New self-orthogonal codes from weakly regular plateaued functions and their application in LCD codes

Melike Çakmak[1 [0000−0003−2505−5676]], Ahmet Sınak[2 [0000−0002−1071−765X]], and Oğuz Yayla[1 [0000−0001−8945−2780]]

[1] Department of Cryptography, Institute of Applied Mathematics, Middle East Technical University, Ankara, Turkey
[2] Department of Mathematics and Computer Science, Necmettin Erbakan University, 42090, Konya, Turkey
sinakahmet@gmail.com

Abstract. A linear code is considered self-orthogonal if it is contained within its dual code. Self-orthogonal codes have applications in linear complementary dual codes, quantum codes and so on. The construction of self-orthogonal codes from functions over finite fields has been studied in the literature. In this paper, we generalize the construction method given by Heng et al. (2023) to weakly regular plateaued functions. We first construct several families of ternary self-orthogonal codes from weakly regular plateaued unbalanced functions. Then we use the self-orthogonal codes to construct new families of ternary LCD codes. As a consequence, we obtain (almost) optimal ternary self-orthogonal codes and LCD codes. Moreover, we propose two new classes of p-ary linear codes from weakly regular plateaued unbalanced functions over the finite fields of odd characteristics.

Keywords: Linear code · self-orthogonal code · LCD code · weakly regular plateaued function

1 Introduction

Linear codes have important applications in secure communication [21], secret sharing schemes [1], [2], [4], [5], [9], [23], authentication codes [8] and secure two-party computation [19], [3]. A linear code is considered self-orthogonal if it is contained within its dual code. Self-orthogonal codes have also applications in linear complementary dual codes, quantum codes and so on. Hence, the construction of linear codes is an interesting research problem. Various methods exist for constructing linear codes and one approach involves utilizing functions defined over finite fields(e.g., [2], [6], [7], [9], [15], [19], [20]). Two generic constructions, referred to as the first and second generic constructions, for generating linear codes from functions have been identified in the literature. Several linear codes with good parameters have been constructed by using the second generic construction method(e.g., [6], [9]). Indeed, Heng et al.(2023) have constructed in [10] ternary self-orthogonal codes from weakly regular bent functions based on the second generic construction. This observation motivates us to construct linear codes from weakly regular plateaued functions over finite fields with odd characteristics. In this paper, we used the second construction method to obtain new families of linear codes with few weights.

The paper is organized as follows. Section 2 establishes the primary notation and provides a review of fundamental concepts in finite fields and coding theory. In Section 3, we give some results related to weakly regular plateaued functions. In Section 4 and 5, we construct several families of self-orthogonal codes and investigate their dual codes. In Section 6, we consider an application of ternary self-orthogonal codes in ternary LCD codes.

2 Preliminaries

Throughout this paper, we fix the following notation. For an odd prime p and a positive integer m, $q = p^m$ denotes the prime power and $\mathbb{F}_q$ is the finite field with q elements. Let α be an element in $\mathbb{F}_q$, then the trace of α over $\mathbb{F}_p$ is given by $\mathrm{Tr}_{p^m/p}(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + \ldots, \alpha^{p^{m-1}}$ and ξ_p denotes the complex primitive p-th root of unity. SQ and NSQ denote, respectively, all squares and non-squares in $\mathbb{F}_p^\star$ and also, η_0 denotes the quadratic characters of $\mathbb{F}_p^\star$. Finally, $p^\star$ denotes $\eta_0(-1)p$.

Cyclotomic Field $\mathbb{Q}(\xi_\mathbf{p})$. Let $\mathbb{Z}$ be the rational integer ring and $\mathbb{Q}$ be the rational field. Then we have the following fact about p-th cyclotomic field $\mathbb{Q}(\xi_p)$.

Lemma 1. *[11] The following results on $\mathbb{Q}(\xi_p)$ hold.*

1. *Let ξ_p be the p-th primitive root of complex unity. Then the ring of integers in $K := \mathbb{Q}(\xi_p)$ is $O_K = \mathbb{Z}(\xi_p)$ and $\{\xi_p^i : 1 \leq i \leq p-1\}$ is an integral basis of O_K*
2. *The field extention $K/\mathbb{Q}$is a Galois extension of degree $p-1$ with Galois group Gal$(K/\mathbb{Q}) = \{\sigma_a : a \in \mathbb{F}_p^\star\}$, where the automorphism σ_a of K is defined by $\sigma_a(\xi_p) = \xi_p^a$*
3. *The field K has unique quadratic subfield $L = \mathbb{Q}(\sqrt{p^\star})$. For $1 \leq a \leq p-1$, $\sigma_a(\sqrt{p^\star}) = \eta_0(a)\sqrt{p^\star}$. Therefore, the Galois group Gal$(K/\mathbb{Q})$ is $\{1, \sigma_\gamma\}$, where γ is a nonsquare in $\mathbb{F}_p^\star$.*

From Lemma 1, for any $a \in \mathbb{F}_p^\star$ and $b \in \mathbb{F}_p$, one can directly write

$$\sigma_a(\xi_p^b) = \xi_p^{ab} \quad \text{and} \quad \sigma_a(\sqrt{p^\star}^{\,m}) = \eta_0^m(a)\sqrt{p^\star}^{\,m}.$$

Characters over finite fields. Given $a \in \mathbb{F}_q$, the function

$$\phi_a(x) = \xi_p^{\mathrm{Tr}p^m/p(ax)}, x \in \mathbb{F}_q$$

defines an additive character of $\mathbb{F}_q$. The orthogonality relation of additive characters ([12]) is given by

$$\sum_{x \in \mathbb{F}_q} \phi_1(ax) = \begin{cases} q, & \text{if } a = 0, \\ 0, & \text{if } a \in \mathbb{F}_q^\star \end{cases}$$

Let α be a primitive element of $\mathbb{F}_q$. Then $\psi_j(\alpha^k) = \xi_{q-1}^{jk}$ for $k = 0, 1, \ldots, q-2$, where $0 \le j \le q-2$ denotes the multipcicative character of $\mathbb{F}_q$. The orthogonality relation of multiplicative characters ([12]) is given by

$$\sum_{x \in \mathbb{F}_q^{\star}} \psi_j(x) = \begin{cases} q-1, & \text{if } j = 0, \\ 0, & \text{if } j \neq 0 \end{cases}$$

2.1 Weakly regular plateaued functions

Let f be a p-ary function from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$. Let $q = p^m$. Then its Walsh transform is defined as

$$\mathcal{W}_f(\beta) = \sum_{x \in \mathbb{F}_q} \xi_p^{f(x) - \mathrm{Tr}_{p^m/p}(\beta x)}, \beta \in \mathbb{F}_q$$

If $\mathcal{W}_f(0) = 0$, then f is called a balanced function over $\mathbb{F}_p$. A function f is the bent function if its Walsh coefficients satisfy $|\mathcal{W}_f(\beta)|^2 = p^m$. A bent function f is called weakly regular bent if there exists a complex number u with $|u| = 1$ and a p-ary function g such that $\mathcal{W}_f(\beta) = u^{-1} p^{\frac{m}{2}} \xi_p^{g(b)}$ for all $\beta \in \mathbb{F}_q$. A p-ary function f is called s-plateaued if $|\mathcal{W}_f(\beta)|^2 \in \{0, p^{m+s}\}$. Now we can define Walsh support of an s-plateaued p-ary function f as

$$\mathrm{Supp}(\mathcal{W}_f) = \{\beta \in \mathbb{F}_q : |\mathcal{W}_f(\beta)|^2 = p^{m+s}\}$$

and we have $\#Supp(\mathcal{W}_f) = p^{m-s}$. Walsh distribution of an s-plateaued p-ary function f follows from Parseval identity.

Lemma 2. *Let $f : \mathbb{F}_{p^m} \to \mathbb{F}_p$ be s-plateaued function. Then*

$$\#\{\beta \in \mathbb{F}_q : |\mathcal{W}_f(\beta)|^2 = p^{m+s}\} = p^{m-s}$$

$$\#\{\beta \in \mathbb{F}_q : |\mathcal{W}_f(\beta)|^2 = 0\} = p^m - p^{m-s}$$

Now, we have the following definition.

Definition 1. *([18]) Let f be p-ary s-plateaued function from $\mathbb{F}_q$ to $\mathbb{F}_p$ with $0 \le s \le m$. Then f is called weakly regular s-plateaued if there exis a complex number u with $|u| = 1$ such that*

$$\mathcal{W}_f(\beta) \in \{\ 0, u p^{\frac{m+s}{2}} \xi_p^{g(\beta)}\}$$

$\forall \beta \in \mathbb{F}_q$, where g is a p-ary function over $\mathbb{F}_q$ and $g(\beta) = 0$ for all $\beta \notin Supp(\mathcal{W}_f)$. Otherwise, f is called non-weakly regular p-ary s-plateaued.

