Turkish Journal of Mathematics

http://journals.tubitak.gov.tr/math/

Research Article

Turk J Math
(2022) 46: 953 – 972
© TÜBİTAK
doi:10.3906/mat-2110-70

Construction of minimal linear codes with few weights from weakly regular plateaued functions

Ahmet SINAK[1,2,*]
[1]Department of Mathematics and Computer Science, Faculty of Science, Necmettin Erbakan University, Konya, Turkey
[2]LAGA UMR 7539, CNRS, Sorbonne Paris Cité, University of Paris XIII, Villetaneuse, France

Received: 20.10.2021 • **Accepted/Published Online:** 03.02.2022 • **Final Version:** 11.03.2022

Abstract: The construction of (minimal) linear codes from functions over finite fields has been greatly studied in the literature, since determining the parameters of codes based on functions is rather easy due to the nice structures of functions. In this paper, we derive 3-weight and 4-weight linear codes from weakly regular plateaued functions in the recent construction method of linear codes over the odd characteristic finite fields. The Hamming weights and weight distributions for codes are, respectively, determined by using the Walsh transform values and Walsh distributions of the employed functions. We also derive projective 3-weight punctured codes with good parameters from the constructed codes. These punctured codes may be almost optimal due to the Griesmer bound, and they can be employed to design association schemes. We lastly show that all constructed codes are minimal, which approves that they can be employed to design high democratic secret sharing schemes.

Key words: Linear code; minimal code; weight distribution; weakly regular plateaued function

1. Introduction

There are many construction methods for linear codes, one of which is derived from functions over finite fields. Constructing linear codes from functions is a popular research topic in the literature although considerable progress has been done in this direction. A great number of linear codes have been obtained from cryptographic functions such as quadratic functions [7, 8, 11, 12, 27, 31], (weakly regular) bent functions [7, 8, 21, 26, 28, 31], (almost) perfect nonlinear functions [4, 16, 29] and (weakly regular) plateaued functions [22, 23, 25]. Two generic (say, *first* and *second*) construction methods of linear codes from functions can be isolated from the others in the literature. Several linear codes with excellent parameters have been derived from cryptographic functions based on the first generic construction method (see for example in [4, 8, 21, 22]) and the second generic construction method (see for example in [8, 12, 23, 26, 27, 31]). Indeed, Ding et al. [9, 10] have initially derived the Hamming weights in any linear codes based on the second generic construction from the Walsh spectrum of the employed functions, with the help of Gaussian sums. Similarly, Mesnager has proposed in [21] the computation method of the Hamming weights in any linear codes based on the first generic construction using the Walsh transform values of the employed functions. Hence, they are the main essential works in terms of tools and methodology in view of computing the Hamming weights of linear codes based on functions over finite fields. It is worth

*Correspondence: sinakahmet@gmail.com
2010 *AMS Mathematics Subject Classification:* 94A60, 68R01, 14G50, 11T23

noting that a very good survey [18] written by Li and Mesnager is devoted to the construction methods of linear codes from cryptographic functions over finite fields. Moreover, Mesnager has written the new chapter in [20] that covers the recent advances in the constructions of linear codes from functions over finite fields.

Recently, weakly regular plateaued (especially, bent) functions have been employed to design (minimal) linear codes with a few weights over the odd characteristic finite fields (see [21–23, 25, 26, 28]). We now in this paper employ weakly regular plateaued functions in the recent construction method of linear codes proposed in [17, 28], and then we obtain several classes of minimal linear codes with new parameters from these functions over the odd characteristic finite fields. The contribution of this paper increases our knowledge of linear codes based on functions over finite fields. It allows to have a relatively large family of linear codes having good parameters (for example, punctured ones are almost optimal codes) and satisfying the minimality property (useful for nice applications) because we employ a new and large family of cryptographic functions: the so-called weakly regular plateaued functions. This paper comes after some known papers [17, 23, 25, 28] available in the literature with the same goal and spirit, but the ingredient here has not been investigated before, and this paper also contributes to completing and improving further known results.

The rest of this paper is organized as follows. In Section 2, we set the main notation and give some properties of weakly regular plateaued functions. In Section 3, we introduce the parameters of 3-weight and 4-weight linear codes derived from these functions over finite fields. We also propose some punctured codes for the constructed codes. We hereby obtain projective 3-weight codes with flexible parameters. We finally highlight that our codes are minimal codes. Section 4 completes the paper.

2. Preliminaries

For a set T, its size is shown by $\#T$, and $T^\star = T\setminus\{0\}$. 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 $q=p^n$ for a positive integer n and an odd prime p. The trace of $\alpha\in\mathbb{F}_q$ over $\mathbb{F}_p$ is defined as $\mathrm{Tr}^n(\alpha)=\alpha+\alpha^p+\alpha^{p^2}+\cdots+\alpha^{p^{n-1}}$. The set of all *non-squares* and *squares* in $\mathbb{F}_p^\star$ are represented by NSQ and SQ, respectively. The *quadratic character* of $\mathbb{F}_p^\star$ is 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 $\{1,\xi_p,\xi_p^2,\dots,\xi_p^{p-2}\}$ of the cyclotomic field $\mathbb{Q}(\xi_p)$. The Galois group $Gal(\mathbb{Q}(\xi_p)/\mathbb{Q})$ is described as the set $\{\sigma_c\colon\, c\in\mathbb{F}_p^\star\}$, where σ_c is the automorphism of $\mathbb{Q}(\xi_p)$ defined as $\sigma_c(\xi_p)=\xi_p^c$. 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 $a,c\in\mathbb{F}_p^\star$, we clearly have $\sigma_c(\xi_p^a)=\xi_p^{ca}$ and $\sigma_c(\sqrt{p^*}^{\,n})={\eta_0}^n(c)\sqrt{p^*}^{\,n}$. The following lemma is used in the subsequent proofs.

Lemma 2.1 *[19] Under the above notation, we have*

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

2.1. Linear codes

A linear $[n,k,d]$ code $\mathcal{C}$ over $\mathbb{F}_p$ is a subspace with k-dimension of vector space $\mathbb{F}_p^n$. Here, n is the length of $\mathcal{C}$, k is its dimension, and d is its minimum Hamming distance. For a vector $\mathbf{v}=(v_1,\dots,v_n)\in\mathbb{F}_p^n$, its Hamming weight $W_H(\mathbf{v})$ is the size of its support described as $\mathrm{supp}(\mathbf{v}) = \{1 \le i \le n\colon\ v_i \neq 0\}$. We remark that d is the smallest Hamming weight of the nonzero codewords of $\mathcal{C}$. The *dual code* of $\mathcal{C}$ is defined to be the set

$$\mathcal{C}^{\perp} = \{(u_1, \dots, u_n) \in \mathbb{F}_p^n\colon\ u_1v_1 + \cdots + u_nv_n = 0 \text{ for all } (v_1, \dots, v_n) \in \mathcal{C}\},$$

which is represented by $[n, n-k, d^{\perp}]$ over $\mathbb{F}_p$, where $d^{\perp}$ is the minimum Hamming distance of $\mathcal{C}^{\perp}$. The *weight distribution* of $\mathcal{C}$ is given by $(1, A_1, \dots, A_n)$ and its *weight enumerator* is the polynomial $1+A_1y+\cdots+A_ny^n$, where A_ω is the number of nonzero codewords with weight ω in $\mathcal{C}$. As a result, we say that $\mathcal{C}$ is an l*-weight linear code* if the number of nonzero A_ω in $\{A_i\}_{i\ge 1}$ is equal to l, where l is an integer with $1 \le l \le n$. The first two Pless power moments are given as

$$\sum_{i=0}^{n} A_i = p^k \quad \text{and} \quad \sum_{i=0}^{n} iA_i = n(p-1)p^{k-1} - A_1^{\perp}p^{k-1},$$

where $A_1^{\perp}$ is the number of codewords with weight 1 in $\mathcal{C}^{\perp}$. For the proposed codes in this paper, $A_1^{\perp} = 0$, since their defining sets do not cover the element $(0, 0)$.

2.2. Weakly regular plateaued functions

Let $f : \mathbb{F}_q \to \mathbb{F}_p$ be a p-ary function. The *Walsh transform* of f is a complex valued function defined as

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

A function f is called *balanced* over $\mathbb{F}_p$ if f gets all elements of $\mathbb{F}_p$ with the same number of pre-images; or else, f is said to be *unbalanced*. Note that f is balanced iff $\mathcal{W}_f(0) = 0$. A function f is said to be a *bent* function if $|\mathcal{W}_f(\beta)|^2 = p^n$ for every $\beta \in \mathbb{F}_q$ (see [24] for Boolean bent and [15] for p-ary bent). In addition, f is said to be s*-plateaued* if $|\mathcal{W}_f(\beta)|^2 \in \{0, p^{n+s}\}$ for every $\beta \in \mathbb{F}_q$, with $0 \le s \le n$, (see [30] for Boolean plateaued and [5] for p-ary plateaued). For an s-plateaued function f, its *Walsh support* is described as the set $\mathcal{S}_f = \{\beta \in \mathbb{F}_q\colon\ |\mathcal{W}_f(\beta)|^2 = p^{n+s}\}$. From the Parseval identity, we have $\#\mathcal{S}_f = p^{n-s}$, and the explicit Walsh distribution of a plateaued function is given as follows.

Lemma 2.2 *Let f be an s-plateaued function. For $\beta \in \mathbb{F}_q$, $|\mathcal{W}_f(\beta)|^2$ takes the values p^{n+s} and 0 for the times p^{n-s} and $p^n - p^{n-s}$, respectively.*

Mesnager et al. [22] have described the notion of (non)-weakly regular plateaued functions. An s-plateaued f is called *weakly regular* if we have $\mathcal{W}_f(\beta) \in \left\{0, up^{\frac{n+s}{2}}\xi_p^{f^\star(\beta)}\right\}$, where $u \in \{\pm1, \pm i\}$ and $f^\star$ is a p-ary function over $\mathbb{F}_q$ with $f^\star(\beta) = 0$ for every $\beta \in \mathbb{F}_q \setminus \mathcal{S}_f$; otherwise, f is called *non-weakly regular*. We remark that a weakly regular 0-plateaued is the weakly regular bent function.

