Two-weight and three-weight linear codes from weakly regular bent functions

Chunming Tang, Yanfeng Qi

Abstract

Linear codes with few weights have applications in consumer electronics, communication, data storage system, secret sharing, authentication codes, association schemes, and strongly regular graphs. This paper first generalizes the method of constructing two-weight and three-weight linear codes of Ding et al. [6] and Zhou et al. [21] to general weakly regular bent functions and determines the weight distributions of these linear codes. It solves the open problem of Ding et al. [6]. Further, this paper constructs new linear codes with two weight or three weight and presents the weight distributions of these codes. They contains some optimal codes meeting certain bound on linear codes. From the point of application, all the linear codes constructed in this paper can be obtained by two functions \( f(x) = \text{Tr}^m_1(x^2) \) and \( f(x) = \text{Tr}^m_1(\alpha x^2) \), where \( \alpha \) is a quadratic nonresidue of \( \mathbb{F}_q \).

Index Terms

Linear codes, weight distribution, weakly regular bent functions, cyclotomic fields, secret sharing schemes

I. INTRODUCTION

Throughout this paper, let \( p \) be an odd prime and \( q = p^m \), where \( m \) is a positive integer. An \([n,k,d]\) code \( C \) is a \( k \)-dimension subspace of \( \mathbb{F}_q^n \) with minimum Hamming distance \( d \). Let \( A_i \) be the number of codewords with Hamming weight \( i \) in \( C \). The polynomial \( 1 + A_1 z + \cdots + A_n z^n \) is called the weight enumerator of \( C \) and \((A_1, \cdots, A_n)\) called the weight distribution of \( C \). The minimum distance \( d \) determines the error correcting capability of \( C \). The weight distribution contains important information for estimating the probability of error detection and correction. Hence, the weight distribution attracts much attention in coding theory and much work focus on the determination of the weight distributions of linear codes. Let \( t \) be the number of nonzero \( A_i \) in the weight distribution. Then the code \( C \) is called a \( t \)-weight code. Linear codes can be applied in consumer electronics, communication and data storage system. Linear codes with few weights are of important in secret sharing [3], [20], authentication codes [10], association schemes [1] and strongly regular graphs [2].

Let \( F(x) \in \mathbb{F}_q[x] \) and \( f(x) = \text{Tr}^m_1(F(x)) \), where \( \text{Tr}^m_1 \) is the trace function from \( \mathbb{F}_q \) to \( \mathbb{F}_p \). Let \( D = \{x \in \mathbb{F}_q^k : f(x) = 0 \} \). Denote \( n = \#(D) \) and \( D = \{d_1, d_2, \cdots, d_n\} \). Then a linear code of length \( n \) defined over \( \mathbb{F}_p \) is

\[
C_D = \{(\text{Tr}^m_1(\beta d_1), \text{Tr}^m_1(\beta d_2), \cdots, \text{Tr}^m_1(\beta d_n)) : \beta \in \mathbb{F}_q \},
\]

where \( D \) is called the defining set of \( C_D \).

Note that by the choice of \( D \) many linear codes can be constructed [7], [8], [9]. Ding et al. [5], [6] and Zhou et al. [21] constructed some classes of two-weight and three-weight linear codes. Ding et al. [6] presented the weight distribution of \( C_D \) for the case \( F(x) = x^2 \) and proposed an open problem on determining the weight distribution of \( C_D \) for general planar functions \( F(x) \). Zhou et al. [21] gave the weight distribution of \( C_D \) for quadratic planar functions \( F(x) \).

In this paper, we consider linear codes with two weight or three weight from weakly regular bent functions. First, we generalize the method of constructing two-weight and three-weight linear codes of Ding et al. [6] and Zhou et al. [21] to general weakly regular bent functions. The weight distributions of these linear codes are determined by the theory of cyclotomic fields. And we solve the open problem of Ding et al. [6]. Further, by choosing the defining sets different from that of Ding et al. [6] and Zhou et al. [21], we construct new linear codes with two weight or three weight and present the weight distributions of these codes. The weight distributions of linear codes constructed in this paper are completely determined by the sign of the Walsh transform of weakly regular bent functions. From the point of application, all the linear codes constructed in this paper can be obtained by two functions \( f(x) = \text{Tr}^m_1(x^2) \) and \( f(x) = \text{Tr}^m_1(\alpha x^2) \), where \( \alpha \) is a quadratic nonresidue of \( \mathbb{F}_q \).

This paper is organized as follows: Section 2 introduces cyclotomic fields, weakly regular bent functions and exponential sums. Section 3 generalizes the method of Ding et al. [6] and Zhou et al. [21] to general weakly regular bent functions and determines the weight distributions of these linear codes. Section 4 constructs new classes of two-weight and three-weight linear codes. Section 5 makes a conclusion.

C. Tang is with School of Mathematics and Information, China West Normal University, Sichuan Nanchong, 637002, China. e-mail: tangchunmingmath@163.com

Y. Qi is with School of Science, Hangzhou Dianzi University, Hangzhou, Zhejiang, 310018, China
II. Preliminaries

In this section, we state some basic facts on cyclotomic fields, weakly regular bent functions and exponential sums. These results are used in the rest of the paper for linear codes with few weights. First some notations are given. Let \( \mathbb{Z} \) be the rational integer ring and \( Q \) the rational field. Let \( \eta \) be the quadratic character of \( \mathbb{F}_p^\ast \) such that \( \eta(a) = a^{(p-1)/2} \) \( (a \in \mathbb{F}_p^\ast) \). Let \( p^* = \eta(-1)p = (-1)^{(p-1)/2}p \) and \( \zeta_p = e^{2\pi \sqrt{-1}/p} \) be the primitive \( p \)-th root of unity.

A. Cyclotomic field \( Q(\zeta_p) \)

Some results on cyclotomic field \( Q(\zeta_p) \) are given in the following lemma.

**Lemma 2.1:** (i) The ring of integers in \( K = Q(\zeta_p) \) is \( \mathcal{O}_K = \mathbb{Z}(\zeta_p) \) and \( \{\zeta_p^i : 1 \leq i \leq p-1\} \) is an integral basis of \( \mathcal{O}_K \), where \( \zeta_p = e^{2\pi \sqrt{-1}/p} \) is the primitive \( p \)-th root of unity.

(ii) The field extension \( K/Q \) is Galois of degree \( p-1 \) and the Galois group \( Gal(K/Q) = \{\sigma_a : a \in (\mathbb{Z}/p\mathbb{Z})^\times\} \), where the automorphism \( \sigma_a \) of \( K \) is defined by \( \sigma_a(\zeta_p) = \zeta_p^a \).

(iii) The field \( K \) has a unique quadratic subfield \( L = Q(\sqrt[p]{\zeta}) \) where \( p^* = (\frac{-1}{p})p = (-1)^{(p-1)/2}p \), where \( (\frac{\cdot}{p}) \) is the Legendre symbol for \( 1 \leq a \leq p-1 \). For \( 1 \leq a \leq p-1, \sigma_a(\sqrt[p]{\zeta}) = (\frac{a}{p})\sqrt[p]{\zeta} \) and the Galois group \( Gal(L/Q) \) is \( \{1, \gamma\} \), where \( \gamma \) is any quadratic nonresidue in \( \mathbb{F}_p \).

B. Weakly regular bent functions

Let \( f(x) \) be a function from \( \mathbb{F}_q \) to \( \mathbb{F}_p \) \( (q = p^m) \), the Walsh transform of \( f \) is defined by

\[
W_f(\beta) := \sum_{x \in \mathbb{F}_q} \zeta_p^{f(x) + Tr_q^m(\beta x)},
\]

where \( \zeta_p = e^{2\pi \sqrt{-1}/p} \) is the primitive \( p \)-th root of unity, \( Tr_q^m(x) = \sum_{i=0}^{m-1} x^{p^i} \) is the trace function from \( \mathbb{F}_q \) to \( \mathbb{F}_p \), and \( \beta \in \mathbb{F}_q \).

The inverse Walsh transform of such \( f(x) \) gives

\[
\zeta_p^{f(x)} = \frac{1}{p^m} \sum_{\beta \in \mathbb{F}_q} W_f(\beta) \zeta_p^{-Tr_q^m(\beta x)}.
\]

The function \( f(x) \) is a \( p \)-ary bent functions, if \( |W_f(\beta)| = \frac{p^m}{\sqrt{p}} \) for any \( \beta \in \mathbb{F}_q \). A bent function \( f(x) \) is regular if it has some \( p \)-ary function \( f^*(x) \) satisfying \( W_f(\beta) = p \zeta_p^{f^*(x)} \) \( \forall \beta \in \mathbb{F}_q \). A bent function \( f(x) \) is weakly regular if it has a complex \( u \) with unit magnitude satisfying that \( W_f(\beta) = up^\varepsilon \zeta_p^{f^*(x)} \) for some function \( f^*(x) \). Such function \( f^*(x) \) is called the dual of \( f(x) \). [14], [16] gives that a weakly regular bent function \( f(x) \) satisfies that

\[
W_f(\beta) = \varepsilon p^m \zeta_p^{f^*(x)},
\]

where \( \varepsilon = \pm 1 \) is called the sign of the Walsh Transform of \( f(x) \) and \( p^* = \eta(-1)p \). From Equation (1), for the weakly regular bent function \( f(x) \), we have \( \sum_{\beta \in \mathbb{F}_q} \zeta_p^{f^*(x) - Tr_q^m(\beta x)} = \varepsilon p^m f^*(x) / \sqrt{p^m} \). Note that \( p^m = (\eta(-1))m \sqrt{p^{2m}} \), we have

\[
W_{f^*}(-x) = (\eta(-1))^m \varepsilon p^m \zeta_p^{f^*(x)}, x \in \mathbb{F}_q.
\]

The dual of a weakly regular bent function is also weakly regular bent and \( f^{**}(x) = f(-x) \). The sign of the Walsh transform of \( f^* \) is \( (\eta(-1))^m \varepsilon \). Some results on weakly regular bent functions can be found in [11], [13], [14], [15], [16], [18].

