# ON OBTAINING REGULAR, WEAKLY REGULAR AND NON-WEAKLY REGULAR BENT FUNCTIONS OVER FINITE FIELDS AND RING OF INTEGERS MODULO $P^M$

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

BY

DİLEK ÇELİK

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

AUGUST 2014

Approval of the thesis:

**ON OBTAINING REGULAR, WEAKLY REGULAR AND NON-WEAKLY REGULAR BENT FUNCTIONS OVER FINITE FIELDS AND RING OF INTEGERS MODULO $P^M$**

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

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

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

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

**Examining Committee Members:**

Prof. Dr. Ferruh Özbudak
Mathematics, METU ______________

Assoc. Prof. Dr. Ali Doğanaksoy
Mathematics, METU ______________

Prof. Dr. Ali Aydın Selçuk
Computer Engineering, TOBB ETÜ ______________

Prof. Dr. İsmail Şuayip Güloğlu
Mathematics, Doğuş University ______________

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

**Date:** ______________

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

Name, Last Name: DİLEK ÇELİK

Signature :

# ABSTRACT

## ON OBTAINING REGULAR, WEAKLY REGULAR AND NON-WEAKLY REGULAR BENT FUNCTIONS OVER FINITE FIELDS AND RING OF INTEGERS MODULO $P^M$

Çelik, Dilek
Ph.D, Department of Cryptography
Supervisor : Prof. Dr. Ferruh Özbudak

August 2014, 47 pages

Bent functions over the finite fields of odd characteristics received a lot of attention of late years. However, the classification and construction of bent functions seems quite tough.

Over the finite fields with characteristic 2, a method is given to construct bent functions using near-bent functions [11]. This method is then generalized to finite fields with $p$ elements for an odd prime $p$ by Çeşmelioğlu et al. [3, 4]. The idea is constructing a bent function $F$ by 'glueing' the near-bent functions in such a way that Walsh spectrum of $F$ do not include zero value. This can be achieved by combining the near-bent functions having no common element in supports of their Walsh transforms and the union of their support of Walsh transforms should be equal to domain of near-bent functions.

In this thesis, we aim to construct regular, weakly regular and non-weakly regular bent functions. For this purpose, we first give an adaptation of the method given in [3], to the finite fields with $p^m$ elements and ring of integers modulo $p^m$, where $m$ is a positive integer greater than 1. Then, we generalize the method by using $s$-plateaued functions, for an integer $s > 1$, instead of using near-bent functions over ring of integers modulo $p^m$. It is notable to emphasize that, we obtain completely different results in every adaptation process.

To apply the method of construction, we compute the Walsh spectrum of quadratic functions over finite fields with $p^m$ elements and ring of integers modulo $p^m$. We evaulate the quadratic Gauss sum over $\mathbb{Z}_q$ to achieve the computation over the ring of integers. Also, we give a technique to classify the constructed bent functions as regular, weakly regular and non-weakly regular.

*Keywords* : Bent, Near-Bent, Plateaued Functions, Weakly Regular, Non-Weakly Regular, Finite Fields, Rings of Integers, Walsh Spectrum, Fourier Transform

# ÖZ

SONLU CİSİMLER VE SONLU TAM SAYI HALKALARI MODULO $P^M$
ÜZERİNDE DÜZENLİ, ZAYIFÇA DÜZENLİ VE ZAYIFÇA OLMAYAN
DÜZENLİ BÜKÜK FONKSİYONLARIN ÜRETİLMESİ ÜZERİNE

Çelik, Dilek
Doktora, Kriptoloji Bölümü
Tez Yöneticisi : Prof. Dr. Ferruh Özbudak

Ağustos 2014, 47 sayfa

Son yıllarda, karakteristiği tek olan sonlu cisimlerde tanımlı bükük fonksiyonlar üzerinde yapılan çalışmalar çok yaygınlaşmıştır. Fakat, bükük fonksiyonların üretimi ve sınıflandırılması oldukça zor gözükmektedir. Karakteristiği $2$ olan sonlu cisimler üzerinde yarı bükük fonksiyonlar kullanarak bükük fonksiyonlar üretme metodu ortaya çıkarılmıştır [11]. Daha sonra bu metot, $p$ tek bir asal sayı olmak üzere, $p$ elemanlı sonlu cisimler üzerinde çalışacak şekilde geliştirilmiştir [3]. Metodun anafikri, yarı bükük fonksiyonları, üretilecek olan $F$ bükük fonksiyonunun Walsh spektrumunda sıfır bulundurmayacak şekilde yapıştırmaktır. Bu amaca, yarı bükük fonksiyonların Walsh dönüşümlerinin desteklerinde (supportlarında) ortak eleman olmayacak ve Walsh dönüşümlerinin desteklerinin (supportlarının) birleşimi yarı bükük fonksiyonların tanım kümesi olacak şekilde seçilmesiyle ulaşılabilir.

Bu çalışmada, düzenli, zayıfça düzenli ve zayıfça olmayan düzenli bükük fonksiyonlar üretmeyi hedeflemekteyiz. Bu amaç için öncelikle [3, 4] makalelerinde verilen bazı çalışmaları $p^m$ elemanlı sonlu cisimler ve tam sayı halkaları modulo $p^m$ üzerine adapte ettik. Ayrıca, tam sayı halkaları modulo $p^m$ üzerinde, metodu yarı bükük fonksiyonlar yerine, $s > 1$ bir tam sayı olmak üzere, $s$-plato fonksiyonlar kullanarak çalışacak şekilde geliştirdik. Adaptasyon çalışmasının her aşamasında farklı sonuçlar elde ettiğimizi vurgulamak isteriz.

Bükük fonksiyon üretme methodunu ikinci dereceden fonksiyonlar kullanarak bir uygulama yapmak amacıyla, $p^m$ elemanlı sonlu cisimler ve tam sayı halkaları modulo $p^m$

üzerinde tanımlı ikinci dereceden fonksiyonların Walsh spektrumunu hesapladık. Tam sayı halkaları modulo $p^m$'deki uygulamayı yapabilmek için, bu kümede ikinci derece Gauss toplamını hesapladık. Ayrıca, ürettiğimiz bu bükük fonksiyonların, düzenli, zayıfça düzenli ve zayıfça olmayan düzenli bükük fonksiyonlar olarak sınıflandırılabilmesi için bir yöntem verdik.

*Anahtar Kelimeler*: Bükük Fonksiyon, Yarı Bükük Fonksiyon, Sonlu Halka, Sonlu Cisim, Zayıfça Düzenli, Zayıfça Olmayan Düzenli

*To My Parents and Vakkas*

# ACKNOWLEDGMENTS

I would like to express my very great appreciation to my thesis supervisor Prof. Dr. Ferruh Özbudak for his enthusiastic encouragement and valuable advices during the development and preparation of this thesis.

I would like to send my special thanks to my husband for his personal support and love. His willingness to encourage me all the time and his great patience has brightened my path.

I am greatful to all my family for their love, endless support, caring and helping they provided me through my entire life.

My sincere thanks also goes to all my friends and collegues for their close friendship and motivation which is very important for me through this period. They always bring joy and happiness to me.

It is a pleasure to thank TUBITAK UEKAE for giving me the opportunity to continue my education. It gives me great pleasure in acknowledging the support and help of my supervisors, Fatih Birinci, Hüseyin Demirci, Orhun Kara, İsa Sertkaya and İhsan Taşkın.

# TABLE OF CONTENTS

CHAPTERS

# CHAPTER 1

# INTRODUCTION

Boolean bent functions were first introduced by Rothaus in 1976 and played a significant role in design theory, coding theory and cryptography due to having the maximum Hamming distance to the set of all affine functions [15]. The general theory of the bent functions over an arbitrary finite field is developed by Kumar, Scholtz and Welch [10]. Ever since that time a lot of studies have been made and interesting results are obtained through studying, for example, monomial, binomial, and quadratic functions. One can study some of them [8], [7], [9], [3], [6], [12], [1].

In 2009, Leander and McGuire has given a method for construction of bent functions using near-bent functions over the finite fields with characteristic $2$ [11]. By this, they get the first examples of non-weakly regular bent functions in dimensions $10$ and $12$. The idea is constructing a bent function $F$ by 'glueing' the near-bent functions in such a way that Walsh spectrum of $F$ do not include zero value. This can be achieved by combining the near-bent functions which have no common element in supports of their Walsh transforms and the union of their support of Walsh transforms should be equal to the domain of near-bent functions.

The idea is later generalized to finite fields with odd characteristic by Çeşmelioğlu et al. [3]. For an odd prime $p$, they give a method that uses a determined number of near-bent functions defined from $\mathbb{F}_p^n$ to $\mathbb{F}_p$ to construct weakly regular and non-weakly regular bent functions. Moreover, they give numerical illustrations using quadratic near-bent functions. Afterwards, they develope the method in such a way that plateaued functions are used instead of near-bent functions for construction [4].

The fundamental aim of this thesis is to give a method to construct regular, weakly-regular and non-weakly regular bent functions over finite fields with $p^m$ elements and the ring of integers modulo $p^m$, for an odd prime $p$ and any integer $m > 1$.

For this purpose, we generalize some of the ideas that are given in [11], [3] and [4]. Using generalized near-bent functions from $\mathbb{F}_{p^m}^n$ to $\mathbb{F}_{p^m}$, we present a method to construct generalized bent functions by adding one more dimension. That is, using this method of construction, we get bent functions from $\mathbb{F}_{p^m}^n \times \mathbb{F}_{p^m}$ to $\mathbb{F}_{p^m}$.

To give concrete examples, we compute Walsh spectrum of all quadratic functions defined from $\mathbb{F}_{p^m}^n$ to $\mathbb{F}_{p^m}$ and apply the construction method on these functions. A process to decide whether the constructed bent function is regular, weakly regular or non-weakly regular is explained in detail.

Then, we adapt this study over ring of integers modulo $p^m$. This adaptation brings some difficulties due to the zero divisors, nonexistence of suitable Lagrange interpo-

lation coefficients and need of the computation of Gauss sums for the ring $\mathbb{Z}_{p^m}$. First, we introduce a method that constructs bent functions over $\mathbb{Z}_{p^m}$. Then, the Walsh spectrum of quadratic functions from $\mathbb{Z}_{p^m}^n$ to $\mathbb{Z}_{p^m}$ defined by $d_1x_1^2 + d_2x_2^2 + ... + d_{n-s}x_{n-s}^2$ is computed to give numerical examples for the construction where $d_i \in \mathbb{Z}_{p^m}^{\times}$ and $0 \leq s \leq n-1$. Using this computation, a simple method is given to obtain quadratic near-bent functions with pairwise disjoint support of Walsh transforms. Also, we evaluate the quadratic Gauss sum over $\mathbb{Z}_{p^m}$ for the computations. We apply the construction method on certain quadratic functions and obtain regular, weakly regular or non-weakly regular bent functions. We emphasize that different results than the results of the finite field case are obtained in every application process.
Lastly, we broaden this study over the ring of integers modulo $p^m$ by giving a method that uses $s$-plateaued functions instead of near-bent functions for a positive integer $s > 1$. Using this method, one can obtain bent functions by adding $s$ more dimensions. That is using $s$-plateaued functions from $\mathbb{Z}_{p^m}^n$ to $\mathbb{Z}_{p^m}$, we can construct bent functions defined from $\mathbb{Z}_{p^m}^n \times \mathbb{Z}_{p^m}^s$ to $\mathbb{Z}_{p^m}$. For illustrations, we use quadratic functions with a determined form, Walsh spectrum of which we compute. Also, we explain how to use these quadratic functions to obtain functions with disjoint support of Walsh transforms. Then, a technique to identify the constructed bent functions as regular, weakly regular and non-weakly regular is given.
The thesis is organized as follows. This first chapter is devoted to explain the purpose of the thesis, give the necessary definitions and notation regarding functions with special properties defined over finite fields with $p^m$ elements and the ring of integers modulo $p^m$. In Chapter 2, we give a method to construct bent functions using near-bent functions defined from $\mathbb{F}_{p^m}^n$ to $\mathbb{F}_{p^m}$. Then, we apply the method on quadratic functions and classify the constructed bent functions as regular, weakly regular or non-weakly regular. Chapter 3 generalizes the idea that is given in Chapter 2 to the ring of integers modulo $p^m$. In Chapter 4, we develop the method of construction that is given in Chapter 3. Instead of near-bent functions, we use $s$-plateaued functions to construct bent functions, for a positive integer $s > 1$. It is notable to emphasize that the dimension increases by $s$ for this case.

### 1.1 Functions Over Finite Fields With Special Properties

This section is devoted to give some necessary notation and definitions restricted to the scope of the thesis. Note that, the notation given in this section is valid for the whole thesis.
Let $p$ be a prime and $q = p^m$ for a positive integer $m$. Let $w_p = e^{\frac{2\pi\sqrt{-1}}{p}}$ be the complex primitive $p$-th root of unity. Consider the finite extension $\mathbb{F}_q$ of the finite field $\mathbb{F}_p$. This extension is of order $m$ and every element $a$ in $\mathbb{F}_q$, can be uniquely represented in the form,

$$a = c_1a_1 + c_2a_2 + \cdots + c_ma_m,$$

where $c_1, c_2, \cdots c_m \in \mathbb{F}_p$ and $\{a_1, a_2, \cdots, a_m\}$ is a basis of $\mathbb{F}_q$ over $\mathbb{F}_p$.

**Definition 1.1.** For $a \in \mathbb{F}_q$, the trace of $a$ over $\mathbb{F}_p$ is denoted and defined as $Tr(a) := a + a^q + \cdots + a^{q^{m-1}}$.

**Definition 1.2.** Let $\mathbb{F}_q^*$ denote the multiplicative group of $\mathbb{F}_q$ which consists of nonzero elements of $\mathbb{F}_q$. Let $t \in \mathbb{F}_q^*$ and $c \in \mathbb{F}_q^n$. Given a function $f(x) : \mathbb{F}_q^n \to \mathbb{F}_q$, Walsh transform (or Fourier transform) of $f$ is defined by,

$$\widehat{f}(t,c) = \sum_{x \in \mathbb{F}_q^n} w_p^{Tr(tf(x)+c \cdot x)},$$

where $w_p = e^{\frac{2\pi\sqrt{-1}}{p}}$ is the complex primitive $p$-th root of unity and $c \cdot x$ denotes the standard inner product of $c$ and $x$.

**Definition 1.3.** For a fixed $t \in \mathbb{F}_q^*$, the Walsh spectrum of $f$ is denoted and defined by $spec(f) := \left\{ \widehat{f}(t,c) : c \in \mathbb{F}_q^n \right\}$. Also, the support of $f$ is given by $supp(f) := \left\{ c \in \mathbb{F}_q^n : f(t,c) \neq 0 \right\}$.

The term *generalized bent functions* is used for various definitions. The natural generalization of bent functions that we use in this thesis is first proposed in 1985 by Kumar et al. [10].

**Definition 1.4.** For a fixed $t \in \mathbb{F}_q^*$, a function $f : \mathbb{F}_q^n \to \mathbb{F}_q$ is called a generalized bent function if $\left| \widehat{f}(t,c) \right| = q^{n/2}$, for all $c \in \mathbb{F}_q^n$.

**Definition 1.5.** For a fixed $t \in \mathbb{F}_q^*$, a function $f : \mathbb{F}_q^n \to \mathbb{F}_q$ is called a generalized near-bent function if $\left| \widehat{f}(t,c) \right| = q^{(n+1)/2}$ or 0, for all $c \in \mathbb{F}_q^n$.

A Boolean function is bent (respectively near-bent) if all Walsh coefficients are equal to $\mp 2^{n/2}$ (respectively $\mp 2^{(n+1)/2}$ or 0). Realize that, this coincides with the concept of bent and near-bent functions over finite fields with odd characteristic. However, there is an important difference which is Boolean bent (respectively near-bent) functions exist only if the number of variables, $n$, is even (respectively odd).

**Definition 1.6.** Let $f$ be a function defined from $\mathbb{F}_q^n$ to $\mathbb{F}_q$. For $t \in \mathbb{F}_q^*$, define $f^t$ from $\mathbb{F}_q^n$ to $\mathbb{F}_p$ as $f^t(x) = Tr(tf(x))$. Then, the Walsh transform of $f^t$ is $\widehat{f^t}(c) = \sum_{x \in \mathbb{F}_q^n} w_p^{f^t(x)+Tr(c \cdot x)}$.

Let $f^*$ be a function from $\mathbb{F}_q^n$ to $\mathbb{F}_p$. The normalized Fourier coefficients of a bent function, $f^t$, can be computed as follows [10, 5],

$$q^{-n/2}\widehat{f^t}(c) = \begin{cases} \mp w_p^{f^*(c)}, & \text{if } (n \text{ is even) or } (n \text{ is odd and } p \equiv 1 \pmod 4) \\ \mp\sqrt{-1}w_p^{f^*(c)}, & \text{if } n \text{ is odd and } p \equiv 3 \pmod 4). \end{cases}$$

**Definition 1.7.** Let $f^t$ be a bent function defined as in the Definition 1.6. Then,

- $f^t$ is called regular, if for every $c \in \mathbb{F}_q^n$, $q^{-n/2}\widehat{f^t}(c) = w_p^{f^*(c)}$.
- $f^t$ is called weakly regular, if there exists a complex $v$ which has unit magnitude such that $vq^{-n/2}\widehat{f^t}(c) = w_p^{f^*(c)}$ for all $c \in \mathbb{F}_q^n$.
- Otherwise, $f^t$ is called non-weakly regular.

## 1.2 Functions with Special Properties over $\mathbb{Z}_q$

In this section, we continue to give some necessary notation and definitions restricted to the scope of the thesis. In Chapter 3, we adapt the study over finite fields that we give in Chapter 2 to the ring of integers modulo $q$. So, the definitions and notation that are given for the finite field case in the previous section, will be customized.
The following notation is valid for whole thesis.

- $p$ is an odd prime and $q = p^m$ for some positive integer $m$.
- $\mathbb{Z}_q$: The ring of integers modulo $q$.
- $\mathbb{Z}_q^n$: The direct sum of $n$ copies of $\mathbb{Z}_q$.
- $\mathbb{Z}_q^\times$: The multiplicative group of $\mathbb{Z}_q$.
- $w$: The complex primitive $q$-th root of unity, that is $w = e^{\frac{2\pi\sqrt{-1}}{q}}$.

Note that, The multiplicative group $(\mathbb{Z}/r\mathbb{Z})^\times$ is cyclic if and only if $r$ is 1, 2, 4, $p^m$ or $2p^m$ ([14], pg. 83). Then, the multiplicative group of $\mathbb{Z}_q$ is a cyclic group of order $\phi(p^m) = p^m - p^{m-1}$.

**Definition 1.8.** Let $c \in \mathbb{Z}_q^n$. Given a function $f$ from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q$, the Walsh transform (or Fourier transform) of $f$ is denoted and defined by,

$$\widehat{f}(c) = \sum_{x \in \mathbb{Z}_q^n} w^{f(x) - c \cdot x},$$

where $c \cdot x$ denotes the standard inner product of $c$ and $x$.
Also, the Walsh spectrum of $f$ is $spec(f) := \left\{\widehat{f}(c) : c \in \mathbb{Z}_q^n\right\}$ and the support of $f$ is $supp(f) := \left\{c \in \mathbb{Z}_q^n : f(c) \neq 0\right\}$.