The following lemma is very useful to compute the Hamming weights of proposed codes.

Lemma 2.3 *[22] Let f be a weakly regular s-plateaued function. Then, for every $\beta \in \mathcal{S}_f$, we have that $\mathcal{W}_f(\beta) = \epsilon\sqrt{p^*}^{\,n+s}\xi_p^{f^\star(\beta)}$, where $\epsilon = \pm1$ is the sign of $\mathcal{W}_f$ and $f^\star$ is a p-ary function over $\mathcal{S}_f$.*

The following two lemmas are needed to determine the weight distributions of proposed codes.

Lemma 2.4 *[23] Let f be a weakly regular s-plateaued function. For $x \in \mathbb{F}_q$,*

$$\sum_{\beta \in \mathcal{S}_f} \xi_p^{f^\star(\beta)+\mathrm{Tr}^n(\beta x)} = \epsilon \eta_0^n(-1)\sqrt{p^*}^{\,n-s} \xi_p^{f(x)},$$

where $\epsilon = \pm 1$ is the sign of $\mathcal{W}_f$ and $f^\star$ is a p-ary function over $\mathcal{S}_f$.

Lemma 2.5 *[23] Let f be a weakly regular s-plateaued function with $0 \le s < n$ and $\mathcal{W}_f(\beta) = \epsilon_f \sqrt{p^*}^{\,n+s} \xi_p^{f^\star(\beta)}$ for every $\beta \in \mathcal{S}_f$. For $j \in \mathbb{F}_p$, define $\mathcal{N}_{f^\star}(j) = \#\{\beta \in \mathcal{S}_f : f^\star(\beta) = j\}$. Then, we have for $n-s$ even*

$$\mathcal{N}_{f^\star}(j) = \begin{cases} p^{n-s-1} + \epsilon \eta_0^{n+1}(-1)(p-1)\sqrt{p^*}^{\,n-s-2}, & \text{if } j = 0, \\ p^{n-s-1} - \epsilon \eta_0^{n+1}(-1)\sqrt{p^*}^{\,n-s-2}, & \text{if not,} \end{cases}$$

and for $n-s$ odd,

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

Very recently, two subclasses of weakly regular plateaued functions over the odd characteristic finite fields have been introduced. Let $f : \mathbb{F}_q \to \mathbb{F}_p$ be a weakly regular s_f-plateaued function that satisfy two homogeneous conditions:

- $f(0) = 0$, and
- $f(ax) = a^{k_f} f(x)$ for all $x \in \mathbb{F}_q$ and $a \in \mathbb{F}_p^\star$, where k_f is an even positive integer with $\gcd(k_f - 1, p-1) = 1$.

The set of such weakly regular plateaued unbalanced and balanced functions has been, respectively, denoted by *WRP* in [23] and *WRPB* in [25]. In this paper, to construct linear codes with flexible parameters, we use these subclasses of plateaued functions in the recent construction method of [28].

We end this section with proposing the following results that are used in the subsequent proofs.

Proposition 2.6 *[23, 25] Let $f \in WRP$ or $f \in WRPB$. Then, $f^\star(0) = 0$ and $f^\star(a\beta) = a^{l_f} f^\star(\beta)$ for all $a \in \mathbb{F}_p^\star$ and $\beta \in \mathcal{S}_f$, where l_f is an even positive integer with $\gcd(l_f - 1, p-1) = 1$.*

Lemma 2.7 *[23, 25] Let $f \in WRP$ or $f \in WRPB$. Then for every $\beta \in \mathcal{S}_f$ (respectively, $\beta \in \mathbb{F}_q \setminus \mathcal{S}_f$), we have $z\beta \in \mathcal{S}_f$ (respectively, $z\beta \in \mathbb{F}_q \setminus \mathcal{S}_f$) for every $z \in \mathbb{F}_p^\star$.*

3. Linear codes derived from weakly regular plateaued functions over $\mathbb{F}_p$

In this section, weakly regular plateaued functions are employed to obtain minimal linear codes in the second generic construction method.

3.1. The construction method of linear codes from functions

For a long time, cryptographic functions have been extensively used to design linear codes with few weights in coding theory. Constructing linear codes from functions including quadratic, almost bent, (almost) perfect nonlinear, (weakly regular) bent and plateaued functions is a highly interesting research topic in the literature. Remarkably, determining the parameters of the codes derived from these functions is rather easy due to the nice structure of these functions although it is generally a difficult problem in coding theory.

Two construction methods of linear codes from functions are generic in the sense that several classes of known codes could be obtained from these construction methods. We below define two generic construction methods of linear codes from functions. For a polynomial $F(x)$ on $\mathbb{F}_q$, the *first* generic construction of linear codes is given by

$$\mathcal{C}(F) = \{(\mathrm{Tr}^n(aF(x) + bx))_{x\in\mathbb{F}_q^\star} \colon\ a, b \in \mathbb{F}_q\}$$

with length $(q-1)$ and dimension at most $2n$. For a subset $D = \{d_1, \ldots, d_m\} \subseteq \mathbb{F}_q$, the *second* generic construction based on D is defined as

$$\mathcal{C}_D = \{(\mathrm{Tr}^n(ad_1), \ldots, \mathrm{Tr}^n(ad_m))\colon\ a \in \mathbb{F}_q\} \tag{3.1}$$

with length m and dimension at most n. The set D is called the *defining set* of $\mathcal{C}_D$, and the quality of its parameters depends on the choice of D. The construction method of the form (3.1) has been initially studied by Ding et al. [9, 10], and many linear codes have been proposed in [7–12]. Furthermore, new linear codes have been obtained from some cryptographic functions in this construction method (see *e.g.* [23, 25–27, 31]). Recently, motivated by the method of the form (3.1), Li et al. [17] have defined for a subset $\mathcal{D} = \{(x_1, y_1), \ldots, (x_m, y_m)\} \subseteq \mathbb{F}_q^2$ the following linear code

$$\mathcal{C}_{\mathcal{D}} = \{\mathbf{c}_{(a,b)} = (\mathrm{Tr}^n(ax_1 + by_1), \ldots, \mathrm{Tr}^n(ax_m + by_m))\colon\ a, b \in \mathbb{F}_q\}, \tag{3.2}$$

whose length is m and dimension is at most $2n$. They have constructed some linear codes by using the set $\mathcal{D} = \{(x, y) \in \mathbb{F}_q^2 \setminus \{(0, 0)\}\colon\ \mathrm{Tr}^n(x^k + y^l) = 0\}$, where $k, l \in \{1, 2, p^{n/2} + 1\}$. Later, Jian et al. [14] have constructed further linear codes of the form (3.2) by using $\mathcal{D} = \{(x, y) \in \mathbb{F}_q^2 \setminus \{(0, 0)\}\colon\ \mathrm{Tr}^n(x^k + y^{p^u+1}) = 0\}$, where $k \in \{1, 2\}$. Very recently, Wu et al. [28] have constructed new linear codes of the form (3.2) based on the set

$$\mathcal{D} = \{(x, y) \in (\mathbb{F}_q^2)^\star\colon\ f(x) + g(y) = 0\} \subset \mathbb{F}_q^2, \tag{3.3}$$

where f and g are two weakly regular bent functions from $\mathbb{F}_q$ to $\mathbb{F}_p$. Motivated by the works [14, 17, 28], we, in this paper, construct minimal linear codes of the form (3.2) based on the set $\mathcal{D}$ of the form (3.3) for weakly regular plateaued functions.

Let f and g be two p-ary functions from $\mathbb{F}_q$ to $\mathbb{F}_p$ and let $\mathcal{D}$ be the set of the form (3.3). From the definition of the code $\mathcal{C}_{\mathcal{D}}$ of the form (3.2), we define

$$\mathcal{N}_{\mathcal{D}}(a, b) = \#\{(x, y) \in (\mathbb{F}_q^2)^\star\colon f(x) + g(y) = 0 \text{ and } \mathrm{Tr}^n(ax + by) = 0\}.$$

Then, the Hamming weight of the nonzero codeword $\mathbf{c}_{(a,b)}$ is given by $W_H(\mathbf{c}_{(a,b)}) = \#\mathcal{D} - \mathcal{N}_{\mathcal{D}}(a, b)$ for every $(a, b) \in (\mathbb{F}_q^2)^\star$, and we clearly have $W_H(\mathbf{c}_{(0,0)}) = 0$.

3.2. Three-weight linear codes derived from $\mathrm{Tr}^n(x) + g(y)$

In this subsection, we construct the linear code $\mathcal{C}_{\mathcal{D}_g}$ of the form (3.2) based on the set

$$\mathcal{D}_g = \{(x, y) \in (\mathbb{F}_q^2)^\star \colon \mathrm{Tr}^n(x) + g(y) = 0\}, \tag{3.4}$$

when g is an s_g-plateaued function in the set *WRPB*, with $1 \le s_g < n$. From the orthogonality of exponential sums, we can derive its size $\#\mathcal{D}_g = p^{2n-1} - 1$, which is the length of the code $\mathcal{C}_{\mathcal{D}_g}$. To find the Hamming weights in $\mathcal{C}_{\mathcal{D}_g}$, for $(a, b) \in (\mathbb{F}_q^2)^\star$ we define

$$\mathcal{N}_{\mathcal{D}_g}(a, b) = \#\{(x, y) \in \mathcal{D}_g \colon \mathrm{Tr}^n(ax + by) = 0\}. \tag{3.5}$$

We can derive the following lemma from the proof of [28, Lemma 5].