Lemma 3. *[18] Let f be p-ary s-plateaued function from $\mathbb{F}_q$ to $\mathbb{F}_p$ and let $\beta \in \mathbb{F}_{p^m}$. Then $\forall \beta \in Supp(\mathcal{W}_f)$, we have the following*

$$\mathcal{W}_f(\beta) = \epsilon \sqrt{p^{\star}}^{\,m+s} \xi_p^{g(\beta)}$$

where $\epsilon \in \{\ -1, 1\}$ is the sign of $\mathcal{W}_f$ and g is a p-ary function over $\mathbb{F}_q$ with $g(\beta) = 0$ for all $\beta \notin Supp(\mathcal{W}_f)$.

Lemma 4. *[17] Let f be p-ary s-plateaued function from $\mathbb{F}_q$ to $\mathbb{F}_p$ and let $\beta \in \mathbb{F}_{p^m}$. Then for $x \in \mathbb{F}_{p^m}$, we have*

$$\sum_{\beta \in Supp(\mathcal{W}_f)} \xi_p^{g(\beta)+\mathrm{Tr}_{p^m/p}(\beta x)} = \epsilon \eta_0^m(-1)\sqrt{p^\star}^{\,m-s}\xi_p^{f(x)}$$

where $\epsilon \in \{-1, 1\}$ is the sign of $\mathcal{W}_f$ and g is a p-ary function over $\mathbb{F}_q$ with $g(\beta) = 0$ for all $\beta \notin Supp(\mathcal{W}_f)$.

Recently, Mesnager et. al. [17] introduced the subset of the set of weakly regular unbalanced plateaued functions. Let $\mathcal{WRP}$ be the set of p-ary weakly regular s-plateaued unbalanced functions with $0 \leq s \leq m$ satisfying the conditions:

1. $f(0) = 0$
2. There exist an even positive integer l such that $\gcd(l-1, p-1) = 1$ and $f(ax) = a^l f(x)$ for any $a \in \mathbb{F}_p^\star$ and $x \in \mathbb{F}_q$.

Lemma 5. *[17] Let $f \in \mathcal{WRP}$ with $\mathcal{W}_f(\beta) = \epsilon\sqrt{p^\star}^{\,m+s}\xi_p^{g(\beta)}$ for all $\beta \in Supp(\mathcal{W}_f)$. Then there exist an even positive integer h such that $\gcd(h-1, p-1) = 1$ and $g(a\beta) = a^h g(\beta)$ for any $a \in \mathbb{F}_p^\star$ and $\beta \in Supp(\mathcal{W}_f)$.*

2.2 Linear codes and LCD codes from self-orthogonal codes

In this subsection, we introduce linear codes, their construction method from functions and LCD codes from self-orthogonal codes.

Let $\mathbb{F}_q$ be finite field with q elements, where q is a power of a prime p and let n be a positive integer. A linear code $\mathcal{C}$ over $\mathbb{F}_p$ with parameters $[n, k, d]$ is a k-dimensioonal liner subspace of $\mathbb{F}_p^n$, where d denotes the minimum Haming distance of $\mathcal{C}$. Let $\mathbf{a}$ be a vector in $\mathbb{F}_p^n$ and its support defined as supp($\mathbf{a}$)$= \{0 \leq i \leq n-1 : a_i \neq 0\}$. The cardinality of supp($\mathbf{a}$) is called the Hamming weight of $\mathbf{a}$. The dual code $\mathcal{C}^\perp$ of an $[n, k]$ linear code $\mathcal{C}$ is defined by $\mathcal{C}^\perp = \{\mathbf{c}^\perp \in \mathbb{F}_p^n : \mathbf{c}^\perp \cdot \mathbf{c}$ for all $\mathbf{c} \in \mathcal{C}\}$, where "$\cdot$ "is the standart inner product over $\mathbb{F}_p^n$. Then $\mathcal{C}^\perp$ is an $[n, n-k]$ linear code over $\mathbb{F}_p^n$. If a linear code $\mathcal{C}$ satisfies $\mathcal{C} \subset \mathcal{C}^\perp$, then $\mathcal{C}$ is referred to as a self-orthogonal code. In particular, if $\mathcal{C} = \mathcal{C}^\perp$, then $\mathcal{C}$ is called sef-dual. If all codewords of $\mathcal{C}$ are divisible by some integer $k > 1$, then the code is said to be divisible by k. For a p-ary linear code $\mathcal{C}$, there is a relation between the self-orthogonality and divisibility of $\mathcal{C}$.

Lemma 6. *[21] Let $\mathcal{C}$ be a linear code over $\mathbb{F}_p$. For $p = 3$, $\mathcal{C}$ is self-orthogonal if and only if every codeword of $\mathcal{C}$ has weight divisible by three.*

By looking at the weight distribution of a code, one can decide whether a ternary code is self-orthogonal or not.

There are different methods to construct linear codes. In this paper, we use the second generic construction method based on the defining set. Let $D = \{d_1, d_2, ..., d_n\} \subseteq \mathbb{F}_{p^m}$. The trace of $x \in \mathbb{F}_{p^m}$ over $\mathbb{F}_p$ is defined by

$$Tr_{p^m/p}(x) = x + x^p + x^{p^2} + \ldots, x^{p^{m-1}}\ ,\ x \in \mathbb{F}_{p^m}$$

Define

$$\mathcal{C}_D = \{Tr_{p^m/p}(bd_1), Tr_{p^m/p}(bd_2), ..., Tr_{p^m/p}(bd_n) : b \in \mathbb{F}_{p^m}\}$$

Then $\mathcal{C}_D$ is a linear code over $\mathbb{F}_p$ with length n and dimension at most m. The set D is called the defining set of $\mathcal{C}_D$. The augmented code of $\mathcal{C}_D$ is defined by

$$\overline{\mathcal{C}_D} = \{Tr_{p^m/p}(bd_1), Tr_{p^m/p}(bd_2), ..., Tr_{p^m/p}(bd_n) + c\mathbf{1} : b \in \mathbb{F}_{p^m}\ ,\ c \in \mathbb{F}_p\}, \tag{2.1}$$

where $\mathbf{1} = (1, 1, ..., 1) \in \mathbb{F}_p^n$. We will construct self-orthogonal code by using this technique.

For a linear code $\mathcal{C}$, if $\mathcal{C} \cap \mathcal{C}^\perp = \mathbf{0}$, where $\mathbf{0}$ is the zero vector in $\mathcal{C}$, then it is called a linear complementary dual code(LCD code). Note that the dual of an LCD code is also an LCD code. The necessary and sufficient conditions for a linear code to be an LCD code were defined in terms of the generator matrix[13]. Besides, LCD codes were shown to give an optimum solution to the two-user binary adder channel[13].

A matrix G is said to be row-orthogonal if $GG^\perp = I$, where I is an identity matrix and if $GG^\perp = \mathbf{0}$, then it is called row-self-orthogonal. A linear code $\mathcal{C}$ is self-orthogonal if and only if its generator matrix is row-self-orthogonal[14]. If G is a generator matrix for $[n, k]$ linear code $\mathcal{C}$, then it can be transformed to the standard form $G = [I : A]$, where I is an identity matrix and it is called the systematic generator matrix of the code. Then $\mathcal{C}$ is called leading-systematic. The following lemma provides a relation between LCD codes and self-orthogonal codes.

Lemma 7. *[14] A leading-systematic linear code $\mathcal{C}$ is an LCD code if its systematic generator matrix $G = [I, A]$ is row-orthogonal.*

The Pless power moment. For a linear $[n, k, d]$ code $\mathcal{C}$ over $\mathbb{F}_p$, we denote the weight distribution of $\mathcal{C}$ and $\mathcal{C}^\perp$ as $(1, A_1, \ldots, A_n)$ and $(1, A_1^\perp, \ldots, A_n^\perp)$, respectively. The first four Pless power moments are given as:

$$\sum_{i=0}^{n} A_i = p^k \tag{2.2}$$

$$\sum_{i=0}^{n} iA_i = p^{k-1}\left(pn - n - A_1^\perp\right) \tag{2.3}$$

$$\sum_{i=0}^{n} i^2 A_i = p^{k-2}\left((p-1)n(pn-n+1) - (2pn - p - 2n + 2)A_1^\perp + 2A_2^\perp\right) \tag{2.4}$$

$$\begin{aligned}\sum_{i=0}^{n} i^3 A_i = p^{k-3}[&(p-1)n(p^2n^2 - 2pn^2 + 3pn - p + n^2 - 3n + 2)\\ &-(3p^2n^2 - 3p^2n - 6pn^2 + 12pn + p^2 - 6p + 3n^2 - 9n + 6)A_1^\perp\\ &+6(pn - p - n + 2)A_2^\perp - 6A_3^\perp]\end{aligned} \tag{2.5}$$

The Pless power moments are used to find the parameters of linear codes.

