Constructions of self-orthogonal codes and LCD codes from functions over finite fields

Sihem MESNAGER[1,2] and Ahmet SINAK[1,3]

[1]Department of Mathematics, University of Paris VIII, Saint-Denis, 93526, France.

[2]LAGA, UMR 7539, CNRS, Sorbonne Paris Cité, University of Paris XIII, Villetaneuse, 93430, France.

[3]Department of Management Information Systems, Akdeniz University, Antalya, 07600, Türkiye.

Contributing authors: smesnager@univ-paris8.fr; sinakahmet@gmail.com;

Abstract

The construction of self-orthogonal codes from functions over finite fields has been widely studied in the literature. In this paper, we construct new families of self-orthogonal linear codes with few weights from trace functions and weakly regular plateaued functions over the finite fields of odd characteristics. We determine all parameters of the constructed self-orthogonal codes and their dual codes. Moreover, we employ the constructed $\boldsymbol{p}$-ary self-orthogonal codes to construct $\boldsymbol{p}$-ary LCD codes.

Keywords: Linear code, Self-orthogonal code, LCD code, Weakly regular plateaued function

1 Introduction

Linear codes have been an attractive research topic in both practice and theory for the last two decades. They have diverse applications in secure communication [1], secret sharing schemes [2–4], authentication codes [5] and secure two-party computation [6, 7]. A linear code is considered self-orthogonal if contained within its dual code. Self-orthogonal codes have applications in Linear Complementary Dual (LCD) codes, quantum codes, etc.. LCD codes also have diverse applications in certain communication systems. Carlet and Guilley [8] demonstrated their significance in information protection and defence against side-channel and fault non-invasive attacks. After these observations, the importance of applications of LCD codes has begun to be revitalized. Massey [9] introduced the LCD codes and showed that they provide an optimum linear coding solution to the two-user binary adder channel. Now, it is known that asymptotically good LCD codes exist and the necessary and sufficient condition for a length n cyclic code to be an LCD code is known. 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, 3, 6, 10–13]). Linear codes derived from cryptographic functions have desirable algebraic structures that are significant from the application point of view. 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 using the second generic construction method (e.g., [3, 10, 14]) and the second generic construction method (e.g., [12, 15]. Recently, Heng et al. [16] have constructed self-orthogonal codes from trace functions and weakly regular bent functions based on the first and second generic construction methods. This work motivates us to construct self-orthogonal codes from trace functions and weakly regular plateaued functions over the odd characteristic finite fields. This paper obtains new families of p-ary self-orthogonal linear codes with few weights based on the first and second generic construction methods. Then, we use the constructed self-orthogonal codes to construct infinite families of LCD codes.

The paper is organized as follows. Section 2 establishes the main notations. In Sections 3 and 4, we construct several families of self-orthogonal codes with few weights over the odd characteristic finite fields by using the first and second generic construction methods. Moreover, we construct LCD codes from the constructed self-orthogonal codes. Section 5 concludes the paper.

2 Preliminaries

For a set S, its size is denoted by $\#S$, and $S^\star = S \setminus \{0\}$. The magnitude of a complex number $z \in \mathbb{C}$ is denoted by $|z|$. The finite field with q elements is represented by $\mathbb{F}_q$, where $q = p^m$ for a positive integer n and an odd prime p. The trace of $a \in \mathbb{F}_q$ over $\mathbb{F}_p$ is defined as $\mathrm{Tr}^m(a) = a + a^p + a^{p^2} + \cdots + a^{p^{m-1}}$. The set of all *nom-squares* and *squares* in $\mathbb{F}_p^\star$ are represented by NSQ and SQ, respectively. The *quadratic character* of $\mathbb{F}_p^\star$ is denoted by η_0, and for simplicity we write $p^* = \eta_0(-1)p$, which is frequently used in the sequel.

A cyclotomic field $\mathbb{Q}(\xi_p)$ can be obtained from the rational field $\mathbb{Q}$ by joining the *complex primitive p-th root of unity* ξ_p. The field $\mathbb{Q}(\xi_p)$ is the splitting field of the polynomial $x^p - 1$, and so the field $\mathbb{Q}(\xi_p)/\mathbb{Q}$ is a Galois extension of degree $p-1$. Here, a field basis for an extension $\mathbb{Q}(\xi_p)/\mathbb{Q}$ is the subset $\{1, \xi_p, \xi_p^2, \ldots, \xi_p^{p-2}\}$ of the cyclotomic field $\mathbb{Q}(\xi_p)$. The Galois group $Gal(\mathbb{Q}(\xi_p)/\mathbb{Q})$ is described as the set $\{\sigma_a \colon a \in \mathbb{F}_p^\star\}$, where σ_a is the automorphism of $\mathbb{Q}(\xi_p)$ defined as $\sigma_a(\xi_p) = \xi_p^a$. The cyclotomic field $\mathbb{Q}(\xi_p)$ has a unique quadratic subfield $\mathbb{Q}(\sqrt{p^*})$, and its Galois group $Gal(\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}) = \{1, \sigma_\gamma\}$ for some $\gamma \in NSQ$. For $a \in \mathbb{F}_p^\star$ and $b \in \mathbb{F}_p$, we clearly have $\sigma_a(\xi_p^b) = \xi_p^{ab}$ and $\sigma_a(\sqrt{p^*}^m) = {\eta_0}^m(a)\sqrt{p^*}^m$.

The following lemma is frequently used in the subsequent proofs.

Lemma 1. *[17] Keeping the above notations, we have the following facts.*

i.) $\sum_{a\in\mathbb{F}_p^\star} \eta_0(a) = 0,$

ii.) $\sum_{a\in\mathbb{F}_p^*} \xi_p^{ab} = -1$ *for every* $b \in \mathbb{F}_p^*,$

iii.) $\sum_{a\in\mathbb{F}_p} \xi_p^{ab} = \begin{cases} p, & \text{if } b = 0, \\ 0, & \text{if } b \in \mathbb{F}_p^\star, \end{cases}$

iv.) $\sum_{a\in\mathbb{F}_p^\star} \eta_0(a)\xi_p^{ab} = \eta_0(b)\sqrt{p^*} = \begin{cases} \sqrt{p^*}, & \text{if } b \in SQ, \\ -\sqrt{p^*}, & \text{if } b \in NSQ, \end{cases}$

v.) $\sum_{a\in\mathbb{F}_p} \xi_p^{a^2 b} = \begin{cases} p, & \text{if } b = 0, \\ \sqrt{p^*}, & \text{if } b \in SQ, \\ -\sqrt{p^*}, & \text{if } b \in NSQ. \end{cases}$

2.1 Weakly regular plateaued functions

Let $f : \mathbb{F}_q \longrightarrow \mathbb{F}_p$ be a p-ary function, where $q = p^m$. The *Walsh transform* of f is a complex-valued function defined as

$$\mathcal{W}_f(b) = \sum_{x\in\mathbb{F}_q} \xi_p^{\,f(x)-\mathrm{Tr}^m(bx)}, \ \ b \in \mathbb{F}_q.$$

A function f is said to be a *bent* function if $|\mathcal{W}_f(b)|^2 = p^m$ for every $b \in \mathbb{F}_q$. In addition, f is said to be s*-plateaued* if $|\mathcal{W}_f(b)|^2 \in \{0, p^{m+s}\}$ for every $b \in \mathbb{F}_q$, with $0 \le s \le n$. For an s-plateaued function f, its *Walsh support* is described as the set

$$\mathcal{S}_f = \{b \in \mathbb{F}_q \colon \ |\mathcal{W}_f(b)|^2 = p^{m+s}\}.$$

Lemma 2. *Let f be an s-plateaued function. For $b \in \mathbb{F}_q$, $|\mathcal{W}_f(b)|^2$ takes the values p^{m+s} and 0 for the times p^{m-s} and $p^m - p^{m-s}$, respectively.*

Lemma 3. *[15] Let f be an s-plateaued function. Define the sets*

$$\begin{aligned} \mathcal{S}(\mathcal{W}_f) &= \{(a,b) \in \mathbb{F}_p^\star \times \mathbb{F}_{p^m} : \mathcal{W}_f(a^{-1}b) \neq 0\}, \\ \mathcal{Z}(\mathcal{W}_f) &= \{(a,b) \in \mathbb{F}_p^\star \times \mathbb{F}_{p^m} : \mathcal{W}_f(a^{-1}b) = 0\}, \end{aligned}$$

where a^{-1} is the multiplicative inverse of $a \in \mathbb{F}_p^\star$. Then, the sizes of $\mathcal{Z}(\mathcal{W}_f)$ and $\mathcal{S}(\mathcal{W}_f)$ are equal respectively to $(p-1)(p^m - p^{m-s})$ and $(p-1)p^{m-s}$.

Mesnager et al. [15] have described the notion of weakly regular plateaued functions. An s-plateaued f is called *weakly regular* if we have

$$\mathcal{W}_f(b) \in \left\{0, up^{\frac{m+s}{2}}\xi_p^{f^\star(b)}\right\},$$

where $u \in \{\pm 1, \pm i\}$, $f^\star$ is a p-ary function over $\mathbb{F}_q$ with $f^\star(b) = 0$ for every $b \in \mathbb{F}_q \backslash \mathcal{S}_f$; otherwise, f is called *non-weakly regular*. A weakly regular 0-plateaued is the weakly regular bent function.

The following lemmas are useful for computing the Hamming weights and their distributions in codes.

Lemma 4. *[15] Let f be a weakly regular s-plateaued function. Then, we have*

$$\mathcal{W}_f(b) = \epsilon_f \sqrt{p^*}^{\,m+s} \xi_p^{f^\star(b)}$$

for every $b \in \mathcal{S}_f$, where $\epsilon_f = \pm 1$ is the sign of $\mathcal{W}_f$ and $f^\star$ is a p-ary function over $\mathcal{S}_f$.