Lemma 3.1 *Let $\mathcal{N}_{\mathcal{D}_g}(a, b)$ be defined as in (3.5) for $(a, b) \in (\mathbb{F}_q^2)^\star$. Then, we have*

$$\mathcal{N}_{\mathcal{D}_g}(a, b) = \begin{cases} p^{2n-2} - 1, & \text{if } a \in \mathbb{F}_q \setminus \mathbb{F}_p^\star, \\ p^{2n-2} - 1 + \frac{A(a,b)}{p^2}, & \text{if } a \in \mathbb{F}_p^\star, \end{cases}$$

for which the value $A(a, b)$ can be expressed as

$$A(a, b) = p^n \sum_{z_1 \in \mathbb{F}_p^\star} \sigma_{z_1} \left(\sum_{y \in \mathbb{F}_q} \xi_p^{g(y) - \mathrm{Tr}^n(a^{-1} b y)} \right) \tag{3.6}$$

where a^{-1} is the multiplicative inverse of $a \in \mathbb{F}_p^\star$.

The following lemma calculates the value $A(a, b)$ by using the Walsh spectrum of the employed plateaued function.

Lemma 3.2 *Let $g \in WRPB$ with $1 \le s_g \le n$. Let $A(a, b)$ be defined as in (3.6) for $a \in \mathbb{F}_p^\star$ and $b \in \mathbb{F}_q$. Then, for every $a^{-1}b \in \mathbb{F}_q \setminus \mathcal{S}_g$ we have $A(a, b) = 0$, and for every $a^{-1}b \in \mathcal{S}_g$ we have for $n + s_g$ even*

$$A(a, b) = \begin{cases} \epsilon_g (p-1) p^n \sqrt{p^*}^{\,n+s_g}, & \text{if } g^\star(a^{-1}b) = 0, \\ -\epsilon_g p^n \sqrt{p^*}^{\,n+s_g}, & \text{if not,} \end{cases}$$

and for $n + s_g$ odd

$$A(a, b) = \begin{cases} 0, & \text{if } g^\star(a^{-1}b) = 0, \\ \epsilon_g p^n \sqrt{p^*}^{\,n+s_g+1}, & \text{if } g^\star(a^{-1}b) \in SQ, \\ -\epsilon_g p^n \sqrt{p^*}^{\,n+s_g+1}, & \text{if } g^\star(a^{-1}b) \in NSQ. \end{cases}$$

Proof The first case is trivial. For the second case: for every $a^{-1}b \in \mathcal{S}_g$, we have by Lemma 2.3

$$A(a, b) = p^n \sum_{z_1 \in \mathbb{F}_p^\star} \sigma_{z_1} \left(\epsilon_g \sqrt{p^*}^{\,n+s_g} \xi_p^{g^\star(a^{-1}b)} \right) = \epsilon_g p^n \sqrt{p^*}^{\,n+s_g} \sum_{z_1 \in \mathbb{F}_p^\star} \eta_0^{n+s_g}(z_1) \xi_p^{z_1 g^\star(a^{-1}b)},$$

The proof is, hence, completed from Lemma 2.1. $\square$

The following lemma helps to determine the weights of codewords in $\mathcal{C}_{\mathcal{D}_g}$.

Lemma 3.3 *Let $g \in WRPB$ with $1 \le s_g \le n$, and $\mathcal{S}_g$ be its Walsh support. Let $\mathcal{N}_{\mathcal{D}_g}(a,b)$ be defined as in (3.5) for $(a,b) \in (\mathbb{F}_q^2)^\star$. Then, we have $\mathcal{N}_{\mathcal{D}_g}(a,b) = p^{2n-2} - 1$ if $a \in \mathbb{F}_q \setminus \mathbb{F}_p^\star$ or if $a^{-1}b \notin \mathcal{S}_g$ where $a \in \mathbb{F}_p^\star$. When $a^{-1}b \in \mathcal{S}_g$ where $a \in \mathbb{F}_p^\star$, we have for $n+s_g$ even*

$$\mathcal{N}_{\mathcal{D}_g}(a,b) = \begin{cases} p^{2n-2} - 1 + \epsilon_g (p-1) p^{n-2} \sqrt{p^*}^{\,n+s_g}, & \text{if } g^\star(a^{-1}b) = 0, \\ p^{2n-2} - 1 - \epsilon_g p^{n-2} \sqrt{p^*}^{\,n+s_g}, & \text{if not,} \end{cases}$$

and for $n+s_g$ odd

$$\mathcal{N}_{\mathcal{D}_g}(a,b) = \begin{cases} p^{2n-2} - 1, & \text{if } g^\star(a^{-1}b) = 0, \\ p^{2n-2} - 1 + \epsilon_g p^{n-2} \sqrt{p^*}^{\,n+s_g+1}, & \text{if } g^\star(a^{-1}b) \in SQ, \\ p^{2n-2} - 1 - \epsilon_g p^{n-2} \sqrt{p^*}^{\,n+s_g+1}, & \text{if } g^\star(a^{-1}b) \in NSQ. \end{cases}$$

Proof The proof follows from the combination of Lemmas 3.1 and 3.2. □

The following theorem proposes the code $\mathcal{C}_{\mathcal{D}_g}$ of the form (3.2) based on the set $\mathcal{D}_g$ of the form (3.4).

Theorem 3.4 *Let $g \in WRPB$ with $1 \le s_g < n$. Then, the code $\mathcal{C}_{\mathcal{D}_g}$ of the form (3.2) with parameters $[p^{2n-1}-1, 2n]$ is the 3-weight linear code over $\mathbb{F}_p$. The weight distributions are listed in Tables 1 and 2 when $n+s_g$ is even and odd, respectively.*

Table 1. The code $\mathcal{C}_{\mathcal{D}_g}$ in Theorem 3.4 when $n+s_g$ is even.

Hamming weight ω	Multiplicity A_ω
0	1
$(p-1)p^{2n-2}$	$p^{2n} - (p-1)p^{n-s_g} - 1$
$(p-1)(p^{2n-2} - \epsilon_g p^{n-2}\sqrt{p^*}^{\,n+s_g})$	$(p-1)(p^{n-s_g-1} + \epsilon_g \eta_0^{n+1}(-1)(p-1)\sqrt{p^*}^{\,n-s_g-2})$
$(p-1)p^{2n-2} + \epsilon_g p^{n-2}\sqrt{p^*}^{\,n+s_g}$	$(p-1)^2(p^{n-s_g-1} - \epsilon_g \eta_0^{n+1}(-1)\sqrt{p^*}^{\,n-s_g-2})$

Table 2. The code $\mathcal{C}_{\mathcal{D}_g}$ in Theorem 3.4 when $n+s_g$ is odd.

Hamming weight ω	Multiplicity A_ω
0	1
$(p-1)p^{2n-2}$	$p^{2n} - (p-1)^2 p^{n-s_g-1} - 1$
$(p-1)p^{2n-2} - \epsilon_g p^{n-2}\sqrt{p^*}^{\,n+s_g+1}$	$\frac{(p-1)^2}{2}(p^{n-s_g-1} + \epsilon_g \eta_0^{n}(-1)\sqrt{p^*}^{\,n-s_g-1})$
$(p-1)p^{2n-2} + \epsilon_g p^{n-2}\sqrt{p^*}^{\,n+s_g+1}$	$\frac{(p-1)^2}{2}(p^{n-s_g-1} - \epsilon_g \eta_0^{n}(-1)\sqrt{p^*}^{\,n-s_g-1})$

Proof From the definition of $\mathcal{C}_{\mathcal{D}_g}$, its length is $\#\mathcal{D}_g = p^{2n-1} - 1$, and for every $(a,b) \in (\mathbb{F}_q^2)^\star$, its Hamming weight $W_H(\mathbf{c}_{(a,b)}) = p^{2n-1} - 1 - \mathcal{N}_{\mathcal{D}_g}(a,b)$, where $\mathcal{N}_{\mathcal{D}_g}(a,b)$ is computed in Lemma 3.3. More clearly, if $a \in \mathbb{F}_q \setminus \mathbb{F}_p^\star$ or if $a^{-1}b \notin \mathcal{S}_g$ for $a \in \mathbb{F}_p^\star$, then we have $W_H(\mathbf{c}_{(a,b)}) = (p-1)p^{2n-2}$ whose weight distribution is $p^{2n} - (p-1)p^{n-s_g} - 1$ from Lemma 2.2. Additionally, for every $a^{-1}b \in \mathcal{S}_g$ where $a \in \mathbb{F}_p^\star$, the weight $W_H(\mathbf{c}_{(a,b)})$ follows from Lemma 3.3, and its weight distribution is derived from Lemma 2.5. This completes the proof. □

Remark 3.5 *In Theorem 3.4, the code* $\mathcal{C}_{\mathcal{D}_g}$ *is the* 2*-weight code when* $s_g = n-1$.

Remark 3.6 *The code* $\mathcal{C}_{\mathcal{D}_g}$ *proposed in Theorem 3.4 has been independently obtained in [6, Theorem 1] when* $g \in WRP$ *with* $0 \le s_g < n$.

3.3. Three-weight and four-weight linear codes derived from weakly regular plateaued functions

In this subsection, we construct the linear code $\mathcal{C}_{\mathcal{D}}$ of the form (3.2) based on the set

$$\mathcal{D} = \{(x,y) \in (\mathbb{F}_q^2)^\star : \ f(x) + g(y) = 0\}, \tag{3.7}$$

where f and g are weakly regular s_f-plateaued and s_g-plateaued functions from $\mathbb{F}_q$ to $\mathbb{F}_p$, respectively, for $0 \le s_f, s_g < n$. Recall that throughout this paper $\mathcal{S}_f$ and $\mathcal{S}_g$ denote the Walsh supports of f and g, and let l_f, l_g be defined as in Proposition 2.6. To calculate the Hamming weight of the nonzero codeword $\mathbf{c}_{(a,b)}$ in $\mathcal{C}_{\mathcal{D}}$ for every $(a,b) \in (\mathbb{F}_q^2)^\star$, we define

$$\mathcal{N}_{\mathcal{D}}(a,b) = \#\{(x,y) \in \mathcal{D} : \ \mathrm{Tr}^n(ax+by) = 0\}. \tag{3.8}$$

We now introduce several lemmas by using the exponential sums and Walsh spectrum of a weakly regular plateaued function. We start with finding the size of the set $\mathcal{D}$.