The construction of bent functions is an interesting and hot research topic. A class of bent functions is derived from planar functions. A function mapping from \( \mathbb{F}_q \) to \( \mathbb{F}_p \) is a planar function, if for any \( a \in \mathbb{F}_q^\times \) and \( b \in \mathbb{F}_q \), \#\( \{x : f(x) + a(x) - f(x) = b\} = 1 \). A simple example of planar functions is the square function \( F(x) = x^2 \). Almost known planar functions are quadratic functions, i.e., \( F(x) = \sum_{0 \leq i \leq m-1} a_i x^{p^i}+p^m \), which are corresponding to semi-fields. Coulet and Matthews [4] introduced a class of non-planar quadratic planar functions \( F(x) = x^{3k+1}/2 \), where \( p = 3 \), \( k \) is odd, and \((m,k) = 1 \). The derived \( p \)-ary functions \( f(x) = Tr_q^m(\beta F(x)) \) for any \( \beta \in \mathbb{F}_q^\times \) from these known planar functions are all weakly regular bent functions. It is often difficult to determine the sign of the Walsh transform of weakly regular functions. However, for some special functions, some results are listed here.

(i) \( f(x) = Tr_q^m(\alpha x^2) \) [14] for \( a \in \mathbb{F}_q^\times \). The sign of the Walsh transform of \( f(x) \) is \( \varepsilon_\alpha = (-1)^{m-1} \alpha^{(q-1)/2} \).

(ii) \( F(x) = \lambda Tr_q^m(\alpha x^{3k+1}) \) \( (m = 2k) \) [12], where \( m = 2k, 2 \mid k, p = 3, \) and \( \alpha \) is a primitive element of \( \mathbb{F}_q \). The sign of the Walsh transform of \( f(x) \) is 1.

(iii) \( f(x) = Tr_q^m(x^{p^3}+x^{p^6}+x^2) \) [16], where \( m = 4k \). The sign of the Walsh transform of \( f(x) \) is -1.

Let \( RF \) be a set of \( p \)-ary weakly regular bent functions with the following conditions:

(i) \( f(0) = 0 \),
(ii) There exist an integer \( h \) such that \( (h-1,p-1) = 1 \) and \( f(ax) = a^h f(x) \) for any \( a \in \mathbb{F}_q^\times \) and \( x \in \mathbb{F}_q \).

Note that \( RF \) contains almost known weakly regular bent functions. We will discuss properties of functions in \( RF \).
Lemma 2.2: Let $a_i, b_i \in \mathbb{Z}$ $(0 \leq i \leq p - 1)$ such that $\sum_{i=0}^{p-1} a_i \equiv \sum_{i=0}^{p-1} b_i \mod 2$ and $\sum_{i=0}^{p-1} a_i \zeta_p^i = \sum_{i=0}^{p-1} b_i \zeta_p^i$. Then $a_i \equiv b_i \mod 2$.

Proof: From $\sum_{i=0}^{p-1} a_i \zeta_p^i = \sum_{i=0}^{p-1} b_i \zeta_p^i$, we have
\[ \sum_{i=0}^{p-1} (a_i - b_i) \zeta_p^i = 0. \]

The minimal polynomial of $\zeta_p$ over $Q$ is $1 + x + \cdots + x^{p-1} = 0$. Then we have
\[ a_0 - b_0 = a_1 - b_1 = \cdots = a_{p-1} - b_{p-1} = \lambda, \]

where $\lambda \in \mathbb{Z}$. Hence,
\[ p\lambda = \left( \sum_{i=0}^{p-1} a_i \right) - \left( \sum_{i=0}^{p-1} b_i \right), \]
\[ \lambda = \frac{1}{p} \left( \sum_{i=0}^{p-1} a_i - \sum_{i=0}^{p-1} b_i \right). \]

From $\sum_{i=0}^{p-1} a_i \equiv \sum_{i=0}^{p-1} b_i \mod 2$, we have
\[ \lambda \equiv 0 \mod 2. \]

Hence, $a_i \equiv b_i \mod 2$. ■

Lemma 2.3: Let $p$ be an odd prime, $p^* = \eta(1)p$, and $a \in \mathbb{F}_q^*$. Then $\sum_{x \in \mathbb{F}_q^*} \zeta_p^{\text{Tr}_p^m(ax^2)} = (-1)^{m-1}p^{(q-1)/2} \sqrt{p^*}^m$. ■

Proof: This can lemma can be found in [19].

Proposition 2.4: If $f(x) \in \mathcal{R}_F$, then $f^*(0) = 0$.

Proof: From $f(x) \in \mathcal{R}_F$, there exists an integer $h$ satisfying $(h - 1, p - 1) = 1$ and $f(ax) = a^h f(x)$. Since $p - 1$ is even, $h$ is obviously even. Then we have $f(-x) = f(x)$. Let $\{P_+, P_-\}$ be a partition of $\mathbb{F}_q^*$ such that $P_- = \{-x : x \in P_+\}$. Let $C_i = \#\{x \in P_+ : f(x) = i\}$, then
\[ \sum_{x \in \mathbb{F}_q^*} \zeta_p^{f(x)} = 1 + 2 \sum_{i=0}^{p-1} C_i \zeta_p^i = \varepsilon \sqrt{p^*}^m \zeta_p^{f^*(0)}. \]

If $m$ is even, then $\varepsilon \sqrt{p^*}^m \in \mathbb{Z}$ and
\[ 1 + 2 \sum_{i=0}^{p-1} C_i \equiv \varepsilon \sqrt{p^*}^m \equiv 1 \mod 2. \]

From Lemma 2.2 we have $f^*(0) = 0$.

If $m$ is odd, from Lemma 2.3
\[ 1 + 2 \sum_{i=0}^{p-1} C_i \zeta_p^i = \varepsilon \sqrt{p^*}^m \zeta_p^{f^*(0)}(1 + 2 \sum_{i=0}^{p-1} C_i^p). \]

Hence, we have
\[ 1 + 2 \sum_{i=0}^{p-1} C_i \zeta_p^i = \varepsilon \sqrt{p^*}^{m-1}(1 + 2 \frac{p-1}{2}) \equiv 1 \mod 2. \]

From Lemma 2.2 we also have $f^*(0) = 0$.

Hence, this proposition follows. ■

Proposition 2.5: If $f(x) \in \mathcal{R}_F$, then $f^*(x) \in \mathcal{R}_F$.

Proof: If $f(x)$ is weakly regular bent, then $f^*(x)$ is also weakly regular bent. From Proposition 2.4 $f^*(0) = 0$. Hence, we just need to prove that $f^*(x)$ satisfies condition (ii) in the definition of $\mathcal{R}_F$.

For $\forall a \in \mathbb{F}_p^*$ and $\beta \in \mathbb{F}_q^*$, we have
\[ \varepsilon \sqrt{p^*}^m \zeta_p^{f^*(a \beta)} = \sum_{x \in \mathbb{F}_q^*} \zeta_p^{f(ax) + a \text{Tr}_p^m(\beta x)} = \sum_{x \in \mathbb{F}_q^*} \zeta_p^{f(ax) + a \text{Tr}_p^m(\beta a^l x)}, \]
where $l$ satisfies that $l(h - 1) \equiv 1 \mod (p - 1)$. Then
\[ \varepsilon \sqrt{p^*}^m \zeta_p^{f^*(a \beta)} = \sum_{x \in \mathbb{F}_q^*} \zeta_p^{a^l f(x) + a^l \text{Tr}_p^m(\beta x)}. \]

Note that $a^{hl} = a^{l+1}$. Then we have
\[ \varepsilon \sqrt{p^*}^m \zeta_p^{f^*(a \beta)} = \sum_{x \in \mathbb{F}_q^*} \zeta_p^{a^{l+1} f(x) + \text{Tr}_p^m(\beta x)} = \sigma_{a^{l+1}}(\varepsilon \sqrt{p^*}^m \zeta_p^{f^*(\beta)}) = \varepsilon \sqrt{p^*}^m \zeta_p^{a^{l+1} f^*(\beta)}. \]
Hence, for $\forall \beta \in \mathbb{F}_q^*$, $f^*(a\beta) = a^l + 1 f^*(\beta)$ and $(l + 1 - 1, p - 1) \equiv 1$.

Hence, $f^*(x) \in \mathcal{R}_F$.

**Remark** By Equation (3), if the sign of the Walsh transform of $f(x)$ is $\varepsilon$, then the sign of the Walsh transform of $f^*(x)$ is $(\eta(-1))^m \varepsilon$.

C. Exponential sums from weakly regular bent functions

For determining parameters and weight distributions of linear codes from weakly regular bent functions, some results on exponential sums from weakly regular bent functions in $\mathcal{R}_F$ are given.

**Lemma 2.6:** Let $p$ be an odd prime and $p^* = \eta(-1)p$. Then $\sum_{x \in \mathbb{F}_p^*} \eta(x) \zeta_p^x = \sqrt{p^*}$.

**Proof:** By the definition of $\eta(x)$,

$$\sum_{x \in \mathbb{F}_p^*} \eta(x) \zeta_p^x = \sum_{x \in \mathbb{F}_p^*} \eta(x) \zeta_p^x + \sum_{x \in \mathbb{F}_p^* \setminus \mathbb{F}_p^{\varepsilon^2}} \eta(x) \zeta_p^x = \sum_{x \in \mathbb{F}_p^{\varepsilon^2}} \zeta_p^x - \sum_{x \in \mathbb{F}_p^* \setminus \mathbb{F}_p^{\varepsilon^2}} \zeta_p^x.$$  

From $\sum_{x \in \mathbb{F}_p^*} \zeta_p^x = 0$, we have

$$\sum_{x \in \mathbb{F}_p^*} \eta(x) \zeta_p^x = \sum_{x \in \mathbb{F}_p^{\varepsilon^2}} \zeta_p^x + \sum_{x \in \mathbb{F}_p^{\varepsilon^2}} \zeta_p^x + 1 = \sum_{x \in \mathbb{F}_p^*} \zeta_p^x.$$

From Lemma 2.3 this lemma follows.