**Definition 1.9.** A function $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$ is called a bent function if $\left|\widehat{f}(c)\right| = q^{n/2}$, for all $c \in \mathbb{Z}_q^n$.

Realize that, this concept coincides with the concept of a generalized bent function given in Definition 1.4.

Consider a function $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$ with a Walsh spectrum such that $\left|\hat{f}(c)\right|^2 = Q$ or $0$ for all $c \in \mathbb{Z}_q^n$. As $\sum_{c\in\mathbb{Z}_q^n} \left|\hat{f}(c)\right|^2 = q^{2n}$ by Parseval's identity, $Q$ equals to $q^{n+s}$, for some integer $s$ with $0 \leq s \leq n$. These functions are called $s$-plateaued functions and the formal definitions are as follows.

**Definition 1.10.** Let $s$ be a positive integer. A function $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$ is called an $s$-plateaued function if $\left|\widehat{f}(c)\right| = q^{(n+s)/2}$ or $0$, for all $c \in \mathbb{Z}_q^n$.

**Definition 1.11.** A function $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$ is called a near-bent function if $\left|\widehat{f}(c)\right| = q^{(n+1)/2}$ or $0$, for all $c \in \mathbb{Z}_q^n$.

Note that, near-bent functions are $1$-plateaued functions, indeed.

Let $f$ be a bent function and $\tilde{f}$ be a function defined from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q$. Then, the normalized Fourier coefficients of $f$ can be computed as follows [10].

$$(q)^{-n/2}\widehat{f}(c) = \begin{cases} \mp w^{\tilde{f}(c)}, & \text{if } (n \text{ is even) or } (n \text{ is odd and } q \equiv 1 \text{ (mod 4)} \\ \mp\sqrt{-1}w^{\tilde{f}(c)}, & \text{if } n \text{ is odd and } q \equiv 3 \text{ (mod 4).} \end{cases}$$

**Definition 1.12.** Let $f$ be a bent function defined from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q$. Then,

- $f$ is called regular, if for every $c \in \mathbb{Z}_q^n$, $q^{-n/2}\widehat{f}(c) = w^{\tilde{f}(c)}$.
- $f$ is called weakly regular, if there exists a complex $v$ which has unit magnitude such that $vq^{-n/2}\widehat{f}(c) = w^{\tilde{f}(c)}$ for all $c \in \mathbb{Z}_q^n$.
- Otherwise, $f$ is called non-weakly regular.

# CHAPTER 2

# A CONSTRUCTION OF BENT FUNCTIONS OVER FINITE FIELDS

## 2.1 Introduction

As this chapter can be seen as a generalization of the techniques given in the Article [3] to $q$-ary case. We would like to give the following list of contributions.

- First, we emphasize that we study over finite fields with $p^m$ elements for an integer $m$ greater than $1$ instead of finite fields with $p$ elements.
- In [3], the authors compute the Walsh spectrum of quadratic functions defined from $\mathbb{F}_p^n$ to $\mathbb{F}_p$ in the form $d_1x_1^2 + d_2x_2^2 + ... + d_{n-s}x_{n-s}^2$ where $d_i \in \mathbb{F}_p^\times$ and $0 \leq s \leq n-1$.
  We compute Walsh spectrum of all quadratic functions defined from $\mathbb{F}_q^n$ to $\mathbb{F}_q$ and obtained a different result than the one in [3]. Moreover, we use a completely different technique for the computation.
- For the construction of bent functions, quadratic near-bent functions having pairwise disjoint support of Walsh transforms are needed. In [3], to show that a set of functions have pairwise disjoint support of Walsh transforms, the authors used the concept of linear structures. Instead of this, we used a simpler and shorter method to demonstrate it.
- We give a comprehensive method to classify the constructed bent function as regular, weakly regular or non-weakly regular.
- For a fixed $p$, more number of bent functions can be constructed compared to [3]. Besides, for a fixed $p$, the percentage of non-weakly regular bent functions are greater than the percentage of regular and weakly regular bent functions.

This chapter is organized as follows. Section 2.2 is devoted to give a method to construct bent functions over finite fields with $q$ elements. In Section 2.3, we determine the Walsh spectrum of $q$-ary quadratic functions. Then, we show how to obtain quadratic near-bent functions with pairwise disjoint support of Walsh transforms. In section 2.4, we give an application of the study over quadratic functions and so, construct bent functions. Then, we give a comprehensive explanation to classify these constructed bent functions as regular weakly regular and non-weakly regular.

## 2.2 A Construction of Bent Functions Using Near-Bent Functions over Finite Fields

Let $f_u : \mathbb{F}_q^n \to \mathbb{F}_q$, for $u \in \mathbb{F}_q$ be near-bent functions. Then, $\left|\widehat{f_u}(t,a)\right|^2 = q^{n+1}$ or $0$ for all $a \in \mathbb{F}_q^n$. The idea is combining these functions in such a way that, for a fixed $t \in \mathbb{F}_q^*$ the support of their Walsh transforms do not have a common element and the union of their support of Walsh transforms should be equal to domain of these near-bent functions. By this way, we construct a function $F : \mathbb{F}_q^n \times \mathbb{F}_q \to \mathbb{F}_q$ such that $\left|\widehat{F}\big(t,(a,b)\big)\right|^2 = q^{n+1}$, for all $(a,b) \in \mathbb{F}_q^n \times \mathbb{F}_q$, which implies that $F$ is bent.

**Lemma 2.1.** *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$. Then, for a fixed $t \in \mathbb{F}_q^*$,*

$$\sum_{c\in\mathbb{F}_q^n} \left|\widehat{f}(t,c)\right|^2 = \begin{cases} q^{2n}, & \textit{if } x = y \\ 0, & \textit{if } x \neq y. \end{cases}$$

*Proof.*

$$\begin{aligned}\sum_{c\in\mathbb{F}_q^n} \left|\widehat{f}(t,c)\right|^2 &= \sum_{c\in\mathbb{F}_q^n}\sum_{x,y\in\mathbb{F}_q^n} w_p^{Tr(tf(x)+c\cdot x-tf(y)-c\cdot y)} \\ &= \sum_{x,y\in\mathbb{F}_q^n} w_p^{Tr(t(f(x)-f(y)))} \sum_{c\in\mathbb{F}_q^n} w_p^{Tr(c\cdot(x-y))}.\end{aligned}$$

Realizing that,

$$\sum_{c\in\mathbb{F}_q^n} w_p^{Tr(c\cdot(x-y))} = \begin{cases} q^n, & \text{if } x = y \\ 0, & \text{if } x \neq y, \end{cases}$$

we get the result. By this lemma, a special case of Parseval's relation can be obtained for $q$-ary case.

□

**Theorem 2.2.** *For $u \in \mathbb{F}_q$, let $f_u : \mathbb{F}_q^n \to \mathbb{F}_q$ be near-bent functions such that $supp(\widehat{f_i}) \cap supp(\widehat{f_j})$ is empty for $i,j \in \mathbb{F}_q$. Let $\xi_i$ be elements of $\mathbb{F}_q$ for $i \in \{0,1,...,q-1\}$. Then, the function $F : \mathbb{F}_q^n \times \mathbb{F}_q \to \mathbb{F}_q$ defined by*

$$F(x,y) = (-1)\sum_{u\in\mathbb{F}_q} \frac{(y-\xi_0)(y-\xi_1)...(y-\xi_{q-1})}{(y-u)} f_u(x)$$

*is bent.*

*Proof.* Let $t \in \mathbb{F}_q^*$ be fixed. Using Lemma 2.1, we have

$$\sum_{c\in\mathbb{F}_q^n} \left|\widehat{f_u}(t,c)\right|^2 = \left|supp(\widehat{f_u})\right| q^{n+1} = q^{2n}.$$

Hence, $\left|supp(\widehat{f_u})\right| = q^{n-1}$. To complete the proof, we need to choose $f_u$ such that $\bigcup_{u\in\mathbb{F}_q} supp(\widehat{f_u}) = \mathbb{F}_q^n$. For the functions $f_u$ to satisfy this property, $q$-many near-bent functions are needed.

Let $(a,b) \in \mathbb{F}_q^n \times \mathbb{F}_q$. Then,

$$\widehat{F}\big(t,(a,b)\big) = \sum_{x\in\mathbb{F}_q^n, y\in\mathbb{F}_q} w_p^{Tr(tF(x,y)+a\cdot x+by)} = \sum_{y\in\mathbb{F}_q} w_p^{Tr(by)} \sum_{x\in\mathbb{F}_q^n} w_p^{Tr(tF(x,y)+a\cdot x)}$$

$$= \sum_{y\in\mathbb{F}_q} w_p^{Tr(by)} \sum_{x\in\mathbb{F}_q^n} w_p^{Tr\left(((-1)\prod_{\alpha\in F_q^*}\alpha)tf_y(x)+a\cdot x\right)}$$

$$= \sum_{y\in\mathbb{F}_q} w_p^{Tr(by)} \sum_{x\in\mathbb{F}_q^n} w_p^{Tr(tf_y(x)+a\cdot x)} = \sum_{y\in\mathbb{F}_q} w_p^{Tr(by)} \widehat{f_y}(t,a).$$

Each $a$ is an element of exactly one $supp(\widehat{f_y})$ because for $u,\ v \in \mathbb{F}_q$, $supp(\widehat{f_u}) \cap supp(\widehat{f_v})$ is empty and $\bigcup_{u\in\mathbb{F}_q} supp(\widehat{f_u}) = \mathbb{F}_q^n$. So, we have

$$\widehat{F}(t,(a,b)) = \sum_{y\in\mathbb{F}_q} w_p^{Tr(by)} \widehat{f_y}(t,a) = w_p^{Tr(by)} \widehat{f_y}(t,a),$$

which implies $\left|\widehat{F}(t,(a,b))\right| = \left|\widehat{f_y}(t,a)\right| = q^{\frac{n+1}{2}}$.

□

### 2.3 Computation of Walsh Spectrum of Quadratic Functions over $\mathbb{F}_q$

To construct bent functions using Theorem 2.2, we need near-bent functions with the desired properties. For this aim, we study on Walsh spectrum of quadratic functions. Every quadratic function $f : \mathbb{F}_q^n \to \mathbb{F}_q$ can be written as,

$$f(x_1, x_2, ..., x_n) = \sum_{i,j=1}^{n} a_{ij} x_i x_j,$$

with $a_{ij} = a_{ji}$. Without loss of generality, we can omit the affine part of $f$ because the absolute value of the Walsh transform of $f$ does not change when a constant value is added to it. Then, $f$ can be associated with a quadratic form as $XAX^T$ where $A$ is an $n \times n$ symmetric matrix with $(i, j)$th entry is $a_{ij}$, $X = [x_1 x_2 ... x_n]$ and $X^T$ is the transpose matrix of $X$.
One can transform a quadratic form by a linear substitution of indeterminates to find a simpler form. This linear substitution can be expressed by a matrix relation. If the square matrix used in this substitution is nonsingular, then we call this, nonsingular linear substitution. Two quadratic forms are said to be equivalent if one can be transformed to the other by means of a nonsingular linear substitution of indeterminates. Any quadratic form over $\mathbb{F}_q$ is equivalent to a diagonal quadratic form [13]. That is, for each quadratic form, there exists $d_1, d_2, ..., d_n \in \mathbb{F}_q$ such that $f(x_1, x_2, ..., x_n) = d_1x_1^2 + d_2x_2^2 + ... + d_nx_n^2$.
So, if we describe the Walsh spectrum of the quadratic form $f_{n,n-s}(x_1, x_2, ..., x_n) := d_1x_1^2+d_2x_2^2+...+d_{n-s}x_{n-s}^2$ for $s \in \{0, 1, ..., n-1\}$, we determine the Walsh spectrum of all quadratic functions.

**Theorem 2.3.** *Let $f_{n,n-s} : \mathbb{F}_{q^n} \to \mathbb{F}_q$ be defined by $f_{n,n-s}(x_1, x_2, ..., x_n) := d_1x_1^2 + d_2x_2^2 + ... + d_{n-s}x_{n-s}^2$ for $d_1, d_2, \cdots, d_{n-s} \in \mathbb{F}_q^*$. Let $D = \prod_{i=1}^{n-s} d_i$ and $s$ be an integer such that $0 \le s \le n-1$. Let $\eta$ denote the quadratic character of $\mathbb{F}_q$.*
*For $c_1, c_2, \cdots c_n \in \mathbb{F}_q$, let*

- $v = Tr(-(c_1^2)(4td_1)^{-1} - (c_2^2)(4td_2)^{-1} - \cdots - (c_{n-s}^2)(4td_{n-s})^{-1})$.
- $v' = Tr(-(c_1^2)(4td_1)^{-1} - (c_2^2)(4td_2)^{-1} - \cdots - (c_n^2)(4td_n)^{-1})$.

*The condition EQ is defined to describe the case when,*

$$Tr(c_n) = \cdots = Tr(c_{n-s+1}) = 0,$$

*and the condition NEQ is defined to describe the case when*

$$(Tr(c_n), Tr(c_{n-1}), \cdots, Tr(c_{n-s+1})) \neq (0, 0, \cdots, 0).$$

*For a fixed $t \in \mathbb{F}_q^*$ and $c \in \mathbb{F}_q^n$, we have the following results.*

1. *The Case $n-s$ is even and $s > 0$:*

$$\widehat{f_{n,n-s}}(t,c) = \begin{cases} \eta(t^{n-s}D)q^{\frac{n+s}{2}}w_p^v, & \textit{if } p \equiv 1 \pmod 4 \textit{ and EQ} \\ \sqrt{-1}^{(n-s)m}\eta(t^{n-s}D)q^{\frac{n+s}{2}}w_p^v, & \textit{if } p \equiv 3 \pmod 4 \textit{ and EQ} \\ 0, & \textit{if NEQ}. \end{cases}$$

2. *The Case $n-s$ is odd and $s > 0$:*

$$\widehat{f_{n,n-s}}(t,c) = \begin{cases} (-1)^{m-1}\eta(t^{n-s}D)q^{\frac{n+s}{2}}w_p^v, & \textit{if } p \equiv 1 \pmod 4 \textit{ and EQ} \\ (-1)^{m-1}\sqrt{-1}^{(n-s)m}\eta(t^{n-s}D)q^{\frac{n+s}{2}}w_p^v, & \textit{if } p \equiv 3 \pmod 4 \textit{ and EQ} \\ 0, & \textit{if NEQ}. \end{cases}$$

*3. The Case* $s = 0$*:*

$$\widehat{f_{n,n}}(t,c) = \begin{cases} \eta(t^nD)q^{\frac{n}{2}}w_p^{v'}, & \textit{if } n \textit{ even and } p \equiv 1 \pmod 4 \\ (-1)^{m-1}\eta(t^nD)q^{\frac{n}{2}}w_p^{v'}, & \textit{if } n \textit{ odd and } p \equiv 1 \pmod 4 \\ \sqrt{-1}^{nm}\eta(t^nD)q^{\frac{n}{2}}w_p^{v'}, & \textit{if } n \textit{ even and } p \equiv 3 \pmod 4 \\ (-1)^{m-1}\sqrt{-1}^{nm}\eta(t^nD)q^{\frac{n}{2}}w_p^{v'}, & \textit{if } n \textit{ odd and } p \equiv 3 \pmod 4. \end{cases}$$

*Proof.* Let $\psi$ be the canonical additive character of $\mathbb{F}_q$ and $G(\eta,\psi)$ be the associated Gaussian sum. Using [13, Theorem 5.33],

$$\widehat{f_{1,1}}(t,c) = \sum_{x\in\mathbb{F}_q} w_p^{Tr(tdx^2+cx)} = w_p^{Tr(-c^2(4td)^{-1})}\eta(td)G(\eta,\psi).$$

The definition of Gauss sum over $\mathbb{F}_q$ is given as [13],

$$G(\eta,\psi) = \begin{cases} (-1)^{m-1}q^{1/2}, & \text{if } p \equiv 1 \pmod 4 \\ (-1)^{m-1}\sqrt{-1}^m q^{1/2}, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

This definition leads to,

$$\widehat{f_{1,1}}(c) = \begin{cases} (-1)^{m-1}q^{\frac{1}{2}}w_p^{Tr(-c^2(4td)^{-1})}\eta(td), & \text{if } p \equiv 1 \pmod 4 \\ (-1)^{m-1}\sqrt{-1}^m q^{\frac{1}{2}}w_p^{Tr(-c^2(4td)^{-1})}\eta(td), & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Now, as $c = (c_1, c_2, ..., c_n) \in \mathbb{F}_q^n$ consider

$$\begin{aligned} \widehat{f_{2,1}}(t,c) &= \sum_{x\in\mathbb{F}_q^2} w_p^{Tr(tf_{2,1}(x)+c\cdot x)} = \sum_{x_1,x_2\in\mathbb{F}_q} w_p^{Tr(tdx_1^2+c_1x_1+c_2x_2)} \\ &= \sum_{x_2\in\mathbb{F}_q} w_p^{Tr(c_2x_2)} \sum_{x_1\in\mathbb{F}_q} w_p^{Tr(tdx_1^2+c_1x_1)} \end{aligned}$$

$$= \begin{cases} (-1)^{m-1}\eta(td)q^{1+\frac{1}{2}}w_p^{Tr(-c_1^2(4td)^{-1})}, & \text{if } Tr(c_2) = 0 \text{ and } p \equiv 1 \pmod 4 \\ (-1)^{m-1}\sqrt{-1}^m\eta(td)\,q^{1+\frac{1}{2}}w_p^{Tr(-c_1^2(4td)^{-1})}, & \text{if } Tr(c_2) = 0 \text{ and } p \equiv 3 \pmod 4 \\ 0, & \text{if } Tr(c_2) \neq 0. \end{cases}$$

Now, consider

$$\widehat{f_{3,1}}(t,c) = \sum_{x\in\mathbb{F}_q^3} w_p^{Tr(tf_{3,1}(x)+c\cdot x)} = \sum_{x_1,x_2,x_3\in\mathbb{F}_q} w_p^{Tr(tdx_1^2+c_1x_1+c_2x_2+c_3x_3)}$$

$$= \sum_{x_3 \in \mathbb{F}_q} w_p^{Tr(c_3x_3)} \sum_{x_2 \in \mathbb{F}_q} w_p^{Tr(c_2x_2)} \sum_{x_1 \in \mathbb{F}_q} w_p^{Tr(tdx_1^2+c_1x_1)}$$

$$= \begin{cases} (-1)^{m-1}\eta(td)q^{2+\frac{1}{2}}w_p^{Tr(-c_1^2(4td)^{-1})}, & \text{if } Tr(c_2) = Tr(c_3) = 0 \text{ and } p \equiv 1 \pmod 4 \\ (-1)^{m-1}\sqrt{-1}^m\eta(td)q^{2+\frac{1}{2}}w_p^{Tr(-c_1^2(4td)^{-1})}, & \text{if } Tr(c_2) = Tr(c_3) = 0 \text{ and } p \equiv 3 \pmod 4 \\ 0, & \text{if } (Tr(c_2), Tr(c_3)) \neq (0,0). \end{cases}$$

