-1}\beta).x$ *is of type* $(-)$, *and* $f(\alpha^{-1}\beta) = u_0$, *where* u_0 *is a non-square in* $\mathbb{F}_p^\star$. *Then by Lemma 5.4.1 and Remark 5.4.1, we have*

$$\begin{aligned} wt(c_{1,\alpha^{-1}\beta}) &= \textstyle\sum_{u \neq -u_0} d_f(\alpha^{-1}\beta, u) \\ &= \frac{p^{n-1}-k}{2} + \frac{p-3}{2}\frac{p^{n-1}-k+2p^{\frac{n-1}{2}}}{2} + \frac{p-1}{2}\frac{p^{n-1}-k-2p^{\frac{n-1}{2}}}{2} \\ &= (p-1)\frac{p^{n-1}-k}{2} - p^{\frac{n-1}{2}} \\ &= (p-1)p^{r-1} - p^{\frac{n-1}{2}}. \end{aligned}$$

If $p \equiv 3$ (mod 4) and $f^*(x) + (\alpha^{-1}\beta).x$ is of type (+), and $f(\alpha^{-1}\beta) = 0$, then by Lemma 5.4.1 and Remark 5.4.1, we have

$$\begin{aligned} wt(c_{1,\alpha^{-1}\beta}) &= \sum_{u=1}^{p-1} d_f(\alpha^{-1}\beta, u) \\ &= \sum_{u=1}^{p-1} \frac{p^{n-1}-k+2\left(\frac{u}{p}\right)p^{\frac{n-1}{2}}}{2} \\ &= (p-1)\frac{p^{n-1}-k}{2} = (p-1)p^{r-1}. \end{aligned}$$

If $p \equiv 3$ (mod 4) and $f^*(x) + (\alpha^{-1}\beta).x$ is of type (+), and $f(\alpha^{-1}\beta) = u_0$, where u_0 is a square in $\mathbb{F}_p^\star$. Then by Lemma 5.4.1 and Remark 5.4.1, we have

$$\begin{aligned} wt(c_{1,\alpha^{-1}\beta}) &= \sum_{u\neq -u_0} d_f(\alpha^{-1}\beta, u) \\ &= \frac{p^{n-1}-k}{2} + \frac{p-3}{2}\frac{p^{n-1}-k-2p^{\frac{n-1}{2}}}{2} + \frac{p-1}{2}\frac{p^{n-1}-k+2p^{\frac{n-1}{2}}}{2} \\ &= (p-1)\frac{p^{n-1}-k}{2} + p^{\frac{n-1}{2}} \\ &= (p-1)p^{r-1} + p^{\frac{n-1}{2}}. \end{aligned}$$

If $p \equiv 3$ (mod 4) and $f^*(x) + (\alpha^{-1}\beta).x$ is of type (+), and $f(\alpha^{-1}\beta) = u_0$, where u_0 is a non-square in $\mathbb{F}_p^\star$. Then by Lemma 5.4.1 and Remark 5.4.1, we have

$$\begin{aligned} wt(c_{1,\alpha^{-1}\beta}) &= \sum_{u\neq -u_0} d_f(\alpha^{-1}\beta, u) \\ &= \frac{p^{n-1}-k}{2} + \frac{p-1}{2}\frac{p^{n-1}-k-2p^{\frac{n-1}{2}}}{2} + \frac{p-3}{2}\frac{p^{n-1}-k+2p^{\frac{n-1}{2}}}{2} \\ &= (p-1)\frac{p^{n-1}-k}{2} - p^{\frac{n-1}{2}} \\ &= (p-1)p^{r-1} - p^{\frac{n-1}{2}}. \end{aligned}$$

As a result of Case 14, we conclude the odd case with the following theorem.