**Lemma 2.7:** Let $f(x)$ be a $p$-ary function from $\mathbb{F}_q$ to $\mathbb{F}_p$ with $W_f(0) = \varepsilon \sqrt{p^*}$, where $\varepsilon \in \{1, -1\}$ and $p^* = \eta(-1)p$. Let $N_f(a) = \#\{x \in \mathbb{F}_q : f(x) = a\}$. Then we have

1. If $m$ is even, then

$$N_f(a) = \begin{cases} \frac{p^m - 1}{p - 1} (\eta(-1))^{m/2} p^{(m-2)/2}, & a = 0; \\ \frac{p^m - 1}{p - 1} (\eta(-1))^{m/2} p^{(m-2)/2}, & a \in \mathbb{F}_p^* \end{cases}.$$

2. If $m$ is odd, then

$$N_f(a) = \begin{cases} \frac{p^m - 1}{p - 1} \varepsilon \sqrt{p^*}^{m-1}, & a \in \mathbb{F}_p^{\varepsilon^2}; \\ \frac{p^m - 1}{p - 1} \varepsilon \sqrt{p^*}^{m-1}, & a \in \mathbb{F}_p^* \setminus \mathbb{F}_p^{\varepsilon^2}. \end{cases}$$

**Proof:** From $W_f(0) = \varepsilon \sqrt{p^*}$, we have

$$\varepsilon \sqrt{p^*} = \sum_{a \in \mathbb{F}_p^*} N_f(a) \zeta_p^a.$$  

1. If $m$ is even, $\varepsilon \sqrt{p^*} \in \mathbb{Z}$, then

$$N_f(0) = \varepsilon \sqrt{p^*} + \sum_{a \in \mathbb{F}_p^*} N_f(a) \zeta_p^a = 0.$$  

Since the minimal polynomial of $\zeta_p$ over $Q$ is $1 + x + \cdots + x^{p-1} = 0$, we have

$$N_f(0) = \varepsilon \sqrt{p^*} = N_f(a), a \in \mathbb{F}_p^*.$$  

From $\sum_{a \in \mathbb{F}_p^*} N_f(a) = q$, we have

$$pN_f(1) = q - \varepsilon \sqrt{p^*}.$$  

Hence,

$$N_f(a) = \begin{cases} \frac{p^m - 1}{p - 1} (\eta(-1))^{m/2} p^{(m-2)/2}, & a = 0; \\ \frac{p^m - 1}{p - 1} (\eta(-1))^{m/2} p^{(m-2)/2}, & a \in \mathbb{F}_p^*. \end{cases}.$$

2. If $m$ is odd, from Lemma 2.3 we have

$$\sum_{x \in \mathbb{F}_p^*} \zeta_p^{x^2} = \sqrt{p^*}.$$  

Further,

$$\sum_{a \in \mathbb{F}_p^*} N_f(a) \zeta_p^a = \varepsilon \sqrt{p^*}^{m-1} (\zeta_p^0 + \sum_{x \in \mathbb{F}_p^{\varepsilon^2}} 2 \zeta_p^a).$$

And we have

$$\left(N_f(0) - \varepsilon \sqrt{p^*}^{m-1}\right) \zeta_p^0 + \sum_{s \in \mathbb{F}_p^{\varepsilon^2}} (N_f(s) - 2 \varepsilon \sqrt{p^*}^{m-1}) + \sum_{t \in \mathbb{F}_p^* \setminus \mathbb{F}_p^{\varepsilon^2}} N_f(t) \zeta_p^t = 0.$$
The minimal polynomial of $\zeta_p$ over $Q$ is $1 + x + \cdots + x^{p-1} = 0$. Then we have
\[
N_f(0) - \varepsilon\sqrt{p}^{m-1} = N_f(s) - 2\varepsilon\sqrt{p}^{m-1} = N_f(t),
\]
where $s \in \mathbb{F}_p^\times$ and $t \in \mathbb{F}_p^\times \mathbb{F}_p^\times$. Note that $\sum_{a \in \mathbb{F}_p} N_f(a) = q$, we have
\[
N_f(t) = p^{m-1} - \varepsilon\sqrt{p}^{m-1},
N_f(0) = p^{m-1},
N_f(s) = p^{m-1} + \varepsilon\sqrt{p}^{m-1},
\]
where $t \in \mathbb{F}_p^\times \mathbb{F}_p^\times$ and $s \in \mathbb{F}_p^\times$.

Hence, this lemma follows.

**Lemma 2.8:** Let $f(x) \in \mathcal{R}_F$ with the sign $\varepsilon$ of the Walsh transform. Then we have
(1) If $m$ is even, then
\[
N_f(a) = \begin{cases} 
  p^{m-1} + \varepsilon(p-1)(\eta(-1))^{m/2}p^{(m-2)/2}, & a = 0; \\
  p^{m-1} - \varepsilon\eta(-1)^{m/2}p^{(m-2)/2}, & a \in \mathbb{F}_p^\times.
\end{cases}
\]
(2) If $m$ is odd, then
\[
N_f(a) = \begin{cases} 
  p^{m-1}, & a = 0; \\
  p^{m-1} + \varepsilon\eta(-1)^{1/2}p^{m-1}, & a \in \mathbb{F}_p^\times; \\
  p^{m-1} - \varepsilon\eta(-1)^{1/2}p^{m-1}, & a \in \mathbb{F}_p^\times \mathbb{F}_p^\times.
\end{cases}
\]

**Proof:** As $f(x) \in \mathcal{R}_F$, $f(0) = 0$. From Equation (3), we have
\[
\mathcal{W}_f(0) = (\eta(-1))^m \varepsilon\sqrt{p}^m.
\]
Hence, from Lemma 2.7, the lemma follows.

**Lemma 2.9:** Let $f(x)$ be a $p$-ary function with $\mathcal{W}_f(0) = \varepsilon\sqrt{p}^m$. Then
\[
\sum_{y \in \mathbb{F}_p^\times} \sum_{x \in \mathbb{F}_p} \zeta_p^{yf(x)} = \begin{cases} 
  \varepsilon(p-1)\sqrt{p}^m, & m \text{ is even}; \\
  0, & m \text{ is odd}.
\end{cases}
\]

**Proof:**
\[
\sum_{y \in \mathbb{F}_p^\times} \sum_{x \in \mathbb{F}_p} \zeta_p^{yf(x)} = \sum_{y \in \mathbb{F}_p^\times} \sum_{x \in \mathbb{F}_p} \zeta_p^{yf(x)} = \sum_{y \in \mathbb{F}_p^\times} \sigma_y(\varepsilon\sqrt{p}^m) = \varepsilon\sqrt{p}^m \sum_{y \in \mathbb{F}_p^\times} (\eta(y))^m.
\]

If $m$ is even, then $\sum_{y \in \mathbb{F}_p^\times} (\eta(y))^m = p - 1$, that is, $\sum_{y \in \mathbb{F}_p^\times} \sum_{x \in \mathbb{F}_p} \zeta_p^{yf(x)} = \varepsilon(p-1)\sqrt{p}^m$.

If $m$ is odd, then $\sum_{y \in \mathbb{F}_p^\times} (\eta(y))^m = \sum_{y \in \mathbb{F}_p^\times} \eta(y) = 0$ and $\sum_{y \in \mathbb{F}_p^\times} \sum_{x \in \mathbb{F}_p} \zeta_p^{yf(x)} = 0$.

Hence, this lemma follows.

**Lemma 2.10:** Let $\beta \in \mathbb{F}_q^\times$ and $f(x) \in \mathcal{R}_F$ with the sign $\varepsilon$ of the Walsh transform.
(1) If $m$ is even, then
\[
\sum_{y \in \mathbb{F}_p^\times} \sum_{x \in \mathbb{F}_p} \zeta_p^{yf(x)+z\text{Tr}^m(\beta x)} = \begin{cases} 
  \varepsilon(p-1)^2\sqrt{p}^m, & f^*(\beta) = 0; \\
  -\varepsilon(p-1)\sqrt{p}^m, & f^*(\beta) \neq 0.
\end{cases}
\]
(2) If $m$ is odd, then
\[
\sum_{y \in \mathbb{F}_p^\times} \sum_{x \in \mathbb{F}_p} \zeta_p^{yf(x)+z\text{Tr}^m(\beta x)} = \begin{cases} 
  0, & f^*(\beta) = 0; \\
  \eta(f^*(\beta))\varepsilon(\eta(-1))^{(m+1)/2}(p-1)p^{(m+1)/2}, & f^*(\beta) \neq 0.
\end{cases}
\]

**Proof:** Let $A = \sum_{y \in \mathbb{F}_p^\times} \sum_{x \in \mathbb{F}_p} \zeta_p^{yf(x)+z\text{Tr}^m(\beta x)}$. Let $l$ be an integer satisfying $l(h-1) \equiv 1 \mod p$.