Augmented code of a linear code. Let $\mathcal{C}$ be an $[n, k, d]$ linear code over $\mathbb{F}_p$ which has generator matrix G. The augmented code $\overline{\mathcal{C}}$ of $\mathcal{C}$ is a linear code over $\mathbb{F}_p$ with generator matrix

$$\begin{bmatrix} G \\ \mathbf{1} \end{bmatrix}$$

where $\mathbf{1} = (1, 1, ..., 1) \in \mathbb{F}_p^n$. Note that if $\mathbf{1}$ is not a codeword in $\mathcal{C}$, then the augmented code $\overline{\mathcal{C}}$ has length n and dimension $k+1$. Determining the weight distribution of a code is a hard problem and finding the minimum distance of $\overline{\mathcal{C}}$ requires the complete weight distribution of the original code $\mathcal{C}$. There are some methods to determine whether the given augmented code is self-orthogonal. In this paper, we will use Lemma 6 to prove the self-orthogonality of the the linear code.

3 Character sums for weakly regular plateaued functions

In this section, we present several useful results on the character sums for weakly regular plateaued functions.

Lemma 8. *[12] Let p be an odd prime, $p^\star = \eta_0(-1)p$ and $a \in \mathbb{F}_{p^m}^\star$. Then*

$$\sum_{x \in \mathbb{F}_{p^m}} \xi_p^{\mathrm{Tr}_{p^m/p}(ax^2)} = (-1)^{m-1} \eta(a) \sqrt{p^\star}^m$$

Particularly, if $m = 1$ and $a = 1$, then $\sum_{x \in \mathbb{F}_{p^m}} \xi_p^{x^2} = \sqrt{p^\star}^m$

Lemma 9. *[12] Let p be an odd prime and $p^\star = \eta_0(-1)p$, then*

1. $\sum_{c \in \mathbb{F}_p^\star} \eta_0(c) = 0$;
2. $\sum_{c \in \mathbb{F}_p^\star} \xi_p^{ca} = -1$ *for every* $a \in \mathbb{F}_p^\star$;
3. $\sum_{c \in \mathbb{F}_p^\star} \eta_0(c) \xi_p^c = \sqrt{p^*}$.

Lemma 10. *[12] Let $b \in \mathbb{F}_{p^m}$ and $c \in \mathbb{F}_p$ and let*

$$B = \sum_{z \in \mathbb{F}_p^\star} \sum_{x \in \mathbb{F}_{p^m}} \xi_p^{z\left(\mathrm{Tr}_{p^m/p}(bx)+c\right)}$$

Then we have

$$B = \begin{cases} 0, & \text{if } c \in \mathbb{F}_p, b \neq 0, \\ p^m(p-1), & \text{if } c = 0, b = 0, \\ -p^m, & \text{if } c \neq 0, b = 0. \end{cases}$$

Lemma 11. *[17] Let* $f : \mathbb{F}_{p^m} \to \mathbb{F}_p$ *be a p-ary function with* $\mathcal{W}_f(0) = \epsilon\sqrt{p^\star}^{m+s}$, *where* $\epsilon \in \{-1, 1\}$ *is the sign of* $\mathcal{W}_f$ *and* $p^\star = \eta_0(-1)p$. *Let* $N_f := \#\{b \in \mathbb{F}_{p^m} : f(b) = 0\}$. *Then we have*

$$N_f = \begin{cases} p^{m-1} + \epsilon\eta_0(-1)(p-1)\sqrt{p^\star}^{m+s-2}, & \text{if } m+s \text{ is even,} \\ p^{m-1}, & \text{if } m+s \text{ is odd.} \end{cases}$$

Lemma 12. *[17] Let f be a weakly regular s-plateaued function with* $\mathcal{W}_f(\beta) = \epsilon\sqrt{p^\star}^{m+s}\xi^{g(\beta)}$. *Define* $N_g := \#\{b \in Supp(\mathcal{W}_f) : g(b) = 0\}$. *Then we have*

$$N_g = \begin{cases} p^{m-s-1} + \epsilon\eta_0^{m+1}(-1)(p-1)\sqrt{p^\star}^{m-s-2}, & \text{if } m-s \text{ is even,} \\ p^{m-s-1}, & \text{if } m-s \text{ is odd.} \end{cases}$$

Lemma 13. *[17] Let* $f \in \mathcal{WRP}$. *Define* $N_{sq} := \#\{b \in Supp(\mathcal{W}_f) : g(b) \in SQ\}$ *and* $N_{nsq} := \#\{b \in Supp(\mathcal{W}_f) : g(b) \in NSQ\}$. *Then we have*

$$N_{sq} = \begin{cases} \frac{p-1}{2}(p^{m-s-1} + \epsilon\eta_0^m(-1)\sqrt{p^\star}^{m-s-1}), & \text{if } m-s \text{ is odd,} \\ \frac{p-1}{2}(p^{m-s-1} - \epsilon\eta_0^{m+1}(-1)\sqrt{p^\star}^{m-s-2}), & \text{if } m-s \text{ is even.} \end{cases}$$

$$N_{nsq} = \begin{cases} \frac{p-1}{2}(p^{m-s-1} - \epsilon\eta_0^m(-1)\sqrt{p^\star}^{m-s-1}), & \text{if } m-s \text{ is odd,} \\ \frac{p-1}{2}(p^{m-s-1} - \epsilon\eta_0^{m+1}(-1)\sqrt{p^\star}^{m-s-2}), & \text{if } m-s \text{ is even.} \end{cases}$$

Remark 1. Let $a \in \mathbb{F}_3^\star$, $f(x) \in \mathcal{WRP}$ and g be the dual of $f(x)$. Define $N_g(a) := \#\{b \in Supp(\mathcal{W}_f) : g(b) + a = 0\}$. Then from Lemma 13, we have

$$N_g(a) = \begin{cases} 3^{m-s-1} - \epsilon(-1)^m\eta_0(a)(-3)^{\frac{m-s-1}{2}}, & \text{if } m-s \text{ is odd,} \\ 3^{m-s-1} + \epsilon(-1)^m(-3)^{\frac{m-s-2}{2}}, & \text{if } m-s \text{ is even.} \end{cases}$$

Lemma 14. *[22] Let* $a \in \mathbb{F}_p^\star$ *and* $f \in \mathcal{WRP}$. *Define* $N_{sq}(a) := \#\{b \in Supp(\mathcal{W}_f) : g(b) + a \in SQ\}$ *and* $N_{nsq}(a) := \#\{b \in Supp(\mathcal{W}_f) : g(b) + a \in NSQ\}$. *Then we have the following.*
If $m-s$ *is even, then*

$$N_{sq}(a) = \frac{p-1}{2}p^{m-s-1} + \frac{1+p\eta_0(a)}{2}\epsilon\eta_0^{m+1}(-1)\sqrt{p^*}^{m-s-2},$$

$$N_{sq}(a) = \frac{p-1}{2}p^{m-s-1} + \frac{1-p\eta_0(a)}{2}\epsilon\eta_0^{m+1}(-1)\sqrt{p^*}^{m-s-2}.$$

If $m-s$ *is odd, then*

$$N_{sq}(a) = \frac{p-1}{2}p^{m-s-1} - \frac{1+\eta_0(a)}{2}\epsilon\eta_0^{m}(-1)\sqrt{p^*}^{m-s-1},$$

$$N_{sq}(a) = \frac{p-1}{2}p^{m-s-1} + \frac{1-\eta_0(a)}{2}\epsilon\eta_0^{m}(-1)\sqrt{p^*}^{m-s-1}.$$

4 The Linear code $\overline{C_{D_f}}$ and its subcode for $a \neq 0$ and $p = 3$

Let $m + s > 3$ be a positive integer with $0 \leq s \leq m$ and p be an odd prime. Let $f(x) \in \mathcal{WRP}$. In this section we construct the augmented code $\overline{C_{D_f}}$ defined in (2.1) based on the defining set

$$D_f = \{x \in \mathbb{F}_{3^m} : f(x) + a = 0\}$$

for $p = 3$ and $a \in \mathbb{F}_3^\star$. The length of the code $\overline{C_{D_f}}$ is the size of the set D_f, and the value $n = \#D_f$ follows from [17, Lemma 9] when $p = 3$.