Theorem 5.4.2 *Let n be an odd integer, and $f : \mathbb{F}_p^n \to \mathbb{F}_p$ be a non-weakly regular bent function such that $f(\mathbf{0}) = 0$, $f(x) = f(-x)$ and f^* is bent. Assume that $B_-(f)$ is an r-dimensional $\mathbb{F}_p$-vector space with $r \geq \frac{n+1}{2}$. Then the codewords $c_{\alpha,\beta}$ of the linear code $\mathcal{C}_{f^*}$ defined by equation (55) has zero-weight, if $\alpha = 0$ and $\beta \in \big(B_-(f)\big)^\perp$. If $p \equiv 1$ (mod 4), then the non-zero weight codewords are as follows*

$$wt(c_{\alpha,\beta}) = \begin{cases} (p-1)p^{r-1} & \text{if } \alpha = 0 \text{ and } \beta \notin \big(B_-(f)\big)^\perp \text{ or } \alpha \neq 0 \text{ and } \alpha^{-1}\beta \in B_+(f^*) \text{ or } \alpha^{-1}\beta \in B_-(f^*) \text{ and } f(\alpha^{-1}\beta) = 0; \\ (p-1)(p^{r-1}) - p^{\frac{n-1}{2}} & \text{if } \alpha \neq 0 \text{ and } \alpha^{-1}\beta \in B_-(f^*) \text{ and } f(\alpha^{-1}\beta) = u_0 \text{ where } u_0 \text{ is a non-square in } \mathbb{F}_p^\star; \\ (p-1)(p^{r-1}) + p^{\frac{n-1}{2}} & \text{if } \alpha \neq 0 \text{ and } \alpha^{-1}\beta \in B_+(f^*) \text{ and } f(\alpha^{-1}\beta) = u_0 \text{ where } u_0 \text{ is a square in } \mathbb{F}_p^\star. \end{cases}$$

If $p \equiv 3 \pmod 4$, then the non-zero weight codewords are as follows

$$wt(c_{\alpha,\beta}) =$$
$$\begin{cases} (p-1)p^{r-1} & \text{if } \alpha = 0 \text{ and } \beta \notin (B_-(f))^{\perp} \text{ or } \alpha \neq 0 \text{ and } \alpha^{-1}\beta \in B_-(f^*) \text{ or } \alpha^{-1}\beta \in B_+(f^*) \text{ and } f(\alpha^{-1}\beta) = 0; \\ (p-1)(p^{r-1}) - p^{\frac{n-1}{2}} & \text{if } \alpha \neq 0 \text{ and } \alpha^{-1}\beta \in B_+(f^*), \text{ and } f(\alpha^{-1}\beta) = u_0, \text{ where } u_0 \text{ is a non-square in } \mathbb{F}_p^\star; \\ (p-1)(p^{r-1}) + p^{\frac{n-1}{2}} & \text{if } \alpha \neq 0 \text{ and } \alpha^{-1}\beta \in B_+(f^*), \text{ and } f(\alpha^{-1}\beta) = u_0, \text{ where } u_0 \text{ is a square in } \mathbb{F}_p^\star. \end{cases}$$

Proposition 5.4.3 *Let $n = m + 2s$ and denote $\mathbb{F}_p^m \times \mathbb{F}_p^s \times \mathbb{F}_p^s$ by $\mathbb{F}_p^n$. Let $F : \mathbb{F}_p^n \to \mathbb{F}_p$ be a non-weakly regular bent function defined by Equation (45) such that $f^{(z)}$ is weakly regular bent for all $z \in \mathbb{F}_p^s$. Let F satisfies the conditions of Theorem 5.4.2. With the above notations, the weight distribution of $\mathcal{C}_{F^*}$ are as in Table 5.4.*

Table 5.4: The weight distribution of $\mathcal{C}_{F^*}$ over $B_-(F)$ when n is odd.