Then, one can easily see that,

$$\widehat{f_{n,1}}(t,c) = \begin{cases} (-1)^{m-1}\eta(td)q^{\frac{n+1}{2}}w_p^{Tr(-c_1^2(4td)^{-1})}, & \text{if } p \equiv 1 \pmod 4 \text{ and EQ} \\ (-1)^{m-1}\sqrt{-1}^m\eta(td)q^{\frac{n+1}{2}}w_p^{Tr(-c_1^2(4td)^{-1})}, & \text{if } p \equiv 3 \pmod 4 \text{ and EQ} \\ 0, & \text{if NEQ.} \end{cases}$$

More concrete examples can be given but instead, we compute the last steps to complete the proof.

$$\widehat{f_{n,n-1}}(t,c) = \sum_{x \in \mathbb{F}_q^n} w_p^{Tr(tf_{n,n-1}(x)+c\cdot x)} = \sum_{x \in \mathbb{F}_q^n} w_p^{Tr(td_1x_1^2+\cdots+td_{n-1}x_{n-1}^2+c_1x_1+\cdots+c_nx_n)}$$

$$= \left(\sum_{x_n \in \mathbb{F}_q} w_p^{Tr(c_nx_n)}\right)\left(\sum_{x_1 \in \mathbb{F}_q} w_p^{Tr(td_1x_1^2+c_1x_1)}\right)\cdots\left(\sum_{x_{n-1} \in \mathbb{F}_q} w_p^{Tr(td_{n-1}x_{n-1}^2+c_{n-1}x_{n-1})}\right).$$

This leads to the followings,

- If $n-1$ is even:

$$\widehat{f_{n,n-1}}(c) = \begin{cases} \eta(t^{n-1}D)q^{\frac{n+1}{2}}w_p^v, & \text{if } p \equiv 1 \pmod 4 \text{ and } Tr(c_n) = 0 \\ \sqrt{-1}^{(n-1)m}\eta(t^{n-1}D)q^{\frac{n+1}{2}}w_p^v, & \text{if } p \equiv 3 \pmod 4 \text{ and } Tr(c_n) = 0 \\ 0, & \text{if } Tr(c_n) \neq 0. \end{cases}$$

- If $n-1$ is odd:

$$\widehat{f_{n,n-1}}(c) = \begin{cases} (-1)^{m-1}\eta(t^{n-1}D)q^{\frac{n+1}{2}}w_p^v, & \text{if } p \equiv 1 \pmod 4 \text{ and } Tr(c_n) = 0 \\ (-1)^{m-1}\sqrt{-1}^{(n-1)m}\eta(t^{n-1}D)q^{\frac{n+1}{2}}w_p^v, & \text{if } p \equiv 3 \pmod 4 \text{ and } Tr(c_n) = 0 \\ 0, & \text{if } Tr(c_n) \neq 0. \end{cases}$$

Lastly, we compute $\widehat{f_{n,n}}$.

$$\widehat{f_{n,n}}(t,c) = \sum_{x \in \mathbb{F}_q^n} w_p^{Tr(tf_{n,n}(x)+c\cdot x)} = \sum_{x \in \mathbb{F}_q^n} w_p^{Tr(td_1x_1^2+\cdots+td_nx_n^2+c_1x_1+\cdots+c_nx_n)}$$

$$= \left(\sum_{x_1\in\mathbb{F}_q} w_p^{Tr(td_1x_1^2+c_1x_1)}\right)\left(\sum_{x_2\in\mathbb{F}_q} w_p^{Tr(td_2x_2^2+c_2x_2)}\right)\cdots\left(\sum_{x_n\in\mathbb{F}_q} w_p^{Tr(td_nx_n^2+c_nx_n)}\right)$$

$$= \begin{cases} \eta(t^nD)q^{\frac{n}{2}}w_p^{v'}, & \text{if } n \text{ even and } p\equiv 1 \pmod 4) \\ (-1)^{m-1}\eta(t^nD)q^{\frac{n}{2}}w_p^{v'}, & \text{if } n \text{ odd and } p\equiv 1 \pmod 4) \\ \sqrt{-1}^{nm}\eta(t^nD)q^{\frac{n}{2}}w_p^{v'}, & \text{if } n \text{ even and } p\equiv 3 \pmod 4) \\ (-1)^{m-1}\sqrt{-1}^{nm}\eta(t^nD)q^{\frac{n}{2}}w_p^{v'}, & \text{if } n \text{ odd and } p\equiv 3 \pmod 4). \end{cases}$$

□

**Lemma 2.4.** *Let $f_u : \mathbb{F}_q^n \to \mathbb{F}_q$ be defined by $f_u(x_1, x_2, ..., x_n) = d_1^u x_1^2 + d_2^u x_2^2 + ... + d_{n-1}^u x_{n-1}^2 + ux_n$, where $u \in \mathbb{F}_q$ and $d_1^u, d_2^u, \cdots, d_{n-1}^u \in \mathbb{F}_q^*$. For $u$, $v \in \mathbb{F}_q$ with $u \neq v$, the supports of the Walsh transforms of $f_u$ and $f_v$ are disjoint.*

*Proof.* Note that, by Theorem 2.3, $f_u$ is a near-bent function because if a linear term is added to a near-bent function it will again be a near-bent function.
Let $t \in \mathbb{F}_q^*$ be fixed and $c = (c_1, c_2, ..., c_n) \in \mathbb{F}_q^n$. Then,

$$\widehat{f_u}(t,c) = \sum_{x\in\mathbb{F}_q^n} w_p^{Tr(tf_u(x)+c\cdot x)} = \sum_{x\in\mathbb{F}_q^n} w_p^{Tr(t(d_1^ux_1^2+d_2^ux_2^2+...+d_{n-1}^ux_{n-1}^2+ux_n)+c\cdot x)}$$

$$= \sum_{x_1,...x_{n-1}\in\mathbb{F}_q} w_p^{Tr(t(d_1^ux_1^2+d_2^ux_2^2+...+d_{n-1}^ux_{n-1}^2)+c_1x_1+...+c_{n-1}x_{n-1})} \sum_{x_n\in\mathbb{F}_q} w_p^{Tr(utx_n+c_nx_n)}$$

The first sum in this product can be computed using Gauss sum and it can be seen that it is nonzero by Theorem 2.3. So, only the second sum, $\sum_{x_n\in\mathbb{F}_q} w_p^{Tr(utx_n+c_nx_n)}$, can make this product zero. If $utx_n + c_nx_n$ is nonzero, then $Tr(utx_n + c_nx_n)$ is linear, so the sum is zero. Hence, fixing $t \in \mathbb{F}_q^*$ we have,

$$supp(\widehat{f_u}) = \left\{c = (c_1, c_2, ..., c_n) \in \mathbb{F}_q^n : ut \equiv -c_n \pmod q\right\}.$$

□

## 2.4 Conclusion and Examples

In Theorem 2.3, we compute Walsh spectrums of certain quadratic functions and in Lemma 2.4, we show how to obtain quadratic functions with pairwise disjoint support of Walsh transforms. Now, using this information we give an application of the constructed method that is given in Theorem 2.2. Moreover, we classify these constructed functions as regular bent, weakly regular bent and non-weakly regular bent.
Let $f_u : \mathbb{F}_q^n \to \mathbb{F}_q$ be defined by $f_u(x_1, x_2, ..., x_n) = d_1^u x_1^2 + d_2^u x_2^2 + ... + d_{n-1}^u x_{n-1}^2 + ux_n$, where $u \in \mathbb{F}_q$ and $d_1^u, d_2^u, \cdots, d_{n-1}^u \in \mathbb{F}_q^*$. Let $F : \mathbb{F}_q^{n+1} \to \mathbb{F}_q$ be a bent function constructed by near-bent functions, $f_u$, using Theorem 2.2.

Let $t \in \mathbb{F}_q^*$. By Definition 1.6, $F^t : \mathbb{F}_q^{n+1} \to \mathbb{F}_p$ is a function with $F^t(x) = Tr(tF(x))$ and $f_u^t : \mathbb{F}_q^n \to \mathbb{F}_p$ is a function with $f_u^t(x) = Tr(tf_u(x))$. Our aim is to determine the cases for which $F^t$ is regular, weakly-regular or non-weakly regular, for a fixed $t \in \mathbb{F}_q^*$.

Let $(a, b) \in \mathbb{F}_q^n \times \mathbb{F}_q$. At the end of the proof of Theorem 2.2, we conclude that, for each $a \in \mathbb{F}_q^n$ and a fixed $t \in \mathbb{F}_q^*$, there exists exactly one $u$ such that $\left|\widehat{F}\big(t, (a, b)\big)\right| = \left|\widehat{f}_u(t, a)\right|$. This is equivalent to $\left|\widehat{F^t}(a, b)\right| = \left|\widehat{f_u^t}(a)\right|$. So, it is enough to investigate the Fourier coefficients of $f_u$ given in Theorem 2.3. For this investigation, we study case by case for the variables $n$, $m$ and $p$.

**First Case ($n - 1$ even)** Assume $n - 1$ is even. By Theorem 2.3,

$$spec\,(f_u) = \begin{cases} \left\{0, \eta(t^{n-1}D_u)q^{\frac{n+1}{2}}w_p^{f^*(c)}\right\}, & \text{if } p \equiv 1 \pmod 4 \\ \left\{0, \sqrt{-1}^{(n-1)m}\eta(t^{n-1}D_u)q^{\frac{n+1}{2}}w_p^{f^*(c)}\right\}, & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

where $u \in \mathbb{F}_q$, $D_u = \prod_{i=1}^{n-1} d_i^u$, $c \in \mathbb{F}_q^n$ and $f^* : \mathbb{F}_q^n \to \mathbb{F}_p$ is a function.

1. Assume $p \equiv 1 \pmod 4$. Then, the result depends on the value of $\eta(t^{n-1}D_u)$.
   - If $\eta(t^{n-1}D_u)$ is 1 for all values of $u \in \mathbb{F}_q$, then $F^t$ is regular.
   - If $\eta(t^{n-1}D_u)$ is $-1$ for all values of $u \in \mathbb{F}_q$, then $F^t$ is weakly regular.
   - If $\eta(t^{n-1}D_u)$ attains both of the values 1 and $-1$, $F^t$ is non-weakly regular.
2. Assume $p \equiv 3 \pmod 4$.
   - If $n - 1$ is equivalent to zero modulo 4, the result is the same with item 1.
   - If $n-1$ is equivalent to 2 modulo 4, we have two different results depending on $m$.
     When $m$ is even, the same conclusion given in item 1 occurs.
     When $m$ is odd, a slightly different situation comprises. $\eta(t^{n-1}D_u) = -1$ $\forall u \in \mathbb{F}_q$ gives that $F^t$ is regular. $\eta(t^{n-1}D_u) = 1$ $\forall u \in \mathbb{F}_q$ gives that $F^t$ is weakly regular. Lastly, when $\eta(t^{n-1}D_u)$ attains both of the values, $F^t$ is non-weakly regular.

**Second Case ($n - 1$ odd)** Assume $n - 1$ is odd. By Theorem 2.3,

$$spec\,(f_u) = \begin{cases} \left\{0, (-1)^{m-1}\eta(t^{n-1}D_u)q^{\frac{n+1}{2}}w_p^{f^*(c)}\right\}, & \text{if } p \equiv 1 \pmod 4 \\ \left\{0, (-1)^{m-1}\sqrt{-1}^{(n-1)m}\eta(t^{n-1}D_u)q^{\frac{n+1}{2}}w_p^{f^*(c)}\right\}, & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

where $u \in \mathbb{F}_q$, $D_u = \prod_{i=1}^{n-1} d_i^u$, $c \in \mathbb{F}_q^n$ and $f^* : \mathbb{F}_q^n \to \mathbb{F}_p$ is a function.

1. Assume $p \equiv 1 \pmod 4$.
   - For $m-1$ even, we have three different results depending on the value of $\eta\left(t^{n-1}D_u\right)$. If $\eta(t^{n-1}D_u)$ is 1 for all values of $u \in \mathbb{F}_q$, $F^t$ is regular. If $\eta(t^{n-1}D_u)$ is $-1$ for all values of $u \in \mathbb{F}_q$, $F^t$ is weakly regular. If $\eta(t^{n-1}D_u)$ takes both of the values $-1$ and 1, $F^u$ is non-weakly regular.
   - For $m-1$ odd, we have similar results to the case $m-1$ even. If $\eta(t^{n-1}D_u)$ is $-1$ for all values of $u \in \mathbb{F}_q$, $F^t$ is regular. If $\eta(t^{n-1}D_u)$ is 1 for all values of $u \in \mathbb{F}_q$, $F^t$ is weakly regular. If $\eta(t^{n-1}D_u)$ takes both of the values $-1$ and 1, $F^t$ is non-weakly regular.
2. Assume $p \equiv 3 \pmod 4$. Then, three different results are obtained depending on the value of $m$.
   - Assume $m \equiv 0 \pmod 4$. Then, the result is the same with the item 1, $(m-1)$ odd case.
   - Assume $m \equiv 2 \pmod 4$. Then, the result is the same with the item 1, $(m-1)$ even case.
   - Lastly, we investigate the case which is the same for $m \equiv 1 \pmod 4$ and $m \equiv 3 \pmod 4$. For all $u \in \mathbb{F}_q$ if $\eta(t^{n-1}D_u)$ is always 1 or always $-1$ , then $F^t$ is weakly regular. Otherwise, $F^t$ is non-weakly regular.

*Remark* 2.1. For a fixed $p$, greater number of bent functions are constructed compared to [3] because the coefficients of near-bent functions are chosen from a set with major number of elements.

*Remark* 2.2. For an odd prime $p$, there are equal numbers of quadratic residues and quadratic non-residues in $\mathbb{F}_p^*$. On the contrary, the number of quadratic non-residues is greater than the number of quadratic residues in $\mathbb{F}_{p^m}^*$. This leads to the situation that the percentage of non-weakly regular bent functions of our construction is grater than the percentage of non-weakly regular bent functions constructed in [3].

**Example 2.1.** Let $p = 3$, $n = 4$ and $q = 3^2$. Choosing the minimal polynomial $x^2 + 2x + 2$ and $a$ to be a root of it to construct $\mathbb{F}_{3^2}$ over $\mathbb{F}_3$, we represent the field $F_{3^2}$ as $\{\alpha a + \beta : \alpha, \beta \in \mathbb{F}_3\}$.
For $u \in \mathbb{F}_{3^2}$, $c_u \in \mathbb{F}_{3^2}^*$ and $x = (x_1, x_2, x_3, x_4)$, the functions $f_u : \mathbb{F}_{3^2}^4 \to \mathbb{F}_{3^2}$ defined by $f_u(x) = c_u x_1^2 + x_2^2 + x_3^2 + u x_4$ are near-bent functions with pairwise disjoint support of Walsh transforms. Now, consider the following identified near-bent functions defined from $\mathbb{F}_{3^2}^4$ to $\mathbb{F}_{3^2}$.

$$f_0(x) = 2x_1^2 + x_2^2 + x_3^2$$

$$f_1(x) = x_1^2 + x_2^2 + x_3^2 + x_4$$

$$f_2(x) = 2x_1^2 + x_2^2 + x_3^2 + 2x_4$$

$$f_a(x) = x_1^2 + x_2^2 + x_3^2 + a x_4$$

$$\begin{aligned}
f_{a+1}(x) &= 2x_1^2 + x_2^2 + x_3^2 + (a+1)x_4 \\
f_{a+2}(x) &= x_1^2 + x_2^2 + x_3^2 + (a+2)x_4 \\
f_{2a}(x) &= 2x_1^2 + x_2^2 + x_3^2 + (2a)x_4 \\
f_{2a+1}(x) &= x_1^2 + x_2^2 + x_3^2 + (2a+1)x_4 \\
f_{2a+2}(x) &= x_1^2 + x_2^2 + x_3^2 + (2a+2)x_4
\end{aligned}$$

By Theorem 2.2, $F(x_1, x_2, x_3, x_4, y)$ defined from $\mathbb{F}_{3^2}^5$ to $\mathbb{F}_{3^2}$ and given by,

$$\textstyle\sum_{u\in\mathbb{F}_{3^2}} \frac{y(y-1)(y-2)(y-a)(y-(a+1))(y-(a+2))(y-2a)(y-(2a+1))(y-(2a+2))}{(y-u)} f_u(x)$$

$= y^8x_1^2 - y^8x_4 + ay^8 + a^2y^6x_1^2 + a^6y^7x_4 + a^3y^7 + y^6x_4 + a^5y^6 + y^4x_1^2 + a^2y^5x_4 + a^7y^5 + a^5y^3 + x_1^2 - y^4x_4 + ay^4 + a^6y^2x_1^2 + a^6y^3x_4 + a^3y^3 + a^7yx_1^2 + y^2x_4 + a^5y^2 + x_1^2 - x_2^2 - x_3^2 + ayx_4 + a^7y,$
is a bent function with algebraic degree 10.
Let $F^t : \mathbb{F}_{3^2}^5 \to \mathbb{F}_3$ with $F^t(x) = Tr(tF(x))$. Let $t \in \mathbb{F}_{3^2}^*$ be fixed. If $t = 1$, then, $F^t$ is a regular bent function because $1$ is a quadratic residue of $\mathbb{F}_{3^2}^*$. If $t = a+2$, then, $F^t$ is weakly regular bent function because $(a+2)^3 = 2a$ is a quadratic non-residue of $\mathbb{F}_{3^2}^*$. Actually, $F^t$ being regular, weakly regular or non-weakly regular does not depend on the value of $t$. This is because multiplying $D_u$ by $t^{n-1}$ does not change the situation whether $\eta(t^{n-1}D_u)$ is stable or variable for all values of $u \in \mathbb{F}_q$. Actually, this depends on the reason that the product of two residues or two non-residues is a residue, whereas the product of a nonresidue and residue is a nonresidue.
In addition, if we choose at least one of the $c_u$ from the set of quadratic non-residues of $\mathbb{F}_{3^2}^*$, namely $\{a, 2a, a+2, 2a+1\}$, and at least one of the $c_u$ from the set of quadratic residues of $\mathbb{F}_{3^2}^*$, namely $\{1, 2, a+1, 2a+2\}$; then $F^t$ is a non-weakly regular bent function for all values of $t \in \mathbb{F}_{3^2}^*$.

# CHAPTER 3

# A CONSTRUCTION OF (NON)-WEAKLY REGULAR BENT FUNCTIONS OVER THE RING OF INTEGERS MODULO $p^m$

## 3.1 Introduction

This chapter is devoted to adapting the methods over finite fields with odd characteristic given in Chapter 2 to the ring of integers modulo $p^m$. Studying over rings brings some difficulties due to the reasons that rings have zero divisors, there is a need of special type of coefficients for Lagrange interpolation and computation of Gauss sums over rings.

In Section 3.2, we give an adaptation of the construction method given in Theorem 2.2. In [3], the authors use polynomials as coefficients for Lagrange interpolation. However, for our case we prove that the functions which can be used as coefficients for Lagrange interpolation cannot be representible as polynomials using the paper of Carlitz [2].