Lemma 15. *The length of $\overline{C_{D_f}}$ is given by*

$$n = \begin{cases} 3^{m-1} - \epsilon\eta_0(a)(-3)^{\frac{m+s-1}{2}}, & \text{if } m+s \text{ is odd,} \\ 3^{m-1} + \epsilon(-3)^{\frac{m+s-2}{2}}, & \text{if } m+s \text{ is even.} \end{cases}$$

Lemma 16. *Let $a \in \mathbb{F}_3^\star$, $b \in \mathbb{F}_{3^m}$, $c \in \mathbb{F}_3$ and $f(x) \in \mathcal{WRP}$. Denote by*

$$S = \sum_{y \in \mathbb{F}_3^\star} \sum_{z \in \mathbb{F}_3^\star} \sum_{x \in \mathbb{F}_{3^m}} \xi_3^{y(f(x)+a)} \xi_3^{z(\mathrm{Tr}_{3^m/3}(bx)+c)}$$

For every $b \notin Supp(\mathcal{W}_f)$, $S = 0$ and for every $b \in Supp(\mathcal{W}_f)$ we have the following. If $m + s$ is even, then we have

$$S = \begin{cases} 4\epsilon(-3)^{\frac{m+s}{2}}, & \text{if } c = 0, g(b) + a = 0, \\ -2\epsilon(-3)^{\frac{m+s}{2}}, & \text{if } c = 0, g(b) + a \neq 0 \text{ or } c \neq 0, g(b) + a = 0, \\ \epsilon(-3)^{\frac{m+s}{2}}, & \text{if } c \neq 0, g(b) + a \neq 0. \end{cases}$$

If $m + s$ is odd, then we have

$$S = \begin{cases} 0, & \text{if } g(b) + a = 0 \\ 2\epsilon(-3)^{\frac{m+s+1}{2}}, & \text{if } c = 0, g(b) + a \in SQ, \\ -2\epsilon(-3)^{\frac{m+s+1}{2}}, & \text{if } c = 0, g(b) + a \in NSQ, \\ -\epsilon(-3)^{\frac{m+s+1}{2}}, & \text{if } c \neq 0, g(b) + a \in SQ, \\ \epsilon(-3)^{\frac{m+s+1}{2}}, & \text{if } c \neq 0, g(b) + a \in NSQ. \end{cases}$$

Proof. The first case is trivial, so we give a short proof for the second case. By definition of S, We have

$$\begin{aligned} S &= \sum_{z \in \mathbb{F}_3^\star} \xi_3^{zc} \sum_{y \in \mathbb{F}_3^\star} \xi_3^{ya} \sum_{x \in \mathbb{F}_{3^m}} \xi_3^{y(f(x) + \frac{z}{y}\mathrm{Tr}_{3^m/3}(bx))} \\ &= \sum_{z \in \mathbb{F}_3^\star} \xi_3^{zc} \sum_{y \in \mathbb{F}_3^\star} \xi_3^{ya} \sigma_y \left(\sum_{x \in \mathbb{F}_{3^m}} \xi_3^{f(x) - \mathrm{Tr}_{3^m/3}\left(\frac{-z}{y}bx\right)} \right) \\ &= \sum_{z \in \mathbb{F}_3^\star} \xi_3^{zc} \sum_{y \in \mathbb{F}_3^\star} \xi_3^{ya} \sigma_y \left(\epsilon\sqrt{3^\star}^{m+s} \xi_3^{g\left(\frac{-z}{y}b\right)} \right) \\ &= \epsilon\sqrt{3^\star}^{m+s} \sum_{z \in \mathbb{F}_3^\star} \xi_3^{zc} \sum_{y \in \mathbb{F}_3^\star} \eta_0^{m+s}(y) \xi_3^{y\left(a + g\left(\frac{-z}{y}b\right)\right)}. \end{aligned}$$

From [17, Proposition 2], there exists a positive even integer l such that $g(\frac{-z}{y}b) = (\frac{-z}{y})^l g(b) = g(b)$ since $z, y \in \mathbb{F}_3^\star$. Then we have

$$S = \epsilon\sqrt{3^\star}^{m+s} \sum_{z\in\mathbb{F}_3^\star} \xi_3^{zc} \sum_{y\in\mathbb{F}_3^\star} \eta_0^{m+s}(y)\xi_3^{y(a+g(b))}$$

If $m+s$ is even, then $\eta_0^{m+s}(y) = 1$ and the value of S directly follows. If $m+s$ is odd, then $\eta_0^{m+s}(y) = \eta_0(y)$ and

$$S = \epsilon\sqrt{3^\star}^{m+s} \sum_{z\in\mathbb{F}_3^\star} \xi_3^{zc} \sum_{y\in\mathbb{F}_3^\star} \eta_0(y)\xi_3^{y(a+g(b))}$$

If $g(b) + a = 0$, then clearly $S = 0$. Otherwise from Lemma 9, we have

$$\begin{aligned} S &= \epsilon\sqrt{3^\star}^{m+s} \textstyle\sum_{z\in\mathbb{F}_3^\star} \xi_3^{zc} \sum_{y\in\mathbb{F}_3^\star} \eta_0\left(y(g(a)+b)\right)\eta_0(g(a)+b)\xi_3^{y(a+g(b))} \\ &= \epsilon(-3)^{\frac{m+s+1}{2}}\eta_0(g(a)+b)\sum_{z\in\mathbb{F}_3^\star} \xi_3^{zc}. \end{aligned}$$

Hence, the proof is complete.

Lemma 17. *Let $f \in \mathcal{WRP}$. Define*

$$N_{f,b,c}(a) := \#\{x \in F_{3^m} : \mathrm{Tr}_{3^m/3}(bx) + c = 0 \text{ and } f(x) + a = 0\}$$

for $b \in \mathbb{F}_{3^m}$ and $c \in \mathbb{F}_3$. Then, for every $b \notin Supp(\mathcal{W}_f)$, we have

$$N_{f,b,c}(a) = \begin{cases} 3^{m-2} - \epsilon(-3)^{\frac{m+s-4}{2}}, & \text{if } m+s \text{ is even,} \\ 3^{m-2} + \epsilon\eta_0(a)(-3)^{\frac{m+s-3}{2}}, & \text{if } m+s \text{ is odd.} \end{cases}$$

For every $b \in Supp(\mathcal{W}_f)$ we have

- *If $m+s$ is even, then*

$$N_{f,b,c}(a) = \begin{cases} 3^{m-1} + \epsilon(-3)^{\frac{m+s-2}{2}}, & \text{if } c = 0, b = 0, \\ 0, & \text{if } c \neq 0, b = 0, \\ 3^{m-2} - \epsilon(-3)^{\frac{m+s-2}{2}}, & \text{if } c = 0, b \neq 0, g(b) + a = 0, \\ 3^{m-2} + \epsilon(-3)^{\frac{m+s-2}{2}}, & \text{if } c = 0, b \neq 0, g(b) + a \neq 0 \text{ or } c \neq 0, b \neq 0, g(b) + a = 0, \\ 3^{m-2}, & \text{if } c \neq 0, b \neq 0, g(b) + a \neq 0. \end{cases}$$

- *If $m+s$ is odd and $a = 1$, then*

$$N_{f,b,c}(a) = \begin{cases} 3^{m-1} - \epsilon(-3)^{\frac{m+s-1}{2}}, & \text{if } c = 0, b = 0, \\ 0, & \text{if } c \neq 0, b = 0, \\ 3^{m-2} + \epsilon(-3)^{\frac{m+s-3}{2}}, & \text{if } c = 0, b \neq 0, g(b) + a = 0 \text{ or } c \neq 0, b \neq 0, g(b) + a = 0, \\ 3^{m-2} - \epsilon(-3)^{\frac{m+s-3}{2}}, & \text{if } b \neq 0, c = 0, g(b) + a \in NSQ, \\ 3^{m-2} - \epsilon(-3)^{\frac{m+s-1}{2}}, & \text{if } b \neq 0, c = 0, g(b) + a \in SQ, \\ 3^{m-2}, & \text{if } b \neq 0, c \neq 0, g(b) + a \in SQ, \\ 3^{m-2} + 2\epsilon(-3)^{\frac{m+s-3}{2}}, & \text{if } b \neq 0, c \neq 0, g(b) + a \in NSQ. \end{cases}$$

– *If* $m+s$ *is odd and* $a=-1$*, then*

$$N_{f,b,c}(a)=\begin{cases}3^{m-1}+\epsilon(-3)^{\frac{m+s-1}{2}}, & \text{if } c=0, b=0,\\ 0, & \text{if } c\neq 0, b=0,\\ 3^{m-2}-\epsilon(-3)^{\frac{m+s-3}{2}}, & \text{if } c=0, b\neq 0, g(b)+a=0 \text{ or } c\neq 0, b\neq 0, g(b)+a=0,\\ 3^{m-2}+\epsilon(-3)^{\frac{m+s-1}{2}}, & \text{if } b\neq 0, c=0, g(b)+a\in NSQ,\\ 3^{m-2}+\epsilon(-3)^{\frac{m+s-3}{2}}, & \text{if } b\neq 0, c=0, g(b)+a\in SQ,\\ 3^{m-2}+\epsilon(-3)^{\frac{m+s-3}{2}}, & \text{if } b\neq 0, c\neq 0, g(b)+a\in SQ,\\ 3^{m-2}, & \text{if } b\neq 0, c\neq 0, g(b)+a\in NSQ.\end{cases}$$

Proof. By the definition of $N_{f,b,c}(a)$, we have

$$\begin{aligned}N_{f,b,c}(a)&=\frac{1}{9}\sum_{x\in\mathbb{F}_{3^m}}\sum_{y\in\mathbb{F}_3}\sum_{z\in\mathbb{F}_3}\xi_3^{y(f(x)+a)}\xi_3^{z\left(\mathrm{Tr}_{3^m/3}(bx)+c\right)}\\ &=3^{m-2}+\frac{1}{9}\sum_{y\in\mathbb{F}_3^\star}\sum_{x\in\mathbb{F}_{3^m}}\xi_3^{y(f(x)+a)}+\frac{1}{9}\sum_{z\in\mathbb{F}_3^\star}\sum_{x\in\mathbb{F}_{3^m}}\xi_3^{z\left(\mathrm{Tr}_{3^m/3}(bx)+c\right)}\\ &+\frac{1}{9}\sum_{x\in\mathbb{F}_{3^m}}\sum_{y\in\mathbb{F}_3^\star}\sum_{z\in\mathbb{F}_3^\star}\xi_3^{y(f(x)+a)}\xi_3^{z\left(\mathrm{Tr}_{3^m/3}(bx)+c\right)}\\ &=3^{m-2}+\frac{1}{9}\sum_{y\in\mathbb{F}_3^\star}\sum_{x\in\mathbb{F}_{3^m}}\xi_3^{y(f(x)+a)}+\frac{B}{9}+\frac{S}{9}\end{aligned}$$

where S and B are defined in Lemma 16 and Lemma 10. From the proof of Lemma 15, we have

$$\sum_{y\in\mathbb{F}_3^\star}\sum_{x\in\mathbb{F}_{3^m}}\xi_3^{y(f(x)+a)}=\begin{cases}-\epsilon(-3)^{\frac{m+s}{2}}, & \text{if } m+s \text{ is even}\\ \epsilon\eta_0(a)(-3)^{\frac{m+s+1}{2}}, & \text{if } m+s \text{ is odd.}\end{cases}$$

Hence we can derive the desired results.