Hamming weight a	Multiplicity E_a
0	1
$(p-1)p^{r-1}$	$p^r - 1 + (p-1)(p^r - p^{2r-n} + p^{2r-1-n})$
$(p-1)p^{r-1} - p^{\frac{n-1}{2}}$	$\frac{(p-1)^2}{2}(p^{2r-1-n} + p^{r-\frac{n+1}{2}})$
$(p-1)p^{r-1} + p^{\frac{n-1}{2}}$	$\frac{(p-1)^2}{2}(p^{2r-1-n} - p^{r-\frac{n+1}{2}})$

Proof. Similar to the proof of Proposition 5.3.3. □

5.5 Minimality of Constructed Linear Codes

In this section, we look into the minimality of linear codes built in Section 5.3 and 5.4 from non-weakly regular bent functions.

The construction of linear codes all of whose non-zero codewords are minimal is of great significance when you consider that minimal linear codes generate secret sharing schemes with desirable access structures. Below, by Lemma 5.1.1, we show that all non-zero codewords of the built codes are minimal for nearly all cases.

We are now going to exhibit that the built linear p-ary code of Theorem 5.3.1 is minimal for nearly all cases.

Theorem 5.5.1 *Let $\mathcal{C}_{f^*}$ be the linear $[p^r-1, r+1, (p-1)(p^{r-1}-p^{\frac{n}{2}-1})]_p$ code of Theorem 5.3.1. Then all non-zero codewords of $\mathcal{C}_{f^*}$ are minimal for $r \geq \frac{n}{2}+2$.*

Proof. We have $a_{\min} = (p-1)(p^{r-1}-p^{\frac{n}{2}-1})$ and $a_{\max} = (p-1)(p^{r-1}-p^{\frac{n}{2}-1})+p^{\frac{n}{2}}$. Then the inequality

$$\frac{p-1}{p} < \frac{a_{\min}}{a_{\max}}$$

can be written as $p^{\frac{n}{2}+1} < (p-1)(p^{r-1}-p^{\frac{n}{2}-1}) + p^{\frac{n}{2}}$. For an odd prime p, this inequality is satisfied when $r \geq \frac{n}{2}+2$. Hence, the proof is done from Lemma 5.1.1.

□

The following theorem proves that the built linear p-ary code of Theorem 5.3.2 is minimal for nearly all cases.

Theorem 5.5.2 *Let $\mathcal{C}_{f^*}$ be the linear $[p^r-1, r+1, (p-1)(p^{r-1}) - p^{\frac{n-1}{2}}]_p$ code of Theorem 5.3.2. Then every non-zero codewords of $\mathcal{C}_{f^*}$ are minimal for $r \geq \frac{n+3}{2}$.*

Proof. We have that $a_{\min} = (p-1)(p^{r-1}) - p^{\frac{n-1}{2}}$ and $a_{\max} = (p-1)(p^{r-1}) + p^{\frac{n-1}{2}}$. Then the inequality given by (52) can be witten as $2p^{(n+1)/2} < (p-1)(p^{r-1}) + p^{\frac{n-1}{2}}$. For an odd prime p, this inequality is satisfied when $r \geq \frac{n+3}{2}$. Hence, the proof is done from Lemma 5.1.1.

□

The following theorem proves that the built linear p-ary code of Theorem 5.4.1 is minimal for nearly all cases.

Theorem 5.5.3 *Let $\mathcal{C}_{f^*}$ be the linear $[p^r-1, r+1, (p-1)(p^{r-1}+p^{\frac{n}{2}-1}) - p^{\frac{n}{2}}]_p$ code of Theorem 5.4.1. Then every non-zero codewords of $\mathcal{C}_{f^*}$ are minimal for $r \geq \frac{n}{2}+2$.*

Proof. We have $a_{\min} = (p-1)(p^{r-1}+p^{\frac{n}{2}-1}) - p^{\frac{n}{2}}$ and $a_{\max} = (p-1)(p^{r-1}+p^{\frac{n}{2}-1})$.