Consider the quadratic functions of the form $d_1x_1^2 + d_2x_2^2 + ... + d_{n-s}x_{n-s}^2$ where $d_i \in \mathbb{Z}_q^\times$ and $0 \leq s \leq n-1$. In Section 3.3, we determine the Walsh spectrum of these functions when they are defined over $\mathbb{Z}_{p^2}$ by a method that is different from the one that is used in [3]. Then, we study the same concept over $\mathbb{Z}_{p^3}$ in Section 3.4. The results are different from each other and to achieve these results, we compute quadratic Gauss sum over $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_{p^3}$. In Section 3.5, we generalize the idea of Section 3.3 and Section 3.4. The Walsh spectrum of quadratic functions that are described at the beginning of this paragraph give different results for odd $m$ and even $m$ when they are defined from $\mathbb{Z}_{p^m}^n$ to $\mathbb{Z}_{p^m}$. Note that, to reach the results we computed quadratic Gauss sums for each case. Moreover, we present a simple technique to obtain quadratic near-bent functions with pairwise disjoint support of Walsh transforms.

In Section 3.6, we conclude the chapter by giving examples to generate regular, weakly regular and non-weakly regular bent functions. For the examples, we use quadratic functions to construct a bent function over $\mathbb{Z}_{p^m}$. If $m$ is even, then all constructed bent functions are regular. If $m$ is odd, the great majority of the constructed bent functions are non-weakly regular similar to [3], but there exists some distinctions. To illustrate, for each $p$, we can construct further bent functions and the percentage of non-weakly regular bent functions is greater. Also, as $p$ and $m$ increase for an odd $m$, this percentage of non-weakly regular gets greater.

### 3.2 A Method to Construct Bent Functions Using near-bent Functions

To combine near-bent functions for constructing a bent function, we study the Lagrange interpolation principle on integers modulo $n$ because we cannot use the same coefficients that are used in [3].

The reason is that $\mathbb{Z}_q^n$ has zero divisors, that is, for every value $u \in \{0, 1, ..., q-1\}$, the coefficient $\frac{y(y-1)...(y-(q-1))}{y-u}$ becomes zero for each $y \in \mathbb{Z}_q^n$. The original coefficients given in the classical definition of Lagrange interpolation cannot be used either because of the same reason. Moreover, we show that one cannot find new coefficients for the construction over the ring of integers using some of the methods in [2].

**Proposition 3.1.** *Let $u \in \mathbb{Z}_q$. The functions $h_u : \mathbb{Z}_q \to \mathbb{Z}_q$ which are defined by*

$$h_u(x) = \begin{cases} a, & \textit{if } x = u \\ 0, & \textit{if } x \neq u, \end{cases}$$

*where $a \not\equiv 0 \pmod p$, cannot be represented in a polynomial form.*

*Proof.* For any polynomial, $g(x)$, it is a fact that $g(x+p) = g(x) \pmod p$. However, $h_u$ does not satisfy this equation for $x = u$ which implies $h_u(x)$ cannot be represented as a polynomial [2]. □

**Proposition 3.2.** *For $u \in \mathbb{Z}_{p^2}$, the functions $h_u : \mathbb{Z}_{p^2} \to \mathbb{Z}_{p^2}$ which are defined as follows*

$$h_u(x) = \begin{cases} p, & \textit{if } x = u \\ 0, & \textit{if } x \neq u, \end{cases}$$

*cannot be represented as a polynomial.*

*Proof.* Note that, a function $f(x)$ over $\mathbb{Z}_{p^2}$ can be represented by a polynomial over $\mathbb{Z}_{p^2}$ if and only if $\sum_{s=0}^{r}(-1)^{r-s}\binom{r}{s}f(s) \equiv 0 \pmod{p^{v(r)}}$ for $0 \leq r < p^2$ where $v(r) = min(2, \mu(r))$ and $\mu(r)$ is the highest power of $p$ that divides $r!$ [2].
Let $j \equiv u \pmod p$. Now, consider $\sum_{s=0}^{r}(-1)^{r-s}\binom{r}{s}h_u(s)$ for the case when $r = 2p+j$. Since $r \geq 2p$, $p^2$ divides $r!$. So, $v(r) = 2$. Then,

$$\sum_{s=0}^{2p+j}(-1)^{2p+j-s}\binom{2p+j}{s}h_u(s) = (-1)^{2p+j-u}\binom{2p+j}{u}h_u(u) = (-1)^{2p+j-u}\binom{2p+j}{u}p.$$

This is not divisible by $p^2$ as $\binom{2p+j}{u}$ is not divisible by $p$. Therefore, the sum is not equivalent to zero modulo $p^2$, which implies $h_u(x)$ cannot be representible in polynomial form. □

*Remark* 3.1. Let $L_c(x)$ be defined from $\mathbb{Z}_q$ to $\mathbb{Z}_q$ and given by $L_c(x) = (1-(x-c)^{p-1})^{p^n-1}$. Carlitz suggested that this polynomial can be used for Lagrange interpolation formula [2]. Actually, the values of the function can be easily computed as:

$$L_c(x) = \begin{cases} 1, & \text{if } x \equiv c \pmod p \\ 0, & \text{if } x \not\equiv c \pmod p. \end{cases}$$

For $i \in \{0, 1, ..., q\}$, letting $f_i : \mathbb{Z}_q^n \to \mathbb{Z}_q$ be near-bent functions with supp$(\hat{f_i})\cap$supp$(\hat{f_j})$ is empty for $i \neq j$, one can consider the following construction: $F : \mathbb{Z}_q^n \times \mathbb{Z}_q \to \mathbb{Z}_q$ defined as

$$F(x,y) = \sum_{i=0}^{p-1} f_i(x)L_i(y)$$

However, using this construction, one can combine $p$-many near-bent functions and so, $F$ cannot be a bent function. Actually, this result is not suprising because in the Theorem 3.3, we explain that we need $q$-many near-bent functions to obtain a bent function. Some values of $\widehat{F}$ are zero as $\bigcup_{i=0}^{p-1} supp(\widehat{f_i})$ is equal to $\mathbb{Z}_q^n$. Example 3.1 is given to illustrate this.

**Example 3.1.** Let $f_0$, $f_1$ and $f_2$ be near-bent functions with disjoint support of Walsh spectrums and defined from $\mathbb{Z}_9^4$ to $\mathbb{Z}_9$. For $c = 0, 1, 2$, let the functions $L_i : \mathbb{Z}_9 \to \mathbb{Z}_9$ be defined by

$$L_c(x) = \begin{cases} 1, & \text{if } x \equiv c \pmod 3 \\ 0, & \text{if } x \not\equiv c \pmod 3. \end{cases}$$

Then, construct the function $F$ which is defined from $\mathbb{Z}_9^4 \times \mathbb{Z}_9$ to $\mathbb{Z}_9$ as $F(x,y) = \sum_{c=0}^{2} f_c(x)L_c(y)$. That is,

$$F(x,y) = f_0(x)L_0(y) + f_1(x)L_1(y) + f_2(x)L_2(y)$$

Then, for $a \in \mathbb{Z}_9^4$ and $b \in \mathbb{Z}_9$, we have

$$\widehat{F}(a,b) = \sum_{x\in\mathbb{Z}_9^4}\sum_{y\in\mathbb{Z}_9} w^{F(x,y)-a\cdot x-by} = \sum_{y\in\mathbb{Z}_9} w^{-by} \sum_{x\in\mathbb{Z}_9^4} w^{F(x,y)-a\cdot x}$$

$$= \sum_{y\in\mathbb{Z}_9} w^{-by} \sum_{x\in\mathbb{Z}_9^4} w^{(f_0(x)L_0(y)+f_1(x)L_1(y)+f_2(x)L_2(y))-a\cdot x}$$

$$= \left(w^0 + w^{-3b} + w^{-6b}\right) \sum_{x\in\mathbb{Z}_9^4} w^{f_0(x)-a\cdot x} +$$

$$\left(w^{-b} + w^{-4b} + w^{-7b}\right) \sum_{x\in\mathbb{Z}_9^4} w^{f_1(x)-a\cdot x} + \left(w^{-2b} + w^{-5b} + w^{-8b}\right) \sum_{x\in\mathbb{Z}_9^4} w^{f_2(x)-a\cdot x}$$

Note that,

$$w^0 + w^{-3b} + w^{-6b} = \begin{cases} 3, & \text{if } b \equiv 0 \pmod 3 \\ 0, & \text{if } b \not\equiv 0 \pmod 3. \end{cases}$$

$$w^{-b} + w^{-4b} + w^{-7b} = \begin{cases} 3, & \text{if } b = 0 \\ -1.5 - 2.5\sqrt{-1}, & \text{if } b = 3 \text{ or b=6} \\ 0, & \text{if } b \not\equiv 0 \pmod 3. \end{cases}$$

$$w^{-2b} + w^{-5b} + w^{-8b} = \begin{cases} 3, & \text{if } b = 0 \\ -1.5 + 2.5\sqrt{-1}, & \text{if } b = 3 \\ -1.5 - 2.5\sqrt{-1}, & \text{if } b = 6 \\ 0, & \text{if } b \not\equiv 0 \pmod 3. \end{cases}$$

Using these results, we have

$$\widehat{F}(a,b) = \begin{cases} 3(\widehat{f_0}(a) + \widehat{f_1}(a) + \widehat{f_2}(a)), & \text{if } b = 0 \\ 3\widehat{f_0}(a) + (-1.5 - 2.5\sqrt{-1})\widehat{f_1}(a) + (-1.5 + 2.5\sqrt{-1})\widehat{f_2}(a), & \text{if } b = 3 \\ 3\widehat{f_0}(a) + (-1.5 - 2.5\sqrt{-1})(\widehat{f_1}(a) + \widehat{f_2}(a)), & \text{if } b = 6 \\ 0, & \text{if } b \not\equiv 0 \pmod 3. \end{cases}$$

Obviously, $F$ is not a bent function.

*Remark* 3.2. Using the same notation and data in Remark 3.1, another construction using $q$-many near-bent functions can be considered as follows:

$$F(x,y) = \sum_{i=0}^{q-1} f_i(x) L_j(y),$$

where $j \equiv i \pmod p$. However, one can see that $F$ is not bent using the definition easily since for each value of $y$, $F$ depends $p^{m-1}$ many $f_i$ functions. To illustrate, consider the following example.

**Example 3.2.** Let $f_0, f_1, \cdots f_8$ be near-bent functions with disjoint support of Walsh transforms and defined from $\mathbb{Z}_9^4$ to $\mathbb{Z}_9$. For $c = 0, 1, 2$, let the functions $L_c : \mathbb{Z}_9 \to \mathbb{Z}_9$ be defined by

$$L_c(x) = \begin{cases} 1, & \text{if } x \equiv c \pmod 3 \\ 0, & \text{if } x \not\equiv c \pmod 3. \end{cases}$$

Then, construct the function $F$ which is defined from $\mathbb{Z}_9^4 \times \mathbb{Z}_9$ to $\mathbb{Z}_9$ as $F(x,y) = \sum_{i=0}^{8} f_i(x) L_j(y)$ where $j \equiv i \pmod p$. Then, we have

$$\begin{aligned}
\widehat{F}(a,b) &= \sum_{x\in\mathbb{Z}_9^4}\sum_{y\in\mathbb{Z}_9} w^{F(x,y)-a\cdot x-by} = \sum_{y\in\mathbb{Z}_9} w^{-by}\sum_{x\in\mathbb{Z}_9^4} w^{F(x,y)-a\cdot x}\\
&= \sum_{y\in\mathbb{Z}_9} w^{-by}\sum_{x\in\mathbb{Z}_9^4} w^{\left(\sum_{i=0}^{8} f_i(x)L_j(y)\right)-a\cdot x}\\
&= \left(w^0+w^{-3b}+w^{-6b}\right)\sum_{x\in\mathbb{Z}_9^4} w^{(f_0(x)+f_3(x)+f_6(x))+-a\cdot x}+\\
&\quad \left(w^{-b}+w^{-4b}+w^{-7b}\right)\sum_{x\in\mathbb{Z}_9^4} w^{(f_1(x)+f_4(x)+f_7(x))-a\cdot x}+\\
&\quad \left(w^{-2b}+w^{-5b}+w^{-8b}\right)\sum_{x\in\mathbb{Z}_9^4} w^{(f_2(x)+f_5(x)+f_8(x))-a\cdot x},
\end{aligned}$$

which gives $F$ is not a bent function.

**Theorem 3.3.** *For $u \in \mathbb{Z}_q$, let $f_u : \mathbb{Z}_q^n \to \mathbb{Z}_q$ be near-bent functions such that $supp(\widehat{f_u}) \cap supp(\widehat{f_v})$ is empty for $u, v \in \mathbb{Z}_q$. Let $h_u$ be a function defined from $\mathbb{Z}_q$ to $\mathbb{Z}_q$ and given by,*

$$h_u(x) = \begin{cases} 1, & \textit{if } x = u\\ 0, & \textit{if } x \neq u.\end{cases}$$

*Then, the function $F : \mathbb{Z}_q^n \times \mathbb{Z}_q \to \mathbb{Z}_q$ defined by*

$$F(x,y) = \sum_{u\in\mathbb{Z}_q} h_u(y) f_u(x),$$

*is bent.*

*Proof.* We first determine the number of near-bent functions that is needed to construct a bent function. For this aim, we obtain a special case of the Parseval's relation. Let $f : \mathbb{Z}_q^n \to \mathbb{Z}_q$, and $a \in \mathbb{Z}_q^n$. Then,

$$\sum_{a\in\mathbb{Z}_q^n}\left|\widehat{f}(a)\right|^2 = \sum_{a\in\mathbb{Z}_q^n}\sum_{x,y\in\mathbb{Z}_q^n} w^{f(x)-a\cdot x-(f(y)-a\cdot y)} = \sum_{x,y\in\mathbb{Z}_q^n} w^{(f(x)-f(y))}\sum_{a\in\mathbb{Z}_q^n} w^{a\cdot(y-x)}.$$

Realizing that,

$$\sum_{a\in\mathbb{Z}_q^n} w^{a\cdot(y-x)} = \begin{cases} q^n, & \text{if } x = y\\ 0, & \text{if } x \neq y,\end{cases}$$

we have

$$\sum_{a\in\mathbb{Z}_q^n}\left|\widehat{f}(a)\right|^2 = \begin{cases} q^{2n}, & \text{if } x = y\\ 0, & \text{if } x \neq y.\end{cases}$$

Then, for a near-bent funtion $f$, we have

$$\sum_{a\in\mathbb{Z}_q^n}\left|\widehat{f}(a)\right|^2=\left|supp(\widehat{f})\right|q^{n+1}=q^{2n},$$

since $\left|\widehat{f}(a)\right|=0$ or $q^{n+1/2}$ for all $a\in\mathbb{Z}_q^n$. By this, one gets $\left|supp(\widehat{f})\right|=q^{n-1}$.

We need to combine the near-bent functions using the principle of Lagrange interpolation. The idea is constructing a function $F$ by 'glueing' the near-bent functions in such a way that Walsh spectrum of $F$ do not include zero value. This can be achieved by combining the near-bent functions having no common element in supports of their Walsh transforms and the union of their support of Walsh transforms should be $\mathbb{Z}_q^n$. Hence, the number of near-bent functions that is needed is $q$ as $\left|supp(\widehat{f})\right|=q^{n-1}$.

Let $f_u:\mathbb{Z}_q^n\to\mathbb{Z}_q$, for $u\in\mathbb{Z}_q$ be near-bent functions. Then, $\left|\widehat{f_u}(a)\right|^2=q^{n+1}$ or $0$ for all $a\in\mathbb{Z}_q^n$.

Let $(a,b)\in\mathbb{Z}_q^n\times\mathbb{Z}_q$ and $w$ be the $q$-th root of unity. Then,

$$\widehat{F}(a,b)=\sum_{x\in\mathbb{Z}_q^n,y\in\mathbb{Z}_q}w^{F(x,y)-a\cdot x-by}=\sum_{y\in\mathbb{Z}_q}w^{-by}\sum_{x\in\mathbb{Z}_q^n}w^{F(x,y)-a\cdot x}$$

$$=\sum_{y\in\mathbb{Z}_q}w^{-by}\sum_{x\in\mathbb{Z}_q^n}w^{(\sum_{u\in\mathbb{Z}_q}h_u(y)f_u(x))-a\cdot x}=\sum_{y\in\mathbb{Z}_q}w^{-by}\sum_{x\in\mathbb{Z}_q^n}w^{(h_0(y)f_0(x)+\cdots+h_{q-1}(y)f_{q-1}(x))-a\cdot x}=$$

$$w^0\sum_{x\in\mathbb{Z}_q^n}w^{f_0(x)-a\cdot x}+w^{-b}\sum_{x\in\mathbb{Z}_q^n}w^{f_1(x)-a\cdot x}+\cdots+w^{-(q-1)y}\sum_{x\in\mathbb{Z}_q^n}w^{f_{q-1}(x)-a\cdot x}=\sum_{y\in\mathbb{Z}_q}w^{-by}\widehat{f_y}(a).$$

Since $supp(\widehat{f_u})\cap supp(\widehat{f_v})$ is empty and $\bigcup_{u\in\mathbb{Z}_q}supp(\widehat{f_u})=\mathbb{Z}_q^n$, each $a$ is an element of exactly one $\widehat{f_y}$. So, we have

$$\left|\widehat{F}(a,b)\right|=\left|\sum_{y\in\mathbb{Z}_q}w^{-by}\widehat{f_y}(a)\right|=\left|w^{-by}\widehat{f_y}(a)\right|=q^{\frac{n+1}{2}}.$$

□

### 3.3 Walsh Spectrum of quadratic Functions over $\mathbb{Z}_{p^2}$

In the whole section, $q$ is $p^2$ and $w$ denotes the $q$-th root of unity, that is $w=e^{2\pi\sqrt{-1}/p^2}$. To construct bent functions using Theorem 3.3, we need near-bent functions with the desired properties.

In this section, we determine Walsh spectrum of quadratic functions, $f_{n,n-s} := d_1x_1^2 + d_2x_2^2 + ... + d_{n-s}x_{n-s}^2$ defined from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q$ for $s \in \{0, 1, ..., n-1\}$ and $d_1, d_2, \cdots, d_{n-s} \in \mathbb{Z}_q^\times$.