Since $x \mapsto (\frac{\beta}{\beta})^l x$ is a permutation of $\mathbb{F}_q$, then
\[
A = \sum_{y, z \in \mathbb{F}_p^\times} \zeta_p^{y f((\frac{\beta}{\beta})^l x) + z \text{Tr}^m(\beta(\frac{\beta}{\beta})^l x)}.
\]

From Condition (ii) in the definition of $\mathcal{R}_F$, we have
\[
A = \sum_{y, z \in \mathbb{F}_p^\times} \zeta_p^{y (\frac{\beta}{\beta})^l f(z) + z \text{Tr}^m(\beta z)}.
\]
Note that \( y(z_y) = y(z_y)^{l+1} = z(z_y) \). Then

\[
A = \sum_{y,z \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_q} c_p^{(f(x) + \text{Tr}_q^m(\beta x))y}.
\]

Since \((l, p - 1) = 1\) and \( y \mapsto z(z_y) \) is a permutation of \( \mathbb{F}_p^* \), then

\[
A = (p - 1) \sum_{y \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_q} c_p^{(f(x) + \text{Tr}_q^m(\beta x))y} = (p - 1) \sum_{y \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_q} \sigma_y (\sum_{x \in \mathbb{F}_q} c_p^{(f(x) + \text{Tr}_q^m(\beta x))}) = (p - 1) \sum_{y \in \mathbb{F}_p^*} \sigma_y (\mathcal{W}_f(\beta)).
\]

From \( f(0) = 0 \),

\[
A = (p - 1) \sum_{y \in \mathbb{F}_p^*} \sigma_y (\sqrt{p^{-m}} c_p^{f^*(\beta)}).
\]

From Lemma 2.1 we have

\[
A = \varepsilon(p - 1) \sqrt{p^{-m}} \sum_{y \in \mathbb{F}_p^*} \eta^m(y) c_p^{f^*(\beta)}.
\]

When \( m \) is even, then

\[
A = \varepsilon(p - 1) \sqrt{p^{-m}} \sum_{y \in \mathbb{F}_p^*} c_p^{f^*(\beta)}.
\]

If \( f^*(\beta) = 0 \), then

\[
A = \varepsilon(p - 1)^2 \sqrt{p^{-m}}.
\]

If \( f^*(\beta) \neq 0 \), then

\[
A = \varepsilon(p - 1) \sqrt{p^{-m}} \sigma_{f^*(\beta)} (\sum_{y \in \mathbb{F}_p^*} c_p^y).
\]

From \( \sum_{y \in \mathbb{F}_p^*} c_p^y = -1 \), we have

\[
A = -\varepsilon(p - 1) \sqrt{p^{-m}}.
\]

When \( m \) is odd, then

\[
A = \varepsilon(p - 1) \sqrt{p^{-m}} \sum_{y \in \mathbb{F}_p^*} \eta(y) c_p^{f^*(\beta)}.
\]

If \( f^*(\beta) = 0 \), then

\[
A = \varepsilon(p - 1) \sqrt{p^{-m}} \sum_{y \in \mathbb{F}_p^*} \eta(y).
\]

From \( \sum_{y \in \mathbb{F}_p^*} \eta(y) = 0 \), we have \( A = 0 \).

If \( f^*(\beta) \neq 0 \), then

\[
A = \varepsilon(p - 1) \sqrt{p^{-m}} \sigma_{f^*(\beta)} (\sum_{y \in \mathbb{F}_p^*} \eta(y) c_p^y).
\]

From Lemma 2.1 we have

\[
A = \varepsilon(p - 1) \sqrt{p^{-m}} \eta^{f^*(\beta)} = \eta^{f^*(\beta)} \varepsilon(\eta(-1))^{(m+1)/2} (p - 1)^{p^{(m+1)/2}}.
\]

Hence, this lemma follows.

**Lemma 2.11:** Let \( \beta \in \mathbb{F}_q^* \) and \( f(x) \in \mathcal{R}_F \) with the sign \( \varepsilon \) of the Walsh transform. Let

\[
N_{f, \beta} = \# \{ x \in \mathbb{F}_q : f(x) = 0, \text{Tr}_q^m(\beta x) = 0 \}.
\]

(1) If \( m \) is even, then

\[
N_{f, \beta} = \begin{cases} p^{m-2} + \varepsilon(\eta(-1))^{m/2} (p - 1)^{p^{(m-2)/2}}, & f^*(\beta) = 0; \\ p^{m-2}, & f^*(\beta) \neq 0. \end{cases}
\]
(2) If $m$ is odd, then

$$N_{f, \beta} = \begin{cases} p^{m-2}, & f^*(\beta) = 0; \\ p^{m-2} + \eta(f^*(\beta))\varepsilon_i^{(m+1)/2}(-1)(p-1)p^{(m-3)/2}, & f^*(\beta) \neq 0. \end{cases}$$

Proof: From $\sum_{x \in \mathbb{F}_p} \zeta_p^{T_n(\alpha x)} = \begin{cases} 0, & a \in \mathbb{F}_p^\times; \\ p, & a = 0, \end{cases}$ we have

$$N_{f, \beta} = p^{-2} \sum_{x \in \mathbb{F}_q^\times} \left( \sum_{y \in \mathbb{F}_p} \zeta_p^{yf(x)} \right) \left( \sum_{z \in \mathbb{F}_p} \zeta_p^{zf(x)} \right) \zeta_p^{\beta x} = p^{-2} \sum_{y,z \in \mathbb{F}_p} \sum_{x \in \mathbb{F}_q} \zeta_p^{yf(x) + zf(x) + \beta x} = p^{-2} \sum_{y \in \mathbb{F}_p^\times} \sum_{x \in \mathbb{F}_q} \zeta_p^{yf(x) + 0 \cdot \zeta_p^{T_n(\beta x)}} + p^{-2} \sum_{y,z \in \mathbb{F}_p^\times} \sum_{x \in \mathbb{F}_q} \zeta_p^{yf(x) + z \cdot \zeta_p^{T_n(\beta x)}}$$

$$= p^{-2} \sum_{y \in \mathbb{F}_p^\times} \sum_{x \in \mathbb{F}_q} \zeta_p^{yf(x) + z \cdot \zeta_p^{T_n(\beta x)}} = p^{-2} \sum_{y,z \in \mathbb{F}_p^\times} \sum_{x \in \mathbb{F}_q} \zeta_p^{yf(x) + z \cdot \zeta_p^{T_n(\beta x)}} = p^{-2} \sum_{y \in \mathbb{F}_p^\times} \sum_{x \in \mathbb{F}_q} \zeta_p^{yf(x) + z \cdot \zeta_p^{T_n(\beta x)}}.$$

When $m$ is even, from Lemma 2.9 and lemma 2.10

If $f^*(\beta) = 0$, then

$$N_{f, \beta} = p^{m-2} + \varepsilon(p-1)\sqrt{p^m} + \varepsilon(p-1)^2\sqrt{p^m} = p^{m-2} + \varepsilon(p-1)\sqrt{p^m} = p^{m-2} + \varepsilon(p-1)\sqrt{p^m}p = p^{m-2} + \varepsilon(p-1)\sqrt{p^m}p^{-1} = p^{m-2} + \varepsilon(p-1)p^{(m-2)/2}.$$ 

If $f^*(\beta) \neq 0$, then

$$N_{f, \beta} = p^{m-2}.$$ 

When $m$ is odd, from Lemma 2.9 and lemma 2.10

If $f^*(\beta) = 0$, then

$$N_{f, \beta} = p^{m-2}.$$ 

If $f^*(\beta) \neq 0$, then

$$N_{f, \beta} = p^{m-2} + \varepsilon\eta(f^*(\beta))(\eta(-1))^{(m+1)/2}(p-1)p^{(m-3)/2}. $$

Hence, this lemma follows.

**Lemma 2.12:** Let $f(x) \in \mathbb{R}\mathbb{F}$, then

$$\sum_{y \in \mathbb{F}_p^\times} \sum_{x \in \mathbb{F}_q} \zeta_p^{yf(x)} = \varepsilon(p-1)\sqrt{p^m},$$

where $\varepsilon$ is the sign of the Walsh transform of $f(x)$.

**Proof:** Let $A = \sum_{y \in \mathbb{F}_p^\times} \sum_{x \in \mathbb{F}_q} \zeta_p^{yf(x)}$. Then

$$A = \sum_{x \in \mathbb{F}_q} \sum_{y \in \mathbb{F}_p^\times} \zeta_p^{yf(x)} = \sum_{x \in \mathbb{F}_q} \sum_{y \in \mathbb{F}_p^\times} \zeta_p^{yf(x)} - q.$$ 

From Lemma 2.3 we have

$$A = N_f(0)p + N_f(sq)\sqrt{p^m} - N_f(nsq)\sqrt{p^m} - q,$$

where $N_f(sq) = \#\{x \in \mathbb{F}_q : f(x) \in \mathbb{F}_p^{\times 2}\}$ and $N_f(nsq) = \#\{x \in \mathbb{F}_q : f(x) \in \mathbb{F}_p^{\times} \setminus \mathbb{F}_p^{\times 2}\}$.

When $m$ is even, from Lemma 2.7 we have

$$N_f(sq) = N_f(nsq).$$

Further, we have

$$A = [p^{m-1} + \varepsilon(p-1)(\eta(-1))^{m/2}p^{(m-2)/2}]p - q = \varepsilon(p-1)\sqrt{p^m}.$$ 

When $m$ is odd, from Lemma 2.7 we have

$$A = p^{m-1} + \frac{p-1}{2}(p^{m-1} + \varepsilon\sqrt{p^m})\sqrt{p^m} - \frac{p-1}{2}(p^{m-1} - \varepsilon\sqrt{p^m})\sqrt{p^m} - q = \varepsilon(p-1)\sqrt{p^m}. $$
Hence, this lemma follows.