Lemma 5. *[14] Let $f : \mathbb{F}_q \to \mathbb{F}_p$ be an unbalanced function with $\mathcal{W}_f(0) = \epsilon_f \sqrt{p^*}^{\,m+s}$, where $\epsilon_f = \pm 1$ is the sign of $\mathcal{W}_f$. For $j \in \mathbb{F}_p$, define $\mathcal{N}_f(j) = \#\{x \in \mathbb{F}_q : f(x) = j\}$. When $m+s$ is even,*

$$\mathcal{N}_f(j) = \begin{cases} p^{m-1} + \epsilon_f \eta_0(-1)(p-1)\sqrt{p^*}^{\,m+s-2}, & \text{if } j = 0, \\ p^{m-1} - \epsilon_f \eta_0(-1)\sqrt{p^*}^{\,m+s-2}, & \text{if } j \in \mathbb{F}_p^\star. \end{cases}$$

When $m+s$ is odd,

$$\mathcal{N}_f(j) = \begin{cases} p^{m-1}, & \text{if } j = 0, \\ p^{m-1} + \epsilon_f \sqrt{p^*}^{m+s-1}, & \text{if } j \in SQ, \\ p^{m-1} - \epsilon_f \sqrt{p^*}^{m+s-1}, & \text{if } j \in NSQ. \end{cases}$$

Lemma 6. *[14] Let f be weakly regular s-plateaued with $\mathcal{W}_f(b) = \epsilon_f \sqrt{p^*}^{\,m+s} \xi_p^{f^\star(b)}$ for every $b \in \mathcal{S}_f$. For $j \in \mathbb{F}_p$, define $\mathcal{N}_{f^\star}(j) = \#\{b \in \mathcal{S}_f : f^\star(b) = j\}$. When $m-s$ is even,*

$$\mathcal{N}_{f^\star}(j) = \begin{cases} p^{m-s-1} + \epsilon_f \eta_0^{m+1}(-1)(p-1)\sqrt{p^*}^{\,m-s-2}, & \text{if } j = 0, \\ p^{m-s-1} - \epsilon_f \eta_0^{m+1}(-1)\sqrt{p^*}^{\,m-s-2}, & \text{if } j \in \mathbb{F}_p^\star. \end{cases}$$

When $m-s$ is odd,

$$\mathcal{N}_{f^\star}(j) = \begin{cases} p^{m-s-1}, & \text{if } j = 0, \\ p^{m-s-1} + \epsilon_f \eta_0^{m}(-1)\sqrt{p^*}^{\,m-s-1}, & \text{if } j \in SQ, \\ p^{m-s-1} - \epsilon_f \eta_0^{m}(-1)\sqrt{p^*}^{\,m-s-1}, & \text{if } j \in NSQ. \end{cases}$$

2.2 Linear codes

Let $\mathbb{F}_p$ be a finite field with p elements and $\mathbb{F}_p^n$ be a vector space over $\mathbb{F}_p$ for a positive integer n. A linear code $\mathcal{C}$ over $\mathbb{F}_p$ with parameters $[n, k, d]$ is a k-dimensional linear subspace of a vector space $\mathbb{F}_p^n$, where d denotes the minimum Hamming distance of $\mathcal{C}$. Let $\mathbf{a}$ be a vector in $\mathbb{F}_p^n$ and its support is defined as supp($\mathbf{a}$)= $\{0 \le i \le n-1 : a_i \ne 0\}$. The cardinality of supp($\mathbf{a}$) is called the Hamming weight of a vector $\mathbf{a}$. Let $\mathbf{c}$ be a codeword of $\mathcal{C}$. The minimum Hamming distance d in $\mathcal{C}$ is the minimum Hamming weight of $\mathbf{c} \in \mathcal{C}$. Let $A_i := |\{\mathbf{c} \in \mathcal{C} : wt(\mathbf{c}) = i$ for $0 \le i \le n\}|$ for a linear code $\mathcal{C}$.

Define the weight enumerator of $\mathcal{C}$ by the polynomial $1 + A_1 y + ... + A_n y^n$. The dual code $\mathcal{C}^\perp$ of an $[n, k]$ linear code $\mathcal{C}$ is defined by

$$\mathcal{C}^\perp = \{\mathbf{c}^\perp \in \mathbb{F}_p^n : \mathbf{c}^\perp \cdot \mathbf{c} \text{ for all } \mathbf{c} \in \mathcal{C}\},$$

where "$\cdot$" is the standard inner product over $\mathbb{F}_p^n$, and $\mathcal{C}^\perp$ 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 code. If the Hamming weight of each codeword in $\mathcal{C}$ is divisible by an integer $k > 1$, then the code $\mathcal{C}$ 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 $\mathcal{C}$, stated in the following lemma.

Lemma 7. *[18] Let $\mathcal{C}$ be an $[n, k, d]$ linear code over $\mathbb{F}_p$ with $\mathbf{1} \in \mathcal{C}$, where $\mathbf{1}$ is the all-1 vector of length n. If $\mathcal{C}$ is p-divisible, then $\mathcal{C}$ is self-orthogonal.*

According to Lemma 7, one can verify whether a p-ary linear code is self-orthogonal.

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 [9]. Besides, LCD codes were shown to give an optimum solution to the two-user binary adder channel [9].

A matrix G is said to be row-orthogonal if $GG^\perp = I$, where I is an identity matrix, and it is called row-self-orthogonal if $GG^\perp = \mathbf{0}$. A linear code $\mathcal{C}$ is self-orthogonal if and only if its generator matrix is row-self-orthogonal [19]. 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 8. *[19] A leading-systematic linear code $\mathcal{C}$ is an LCD code if its systematic generator matrix $G = [I : A]$ is row-orthogonal.*

According to Lemma 8, if a code $\mathcal{C}$ is self-orthogonal with a generator matrix G, we can construct a leading-systematic LCD code with a generator matrix $G' = [I : G]$.

Augmented code of a linear code. Let $\mathcal{C}$ be an $[n, k, d]$ linear code over $\mathbb{F}_p$ with a generator matrix G. The augmented code $\overline{\mathcal{C}}$ of the code $\mathcal{C}$ 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 $\mathbf{1} \notin \mathcal{C}$, 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. The codes constructed in this paper are self-orthogonal due to Lemma 7 for almost all cases.

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 $\mathcal{C}^{\perp}$ by $(1, A_1, \ldots, A_n)$ and $(1, A_1^{\perp}, \ldots, A_n^{\perp})$, respectively. The first four Pless power moments are given [1, Page 260] as:

$$\begin{aligned}
\sum_{i=0}^{n} A_i &= p^k \\
\sum_{i=0}^{n} iA_i &= p^{k-1}\left(pn - n - A_1^{\perp}\right) \\
\sum_{i=0}^{n} i^2 A_i &= p^{k-2}[(p-1)n(pn-n+1) - (2pn-p-2n+2)A_1^{\perp} + 2A_2^{\perp}] \\
\sum_{i=0}^{n} i^3 A_i &= p^{k-3}[(p-1)nL - TA_1^{\perp} + 6(pn-p-n+2)A_2^{\perp} - 6A_3^{\perp}],
\end{aligned}$$

where we have $T = (3p^2n^2 - 3p^2n - 6pn^2 + 12pn + p^2 - 6p + 3n^2 - 9n + 6)$ and $L = (p^2n^2 - 2pn^2 + 3pn - p + n^2 - 3n + 2)$.

Some codes proposed in this paper are (almost) optimal codes due to the following Griesmer bound.

Lemma 9. *(Griesmer bound) [20] Let $\mathcal{C}$ be a linear $[n,k,d]$ code over $\mathbb{F}_p$. Then, the code $\mathcal{C}$ satisfies the following well-known bound:*

$$n \geq \sum_{i=0}^{k-1} \lceil \frac{d}{p^i} \rceil,$$

where $\lceil \cdot \rceil$ is the ceiling function.

3 Constructions of self-orthogonal codes from the second generic construction method

In this section, we define the augmented code construction of the variation of the second generic construction method given in [21].

For $\lambda \in \mathbb{F}_p$ and $d \in \mathbb{Z}^+$, define a set $D_\lambda^* = \left\{(x,y) \in \mathbb{F}_{p^m}^{\star} \times \mathbb{F}_{p^m} \mid \mathrm{Tr}(yx^{d+1}) = \lambda\right\}$ and define a linear code $C_{D_\lambda^*}$ as follows:

$$C_{D_\lambda^*} = \left\{\mathbf{c}_{(a,b)} = (\mathrm{Tr}(ayx^d + bx))_{(x,y)\in D_\lambda^*} \mid (a,b) \in \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}\right\}. \quad (1)$$

The linear code $C_{D_\lambda^*}$ of length $\#D_\lambda^*$ is an $2m$-dimensional subspace of $\mathbb{F}_p^m$ over $\mathbb{F}_p$, and denoted by $[\#D_\lambda^*, 2m]_p$. The code $\mathcal{C}_{D_\lambda^*}$ defined in (1) has been recently studied in [21] and two new classes of projective two-weight codes are constructed.

For every $\lambda \in \mathbb{F}_p$ and $d \in \mathbb{Z}^+$, we define the set

$$D_\lambda = \left\{(x,y) \in \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \mid \mathrm{Tr}(yx^{d+1}) = \lambda\right\}. \quad (2)$$

The *augmented code* $\overline{\mathcal{C}_{D_\lambda}}$ is defined as

$$\overline{\mathcal{C}_{D_\lambda}} = \{\mathbf{c}_{(a,b,c)} = \big((\mathrm{Tr}(ayx^d + bx))_{(x,y)\in D_\lambda} + c\mathbf{1}\big) \, : \, (a,b,c) \in \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \times \mathbb{F}_p\}. \quad (3)$$

The length of the augmented code $\overline{\mathcal{C}_{D_\lambda}}$ is the same as that of the original code. If $\mathbf{1} \notin \overline{\mathcal{C}_{D_\lambda}}$, then the augmented code $\overline{\mathcal{C}_{D_\lambda}}$ has larger dimension than that of the original code $\mathcal{C}_{D^\star_\lambda}$. Thus, the augmented code $\overline{\mathcal{C}_{D_\lambda}}$ is $(2m+1)$-dimensional subspace of $\mathbb{F}_p^m$ over $\mathbb{F}_p$ and denoted by $[\#D_\lambda, 2m+1]_p$. In this paper, we study the augmented code $\overline{\mathcal{C}_{D_\lambda}}$ for every $\lambda \in \mathbb{F}_p$, and obtain self-orthogonal codes, LCD codes, LRC codes etc.

The length of the code $\overline{\mathcal{C}_{D_\lambda}}$ is the size of the defining set D_λ, which is calculated in Lemma 10. It is clear that, for $a = b = c = 0$, the Hamming weight of the zero vector is $wt(\mathbf{c}_{(0,0,0)}) = 0$. To find Hamming weights in the augmented code $\overline{\mathcal{C}_{D_\lambda}}$, for $\lambda \in \mathbb{F}_p$, $a, b \in \mathbb{F}_q$ and $c \in \mathbb{F}_p$, we define the following set

$$\begin{aligned} N_\lambda(a,b,c) \quad &= \big\{(x,y) \in \mathbb{F}_q \times \mathbb{F}_q \mid (x,y) \in D_\lambda \ \textit{and} \ \mathrm{Tr}(ax^d y + bx) + c = 0\big\} \\ &= \big\{(x,y) \in \mathbb{F}_q \times \mathbb{F}_q \mid \mathrm{Tr}(x^{d+1}y) = \lambda \ \textit{and} \ \mathrm{Tr}(ax^d y + bx) + c = 0\big\}. \end{aligned} \quad (4)$$

It is obvious that $\#N_\lambda(0,0,c) = 0$ when $a = b = 0$ and $c \neq 0$. This implies that $wt(\mathbf{c}_{(0,0,c)}) = \#D_\lambda$. For every $(a,b,c) \in \mathbb{F}_{p^m} \times \mathbb{F}_{p^m} \times \mathbb{F}_p \setminus \{(0,0,c)\}$, the Hamming weight of each codeword $\mathbf{c}_{(a,b,c)}$ in $\overline{\mathcal{C}_{D_\lambda}}$ is

$$wt(\mathbf{c}_{(a,b,c)}) = \#D_\lambda - \#N_\lambda(a,b,c). \quad (5)$$

Lemma 11 calculates the value $\#N_\lambda(a,b,c)$ for each case in the following section.

We now present three lemmas to find the parameters of the codes.