**Lemma 3.4.** *Let $q = p^2$, $d \in \mathbb{Z}_q^\times$ and $c \in \mathbb{Z}_q$. The quadratic Gauss sum over $\mathbb{Z}_q$, namely $\sum_{x\in\mathbb{Z}_q} w^{dx^2-cx}$, equals to $pw^{-c^2/4d}$.*

*Proof.* A change of variables will be helpful, so replacing $x$ with $y + \alpha$ for $\alpha = c/2d$ we have,

$$dx^2 - cx = d(y+\alpha)^2 - c(y+\alpha) = dy^2 + cy + \frac{c^2}{4d} - cy - \frac{c^2}{2d} = dy^2 - \frac{c^2}{4d}.$$

Hence, $\sum_{x\in\mathbb{Z}_q} w^{dx^2-cx} = w^{-c^2/4d} \sum_{x\in\mathbb{Z}_q} w^{dx^2}$. For $x \in \mathbb{Z}_q$, there exists $a_0$, $a_1 \in \mathbb{Z}_p$ such that $x = a_0 + a_1p$. Then,

$$\sum_{x\in\mathbb{Z}_q} w^{dx^2} = \sum_{a_0,a_1\in\mathbb{Z}_p} w^{d(a_0+a_1p)^2} = \sum_{a_0,a_1\in\mathbb{Z}_p} w^{da_0^2+2da_0a_1p+da_1^2p^2}$$

$$= \sum_{a_0\in\mathbb{Z}_p} e^{\frac{2\pi\sqrt{-1}(da_0^2)}{p^2}} \sum_{a_1\in\mathbb{Z}_p} e^{\frac{2\pi\sqrt{-1}(da_0a_1)}{p}} = p,$$

because $\sum_{a_1\in\mathbb{Z}_p} e^{\frac{2\pi\sqrt{-1}(da_0a_1)}{p}}$ is $p$ for $a_0 = 0$ and zero otherwise as $d \in \mathbb{Z}_q^\times$. □

**Theorem 3.5.** *Let $q = p^2$. Let $f_{n,n-s} : \mathbb{Z}_q^n \to \mathbb{Z}_q$ be defined by $f_{n,n-s}(x_1, x_2, \cdots, x_n) := d_1x_1^2 + d_2x_2^2 + ... + d_{n-s}x_{n-s}^2$ where $d_1, d_2, \cdots, d_{n-s} \in \mathbb{Z}_q^\times$. Let $w$ be the $q$-th root of unity, that is $w = e^{2\pi\sqrt{-1}/p^2}$. Then,*

$$\widehat{f_{n,n-s}}(c) = \begin{cases} q^{\frac{n+s}{2}} w^{-\frac{c_1^2}{4d_1} - \frac{c_2^2}{4d_2} - \cdots \frac{c_{n-s}^2}{4d_{n-s}}}, & \textit{if } c_n = c_{n-1} = \cdots = c_{n-s+1} = 0 \\ 0, & \textit{if otherwise}, \end{cases}$$

*where $s$ is a positive integer with $0 < s \leq n-1$ and $c = (c_1, c_2, \cdots, c_n)$ for $c_i \in \mathbb{Z}_q$.*

*Moreover, for $s = 0$, the result is simply $\widehat{f_{n,n}}(c) = q^{\frac{n}{2}} w^{-\frac{c_1^2}{4d_1} - \frac{c_2^2}{4d_2} - \cdots \frac{c_n^2}{4d_n}}$.*

*Proof.* It is useful to compute the Walsh spectrum of $f_{1,1}(x) = dx^2$, first. Then, $\widehat{f_{n,1}}$ is obtained and this leads to the determination of the general form. Using Lemma 3.4, we have

$$\widehat{f_{1,1}}(c) = \sum_{x\in\mathbb{Z}_q} w^{dx^2-cx} = w^{-c^2/4d} q^{1/2}.$$

Then,

$$\widehat{f_{2,1}}(c) = \sum_{x\in\mathbb{Z}_q^2} w^{f_{2,1}(x)-c\cdot x} = \sum_{x_1,x_2\in\mathbb{Z}_q} w^{dx_1^2-c_1x_1-c_2x_2}$$

$$= \sum_{x_2\in\mathbb{Z}_q} w^{-c_2x_2} \sum_{x_1\in\mathbb{Z}_q} w^{dx_1^2-c_1x_1} = \begin{cases} q^{3/2}w^{-c_1^2/4d}, & \text{if } c_2 = 0 \\ 0, & \text{if } c_2 \neq 0. \end{cases}$$

Similarly,

$$\widehat{f_{3,1}}(c) = \sum_{x\in\mathbb{Z}_q^3} w^{f_{3,1}(x)-c\cdot x} = \sum_{x_1,x_2,x_3\in\mathbb{Z}_q} w^{dx_1^2-c_1x_1-c_2x_2-c_3x_3}$$

$$= \sum_{x_3\in\mathbb{Z}_q} w^{-c_3x_3} \sum_{x_2\in\mathbb{Z}_q} w^{-c_2x_2} \sum_{x_1\in\mathbb{Z}_q} w^{dx_1^2-c_1x_1}$$

$$= \begin{cases} q^{5/2}w^{-c_1^2/4d}, & \text{if } c_2 = c_3 = 0 \\ 0, & \text{if otherwise.} \end{cases}$$

Then, $\widehat{f_{n,1}}(c)$ can be easily computed as,

$$\widehat{f_{n,1}}(c) = \begin{cases} q^{\frac{n+s}{2}}w^{-c_1^2/4d}, & \text{if } c_n = c_{n-1} = \cdots = c_2 = 0 \\ 0, & \text{if otherwise.} \end{cases}$$

Now, consider $f_{n,n}$. We have,

$$\widehat{f_{n,n}}(c) = \sum_{x\in\mathbb{Z}_q^n} w^{f_{n,n}(x)-c\cdot x} = \sum_{x\in\mathbb{Z}_q^n} w^{d_1x_1^2+\cdots+d_nx_n^2-c_1x_1-\cdots-c_nx_n}$$

$$= \left(\sum_{x_1\in\mathbb{Z}_q} w^{d_1x_1^2-c_1x_1}\right)\left(\sum_{x_2\in\mathbb{Z}_q} w^{d_2x_2^2-c_2x_2}\right)\cdots\left(\sum_{x_n\in\mathbb{Z}_q} w^{d_nx_n^2-c_nx_n}\right)$$

$$= q^{n/2}w^{-\frac{c_1^2}{4d_1}-\frac{c_2^2}{4d_2}-\cdots\frac{c_n^2}{4d_n}}.$$

Next, we consider $f_{n,n-1}$. We have,

$$\widehat{f_{n,n-1}}(c) = \sum_{x\in\mathbb{Z}_q^n} w^{f_{n,n-1}(x)-c\cdot x} = \sum_{x\in\mathbb{Z}_q^n} w^{d_1x_1^2+\cdots+d_{n-1}x_{n-1}^2-c_1x_1-\cdots-c_nx_n}$$

$$= \left(\sum_{x_1\in\mathbb{Z}_q} w^{d_1x_1^2-c_1x_1}\right)\cdots\left(\sum_{x_{n-1}\in\mathbb{Z}_q} w^{d_{n-1}x_{n-1}^2-c_{n-1}x_{n-1}}\right)\left(\sum_{x_n\in\mathbb{Z}_q} w^{-c_nx_n}\right)$$

$$= \begin{cases} q^{\frac{n+1}{2}} w^{-\frac{c_1^2}{4d_1}-\frac{c_2^2}{4d_2}-\dots\frac{c_{n-1}^2}{4d_{n-1}}}, & \text{if } c_n = 0 \\ 0 & \text{if } c_n \neq 0. \end{cases}$$

The general case can be achieved, similarly.

□

### 3.4 Walsh Spectrum of Quadratic Functions over $\mathbb{Z}_{p^3}$

In this section, we give an adaptation of the study given in Section 3.3. That is, for $q = p^3$, we determine the Walsh spectrum of quadratic functions $f_{n,n-s} := d_1x_1^2 + d_2x_2^2 + \dots + d_{n-s}x_{n-s}^2$ defined from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q$, for $s \in \{0, 1, ..., n-1\}$ and $d_1, d_2, ..., d_{n-s} \in \mathbb{Z}_q^\times$.

**Lemma 3.6.** *Let $q = p^3$, $d \in \mathbb{Z}_q^\times$ and $c \in \mathbb{Z}_q$. Then, the quadratic Gauss sum over $\mathbb{Z}_q$ is as follows.*

$$\sum_{x\in\mathbb{Z}_q} w^{dx^2-cx} = \begin{cases} w^{-c^2/4d}q^{1/2}\eta(d), & \textit{if } p \equiv 1 \pmod 4 \\ w^{-c^2/4d}q^{1/2}\eta(d)\sqrt{-1}, & \textit{if } p \equiv 3 \pmod 4). \end{cases}$$

*Proof.* For simplicity, replace $x$ with $y + \alpha$ for $\alpha = c/2d$. Then,

$$dx^2 - cx = d(y+\alpha)^2 - c(y+\alpha) = dy^2 + cy + \frac{c^2}{4d} - cy - \frac{c^2}{2d} = dy^2 - \frac{c^2}{4d}.$$

We have $\mathbb{Z}_q = \mathbb{Z}_{p^3} = \{a_0 + pa_1 + p^2a_2 : a_0, a_1, a_2 \in \mathbb{Z}_p\}$.

$$\sum_{x\in\mathbb{Z}_q} w^{dx^2} = \sum_{a_0,a_1,a_2\in\mathbb{Z}_p} w^{d(a_0+a_1p+a_2p^2)^2} = \sum_{a_0,a_1,a_2\in\mathbb{Z}_p} w^{da_0^2+2da_0a_1p+(2da_0a_2+da_1^2)p^2}$$

$$= \sum_{a_0\in\mathbb{Z}_p} e^{\frac{2\pi\sqrt{-1}(da_0^2)}{p^3}} \sum_{a_1\in\mathbb{Z}_p} e^{\frac{2\pi\sqrt{-1}(2da_0a_1p+da_1^2p^2)}{p^3}} \sum_{a_2\in\mathbb{Z}_p} e^{\frac{2\pi\sqrt{-1}(2da_0a_2)}{p}} = p\sum_{a_1\in\mathbb{Z}_p} e^{\frac{2\pi\sqrt{-1}(da_1^2)}{p}}.$$

The last equality comes from the fact that $d \in \mathbb{Z}_q^\times$ and

$$\sum_{a_2\in\mathbb{Z}_p} e^{\frac{2\pi\sqrt{-1}(2da_0a_2)}{p}} = \begin{cases} p, & \text{if } a_0 = 0 \\ 0, & \text{if otherwise.} \end{cases}$$

Using [13, Theorem 5.33] and the definition of the Gauss sum over finite fields with $p$ elements, we conclude that

$$p\sum_{a_1\in\mathbb{Z}_p} e^{\frac{2\pi\sqrt{-1}(da_1^2)}{p}} = \begin{cases} p^{3/2}\eta(d), & \text{if } p \equiv 1 \pmod 4 \\ p^{3/2}\eta(d)\sqrt{-1}, & \text{if } p \equiv 3 \pmod 4). \end{cases}$$

□

**Theorem 3.7.** *For $q = p^3$, let $f_{n,n-s} : \mathbb{Z}_q^n \to \mathbb{Z}_q$ be defined by $f_{n,n-s}(x_1, x_2, \cdots, x_n) := d_1x_1^2 + d_2x_2^2 + ... + d_{n-s}x_{n-s}^2$ for $d_i \in \mathbb{Z}_q^\times$. Let $\eta$ be the quadratic character of $\mathbb{Z}_q$ and $w$ be the $q$-th root of unity, that is $w = e^{2\pi\sqrt{-1}/p^3}$. Then, for a positive integer $s$ such that $0 < s \leq n-1$, we have,*

$$\widehat{f_{n,n-s}}(c) = \begin{cases} q^{\frac{n+s}{2}} w^v \eta(D), & \textit{if } p \equiv 1 \pmod 4 \textit{ and } c_n = c_{n-1} = \cdots = c_{n-s+1} = 0 \\ q^{\frac{n+s}{2}} w^v \eta(D)\sqrt{-1}^{n-s}, & \textit{if } p \equiv 3 \pmod 4 \textit{ and } c_n = c_{n-1} = \cdots = c_{n-s+1} = 0 \\ 0, & \textit{if otherwise}, \end{cases}$$

*where $D = d_1d_2\cdots d_{n-s}$, $v = -\frac{c_1^2}{4d_1} - \frac{c_2^2}{4d_2} - \cdots \frac{c_{n-s}^2}{4d_{n-s}}$, and $c = (c_1, c_2, \cdots, c_n)$ such that $c_1, c_2, \cdots, c_n \in \mathbb{Z}_q$.*

*Moreover, for $s = 0$ the result becomes*

$$\widehat{f_{n,n}}(c) = \begin{cases} q^{\frac{n}{2}} w^v \eta(D), & \textit{if } p \equiv 1 \pmod 4 \\ q^{\frac{n}{2}} w^v \eta(D)\sqrt{-1}^n, & \textit{if } p \equiv 3 \pmod 4. \end{cases}$$

*Proof.* We use very similar arguments that we used previously to prove Theorem 3.5. So, we do not give much detail. For $c \in \mathbb{Z}_q$, we have the following fact using Lemma 3.6,

$$\widehat{f_{1,1}}(c) = \sum_{x\in\mathbb{Z}_q} w^{dx^2-cx} = \begin{cases} q^{1/2} w^{-c^2/4d} \eta(d), & \text{if } p \equiv 1 \pmod 4 \\ q^{1/2} w^{-c^2/4d} \eta(d)\sqrt{-1}, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

The Walsh spectrum of $f_{n,1}$ can be computed as,

$$\widehat{f_{n,1}}(c) = \begin{cases} q^{\frac{n+s}{2}} w^{-c_1^2/4d} \eta(d), & \text{if } p \equiv 1 \pmod 4 \text{ and } c_n = c_{n-1} = \cdots = c_2 = 0 \\ q^{\frac{n+s}{2}} w^{-c_1^2/4d} \eta(d)\sqrt{-1}, & \text{if } p \equiv 3 \pmod 4 \text{ and } c_n = c_{n-1} = \cdots = c_2 = 0 \\ 0, & \text{if otherwise.} \end{cases}$$

To obtain the general form, one can find some of the results as follows.

1.
$$\widehat{f_{2,2}}(c) = \sum_{x\in\mathbb{Z}_q^2} w^{f_{2,2}(x)-c\cdot x} = \sum_{x_1,x_2\in\mathbb{Z}_q} w^{d_1x_1^2+d_2x_2^2-c_1x_1-c_2x_2}$$

$$= \sum_{x_1\in\mathbb{Z}_q} w^{d_1x_1^2-c_1x_1} \sum_{x_2\in\mathbb{Z}_q} w^{d_2x_2^2-c_2x_2} = \begin{cases} qw^{-\frac{c_1^2}{4d_1}-\frac{c_2^2}{4d_2}} \eta(d_1d_2), & \text{if } p \equiv 1 \pmod 4 \\ qw^{-\frac{c_1^2}{4d_1}-\frac{c_2^2}{4d_2}} \eta(d_1d_2)\sqrt{-1}^2, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

2.

$$\widehat{f_{3,2}}(c) = \sum_{x\in\mathbb{Z}_q^3} w^{f_{3,2}(x)-c\cdot x} = \sum_{x_1,x_2,x_3\in\mathbb{Z}_q} w^{d_1x_1^2+d_2x_2^2-c_1x_1-c_2x_2-c_3x_3}$$

$$= \sum_{x_3\in\mathbb{Z}_q} w^{-c_3x_3} \sum_{x_1,x_2\in\mathbb{Z}_q} w^{d_1x_1^2+d_2x_2^2-c_1x_1-c_2x_2}$$

$$= \begin{cases} q^2 w^{-\frac{c_1^2}{4d_1}-\frac{c_2^2}{4d_2}}\eta(d_1d_2), & \text{if } p\equiv 1 \pmod 4 \text{ and } c_3=0 \\ q^2 w^{-\frac{c_1^2}{4d_1}-\frac{c_2^2}{4d_2}}\eta(d_1d_2)\sqrt{-1}^2, & \text{if } p\equiv 3 \pmod 4 \text{ and } c_3=0 \\ 0, & \text{if } c_3\neq 0. \end{cases}$$

3.

$$\widehat{f_{3,3}}(c) = \sum_{x\in\mathbb{Z}_q^3} w^{f_{3,3}(x)-c\cdot x} = \sum_{x_1,x_2,x_3\in\mathbb{Z}_q} w^{d_1x_1^2+d_2x_2^2+d_3x_3^2-c_1x_1-c_2x_2-c_3x_3}$$

$$= \sum_{x_1\in\mathbb{Z}_q} w^{d_1x_1^2-c_1x_1} \sum_{x_3\in\mathbb{Z}_q} w^{d_2x_2^2-c_2x_2} \sum_{x_3\in\mathbb{Z}_q} w^{d_3x_3^2-c_3x_3}$$

$$= \begin{cases} q^{3/2} w^{-\frac{c_1^2}{4d_1}-\frac{c_2^2}{4d_2}-\frac{c_3^2}{4d_3}}\eta(d_1d_2d_3), & \text{if } p\equiv 1 \pmod 4 \\ q^{3/2} w^{-\frac{c_1^2}{4d_1}-\frac{c_2^2}{4d_2}-\frac{c_3^2}{4d_3}}\eta(d_1d_2d_3)\sqrt{-1}^3, & \text{if } p\equiv 3 \pmod 4). \end{cases}$$

□

### 3.5 Walsh Spectrum of Quadratic Functions over $\mathbb{Z}_{p^m}$

**Lemma 3.8.** *Let $d \in \mathbb{Z}_q^\times$ and $c \in \mathbb{Z}_q$ for $q = p^m$. Let $\eta$ be the quadratic character of $\mathbb{Z}_q$. Then, the quadratic Gauss sum over $\mathbb{Z}_q$ is as follows.*

- *The Case $m$ is even: $\sum_{x\in\mathbb{Z}_q} w^{dx^2-cx} = q^{1/2}w^{-c^2/4d}$.*
- *The Case $m$ is odd:*

$$\sum_{x\in\mathbb{Z}_q} w^{dx^2-cx} = \begin{cases} w^{-c^2/4d}q^{1/2}\eta(d), & \text{if } p\equiv 1 \pmod 4 \\ w^{-c^2/4d}q^{1/2}\eta(d)\sqrt{-1}, & \text{if } p\equiv 3 \pmod 4). \end{cases}$$

*Proof.* In Lemma 3.4 and Lemma 3.6, we give detailed proofs for $m = 2$ and $m = 3$. Now, for simplicity, we continue to give detailed proofs for $m = 4$ and $m = 5$. Then, the generalizations get easier to understand.
A change of variables will be helpful. Hence we replace $x$ with $y + \alpha$ for $\alpha = c/2d$ to have

$$dx^2 - cx = d(y+\alpha)^2 - c(y+\alpha) = dy^2 + cy + \frac{c^2}{4d} - cy - \frac{c^2}{2d} = dy^2 - \frac{c^2}{4d}.$$