**Lemma 2.13:** Let \( f(x) \in \mathcal{R}F \) and \( \beta \in \mathbb{F}_q^\times \). Then

\[
\sum_{y \in \mathbb{F}_p^\times} \sum_{x \in \mathbb{F}_q} \zeta_p^y f(x) + z Tr^n_m(\beta x) = \begin{cases} 
\varepsilon(p-1)^2 \sqrt{p}^m, & f^*(\beta) = 0; \\
\varepsilon(p-1) \sqrt{p}^m (\sqrt{p} - 1), & f^*(\beta) \in \mathbb{F}_p^{\times 2}; \\
-\varepsilon(p-1) \sqrt{p}^m (\sqrt{p} + 1), & f^*(\beta) \in \mathbb{F}_p \setminus \mathbb{F}_p^{\times 2}.
\end{cases}
\]

**Proof:** Let \( A = \sum_{y \in \mathbb{F}_p^\times} \sum_{x \in \mathbb{F}_q} \zeta_p^y f(x) + z Tr^n_m(\beta x) \). Let \( l \) be an integer such that \( l(h-1) \equiv 1 \mod (p-1) \). Then

\[
A = \sum_{y \in \mathbb{F}_p^\times} \sum_{x \in \mathbb{F}_q} \zeta_p^y (\sum_{y \in \mathbb{F}_q} \zeta_p^y f(x) + z Tr^n_m(\beta x))
\]

Since \( y^2 (\frac{\sqrt{y}}{y})^l = y^2 (\frac{\sqrt{y}}{y})^l = z (\frac{\sqrt{y}}{y})^l \),

\[
A = \sum_{y \in \mathbb{F}_p^\times} \sigma_z(\frac{\sqrt{y}}{y})^l ( \sum_{x \in \mathbb{F}_q} \zeta_p^x f(x) + Tr^n_m(\beta x) )
\]

As \( y \) runs through \( \mathbb{F}_p^\times \), \( (\frac{\sqrt{y}}{y})^l \) will run through \( \mathbb{F}_p^{\times 2} \) and every value in \( \mathbb{F}_p^{\times 2} \) is taken twice. Then

\[
A = \sum_{z \in \mathbb{F}_p^\times} \sum_{y \in \mathbb{F}_p^\times} \sigma_{y^2} (W_f(\beta))
\]

\[
= (p-1) \sum_{y \in \mathbb{F}_p^\times} \sigma_{y^2} (W_f(\beta))
\]

\[
= (p-1) \sum_{y \in \mathbb{F}_p^\times} \sigma_{y^2} (\varepsilon \sqrt{p}^m \zeta_p^f(\beta))
\]

\[
= \varepsilon(p-1) \sqrt{p}^m \sum_{y \in \mathbb{F}_p^\times} \sigma_{y^2} (\zeta_p^f(\beta))
\]

\[
= \varepsilon(p-1) \sqrt{p}^m \sum_{y \in \mathbb{F}_p^\times} \zeta_p^y f^*(\beta)
\]

Hence,

\[
A = \varepsilon(p-1) \sqrt{p}^m \sum_{y \in \mathbb{F}_p^\times} \zeta_p^y f^*(\beta) - \varepsilon(p-1) \sqrt{p}^m.
\]

From Lemma 2.3 if \( f^*(\beta) = 0 \), then \( A = \varepsilon(p-1)^2 \sqrt{p}^m \).

If \( f^*(\beta) \in \mathbb{F}_p^{\times 2} \), then \( A = \varepsilon(p-1) \sqrt{p}^m (\sqrt{p} - 1) \).

If \( f^*(\beta) \in \mathbb{F}_p \setminus \mathbb{F}_p^{\times 2} \), then \( A = -\varepsilon(p-1) \sqrt{p}^m (\sqrt{p} + 1) \).

Hence, this lemma follows.

**Lemma 2.14:** Let \( f(x) \in \mathcal{R}F \) and \( \beta \in \mathbb{F}_q^\times \). Let

\[
N_{sq, \beta} = \# \{ x \in \mathbb{F}_q : f(x) \in \mathbb{F}_p^{\times 2}, Tr^n_m(\beta x) = 0 \},
\]

\[
N_{nsq, \beta} = \# \{ x \in \mathbb{F}_q : f(x) \in \mathbb{F}_p \setminus \mathbb{F}_p^{\times 2}, Tr^n_m(\beta x) = 0 \}.
\]

(1) If \( m \) is even, then

\[
N_{sq, \beta} = \begin{cases} 
\frac{p-1}{p^m} \left[ p^{m-2} - \varepsilon(\eta(-1)) m/2 / p^{(m-2)/2} \right], & f^*(\beta) = 0 \text{ or } f^*(\beta) \in \mathbb{F}_p \setminus \mathbb{F}_p^{\times 2}; \\
\frac{p-1}{p^2} \left[ p^{m-2} + \varepsilon(\eta(-1)) m/2 / p^{(m-2)/2} \right], & f^*(\beta) \in \mathbb{F}_p^{\times 2}.
\end{cases}
\]
\[ N_{nsq,\beta} = \begin{cases} \frac{p-1}{2} [p^{m-2} - \varepsilon (\eta(-1))^{m/2} p^{(m-2)/2}], & f^*(\beta) = 0 \text{ or } f^*(\beta) \in \mathbb{F}_p^2; \\ \frac{p-1}{2} [p^{m-2} + \varepsilon (\eta(-1))^{m/2} p^{(m-2)/2}], & f^*(\beta) \in \mathbb{F}_p^\times \setminus \mathbb{F}_p^2. \end{cases} \]

(2) If \( m \) is odd, then

\[ N_{sq,\beta} = \begin{cases} \frac{p-1}{2} [p^{m-2} + \varepsilon \sqrt{p}^{m-1}], & f^*(\beta) = 0; \\ \frac{p-1}{2} [p^{m-2} - \varepsilon \sqrt{p}^{m-1}], & f^*(\beta) \in \mathbb{F}_p^\times. \\
\end{cases} \]

\[ N_{nsq,\beta} = \begin{cases} \frac{p-1}{2} [p^{m-2} - \varepsilon \sqrt{p}^{m-1}], & f^*(\beta) = 0; \\ \frac{p-1}{2} [p^{m-2} - \varepsilon \sqrt{p}^{m-1}], & f^*(\beta) \in \mathbb{F}_p^\times. \\
\end{cases} \]

Proof: Let \( A = \sum_{x \in \mathbb{F}_p} (\sum_{y \in \mathbb{F}_p} \zeta_p y^2 f(x)) (\sum_{z \in \mathbb{F}_p} \zeta_p z^{2 \sqrt{p}} \sqrt{z} \beta z). \) Note that

\[ \sum_{z \in \mathbb{F}_p} \zeta_p \sqrt{z} \beta z = \begin{cases} p, & \text{Tr}_1^m(\beta x) = 0; \\ 0, & \text{Tr}_1^m(\beta x) \neq 0. \end{cases} \]

and

\[ \sum_{y \in \mathbb{F}_p} \zeta_p y^2 f(x) = \begin{cases} p, & f(x) = 0; \\ \sqrt{p}, & f(x) \in \mathbb{F}_p^\times; \\ -\sqrt{p}, & f(x) \in \mathbb{F}_p^\times \setminus \mathbb{F}_p^2. \end{cases} \]

Then, we have

\[ A = N_{f,\beta} p^2 + N_{sq,\beta} (\sqrt{p^*}) p + N_{nsq,\beta} (-\sqrt{p^*}) p = N_{f,\beta} p^2 + (N_{sq,\beta} - N_{nsq,\beta}) p \sqrt{p^*}, \]

where \( N_{f,\beta} = \{ x \in \mathbb{F}_q : f(x) = 0, \text{Tr}_1^m(\beta x) = 0 \}. \) Further, we have

\[ A = \sum_{z \in \mathbb{F}_p^\times} \sum_{x \in \mathbb{F}_q} \zeta_p \sqrt{z p^x} \zeta_p \text{Tr}_1^m(\beta x). \]

From Lemma 2.12, we have

\[ A = q + \varepsilon (p - 1) \sqrt{p^*} \text{Tr}_1^m + \sum_{y,z \in \mathbb{F}_p^\times} \zeta_p y^2 f(x) \sqrt{z \text{Tr}_1^m(\beta x)}. \]

When \( m \) is even, from Lemma 2.13, if \( f^*(\beta) = 0 \), then

\[ A = q + \varepsilon (p - 1) \sqrt{p^*} \text{Tr}_1^m + \varepsilon (p - 1)^2 \sqrt{p^*} \text{Tr}_1^m = q + \varepsilon (p - 1) p \sqrt{p^*}. \]

From Equation (4),

\[ N_{sq,\beta} = N_{nsq,\beta} = \frac{p-1}{2} [p^{m-2} - \varepsilon (\eta(-1))^{m/2} p^{(m-2)/2}], \]

If \( f^*(\beta) \in \mathbb{F}_p^\times \), then

\[ A = q + \varepsilon (p - 1) \sqrt{p^*} \text{Tr}_1^m + \varepsilon (p - 1) \sqrt{p^*} \text{Tr}_1^m (\sqrt{p^*} - 1) = q + \varepsilon (p - 1) \sqrt{p^*} \text{Tr}_1^{m+1}. \]

From Equation (4), we have

\[ N_{sq,\beta} = \frac{p-1}{2} [p^{m-2} + \varepsilon (\eta(-1))^{m/2} p^{(m-2)/2}], \]

\[ N_{nsq,\beta} = \frac{p-1}{2} [p^{m-2} - \varepsilon \eta^{m/2} (-1) p^{(m-2)/2}], \]

If \( f^*(\beta) \in \mathbb{F}_p^\times \setminus \mathbb{F}_p^2 \), then

\[ A = q + \varepsilon (p - 1) \sqrt{p^*} \text{Tr}_1^m - \varepsilon (p - 1) \sqrt{p^*} (\sqrt{p^*} + 1) = q - \varepsilon (p - 1) \sqrt{p^*} \text{Tr}_1^{m+1}. \]
From Equation (4), we have

\[ N_{sq, \beta} = \frac{p-1}{2} [p^{m-2} - \varepsilon (\eta(-1))^{m/2} (p^{m-2})^{2/2}], \]
\[ N_{nsq, \beta} = \frac{p-1}{2} [p^{m-2} + \varepsilon \eta^{m/2} (-1) (p^{m-2})^{2/2}]. \]