Lemma 3.7 *Let* $\mathcal{D}$ *be defined as in (3.7). If* $f,g \in WRPB$*, then* $\#\mathcal{D} = p^{2n-1} - 1$*. If* $f,g \in WRP$*, then*

$$\#\mathcal{D} = \begin{cases} p^{2n-1} - 1, & \text{if } 2n + s_f + s_g \text{ is odd,} \\ p^{2n-1} - 1 + \epsilon_f \epsilon_g \frac{p-1}{p} \sqrt{p^*}^{2n+s_f+s_g}, & \text{otherwise.} \end{cases}$$

Proof From the orthogonality of exponential sums, we have

$$\#\mathcal{D} + 1 = \frac{1}{p} \sum_{x,y \in \mathbb{F}_q} \sum_{z \in \mathbb{F}_p} \xi_p^{z(f(x)+g(y))} = p^{2n-1} + \frac{1}{p} \sum_{z \in \mathbb{F}_p^\star} \sigma_z \left(\sum_{x \in \mathbb{F}_q} \xi_p^{f(x)} \sum_{y \in \mathbb{F}_q} \xi_p^{g(y)} \right).$$

When $f,g \in WRPB$, we clearly get $\#\mathcal{D} = p^{2n-1} - 1$. On the other hand, when $f,g \in WRP$, from Lemma 2.3 we write $\mathcal{W}_f(0) = \epsilon_f \sqrt{p^*}^{\,n+s_f}$ and $\mathcal{W}_g(0) = \epsilon_g \sqrt{p^*}^{\,n+s_g}$, where $\epsilon_f, \epsilon_g \in \{\pm 1\}$, since we know $f^\star(0) = g^\star(0) = 0$ from Proposition 2.6. We then have

$$\#\mathcal{D} + 1 = p^{2n-1} + \frac{1}{p} \sum_{z \in \mathbb{F}_p^\star} \sigma_z(\epsilon_f \epsilon_g \sqrt{p^*}^{2n+s_f+s_g}) = p^{2n-1} + \epsilon_f \epsilon_g \frac{1}{p} \sqrt{p^*}^{2n+s_f+s_g} \sum_{z \in \mathbb{F}_p^\star} \eta_0^{2n+s_f+s_g}(z)).$$

Hence, the proof is completed from Lemma 2.1. □

The following lemmas are needed to find the Hamming weights and weight distributions of proposed codes.

Lemma 3.8 *Let* $f,g \in WRP$*. For* $(a,b) \in (\mathbb{F}_q^2)^\star$*, define*

$$B(a,b) = \sum_{z_1, z_2 \in \mathbb{F}_p^\star} \sum_{x,y \in \mathbb{F}_q} \xi_p^{z_1(f(x)+g(y)) - z_2 \mathrm{Tr}^n(ax+by)}.$$

Then, for $(a,b) \notin \mathcal{S}_f \times \mathcal{S}_g$ *we have* $B(a,b)=0$, *and for* $(a,b) \in \mathcal{S}_f \times \mathcal{S}_g$, *we have the following cases. When* $2n+s_f+s_g$ *is odd and* $l_f = l_g$, *we have*

$$B(a,b) \quad = \begin{cases} 0, & \text{if } f^\star(a)=b=0 \text{ or } a=g^\star(b)=0 \text{ or } f^\star(a)+g^\star(b)=0 \text{ for } ab\neq 0, \\ K, & \text{if } f^\star(a)\in SQ \text{ for } b=0 \text{ or } g^\star(b)\in SQ \text{ for } a=0 \text{ or } f^\star(a)+g^\star(b)\in SQ \text{ for } ab\neq 0, \\ -K, & \text{if } f^\star(a)\in NSQ \text{ for } b=0 \text{ or } g^\star(b)\in NSQ \text{ for } a=0 \text{ or } f^\star(a)+g^\star(b)\in NSQ \text{ for } ab\neq 0, \end{cases}$$

where $K=\epsilon_f\epsilon_g(p-1)\sqrt{p^*}^{2n+s_f+s_g+1}$. *When* $2n+s_f+s_g$ *is even, we have for* $l_f=l_g$

$$B(a,b) \quad = \begin{cases} (p-1)L, & \text{if } a=g^\star(b)=0 \text{ or } f^\star(a)=b=0 \text{ or } f^\star(a)+g^\star(b)=0 \text{ for } ab\neq 0, \\ -L, & \text{otherwise}, \end{cases}$$

and for $l_f \neq l_g$

$$B(a,b) \quad = \begin{cases} (p-1)L, & \text{if } a=g^\star(b)=0 \text{ or } f^\star(a)=b=0 \text{ or } f^\star(a)=g^\star(b)=0 \text{ for } ab\neq 0, \\ \frac{(p+1)L}{p-1}, & \text{if } -\frac{f^\star(a)}{g^\star(b)}\in SQ, \\ -L, & \text{otherwise}, \end{cases}$$

where $L=\epsilon_f\epsilon_g(p-1)\sqrt{p^*}^{2n+s_f+s_g}$.

Proof From the definition of $B(a,b)$, we have

$$B(a,b) \quad = \sum_{z_1,z_2\in\mathbb{F}_p^\star}\sum_{x\in\mathbb{F}_q}\xi_p^{z_1(f(x)-\mathrm{Tr}^n(z_2ax))}\sum_{y\in\mathbb{F}_q}\xi_p^{z_1(g(y)-\mathrm{Tr}^n(z_2by))} = \sum_{z_1\in\mathbb{F}_p^\star}\sigma_{z_1}\Big(\sum_{z_2\in\mathbb{F}_p^\star}\mathcal{W}_f(z_2a)\mathcal{W}_g(z_2b)\Big),$$

where we use the fact that $\frac{z_2}{z_1}$ passes all over $\mathbb{F}_p^\star$ for a fixed z_1 while z_2 passes through $\mathbb{F}_p^\star$ in the first equality.

- If $(a,b)\notin\mathcal{S}_f\times\mathcal{S}_g$, equiv., $(z_2a,z_2b)\notin\mathcal{S}_f\times\mathcal{S}_g$ for every $z_2\in\mathbb{F}_p^\star$ (see Lemma 2.7), then $B(a,b)=0$.
- If $(a,b)\in\mathcal{S}_f\times\mathcal{S}_g$, equiv., $(z_2a,z_2b)\in\mathcal{S}_f\times\mathcal{S}_g$ for every $z_2\in\mathbb{F}_p^\star$, there are two cases: $ab=0$ and $ab\neq 0$.
  - In the case of $ab=0$, suppose $a=0$ and $b\neq 0$, without loss of generality. We then have

$$\begin{aligned} B(a,b) \quad &= \sum_{z_1\in\mathbb{F}_p^\star}\sigma_{z_1}\left(\sum_{z_2\in\mathbb{F}_p^\star}\epsilon_f\sqrt{p^*}^{\,n+s_f}\epsilon_g\sqrt{p^*}^{\,n+s_g}\xi_p^{g^\star(z_2b)}\right) \\ &= \sum_{z_1\in\mathbb{F}_p^\star}\sigma_{z_1}\left(\sum_{z_2\in\mathbb{F}_p^\star}\epsilon_f\epsilon_g\sqrt{p^*}^{2n+s_f+s_g}\xi_p^{z_2^{l_g}g^\star(b)}\right) \\ &= \epsilon_f\epsilon_g\sqrt{p^*}^{2n+s_f+s_g}\sum_{z_1\in\mathbb{F}_p^\star}\eta_0^{2n+s_f+s_g}(z_1)\sum_{z_2\in\mathbb{F}_p^\star}\xi_p^{z_1z_2^{l_g}g^\star(b)}, \end{aligned}$$

    where we use Lemmas 2.3, 2.7 and Proposition 2.6 in the first and second equality, respectively. Thus, with the help of Lemma 2.1, we get for $2n+s_f+s_g$ odd

$$B(a,b) \quad = \begin{cases} 0, & \text{if } g^\star(b)=0, \\ K, & \text{if } g^\star(b)\in SQ, \\ -K, & \text{if } g^\star(b)\in NSQ, \end{cases}$$

and for $2n+s_f+s_g$ even

$$B(a,b) \quad = \begin{cases} (p-1)L, & \text{if } g^\star(b)=0, \\ -L, & \text{if not.} \end{cases}$$

Similarly, for $b=0$ and $a\neq 0$, the analogous computations yield the same results above with respect to the parameter a.