Lemma 10. *Let D_λ be the set defined in (2). Then,*

$$\#D_\lambda = \begin{cases} p^{2m-1} + (p-1)p^{m-1}, & \textit{if } \lambda = 0, \\ p^{2m-1} - p^{m-1}, & \textit{if } \lambda \neq 0. \end{cases} \quad (6)$$

Proof. From the definition of D_λ, we have

$$\begin{aligned}
\#D_\lambda &= \sum_{x\in\mathbb{F}_q}\sum_{y\in\mathbb{F}_q}\left(p^{-1}\sum_{z_1\in\mathbb{F}_p}\epsilon^{z_1(\mathrm{Tr}(yx^{d+1})-\lambda)}\right)\\
&= \tfrac{1}{p}\sum_{x\in\mathbb{F}_q}\sum_{y\in\mathbb{F}_q}\left(\sum_{z_1\in\mathbb{F}_p^\star}\epsilon_p^{z_1(\mathrm{Tr}(yx^{d+1})-\lambda)}+1\right)\\
&= p^{2m-1}+\tfrac{1}{p}\sum_{z_1\in\mathbb{F}_p^\star}\epsilon_p^{-\lambda z_1}\sigma_{z_1}\left(\sum_{x\in\mathbb{F}_q}\sum_{y\in\mathbb{F}_q}\epsilon_p^{\mathrm{Tr}(yx^{d+1})}\right)\\
&= p^{2m-1}+\tfrac{1}{p}\sum_{z_1\in\mathbb{F}_p^\star}\epsilon_p^{-\lambda z_1}\sigma_{z_1}\left(p^m+\sum_{x\in\mathbb{F}_q^\star}\sum_{y\in\mathbb{F}_q}\epsilon_p^{\mathrm{Tr}(yx^{d+1})}\right)\\
&= p^{2m-1}+p^{m-1}\sum_{z_1\in\mathbb{F}_p^\star}\epsilon_p^{-\lambda z_1}.
\end{aligned}$$

The proof is complete from Lemma 1. □

Lemma 11. *Let $N_\lambda(a,b,c)$ be the set in (4) for $(a,b,c)\in\mathbb{F}_{p^m}\times\mathbb{F}_{p^m}\times\mathbb{F}_p\setminus\{(0,0,c)\}$. Then we have the following results. If $\lambda=0$, then*

$$\#N_0(a,b,c)=\begin{cases}
p^{2m-2}+(p-1)p^{m-1}, & \text{if } a=0\wedge b\neq 0\wedge c=0,\\
 & \text{or } a\neq 0\wedge b\in\mathbb{F}_q\wedge c=0\wedge \mathrm{Tr}(ab)\neq 0,\\
p^{2m-2}, & \text{if } a=0\wedge b\neq 0\wedge c\neq 0,\\
 & \text{or } a\neq 0\wedge b\in\mathbb{F}_q\wedge c\neq 0\wedge \mathrm{Tr}(ab)\neq 0,\\
p^{2m-2}+2(p-1)p^{m-1}, & \text{if } a\neq 0\wedge b\in\mathbb{F}_q\wedge c=0\wedge \mathrm{Tr}(ab)=0\\
p^{2m-2}-p^{m-1}, & \text{if } a\neq 0\wedge b\in\mathbb{F}_q\wedge c\neq 0\wedge \mathrm{Tr}(ab)=0.
\end{cases}\tag{7}$$

If $\lambda\neq 0$, then

$$\#N_\lambda(a,b,c)=\begin{cases}
p^{2m-2}-p^{m-1}, & \text{if } a=0\wedge b\neq 0\wedge c=0,\\
 & \text{or } a\neq 0\wedge b\in\mathbb{F}_q\wedge c=0\wedge \mathrm{Tr}(ab)=0\\
 & \text{or } a\neq 0\wedge b\in\mathbb{F}_q\wedge c=0\wedge \mathrm{Tr}(ab)\neq 0\wedge k\in NSQ\\
 & \text{or } a\neq 0\wedge b\in\mathbb{F}_q\wedge c\neq 0\wedge \mathrm{Tr}(ab)\neq 0\wedge k\in NSQ\\
p^{2m-2}, & \text{if } a=0\wedge b\neq 0\wedge c\neq 0,\\
 & \text{or } a\neq 0\wedge b\in\mathbb{F}_q\wedge c\neq 0\wedge \mathrm{Tr}(ab)=0\\
p^{2m-2}+p^{m-1}, & \text{if } a\neq 0\wedge b\in\mathbb{F}_q\wedge c=0\wedge \mathrm{Tr}(ab)\neq 0\wedge k\in SQ\\
 & \text{or } a\neq 0\wedge b\in\mathbb{F}_q\wedge c\neq 0\wedge \mathrm{Tr}(ab)\neq 0\wedge k\in SQ,
\end{cases}\tag{8}$$

where $k=c^2-4\lambda\mathrm{Tr}(ab)$.

Proof. From the definition of the set, we have the following

$$\begin{aligned}
\#N(a,b,c) &= \sum_{x\in\mathbb{F}_q}\sum_{y\in\mathbb{F}_q}\left(p^{-1}\sum_{z_1\in\mathbb{F}_p}\epsilon_p^{z_1(\mathrm{Tr}(x^{d+1}y)-\lambda)}\right)\left(p^{-1}\sum_{z_2\in\mathbb{F}_p}\epsilon_p^{z_2(\mathrm{Tr}(ayx^d+bx)+c)}\right)\\
&= p^{-2}\sum_{z_1,z_2\in\mathbb{F}_p}\left(\sum_{x,y\in\mathbb{F}_q}\epsilon_p^{z_1(\mathrm{Tr}(yx^{d+1})-\lambda)+z_2(\mathrm{Tr}(ax^dy+bx)+c)}\right)\\
&= p^{2m-2}+p^{-2}\sum_{z_1\in\mathbb{F}_p^\star}\left(\sum_{x,y\in\mathbb{F}_q}\epsilon_p^{z_1(\mathrm{Tr}(yx^{d+1})-\lambda)+0(\mathrm{Tr}(ax^dy+bx)+c)}\right)\\
&+p^{-2}\sum_{z_2\in\mathbb{F}_p^\star}\left(\sum_{x,y\in\mathbb{F}_q}\epsilon_p^{0(\mathrm{Tr}(yx^{d+1})-\lambda)+z_2(\mathrm{Tr}(ax^dy+bx)+c)}\right)\\
&+p^{-2}\sum_{z_1,z_2\in\mathbb{F}_p^\star}\left(\sum_{x,y\in\mathbb{F}_q}\epsilon_p^{z_1(\mathrm{Tr}(yx^{d+1})-\lambda)+z_2(\mathrm{Tr}(ax^dy+bx)+c)}\right)\\
&= p^{2m-2}+\frac{1}{p^2}\left(\Omega_0+\Omega_1+\Omega_2\right)
\end{aligned}$$

where

$$\begin{aligned}
\Omega_0 &= \sum_{z_1\in\mathbb{F}_p^\star}\left(\sum_{x,y\in\mathbb{F}_q}\epsilon_p^{z_1(\mathrm{Tr}(yx^{d+1})-\lambda)}\right)\\
\Omega_1 &= \sum_{z_2\in\mathbb{F}_p^\star}\left(\sum_{x,y\in\mathbb{F}_q}\epsilon_p^{z_2(\mathrm{Tr}(ax^dy+bx)+c)}\right)\\
\Omega_2 &= \sum_{z_1,z_2\in\mathbb{F}_p^\star}\left(\sum_{x,y\in\mathbb{F}_q}\epsilon_p^{z_1(\mathrm{Tr}(yx^{d+1})-\lambda)+z_2(\mathrm{Tr}(ax^dy+bx)+c)}\right).
\end{aligned}$$

We now calculate these statements for each case. It is easy to verify that

$$\begin{aligned}
\Omega_0 &= \sum_{z_1\in\mathbb{F}_p^\star}\epsilon_p^{-\lambda z_1}\left(\sum_{x,y\in\mathbb{F}_q}\epsilon_p^{z_1\mathrm{Tr}(yx^{d+1})}\right)\\
&= \sum_{z_1\in\mathbb{F}_p^\star}\epsilon_p^{-\lambda z_1}\left(\sum_{x\in\mathbb{F}_q^\star}\sum_{y\in\mathbb{F}_q}\epsilon_p^{\mathrm{Tr}(z_1yx^{d+1})}+p^m\right)\\
&= p^m\sum_{z_1\in\mathbb{F}_p^\star}\epsilon_p^{-\lambda z_1}=\begin{cases}(p-1)p^m, & \textit{if } \lambda=0,\\ -p^m, & \textit{if } \lambda\neq 0.\end{cases}
\end{aligned} \tag{9}$$

There are two cases for Ω_1. When $a=0\wedge b\neq 0\wedge c\in\mathbb{F}_p$, we have

$$\Omega_1=\sum_{z_2\in\mathbb{F}_p^\star}\left(\sum_{x,y\in\mathbb{F}_q}\epsilon_p^{z_2(\mathrm{Tr}(bx)+c)}\right)=\sum_{z_2\in\mathbb{F}_p^\star}\epsilon_p^{z_2c}\sum_{y\in\mathbb{F}_q}\left(\sum_{x\in\mathbb{F}_q}\epsilon_p^{\mathrm{Tr}(z_2bx)}\right)=0$$

When $a \neq 0 \wedge b \in \mathbb{F}_q \wedge c \in \mathbb{F}_p$, we have

$$\begin{aligned}
\Omega_1 &= \sum_{z_2 \in \mathbb{F}_p^\star} \left(\sum_{x,y \in \mathbb{F}_q} \epsilon_p^{z_2(\mathrm{Tr}(ax^d y+bx)+c)} \right) \\
&= \sum_{z_2 \in \mathbb{F}_p^\star} \epsilon_p^{z_2 c} \left(\sum_{x \in \mathbb{F}_q^\star} \sum_{y \in \mathbb{F}_q} \epsilon_p^{z_2 \mathrm{Tr}(ax^d y+bx)} + p^m \right) \\
&= p^m \sum_{z_2 \in \mathbb{F}_p^\star} \epsilon_p^{z_2 c} + \sum_{z_2 \in \mathbb{F}_p^\star} \epsilon_p^{z_2 c} \left(\sum_{x \in \mathbb{F}_q^\star} \sum_{y \in \mathbb{F}_q} \epsilon_p^{z_2 \mathrm{Tr}(ax^d y+bx)} \right) \\
&= p^m \sum_{z_2 \in \mathbb{F}_p^\star} \epsilon_p^{z_2 c} + \sum_{z_2 \in \mathbb{F}_p^\star} \epsilon_p^{z_2 c} \sum_{x \in \mathbb{F}_q^\star} \epsilon_p^{\mathrm{Tr}(z_2 bx)} \left(\sum_{y \in \mathbb{F}_q} \epsilon_p^{\mathrm{Tr}(z_2 ax^d y)} \right) \\
&= \begin{cases} (p-1)p^m, & \textit{if } c = 0, \\ -p^m, & \textit{if } c \neq 0. \end{cases}
\end{aligned}$$