Then the inequality

$$\frac{p-1}{p} < \frac{a_{\min}}{a_{\max}}$$

can be written as $p^{\frac{n}{2}+1} < (p-1)(p^{r-1} + p^{\frac{n}{2}-1})$. For an odd prime p, this inequality is satisfied when $r \geq \frac{n}{2} + 2$. Hence, the proof is done from Lemma 5.1.1.

□

The following theorem proves that the built linear p-ary code of Theorem 5.4.2 is minimal for nearly all cases.

Theorem 5.5.4 *Let $\mathcal{C}_{f^*}$ be the linear $[p^r - 1, r+1, (p-1)(p^{r-1}) - p^{\frac{n-1}{2}}]_p$ code of Theorem 5.4.2. Then every non-zero codewords of $\mathcal{C}_{f^*}$ are minimal for $r \geq \frac{n+3}{2}$.*

Proof. We have that $a_{\min} = (p-1)(p^{r-1}) - p^{\frac{n-1}{2}}$ and $a_{\max} = (p-1)(p^{r-1}) + p^{\frac{n-1}{2}}$. Then the inequality given by (52) can be written as $2p^{(n+1)/2} < (p-1)(p^{r-1}) + p^{\frac{n-1}{2}}$. For an odd prime p, this inequality is satisfied when $r \geq \frac{n+3}{2}$. Hence, the proof is done from Lemma 5.1.1.

□

CHAPTER 6

CONCLUSION

The main objective of this thesis is to investigate the various properties of non-weakly regular bent functions and to relate them with certain combinatorial structures. It should be noted that the main techniques used in thesis are new. Also note that bent functions over finite fields of odd characteristic have been intensely studied in recent years. However, most of the known bent functions having relations with other structures are weakly regular. For the first time we show that non-weakly regular bent functions also have relations with other combinatorial structures such as partial difference sets, strongly regular graphs, association schemes and few weight linear codes. In this chapter, we briefly discuss the main results of the thesis emphasizing the profiles of the methods to build them.

It is known that weakly regular bent functions appear in pairs i.e. their dual functions are also weakly regular. On the other hand, the dual of a non-weakly regular bent function even may not be a bent function. To solve the open problem proposed by Çeşmelioğlu, Meidl and Pott, we partition the finite fields into two special subsets with respect to the sign of the Walsh transform of non-weakly regular bent functions. We use the value distributions of bent functions on these subsets to prove that if the dual function f^* of a non-weakly regular bent function f is bent then we have $f(x) = f^{**}(-x)$ which holds also for weakly regular bent functions. Moreover, we also would like to mention that our contribution [38], in which we also generalize our solution to plateaued functions.

One of the tools to construct partial difference sets are bent functions. The general idea is to use pre-image sets of bent functions. However, it doesnt work for non-weakly regular bent functions. Fortunately, the two special subsets which are obtained

by the partition of the finite fields with respect to the sign of the Walsh transform of non-weakly regular bent functions give rise to obtain partial difference sets in certain cases. At this point, we also would like to express that our contribution [37], in which we observe the relation between cyclotomic cosets and these special subsets, will give a different perspective to the researchers in this area.

The concept of association schemes is a very vast theme that has connections with numerous extraordinary areas of algebraic combinatorics, for example, coding theory, design theory, algebraic graph theory, finite group theory, and finite geometry. From graph theoretical point of view, association schemes can be seen as the generalization of strongly regular graphs. One of the tools to construct association schemes are bent functions. Similar to the partial difference sets and hence to the strongly regular graphs, most of the known methods in literature use pre-image sets of weakly regular bent functions. We generalize this approach by using pre-image sets of non-weakly regular ternary bent functions in a subclass of the *GMMF* class with respect to the associated special subsets. We leave reader to generalize this result to arbitrary characteristic as an open problem.