Theorem 1. *Let* $m+s>4$ *be even,* $f(x)\in\mathcal{WRP}$ *and* ϵ *be the sign of the Walsh transform of* $f(x)$*. Let* $p=3$ *and* $D_f=\{x\in\mathbb{F}_{3^m}: f(x)+a=0\}$ *for* $a\in\mathbb{F}_3^\star$*. Then* $\overline{C_{D_f}}$ *is five-weight self orthogonal* $[3^{m-1}+\epsilon(-3)^{\frac{m+s-2}{2}}, m+1]$ *ternary linear code with weight distribution in Table* 1*.*

Proof. Let $\mathbf{c}$ be any codeword of $\overline{C_{D_f}}$. Then we can write

$$\mathbf{c}=\left(\mathrm{Tr}_{3^m/3}(bx)\right)_{x\in D_f}+c\mathbf{1}$$

with $b\in\mathbb{F}_{3^m}$ and $c\in\mathbb{F}_3$. From the definition of the code, its length $\#D_f=n$ follows from Lemma 15. Similarly, the Hamming weight of a codeword $\mathbf{c}$ is obtained as

$$wt(\mathbf{c})=n-N_{f,b,c}(a)$$

which follows from Lemma 17. The weight distribution also follows from Lemma 1. The dimension of $\overline{C_{D_f}}$ is $m+1$ since $A_0=1$. By Lemma 6, $\overline{C_{D_f}}$ is self-orthogonal for $m+s>4$ since all codewords have weights divisible by 3.

Example 1. Let $f(x) = Tr_{3^4/3}(\zeta x^{10} + \zeta^{51}x^4 + \zeta^{68}x^2)$, where ζ is a generator of $\mathbb{F}_{3^4}^* = \langle\zeta\rangle$ for $\zeta^4 + 2\zeta^3 + 2 = 0$. Then, f is a quadratic 2-plateaued unbalanced function in the set $\mathcal{WRP}$ and for all $\beta \in \mathbb{F}_{3^4}$, we have $\mathcal{W}_f(\beta) \in \{0, -27, -27\xi_3, -27\xi_3^2\}$ with $\epsilon = 1$. Then the code $\overline{C_{D_f}}$ in Theorem 1 has parameters $[36, 5, 18]$ and weight enumerator $1 + 12y^{18} + 216y^{24} + 8y^{27} + 6y^{36}$, which are verified by Sage program.

Table 1. The code $\overline{C_{D_f}}$ in Theorem 1 when $m + s$ is even.

Hamming weight ω	Multiplicity A_ω
0	1
$2\left(3^{m-2} + \epsilon(-3)^{\left(\frac{m+s-2}{2}\right)}\right)$	$3^{m-s-1} + \epsilon(-1)^m(-3)^{\left(\frac{m-s-2}{2}\right)}$
$2 \cdot 3^{m-2} + \epsilon(-3)^{\left(\frac{m+s-2}{2}\right)}$	$2\left(2 \cdot 3^{m-s-1} - \epsilon(-1)^m(-3)^{\left(\frac{m-s-2}{2}\right)} - 1\right)$
$2 \cdot 3^{m-2}$	$4 \cdot 3^{m-s-1} + \epsilon(-1)^m(-3)^{\left(\frac{m-s-2}{2}\right)} - 1$
$3^{m-1} + \epsilon(-3)^{\left(\frac{m+s-2}{2}\right)}$	2
$2 \cdot 3^{m-2} - 2\epsilon(-3)^{\left(\frac{m+s-4}{2}\right)}$	$3^{m+1} - 3^{m-s+1}$

Theorem 2. *Let $m+s > 3$ be odd, $f(x) \in \mathcal{WRP}$ and ϵ be the sign of Walsh transform of $f(x)$. Let $p = 3$ and $D_f = \{x \in \mathbb{F}_{3^m} : f(x)+a = 0\}$ for $a \in \mathbb{F}_3^\star$. Then $\overline{C_{D_f}}$ is a six-weight self orthogonal $[3^{m-1} - \eta_0(a)\epsilon(-3)^{\frac{m+s-1}{2}}, m + 1]$ linear code with weight distributions in Table 2.*

Proof. Similarly to Theorem 1, we can find the Hamming weight of any codeword in $\overline{C_{D_f}}$ by using Lemmas 15 and 17. The weight distribution follows from Lemmas 1, 14 and Remark 1.

Example 2. Let $a = -1$, $f(x) = Tr_{3^6/3}(\zeta x^4 + \zeta^{27}x^2)$, where ζ is a generator of $\mathbb{F}_{3^6}^* = \langle\zeta\rangle$ for $\zeta^6 + 2\zeta^4 + \zeta^2 + 2\zeta + 2 = 0$. Then, f is a quadratic 1-plateaued unbalanced function in the set $\mathcal{WRP}$ and for all $\beta \in \mathbb{F}_{3^4}$, we have $\mathcal{W}_f(\beta) \in \{0, 54\xi_3 + 27, -27\xi_3 - 54, -27\xi_3 + 27\}$ with $\epsilon = -1$. Then the code $\overline{C_{D_f}}$ in Theorem 2 has parameters $[270, 7, 162]$ and weight enumerator $1 + 81y^{162} + 178y^{171} + 1674y^{180} + 169y^{189} + 89y^{198} + 2y^{270}$,which are verified by Sage program.

Theorem 3. *Let $a \in \mathbb{F}_3^\star$ and $f(x) \in \mathcal{WRP}$ with ϵ the sign of the Walsh transform of $f(x)$. If $m+s > 4$ is even, then $\overline{C_{D_f}}^\perp$ is a $[3^{m-1}+\epsilon(-3)^{\frac{m+s-2}{2}}, 3^{m-1}+\epsilon(-3)^{\frac{m+s-2}{2}} - m - 1, 3]$ linear code. If $m + s > 3$ is odd, then $\overline{C_{D_f}}^\perp$ is a $[3^{m-1} - \epsilon\eta_0(a)(-3)^{\frac{m+s-1}{2}}, 3^{m-1} - \epsilon\eta_0(a)(-3)^{\frac{m+s-1}{2}} - m - 1, 3]$ linear code.*

Proof. Denote by $d^\perp$ the minimum distance of $\overline{C_{D_f}}^\perp$. By the definition of $\overline{C_{D_f}}$, we deduce that $d^\perp \geq 2$. Denote by $(1, A_1, \ldots, A_n)$ and $(1, A_1^\perp, \ldots, A_n^\perp)$ the weight distributions of $\overline{C_{D_f}}$ and $\overline{C_{D_f}}^\perp$, respectively.

Table 2. The code $\overline{C_{D_f}}$ in Theorem 2 when $m+s$ is odd.

Hamming weight ω	Multiplicity A_ω
0	1
$3^{m-1}-\epsilon\eta_0(a)(-3)^{\left(\frac{m+s-1}{2}\right)}$	2
$2\left(3^{m-2}+\epsilon\eta_0(a)(-3)^{\left(\frac{m+s-3}{2}\right)}\right)$	$3^{m+1}-2\cdot 3^{m-s}+\epsilon\eta_0(a)(-1)^m(-3)^{\left(\frac{m-s+1}{2}\right)}$
$2\cdot 3^{m-2}+4\epsilon\eta_0(a)(-3)^{\left(\frac{m+s-3}{2}\right)}$	$3^{m-s-1}+\epsilon\eta_0(a)(-1)^m(-3)^{\left(\frac{m-s-1}{2}\right)}$
$2\cdot 3^{m-2}$	$3^{m-s-1}-1$
$2\cdot 3^{m-2}-\epsilon\eta_0(a)(-3)^{\left(\frac{m+s-1}{2}\right)}$	$2\left(3^{m-s-1}-1\right)$
$2\cdot 3^{m-2}+\epsilon\eta_0(a)(-3)^{\left(\frac{m+s-3}{2}\right)}$	$2\left(3^{m-s-1}+\epsilon\eta_0(a)(-1)^m(-3)^{\frac{m-s-1}{2}}\right)$

,

Let $m+s$ be even. By Equations 2.3, 2.4 and Theorem 1, we derive

$$A_1^{\perp}=0 \text{ and } A_2^{\perp}=0$$

Combining 1 and Equation 2.5, we obtain

$$A_3^{\perp}=(3^{m-2}-1)(3^{m-2}-\epsilon(-3)^{\frac{m+s-4}{2}})>0$$

and $d^{\perp}=3$. This completes the proof when $m+s$ is even.