To calculate Ω_2, we first verify the following equation

$$\begin{aligned}
\Omega_2 &= \sum_{z_1, z_2 \in \mathbb{F}_p^\star} \left(\sum_{x,y \in \mathbb{F}_q} \epsilon_p^{z_1(\mathrm{Tr}(yx^{d+1})-\lambda)+z_2(\mathrm{Tr}(ayx^d+bx)+c)} \right) \\
&= \sum_{z_1, z_2 \in \mathbb{F}_p^\star} \epsilon_p^{cz_2-\lambda z_1} \left(\sum_{x,y \in \mathbb{F}_q} \epsilon_p^{\mathrm{Tr}(z_1 yx^{d+1})+\mathrm{Tr}(z_2 ayx^d+z_2 bx)} \right) \\
&= \sum_{z_1, z_2 \in \mathbb{F}_p^\star} \epsilon_p^{cz_2-\lambda z_1} \sum_{x \in \mathbb{F}_q} \epsilon_p^{\mathrm{Tr}(z_2 bx)} \left(\sum_{y \in \mathbb{F}_q} \epsilon_p^{\mathrm{Tr}(z_1 yx^{d+1}+z_2 ayx^d)} \right) \\
&= p^m \sum_{z_1, z_2 \in \mathbb{F}_p^\star} \epsilon_p^{cz_2-\lambda z_1} + \sum_{z_1, z_2 \in \mathbb{F}_p^\star} \epsilon_p^{cz_2-\lambda z_1} \sum_{x \in \mathbb{F}_q^\star} \epsilon_p^{\mathrm{Tr}(z_2 bx)} \left(\sum_{y \in \mathbb{F}_q} \epsilon_p^{\mathrm{Tr}(z_1 yx^{d+1}+z_2 ayx^d)} \right).
\end{aligned}$$

There are four cases for Ω_2. Case 1: when $a = 0 \wedge b \neq 0 \wedge c \neq 0$, we have

$$\begin{aligned}
\Omega_2 &= p^m \sum_{z_1 \in \mathbb{F}_p^\star} \epsilon_p^{-\lambda z_1} \sum_{z_2 \in \mathbb{F}_p^\star} \epsilon_p^{cz_2} + \sum_{z_1, z_2 \in \mathbb{F}_p^\star} \epsilon_p^{cz_2-\lambda z_1} \sum_{x \in \mathbb{F}_q^\star} \epsilon_p^{\mathrm{Tr}(z_2 bx)} \left(\sum_{y \in \mathbb{F}_q} \epsilon_p^{\mathrm{Tr}(z_1 yx^{d+1})} \right) \\
&= \begin{cases} -(p-1)p^m, & \textit{if } \lambda = 0, \\ p^m, & \textit{if } \lambda \neq 0. \end{cases}
\end{aligned}$$

Case 2: when $a = 0 \wedge b \neq 0 \wedge c = 0$, we have

$$\begin{aligned}\Omega_2 &= p^m \sum_{z_2 \in \mathbb{F}_p^\star} \sum_{z_1 \in \mathbb{F}_p^\star} \epsilon_p^{-\lambda z_1} + \sum_{z_1 \in \mathbb{F}_p^\star} \epsilon_p^{-\lambda z_1} \sum_{z_2 \in \mathbb{F}_p^\star} \sum_{x \in \mathbb{F}_q^\star} \epsilon_p^{\mathrm{Tr}(z_2 bx)} \left(\sum_{y \in \mathbb{F}_q} \epsilon_p^{\mathrm{Tr}(z_1 y x^{d+1})} \right) \\ &= \begin{cases} (p-1)^2 p^m, & \textit{if } \lambda = 0, \\ -(p-1)p^m, & \textit{if } \lambda \neq 0. \end{cases}\end{aligned}$$

Case 3: when $a \neq 0 \wedge b \in \mathbb{F}_q \wedge c \neq 0$, we have

$$\begin{aligned}\Omega_2 &= p^m \sum_{z_1, z_2 \in \mathbb{F}_p^\star} \epsilon_p^{cz_2 - \lambda z_1} + \sum_{z_1, z_2 \in \mathbb{F}_p^\star} \epsilon_p^{cz_2 - \lambda z_1} \sum_{x \in \mathbb{F}_q^\star} \epsilon_p^{\mathrm{Tr}(z_2 bx)} \left(\sum_{y \in \mathbb{F}_q} \epsilon_p^{\mathrm{Tr}((z_1 x + z_2 a) y x^d)} \right) \\ &= p^m \sum_{z_1, z_2 \in \mathbb{F}_p^\star} \epsilon_p^{cz_2 - \lambda z_1} + \sum_{z_1, z_2 \in \mathbb{F}_p^\star} \epsilon_p^{cz_2 - \lambda z_1} \sum_{z_1 x + z_2 a = 0} \epsilon_p^{\mathrm{Tr}(z_2 bx)} p^m \\ &= p^m \sum_{z_1, z_2 \in \mathbb{F}_p^\star} \epsilon_p^{cz_2 - \lambda z_1} + p^m \sum_{z_1, z_2 \in \mathbb{F}_p^\star} \epsilon_p^{cz_2 - \lambda z_1} \epsilon_p^{-z_1^{-1} z_2^2 \mathrm{Tr}(ab)}.\end{aligned} \tag{10}$$

If $\mathrm{Tr}(ab) = 0$, then

$$\Omega_2 = 2p^m \sum_{z_1 \in \mathbb{F}_p^\star} \epsilon_p^{-\lambda z_1} \sum_{z_2 \in \mathbb{F}_p^\star} \epsilon_p^{cz_2} = \begin{cases} -2(p-1)p^m, & \textit{if } \lambda = 0, \\ 2p^m, & \textit{if } \lambda \neq 0. \end{cases}$$

If $\mathrm{Tr}(ab) \neq 0$, then

$$\begin{aligned}\Omega_2 &= p^m \sum_{z_1, z_2 \in \mathbb{F}_p^\star} \epsilon_p^{cz_2 - \lambda z_1} + p^m \sum_{z_1, z_2 \in \mathbb{F}_p^\star} \epsilon_p^{cz_2 - \lambda z_1} \epsilon_p^{-z_1^{-1} z_2^2 \mathrm{Tr}(ab)} \\ &= p^m \sum_{z_1, z_2 \in \mathbb{F}_p^\star} \epsilon_p^{cz_2 - \lambda z_1} + p^m \sum_{z_1 \in \mathbb{F}_p^\star} \epsilon_p^{-\lambda z_1} \sum_{z_2 \in \mathbb{F}_p^\star} \epsilon_p^{-z_1^{-1} \mathrm{Tr}(ab) z_2^2 + cz_2} \\ &= p^m \sum_{z_1, z_2 \in \mathbb{F}_p^\star} \epsilon_p^{cz_2 - \lambda z_1} + p^m \sum_{z_1 \in \mathbb{F}_p^\star} \epsilon_p^{-\lambda z_1} \left(\eta_1(-\mathrm{Tr}(ab) z_1^{-1}) G_1 \epsilon_p^{z_1 c^2 (4\mathrm{Tr}(ab))^{-1}} - 1 \right) \\ &= p^m \sum_{z_1, z_2 \in \mathbb{F}_p^\star} \epsilon_p^{cz_2 - \lambda z_1} - p^m \sum_{z_1 \in \mathbb{F}_p^\star} \epsilon_p^{-\lambda z_1} + p^m G_1 \eta_1(-1) \sum_{z_1 \in \mathbb{F}_p^\star} \eta_1 \left(\frac{z_1}{4\mathrm{Tr}(ab)} \right) \epsilon_p^{z_1 c^2 (4\mathrm{Tr}(ab))^{-1} - \lambda z_1} \\ &= p^m \sum_{z_1, z_2 \in \mathbb{F}_p^\star} \epsilon_p^{cz_2 - \lambda z_1} - p^m \sum_{z_1 \in \mathbb{F}_p^\star} \epsilon_p^{-\lambda z_1} + p^m G_1 \eta_1(-1) \sum_{z_1 \in \mathbb{F}_p^\star} \eta_1 \left(\frac{z_1}{4\mathrm{Tr}(ab)} \right) \epsilon_p^{\frac{z_1}{4\mathrm{Tr}(ab)} \left(c^2 - 4\lambda \mathrm{Tr}(ab) \right)} \\ &= \begin{cases} (2-p)p^m, & \textit{if } \lambda = 0, \\ 2p^m, & \textit{if } \lambda \neq 0 \textit{ and } c^2 - 4\lambda \mathrm{Tr}(ab) = 0, \\ (2+p)p^m, & \textit{if } \lambda \neq 0 \textit{ and } c^2 - 4\lambda \mathrm{Tr}(ab) \in SQ, \\ (2-p)p^m, & \textit{if } \lambda \neq 0 \textit{ and } c^2 - 4\lambda \mathrm{Tr}(ab) \in NSQ. \end{cases}\end{aligned} \tag{11}$$

Case 4: when $a \neq 0 \wedge b \in \mathbb{F}_q \wedge c = 0$, we have the following two cases. If $\mathrm{Tr}(ab) = 0$, then from (10) we have

$$\Omega_2 = 2p^m \sum_{z_1 \in \mathbb{F}_p^\star} \epsilon_p^{-\lambda z_1} = \begin{cases} 2(p-1)^2 p^m, & \textit{if } \lambda = 0, \\ -2(p-1)p^m, & \textit{if } \lambda \neq 0. \end{cases}$$

If $\mathrm{Tr}(ab) \neq 0$, then the results are deduced from (11) and Lemma 1.

$$\begin{aligned} \Omega_2 &= p^m \sum_{z_1, z_2 \in \mathbb{F}_p^\star} \epsilon_p^{-\lambda z_1} - p^m \sum_{z_1 \in \mathbb{F}_p^\star} \epsilon_p^{-\lambda z_1} + p^m G_1 \eta_1(-1) \sum_{z_1 \in \mathbb{F}_p^\star} \eta_1 \left(\frac{z_1}{4\mathrm{Tr}(ab)} \right) \epsilon_p^{\frac{z_1}{4\mathrm{Tr}(ab)}(-4\lambda \mathrm{Tr}(ab))} \\ &= \begin{cases} (p-2)(p-1)p^m, & \textit{if } \lambda = 0, \\ 2p^m, & \textit{if } \lambda \neq 0 \textit{ and } -4\lambda \mathrm{Tr}(ab) \in SQ. \\ -2(p-1)p^m, & \textit{if } \lambda \neq 0 \textit{ and } -4\lambda \mathrm{Tr}(ab) \in NSQ. \end{cases} \end{aligned}$$

Hence, the desired results are derived from $\#N(a,b,c) = p^{2m-2} + \frac{1}{p^2}(\Omega_0 + \Omega_1 + \Omega_2)$ for each case. This completes the proof. □

The following lemma is used to find the weight distributions in codes.

Lemma 12. *For $t \in \mathbb{F}_p$, define the set*

$$S = \left\{ (a,b) \in \mathbb{F}_{p^m}^\star \times \mathbb{F}_{p^m} \mid \mathrm{Tr}(ab) = t \right\}.$$

Then, $\#S = p^{m-1}(p^m - 1)$.

We collect the parameters of the code $\overline{\mathcal{C}_{D_0}}$ in the following theorem.