There are several approaches to build linear codes from bent functions over finite fields. The two of the known approches are kept apart from others in the literature which are called first and second conventional construction methods. Until now, the only bent functions which are used to build linear codes are weakly regular bent functions. In the present thesis, it is the first time that non-weakly regular bent functions over finite fields are used to build linear codes. It should be stated that we used a generic construction method, but the restricted domains $B_+(f)$ and $B_-(f)$ that we used are new. More precisely, we obtained the class of three-weight p-ary linear codes from non-weakly regular dual-bent functions and determined their weight distribution when corresponding non-weakly regular bent functions belong to a certain subclass of GMMF bent functions. We subsequently found that the developed codes are minimal for nearly all cases. The built codes are inequivalent to the recognised ones in the literature as a ways as we know.

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] E. Bannai. Subschemes of some association schemes. *J. Algebra*, 23(5):874–883, 1991.

[5] E. Bannai and T. Ito. *Algebraic combinatorics*. Benjamin/Cummings Menlo Park, 1984.

[6] R. C. Bose and D. M. Mesner. *Linear Associative Algebras Corresponding to Association Schemes of Partially Balanced Designs*. United States Air Force, Office of Scientific Research, 1958.

[7] R. C. Bose and T. Shimamoto. Classification and analysis of partially balanced incomplete block designs with two associate classes. *Journal of the American Statistical Association*, 47(258):151–184, 1952.

[8] W. Bridges and R. Mena. Rational g-matrices with rational eigenvalues. *Journal of Combinatorial Theory, Series A*, 32(2):264–280, 1982.

[9] A. Brouwer. Web database of strongly regular graphs. *http://www.win.tue.nl/ aeb/graphs/srg/srgtab.html (online)*.

[10] A. R. Calderbank and A. R. Goethals. Three-weight codes and association schemes. *Philips J. Res.*, 39:143–152, 1984.

[11] A. R. Calderbank and K. W. M. Kantor. The geometry of two-weight codes. *Bull. London Math. Soc.*, 18:97–122, 1986.

[12] 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.

[13] A. Çesmelioğlu, W. Meidl, and A. Pott. Generalized maiorana mcfarland class and normality of p-ary bent functions. *Finite Fields and Their Applications*, 24:105–117, 2013.

[14] A. Çesmelioğlu, W. Meidl, and A. Pott. On the dual of (non)-weakly regular bent functions and self-dual bent functions. *Adv. Math. Commun.*, 7(4):425–440, 2013.

[15] A. Çesmelioğlu, W. Meidl, and A. Pott. There are infinitely many bent functions for which the dual is not bent. *IEEE Transactions on Information Theory*, 62(9):5204–5208, 2016.

[16] Y. M. Chee, Y. Tan, and X. De Zhang. Strongly regular graphs constructed from p-ary bent functions. *Journal of Algebraic Combinatorics*, 34(2):251–266, 2011.

[17] 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.

[18] B. Courteau and J. Wolfmann. On triple-sum-sets and two or three weights codes. *Discrete Mathematics*, 50:179–191, 1984.

[19] P. Delsarte. *An Algebraic Approach to the Association Schemes of Coding Theory*. Philips journal of research / Supplement. N.V. Philips' Gloeilampenfabrieken, 1973.

[20] C. Ding and X. Wang. A coding theory construction of new systematic authentication codes. *Theoretical Comput. Sci.*, 330(1):81–99, 2005.

[21] K. Ding and C. Ding. Binary linear codes with three weights. *IEEE Communications Letters*, 18(11):1879–1882, 2014.

[22] 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.

[23] C. Godsil. *Algebraic Combinatorics*. CRC Press, 2017.

[24] 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.

[25] T. Helleseth and A. Kholosha. Crosscorrelation of m-sequences exponential sums bent functions and jacobsthal sums. *Cryptography and Communications*, 3(4):281–291, 2011.

[26] Z. Heng, C. Ding, and Z. Zhou. Minimal linear codes over finite fields. *Finite Fields and Their Applications*, 54:176 – 196, 2018.

[27] 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.

[28] T. Ikuta and A. Munemasa. Pseudocyclic association schemes and strongly regular graphs. *European J. Combin.*, 31:1513–1519, 2010.