Assume that $m = 4$. Let $x \in \mathbb{Z}_{p^4}$. As we have
$\mathbb{Z}_q = \mathbb{Z}_{p^4} = \{a_0 + pa_1 + p^2a_2 + p^3a_3 : a_0, a_1, a_2, a_3 \in \mathbb{Z}_p\}$, there exist some $a_0, a_1, a_2, a_3 \in \mathbb{Z}_p$ such that

$$x^2 = a_0^2 + a_1^2p^2 + 2a_0a_1p + 2a_0a_2p^2 + 2a_0a_3p^3 + 2a_1a_2p^3 \pmod{p^4}.$$

$$\sum_{x\in\mathbb{Z}_{p^4}} e^{\frac{2\pi\sqrt{-1}(x^2)}{p^4}} = \sum_{a_0\in\mathbb{Z}_p} e^{\frac{2\pi\sqrt{-1}(a_0^2)}{p^4}} \sum_{a_1\in\mathbb{Z}_p} e^{\frac{2\pi\sqrt{-1}(a_1^2p^2+2a_0a_1p)}{p^4}} \sum_{a_2\in\mathbb{Z}_p} e^{\frac{2\pi\sqrt{-1}(2a_0a_2p^2+2a_1a_2p^3)}{p^4}} \sum_{a_3\in\mathbb{Z}_p} e^{\frac{2\pi\sqrt{-1}(2a_0a_3)}{p}}$$

$$= p \sum_{a_1\in\mathbb{Z}_p} e^{\frac{2\pi\sqrt{-1}(a_1^2p^2)}{p^4}} \sum_{a_2\in\mathbb{Z}_p} e^{\frac{2\pi\sqrt{-1}(2a_1a_2)}{p}} = p^2$$

To write the last two equalities, we used the following two facts, respectively.

$$\sum_{a_3\in\mathbb{Z}_p} e^{\frac{2\pi\sqrt{-1}(2a_0a_3)}{p}} = \begin{cases} p, & \text{if } a_0 = 0 \\ 0, & \text{if } a_0 \neq 0 \end{cases}$$

and

$$\sum_{a_2\in\mathbb{Z}_p} e^{\frac{2\pi\sqrt{-1}(2a_1a_2)}{p}} = \begin{cases} p, & \text{if } a_1 = 0 \\ 0, & \text{if } a_1 \neq 0. \end{cases}$$

Now, assume $m = 5$. Let $x \in \mathbb{Z}_{p^5}$. Then, there exists some $a_0, a_1, a_2, a_3, a_4 \in \mathbb{Z}_p$ such that $x = a_0 + a_1p + a_2p^2 + a_3p^3 + a_4p^4$. This implies,

$$x^2 = a_0^2+a_1^2p^2+a_2^2p^4+2a_0a_1p+2a_0a_2p^2+2a_0a_3p^3+2a_0a_4p^4+2a_1a_2p^3+2a_1a_3p^4 \pmod{p^5}$$

Let $A = a_1^2p^2 + 2a_0a_1p$, $B = 2a_0a_2p^2 + 2a_1a_2p^3 + a_2^2p^4$ and $C = 2a_0a_3p^3 + 2a_1a_3p^4$.

$$\sum_{x\in\mathbb{Z}_{p^5}} e^{\frac{2\pi\sqrt{-1}(x^2)}{p^5}} = \sum_{a_0\in\mathbb{Z}_p} e^{\frac{2\pi\sqrt{-1}(a_0^2)}{p^5}} \sum_{a_1\in\mathbb{Z}_p} e^{\frac{2\pi\sqrt{-1}A}{p^5}} \sum_{a_2\in\mathbb{Z}_p} e^{\frac{2\pi\sqrt{-1}B}{p^5}} \sum_{a_3\in\mathbb{Z}_p} e^{\frac{2\pi\sqrt{-1}C}{p^5}} \sum_{a_4\in\mathbb{Z}_p} e^{\frac{2\pi\sqrt{-1}(2a_0a_4)}{p}}$$

$$= p \sum_{a_1\in\mathbb{Z}_p} e^{\frac{2\pi\sqrt{-1}(a_1^2)}{p^3}} \sum_{a_2\in\mathbb{Z}_p} e^{\frac{2\pi\sqrt{-1}(a_2^2)}{p}} \sum_{a_3\in\mathbb{Z}_p} e^{\frac{2\pi\sqrt{-1}(2a_1a_3)}{p}} = p^2 \sum_{a_2\in\mathbb{Z}_p} e^{\frac{2\pi\sqrt{-1}(a_2^2)}{p}}$$

Using [13, Theorem 5.33], the definition of the Gauss sum over finite fields with $p$ elements, and considering the fact that $d \in \mathbb{Z}_{p^5}^{\times}$, we have

$$\sum_{x\in\mathbb{Z}_{p^5}} e^{\frac{2\pi\sqrt{-1}(dx^2)}{p^5}} = p^2 \sum_{a_2\in\mathbb{Z}_p} e^{\frac{2\pi\sqrt{-1}(da_2^2)}{p}} = \begin{cases} p^{5/2}\eta(d), & \text{if } p \equiv 1 \pmod 4 \\ p^{5/2}\eta(d)\sqrt{-1}, & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

where $\eta$ is the quadratic character of $\mathbb{Z}_p$.
Now, let $x \in \mathbb{Z}_q = \mathbb{Z}_{p^m}$. As $\mathbb{Z}_{p^m} = \{a_0 + pa_1 + \cdots + p^{m-1}a_{m-1} : a_0, a_1, \cdots, a_{m-1} \in \mathbb{Z}_p\}$, there exist $a_0, a_1, \cdots, a_{m-1} \in \mathbb{Z}_p$ such that $x = a_0 + a_1p + a_2p^2 + \cdots + a_{m-1}p^{m-1}$.

$$x^2 = \sum_{i=0}^{\frac{m}{2}-1} \left(a_ip^i\right)^2 + 2p(a_0a_1) + 2p^2(a_0a_2) + 2p^3(a_0a_3 + a_1a_2) + 2p^4(a_0a_4 + a_1a_3) +$$

$+2p^5(a_0a_5+a_1a_4+a_3a_2)+\cdots+2p^{m-1}(a_0a_{m-1}+a_1a_{m-2}+\cdots+a_{\frac{m}{2}-1}a_{\frac{m}{2}}) \pmod{p^m}\cdots(*)$

There are two cases depending on $m$.

1. Assume $m$ is even. Then, the sum $(*)$ does not include the square of the summands $a_i$ such that $i \geq m/2$. The result is $q^{1/2}$, since we get $p$ as a factor for each of these summands.
2. Assume $m$ is odd. Note that, for each of the $(\frac{m-1}{2})$-many summands which do not appear in $(*)$, we get $p$ as a factor. [13, Theorem 5.33] and the definition of the Gauss sum over finite fields with $p$ elements leads to the following result.

$$\sum_{x\in\mathbb{Z}_q} w^{dx^2-cx} = \begin{cases} w^{-c^2/4d}q^{1/2}\eta(d), & \text{if } p \equiv 1 \pmod 4 \\ w^{-c^2/4d}q^{1/2}\eta(d)\sqrt{-1}, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

□

**Theorem 3.9.** *Let $q = p^m$ and $m$ be an even integer. Let $f_{n,n-s} : \mathbb{Z}_q^n \to \mathbb{Z}_q$ be defined by $f_{n,n-s}(x_1, x_2, \cdots, x_n) := d_1x_1^2 + d_2x_2^2 + ... + d_{n-s}x_{n-s}^2$ for $d_1, d_2, \cdots, d_{n-s} \in \mathbb{Z}_q^\times$. Then, for a positive integer $s$ such that $0 < s \leq n-1$ and $c = (c_1, c_2, \cdots, c_n)$ with $c_1, c_2, \cdots, c_n \in \mathbb{Z}_q$ we have,*

$$\widehat{f_{n,n-s}}(c) = \begin{cases} q^{\frac{n+s}{2}} w^{-\frac{c_1^2}{4d_1}-\frac{c_2^2}{4d_2}-\cdots\frac{c_{n-s}^2}{4d_{n-s}}}, & \textit{if } c_n = c_{n-1} = \cdots = c_{n-s+1} = 0 \\ 0, & \textit{if otherwise}. \end{cases}$$

*Moreover, for $s = 0$, the result is simply $\widehat{f_{n,n}}(c) = q^{\frac{n}{2}} w^{-\frac{c_1^2}{4d_1}-\frac{c_2^2}{4d_2}-\cdots\frac{c_n^2}{4d_n}}$.*

*Proof.* By Lemma 3.8, we have

$$\widehat{f_{1,1}^d}(c) = \sum_{x\in\mathbb{Z}_q} w^{dx^2-cx} = w^{-c^2/4d}p^{m/2} = w^{-c^2/4d}q^{1/2}.$$

Realize that, this assertion is exactly the same with the one in the proof of Theorem 3.5. Applying the same method, the result can be achieved, easily.

□

**Theorem 3.10.** *Let $q = p^m$ and $m$ be an odd integer. Let $f_{n,n-s} : \mathbb{Z}_q^n \to \mathbb{Z}_q$ be defined by $f_{n,n-s}(x_1, x_2, \cdots, x_n) := d_1x_1^2 + d_2x_2^2 + ... + d_{n-s}x_{n-s}^2$ for $d_1, d_2, \cdots, d_{n-s} \in \mathbb{Z}_q^\times$. Let $\eta$ be the quadratic character of $\mathbb{Z}_q$. Then, for a positive integer $s$ such that $0 < s \leq n-1$ and $c = (c_1, c_2, \cdots, c_n)$ such that $c_1, c_2, \cdots, c_n \in \mathbb{Z}_q$ we have,*

$$\widehat{f_{n,n-s}}(c) = \begin{cases} q^{\frac{n+s}{2}} w^v \eta(D), & \textit{if } p \equiv 1 \pmod 4 \textit{ and } c_n = c_{n-1} = \cdots = c_{n-s+1} = 0 \\ q^{\frac{n+s}{2}} w^v \eta(D)\sqrt{-1}^{n-s}, & \textit{if } p \equiv 3 \pmod 4 \textit{ and } c_n = c_{n-1} = \cdots = c_{n-s+1} = 0 \\ 0, & \textit{if otherwise}, \end{cases}$$

*where* $D = d_1 d_2 \cdots d_{n-s}$ *and* $v = -\frac{c_1^2}{4d_1} - \frac{c_2^2}{4d_2} - \cdots \frac{c_{n-s}^2}{4d_{n-s}}$*.*

*Moreover, for* $s = 0$ *the result becomes*

$$\widehat{f_{n,n}}(c) = \begin{cases} q^{\frac{n}{2}} w^v \eta(D), & \textit{if } p \equiv 1 \pmod 4 \\ q^{\frac{n}{2}} w^v \eta(D)\sqrt{-1}^n, & \textit{if } p \equiv 3 \pmod 4). \end{cases}$$

*Proof.* Using Lemma 3.8, we have the following,

$$\widehat{f_{1,1}^d}(c) = \sum_{x \in \mathbb{Z}_q} w^{dx^2 - cx} = \begin{cases} w^{-c^2/4d} q^{1/2} \eta(d), & \text{if } p \equiv 1 \pmod 4) \\ w^{-c^2/4d} q^{1/2} \eta(d)\sqrt{-1}, & \text{if } p \equiv 3 \pmod 4). \end{cases}$$

Then, the result can be achieved by following the steps given in proof of Theorem 3.7.

□

**Lemma 3.11.** *Let* $f_u : \mathbb{Z}_q^n \to \mathbb{Z}_q$ *be defined by* $f_u(x_1, x_2, ..., x_n) = d_1^u x_1^2 + d_2^u x_2^2 + ... + d_{n-1}^u x_{n-1}^2 + u x_n$*, where* $u \in \mathbb{Z}_q$ *and* $d_i^u \in \mathbb{Z}_q^\times$ *for* $1 \le i \le n-1$*. Then, the set* $\{f_u(x) : u \in \mathbb{Z}_q\}$ *gives a set of near-bent functions having pairwise disjoint support of Walsh transforms.*

*Proof.* By Theorem 3.9 and Theorem 3.10, $f_u$ is a near-bent function. Note that, adding a linear term to a near-bent function, it will again be a near-bent function. Let $c = (c_1, c_2, ..., c_n) \in \mathbb{Z}_q^n$.

$$\widehat{f_u}(c) = \sum_{x \in \mathbb{Z}_q^n} w^{f_u(x) - c \cdot x} = \sum_{x_1, ... x_n \in \mathbb{Z}_q} w^{(d_1^u x_1^2 + d_2^u x_2^2 + ... + d_{n-1}^u x_{n-1}^2 + u x_n) - c_1 x_1 - \cdots - c_n x_n}$$

$$= \sum_{x_1, ... x_{n-1} \in \mathbb{Z}_q} w^{(d_1^u x_1^2 + d_2^u x_2^2 + \cdots + d_{n-1}^u x_{n-1}^2) - c_1 x_1 - \cdots - c_{n-1} x_{n-1}} \sum_{x_n \in \mathbb{Z}_q} w^{u x_n - c_n x_n}.$$

The first sum in this product is nonzero by Theorem 3.9 and Theorem 3.10. So, only the second sum, $\sum_{x_n \in \mathbb{Z}_q} w^{u x_n - c_n x_n}$, can make this product zero. If $u x_n - c_n x_n$ is nonzero, then the sum is zero. Hence, we have

$$supp(\widehat{f_u}) = \left\{ c = (c_1, c_2, \cdots, c_n) \in \mathbb{Z}_q^n : u \equiv c_n \pmod q) \right\},$$

which gives $supp(\widehat{f_i}) \cap supp(\widehat{f_j})$ is empty, for $i, j \in \mathbb{Z}_q$ and $i \neq j$.

□

### 3.6 An Application on Quadratic Functions

In this section, we give an application of the study of this chapter on quadratic functions. In Theorem 3.9 and Theorem 3.10, we determine the Walsh spectrum of certain quadratic functions. Using these theorems, we can obtain necessary number of near-bent functions with desired properties to construct bent functions by Theorem 3.3. We also give a simple technique to determine whether the constructed bent functions using these quadratic near-bent functions are regular, weakly regular or non-weakly regular.
Let $f_u : \mathbb{Z}_q^n \to \mathbb{Z}_q$ be defined by $f_u(x_1, x_2, ..., x_n) = d_1^u x_1^2 + d_2^u x_2^2 + ... + d_{n-1}^u x_{n-1}^2 + u x_n$, where $u \in \mathbb{Z}_q$ and $d_i^u \in \mathbb{Z}_q^\times$ for $1 \leq i \leq n-1$. Let $F : \mathbb{Z}_q^{n+1} \to \mathbb{Z}_q$ be the bent function constructed by Theorem 3.3 using these near-bent functions. Recall that, for each $a \in \mathbb{Z}_q^n$, there exists exactly unique $u$ such that $\left|\widehat{F}(a,b)\right| = \left|\widehat{f_u}(a)\right|$. So, it is enough to observe the Fourier coefficients of $\widehat{f_u}$, for $0 \leq u \leq q-1$, to determine whether $F$ is weakly regular or not.

#### 3.6.1 A Classification of the Constructed Bent Functions When $m$ is Even

Let $q = p^m$ such that $m$ is even. By Theorem 3.9, $spec(f_u) = \left\{0, q^{n+1/2} w^{\tilde{f}(c)}\right\}$ where $\tilde{f}$ is the function from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q$ and $c \in \mathbb{Z}_q^n$. For this case, all constructed bent functions using Theorem 3.3 are regular by the first item of Definition 1.12.

#### 3.6.2 A Classification of the Constructed Bent Functions When $m$ is Odd

Let $q = p^m$ such that $m$ is odd. Then, by Theorem 3.10,

$$spec\,(f_u) = \begin{cases} \left\{0, q^{\frac{n+1}{2}} \eta(D_u) w^{\tilde{f}(c)}\right\}, & \text{if } p \equiv 1 \pmod 4 \\ \left\{0, q^{\frac{n+1}{2}} w^{\tilde{f}(c)} \eta(D_u) \sqrt{-1}^{\,n-1}\right\}, & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

where $D_u = d_1^u d_2^u \cdots d_{n-1}^u$, $\tilde{f}$ is the function from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q$ and $c \in \mathbb{Z}_q^n$.

**The Case $p \equiv 1 \pmod 4$:**

- $\eta(D_u) = 1$ for all $u \in \mathbb{Z}_q \Rightarrow F$ is a regular bent function.
- $\eta(D_u) = -1$ for all $u \in \mathbb{Z}_q \Rightarrow F$ is a weakly regular bent function.
- $\eta(D_u)$ attains both of the values $\{-1, 1\} \Rightarrow F$ is a non-weakly regular bent function.

**The Case** $p \equiv 3 \pmod 4$**:**

1. Assume $n-1 \equiv 0 \pmod 4$.
   - $\eta(D_u) = 1$ for all $u \in \mathbb{Z}_q \Rightarrow F$ is a regular bent function.
   - $\eta(D_u) = -1$ for all $u \in \mathbb{Z}_q \Rightarrow F$ is a weakly regular bent function.
   - $\eta(D_u)$ attains both of the values $\{-1, 1\} \Rightarrow F$ is a non-weakly regular bent function.
2. Assume $n-1 \equiv 2 \pmod 4$.
   - $\eta(D_u) = -1$ for all $u \in \mathbb{Z}_q \Rightarrow F$ is a regular bent function.
   - $\eta(D_u) = 1$ for all $u \in \mathbb{Z}_q \Rightarrow F$ is a weakly regular bent function.
   - $\eta(D_u)$ attains both of the values $\{-1, 1\} \Rightarrow F$ is a non-weakly regular bent function.
3. Assume $n-1 \equiv 1 \pmod 4$ or $n-1 \equiv 3 \pmod 4$.
   - No regular bent function is constructed.
   - $\eta(D_u) = 1$ for all $u \in \mathbb{Z}_q$ or $\eta(D_u) = -1$ for all $u \in \mathbb{Z}_q$ implies that $F$ is a weakly regular bent function.
   - $\eta(D_u)$ attains both of the values $\{-1, 1\} \Rightarrow F$ is a non-weakly regular bent function.

*Remark* 3.3. Great majority of the constructed bent functions using Theorem 3.3 are non-weakly regular. As $p$ and $m$ get greater, the percentage of non-weakly regular bent functions increases.

**Example 3.3.** For $u \in \{0, 1, \cdots, 26\}$, let $f_u : \mathbb{Z}_{27}^5 \to \mathbb{Z}_{27}$ be near-bent functions defined as

$$f_u(x_1, x_2, x_3, x_4, x_5) = d_1^u x_1^2 + d_2^u x_2^2 + d_3^u x_3^2 + d_4^u x_4^2 + u x_5,$$

where $d_1^u, d_2^u, d_3^u, d_4^u \in \mathbb{Z}_{27}^{\times}$.
The set of quadratic residues of $\mathbb{Z}_{27}^{\times}$ is $QR := \{1, 4, 7, 10, 13, 16, 19, 22, 25\}$ and the set of quadratic non-residues of $\mathbb{Z}_{27}^{\times}$ is $QnR := \{2, 5, 8, 11, 14, 17, 20, 23, 26\}$. Let $h_u$ be functions defined from $\mathbb{Z}_{27}$ to $\mathbb{Z}_{27}$ such that,

$$h_u(y) = \begin{cases} 1, & \text{if } y = u \\ 0, & \text{if otherwise.} \end{cases}$$

Let $F : \mathbb{Z}_{27}^5 \times Z_{27} \to \mathbb{Z}_{27}$ be defined by $F(x, y) = \sum_{u=0}^{26} f_u(x) h_u(y)$. Then, by Theorem 3.3, $F$ is a bent function.