By using same Equations 2.3, 2.4, 2.5 and Theorem 2, we obtain the desired conclusions for odd $m+s$.

5 The second family of linear codes from weakly regular plateaued functions for $a=0$

Let $m+s>3$ be a positive integer with $0\le s\le m$ and p be an odd prime. Let $f(x)\in\mathcal{WRP}$. In this section we construct the augmented code $\overline{C_{D_f}}$ based on the defining set

$$D_f=\{x\in\mathbb{F}_{p^m}: f(x)=0\}.$$

The length of the code $\overline{C_{D_f}}$ is the size of the set D_f, and the value $n=\#D_f$ follows from [17, Lemma 7].

Lemma 18. *The length of $\overline{C_{D_f}}$ is given by*

$$n=\begin{cases} p^{m-1}+\epsilon\eta_0(-1)(p-1)\sqrt{p^\star}^{\,m+s-2}, & \text{if } m+s \text{ is even},\\ p^{m-1}, & \text{if } m+s \text{ is odd.}\end{cases}$$

The following lemma follows from the combinations of [17, Lemma 12] and [16, Lemma 6].

Lemma 19. *Let $b\in\mathbb{F}_{p^m}$, $c\in\mathbb{F}_p$ and $f(x)\in\mathcal{WRP}$. Denote by*

$$S'=\sum_{y\in\mathbb{F}_p^\star}\sum_{z\in\mathbb{F}_p^\star}\sum_{x\in\mathbb{F}_{p^m}}\xi_p^{yf(x)}\xi_p^{z(\mathrm{Tr}_{p^m/p}(bx)+c)}$$

For every $b \notin$ *Supp*$(\mathcal{W}_f)$, $S' = 0$ *and for every* $b \in$*Supp*$(\mathcal{W}_f)$ *we have the following.*
If $m+s$ *is even, then we have*

$$S' = \begin{cases} \epsilon(p-1)^2\sqrt{p^\star}^{m+s}, & \text{if } c=0, g(b)=0, \\ -\epsilon(p-1)\sqrt{p^\star}^{m+s}, & \text{if } c=0, g(b)\neq 0 \text{ or } c\neq 0, g(b)=0, \\ \epsilon\sqrt{p^\star}^{m+s}, & \text{if } c\neq 0, g(b)\neq 0. \end{cases}$$

If $m+s$ *is odd, then we have*

$$S' = \begin{cases} 0, & \text{if } g(b)=0, \\ \epsilon(p-1)\sqrt{p^\star}^{m+s+1}, & \text{if } c=0, g(b)\in SQ, \\ -\epsilon(p-1)\sqrt{p^\star}^{m+s+1}, & \text{if } c=0, g(b)\in NSQ, \\ -\epsilon\sqrt{p^\star}^{m+s+1}, & \text{if } c\neq 0, g(b)\in SQ, \\ \epsilon\sqrt{p^\star}^{m+s+1}, & \text{if } c\neq 0, g(b)\in NSQ. \end{cases}$$

The following lemma will be used to find the Hamming weights for $\overline{C_{D_f}}$.

Lemma 20. *Let* $f \in \mathcal{WRP}$. *Define*

$$N_{f,b,c} := \#\{x \in F_{p^m} : \mathrm{Tr}_{p^m/p}(bx) + c = 0 \text{ and } f(x) = 0\}$$

for $b \in \mathbb{F}_{p^m}$ *and* $c \in \mathbb{F}_p$. *Then, for every* $b \notin$*Supp*$(\mathcal{W}_f)$, *we have*

$$N_{f,b,c} = \begin{cases} p^{m-2} & \text{if } m+s \text{ is odd}, \\ p^{m-2} + \epsilon(p-1)\sqrt{p^\star}^{m+s-4}, & \text{if } m+s \text{ is even}. \end{cases}$$

For every $b \in$*Supp*$(\mathcal{W}_f)$, *we have the following.*

– *If* $m+s$ *is even, then*

$$N_{f,b,c} = \begin{cases} p^{m-1} + \epsilon(p-1)\eta_0(-1)\sqrt{p^\star}^{m+s-2}, & \text{if } c=0, b=0, \\ 0, & \text{if } c\neq 0, b=0, \\ p^{m-2} + \epsilon(p-1)\eta_0(-1)\sqrt{p^\star}^{m+s-2}, & \text{if } c=0, b\neq 0, g(b)=0, \\ p^{m-2}, & \text{if } c=0, b\neq 0, g(b)\neq 0 \text{ or } c\neq 0, b\neq 0, g(b)=0, \\ p^{m-2} + \epsilon\eta_0(-1)\sqrt{p^\star}^{m+s-2}, & \text{if } c\neq 0, b\neq 0, g(b)\neq 0. \end{cases}$$

– *If* $m+s$ *is odd, then*

$$N_{f,b,c} = \begin{cases} p^{m-1}, & \text{if } c=0, b=0, \\ 0, & \text{if } c\neq 0, b=0, \\ p^{m-2}, & \text{if } c=0, b\neq 0, g(b)=0 \text{ or } c\neq 0, b\neq 0, g(b)=0, \\ p^{m-2} - \epsilon(p-1)\sqrt{p^\star}^{m+s-3}, & \text{if } b\neq 0, c=0, g(b)\in NSQ, \\ p^{m-2} + \epsilon(p-1)\sqrt{p^\star}^{m+s-3}, & \text{if } b\neq 0, c=0, g(b)\in SQ, \\ p^{m-2} - \epsilon\sqrt{p^\star}^{m+s-3}, & \text{if } b\neq 0, c\neq 0, g(b)\in SQ, \\ p^{m-2} + \epsilon\sqrt{p^\star}^{m+s-3}, & \text{if } b\neq 0, c\neq 0, g(b)\in NSQ. \end{cases}$$

Proof. By the definition of $N_{f,b,c}$, we have

$$\begin{aligned} N_{f,b,c} &= \frac{1}{p^2} \sum_{x\in\mathbb{F}_{p^m}} \sum_{y\in\mathbb{F}_p} \sum_{z\in\mathbb{F}_p} \xi_p^{yf(x)} \xi_p^{z\left(\mathrm{Tr}_{p^m/p}(bx)+c\right)} \\ &= p^{m-2} + \frac{1}{p^2} \sum_{y\in\mathbb{F}_p^\star} \sum_{x\in\mathbb{F}_{p^m}} \xi_p^{yf(x)} + \frac{1}{p^2} \sum_{z\in\mathbb{F}_p^\star} \sum_{x\in\mathbb{F}_{p^m}} \xi_p^{z\left(\mathrm{Tr}_{p^m/p}(bx)+c\right)} \\ &+ \frac{1}{p^2} \sum_{x\in\mathbb{F}_{p^m}} \sum_{y\in\mathbb{F}_p^\star} \sum_{z\in\mathbb{F}_p^\star} \xi_p^{y(f(x))} \xi_p^{z\left(\mathrm{Tr}_{p^m/p}(bx)+c\right)} \\ &= p^{m-2} + \frac{1}{p^2} \sum_{y\in\mathbb{F}_p^\star} \sum_{x\in\mathbb{F}_{p^m}} \xi_p^{yf(x)} + \frac{B'}{p^2} + \frac{S'}{p^2} \end{aligned}$$

where S' and B' are defined in Lemma 19 and Lemma 10. From Lemma 18,

$$\sum_{y\in\mathbb{F}_p^\star} \sum_{x\in\mathbb{F}_{p^m}} \xi_p^{yf(x)} = \begin{cases} \epsilon(p-1)\sqrt{p^\star}^{\,m+s}, & \text{if } m+s \text{ is even}, \\ 0, & \text{if } m+s \text{ is odd}. \end{cases}$$

Then we can obtain the desired results.

Theorem 4. *Let $m+s>3$ be even, $f(x)\in\mathcal{WRP}$ and ϵ be the sign of Walsh transform of $f(x)$. Let $D_f=\{x\in\mathbb{F}_{3^m} : f(x)=0\}$. Then $\overline{C_{D_f}}$ is five-weight linear code with parameters $[\frac{1}{p}(p^m+\epsilon(p-1)\sqrt{p^\star}^{m+s}), m+1]$ and weight distribution in Table 3. In particular, $\overline{C_{D_f}}$ is self-orthogonal if $p=3$.*

Proof. Let $\mathbf{c}$ be any codeword of $\overline{C_{D_f}}$. Then we can write

$$\mathbf{c} = \left(\mathrm{Tr}_{p^m/p}(bx)\right)_{x\in D_f} + c\mathbf{1}$$

with $b\in\mathbb{F}_{p^m}$ and $c\in\mathbb{F}_p$. From the definition of the code, its length $\#D_f=n$ follows from Lemma 18. Similarly, the Hamming weight of a codeword $\mathbf{c}$ is obtained as

$$wt(\mathbf{c}) = n - N_{f,b,c}$$

which follows from Lemma 20. The weight distribution also follows from Lemma 12. The dimension of $\overline{C_{D_f}}$ is $m+1$ since $A_0=1$. By Lemma 6, $\overline{C_{D_f}}$ is self-orthogonal for $m+s>2$ since all codewords have weights divisible by 3.