[29] P. Kumar, R. A. Scholtz, and L. R. Welch. Generalized bent functions and their properties. *J. Combinatorial Theory Ser. A*, 40(1):90–107, 1985.

[30] R. Lidl and H. Niederreiter. *Finite fields*, volume 20. Cambridge university press, 1997.

[31] S. Ma. A survey of partial difference sets. *Des. Codes Crypt.*, 4(4):221–261, 1994.

[32] 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.

[33] S. Mesnager, F. Özbudak, and A. Sınak. Linear codes from weakly regular plateaued functions and their secret sharing schemes. *Des. Codes Cryptogr.*, 87(2-3):463–480, 2019.

[34] S. Mesnager and A. Sınak. Several classes of minimal linear codes with few weights from weakly regular plateaued functions. *IEEE Transactions on Information Theory*, 66(4):2296–2310, 2020.

[35] M. Muzychuk. V-rings of permutation groups with invariant metric. *Ph.D. Thesis, Kiev State University*, 1987.

[36] K. Nyberg. Constructions of bent functions and difference sets. In *Advances in Cryptology — EUROCRYPT 1990*, volume 473, pages 72–82. Springer, 1991.

[37] F. Özbudak and R. M. Pelen. Strongly regular graphs arising from non-weakly regular bent functions. *Cryptogr. Commun.*, 11:1297–1306, 2019.

[38] F. Özbudak and R. M. Pelen. Duals of non weakly regular bent functions are not weakly regular and generalization to plateaued functions. *Finite Fields and Their Applications*, 64, 2020.

[39] A. Pott, Y. Tan, T. Feng, and S. Ling. Association schemes arising from bent functions. *Designs, Codes and Cryptography*, 59(1-3):319–331, 2011.

[40] Q. X. T. Feng, K. Momihara. Constructions of strongly regular cayley graphs and skew hadamard difference sets from cyclotomic classes. *Combinatorica*, 35:413–434, 2015.

[41] Y. Tan, A. Pott, and T. Feng. Strongly regular graphs associated with ternary bent functions. *J. Combinatorial Theory Ser. A*, 117(6):668–682, 2010.

[42] 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*, pages 156–159, 2010.

[43] 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.

[44] J. Yuan and C. Ding. Secret sharing schemes from three classes of linear codes. *IEEE Transactions on Information Theory*, 52(1):206–212, 2006.

[45] Y. Zheng and X.-M. Zhang. Plateaued functions. In *ICICS*, volume 99, pages 284–300. Springer, 1999.

[46] 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: Pelen, Rumi Melih
Nationality: Turkish (TC)
Date and Place of Birth: 1984, Erzurum

EDUCATION

Degree	Institution	Year of Graduation
M.Sc.	Department of Mathematics, Koc University	2018
B.Sc.	Department of Mathematics, Izmir U. of Economics	2009

PROFESSIONAL EXPERIENCE

Year	Place	Enrollment
2018-Prs.	Middle Black Sea Development Agency	Specialist
2012-2018	Department of Mathematics, METU	Research Assist.
2012-2012	Department of Mathematics, Bahcesehir U.	Research Assist.
2009-2011	Department of Mathematics, Koc University	Teaching Assist.

PUBLICATIONS

International Journal Publications

- F. Özbudak, R.M.Pelen, Strongly regular graphs arising from non-weakly regular bent functions. Cryptogr. Commun.,11, pp. 1297–1306, 2019.

- F. Özbudak, R.M.Pelen, “Duals of non weakly regular bent functions are not weakly regular and generalization to plateaued functions”, Finite Fields and Their Applications, vol. 64, June 2020.

Preprints

- F. Özbudak, R.M.Pelen, Association Schemes of Classes 5 and 6 Arising From Ternary Non-Weakly Regular Bent Functions, preprint.
- F. Özbudak, R.M.Pelen, Three Weight Linear Codes From Non-Weakly Regular Bent Functions, preprint.