– In the case of $ab\neq 0$, we get

$$\begin{aligned} B(a,b) &= \sum_{z_1\in\mathbb{F}_p^\star} \sigma_{z_1}\left(\sum_{z_2\in\mathbb{F}_p^\star} \epsilon_f\sqrt{p^*}^{\,n+s_f}\xi_p^{f^\star(z_2a)}\epsilon_g\sqrt{p^*}^{\,n+s_g}\xi_p^{g^\star(z_2b)}\right) \\ &= \sum_{z_1\in\mathbb{F}_p^\star} \sigma_{z_1}\left(\sum_{z_2\in\mathbb{F}_p^\star} \epsilon_f\epsilon_g\sqrt{p^*}^{2n+s_f+s_g}\xi_p^{z_2^{l_f}f^\star(a)+z_2^{l_g}g^\star(b)}\right) \\ &= \epsilon_f\epsilon_g\sqrt{p^*}^{2n+s_f+s_g}\sum_{z_1\in\mathbb{F}_p^\star}\eta_0^{2n+s_f+s_g}(z_1)\sum_{z_2\in\mathbb{F}_p^\star}\xi_p^{z_1(z_2^{l_f}f^\star(a)+z_2^{l_g}g^\star(b))}, \end{aligned}$$

where we use Lemmas 2.3, 2.7 and Proposition 2.6 in the first and second equality, respectively. We can compute the value $B(a,b)$ by using Lemma 2.1 and some properties of the cyclotomic field. When $2n+s_f+s_g$ is odd, we get for $l_f=l_g$

$$B(a,b) \quad = \begin{cases} 0, & \text{if } f^\star(a)+g^\star(b)=0, \\ K, & \text{if } f^\star(a)+g^\star(b)\in SQ, \\ -K, & \text{if } f^\star(a)+g^\star(b)\in NSQ. \end{cases}$$

When $2n+s_f+s_g$ is even, we get for $l_f=l_g$

$$B(a,b) \quad = \begin{cases} (p-1)L, & \text{if } f^\star(a)+g^\star(b)=0, \\ -L, & \text{otherwise,} \end{cases}$$

and for $l_f\neq l_g$

$$B(a,b) \quad = \begin{cases} (p-1)L, & \text{if } f^\star(a)=g^\star(b)=0, \\ \frac{(p+1)L}{p-1}, & \text{if } -\frac{f^\star(a)}{g^\star(b)}\in SQ, \\ -L, & \text{otherwise.} \end{cases}$$

□

Lemma 3.9 *Let $f,g\in WRPB$ with $1\leq s_f,s_g<n$. For $(a,b)\in(\mathbb{F}_q^2)^\star$, let $B(a,b)$ be defined as in Lemma 3.8. For $(a,b)\notin\mathcal{S}_f\times\mathcal{S}_g$, we have $B(a,b)=0$, and for $(a,b)\in\mathcal{S}_f\times\mathcal{S}_g$ we have the following cases. When $2n+s_f+s_g$ is odd and $l_f=l_g$,*

$$B(a,b) \quad = \begin{cases} 0, & \text{if } f^\star(a)+g^\star(b)=0, \\ K, & \text{if } f^\star(a)+g^\star(b)\in SQ, \\ -K, & \text{if } f^\star(a)+g^\star(b)\in NSQ, \end{cases}$$

where $K=\epsilon_f\epsilon_g(p-1)\sqrt{p^*}^{2n+s_f+s_g+1}$. When $2n+s_f+s_g$ is even, we have for $l_f=l_g$

$$B(a,b) \quad = \begin{cases} (p-1)L, & \text{if } f^\star(a)+g^\star(b)=0, \\ -L, & \text{otherwise,} \end{cases}$$

and for $l_f \neq l_g$

$$B(a,b) \quad = \begin{cases} (p-1)L, & \text{if } f^\star(a) = g^\star(b) = 0, \\ \frac{(p+1)L}{p-1}, & \text{if } -\frac{f^\star(a)}{g^\star(b)} \in SQ, \\ -L, & \text{otherwise,} \end{cases}$$

where $L = \epsilon_f \epsilon_g (p-1)\sqrt{p^*}^{2n+s_f+s_g}$.

Proof The proof is very similar to that of Lemma 3.8. □

Lemma 3.10 *Let* $f, g \in WRP$. *Let* $\mathcal{N}_{\mathcal{D}}(a,b)$ *be defined as in (3.8) for* $(a,b) \in (\mathbb{F}_q^2)^\star$.

- *Suppose that* $2n+s_f+s_g$ *is odd and* $l_f = l_g$. *For every* $(a,b) \notin \mathcal{S}_f \times \mathcal{S}_g$, *we have* $\mathcal{N}_{\mathcal{D}}(a,b) = p^{2n-2}-1$, *and for every* $(a,b) \in \mathcal{S}_f \times \mathcal{S}_g$,

$$\mathcal{N}_{\mathcal{D}}(a,b) \quad = \begin{cases} p^{2n-2}-1, & \text{if } f^\star(a)+g^\star(b)=0, \\ p^{2n-2}-1+\epsilon_f\epsilon_g \frac{1}{p^2}(p-1)\sqrt{p^*}^{2n+s_f+s_g+1}, & \text{if } f^\star(a)+g^\star(b) \in SQ, \\ p^{2n-2}-1-\epsilon_f\epsilon_g \frac{1}{p^2}(p-1)\sqrt{p^*}^{2n+s_f+s_g+1}, & \text{if } f^\star(a)+g^\star(b) \in NSQ. \end{cases}$$

- *Suppose that* $2n+s_f+s_g$ *is even. For every* $(a,b) \notin \mathcal{S}_f \times \mathcal{S}_g$, *we have* $\mathcal{N}_{\mathcal{D}}(a,b) = p^{2n-2}-1+\epsilon_f\epsilon_g\frac{1}{p^2}(p-1)\sqrt{p^*}^{2n+s_f+s_g}$. *For every* $(a,b) \in \mathcal{S}_f \times \mathcal{S}_g$, *we have for* $l_f = l_g$

$$\mathcal{N}_{\mathcal{D}}(a,b) \quad = \begin{cases} p^{2n-2}-1+\epsilon_f\epsilon_g \frac{1}{p}(p-1)\sqrt{p^*}^{2n+s_f+s_g}, & \text{if } f^\star(a)+g^\star(b)=0, \\ p^{2n-2}-1, & \text{otherwise,} \end{cases}$$

and for $l_f \neq l_g$

$$\mathcal{N}_{\mathcal{D}}(a,b) \quad = \begin{cases} p^{2n-2}-1+\epsilon_f\epsilon_g \frac{1}{p}(p-1)\sqrt{p^*}^{2n+s_f+s_g}, & \text{if } f^\star(a)=g^\star(b)=0, \\ p^{2n-2}-1+\epsilon_f\epsilon_g \frac{2}{p}\sqrt{p^*}^{2n+s_f+s_g}, & \text{if } -\frac{f^\star(a)}{g^\star(b)} \in SQ, \\ p^{2n-2}-1, & \text{otherwise.} \end{cases}$$

Proof By the definition of $\mathcal{N}_{\mathcal{D}}(a,b)$ and using the orthogonality of exponential sums, we get

$$\mathcal{N}_{\mathcal{D}}(a,b)+1 \quad = p^{-2}\sum_{x,y\in\mathbb{F}_q}\sum_{z_1\in\mathbb{F}_p}\xi_p^{z_1(f(x)+g(y))}\sum_{z_2\in\mathbb{F}_p}\xi_p^{-z_2\mathrm{Tr}^n(ax+by)} = p^{2n-2}+\frac{1}{p^2}(A+B(a,b)),$$

where

$$A = \sum_{z_1\in\mathbb{F}_p^\star}\sum_{x,y\in\mathbb{F}_q}\xi_p^{z_1(f(x)+g(y))} \text{ and } B(a,b) = \sum_{z_1,z_2\in\mathbb{F}_p^\star}\sum_{x,y\in\mathbb{F}_q}\xi_p^{z_1(f(x)+g(y))-z_2\mathrm{Tr}^n(ax+by)}.$$

We clearly have $A = p(\#\mathcal{D}+1)-p^{2n}$ in the light of Lemma 3.7. The proof is then completed from Lemmas 3.7 and 3.8. □

From Lemma 3.9, the following lemma can be proven with the same technique used in Lemma 3.10.

Lemma 3.11 *Let $f, g \in WRPB$ and let $\mathcal{N}_{\mathcal{D}}(a,b)$ be defined as in (3.8) for $(a,b) \in (\mathbb{F}_q^2)^\star$. Assume that $2n + s_f + s_g$ is even. Then we have $\mathcal{N}_{\mathcal{D}}(a,b) = p^{2n-2} - 1$ for every $(a,b) \notin \mathcal{S}_f \times \mathcal{S}_g$, and for every $(a,b) \in \mathcal{S}_f \times \mathcal{S}_g$, we have for $l_f = l_g$*

$$\mathcal{N}_{\mathcal{D}}(a,b) = \begin{cases} p^{2n-2} - 1 + \epsilon_f \epsilon_g \frac{1}{p^2}(p-1)^2 \sqrt{p^*}^{2n+s_f+s_g}, & \text{if } f^\star(a) + g^\star(b) = 0, \\ p^{2n-2} - 1 - \epsilon_f \epsilon_g \frac{1}{p^2}(p-1)\sqrt{p^*}^{2n+s_f+s_g}, & \text{otherwise}, \end{cases}$$

and for $l_f \neq l_g$

$$\mathcal{N}_{\mathcal{D}}(a,b) = \begin{cases} p^{2n-2} - 1 + \epsilon_f \epsilon_g \frac{1}{p^2}(p-1)^2 \sqrt{p^*}^{2n+s_f+s_g}, & \text{if } f^\star(a) = g^\star(b) = 0, \\ p^{2n-2} - 1 + \epsilon_f \epsilon_g \frac{1}{p^2}(p+1)\sqrt{p^*}^{2n+s_f+s_g}, & \text{if } -\frac{f^\star(a)}{g^\star(b)} \in SQ, \\ p^{2n-2} - 1 - \epsilon_f \epsilon_g \frac{1}{p^2}(p-1)\sqrt{p^*}^{2n+s_f+s_g} & \text{otherwise}. \end{cases}$$

We provide the following lemma in order to determine the weight distributions of proposed codes.