Theorem 1. *Let m be an integer with $m \geq 2$. For $\lambda = 0$, let D_0 be the set defined in (2). Let $\overline{\mathcal{C}_{D_0}}$ be a linear code over $\mathbb{F}_p$ defined in (3). Then, the code $\overline{\mathcal{C}_{D_0}}$ has parameters $[p^{2m-1} + (p-1)p^{m-1}, 2m+1, (p-1)(p^{2m-2} - p^{m-1})]_p$ with the Hamming weights listed in Table 1. Besides, the code $\overline{\mathcal{C}_{D_0}}$ is five-weight self-orthogonal code over $\mathbb{F}_p$. The dual code $\overline{\mathcal{C}_{D_0}}^\perp$ has parameters $[p^{2m-1} + (p-1)p^{m-1}, p^{2m-1} + (p-1)p^{m-1} - 2m - 1, 2]_p$.*

Table 1 The Hamming weights in $\overline{\mathcal{C}_{D_0}}$, where $A = (p-1)(p^m - 1)p^{m-1}$

Hamming weight w	Multiplicity A_w
0	1
$p^{2m-1} + (p-1)p^{m-1}$	$(p-1)$
$(p-1)p^{2m-2}$	$p^m - 1 + A$
$(p-1)(p^{2m-2} + p^{m-1})$	$(p-1)(p^m - 1 + A)$
$(p-1)(p^{2m-2} - p^{m-1})$	$(p^m - 1)p^{m-1}$
$(p-1)p^{2m-2} + p^m$	A

Proof. From the definition of the code $\overline{\mathcal{C}_{D_0}}$, its length is the size of its defining set D_0 and the Hamming weight of each codeword $\mathbf{c}_{(a,b,c)}$ in $\overline{\mathcal{C}_{D_0}}$ is

$$wt(\mathbf{c}_{(a,b,c)}) = n - \#N_0(a,b,c). \tag{12}$$

Thus, the length follows from Lemma 10, and every Hamming weight follows from Lemmas 10 and 11. Explicitly, the Hamming weights $wt(\mathbf{c}_{(a,b,c)})$ are given as

$$\begin{cases} p^{2m-1} + (p-1)p^{m-1}, & \textit{if } a = 0 \wedge b = 0 \wedge c \neq 0, \\ p^{2m-1} - p^{2m-2}, & \textit{if } a = 0 \wedge b \neq 0 \wedge c = 0, \\ & \textit{or } a \neq 0 \wedge b \in \mathbb{F}_q \wedge c = 0 \wedge \mathrm{Tr}(ab) \neq 0, \\ p^{2m-1} - p^{2m-2} + (p-1)p^{m-1}, & \textit{if } a = 0 \wedge b \neq 0 \wedge c \neq 0, \\ & \textit{or } a \neq 0 \wedge b \in \mathbb{F}_q \wedge c \neq 0 \wedge \mathrm{Tr}(ab) \neq 0, \\ p^{2m-1} - p^{2m-2} - (p-1)p^{m-1}, & \textit{if } a \neq 0 \wedge b \in \mathbb{F}_q \wedge c = 0 \wedge \mathrm{Tr}(ab) = 0 \\ p^{2m-1} - p^{2m-2} + p^m, & \textit{if } a \neq 0 \wedge b \in \mathbb{F}_q \wedge c \neq 0 \wedge \mathrm{Tr}(ab) = 0. \end{cases}$$

The weight distribution of each Hamming weight can be determined with the help of Lemma 12. Besides, since the vector $\mathbf{1} \in \overline{\mathcal{C}_{D_0}}$ and the code $\overline{\mathcal{C}_{D_0}}$ is p-divisible for $m \geq 2$, it is self-orthogonal code due to Lemma 7. From the second Pless power moment, one can easily observe that $A_2^{\perp} > 0$, which approves that the dual distance $d^{\perp} = 2$. This completes the proof. □

We collect the parameters of the code $\overline{\mathcal{C}_{D_\lambda}}$ in the following theorem.

Theorem 2. *Let m be an integer with $m \geq 2$. For $\lambda \in \mathbb{F}_p^{\star}$, let D_λ be the set defined in (2). Let $\overline{\mathcal{C}_{D_\lambda}}$ be a linear code over $\mathbb{F}_p$ defined in (3). Then, the code $\overline{\mathcal{C}_{D_\lambda}}$ has parameters $[p^{2m-1} - p^{m-1}, 2m+1, (p-1)p^{2m-2} - 2p^{m-1}]_p$ with the Hamming weights listed in Table 2. Moreover, the code $\overline{\mathcal{C}_{D_\lambda}}$ is four-weight self-orthogonal code over $\mathbb{F}_p$. The dual code $\overline{\mathcal{C}_{D_\lambda}}^{\perp}$ has parameters $[p^{2m-1} - p^{m-1}, p^{2m-1} - p^{m-1} - 2m - 1, 2]_p$.*

Table 2 The Hamming weights in $\overline{\mathcal{C}_{D_\lambda}}$

Hamming weight w	Multiplicity A_w
0	1
$p^{2m-1} - p^{m-1}$	$(p-1)$
$(p-1)p^{2m-2}$	$(p^m - 1)(1 + p^{m-1} + p^m(\frac{p-1}{2}))$
$(p-1)p^{2m-2} - p^{m-1}$	$(p^m - 1)(p-1)(1 + p^{m-1})$
$(p-1)p^{2m-2} - 2p^{m-1}$	$p^m(p^m - 1)(\frac{p-1}{2})$

Proof. From the definition of the code $\overline{\mathcal{C}_{D_\lambda}}$, its length is the size of its defining set D_λ and the Hamming weight of each codeword $\mathbf{c}_{(a,b,c)}$ in $\overline{\mathcal{C}_{D_\lambda}}$ is

$$wt(\mathbf{c}_{(a,b,c)}) = n - \#N_\lambda(a,b,c).$$

Thus, the length follows from Lemma 10, and every Hamming weight follows from Lemmas 10 and 11. Explicitly, the Hamming weights $wt(\mathbf{c}_{(a,b,c)})$ are given as

$$\begin{cases} p^{2m-1}-p^{m-1}, & \textit{if } a=0\wedge b=0\wedge c\neq 0,\\ (p-1)p^{2m-2}, & \textit{if } a=0\wedge b\neq 0\wedge c=0,\\ & \textit{or } a\neq 0\wedge b\in\mathbb{F}_q\wedge c=0\wedge \mathrm{Tr}(ab)=0\\ & \textit{or } a\neq 0\wedge b\in\mathbb{F}_q\wedge c\in\mathbb{F}_p\wedge \mathrm{Tr}(ab)\neq 0\wedge k\in NSQ\\ (p-1)p^{2m-2}-p^{m-1}, & \textit{if } a=0\wedge b\neq 0\wedge c\neq 0,\\ & \textit{or } a\neq 0\wedge b\in\mathbb{F}_q\wedge c\neq 0\wedge \mathrm{Tr}(ab)=0\\ (p-1)p^{2m-2}-2p^{m-1}, & \textit{if } a\neq 0\wedge b\in\mathbb{F}_q\wedge c\in\mathbb{F}_p\wedge \mathrm{Tr}(ab)\neq 0\wedge k\in SQ \end{cases}$$

where $k=c^2-4\lambda\mathrm{Tr}(ab)$. The weight distribution of each Hamming weight can be determined with the help of Lemma 12. Besides, since the vector $\mathbf{1}\in\overline{\mathcal{C}_{D_\lambda}}$ and the code $\overline{\mathcal{C}_{D_\lambda}}$ is p-divisible for $m\geq 2$, it is self-orthogonal code due to Lemma 7. From the second Pless power moment, one can easily observe that $A_2^\perp>0$, which approves that the dual distance $d^\perp=2$. The proof is complete. □

4 Constructions of self-orthogonal codes from the first generic construction

In this section, we construct new classes of self-orthogonal codes and LCD codes over the odd characteristic finite fields in the first generic construction method.

4.1 On the first generic construction of linear codes from functions

In this subsection, we review the first generic construction method for linear codes involving special functions.

The first generic construction is obtained by considering a code $\mathcal{C}(h)$ over $\mathbb{F}_p$ involving a mapping h from $\mathbb{F}_q$ to $\mathbb{F}_q$ (where $q=p^t$) defined by

$$\mathcal{C}(h):=\{\tilde{c}=(\mathrm{Tr}_p^q(ah(x)+bx))_{x\in\mathbb{F}_q^*}:a,b\in\mathbb{F}_q\}.$$

The code $\mathcal{C}(h)$ from h is a linear code of length $(q-1)$ and its dimension is upper bounded by $2t$. For any $a,b\in\mathbb{F}_{q^m}$, we define a function

$$\begin{aligned} f_{a,b}\,:\,\mathbb{F}_{q^m} &\longrightarrow \mathbb{F}_q\\ x &\longmapsto f_{a,b}(x):=\mathrm{Tr}_q^{q^m}(a\Psi(x)-bx), \end{aligned}$$

where Ψ is a mapping from $\mathbb{F}_{q^m}$ to $\mathbb{F}_{q^m}$ such that $\Psi(0)=0$. Then a linear code $\mathcal{C}_\Psi$ over $\mathbb{F}_q$ is defined as

$$\mathcal{C}_\Psi:=\{\mathbf{c}_{(a,b)}=(f_{a,b}(\zeta_1),f_{a,b}(\zeta_2),\ldots,f_{a,b}(\zeta_{q^m-1}))\,:\,a,b\in\mathbb{F}_{q^m}\},$$

where $\zeta_1,\ldots,\zeta_{q^m-1}$ are the elements of $\mathbb{F}_{q^m}^\star$ and $\mathbf{c}_{(a,b)}$ denotes a codeword of $\mathcal{C}_\Psi$. The linear code $\mathcal{C}_\Psi$ of length q^m-1 is an $(2m)$-dimensional subspace of $\mathbb{F}_q^m$ over $\mathbb{F}_q$, and denoted by $[q^m-1,2m]_q$. To get a subclass of the class of the linear code $\mathcal{C}_\Psi$, one can assume that $t=1$ and $a\in\mathbb{F}_p$. Let

$$f(x)=\mathrm{Tr}_p^{p^m}(\Psi(x)) \tag{13}$$

be a p-ary function such that $\Psi:\mathbb{F}_{p^m}\to\mathbb{F}_{p^m}$ is a mapping with $\Psi(0)=0$. From now on, let $f:\mathbb{F}_{p^m}\to\mathbb{F}_p$ be a p-ary function with $f(0)=0$. Define a subcode $\mathcal{C}_f^*$ of the code $\mathcal{C}_\Psi$ as follows:

$$\mathcal{C}_f^*=\{\mathbf{c}_{(a,b)}=\left(af(x)-\mathrm{Tr}_p^{p^m}(bx)\right)_{x\in\mathbb{F}_{p^m}^\star}\ :\ a\in\mathbb{F}_p \text{ and } b\in\mathbb{F}_{p^m}\}. \tag{14}$$

The linear code $\mathcal{C}_f^*$ of length p^m-1 is an $(m+1)$-dimensional subspace of $\mathbb{F}_p^m$ over $\mathbb{F}_p$, and denoted by $[p^m-1,m+1]_p$. Moreover, for $f(0)\neq 0$, one can define an extended code $\mathcal{C}_f$ of the code $\mathcal{C}_f^*$

$$\mathcal{C}_f=\{\mathbf{c}_{(a,b)}=\left(af(x)-\mathrm{Tr}_p^{p^m}(bx)\right)_{x\in\mathbb{F}_{p^m}}\ :\ a\in\mathbb{F}_p \text{ and } b\in\mathbb{F}_{p^m}\}. \tag{15}$$

The linear code $\mathcal{C}_f$ of length p^m is an $(m+1)$-dimensional subspace of $\mathbb{F}_p^m$ over $\mathbb{F}_p$, and denoted by $[p^m,m+1]_p$. The *augmented code* of the code $\mathcal{C}_f$ is defined as

$$\overline{\mathcal{C}_f}=\{\mathbf{c}_{(a,b,c)}=\left(af(x)-\mathrm{Tr}_p^{p^m}(bx)+c\right)_{x\in\mathbb{F}_{p^m}}\ :\ a\in\mathbb{F}_p, b\in\mathbb{F}_{p^m}, c\in\mathbb{F}_p\}. \tag{16}$$

The length of the augmented code $\overline{\mathcal{C}_f}$ is the same as that of the original code $\mathcal{C}_f$. Note that the augmented code $\overline{\mathcal{C}_f}$ has larger dimension than that of $\mathcal{C}_f$ since $\mathbf{1}\notin\mathcal{C}_f$. Thus, the augmented code $\overline{\mathcal{C}_f}$ is $(m+2)$-dimensional subspace of $\mathbb{F}_p^m$ over $\mathbb{F}_p$ and denoted by $[p^m,m+2]_p$.