When \( m \) is odd, from Lemma 2.13 if \( f^*(\beta) = 0 \), then

\[ A = q + \varepsilon (p-1) \sqrt{p^m} + \varepsilon (p-1)^2 \sqrt{p^m} = q + \varepsilon (p-1) p \sqrt{p^m}. \]

From Equation (4), we have

\[ N_{sq, \beta} = \frac{p-1}{2} [p^{m-2} + \varepsilon \sqrt{p^{m-1}}], \]
\[ N_{nsq, \beta} = \frac{p-1}{2} [p^{m-2} - \varepsilon \sqrt{p^{m-1}}]. \]

If \( f^*(\beta) \in \mathbb{F}_p^2 \), then

\[ A = q + \varepsilon (p-1) \sqrt{p^{m+1}}. \]

From Equation (4), we have

\[ N_{sq, \beta} = N_{nsq, \beta} = \frac{p-1}{2} [p^{m-2} - \varepsilon \sqrt{p^{m-3}}]. \]

If \( f^*(\beta) \in \mathbb{F}_p \setminus \mathbb{F}_p^2 \), then

\[ A = q - \varepsilon (p-1) \sqrt{p^{m+1}}. \]

From Equation (4), we have

\[ N_{sq, \beta} = N_{nsq, \beta} = \frac{p-1}{2} [p^{m-2} + \varepsilon \sqrt{p^{m-3}}]. \]

Hence, this lemma follows.

III. THE WEIGHT DISTRIBUTIONS OF LINEAR CODES FROM WEAKLY REGULAR BENT FUNCTIONS

In this section, we generalize the construction method of linear codes with few weights by Ding et al.\cite{5, 6} to general weakly regular bent functions and determine the weight distributions of the corresponding linear codes.

Let \( f(x) \) be a \( p \)-ary function mapping from \( \mathbb{F}_q \) to \( \mathbb{F}_p \). Define

\[ D_f = \{ x \in \mathbb{F}_q^* : f(x) = 0 \}. \]

Let \( n = \#(D_f) \) and \( D_f = \{ d_1, d_2, \ldots, d_n \} \). A linear code defined from \( D_f \) is

\[ C_{D_f} = \{ c_\beta : \beta \in \mathbb{F}_q \}, \]

where \( c_\beta = (\text{Tr}_{1}^{x}(\beta d_1), \text{Tr}_{1}^{x}(\beta d_2), \ldots, \text{Tr}_{1}^{x}(\beta d_n)) \). For a general function \( f(x) \), it is difficult to determine the weight distribution of \( C_{D_f} \). However, for some special function \( f(x) \), this problem can be solved. Ding et al.\cite{5} determined the weight distribution of \( C_{D_f} \) for \( f(x) = \text{Tr}_{1}^{m}(x^2) \) and proposed an open problem on determining the weight distribution of \( C_{D_f} \) for general planar functions \( F(x) \), where \( f(x) = \text{Tr}_{1}^{m}(F(x)) \). Zhou et al.\cite{21} solved the weight distribution of \( C_{D_f} \) for the case that \( F(x) \) is a quadratic planar function. We generalize their work to weakly regular bent functions and solve the open problem by Ding et al.\cite{6}. Our results on linear codes \( C_{D_f} \) from weakly regular bent functions in \( \mathcal{R} \) are listed in the following theorems and corollaries.

Theorem 3.1: Let \( m \) be even and \( \varepsilon f(x) \in \mathcal{R} \) with the sign \( \varepsilon \) of the Walsh transform. Then \( C_{D_f} \) is a two-weight linear code with parameters \([p^{m-1} - 1 + \varepsilon (p-1) p^{m-2}/2, m]\), whose weight distribution is listed in Table I.

| Weight | Multiplicity |
|--------|--------------|
| 0      | \( (p-1)p^{m-2} \) |
| \( (p-1)p^{m-2} + \varepsilon (\eta(-1))^{m/2} p^{m-2}/2 \) | \( p^{m-1} + \varepsilon (p-1) p^{m-2}/2 \) |
| \( (p-1)p^{m-2} + \varepsilon (\eta(-1))^{m/2} p^{m-2}/2 \) | \( (p-1)p^{m-1} - \varepsilon (\eta(-1))^{m/2} p^{m-2}/2 \) |

Proof: From Lemma 2.7 and Lemma 2.11 this theorem follows.

Theorem 3.2: Let \( m \) be odd and \( \varepsilon f(x) \in \mathcal{R} \). Then \( C_{D_f} \) is a three-weight linear code with parameters \([p^{m-1} - 1, m]\), whose weight distribution is listed in Table II.

Proof: From Lemma 2.7 and Lemma 2.11 this theorem follows.
Let \( f(x) \in \mathcal{RF} \). For any \( a \in \mathbb{F}_p^* \) and \( x \in \mathbb{F}_q \), \( f(x) = 0 \) if and only if \( f(ax) = a^h f(x) = 0 \). Then we can select a subset \( \mathcal{J}_f \) of \( D_f \) such that \( \bigcup_{a \in \mathbb{F}_p^*} a \mathcal{J}_f \) is just a partition of \( D_f \). Hence, the code \( C_{\mathcal{J}_f} \) can be punctured into a shorter linear codes \( C_{\mathcal{J}_f} \), whose parameters and the weight distributions are given in the following two corollaries.

**Corollary 3.3:** Let \( m \) be even and \( f(x) \in \mathcal{RF} \) with the sign \( \epsilon \) of the Walsh transform. Then \( C_{\mathcal{J}_f} \) is a two-weight linear code with parameters \( [\frac{p^{m-1}-1}{p-1} + \varepsilon p^{(m-2)/2}, m] \), whose weight distribution is listed in Table III.

**Proof:** From Theorem 3.1 this corollary follows.

**Corollary 3.4:** Let \( m \) be odd and \( f(x) \in \mathcal{RF} \). Then \( C_{\mathcal{J}_f} \) is a three-weight linear code with parameters \( [(p^{m-1}-1)/(p-1), m] \), whose weight distribution is listed in Table IV.

**Proof:** From Theorem 3.2 this corollary follows.

**Remark** When \( m \) is even, from Theorem 3.1 and Corollary 3.3 parameters and weight distributions of \( C_{D_f} \) and \( C_{\mathcal{J}_f} \) are determined by the sign of the Walsh transform of \( f(x) \) and have two cases. Therefore, these linear codes can be obtained by \( f(x) = \text{Tr}_1^m(x^2) \) and \( f(x) = \text{Tr}_1^m(\alpha x^2) \), where \( \alpha \) is a quadratic nonresidue in \( \mathbb{F}_q \).

When \( m \) is odd, from Theorem 3.2 and Corollary 3.4 parameters and weight distributions of \( C_{D_f} \) are all the same for any the weakly regular bent function \( f(x) \) in \( \mathcal{RF} \). This holds also for \( C_{\mathcal{J}_f} \). Therefore, this class of linear codes can be obtained by \( f(x) = \text{Tr}_1^m(x^2) \).

**IV. NEW TWO-WEIGHT AND THREE-WEIGHT LINEAR CODES FROM WEAKLY REGULAR BENT FUNCTIONS**

In this section, by choosing defining sets different from that in Section 3, we construct new linear codes with two weight or three weight and determine their weight distributions. Define

\[
\begin{align*}
D_{f,nsq} &= \{ x \in \mathbb{F}_q : f(x) \in \mathbb{F}_p^* \setminus \mathbb{F}_p^2 \}, \\
D_{f,sk} &= \{ x \in \mathbb{F}_q : f(x) \in \mathbb{F}_p^2 \},
\end{align*}
\]

where \( f(x) \in \mathcal{RF} \).

**Theorem 4.1:** Let \( m \) be even. Let \( f(x) \in \mathcal{RF} \) with the sign \( \epsilon \) of the Walsh transform. Then \( C_{D_{f,nsq}} \) and \( C_{D_{f,sk}} \) are two-weight linear codes with the same parameters \( [\frac{p^{m-1}-1}{p-1} - \epsilon (\eta(-1))^{m/2} (p-1)p^{(m-2)/2}, m] \) and the same weight distribution in Table IV.

**Proof:** From Lemma 2.7 and Lemma 2.14 this theorem follows.

**Example** Let \( p = 3 \), \( m = 6 \), and \( f(x) = \text{Tr}_1^6(w^7 x^{210}) \), where \( w \) is a primitive element of \( \mathbb{F}_{3^6} \). The sign of the Walsh transform of \( f(x) \) is \( \epsilon = 1 \). Then \( C_{D_{f,nsq}} \) and \( C_{D_{f,sk}} \) in Theorem 4.1 have the same parameters \( [252, 6, 162] \) and the same weight enumerator \( 1 + 476z^{162} + 252z^{180} \), which is verified by the Magma program.
Example Let $p = 3$, $m = 6$, and $f(x) = \text{Tr}_1^6(x^{10})$. The sign of the Walsh transform of $f(x)$ is $\varepsilon = -1$. Then $C_{D_f,nsq}$ and $C_{D_{f,eq}}$ in Theorem 4.1 have the same parameters $[234, 6, 144]$ and the same weight enumerator $1 + 234z^{144} + 494z^{162}$, which is verified by the Magma program.

Example Let $p = 5$, $m = 6$, and $f(x) = \text{Tr}_1^6(x^{26})$. The sign of the Walsh transform of $f(x)$ is $\varepsilon = -1$. Then $C_{D_{f,nsq}}$ and $C_{D_{f,eq}}$ in Theorem 4.1 have the same parameters $[6300, 6, 5000]$ and the same weight enumerator $1 + 9324z^{5000} + 6300z^{6100}$, which is verified by the Magma program.