Lemma 3.12 *Let $f, g \in WRP$ or $f, g \in WRPB$. For $a, b \in \mathbb{F}_q$ and $t \in \mathbb{F}_p$, define $S_{fg}(t) = \#\{(a,b) \in \mathcal{S}_f \times \mathcal{S}_g \colon f^\star(a) + g^\star(b) = t\}$. Then, we have for $2n - s_f - s_g$ odd*

$$S_{fg}(t) = \begin{cases} p^{2n-s_f-s_g-1}, & \text{if } t = 0, \\ p^{2n-s_f-s_g-1} + \epsilon_f \epsilon_g \eta_0(-t) \frac{1}{p} \sqrt{p^*}^{2n-s_f-s_g+1}, & \text{if } t \neq 0, \end{cases}$$

and for $2n - s_f - s_g$ even

$$S_{fg}(t) = \begin{cases} p^{2n-s_f-s_g-1} + \epsilon_f \epsilon_g \frac{p-1}{p} \sqrt{p^*}^{2n-s_f-s_g}, & \text{if } t = 0, \\ p^{2n-s_f-s_g-1} - \epsilon_f \epsilon_g \frac{1}{p} \sqrt{p^*}^{2n-s_f-s_g}, & \text{if } t \neq 0. \end{cases}$$

Proof From the orthogonality of exponential sums, we have

$$\begin{aligned} S_{fg}(t) &= \frac{1}{p} \sum_{a \in \mathcal{S}_f} \sum_{b \in \mathcal{S}_g} \sum_{z \in \mathbb{F}_p} \xi_p^{z(f^\star(a)+g^\star(b))-zt} \\ &= \frac{1}{p}(p^{2n-s_f-s_g} + \sum_{z \in \mathbb{F}_p^\star} \xi_p^{-zt} \sigma_z(\sum_{a \in \mathcal{S}_f} \xi_p^{f^\star(a)} \sum_{b \in \mathcal{S}_g} \xi_p^{g^\star(b)})) \\ &= p^{2n-s_f-s_g-1} + \epsilon_f \epsilon_g \frac{1}{p} \sqrt{p^*}^{2n-s_f-s_g} \sum_{z \in \mathbb{F}_p^\star} \eta_0^{2n-s_f-s_g}(z) \xi_p^{-zt}, \end{aligned}$$

where Lemma 2.4 is used in the last equality. The proof is, hence, completed by Lemma 2.1. □

We now construct the code $\mathcal{C}_{\mathcal{D}}$ of the form (3.2) from weakly regular plateaued unbalanced functions.

Theorem 3.13 *Let $f, g \in WRP$ with $l_f = l_g$, where l_f, l_g are defined as in Proposition 2.6. Let $\mathcal{D}$ be defined as in (3.7). Suppose that $n + s_f$ is odd and $n + s_g$ is even with $0 \leq s_f, s_g < n$. Then, the code $\mathcal{C}_{\mathcal{D}}$ of the from (3.2) with parameters $[p^{2n-1} - 1, 2n, (p-1)(p^{2n-2} - \sqrt{p}^{2n+s_f+s_g-3})]$ is the 3-weight linear code whose weight distribution is listed in Table 3. For simplicity, we denote $m = 2n + s_f + s_g$ and $r = 2n - s_f - s_g$ in Table 3.*

Proof From the definition of $\mathcal{C}_{\mathcal{D}}$, its length equals the size of $\mathcal{D}$, and the weight of each codeword is $W_H(\mathbf{c}_{(a,b)}) = \#\mathcal{D} - \mathcal{N}_{\mathcal{D}}(a,b)$ for every $(a,b) \in (\mathbb{F}_q^2)^\star$, where $\mathcal{N}_{\mathcal{D}}(a,b)$ is defined as in (3.8). By Lemma 3.7,

Table 3. The code $\mathcal{C}_{\mathcal{D}}$ in Theorem 3.13 when $n+s_f$ is odd and $n+s_g$ is even.

Hamming weight ω	Multiplicity A_ω
0	1
$(p-1)p^{2n-2}$	$p^{2n}-p^r+p^{r-1}-1$
$(p-1)(p^{2n-2}-\epsilon_f\epsilon_g\sqrt{p^*}^{m-3})$	$\frac{(p-1)}{2}(p^{r-1}+\epsilon_f\epsilon_g\eta_0(-1)\frac{1}{p}\sqrt{p^*}^{r+1})$
$(p-1)(p^{2n-2}+\epsilon_f\epsilon_g\sqrt{p^*}^{m-3})$	$\frac{(p-1)}{2}(p^{r-1}-\epsilon_f\epsilon_g\eta_0(-1)\frac{1}{p}\sqrt{p^*}^{r+1})$

we have $\#\mathcal{D}=p^{2n-1}-1$, and so the Hamming weights can be derived from Lemma 3.10. To put it more explicitly, for every $(a,b)\notin\mathcal{S}_f\times\mathcal{S}_g$, we have $W_H(\mathbf{c}_{(a,b)})=(p-1)p^{2n-2}$, and the number of such codewords equals $p^{2n}-p^{2n-s_f-s_g}$ by Lemma 2.2. Additionally, by Lemma 3.10, for every $(a,b)\in\mathcal{S}_f\times\mathcal{S}_g$, we get

$$W_H(\mathbf{c}_{(a,b)}) = \begin{cases} (p-1)p^{2n-2}, & S_{fg}(0)-1 \text{ times},\\ (p-1)p^{2n-2}-\epsilon_f\epsilon_g(p-1)\sqrt{p^*}^{2n+s_f+s_g-3}, & (\frac{p-1}{2})S_{fg}(i) \text{ times},\\ (p-1)p^{2n-2}+\epsilon_f\epsilon_g(p-1)\sqrt{p^*}^{2n+s_f+s_g-3}, & (\frac{p-1}{2})S_{fg}(j) \text{ times}, \end{cases}$$

where the values $S_{fg}(0)$, $S_{fg}(i)$ and $S_{fg}(j)$ are computed in Lemma 3.12 for $i\in SQ$ and $j\in NSQ$. This completes the proof. □

Remark 3.14 *In Theorem 3.13, when we employ $f,g\in WRPB$ in the set $\mathcal{D}$ for $1\le s_f,s_g<n$, we obtain the same code $\mathcal{C}_{\mathcal{D}}$.*

The following examples for the code $\mathcal{C}_{\mathcal{D}}$ given in Theorem 3.13 are verified by MAGMA in [2].

Example 3.15 *Let $f,g:\mathbb{F}_{3^2}\to\mathbb{F}_3$ be defined as $f(x)=\mathrm{Tr}^2(\zeta x^4+\zeta^8x^2)$ and $g(x)=\mathrm{Tr}^2(x^{10})$, for a primitive element ζ of $\mathbb{F}_{3^2}$. Then $f,g\in WRP$ with $s_f=1,s_g=0$ and $\epsilon_f=\epsilon_g=1$, and hence $\mathcal{C}_{\mathcal{D}}$ is the 3-weight ternary $[26,4,12]$ code with $1+12y^{12}+62y^{18}+6y^{24}$.*

Example 3.16 *Let $f,g:\mathbb{F}_{3^3}\to\mathbb{F}_3$ be defined as $f(x)=\mathrm{Tr}^3(x^{10})$ and $g(x)=\mathrm{Tr}^3(\zeta x^4+\zeta^8x^2)$, for a primitive element ζ of $\mathbb{F}_{3^3}$. Then $f,g\in WRP$ with $s_f=0,s_g=1$ and $\epsilon_f=\epsilon_g=1$, and hence $\mathcal{C}_{\mathcal{D}}$ is the 3-weight minimal ternary $[242,6,144]$ code with $1+90y^{144}+566y^{162}+72y^{180}$. It is worth noting that this code is better than the code $[242,6,135]_3$, which is obtained in [28, Example 6] only from quadratic weakly regular bent $f(x)=\mathrm{Tr}^3(x^{10})$.*

Theorem 3.17 *Let $f,g\in WRP$ and let l_f,l_g be defined as in Proposition 2.6. Let $\mathcal{D}$ be defined as in (3.7). Suppose that $2n+s_f+s_g$ is even with $0\le s_f,s_g<n-1$. Then, the code $\mathcal{C}_{\mathcal{D}}$ of the form (3.2) with parameters $[p^{2n-1}-1+\epsilon_f\epsilon_g\frac{1}{p}(p-1)\sqrt{p^*}^{2n+s_f+s_g},2n]$ is the 3-weight and 4-weight linear code over $\mathbb{F}_p$, respectively, when $l_f=l_g$ and $l_f\ne l_g$ for $p>3$. The weight distributions are given in Tables 4 and 5, where $m=2n+s_f+s_g$ and $r=2n-s_f-s_g$.*

Proof The length of the code $\mathcal{C}_{\mathcal{D}}$ follows from Lemma 3.7, and for every $(a,b)\in(\mathbb{F}_q^2)^\star$, the Hamming weight $W_H(\mathbf{c}_{(a,b)})=\#\mathcal{D}-\mathcal{N}_{\mathcal{D}}(a,b)$ can be obtained from Lemmas 3.7 and 3.10. To be more precise, when

Table 4. The code $\mathcal{C}_{\mathcal{D}}$ in Theorem 3.17 when m is even and $l_f = l_g$.

Hamming weight ω	Multiplicity A_ω
0	1
$(p-1)(p^{2n-2}+\epsilon_f\epsilon_g(p-1)\sqrt{p^*}^{m-4})$	$p^{2n}-p^r$
$(p-1)p^{2n-2}$	$p^{r-1}+\epsilon_f\epsilon_g\frac{1}{p}(p-1)\sqrt{p^*}^{r}-1$
$(p-1)(p^{2n-2}+\epsilon_f\epsilon_g\frac{1}{p}\sqrt{p^*}^{m})$	$(p-1)(p^{r-1}-\epsilon_f\epsilon_g\frac{1}{p}\sqrt{p^*}^{r})$

Table 5. The code $\mathcal{C}_{\mathcal{D}}$ in Theorem 3.17 when $p>3$, m is even and $l_f \neq l_g$.