- For each $u$, if even number of $\{d_1^u, d_2^u, d_3^u, d_4^u\}$ are chosen from the set QnR, then $F$ is a regular bent function.
- For each $u$, if odd number of $\{d_1^u, d_2^u, d_3^u, d_4^u\}$ are chosen from the set QnR, then $F$ is a weakly regular bent function.

- If at least for one $u$, odd number of $\{d_1^u, d_2^u, d_3^u, d_4^u\}$ are chosen from the set QnR and at least for one $u$, even number of $\{d_1^u, d_2^u, d_3^u, d_4^u\}$ are chosen from the set QnR, then $F$ is a non-weakly regular bent function.

To be more clear, we will give some numerical illustrations.

1. For $u \in \mathbb{Z}_{27}$ if we choose $f_u$ as in the following way, then $F$ is a weakly regular bent function.

$$\begin{aligned}
f_0(x) &= 5x_1^2 + 2x_2^2 + 7x_3^2 + 8x_4^2 \\
f_1(x) &= 4x_1^2 + 10x_2^2 + 7x_3^2 + 2x_4^2 + x_5 \\
f_2(x) &= x_1^2 + 23x_2^2 + 2x_3^2 + 2x_4^2 + 2x_5 \\
f_3(x) &= x_1^2 + 17x_2^2 + x_3^2 + x_4^2 + 3x_5 \\
f_4(x) &= x_1^2 + 10x_2^2 + 8x_3^2 + 22x_4^2 + 4x_5 \\
f_5(x) &= 11x_1^2 + 8x_2^2 + 5x_3^2 + 4x_4^2 + 5x_5 \\
f_6(x) &= 2x_1^2 + 4x_2^2 + 5x_3^2 + 8x_4^2 + 6x_5 \\
f_7(x) &= 2x_1^2 + 8x_2^2 + 20x_3^2 + 7x_4^2 + 7x_5 \\
f_8(x) &= x_1^2 + 4x_2^2 + 7x_3^2 + 2x_4^2 + 8x_5 \\
f_9(x) &= 8x_1^2 + x_2^2 + 4x_3^2 + 4x_4^2 + 9x_5 \\
f_{10}(x) &= 11x_1^2 + 14x_2^2 + x_3^2 + 2x_4^2 + 10x_5 \\
f_{11}(x) &= 2x_1^2 + 2x_2^2 + 4x_3^2 + 2x_4^2 + 11x_5 \\
f_{12}(x) &= x_1^2 + 10x_2^2 + 8x_3^2 + x_4^2 + 12x_5
\end{aligned}$$

$$\begin{aligned}
f_{13}(x) &= 2x_1^2 + 16x_2^2 + 2x_3^2 + 17x_4^2 + 13x_5 \\
f_{14}(x) &= 2x_1^2 + 19x_2^2 + 13x_3^2 + x_4^2 + 14x_5 \\
f_{15}(x) &= 25x_1^2 + 22x_2^2 + x_3^2 + 26x_4^2 + 15x_5 \\
f_{16}(x) &= 26x_1^2 + 2x_2^2 + 5x_3^2 + x_4^2 + 16x_5 \\
f_{17}(x) &= x_1^2 + 25x_2^2 + x_3^2 + 23x_4^2 + 17x_5 \\
f_{18}(x) &= 20x_1^2 + 11x_2^2 + 8x_3^2 + 19x_4^2 + 18x_5 \\
f_{19}(x) &= x_1^2 + 13x_2^2 + 22x_3^2 + 14x_4^2 + 19x_5 \\
f_{20}(x) &= 10x_1^2 + 17x_2^2 + 14x_3^2 + 14x_4^2 + 20x_5 \\
f_{21}(x) &= 7x_1^2 + 7x_2^2 + 7x_3^2 + 8x_4^2 + 21x_5 \\
f_{22}(x) &= 7x_1^2 + 5x_2^2 + 5x_3^2 + 5x_4^2 + 22x_5 \\
f_{23}(x) &= 4x_1^2 + 23x_2^2 + 2x_3^2 + 23x_4^2 + 23x_5 \\
f_{24}(x) &= 5x_1^2 + 4x_2^2 + 13x_3^2 + 22x_4^2 + 24x_5 \\
f_{25}(x) &= x_1^2 + 11x_2^2 + 20x_3^2 + 26x_4^2 + 25x_5 \\
f_{26}(x) &= 23x_1^2 + 25x_2^2 + 11x_3^2 + 2x_4^2 + 26x_5
\end{aligned}$$

2

2. For $u \in \mathbb{Z}_{27}$ if we choose $f_u$ as in the following way, then $F$ is a non-weakly regular bent function.

$$\begin{aligned}
f_0(x) &= x_1^2 + x_2^2 + 2x_3^2 + 7x_4^2 \\
f_1(x) &= 4x_1^2 + x_2^2 + 8x_3^2 + x_4^2 + x_5 \\
f_2(x) &= x_1^2 + x_2^2 + x_3^2 + x_4^2 + 2x_5 \\
f_3(x) &= x_1^2 + 10x_2^2 + 11x_3^2 + 20x_4^2 + 3x_5 \\
f_4(x) &= x_1^2 + x_2^2 + x_3^2 + x_4^2 + 4x_5 \\
f_5(x) &= 2x_1^2 + 5x_2^2 + 23x_3^2 + x_4^2 + 5x_5 \\
f_6(x) &= 10x_1^2 + 11x_2^2 + 14x_3^2 + 23x_4^2 + 6x_5
\end{aligned}$$

$$\begin{aligned}
f_7(x) &= 23x_1^2 + 4x_2^2 + 5x_3^2 + 4x_4^2 + 7x_5 \\
f_8(x) &= 7x_1^2 + 7x_2^2 + 7x_3^2 + 7x_4^2 + 8x_5 \\
f_9(x) &= 4x_1^2 + x_2^2 + x_3^2 + 2x_4^2 + 9x_5 \\
f_{10}(x) &= 5x_1^2 + 26x_2^2 + x_3^2 + x_4^2 + 10x_5 \\
f_{11}(x) &= x_1^2 + x_2^2 + 11x_3^2 + 14x_4^2 + 11x_5 \\
f_{12}(x) &= 2x_1^2 + 4x_2^2 + 8x_3^2 + 16x_4^2 + 12x_5 \\
f_{13}(x) &= x_1^2 + 5x_2^2 + 7x_3^2 + 11x_4^2 + 13x_5 \\
f_{14}(x) &= 13x_1^2 + 17x_2^2 + 19x_3^2 + 23x_4^2 + 14x_5 \\
f_{15}(x) &= 26x_1^2 + x_2^2 + x_3^2 + 2x_4^2 + 15x_5
\end{aligned}$$

$$f_{16}(x) = 11x_1^2+2x_2^2+16x_3^2+22x_4^2+16x_5$$
$$f_{17}(x) = 22x_1^2 + x_2^2 + x_3^2 + x_4^2 + 17x_5$$
$$f_{18}(x) = x_1^2 + x_2^2 + x_3^2 + x_4^2 + 18x_5$$
$$f_{19}(x) = x_1^2+20x_2^2+7x_3^2+4x_4^2+19x_5$$
$$f_{20}(x) = 2x_1^2+22x_2^2+16x_3^2+5x_4^2+20x_5$$
$$f_{21}(x) = 4x_1^2+x_2^2+13x_3^2+4x_4^2+21x_5$$
$$f_{22}(x) = x_1^2+11x_2^2+11x_3^2+x_4^2+22x_5$$
$$f_{23}(x) = 17x_1^2+x_2^2+13x_3^2+x_4^2+23x_5$$
$$f_{24}(x) = x_1^2 + x_2^2 + 17x_3^2 + x_4^2 + 24x_5$$
$$f_{25}(x) = 16x_1^2+19x_2^2+19x_3^2+22x_4^2+25x_5$$
$$f_{26}(x) = 11x_1^2+17x_2^2+22x_3^2+23x_4^2+26x_5$$

2

*Remark* 3.4. In Example 3.3, by different choices of $f_u$, we can construct

- $(8 \times 9^4)^{27}$ many regular bent functions.
- $(8 \times 9^4)^{27}$ many weakly regular bent functions.
- $(16 \times 9^4)^{27} - 2\,(8 \times 9^4)^{27}$ many regular bent functions.

# CHAPTER 4

# A TECHNIQUE TO OBTAIN WEAKLY AND NON-WEAKLY REGULAR BENT FUNCTIONS USING $S$-PLATEAUED FUNCTIONS

## 4.1 Introduction

A method to construct regular and (non)-weakly regular bent functions over the ring of integers modulo $p^m$ using near-bent functions is given in Chapter 3. Note that, near-bent functions are 1-plateaued functions, indeed. In this chapter, we broaden this study such that it uses $s$-plateaued functions for a positive integer $s > 1$. For this purpose, the number of functions to produce a bent function is increased but there is no problem to obtain that number of $s$-plateaued functions.
One of the most important differences of this construction to the one in Theorem 3.3 is that the dimension increases by $s$, instead of 1.

In Section 4.2, we explain how to achieve $s$-plateaued functions with pairwise disjoint support of Walsh transforms and give a method of construction of bent functions using these $s$-plateaued functions. Also, we prove that the function $h_u$ that is used for construction, cannot be represented in a polynomial form.
Section 4.3 studies an application of the construction method using quadratic $s$-plateaued functions. Moreover, a technique is given to classify the bent functions as regular, weakly regular and non-weakly regular.

## 4.2 A Construction of Bent Functions Using $s$-Plateaued functions

In this section, our aim is to expand the method that is given in Theorem 3.3. Recall that, in that theorem, we indicate a method that constructs a bent function using a determined number of 1-plateaued functions, namely near-bent functions. Now, we aim to construct a bent function using $s$-plateaued functions for a positive number $s$ greater than 1.
The idea is to construct a bent function, $F$, by combining the $s$-plateaued functions in such a way that Walsh spectrum of $F$ do not have zero value. This can be achieved by combining the $s$-plateaued functions having no common element in supports of their

Walsh transforms and the union of their support of Walsh transforms should be $\mathbb{Z}_q^n$.

**Theorem 4.1.** *Let $s$ be a positive integer and $u \in \mathbb{Z}_{q^s}$ such that $u = u_1 q^{s-1} + u_2 q^{s-2} + \cdots + u_s$ with $u_i \in \mathbb{Z}_q$. For each $u \in \mathbb{Z}_{q^s}$, let $f_u$ be an $s$-plateaued function defined from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q$. Assume, $supp(\widehat{f_u}) \cap supp(\widehat{f_v})$ is empty for $u, v \in \mathbb{Z}_{q^s}$ and $u \neq v$.*

*Then, the function $F : \mathbb{Z}_q^n \times \mathbb{Z}_q^s \to \mathbb{Z}_q$ defined by*

$$F(x, y_1, y_2, \cdots, y_s) = \sum_{u \in \mathbb{Z}_{q^s}} h_u(y_1, y_2, \cdots, y_s) f_u(x),$$

*is bent where $h_u$ is function defined from $\mathbb{Z}_q^s$ to $\mathbb{Z}_q$ and given by,*

$$h_u(y_1, y_2, \cdots, y_s) = \begin{cases} 1, & \textit{if } u = y_1 q^{s-1} + y_2 q^{s-2} + \cdots + y_s \\ 0, & \textit{if otherwise.} \end{cases}$$

*Proof.* Recall that, a special case of Parseval's identity is computed for the proof of Theorem 3.3. Hence, for $c \in \mathbb{Z}_q^n$ we have,

$$\sum_{c \in \mathbb{Z}_q^n} \left| \widehat{f_u}(c) \right|^2 = \begin{cases} q^{2n}, & \text{if } x = y \\ 0, & \text{if } x \neq y. \end{cases}$$

Then, we have

$$\sum_{c \in \mathbb{Z}_q^n} \left| \widehat{f_u}(c) \right|^2 = \left| supp(\widehat{f_u}) \right| q^{n+s} = q^{2n},$$

since $\left| \widehat{f_u}(c) \right| = 0$ or $q^{n+s/2}$ for all $c \in \mathbb{Z}_q^n$. So, $\left| supp(\widehat{f_u}) \right| = q^{n-s}$. Therefore, the number of $s$-plateaued functions that is needed to construct a bent function is $q^s$.

Let $(a, b) \in \mathbb{Z}_q^n \times \mathbb{Z}_q^s$. Then,

$$\widehat{F}(a, b) = \sum_{x \in \mathbb{Z}_q^n, y \in \mathbb{Z}_q^s} w^{F(x,y) - a\cdot x - b\cdot y} = \sum_{y \in \mathbb{Z}_q^s} w^{-b\cdot y} \sum_{x \in \mathbb{Z}_q^n} w^{F(x,y) - a\cdot x}$$

$$= \sum_{y \in \mathbb{Z}_q^s} w^{-b\cdot y} \sum_{x \in \mathbb{Z}_q^n} w^{\sum_{u \in \mathbb{Z}_{q^s}} h_u(y) f_u(x) - a\cdot x} =$$

$$= \sum_{y \in \mathbb{Z}_q^s} w^{-b\cdot y} \sum_{x \in \mathbb{Z}_q^n} w^{\left(h_0(y) f_0(x) + \cdots + h_{q^s-1}(y) f_{q^s-1}(x)\right) - a\cdot x} = \sum_{y \in \mathbb{Z}_q^s} w^{-b\cdot y} \widehat{f_{y'}}(a),$$

where $\acute{y} = y_1 q^{s-1} + y_2 q^{s-2} + \cdots + y_s$ for $y = (y_1, y_2, \cdots, y_s)$ and each $y_i \in \mathbb{Z}_q$. Since $supp(\widehat{f_i}) \cap supp(\widehat{f_j})$ is empty and $\bigcup_{i \in \mathbb{Z}_q} supp(\widehat{f_i}) = \mathbb{Z}_q^n$, each $a$ is an element of exactly one $\widehat{f_{\acute{y}}}$. So, we have

$$\left|\widehat{F}(a,b)\right| = \left|\sum_{y\in\mathbb{Z}_q^s} w^{-b\cdot y}\widehat{f_{\acute{y}}}(a)\right| = \left|w^{-b\cdot y}\widehat{f_{\acute{y}}}(a)\right| = q^{\frac{n+s}{2}}.$$

□

To apply Theorem 4.1 on quadratic functions, we need $q$-many quadratic $s$-plateaued functions with pairwise disjoint support of Walsh transforms and the union of their Walsh transforms is $\mathbb{Z}_q^n$. In Chapter 3, we determine the Walsh spectrum of certain quadratic functions from $\mathbb{Z}_q^n$ to $\mathbb{Z}_q$. These quadratic functions can be shown to be $s$-plateaued functions.The Walsh spectrum depends heavily on whether $m$ is even or odd (see Theorem 3.9 and Theorem 3.10). The following Lemma 4.2 is given to seperate the Walsh spectrum of these quadratic $s$-plateaued functions.

**Lemma 4.2.** *For $n \geq 2$, $n > s > 0$, and $m \geq 1$, let $d_1^u, d_2^u, \cdots, d_{n-s}^u \in \mathbb{Z}_q^\times$. For $u \in \mathbb{Z}_{q^s}$, we consider the correponding uniquely determined elements $u_1, u_2, \cdots, u_s \in \mathbb{Z}_q$ with $u = u_1q^{s-1} + u_2q^{s-2} + \cdots + u_s$ and we define the function $f_u : \mathbb{Z}_q^n \to \mathbb{Z}_q$ by,*

$$f_u(x_1, x_2, ..., x_n) = d_1^u x_1^2 + d_2^u x_2^2 + ... + d_{n-s}^u x_{n-s}^2 + u_1x_{n-s+1} + u_2x_{n-s+2} + \cdots + u_sx_n.$$

*For $u, v \in \mathbb{Z}_{q^s}$ with $u \neq v$, the supports of the Walsh transforms of $f_u$ and $f_v$ are disjoint.*

*Proof.* Using the method of the proof of Lemma 3.11, we obtain that,

$$\widehat{f_u}(c_1, c_2, \cdots, c_n) \neq 0 \Leftrightarrow (c_{n-s+1}, c_{n-s+2}, \cdots c_n) = (u_1, u_2, \cdots, u_s).$$

Therefore, the supports of the Walsh transforms of $f_u$ and $f_v$ intersect if and only if there exists $(c_1, c_2, \cdots, c_n) \in \mathbb{Z}_q^n$ with,

$$(c_{n-s+1}, c_{n-s+2}, \cdots c_n) = (u_1, u_2, \cdots, u_s) = (v_1, v_2, \cdots, v_s),$$

which is not possible as $(u_1, u_2, \cdots, u_s) \neq (v_1, v_2, \cdots, v_s)$. □

Using Lemma 4.2, we can easily obtain necessary number of quadratic $s$-plateaued functions with desired properties in order to construct bent functions using Theorem 4.1 which is a generalization of Theorem 3.3. In Theorem 3.3, we use the idea of Lagrange interpolation and explain that the coefficients used for the interpolation cannot be represented as polynomials using the paper of Carlitz [2]. The same study is valid for this case. In the following Proposition 4.3, we show that the function that is used for the construction in Theorem 4.1 cannot be representible as a polynomial.

**Proposition 4.3.** *For $u \in \mathbb{Z}_{q^s}$, let $h_u$ be a function defined from $\mathbb{Z}_q^s$ to $\mathbb{Z}_q$ and given by,*

$$h_u(x_1, x_2, \cdots, x_s) = \begin{cases} a, & \textit{if } u = x_1 q^{s-1} + x_2 q^{s-2} + \cdots + x_s \\ 0, & \textit{if otherwise}, \end{cases}$$

*where $a \not\equiv 0 \pmod{p}$. Then, $h_u$, cannot be represented in a polynomial form.*

*Proof.* In Proposition 3.1, we have shown this for $s = 1$ using the arguments in [2]. The generalization can be achieved easily. □

### 4.3 Examples and Classification of the Constructed Bent Functions

In this section, we give an application of Theorem 4.1 on certain quadratic functions. For this purpose, we use the functions and their Walsh spectrums that are given in Theorem 3.10 and Theorem 3.9. Then, we show how to classify the constructed functions as regular, weakly regular and non-weakly regular bent functions. The notation given as follows is valid for the whole section. For a positive integer $s$ such that $n > s > 0$, let $f_u : \mathbb{Z}_q^n \to \mathbb{Z}_q$ be defined by

$$f_u(x_1, x_2, ..., x_n) = d_1^u x_1^2 + d_2^u x_2^2 + ... + d_{n-s}^u x_{n-s}^2 + u_1 x_{n-s+1} + u_2 x_{n-s+2} + \cdots + u_s x_n,$$

where $u = u_1 q^{s-1} + u_2 q^{s-2} + \cdots + u_s$ for $u_1, u_2, \cdots u_s \in \mathbb{Z}_q$ and $d_1^u, d_2^u, \cdots d_{n-s}^u \in \mathbb{Z}_q^{\times}$. Then, by Theorem 3.9 and Theorem 3.10, $f_u$ is an $s$-plateaued function. Note that, if we add a linear term to an $s$-plateaued function, it will again be an $s$-plateaued function.
Also, by Lemma 4.2 the set $\{f_u(x) : u \in \mathbb{Z}_{q^s}\}$ consists of $s$-plateaued functions having pairwise disjoint support of Walsh transforms.
Let $F : \mathbb{Z}_q^{n+s} \to \mathbb{Z}_q$ be the bent function constructed by Theorem 4.1 using these functions. According to the last part of the proof of Theorem 4.1, for each $a \in \mathbb{Z}_q^n$, there exists exactly unique $u$ such that $\left|\widehat{F}(a, b)\right| = \left|\widehat{f_u}(a)\right|$. Thus, it is enough to observe the Fourier coefficients of $f_u$ in order to determine whether $F$ is regular, weakly regular or non-weakly regular.