Example Let $p = 5$, $m = 6$, and $f(x) = \text{Tr}_1^6(wx^{26})$, where $w$ is a primitive element of $\mathbb{F}_{5^5}$. The sign of the Walsh transform of $f(x)$ is $\varepsilon = 1$. Then $C_{D_{f,nsq}}$ and $C_{D_{f,eq}}$ in Theorem 4.1 have the same parameters $[6200, 6, 4900]$ and the same weight enumerator $1 + 6200z^{4900} + 9424z^{5000}$, which is verified by the Magma program.

Theorem 4.2: Let $m$ be odd and $f(x) \in R_F$ with the sign $\varepsilon$ of the Walsh transform. Then $C_{D_{f,eq}}$ is a three-weight linear code with parameters $[\frac{p-1}{2}(p^{m-1} - \varepsilon \sqrt{p^{m-1}}), m]$ and the weight distribution in Table VII

| Weight | Multiplicity |
|--------|--------------|
| 0      | $1$          |
| $\frac{p-1}{2}p^{m-2}$ | $p^{m-1} - 1$ |
| $\frac{p-1}{2}(p-1)p^{m-2} + (1-p^*)\sqrt{p^{m-1}} - 1$ | $\frac{p^{m-1} + \varepsilon(1-p^*)\sqrt{p^{m-1}}}{2}$ |
| $\frac{p-1}{2}(p-1)p^{m-2} + \varepsilon(1-p^*)\sqrt{p^{m-1}} - 1$ | $\frac{p^{m-1} - \varepsilon(1-p^*)\sqrt{p^{m-1}}}{2}$ |

Proof: From Lemma 2.7 and Lemma 2.14 this theorem follows.

Example Let $p = 5$, $m = 5$, and $f(x) = \text{Tr}_1^5(x^2)$. The sign of the Walsh transform of $f(x)$ is $\varepsilon = 1$. Then the code $C_{D_{f,eq}}$ has parameters $[1200, 5, 940]$, which is verified by the Magma program.

Example Let $p = 3$, $m = 5$, and $f(x) = \text{Tr}_1^5(wx^2)$, where $w$ is a primitive element of $\mathbb{F}_{3^5}$. The sign of the Walsh transform of $f(x)$ is $\varepsilon = -1$. Then the code $C_{D_{f,eq}}$ in Theorem 4.2 has parameters $[60, 5, 40]$ and weight enumerator $1 + 24z^{40} + 40z^{48} + 60z^{52}$, which is verified by the Magma program.

Theorem 4.3: Let $m$ be odd and $f(x) \in R_F$ with the sign $\varepsilon$ of the Walsh transform. Then $C_{D_{f,eq}}$ is a three-weight linear code with parameters $[\frac{p-1}{2}(p^{m-1} - \varepsilon \sqrt{p^{m-1}}), m]$ and the weight distribution in Table VII

| Weight | Multiplicity |
|--------|--------------|
| 0      | $1$          |
| $\frac{p-1}{2}p^{m-2}$ | $p^{m-1} - 1$ |
| $\frac{p-1}{2}(p-1)p^{m-2} + (1-p^*)\sqrt{p^{m-1}} - 1$ | $\frac{p^{m-1} + \varepsilon(1-p^*)\sqrt{p^{m-1}}}{2}$ |
| $\frac{p-1}{2}(p-1)p^{m-2} + \varepsilon(1-p^*)\sqrt{p^{m-1}} - 1$ | $\frac{p^{m-1} - \varepsilon(1-p^*)\sqrt{p^{m-1}}}{2}$ |

Proof: From Lemma 2.7 and Lemma 2.14 this theorem follows.

Example Let $p = 5$, $m = 5$, and $f(x) = \text{Tr}_1^5(x^2)$. The sign of the Walsh transform of $f(x)$ is $\varepsilon = 1$. Then the code $C_{D_{f,eq}}$ in Theorem 4.3 has parameters $[1300, 5, 1000]$ and weight enumerator $1 + 624z^{1000} + 1200z^{1040} + 1300z^{1060}$, which is verified by the Magma program.

Example Let $p = 3$, $m = 5$, and $f(x) = \text{Tr}_1^5(wx^2)$, where $w$ is a primitive element of $\mathbb{F}_{3^5}$. The sign of the Walsh transform of $f(x)$ is $\varepsilon = -1$. Then the code $C_{D_{f,eq}}$ in Theorem 4.3 has parameters $[40, 5, 28]$ and weight enumerator $1 + 40z^{28} + 60z^{32} + 24z^{40}$, which is verified by the Magma program.

Let $f(x) \in \mathcal{R}_F$. There exists an integer $h$ such that $(h - 1, p - 1)$ and $f(ax) = a^h f(x)$ for any $a \in \mathbb{F}_p^\times$ and $x \in \mathbb{F}_q^\times$. Note that $m$ is even. Therefore, $f(ax)$ is a quadratic residue (quadratic nonresidue) in $\mathbb{F}_p^\times$ if and only if $f(x)$ is a quadratic residue (quadratic nonresidue) in $\mathbb{F}_p^\times$. With the similar definition of $\overline{D}_f$, we define $\overline{D}_{f,eq}$ as a subset of $D_{f,eq}$ such that
Let \( f(x) \in \mathcal{R} \mathcal{F} \) with the sign \( \varepsilon \) of the Walsh transform. Then \( C_{\overline{D}_f,n_{sq}} \) and \( C_{\overline{D_f},m_{sq}} \) are two-weight linear codes with the same parameters \( \left\lceil \frac{1}{2}(p^{m-1} - \varepsilon(\eta(-1))m/2)p^{m-2}/2, m \right\rceil \) and the same weight distribution in Table VIII.

**Table VIII**

| Weight | Multiplicity |
|--------|--------------|
| \( \frac{1}{p}p^{m-2} \) | \( \frac{1}{2} \) |
| \( \frac{1}{p}p^{m-2} + \frac{1}{p}p^{m-2} \) | \( \frac{1}{2} \) |

**Proof:** From Theorem 4.1 this corollary follows.

**Example** Let \( p = 3, m = 4, \) and \( f(x) = \text{Tr}_4^1(x^2) \). The sign of the Walsh transform of \( f(x) \) is \( \varepsilon = -1 \). Then \( C_{\overline{D}_f,n_{sq}} \) and \( C_{\overline{D_f},m_{sq}} \) in Corollary 4.4 have the same parameters \([15, 4, 9] \) and the same weight enumerator \( 1 + 50z^9 + 30z^{12} \), which is verified by the Magma program. This code is optimal due to the Griesmer bound.

**Example** Let \( p = 3, m = 4, \) and \( f(x) = \text{Tr}_4^1(wx^2) \), where \( w \) is a primitive element of \( \mathbb{F}_{27} \). The sign of the Walsh transform of \( f(x) \) is \( \varepsilon = 1 \). Then \( C_{\overline{D}_f,n_{sq}} \) and \( C_{\overline{D_f},m_{sq}} \) in Corollary 4.4 have the same parameters \([12, 6, 4] \) and the same weight enumerator \( 1 + 24z^6 + 56z^9 \), which is verified by the Magma program. This code is optimal due to the Griesmer bound.

**Example** Let \( p = 3, m = 6, \) and \( f(x) = \text{Tr}_4^3(wx^2) \), where \( w \) is a primitive element of \( \mathbb{F}_{27} \). The sign of the Walsh transform of \( f(x) \) is \( \varepsilon = 1 \). Then \( C_{\overline{D}_f,n_{sq}} \) and \( C_{\overline{D_f},m_{sq}} \) in Corollary 4.4 have the same parameters \([126, 6, 81] \) and the same weight enumerator \( 1 + 476z^{81} + 252z^{90} \), which is verified by the Magma program. This code is optimal due to the Griesmer bound.

**Example** Let \( p = 5, m = 4, \) and \( f(x) = \text{Tr}_5^1(x^2) \), where \( w \) is a primitive element of \( \mathbb{F}_{5^4} \). The sign of the Walsh transform of \( f(x) \) is \( \varepsilon = 1 \). Then \( C_{\overline{D}_f,n_{sq}} \) and \( C_{\overline{D_f},m_{sq}} \) in Corollary 4.4 have the same parameters \([65, 4, 50] \) and the same weight enumerator \( 1 + 364z^{50} + 260z^{55} \), which is verified by the Magma program. This code is optimal due to the Griesmer bound.

**Example** Let \( p = 5, m = 4, \) and \( f(x) = \text{Tr}_5^1(wx^2) \), where \( w \) is a primitive element of \( \mathbb{F}_{5^5} \). The sign of the Walsh transform of \( f(x) \) is \( \varepsilon = 1 \). Then \( C_{\overline{D}_f,n_{sq}} \) and \( C_{\overline{D_f},m_{sq}} \) in Corollary 4.4 have the same parameters \([60, 4, 45] \) and the same weight enumerator \( 1 + 240z^{45} + 384z^{50} \), which is verified by the Magma program. This code is almost optimal since the optimal code with length 60 and dimension 4 has minimal weight 51.

**Corollary 4.5** Let \( m \) be odd and \( f(x) \in \mathcal{R} \mathcal{F} \) with the sign \( \varepsilon \) of the Walsh transform. Then \( C_{\overline{D}_f,n_{sq}} \) is a three-weight linear code with parameters \([\frac{1}{2}(p^{m-1} - \varepsilon(\eta(-1))\sqrt{p^{m-1}}), m] \) and the weight distribution in Table IX.