Hamming weight ω	Multiplicity A_ω
0	1
$(p-1)(p^{2n-2}+\epsilon_f\epsilon_g(p-1)\sqrt{p^*}^{m-4})$	$p^{2n}-p^r$
$(p-1)p^{2n-2}$	A_{ω_1}
$(p-1)p^{2n-2}+\epsilon_f\epsilon_g\frac{(p-3)}{p}\sqrt{p^*}^{m}$	A_{ω_2}
$(p-1)(p^{2n-2}+\epsilon_f\epsilon_g\frac{1}{p}\sqrt{p^*}^{m})$	$p^r-1-A_{\omega_1}-A_{\omega_2}$

$(a,b) \notin \mathcal{S}_f \times \mathcal{S}_g$, we have $W_H(\mathbf{c}_{(a,b)}) = (p-1)(p^{2n-2}+\epsilon_f\epsilon_g(p-1)\sqrt{p^*}^{2n+s_f+s_g-4})$ whose weight distribution is $p^{2n}-p^{2n-s_f-s_g}$ from Lemma 2.2. In addition, when $(a,b)\in \mathcal{S}_f \times \mathcal{S}_g$, there are two distinct cases. When $l_f = l_g$,

$$W_H(\mathbf{c}_{(a,b)}) \quad = \begin{cases} (p-1)p^{2n-2}, & S_{fg}(0)-1 \text{ times}, \\ (p-1)(p^{2n-2}+\epsilon_f\epsilon_g\frac{1}{p}\sqrt{p^*}^{2n+s_f+s_g}), & (p-1)S_{fg}(t) \text{ times}, \end{cases}$$

where $S_{fg}(0)$ and $S_{fg}(t)$ for $t\in\mathbb{F}_p^{\star}$ are computed in Lemma 3.12. When $l_f \neq l_g$,

$$W_H(\mathbf{c}_{(a,b)}) \quad = \begin{cases} (p-1)p^{2n-2}, & A_{\omega_1} \text{ times}, \\ (p-1)p^{2n-2}+\epsilon_f\epsilon_g\frac{(p-3)}{p}\sqrt{p^*}^{2n+s_f+s_g}, & A_{\omega_2} \text{ times}, \\ (p-1)(p^{2n-2}+\epsilon_f\epsilon_g\frac{1}{p}\sqrt{p^*}^{2n+s_f+s_g}), & p^{2n-s_f-s_g}-1-A_{\omega_1}-A_{\omega_2} \text{ times}, \end{cases}$$

where

$$\begin{aligned} A_{\omega_1} &= \#\{(a,b)\in\mathcal{S}_f\times\mathcal{S}_g:\ f^\star(a)=g^\star(b)=0\}-1=\mathcal{N}_{f^\star}(0)*\mathcal{N}_{g^\star}(0)-1, \\ A_{\omega_2} &= \#\{(a,b)\in\mathcal{S}_f^\star\times\mathcal{S}_g^\star:\ -\tfrac{f^\star(a)}{g^\star(b)}\in SQ\}=\tfrac{(p-1)^2}{2}\mathcal{N}_{f^\star}(i)*\mathcal{N}_{g^\star}(j),\ \text{for } i,j\in SQ. \end{aligned}$$

Here, the numbers $\mathcal{N}_{f^\star}(i)$ and $\mathcal{N}_{g^\star}(j)$ depend on the parity of s_f and s_g, and the weight distributions follow from Lemma 2.5. This completes the proof. □

We give an example for the code $\mathcal{C}_{\mathcal{D}}$ obtained in Theorem 3.17, verified by MAGMA in [2].

Example 3.18 *Let $f,g:\mathbb{F}_{3^5}\to\mathbb{F}_3$ be defined as $f(x)=\mathrm{Tr}^5(\zeta x^{10}+\zeta^{20}x^4)$ and $g(x)=\mathrm{Tr}^5(\zeta x^{10}+2x^4+x^2)$, for a primitive element ζ of $\mathbb{F}_{3^5}$. Then $f,g\in WRP$ with $s_f=s_g=1$, $l_f=l_g=2$, $\epsilon_f=1$ and $\epsilon_g=-1$. Hence, $\mathcal{C}_{\mathcal{D}}$ is the 3-weight minimal ternary $[19196,10,12636]$ code with $1+4428y^{12636}+52488y^{12798}+2132y^{13122}$.*

Remark 3.19 *In Theorem 3.17, when f and g are two weakly regular 0-plateaued (bent) functions, we obtain*

2-weight and 3-weight linear codes when $l_f = l_g$ and $l_f \neq l_g$, respectively, which were already presented in [28, Theorem 4].

Remark 3.20 *The very special case of Theorem 3.17 has been independently proposed in [6, Theorem 4]. To be more precise, when we assume $s_f = s_g$ in Theorem 3.17, we get the code $\mathcal{C}_{\mathcal{D}_{fg}}$ proposed in [6, Theorem 4].*

We lastly construct the code $\mathcal{C}_{\mathcal{D}}$ of the form (3.2) from weakly regular plateaued balanced functions.

Theorem 3.21 *Let $f, g \in WRPB$ and let l_f, l_g be defined as in Proposition 2.6. Let $\mathcal{D}$ be defined as in (3.7). Suppose that $2n+s_f+s_g$ is even with $1 \leq s_f, s_g < n-1$. Then, the code $\mathcal{C}_{\mathcal{D}}$ of the form (3.2) with parameters $[p^{2n-1}-1, 2n]$ is the 3-weight and 4-weight linear code over $\mathbb{F}_p$, respectively, when $l_f = l_g$ and $l_f \neq l_g$. The weight distributions are listed in Tables 6 and 7, where $m = 2n+s_f+s_g$ and $r = 2n-s_f-s_g$.*

Table 6. The code $\mathcal{C}_{\mathcal{D}}$ in Theorem 3.21 when m is even and $l_f = l_g$.

Hamming weight ω	Multiplicity A_ω
0	1
$(p-1)p^{2n-2}$	$p^{2n} - p^r - 1$
$(p-1)(p^{2n-2} - \epsilon_f\epsilon_g(p-1)\sqrt{p^*}^{m-4})$	$p^{r-1} + \epsilon_f\epsilon_g\frac{1}{p}(p-1)\sqrt{p^*}^r$
$(p-1)(p^{2n-2} + \epsilon_f\epsilon_g\sqrt{p^*}^{m-4})$	$(p-1)(p^{r-1} - \epsilon_f\epsilon_g\frac{1}{p}\sqrt{p^*}^r)$

Table 7. The code $\mathcal{C}_{\mathcal{D}}$ in Theorem 3.21 when m is even and $l_f \neq l_g$.

Hamming weight ω	Multiplicity A_ω
0	1
$(p-1)p^{2n-2}$	$p^{2n} - p^r - 1$
$(p-1)(p^{2n-2} - \epsilon_f\epsilon_g(p-1)\sqrt{p^*}^{m-4})$	A_{ω_1}
$(p-1)p^{2n-2} - \epsilon_f\epsilon_g(p+1)\sqrt{p^*}^{m-4}$	A_{ω_2}
$(p-1)(p^{2n-2} + \epsilon_f\epsilon_g\sqrt{p^*}^{m-4})$	$p^r - A_{\omega_1} - A_{\omega_2}$

Proof For every $(a,b) \in (\mathbb{F}_q^2)^\star$, $W_H(\mathbf{c}_{(a,b)}) = \#\mathcal{D} - \mathcal{N}_{\mathcal{D}}(a,b)$ can be obtained from Lemmas 3.7 and 3.11. To be more precise, when $(a,b) \notin \mathcal{S}_f \times \mathcal{S}_g$, we have $W_H(\mathbf{c}_{(a,b)}) = p^{2n-2}(p-1)$ whose weight distribution is $p^{2n} - p^{2n-s_f-s_g} - 1$ from Lemma 2.2. In addition, when $(a,b) \in \mathcal{S}_f \times \mathcal{S}_g$, there are two distinct cases. For $l_f = l_g$, we have

$$W_H(\mathbf{c}_{(a,b)}) = \begin{cases} (p-1)p^{2n-2} - \epsilon_f\epsilon_g(p-1)^2\sqrt{p^*}^{2n+s_f+s_g-4}, & \text{if } f^\star(a)+g^\star(b)=0, \\ (p-1)p^{2n-2} + \epsilon_f\epsilon_g(p-1)\sqrt{p^*}^{2n+s_f+s_g-4}, & \text{otherwise,} \end{cases}$$

whose weight distribution can be determined from Lemma 3.12. For $l_f \neq l_g$, we have

$$W_H(\mathbf{c}_{(a,b)}) = \begin{cases} (p-1)p^{2n-2} - \epsilon_f\epsilon_g(p-1)^2\sqrt{p^*}^{2n+s_f+s_g-4}, & A_{\omega_1} \text{ times,} \\ (p-1)p^{2n-2} - \epsilon_f\epsilon_g(p+1)\sqrt{p^*}^{2n+s_f+s_g-4}, & A_{\omega_2} \text{ times,} \\ (p-1)p^{2n-2} + \epsilon_f\epsilon_g(p-1)\sqrt{p^*}^{2n+s_f+s_g-4} & p^{2n-s_f-s_g} - A_{\omega_1} - A_{\omega_2} \text{ times,} \end{cases}$$

where we define that $A_{\omega_1} = \#\{(a,b) \in \mathcal{S}_f \times \mathcal{S}_g \colon f^\star(a) = g^\star(b) = 0\} = \mathcal{N}_{f^\star}(0) * \mathcal{N}_{g^\star}(0)$ and $A_{\omega_2} = \#\{(a,b) \in \mathcal{S}_f \times \mathcal{S}_g \colon -\frac{f^\star(a)}{g^\star(b)} \in SQ\} = \frac{(p-1)^2}{2}\mathcal{N}_{f^\star}(i) * \mathcal{N}_{g^\star}(j)$ for $i,j \in SQ$. In this case, the weight distribution follows from Lemma 2.5. Hence, the proof is completed. □

3.4. Three-weight punctured codes

In this subsection, we derive shorter linear codes from the constructed codes by using a special subset of the defining set $\mathcal{D}$. Such a code is said to be a *punctured code* of the original code. It is known that the minimum distance and length of a punctured code are rather smaller than the original code, while its dimension is the same as the original code.