The code $\mathcal{C}_f^*$ defined in (14) has been studied in [12] and [15] for weakly regular bent and plateaued function f, respectively. Very recently, the augmented code $\overline{\mathcal{C}_f}$ defined in (16) has been studied in [14] for weakly regular bent function f. In this paper, we study the augmented code $\overline{\mathcal{C}_f}$ for weakly regular plateaued functions and construct self-orthogonal codes, LCD codes and LRC codes.

The Hamming weights in $\mathcal{C}_f^*$ are presented in [12, 15] in the following propositions.

Proposition 1. *[12] Let $\mathcal{C}_f^*$ be the code defined in (14). For $a\in\mathbb{F}_p$ and $b\in\mathbb{F}_{p^m}$, the codewords $\mathbf{c}_{(a,b)}\in\mathcal{C}_f^*$ have the following Hamming weights.*

- *If $a=0$, we have $wt(\tilde{c}_{0,0})=0$ and $wt(\tilde{c}_{0,b})=p^m-p^{m-1}$ for all $b\in\mathbb{F}_{p^m}^\star$.*
- *If $a\in\mathbb{F}_p^\star$ and $b\in\mathbb{F}_{p^m}$, we have*

$$wt(\mathbf{c}_{(a,b)})=p^m-p^{m-1}-\frac{1}{p}\sum_{\omega\in\mathbb{F}_p^\star}\sigma_\omega\left(\sigma_a(\mathcal{W}_f(a^{-1}b))\right), \tag{17}$$

where σ_a is the automorphism of the cyclotomic field $\mathbb{Q}(\xi_p)$ for $a\in\mathbb{F}_p^\star$.

The following proposition calculates the Hamming weights in (17) for a weakly regular plateaued (and also bent) function f.

Proposition 2. *[15] Let f be weakly regular s-plateaued with $f(0)=0$ for $0 \leq s \leq m-2$. Let $\epsilon_f = \pm 1$ be the sign of $\mathcal{W}_f$ and $f^\star$ be a p-ary function of $\mathcal{W}_f$ over $\mathcal{S}_f$. Let $\mathcal{C}_f^*$ be defined in (14). For $a \in \mathbb{F}_p^\star$ and $b \in \mathbb{F}_{p^m}$,*

- *if $a^{-1}b \notin \mathcal{S}_f$, then we get $wt(\mathbf{c}_{(a,b)}) = p^m - p^{m-1}$,*
- *if $a^{-1}b \in \mathcal{S}_f$, when $m+s$ is even,*

$$wt(\mathbf{c}_{(a,b)}) = \begin{cases} p^m - p^{m-1} - \epsilon_f \frac{(p-1)}{p} \sqrt{p^*}^{m+s}, & \text{if } f^\star(a^{-1}b) = 0, \\ p^m - p^{m-1} + \epsilon_f \frac{1}{p} \sqrt{p^*}^{m+s}, & \text{if } f^\star(a^{-1}b) \in \mathbb{F}_p^\star, \end{cases}$$

when $m+s$ is odd,

$$wt(\mathbf{c}_{(a,b)}) = \begin{cases} p^m - p^{m-1}, & \text{if } f^\star(a^{-1}b) = 0, \\ p^m - p^{m-1} - \epsilon_f \frac{1}{p} \sqrt{p^*}^{m+s+1}, & \text{if } f^\star(a^{-1}b) \in SQ, \\ p^m - p^{m-1} + \epsilon_f \frac{1}{p} \sqrt{p^*}^{m+s+1}, & \text{if } f^\star(a^{-1}b) \in NSQ. \end{cases}$$

4.2 Construction of self-orthogonal codes

In this subsection, we deal with the augmented code $\overline{\mathcal{C}_f}$ for weakly regular plateaued functions and propose self-orthogonal codes.

We first need the following lemma to find Hamming weights in the augmented code.

Lemma 13. *Let $f : \mathbb{F}_{p^m} \to \mathbb{F}_p$ be an s-plateaued function. For $a \in \mathbb{F}_p, b \in \mathbb{F}_{p^m}$, $c \in \mathbb{F}_p^\star$, define*

$$N_f(a,b,c) := \#\{x \in \mathbb{F}_{p^m} : af(x) - \mathrm{Tr}_p^{p^m}(bx) + c = 0\}.$$

- *When $a=0$, we have $N_f(0,0,c) = 0$ and $N_f(0,b,c) = p^{m-1}$ for every $b \in \mathbb{F}_{p^m}^\star$.*
- *When $a \neq 0$, we have $N_f(a,b,c) = p^{m-1}$ for every $a^{-1}b \in \mathbb{F}_{p^m} \setminus \mathcal{S}_f$, and for every $a^{-1}b \in \mathcal{S}_f$,*
  - *if $m+s$ is even,*

$$N_f(a,b,c) = \begin{cases} p^{m-1} + \epsilon_f \frac{(p-1)}{p} \sqrt{p^*}^{m+s}, & \text{if } f^\star(a^{-1}b) + ca^{-1} = 0, \\ p^{m-1} - \epsilon_f \frac{1}{p} \sqrt{p^*}^{m+s}, & \text{if } f^\star(a^{-1}b) + ca^{-1} \neq 0 \end{cases}$$

  - *if $m+s$ is odd,*

$$N_f(a,b,c) = \begin{cases} p^{m-1}, & \text{if } f^\star(a^{-1}b) + ca^{-1} = 0, \\ p^{m-1} + \epsilon_f \frac{1}{p} \sqrt{p^*}^{m+s+1}, & \text{if } \eta_0(f^\star(a^{-1}b) + ca^{-1}) = 1, \\ p^{m-1} - \epsilon_f \frac{1}{p} \sqrt{p^*}^{m+s+1}, & \text{if } \eta_0(f^\star(a^{-1}b) + ca^{-1}) = -1. \end{cases}$$

Proof. For $a \in \mathbb{F}_p, b \in \mathbb{F}_{p^m}$ and $c \in \mathbb{F}_p^\star$, by the definition of $N_f(a,b,c)$, we have

$$\begin{aligned} N_f(a,b,c) &= \tfrac{1}{p} \sum_{y \in \mathbb{F}_p} \sum_{x \in \mathbb{F}_{p^m}} \xi_p^{y\left(af(x) - \mathrm{Tr}_p^{p^m}(bx) + c\right)} \\ &= p^{m-1} + \tfrac{1}{p} \sum_{y \in \mathbb{F}_p^\star} \xi_p^{yc} \sum_{x \in \mathbb{F}_{p^m}} \xi_p^{y\left(af(x) - \mathrm{Tr}_p^{p^m}(bx)\right)}. \end{aligned}$$

We consider the following cases: For $a = 0$, we have by Lemma 1 (*ii*)

$$N_f(a,b,c) = p^{m-1} + \tfrac{1}{p} \sum_{y \in \mathbb{F}_p^\star} \xi_p^{yc} \sum_{x \in \mathbb{F}_{p^m}} \xi_p^{-\mathrm{Tr}_p^{p^m}(ybx)} = \begin{cases} p^{m-1}, & \text{if } b \neq 0, \\ 0, & \text{if } b = 0. \end{cases}$$

For $a \neq 0$, we have

$$\begin{aligned} N_f(a,b,c) &= p^{m-1} + \tfrac{1}{p} \sum_{y \in \mathbb{F}_p^\star} \xi_p^{yc} \sum_{x \in \mathbb{F}_{p^m}} \xi_p^{ya\left(f(x) - \mathrm{Tr}_p^{p^m}(a^{-1}bx)\right)} \\ &= p^{m-1} + \tfrac{1}{p} \sum_{y \in \mathbb{F}_p^\star} \xi_p^{yc} \sigma_{ya}(\mathcal{W}_f(a^{-1}b)) \\ &= p^{m-1} + \tfrac{1}{p} \sum_{y \in \mathbb{F}_p^\star} \xi_p^{yca^{-1}} \sigma_y(\mathcal{W}_f(a^{-1}b)), \end{aligned}$$

where σ_y is the automorphism of $\mathbb{Q}(\xi_p)$ defined as $\sigma_y(\xi_p) = \xi_p^y$. Since f is weakly regular plateaued function, we have the following two cases:

- If $a^{-1}b \notin \mathcal{S}_f$, then $N_f(a,b,c) = p^{m-1}$.
- If $a^{-1}b \in \mathcal{S}_f$, since

$$\sigma_y(\mathcal{W}_f(a^{-1}b)) = \sigma_y(\epsilon_f \sqrt{p^*}^{m+s} \xi_p^{f^\star(b)}) = \epsilon_f \eta_0^{m+s}(y) \sqrt{p^*}^{m+s} \xi_p^{yf^\star(a^{-1}b)},$$

we have

$$\begin{aligned} N_f(a,b,c) &= p^{m-1} + \tfrac{1}{p} \sum_{y \in \mathbb{F}_p^\star} \xi_p^{yca^{-1}} \sigma_y(\mathcal{W}_f(a^{-1}b)) \\ &= p^{m-1} + \tfrac{1}{p} \sum_{y \in \mathbb{F}_p^\star} \xi_p^{yca^{-1}} \epsilon_f \eta_0^{m+s}(y) \sqrt{p^*}^{m+s} \xi_p^{yf^\star(a^{-1}b)} \\ &= p^{m-1} + \epsilon_f \sqrt{p^*}^{m+s} \tfrac{1}{p} \sum_{y \in \mathbb{F}_p^\star} \eta_0^{m+s}(y) \xi_p^{y(f^\star(a^{-1}b) + ca^{-1})}. \end{aligned}$$

We deal with it for $m+s$ even and odd.