Example 3. Let $f(x) = Tr_{3^5/3}(\zeta^{19}x^4+\zeta^{238}x^2)$, where ζ is a generator of $\mathbb{F}_{3^5}^* = \langle\zeta\rangle$ for $\zeta^5+2\zeta+1=0$. Then, f is a quadratic 1-plateaued unbalanced function in the set $\mathcal{WRP}$ and for all $\beta\in\mathbb{F}_{3^4}$, we have $\mathcal{W}_f(\beta)\in\{0,-27,-27\xi_3,-27\xi_3^2\}$ with $\epsilon=1$. Then the code $\overline{C_{D_f}}$ in Theorem 4 has parameters $[63,6,36]$ and weight enumerator $1+100y^{36}+486y^{42}+120y^{45}+20y^{54}+2y^{63}$, which are verified by Sage program.

Table 3. The code $\overline{C_{D_f}}$ in Theorem 4 when $m+s$ is even.

Hamming weight ω	Multiplicity A_ω
0	1
$(p-1)p^{m-2}$	$\frac{1}{p}\left(p^{m-s}+\epsilon\eta_0^m(-1)(p-1)\sqrt{p^\star}^{\,m-s}\right)-1$
$\frac{p-1}{p}\left(p^{m-1}+\epsilon\sqrt{p^\star}^{\,m+s}\right)$	$\frac{p-1}{p}\left(2\cdot p^{m-s}+\epsilon\eta_0^m(-1)(p-2)\sqrt{p^\star}^{\,m-s}-p\right)$
$\frac{1}{p}\left(p^{m}+\epsilon(p-1)\sqrt{p^\star}^{\,m+s}\right)$	$p-1$
$\frac{1}{p}\left((p-1)p^{m-1}+\epsilon(p-2)\sqrt{p^\star}^{\,m+s}\right)$	$\frac{(p-1)^2}{p}\left(p^{m-s}-\epsilon\eta_0^m(-1)\sqrt{p^\star}^{\,m-s}\right)$
$(p-1)\left(p^{m-2}+\epsilon(p-1)\sqrt{p^\star}^{\,m+s-4}\right)$	$p^{m+1}-p^{m-s+1}$

Theorem 5. *Let $m+s>3$ be odd, $f(x)\in\mathcal{WRP}$ and ϵ be the sign of Walsh transform of $f(x)$. Let $D_f=\{x\in\mathbb{F}_{3^m}: f(x)=0\}$. Then $\overline{C_{D_f}}$ is seven-weight linear code with parameters $[p^{m-1}, m+1]$ and weight distribution in table 4. In particular, $\overline{C_{D_f}}$ is self-orthogonal if $p=3$.*

Proof. We can find the parameters and weight distribution of $\overline{C_{D_f}}$ by using similar steps in Theorem 4. Then we can obtain the frequency of each weight by Lemmas 12 and 13. $\overline{C_{D_f}}$ is self-orthogonal if $p=3$ by Lemma 6.

Example 4. Let $f(x)=Tr_{3^6/3}(\zeta x^4+\zeta^{27}x^2)$, where ζ is a generator of $\mathbb{F}_{3^6}^*=\langle\zeta\rangle$ for $\zeta^6+2\zeta^4+\zeta^2+2\zeta+2=0$. Then, f is a quadratic 1-plateaued unbalanced function in the set $\mathcal{WRP}$ and for all $\beta\in\mathbb{F}_{3^4}$, we have $\mathcal{W}_f(\beta)\in\{0, 54\xi_3+27, -27\xi_3-54, -27\xi_3+27\}$ with $\epsilon=-1$. Then the code $\overline{C_{D_f}}$ in Theorem 5 has parameters $[243, 7, 144]$ and weight enumerator $1+90y^{144}+144y^{153}+1698y^{162}+180y^{171}+72y^{180}+2y^{243}$, which are verified by Sage program.

Table 4. The code $\overline{C_{D_f}}$ in Theorem 5 when $m+s$ is odd.

Hamming weight ω	Multiplicity A_ω
0	1
p^{m-1}	$p-1$
$(p-1)p^{m-2}$	$p^{m+1}-p-p^{m-s}(p-1)$
$\frac{p-1}{p^2}\left(p^{m}+\epsilon\sqrt{p^\star}^{\,m+s+1}\right)$	$\frac{p-1}{2}\left(p^{m-s-1}-\epsilon\eta_0^m(-1)\sqrt{p^\star}^{\,m-s-1}\right)$
$\frac{p-1}{p^2}\left(p^{m}-\epsilon\sqrt{p^\star}^{\,m+s+1}\right)$	$\frac{p-1}{2}\left(p^{m-s-1}+\epsilon\eta_0^m(-1)\sqrt{p^\star}^{\,m-s-1}\right)$
$\frac{1}{p^2}\left((p-1)p^{m}+\epsilon\sqrt{p^\star}^{\,m+s+1}\right)$	$\frac{(p-1)^2}{2}\left(p^{m-s-1}+\epsilon\eta_0^m(-1)\sqrt{p^\star}^{\,m-s-1}\right)$
$\frac{1}{p^2}\left((p-1)p^{m}-\epsilon\sqrt{p^\star}^{\,m+s+1}\right)$	$\frac{(p-1)^2}{2}\left(p^{m-s-1}-\epsilon\eta_0^m(-1)\sqrt{p^\star}^{\,m-s-1}\right)$

Theorem 6. *Let $f(x) \in \mathcal{WRP}$ with ϵ the sign of the Walsh transform of $f(x)$. If $m+s > 3$ is even, then $\overline{C_{D_f}}^{\perp}$ is a $[\frac{1}{p}(p^m + \epsilon(p-1)\sqrt{p^{\star}}^{m+s}), \frac{1}{p}(p^m + \epsilon(p-1)\sqrt{p^{\star}}^{m+s}) - m - 1, 3]$ linear code. If $m+s > 3$ is odd, then $\overline{C_{D_f}}^{\perp}$ is a $[p^{m-1}, p^{m-1} - m - 1, 3]$ linear code.*

Proof. By a similar proof as that of 3, we can derive the desired conclusions based on the weight distribution of $\overline{C_{D_f}}$.

6 Ternary LCD codes from self-orthogonal codes

In this section, we construct new families of ternary LCD codes from self-orthogonal codes constructed in this paper.

For the p-ary linear code $\overline{C_{D_f}}$ in Equation 2.1 with the defining set

$$D_f = \{x \in \mathbb{F}_{p^m} : f(x) + a = 0\}, \ a \in \mathbb{F}_p$$

we assume that $|D_f| = n$ and $D_f = \{d_1, d_2, ..., d_n\}$, where $f(x)$ is a weakly regular plateaued function from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$ and p is an odd prime.

For the generator matrix of $\overline{C_{D_f}}$, consider the following lemma.

Lemma 21. *Let $\overline{C_{D_f}}$ is defined as above and $\mathbb{F}_{p^m}^{\star} = \langle \alpha \rangle$. Then a generator matrix of $\overline{C_{D_f}}$ is given by*

$$\begin{bmatrix} \mathrm{Tr}_{p^m/p}(\alpha^0 d_1) & \mathrm{Tr}_{p^m/p}(\alpha^0 d_2) & \ldots & \mathrm{Tr}_{p^m/p}(\alpha^0 d_n) \\ \mathrm{Tr}_{p^m/p}(\alpha^1 d_1) & \mathrm{Tr}_{p^m/p}(\alpha^1 d_2) & \ldots & \mathrm{Tr}_{p^m/p}(\alpha^1 d_n) \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \mathrm{Tr}_{p^m/p}(\alpha^{m-1} d_1) & \mathrm{Tr}_{p^m/p}(\alpha^{m-1} d_2) & \ldots & \mathrm{Tr}_{p^m/p}(\alpha^{m-1} d_n) \\ 1 & 1 & \ldots & 1 \end{bmatrix}.$$

Proof. The generator matrix G follows from the definition of the augmented code $\overline{C_{D_f}}$ and the fact that $\{\alpha^0, \alpha^1, ..., \alpha^{m-1}\}$ form a basis of $\mathbb{F}_{p^m}$ over $\mathbb{F}_p$.