*Remark* 4.1. Let $m$ be **even**. According to Theorem 3.9, $spec(f_u) = \left\{0, q^{n+s/2} w^v\right\}$ for $v \in \mathbb{Z}_q$. This gives all the constructed bent functions using $f_u$ are regular by the first item of Definition 1.12.

*Remark* 4.2. Let $m$ be **odd** and $p \equiv 1 \pmod{4}$. Then, by Theorem 3.10, $spec\,(f_u) = \left\{q^{\frac{n+s}{2}} \eta(D_u) w^v\right\}$, for $v \in \mathbb{Z}_q$ and $D_u = d_1^u d_2^u \cdots d_{n-s}^u$. Let $F : \mathbb{Z}_q^{n+s} \to \mathbb{Z}_q$ be the bent function constructed by Theorem 4.1 using $f_u$ for $u \in \mathbb{Z}_{q^s}$. Then, using Definition 1.12,

- $\eta(D_u) = 1$ for all $u \in \mathbb{Z}_{q^s} \Rightarrow F$ is a regular bent function.

- $\eta(D_u) = -1$ for all $u \in \mathbb{Z}_{q^s} \Rightarrow F$ is a weakly regular bent function.
- $\eta(D_u)$ attains both of the values $\{-1, 1\} \Rightarrow F$ is a non-weakly regular bent function.

*Remark* 4.3. Let $m$ be **odd** and $p \equiv 3 \pmod 4$. Using Theorem 3.10, we have $spec\,(f_u) = \left\{0, q^{\frac{n+s}{2}} w^v \eta(D_u) \sqrt{-1}^{n-s}\right\}$ where $v$ is a determined element of $\mathbb{Z}_q$ and $D_u = d_1^u d_2^u \cdots d_{n-s}^u$. Let $F : \mathbb{Z}_q^{n+s} \to \mathbb{Z}_q$ be the bent function constructed by Theorem 4.1 using the $s$-plateaued functions $f_u$. Then,

1. Assume $n - s \equiv 0 \pmod 4$.
   - $\eta(D_u) = 1$ for all $u \in \mathbb{Z}_{q^s} \Rightarrow F$ is a regular bent function.
   - $\eta(D_u) = -1$ for all $u \in \mathbb{Z}_{q^s} \Rightarrow F$ is a weakly regular bent function.
   - $\eta(D_u)$ attains both of the values $\{-1, 1\} \Rightarrow F$ is a non-weakly regular bent function.
2. Assume $n - s \equiv 2 \pmod 4$.
   - $\eta(D_u) = -1$ for all $u \in \mathbb{Z}_{q^s} \Rightarrow F$ is a regular bent function.
   - $\eta(D_u) = 1$ for all $u \in \mathbb{Z}_{q^s} \Rightarrow F$ is a weakly regular bent function.
   - $\eta(D_u)$ attains both of the values $\{-1, 1\} \Rightarrow F$ is a non-weakly regular bent function.
3. Assume $n - s \equiv 1 \pmod 4$ or $n - s \equiv 3 \pmod 4$.
   - No regular bent function is constructed.
   - $\eta(D_u) = 1$ for all $u \in \mathbb{Z}_{q^s}$ or $\eta(D_u) = -1$ for all $u \in \mathbb{Z}_{q^s}$ implies that $F$ is a weakly regular bent function.
   - $\eta(D_u)$ attains both of the values $\{-1, 1\} \Rightarrow F$ is a non-weakly regular bent function.

**Example 4.1.** Let $u \in \mathbb{Z}_{27^2}$ and $u = 27u_1 + u_2$ for $u_1, u_2 \in \mathbb{Z}_{27}$. Let $h_u : \mathbb{Z}_{27}^2 \to \mathbb{Z}_{27}$ be functions defined as

$$h_u(y_1, y_2) = \begin{cases} 1, & \text{if } u = 27y_1 + y_2 \\ 0, & \text{if otherwise.} \end{cases}$$

For each $u$, the 2-plateaued functions, $f_u : \mathbb{Z}_{27}^4 \to \mathbb{Z}_{27}$ are defined as

$$f_u(x_1, x_2, x_3, x_4) = d_1^u x_1^2 + d_2^u x_2^2 + u_1 x_3 + u_2 x_4,$$

where $d_1^u, d_2^u \in \mathbb{Z}_{27}^{\times}$. Then, $F : \mathbb{Z}_{27}^4 \times \mathbb{Z}_{27}^2 \to \mathbb{Z}_{27}$ defined by
$F(x, y_1, y_2) = \sum_{u \in \mathbb{Z}_{27^2}} f_u(x) h_u(y_1, y_2)$ is a bent function by Theorem 4.1.
The set of quadratic residues of 27 is $QR = \{1, 4, 7, 10, 13, 16, 19, 22, 25\}$ and the set of quadratic non-residues of 27 is $QnR = \{2, 5, 8, 11, 14, 17, 20, 23, 26\}$. $F$ can be classified by investigating the coefficients, $d_1^u$ and $d_2^u$.

- For each $f_u$, if $d_1^u$ and $d_2^u$ are chosen from the same set, QR or QnR, then $F$ is a weakly regular bent function.
- For each $f_u$, if $d_1^u$ is chosen from QR and $d_2^u$ is chosen from QnR, or vice versa, then $F$ is a regular bent function.
- If for some $f_u$ we choose $d_1^u$ and $d_2^u$ according to the first item and for the rest of $f_u$, the choice is done according to the second item, then $F$ is a non-weakly regular bent function.

In the light of this information, a numerical example is given. For $x = (x_1, x_2, x_3, x_4)$, let $f_u$ be defined as follows

$$f_u(x) = \begin{cases} x_1^2 + x_2^2 + u_1x_3 + u_2x_4, & \text{if } u_2 = 0 \\ x_1^2 + 2x_2^2 + u_1x_3 + u_2x_4, & \text{if } u_2 \neq 0. \end{cases}$$

Then, $F(x, y_1, y_2) = \sum_{u \in \mathbb{Z}_{27^2}} f_u(x)h_u(y_1, y_2)$ is a non-weakly regular bent function defined from $\mathbb{Z}_{27}^6$ to $\mathbb{Z}_{27}$ using the arguments given by Remark 4.3. Realize that, $F(x, y_1, y_2) = f_y(x)$ which implies

$$F(x, y_1, y_2) = \begin{cases} x_1^2 + x_2^2 + y_1x_3 + y_2x_4, & \text{if } y_2 = 0 \\ x_1^2 + 2x_2^2 + y_1x_3 + y_2x_4, & \text{if } y_2 \neq 0. \end{cases}$$

**Example 4.2.** For $u \in \mathbb{Z}_{25^3}$, let $f_u : \mathbb{Z}_{25}^5 \to \mathbb{Z}_{25}$ be 3-plateaued functions defined as

$$f_u(x_1, x_2, x_3, x_4, x_5) = d_1^u x_1^2 + d_2^u x_2^2 + u_1x_3 + u_2x_4 + u_3x_5,$$

where $u = 125u_1 + 25u_2 + u_3$ for $u_1, u_2, u_3 \in \mathbb{Z}_{25}$ and $d_1^u, d_2^u \in \mathbb{Z}_{25}^\times$.
Define, $h_u : \mathbb{Z}_{25}^3 \to \mathbb{Z}_{25}$ as

$$h_u(y_1, y_2, y_3) = \begin{cases} 1, & \text{if } u = 125y_1 + 25y_2 + y_3 \\ 0, & \text{if otherwise.} \end{cases}$$

For all choices of $d_1^u, d_2^u$, $F : \mathbb{Z}_{25}^5 \times \mathbb{Z}_{25}^3 \to \mathbb{Z}_{25}$ defined by,

$$F(x, y_1, y_2, y_3) = \sum_{u \in \mathbb{Z}_{25^3}} f_u(x)h_u(y_1, y_2, y_3)$$

is a regular bent function by Remark 4.1.

# CHAPTER 5

# CONCLUSION

Bent functions are significant tools as they have the maximum Hamming distance to the set of all affine functions and they are connected into various areas of mathematics and computer science. It is crucial to study bent functions over the finite fields of odd characteristics due to the interesting results.

The idea of construction of bent functions using near-bent functions or construction of near-bent functions using bent functions is first considered in [11]. The study is over finite fields with characteristic 2. Let $\mathbb{F}_2^n$ be an $n$-dimensional vector space over $\mathbb{F}_2$. As near-bent functions exist over $\mathbb{F}_2^n$ with $n$ odd and bent functions exist over $\mathbb{F}_2^n$ with $n$ even, it is possible to get one from another by either decreasing or increasing the dimension by one. All the four cases are considered. The case of the study in [11], we are especially concerned in this thesis is to get a bent function using near-bent functions by increasing the dimension. We would like to mention this part briefly because it summarizes the idea of our construction methods in a simple manner.

Let $f_1$, $f_2$ be near-bent functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ with the property that $supp(\widehat{f_1}) \cap supp(\widehat{f_2}) = \emptyset$ and $\bigcup_{i=1,2} supp(\widehat{f_i}) = \mathbb{F}_2^n$. Then, $F(x,y)$ from $\mathbb{F}_2^n \times \mathbb{F}_2$ to $\mathbb{F}_2$ defined by

$$F(x,y) = yf_1(x) + (y+1)f_2(x),$$

is bent. It is very easy to show this, actually. Let $\lambda$ be a linear functional on $\mathbb{F}_2^n \times \mathbb{F}_2$. Then,

$$\widehat{F}(\lambda) = \sum_{(x,y)\in\mathbb{F}_2^n\times\mathbb{F}_2} (-1)^{F(x,y)+\lambda(x,y)}$$

$$= \sum_{(x,0)\in\mathbb{F}_2^n\times\mathbb{F}_2} (-1)^{f_2(x)+\lambda(x,0)} + \sum_{(x,1)\in\mathbb{F}_2^n\times\mathbb{F}_2} (-1)^{f_1(x)+\lambda(x,1)}$$

$$\Rightarrow \widehat{F}(\lambda) = \widehat{f_1}(\lambda) + \widehat{f_2}(\lambda).$$

Since $supp(\widehat{f_1})$ and $supp(\widehat{f_2})$ partition $\mathbb{F}_2^n$, we have $\widehat{F}(\lambda) = \mp 2^{\frac{n+1}{2}}$. Hence $F$ is bent. This construction method is then adapted to the finite fields with characteristic $p$ [3]. They joint the near-bent functions using the Lagrange interpolation formula and obtain a bent function by increasing the dimension by $p$. Let $\mathbb{F}_p$ be the finite field with $p$ elements and $\mathbb{F}_p^n$ be an $n$-dimensional vector space over $\mathbb{F}_p$. To give examples, they compute the Walsh spectrums of all quadratic functions defined from $\mathbb{F}_p^n$ to $\mathbb{F}_p$. The Walsh spectrum of quadratic functions defined over $\mathbb{F}_q$ and the ring of integers modulo

$q$ gives completely different results than the results in [3]. Then, they develope their construction method such that the method uses $s$-plateaued functions instead of near-bent functions and apply on quadratic functions.
In this thesis, we give an adaptation of some of the studies given in [3, 4, 11]. Over finite fields with $q$ elements, we give a method to obtain bent functions using near-bent functions (see Theorem 2.2). Then, we compute the Walsh spectrum of all quadratic functions defined from $\mathbb{F}_q^n$ to $\mathbb{F}_q$ (see Theorem 2.3). This ensures us to apply the construction method on quadratic functions. Moreover, we adapt the method of construction to the ring of integers modulo $q$. Then, we generalize the method in such a way that it uses $s$-plateaued functions instead of near-bent functions. Consider the quadratic functions $d_1x_1^2 + d_2x_2^2 + ... + d_{n-s}x_{n-s}^2$ for $d_1, d_2, \cdots, d_{n-s} \in \mathbb{Z}_q^\times$. We compute the Walsh spectrum of these quadratic functions. Thus, we give examples of constructions using these quadratic functions. To classify the constructed bent functions as regular, weakly regular and non-weakly regular, we give detailed explanations.
Let $h(x)$ be a monic, basic irreducible polynomial of degree $k$ in $\mathbb{Z}_q[x]$. Then, the ring $R = \mathbb{Z}_q[x]/\big(h(x)\big)$ is a commutative ring with identity. It is proven that $R$ is a Galois ring by showing the principal ideal $\big(p + h(x)\big)$ consists of all zero divisors and zero. Actually, $R$ is shown to be a Galois ring with $q^k$ elements and characteristic $q$ [16]. Therefore, the studies given in Chapter 3 and Chapter 4 are also valid on Galois rings.

Now, we would like to give a summarized list of contributions.

- We give the first adaptation of some of the studies in [3, 4, 11] to the finite fields with $q$ elements and the ring of integers modulo $q$.
- The functions that are used as a Lagrange coefficient in Theorem 3.3 and Theorem 4.1, cannot be represented as polynomials. We demonstrate this using some of the arguments given in [2]. Moreover, we show that there is no alternative of a polynomial to use for Lagrange interpolation formula.
- Consider the functions $d_1x_1^2 + d_2x_2^2 + ... + d_{n-s}x_{n-s}^2$ for $d_1, d_2, \cdots, d_{n-s} \in \mathbb{Z}_q^\times$ and $0 \leq s \leq n-1$. We compute the Walsh spectrum of these quadratic functions over $\mathbb{Z}_q$ and all quadratic functions over $\mathbb{F}_q$. The results and techniques used for the computations are completely different than the ones in [3].
- We compute the Gauss sum over $Z_q$. That ensures us to obtain the Walsh spectrum of the quadratic functions, defined as $d_1x_1^2 + d_2x_2^2 + ... + d_{n-s}x_{n-s}^2$ for $d_1, d_2, \cdots, d_{n-s} \in \mathbb{Z}_q^\times$ and $0 \leq s \leq n-1$
- To apply the construction theorems (Theorem 2.2,Theorem 3.3,Theorem 4.1), we need functions having pairwise disjoint support of Walsh transforms. So, we give a technique to determine quadratic functions with pairwise disjoint support of Walsh transforms.
- In the application parts, we explained how to classify the constructed bent functions as regular, weakly regular and non-weakly regular in detail. (see Sections 2.4, 3.6, 4.3).
  In Section 2.4, we construct bent functions using near-bent functions over $\mathbb{F}_q$.

When $p$ is fixed, the percentage of the non-weakly regular bent functions is greater than the percentage of regular and weakly regular bent functions. Also, the number of bent functions we constructed is greater than the number of bent functions constructed in [3] for a fixed $p$.
In Section 3.6 and Section 4.3, we give applications using near-bent functions and $s$-plateaued functions over $\mathbb{Z}_q = \mathbb{Z}_{p^m}$. For these cases, if $m$ is even all the constructed bent functions are regular. If $m$ is odd great majority of the bent functions are non-weakly regular. Moreover, we construct more bent functions compared to [3] and the percentage of non-weakly regular bent functions is greater. For an odd $m$, as $p$ or $m$ increases this percentage of non-weakly regular functions gets greater.

To construct bent functions, we use the idea of Lagrange's interpolation formula. As a future work, one can search for any other idea to joint the $s$-plateaued functions to obtain bent functions.
In [11], different ideas are given to obtain a bent function from near-bent functions or obtain a near-bent function from bent functions. Generalizing these ideas to the characteristic $p$ case might be interesting.

# REFERENCES

[1] L. Budaghyan, C. Carlet, T. Helleseth, and A. Kholosha, Generalized bent functions and their relation to maiorana-mcfarland class, pp. 1212–1215, 2012.

[2] L. Carlitz, Functions and polynomials (mod $p^n$), Acta Arithmetica, 9, p. 67–78, 1964.

[3] A. Çeşmelioğlu, G. McGuire, and W. Meidl, A construction of weakly and non-weakly regular bent functions, Journal of Combinatorial Theory, 119 A, pp. 420–429, 2012.

[4] A. Cesmelioglu and W. Meidl, A construction of bent functions from plateaued functions, Des. Codes Cryptogr., 66, pp. 231–242, 2013.

[5] T. Helleseth and A. Kholosha, Monomial and quadratic bent functions over the finite field of odd characteristic, IEEE Transactions on Information Theory, 52(5), pp. 2018–2032, 2006.

[6] T. Helleseth and A. Kholosha, New binomial bent functions over the finite fields of odd characteristic, IEEE Transactions on Information Theory, 56(9), pp. 4646–4652, 2010.

[7] X. D. Hou, $q$-ary bent functions constructed from chain rings, Finite Fields and Their Applications, 4(1), pp. 55–61, 1998.

[8] X. D. Hou, $p$-ary and $q$-ary versions of certain results about bent functions and resilient functions, Finite Fields and Their Applications, 10(4), pp. 566–582, 2004.

[9] W. Jia, X. Zeng, T. Helleseth, and C. Li, A class of binomial bent functions over the finite fields of odd characteristic, IEEE Transactions on Information Theory, 58(9), pp. 6054–6063, 2012.

[10] P. V. Kumar, R. A. Scholtz, and L. R. Welch, Generalized bent functions and their properties, Journal of Combinatorial Theory, Series A, 40, pp. 90–107, 1985.

[11] G. Leander and G. McGuire, Construction of bent functions from near-bent functions, Journal of Combinatorial Theory, 116 A, pp. 960–970, 2009.

[12] N. Li, X. Tang, and T. Helleseth, New classes of generalized boolean bent functions over z4, pp. 841–845, 2012.

[13] R. Lidl and H. Neiderreiter, *Finite Fields*, Cambridge University Press, 1997.

[14] H. E. Rose, *A Course on Finite Groups*, Springer, 2009.

[15] O. Rothaus, On bent functions, Journal of Combinatorial Theory, 20 A, p. 300–305, 1976.

[16] Z. X. Wan, *Lectures on Finite Fields and Galois Rings*, World Scientific Pub Co Inc, 2003.

# CURRICULUM VITAE

## PERSONAL INFORMATION

**Surname, Name:** Çelik, Dilek
**Nationality:** Turkish
**Date and Place of Birth:** 26.02.1985, Gaziantep
**Marital Status:** Married

## EDUCATION

| **Degree** | **Institution** | **Year of Graduation** |
|---|---|---|
| M.S. | Department of Cryptography, METU | 2010 |
| B.S. | Department of Mathematics, METU | 2007 |
| High School | Gaziantep Anatolian High School | 2003 |

## PROFESSIONAL EXPERIENCE

| **Year** | **Place** | **Enrollment** |
|---|---|---|
| 2007-2013 | Department of Mathematics, METU | Research Assistant |
| 2013-Still | Department of Cryptology, Tubitak UEKAE | Senior Research Assistant |