– When $m+s$ is even, by Lemma 1 (*ii*),

$$N_f(a,b,c) = \begin{cases} p^{m-1} + \epsilon_f \frac{(p-1)}{p} \sqrt{p^*}^{m+s}, & \text{if } f^\star(a^{-1}b) + ca^{-1} = 0, \\ p^{m-1} - \epsilon_f \frac{1}{p} \sqrt{p^*}^{m+s}, & \text{if } f^\star(a^{-1}b) + ca^{-1} \neq 0. \end{cases}$$

– When $m+s$ is odd, by Lemma 1 (i) and (iii),

$$\begin{aligned} N_f(a,b,c) &= p^{m-1} + \epsilon_f \sqrt{p^*}^{m+s} \tfrac{1}{p} \sum_{y \in \mathbb{F}_p^\star} \eta_0(y) \xi_p^{y(f^\star(a^{-1}b)+ca^{-1})} \\ &= \begin{cases} p^{m-1}, & \text{if } f^\star(a^{-1}b)+ca^{-1}=0, \\ p^{m-1} + \epsilon_f \frac{1}{p}\sqrt{p^*}^{m+s+1}, & \text{if } \eta_0(f^\star(a^{-1}b)+ca^{-1})=1, \\ p^{m-1} - \epsilon_f \frac{1}{p}\sqrt{p^*}^{m+s+1}, & \text{if } \eta_0(f^\star(a^{-1}b)+ca^{-1})=-1. \end{cases} \end{aligned}$$

Hence, the proof is complete. □

Remark 1. *In the construction of* (16)*, when $c=0$, the augmented code $\overline{\mathcal{C}_f}$ corresponds to the extension code $\mathcal{C}_f$ in* (15) *of the original code $\mathcal{C}_f^*$ in* (14)*. Since the Hamming weights in $\mathcal{C}_f$ are the same as the Hamming weights in $\mathcal{C}_f^*$, then the Hamming weights $wt(\mathbf{c}_{(a,b,0)})$ in the augmented code $\overline{\mathcal{C}_f}$ are the same as the Hamming weights $wt(\mathbf{c}_{(a,b)})$ in $\mathcal{C}_f^*$ when $c=0$.*

We collect the parameters of the augmented code $\overline{\mathcal{C}_f}$ in the following theorem.

Theorem 3. *Let $m+s$ be an integer with $0 \le s \le m-2$. Let f be a weakly regular p-ary s-plateaued function with $f(0)=0$. Let $\overline{\mathcal{C}_f}$ defined in* (16) *be a linear $[p^m, m+2]_p$ code over $\mathbb{F}_p$. Then, the $\overline{\mathcal{C}_f}$ is a four-weight self-orthogonal code with the Hamming weights listed in Tables* 3 *and* 4 *when $m+s$ is even and odd, respectively.*

Table 3 The Hamming weights in $\overline{\mathcal{C}_f}$ when $m+s$ is even

Hamming weight w	Multiplicity A_w
0	1
p^m	$p-1$
$(p-1)p^{m-1}$	$p(p^m-1+(p-1)(p^m-p^{m-s}))$
$(p-1)(p^{m-1}-\epsilon_f \frac{1}{p}\sqrt{p^*}^{m+s})$	$(p-1)p^{m-s}$
$(p-1)p^{m-1}+\epsilon_f \frac{1}{p}\sqrt{p^*}^{m+s}$	$(p-1)^2 p^{m-s}$

Table 4 The Hamming weights in $\overline{\mathcal{C}_f}$ when $m+s$ is odd

Hamming weight w	Multiplicity A_w
0	1
p^m	$p-1$
$(p-1)p^{m-1}$	$2p^{m+1}-p^m-p$
$(p-1)p^{m-1}-\epsilon_f \frac{1}{p}\sqrt{p^*}^{m+s+1}$	$\frac{1}{2}(p-1)^2 p^m$
$(p-1)p^{m-1}+\epsilon_f \frac{1}{p}\sqrt{p^*}^{m+s+1}$	$\frac{1}{2}(p-1)^2 p^m$

Proof. We first consider the case $c=0$. By Remark 1, when $c=0$, the Hamming weights $wt(\mathbf{c}_{(a,b,0)})$ follow from Propositions 1 and 2. For $\mathbf{c}_{(a,b,0)} \in \overline{\mathcal{C}_f}$, we have the following cases:

- When $a=0$, we have $wt(\tilde{c}_{(0,0,0)})=0$ and $wt(\tilde{c}_{(0,b,0)})=p^m-p^{m-1}$ for all $b \in \mathbb{F}_{p^m}^\star$.
- When $a \in \mathbb{F}_p^\star$ and $b \in \mathbb{F}_{p^m}$, we have

  – if $a^{-1}b \notin \mathcal{S}_f$, then we get $wt(\mathbf{c}_{(a,b,0)}) = p^m - p^{m-1}$,

- if $a^{-1}b \in \mathcal{S}_f$, then for $m+s$ even,

$$wt(\mathbf{c}_{(a,b,0)}) = \begin{cases} p^m - p^{m-1} - \epsilon_f \frac{(p-1)}{p} \sqrt{p^*}^{m+s}, & \text{if } f^\star(a^{-1}b) = 0, \\ p^m - p^{m-1} + \epsilon_f \frac{1}{p} \sqrt{p^*}^{m+s}, & \text{if } f^\star(a^{-1}b) \in \mathbb{F}_p^\star, \end{cases}$$

for $m+s$ odd,

$$wt(\mathbf{c}_{(a,b,0)}) = \begin{cases} p^m - p^{m-1}, & \text{if } f^\star(a^{-1}b) = 0, \\ p^m - p^{m-1} - \epsilon_f \frac{1}{p} \sqrt{p^*}^{m+s+1}, & \text{if } f^\star(a^{-1}b) \in SQ, \\ p^m - p^{m-1} + \epsilon_f \frac{1}{p} \sqrt{p^*}^{m+s+1}, & \text{if } f^\star(a^{-1}b) \in NSQ. \end{cases}$$

We now compute the Hamming weights of $\mathbf{c}_{(a,b,c)}$ when $c \neq 0$. The Hamming weights $wt(\mathbf{c}_{(a,b,c)}) = p^m - N_f(a,b,c)$ follow from Lemma 13 as follows:

- $wt(\mathbf{c}_{(0,0,c)}) = p^m - N_f(0,0,c) = p^m$ for every $c \in \mathbb{F}_p^\star$.
- $wt(\mathbf{c}_{(0,b,c)}) = p^m - N_f(0,b,c) = p^m - p^{m-1}$ for every $b \in \mathbb{F}_{p^m}^\star$ and $c \in \mathbb{F}_p^\star$.
- When $a, c \in \mathbb{F}_p^\star$, $wt(\mathbf{c}_{(a,b,c)}) = p^m - N_f(a,b,c) = p^m - p^{m-1}$ $\forall a^{-1}b \in \mathbb{F}_{p^m} \setminus \mathcal{S}_f$, and for every $a^{-1}b \in \mathcal{S}_f$,
  - for $m+s$ even,

$$wt(\mathbf{c}_{(a,b,c)}) = \begin{cases} p^m - p^{m-1} - \epsilon_f \frac{(p-1)}{p} \sqrt{p^*}^{m+s}, & \text{if } f^\star(a^{-1}b) + ca^{-1} = 0, \\ p^m - p^{m-1} + \epsilon_f \frac{1}{p} \sqrt{p^*}^{m+s}, & \text{if } f^\star(a^{-1}b) + ca^{-1} \neq 0 \end{cases}$$

  - for $m+s$ odd,

$$wt(\mathbf{c}_{(a,b,c)}) = \begin{cases} p^m - p^{m-1}, & \text{if } f^\star(a^{-1}b) + ca^{-1} = 0, \\ p^m - p^{m-1} - \epsilon_f \frac{1}{p} \sqrt{p^*}^{m+s+1}, & \text{if } \eta_0(f^\star(a^{-1}b) + ca^{-1}) = 1, \\ p^m - p^{m-1} + \epsilon_f \frac{1}{p} \sqrt{p^*}^{m+s+1}, & \text{if } \eta_0(f^\star(a^{-1}b) + ca^{-1}) = -1. \end{cases}$$

From the above results, we can list below the Hamming weights under the corresponding conditions. the Hamming weights $wt(\mathbf{c}_{(a,b,c)})$ are given as for even $m+s$

$$\begin{cases} 0, & \text{if } a = b = c = 0, \\ w_1 = p^m, & \text{if } a = b = 0, c \in \mathbb{F}_p^\star, \\ w_2 = p^m - p^{m-1}, & \text{if } a = 0, b \in \mathbb{F}_{p^m}^\star \text{ or } a \in \mathbb{F}_p^\star, a^{-1}b \notin \mathcal{S}_f, \\ w_3 = p^m - p^{m-1} - \epsilon_f \frac{(p-1)}{p} \sqrt{p^*}^{m+s}, & \text{if } a \in \mathbb{F}_p^\star, a^{-1}b \in \mathcal{S}_f, f^\star(a^{-1}b) + ca^{-1} = 0, \\ w_4 = p^m - p^{m-1} + \epsilon_f \frac{1}{p} \sqrt{p^*}^{m+s}, & \text{if } a \in \mathbb{F}_p^\star, a^{-1}b \in \mathcal{S}_f, f^\star(a^{-1}b) + ca^{-1} \neq 0, \end{cases}$$

for odd $m+s$,

$$\begin{cases} 0, & \text{if } a=b=c=0, \\ w_1 = p^m, & \text{if } a=b=0, c \in \mathbb{F}_p^\star, \\ w_2 = p^m - p^{m-1}, & \text{if } a=0, b \in \mathbb{F}_{p^m}^\star \text{ or } a \in \mathbb{F}_p^\star, a^{-1}b \notin \mathcal{S}_f \\ & \text{or } a \in \mathbb{F}_p^\star, a^{-1}b \in \mathcal{S}_f, f^\star(a^{-1}b)+ca^{-1}=0, \\ w_3 = p^m - p^{m-1} - \epsilon_f \frac{1}{p}\sqrt{p^*}^{\,m+s+1}, & \text{if } a \in \mathbb{F}_p^\star, a^{-1}b \in \mathcal{S}_f, \eta_0(f^\star(a^{-1}b)+ca^{-1})=1, \\ w_4 = p^m - p^{m-1} + \epsilon_f \frac{1}{p}\sqrt{p^*}^{\,m+s+1}, & \text{if } a \in \mathbb{F}_p^\star, a^{-1}b \in \mathcal{S}_f, \eta_0(f^\star(a^{-1}b)+ca^{-1})=-1. \end{cases}$$

We determine the weight distribution of each codeword. Let A_{w_i} be the weight distribution of the Hamming weight w_i, for $1 \le i \le 4$. When $m+s$ is even.

- It is clear that $A_{w_1} = p-1$.
- By Lemma 3, we have $A_{w_2} = p(p^m-1) + p(p-1)(p^m - p^{m-s})$.
- Define $A_{w_3} = \#\{(a,b,c) \in \mathbb{F}_p^\star \times \mathcal{S}_f \times \mathbb{F}_p \,:\, f^\star(a^{-1}b)+ca^{-1}=0\}$. For fixed a and b, the equation $-af^\star(a^{-1}b)=c$ has the unique solution. Then, $A_{w_3} = (p-1)p^{m-s}$.
- Define $A_{w_4} = \#\{(a,b,c) \in \mathbb{F}_p^\star \times \mathcal{S}_f \times \mathbb{F}_p \,:\, f^\star(a^{-1}b)+ca^{-1} \neq 0\}$. Then, $A_{w_4} = (p-1)p^{m-s}p - A_{w_3} = (p-1)p^{m-s+1} - (p-1)p^{m-s} = (p-1)^2p^{m-s}$.

When $m+s$ is odd.