**Table IX**

| Weight | Multiplicity |
|--------|--------------|
| \( \frac{1}{2}p^{m-2} \) | \( \frac{1}{2}p^{m-1} \) |
| \( \frac{1}{2}p^{m-2} + \frac{1}{2}p^{m-2} \) | \( \frac{1}{2}p^{m-1} \) |

**Proof:** From Theorem 4.2 this corollary follows.

**Example** Let \( p = 3, m = 5, \) and \( f(x) = \text{Tr}_5^2(x^2) \), where \( w \) is a primitive element of \( \mathbb{F}_{3^5} \). The sign of the Walsh transform of \( f(x) \) is \( \varepsilon = 1 \). Then \( C_{\overline{D}_f,n_{sq}} \) in Corollary 4.5 has parameters \([36, 5, 21] \) and the weight enumerator \( 1 + 72z^{21} + 90z^{24} + 80z^{27} \), which is verified by the Magma program. This code is almost optimal since the optimal code with length 36 and dimension 5 has minimal weight 22.

**Example** Let \( p = 3, m = 5, \) and \( f(x) = \text{Tr}_5^2(wx^2) \), where \( w \) is a primitive element of \( \mathbb{F}_{3^5} \). The sign of the Walsh transform of \( f(x) \) is \( \varepsilon = -1 \). Then \( C_{\overline{D}_f,n_{sq}} \) in Corollary 4.5 has parameters \([45, 5, 27] \) and the weight enumerator \( 1 + 80z^{27} + 72z^{30} + 90z^{33} \), which is verified by the Magma program. This code is almost optimal since the optimal code with length 45 and dimension 5 has minimal weight 28.

**Corollary 4.6** Let \( m \) be odd and \( f(x) \in \mathcal{R} \mathcal{F} \) with the sign \( \varepsilon \) of the Walsh transform. Then \( C_{\overline{D}_f,m_{sq}} \) is a three-weight linear code with parameters \([\frac{1}{2}(p^{m-1} + \varepsilon\sqrt{p^{m-1}}), m] \) and the weight distribution in Table X.

**Proof:** From Theorem 4.3 this corollary follows.
The following work will study how to construct the linear codes with few weights from more general function $f$. We did not find the parameters of these linear codes in this paper in the literature. From the certain bound on linear codes, the weight distributions of these codes are determined by the sign of the Walsh transform of weakly regular bent functions. In fact, all these linear codes can be obtained from two functions $\alpha x$ and $\alpha x^2$, where $\alpha$ is a quadratic nonresidue of $\mathbb{F}_q$.

Example Let $p = 3$, $m = 3$, and $f(x) = \text{Tr}_3^m(wx^2)$, where $w$ is a primitive element of $\mathbb{F}_{3^2}$. The sign of the Walsh transform of $f(x)$ is $\varepsilon = -1$. Then $C_{f,sq}$ in Corollary 4.6 has parameters $[6, 3, 3]$ and the weight enumerator $1 + 8z^3 + 6z^4 + 12z^5$, which is verified by the Magma program. This code is optimal due to the Griesmer bound.

Example Let $p = 5$, $m = 3$, and $f(x) = \text{Tr}_3^m(wx^2)$, where $w$ is a primitive element of $\mathbb{F}_{5^2}$. The sign of the Walsh transform of $f(x)$ is $\varepsilon = -1$. Then $C_{f,sq}$ in Corollary 4.6 has parameters $[10, 3, 7]$ and the weight enumerator $1 + 40z^7 + 60z^8 + 24z^{10}$, which is verified by the Magma program. This code is optimal due to the Griesmer bound.

Example Let $p = 7$, $m = 3$, and $f(x) = \text{Tr}_3^m(x^2)$, where $w$ is a primitive element of $\mathbb{F}_{7^2}$. The sign of the Walsh transform of $f(x)$ is $\varepsilon = 1$. Then $C_{f,sq}$ in Corollary 4.6 has parameters $[21, 3, 17]$ and the weight enumerator $1 + 126z^{17} + 168z^{18} + 48z^{21}$, which is verified by the Magma program. This code is optimal due to the Griesmer bound.

Remark These linear codes constructed in this section are two-weight and three-weight codes. The weight distributions of these codes are determined by the sign of the Walsh transforms of weakly regular bent functions. In fact, all these linear codes can be obtained from two functions $f(x) = \text{Tr}_1^m(x^2)$ and $f(x) = \text{Tr}_1^m(\alpha x^2)$, where $\alpha$ is a quadratic nonresidue of $\mathbb{F}_q$.

V. Conclusion

In this paper, we construct linear codes with two weight or three weight from weakly regular bent functions. We first generalize the constructing method of Ding et al. [6] and Zhou et al. [21] and determine the weight distributions of these linear codes. We solve the open problem proposed by Ding et al. [6].

Further, by choosing defining sets different from Ding et al. [6] and Zhou et al. [21], we construct new linear codes with two weights or three weights from weakly regular bent functions, which contain some optimal linear codes with parameters meeting certain bound on linear codes. The weight distributions of these codes are determined by the sign of the Walsh transform of weakly regular bent functions. We did not find the parameters of these linear codes in this paper in the literature. From the point of application, all the linear codes constructed in this paper can be obtained by two functions $f(x) = \text{Tr}_1^m(x^2)$ and $f(x) = \text{Tr}_1^m(\alpha x^2)$, where $\alpha$ is a quadratic nonresidue of $\mathbb{F}_q$. The two-weight codes in this paper can be used in strongly regular graphs with the method in [2], and the three-weight codes in this paper can give association schemes introduced in [1]. The following work will study how to construct the linear codes with few weights from more general function $f(x)$.

ACKNOWLEDGMENT

This work was supported by the Natural Science Foundation of China (Grant No. 11401480, No. 10990011 & No. 61272499). Yanfeng Qi also acknowledges support from KSY075614050 of Hangzhou Dianzi University.

REFERENCES

[1] A. R. Calderbank and J. M. Goethals, "Three-weight codes and association schemes," Philips J. Res., vol. 39, pp. 143C152, 1984.
[2] A. R. Calderbank and W. M. Kantor, "The geometry of two-weight codes," Bull. London Math. Soc., vol. 18, pp. 97-122, 1986.
[3] C. Carlet, C. Ding, and J. Yuan, "Linear codes from perfect nonlinear mappings and their secret sharing schemes," IEEE Trans. Inform. Theory, vol. 51, no.6, pp. 2089-2102, 2005.
[4] R. S. Coulter, R. W. Matthews, "Planar functions and planes of Lenz-Barlotti class II," Des. Codes Cryptogr. 10 (1997), 167-184.
[5] C. Ding, "Linear codes from some 2-designs," IEEE Trans. Inform. Theory, vol. 61, no. 6, pp. 3265-3275, June 2015.
[6] K. Ding and C. Ding, "A class of two-weight and three-weight codes and their applications in secret sharing," arXiv:1503.06512
[7] K. Ding, C. Ding, "Binary linear codes with three weights," Trans. Inf. Theory, vol. 18, no. 11, pp. 1879-1882, November 2014.
[8] C. Ding, J. Luo and H. Niederreiter, "Two weight codes punctured from irreducible cyclic codes," in: Proc. of the First International Workshop on Coding Theory and Cryptography, pp. 119-124. Singapore, World Scientific, 2008.
[9] C. Ding and H. Niederreiter, "Cyclotomic linear codes of order 3," IEEE Trans. Inform. Theory, vol. 53, no. 6, pp. 2274-2277, 2007.
[10] C. Ding and X. Wang, "A coding theory construction of new systematic authentication codes," Theoretical Computer Science, vol. 330, pp. 81-99, 2005.
[11] K. Feng, J. Luo, "Value distributions of exponential sums from perfect nonlinear functions and their applications," Trans. Inf. Theory, vol. 53, no. 9, pp. 3035-3041, August 2007.
[12] G. Gong, T. Helleseth, H. Hu, and A. Kholosha. "On the Dual of Certain Ternary Weakly Regular Bent Functions," IEEE Trans. Inform. Theory, vol. 58, no. 4, pp. 2237-2243, April 2012.
[13] T. Helleseth, H. D. L. Hollmann, A. Kholosha, Z. Wang, and Q. Xiang, "Proofs of two conjectures on ternary weakly regular bent functions," IEEE Trans. Inf. Theory, vol. 55, no. 11, pp. 5272C5283, Nov. 2009.
[14] T. Helleseth and A. Kholosha, "Monomial and quadratic bent functions over the finite fields of odd characteristic," IEEE Trans. Inf. Theory, vol. 52, no. 5, pp. 2018-2032, May 2006.
[15] T. Helleseth and A. Kholosha, “On the dual of monomial quadratic p-ary bent functions,” in Sequences, Subsequences, and Consequences, ser. Lecture Notes in Computer Science, S. Golomb, G. Gong, T. Helleseth, and H. Y. Song, Eds. Berlin: Springer-Verlag, 2007, vol. 4893, pp. 50-61.

[16] T. Helleseth and A. Kholosha, “New binomial bent functions over the finite fields of odd characteristic,” IEEE Trans. Inf. Theory, vol. 56, no. 9, pp. 4646-4652, Sep. 2010.

[17] K. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory, 2nd ed. New York: Springer-Verlag, 1990, vol. 84, Graduate Texts in Mathematics.

[18] P.V. Kumar, R.A. Scholtz, L.R. Welch, “Generalized bent functions and their properties”, J. Combin. Theory Ser. A 40 (1985) 90-107.

[19] R. Lidl and H. Niederreiter, Finite Fields, Cambridge: Cambridge University Press, 1997.

[20] J. Yuan and C. Ding, “Secret sharing schemes from three classes of linear codes,” IEEE Trans. Inf. Theory, vol. 52, no. 1, pp. 206-212, Jan. 2006.

[21] Z. Zhou, N. Li, C. Fan, T. Helleseth. "Linear Codes with Two or Three Weights From Quadratic Bent Functions." [arXiv:1506.06830v1]