Theorem 7. *Let $m + s > 4$ be even, $f(x) \in \mathcal{WRP}$ and ϵ be the sign of the Walsh transform of $f(x)$. Let $p = 3$ and $D_f = \{x \in \mathbb{F}_{3^m} : f(x) + a = 0\}$ for $a \in \mathbb{F}_3^{\star}$. Let $\overline{C_{D_f}}$ be defined as above and its generator matrix G is given in Lemma 21. Then the matrix $\overline{G} = [I : G]$ generates a ternary LCD code $\mathcal{C}$ with parameters*
$\left[3^{m-1} + \epsilon(-3)^{\frac{m+s-2}{2}} + m + 1, m + 1, d \geq min\{2 \cdot 3^{m-2}, 2 \cdot (3^{m-2} + \epsilon(-3)^{\frac{m+s-2}{2}})\}\right]$
Besides, $\mathcal{C}^{\perp}$ is a ternary $\left[3^{m-1} + \epsilon(-3)^{\frac{m+s-2}{2}} + m + 1, 3^{m-1} + \epsilon(-3)^{\frac{m+s-2}{2}}, 3\right]$ LCD codes which is at least almost optimal according to the sphere-packing bound.

Proof. In view of Theorems 1 and 3, the proof can proceed using the same argument given in the proof of Theorem 7 in [10]

Theorem 8. *Let $m+s>3$ be odd, $f(x)\in\mathcal{WRP}$ and ϵ be the sign of the Walsh transform of $f(x)$. Let $p=3$ and $D_f=\{x\in\mathbb{F}_{3^m}: f(x)+a=0\}$ for $a\in\mathbb{F}_3^\star$. Let $\overline{C_{D_f}}$ be defined as above and its generator matrix G is given in Lemma 21. Then the matrix $\overline{G}=[I:G]$ generates a ternary LCD code $\mathcal{C}$ with parameters*
$\left[3^{m-1}-\eta_0(a)\epsilon(-3)^{\frac{m+s-1}{2}}+m+1, m+1, d\geq min\{2\cdot 3^{m-2}, 2\cdot(3^{m-2}+2\epsilon\cdot\eta_0(a)(-3)^{\frac{m+s-3}{2}})\}\right]$
and $\mathcal{C}^\perp$ is a ternary $\left[3^{m-1}-\eta_0(a)\epsilon(-3)^{\frac{m+s-1}{2}}+m+1, 3^{m-1}-\eta_0(a)\epsilon(-3)^{\frac{m+s-1}{2}}, 3\right]$ LCD code which is at least almost optimal according to the sphere-packing bound.

Proof. Similarly to the proof of Theorem 7, the desired conclusion follows from Theorem 2 and the proof of Theorem 7 in [10]

Theorem 9. *Let $m+s>3$ be even, $f(x)\in\mathcal{WRP}$ and ϵ be the sign of the Walsh transform of $f(x)$. Let $p=3$ and $D_f=\{x\in\mathbb{F}_{3^m}: f(x)=0\}$. Let $\overline{C_{D_f}}$ be defined as above and its generator matrix G is given in Lemma 21. Then the matrix $\overline{G}=[I:G]$ generates a ternary LCD code $\mathcal{C}$ with parameters*
$\left[\frac{1}{3}\left(3^m+2\epsilon\sqrt{-3}^{m+s}\right)+m+1, m+1, d\geq 1\min\left\{2\cdot 3^{m-2}, \frac{2}{3}\left(3^{m-1}+\epsilon\sqrt{-3}^{m+s}\right)\right\}\right]$.

Proof. Similarly to the proof of Theorem 7, the desired conclusion follows from Theorem 4 and the proof of Theorem 7 in [10]

Theorem 10. *Let $m+s>3$ be odd, $f(x)\in\mathcal{WRP}$ and ϵ be the sign of the Walsh transform of $f(x)$. Let $p=3$ and $D_f=\{x\in\mathbb{F}_{3^m}: f(x)=0\}$. Let $\overline{C_{D_f}}$ be defined as above and its generator matrix G is given in Lemma 21. Then the matrix $\overline{G}=[I:G]$ generates a ternary LCD code $\mathcal{C}$ with parameters*
$\left[3^{m-1}+m+1, m+1, d\geq 1\min\left\{\frac{2}{9}\left(3^m\pm\epsilon\sqrt{-3}^{m+s+1}\right)\right\}\right]$.

Proof. Similarly to the proof of Theorem 7, the desired conclusion follows from Theorem 5 and the proof of Theorem 7 in [10]

7 Concluding Remarks and Future Work

We generalize the recent construction method introduced by Heng et. al. [10] to weakly regular plateaued unbalanced functions. We constructed new families of ternary self-orthogonal codes from weakly regular plateaued unbalanced functions over $\mathbb{F}_3$. Then we used self-orthogonal codes to construct infinite families of ternary LCD codes and we observed that some codes are at least almost optimal according to the sphere-packing bound. Moreover, we constructed new families of p-ary linear codes from weakly regular plateaued unbalanced functions over $\mathbb{F}_p$ for any odd prime p.

As future work, we are studying the construction of self-orthogonal p-ary linear codes from weakly regular plateaued balanced functions over the finite fields of any odd characteristics. We hope to obtain new families of (self-orthogonal) p-ary linear codes from weakly regular plateaued balanced functions over $\mathbb{F}_p$ for any odd prime p.

References

1. Anderson, R., Ding, C., Helleseth, T., Klove, T.: How to build robust shared control systems. Designs, Codes and Cryptography **15**(2), 111–124 (1998)
2. Carlet, C., Ding, C., Yuan, J.: Linear codes from perfect nonlinear mappings and their secret sharing schemes. IEEE Transactions on Information Theory **51**(6), 2089–2102 (2005)
3. Chabanne, H., Cohen, G., Patey, A.: Towards secure two-party computation from the wire-tap channel. In: International Conference on Information Security and Cryptology. pp. 34–46. Springer (2013)
4. Cohen, G., Mesnager, S., Randriam, H.: Yet another variation on minimal linear codes. In: 2015 Information Theory and Applications Workshop (ITA). pp. 329–330. IEEE (2015)
5. Cohen, G.D., Mesnager, S., Patey, A.: On minimal and quasi-minimal linear codes. In: Cryptography and Coding: 14th IMA International Conference, IMACC 2013, Oxford, UK, December 17-19, 2013. Proceedings 14. pp. 85–98. Springer (2013)
6. Ding, C.: A construction of binary linear codes from boolean functions. Discrete mathematics **339**(9), 2288–2303 (2016)
7. Ding, C., Heng, Z., Zhou, Z.: Minimal binary linear codes. IEEE Transactions on Information Theory **64**(10), 6536–6545 (2018)
8. Ding, C., Wang, X.: A coding theory construction of new systematic authentication codes. Theoretical computer science **330**(1), 81–99 (2005)
9. Ding, K., Ding, C.: A class of two-weight and three-weight codes and their applications in secret sharing. IEEE Transactions on Information Theory **61**(11), 5835–5842 (2015)
10. Heng, Z., Li, D., Liu, F.: Ternary self-orthogonal codes from weakly regular bent functions and their application in LCD codes. Des. Codes Cryptogr. **91**(12), 3953–3976 (2023). https://doi.org/10.1007/S10623-023-01287-5, `https://doi.org/10.1007/s10623-023-01287-5`
11. Kenneth Ireland, M.R.: A Classical Introduction to Modern Number Theory. Springer New York, NY (2013)
12. Lidl, R., Niederreiter, H.: Finite fields, vol. 20. Cambridge university press (1997)
13. Massey, J.L.: Linear codes with complementary duals. Discrete Mathematics **106**, 337–342 (1992)
14. Massey, J.L.: Orthogonal , antiorthogonal and self-orthogonal matrices and their codes (1998), `https://api.semanticscholar.org/CorpusID:6889914`
15. Mesnager, S.: Linear codes with few weights from weakly regular bent functions based on a generic construction. Cryptography and Communications **9**(1), 71–84 (2017)
16. Mesnager, S., Sınak, A.: Infinite classes of six-weight linear codes derived from weakly regular plateaued functions. In: 2020 International Conference on Information Security and Cryptology (ISCTURKEY). pp. 93–100. IEEE (2020)
17. Mesnager, S., Sınak, A.: Several classes of minimal linear codes with few weights from weakly regular plateaued functions. IEEE Transactions on Information Theory **66**(4), 2296–2310 (2020). https://doi.org/10.1109/TIT.2019.2956130
18. Mesnager, S., Özbudak, F., Sinak, A.: Linear codes from weakly regular plateaued functions and their secret sharing schemes. DESIGNS CODES AND CRYPTOGRAPHY p. 463–480 (2019)
19. Schoenmakers, B.: A simple publicly verifiable secret sharing scheme and its application to electronic voting. In: Annual International Cryptology Conference. pp. 148–164. Springer (1999)
20. Tang, C., Li, N., Qi, Y., Zhou, Z., Helleseth, T.: Linear codes with two or three weights from weakly regular bent functions. IEEE Transactions on Information Theory **62**(3), 1166–1176 (2016)
21. W. Cary Huffman, V.P.: Fundamentals of Error-Correcting Codes. Cambridge University Press (2003)
22. Yang, S., Zhang, T., Li, P.: Linear codes from two weakly regular plateaued balanced functions. Entropy **25**(2), 369 (2023)
23. Yuan, J., Ding, C.: Secret sharing schemes from three classes of linear codes. IEEE Transactions on Information Theory **52**(1), 206–212 (2006)