- It is clear that $A_{w_1} = p-1$.
- By Lemma 2, we have $A_{w_2} = p(p^m-1) + (p-1)(p^m - p^{m-s}) + (p-1)p^{m-s} = p(p^m-1) + (p-1)p^m = 2p^{m+1} - p^m - p$.
- $A_{w_3} = \#\{(a,b,c) \in \mathbb{F}_p^\star \times \mathbb{F}_{p^m} \times \mathbb{F}_p \,:\, f^\star(a^{-1}b)+ca^{-1} \in SQ\} = \frac{1}{2}(p-1)^2p^m$.
- $A_{w_4} = \#\{(a,b,c) \in \mathbb{F}_p^\star \times \mathbb{F}_{p^m} \times \mathbb{F}_p \,:\, f^\star(a^{-1}b)+ca^{-1} \in NSQ\} = \frac{1}{2}(p-1)^2p^m$.

This completes the proof. □

Corollary 1. *Let $\overline{\mathcal{C}_f}$ be the code proposed in Theorem 3. Then, the code $\overline{\mathcal{C}_f}$ is self-orthogonal code over $\mathbb{F}_p$ when $m+s \ge 4$ and $m+s \ge 3$ for even and odd cases, respectively.*

Proof. Since the vector $\mathbf{1} \in \overline{\mathcal{C}_f}$ and $\overline{\mathcal{C}_f}$ is p-divisible for each case, then the augmented code $\overline{\mathcal{C}_f}$ is self-orthogonal due to Lemma 7. □

Remark 2. *Let $\overline{\mathcal{C}_f}$ be a linear $[p^m, m+2, d]_p$ code in Theorem 3.*

- *When $m+s$ is even, $d = (p-1)(p^{m-1} - p^{\frac{m+s-2}{2}})$ if $\epsilon_f(\eta_0(-1))^{\frac{m+s}{2}} = 1$; otherwise, $d = p^m - p^{m-1} - p^{\frac{m+s-2}{2}}$.*
- *When $m+s$ is odd, $d = p^m - p^{m-1} - p^{\frac{m+s-1}{2}}$.*

4.3 Construction of LCD codes

In this section, we observe that the constructed self-orthogonal code $\overline{\mathcal{C}_f}$ is the (optimally) extendable code, and new families of LCD codes are constructed from the codes $\overline{\mathcal{C}_f}$.

Let $f : \mathbb{F}_{p^m} \to \mathbb{F}_p$ be a weakly regular p-ary s-plateaued function with $f(0) = 0$. Let $\overline{\mathcal{C}_f}$ be a linear $[p^m, m + 2]_p$ code over $\mathbb{F}_p$ defined in (16). Let $\mathbb{F}^*_{p^m} = \langle \beta \rangle$. Let $D = \{d_1, d_2, ..., d_n\}$ be a defining set. The generator matrix G of the code $\overline{\mathcal{C}_f}$ is given by

$$G = \begin{bmatrix} 1 & 1 & \dots & 1 \\ f(d_1) & f(d_2) & \dots & f(d_n) \\ \mathrm{Tr}_p^{p^m}(\beta^0 d_1) & \mathrm{Tr}_p^{p^m}(\beta^0 d_2) & \dots & \mathrm{Tr}_p^{p^m}(\beta^0 d_n) \\ \mathrm{Tr}_p^{p^m}(\beta^1 d_1) & \mathrm{Tr}_p^{p^m}(\beta^1 d_2) & \dots & \mathrm{Tr}_p^{p^m}(\beta^1 d_n) \\ . & . & & . \\ . & . & & . \\ . & . & & . \\ \mathrm{Tr}_p^{p^m}(\beta^{m-1} d_1) & \mathrm{Tr}_p^{p^m}(\beta^{m-1} d_2) & \dots & \mathrm{Tr}_p^{p^m}(\beta^{m-1} d_n) \end{bmatrix} \tag{18}$$

By an elementary row transformation on G, one can obtain the following generator matrix G_2 of $\overline{\mathcal{C}_f}$:

$$G_2 = \begin{bmatrix} 1 & 1 & \dots & 1 \\ f(d_1)+1 & f(d_2)+1 & \dots & f(d_n)+1 \\ \mathrm{Tr}_p^{p^m}(\beta^0 d_1) & \mathrm{Tr}_p^{p^m}(\beta^0 d_2) & \dots & \mathrm{Tr}_p^{p^m}(\beta^0 d_n) \\ \mathrm{Tr}_p^{p^m}(\beta^1 d_1) & \mathrm{Tr}_p^{p^m}(\beta^1 d_2) & \dots & \mathrm{Tr}_p^{p^m}(\beta^1 d_n) \\ . & . & & . \\ . & . & & . \\ . & . & & . \\ \mathrm{Tr}_p^{p^m}(\beta^{m-1} d_1) & \mathrm{Tr}_p^{p^m}(\beta^{m-1} d_2) & \dots & \mathrm{Tr}_p^{p^m}(\beta^{m-1} d_n) \end{bmatrix} \tag{19}$$

Let $\overline{\mathcal{C}_f}'$ be the linear code with generator matrix $G'_2 = [I_{(m+2,m+2)} : G_2]$. Since the code $\overline{\mathcal{C}_f}$ is self-orthogonal in Theorem 3, the code $\overline{\mathcal{C}_f}'$ is an LCD code due to Lemma 8.

The following propositions derive the parameters of the LCD code $\overline{\mathcal{C}_f}'$ and its dual code $\overline{\mathcal{C}_f}'^{\perp}$.

Proposition 3. *Let $m + s$ be an even integer with $0 \leq s \leq m - 2$. Let $\overline{\mathcal{C}_f}$ be the code given in Theorem 3 with the generator matrix G_2 in (19). Then, a matrix G'_2 generates an LCD code $\overline{\mathcal{C}_f}'$ with the parameters $[p^m + m + 2, m + 2, d]_p$ for*

- $d = p^m - p^{m-1} - (p-1)p^{\frac{m+s-2}{2}} + 2$ *when* $\epsilon_f(\eta_0(-1))^{\frac{m+s}{2}} = 1$,
- $d = p^m - p^{m-1} - p^{\frac{m+s-2}{2}} + 1$ *when* $\epsilon_f(\eta_0(-1))^{\frac{m+s}{2}} = -1$.

Moreover, the dual code $\overline{\mathcal{C}_f}'^{\perp}$ has parameters $[p^m + m + 2, p^m, 3]$.

Proposition 4. *Let $m + s$ be an odd integer with $0 \leq s \leq m - 2$. Let $\overline{\mathcal{C}_f}$ be the code given in Theorem 3 with the generator matrix G_2 in (19). Then, a matrix G'_2 generates an LCD code $\overline{\mathcal{C}_f}'$ with the parameters $[p^m + m + 2, m + 2, d]_p$ for*

- $d = p^m - p^{m-1} - p^{\frac{m+s-1}{2}} + 1$ *when* $\epsilon_f(\eta_0(-1))^{\frac{m+s+1}{2}} = 1$,
- $d = p^m - p^{m-1} - p^{\frac{m+s-1}{2}} + 2$ *when* $\epsilon_f(\eta_0(-1))^{\frac{m+s+1}{2}} = -1$.

Moreover, the dual code $\overline{\mathcal{C}_f}'^{\perp}$ has parameters $[p^m + m + 2, p^m, 3]$.

5 Conclusion and Future Work

This paper is based on the recent papers [16, 21]. Motivated by the paper [16], we propose the augmented code construction method for the linear code construction methods introduced in [21] and [12]. In Section 3, we propose the augmented code of the code proposed in [22] based on the defining set. We obtain new families of four-weight and five-weight self-orthogonal codes from the trace function over the odd characteristic finite fields. Moreover, we determine all parameters of the obtained codes and their dual codes. In Section 4, we propose the augmented code of the code proposed in [12]. We obtain new families of four-weight self-orthogonal codes from weakly regular plateaued functions over the odd characteristic finite fields. Moreover, we determine all parameters of the obtained codes and their dual codes. Finally, we employ the constructed p-ary self-orthogonal codes to construct p-ary LCD codes.

We are currently working on the locality and optimality of the constructed self-orthogonal codes. We hope some constructed codes are locally recoverable codes under certain conditions. Moreover, we estimate that they are (almost) optimally extendable linear codes under certain conditions due to Griesmer bound.

References

[1] Huffman, W.C., Pless, V.: Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge (2003)

[2] Carlet, C., Ding, C., Yuan, J.: Linear codes from perfect nonlinear mappings and their secret sharing schemes. IEEE Trans. Inf. Theory **51**(6), 2089–2102 (2005)

[3] Ding, K., Ding, C.: A class of two-weight and three-weight codes and their applications in secret sharing. IEEE Trans. Inf. Theory **61**(11), 5835–5842 (2015)

[4] Yuan, J., Ding, C.: Secret sharing schemes from three classes of linear codes. IEEE Trans. Inf. Theory **52**(1), 206–212 (2006)

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

[6] Schoenmakers, B.: A simple publicly verifiable secret sharing scheme and its application to electronic voting. In: Annual International Cryptology Conference, pp. 148–164 (1999). Springer

[7] 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 (2013). Springer

[8] Carlet, C., Guilley, S.: Complementary dual codes for counter-measures to side-channel attacks. Adv. Math. Commun. **10**(1), 131–150 (2016)

[9] Massey, J.L.: Linear codes with complementary duals. Discrete Math. **106**, 337–342 (1992)

[10] Ding, C.: A construction of binary linear codes from boolean functions. Discrete Math. **339**(9), 2288–2303 (2016)

[11] Ding, C., Heng, Z., Zhou, Z.: Minimal binary linear codes. IEEE Trans. Inf. Theory **64**(10), 6536–6545 (2018)

[12] 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)

[13] Tang, C., Li, N., Qi, Y., Zhou, Z., Helleseth, T.: Linear codes with two or three weights from weakly regular bent functions. IEEE Trans. Inf. Theory **62**(3), 1166–1176 (2016)

[14] 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

[15] Mesnager, S., Özbudak, F., Sinak, A.: Linear codes from weakly regular plateaued functions and their secret sharing schemes. Des., Codes Cryptogr., 463–480 (2019)

[16] Heng, Z., Li, X., Wu, Y., Wang, Q.: Two families of linear codes with desirable properties from some functions over finite fields. IEEE Transactions on Information Theory (2024)

[17] Lidl, R., Niederreiter, H.: Finite Fields vol. 20. Cambridge university press, New York (1997)

[18] Li, X., Heng, Z.: Self-orthogonal codes from p-divisible codes. arXiv preprint arXiv:2311.11634 (2023)

[19] Massey, J.L.: Orthogonal , antiorthogonal and self-orthogonal matrices and their codes. (1998). https://api.semanticscholar.org/CorpusID:6889914

[20] Griesmer, J.H.: A bound for error-correcting codes. IBM Journal of Research and Development **4**(5), 532–542 (1960)

[21] Zhu, C., Liao, Q.: Two new classes of projective two-weight linear codes. Finite Fields and Their Applications **88**, 102186 (2023)

[22] Heng, Z., Li, D., Liu, F.: Ternary self-orthogonal codes from weakly regular bent functions and their application in lcd codes. Designs, Codes and Cryptography **91**(12), 3953–3976 (2023)