We deal with the code $\mathcal{C}_\mathcal{D}$ of the form (3.2) for the defining set $\mathcal{D}$ of the form (3.7). In Theorems 3.13, 3.17 and 3.21, when $l_f = l_g$, the length of $\mathcal{C}_\mathcal{D}$ and Hamming weights in $\mathcal{C}_\mathcal{D}$ have a common factor $(p-1)$, which suggests that $\mathcal{C}_\mathcal{D}$ can be punctured into a shorter linear code over $\mathbb{F}_p$. Let $f,g \in WRP$ or $WRPB$ with $k_f = k_g$. For every $x,y \in \mathbb{F}_q$, $f(cx)+g(cy) = 0$ iff $f(x)+g(y) = 0$ for every $c \in \mathbb{F}_p^\star$ because $f(cx)+g(cy) = c^{k_f}(f(x)+g(y))$. We can then choose a subset $\overline{\mathcal{D}}$ of the set $\mathcal{D}$ such that $\bigcup_{c\in\mathbb{F}_p^\star} c\overline{\mathcal{D}}$ is a partition of $\mathcal{D}$:

$$\mathcal{D} = \mathbb{F}_p^\star\overline{\mathcal{D}} = \{c\overline{(x,y)} \colon c \in \mathbb{F}_p^\star \text{ and } \overline{(x,y)} \in \overline{\mathcal{D}}\}.$$

Thus, $\mathcal{C}_\mathcal{D}$ can be punctured into a shorter one $\mathcal{C}_{\overline{\mathcal{D}}}$ based on the defining set $\overline{\mathcal{D}}$. Since $\#\mathcal{D} = (p-1)\#\overline{\mathcal{D}}$, the length and Hamming weights of the punctured code $\mathcal{C}_{\overline{\mathcal{D}}}$ can be derived from that of $\mathcal{C}_\mathcal{D}$ by dividing by $(p-1)$.

We introduce the parameters of the punctured codes in the following corollaries.

Corollary 3.22 *Let $f,g \in WRP$ with $l_f = l_g$ and $k_f = k_g$. Let $\mathcal{C}_\mathcal{D}$ be the 3-weight code proposed in Theorem 3.13. Then, its punctured code $\mathcal{C}_{\overline{\mathcal{D}}}$ with parameters $[(p^{2n-1}-1)/(p-1), 2n, p^{2n-2} - \sqrt{p}^{2n+s_f+s_g-3}]$ is the 3-weight linear code with weight distribution listed in Table 8.*

Table 8. The code $\mathcal{C}_{\overline{\mathcal{D}}}$ in Corollary 3.22 when m is odd and $k_f = k_g$.

Hamming weight ω	Multiplicity A_ω
0	1
p^{2n-2}	$p^{2n} - p^r + p^{r-1} - 1$
$p^{2n-2} - \epsilon_f\epsilon_g\sqrt{p^*}^{m-3}$	$\frac{(p-1)}{2}(p^{r-1} + \epsilon_f\epsilon_g\eta_0(-1)\frac{1}{p}\sqrt{p^*}^{r+1})$
$p^{2n-2} + \epsilon_f\epsilon_g\sqrt{p^*}^{m-3}$	$\frac{(p-1)}{2}(p^{r-1} - \epsilon_f\epsilon_g\eta_0(-1)\frac{1}{p}\sqrt{p^*}^{r+1})$

As examples, we give the following punctured codes, which are almost optimal.

Example 3.23 *The punctured code $\mathcal{C}_{\overline{\mathcal{D}}}$ of the code given in Example 3.15 is the 3-weight ternary $[13,4,6]$ code with $1 + 12y^6 + 62y^9 + 6y^{12}$. This punctured code is almost optimal ternary code because the best ternary code with length 13 and dimension 4 has $d = 7$ according to the online Database of Grassl [13].*

Example 3.24 *The punctured code $\mathcal{C}_{\overline{\mathcal{D}}}$ of the code given in Example 3.16 is the 3-weight ternary $[121,6,72]$ minimal code with $1 + 90y^{72} + 566y^{81} + 72y^{90}$. Note that $d = 78$ for the best ternary code with length 121 and dimension 6 in [13].*

Corollary 3.25 *Let $f, g \in WRP$ with $k_f = k_g$ and $l_f = l_g$. Let $\mathcal{C}_{\mathcal{D}}$ be the 3-weight code proposed in Theorem 3.17. Then, its punctured code $\mathcal{C}_{\overline{\mathcal{D}}}$ with parameters $[(p^{2n-1}-1)/(p-1)+\epsilon_f\epsilon_g\frac{1}{p}\sqrt{p^*}^{2n+s_f+s_g}, 2n]$ is the 3-weight linear code with weight distribution listed in Table 9.*

Table 9. The code $\mathcal{C}_{\overline{\mathcal{D}}}$ in Corollary 3.25 when m is even, $k_f = k_g$ and $l_f = l_g$.

Hamming weight ω	Multiplicity A_ω
0	1
$p^{2n-2} + \epsilon_f\epsilon_g(p-1)\sqrt{p^*}^{m-4}$	$p^{2n} - p^r$
p^{2n-2}	$p^{r-1} + \epsilon_f\epsilon_g\frac{1}{p}(p-1)\sqrt{p^*}^r - 1$
$p^{2n-2} + \epsilon_f\epsilon_g\frac{1}{p}\sqrt{p^*}^m$	$(p-1)(p^{r-1} - \epsilon_f\epsilon_g\frac{1}{p}\sqrt{p^*}^r)$

Corollary 3.26 *Let $f, g \in WRPB$ with $k_f = k_g$ and $l_f = l_g$. Let $\mathcal{C}_{\mathcal{D}}$ be the 3-weight code proposed in Theorem 3.21. Then, its punctured code $\mathcal{C}_{\overline{\mathcal{D}}}$ with parameters $[(p^{2n-1}-1)/(p-1), 2n]$ is the 3-weight linear code with weight distribution listed in Table 10.*

Table 10. The code $\mathcal{C}_{\overline{\mathcal{D}}}$ in Corollary 3.26 when m is even, $k_f = k_g$ and $l_f = l_g$.

Hamming weight ω	Multiplicity A_ω
0	1
p^{2n-2}	$p^{2n} - p^r - 1$
$p^{2n-2} - \epsilon_f\epsilon_g(p-1)\sqrt{p^*}^{m-4}$	$p^{r-1} + \epsilon_f\epsilon_g\frac{1}{p}(p-1)\sqrt{p^*}^r$
$p^{2n-2} + \epsilon_f\epsilon_g\sqrt{p^*}^{m-4}$	$(p-1)(p^{r-1} - \epsilon_f\epsilon_g\frac{1}{p}\sqrt{p^*}^r)$

3.5. Minimality of the constructed codes

In this subsection, we show that the constructed codes are minimal and investigate the minimum Hamming distances of their dual codes.

A linear code $\mathcal{C}$ is *minimal* if every nonzero codeword $\mathbf{v}$ in $\mathcal{C}$ covers only the codewords $j\mathbf{v}$ for all $j \in \mathbb{F}_p$. The following lemma introduces the well-known sufficient condition on the minimal codes.

Lemma 3.27 *(Ashikhmin-Barg) [1] Let $\mathcal{C}$ be a linear code over $\mathbb{F}_p$ and let $w_{\min}$ and $w_{\max}$ represent, respectively, the minimum and maximum Hamming weights of $\mathcal{C}$. Then, $\mathcal{C}$ is minimal if*

$$\frac{p-1}{p} < \frac{w_{\min}}{w_{\max}}. \tag{3.9}$$

By (3.9), our linear codes are minimal codes for almost all integers s_f and s_g with $0 \le s_f, s_g < n$. The following proposition gives the bounds on the integers s_f and s_g that make the associated codes are minimal.

Proposition 3.28 *We have the following bounds on the parameters.*

i.) *The code* $\mathcal{C}_{\mathcal{D}}$ *in Theorem 3.4 is minimal for* $0 \le s_g \le n-4$ *if* $n+s_g$ *is even; otherwise, it is minimal for* $0 \le s_g \le n-3$ *and* $4 \le n$.

ii.) *The code* $\mathcal{C}_{\mathcal{D}}$ *in Theorem 3.13 is minimal when* $0 \le s_f + s_g \le 2n-4$ *and* $3 \le n$.

iii.) *The codes* $\mathcal{C}_{\mathcal{D}}$ *proposed in both Theorems 3.17 and 3.21 are minimal for* $0 \le s_f + s_g \le 2n-4$ *if we have* $\epsilon_f \epsilon_g \eta_0^{(2n+s_f+s_g)/2}(-1) = 1$; *otherwise, they are minimal for* $0 \le s_f + s_g \le 2n-6$.

Remark 3.29 *Our punctured codes are minimal for almost all cases.*

Since our codes are minimal, we can describe the access structures of the secret sharing schemes based on their dual codes as described in [4, Theorem 17]. We first consider the minimum distances $d^{\perp}$ of the dual codes of our minimal codes.

For the codes $\mathcal{C}_{\mathcal{D}}$ constructed in Theorems 3.4, 3.13, 3.17 and 3.21, their dual codes $\mathcal{C}_{\mathcal{D}}^{\perp}$ have $d^{\perp} = 2$ due to the fact that two entries of each codeword in $\mathcal{C}_{\mathcal{D}}$ are linearly dependent iff the minimum distance $d^{\perp}$ of $\mathcal{C}_{\mathcal{D}}^{\perp}$ is equal to 2. This suggests that these minimal codes can be used to design high democratic secret sharing schemes with good access structures as introduced in [4, Theorem 17] (and developed in [10, Proposition 2]). On the other hand, for the punctured codes $\mathcal{C}_{\overline{\mathcal{D}}}$ given in Corollaries 3.22, 3.25 and 3.26, the minimum distances of their dual codes are at least 3 since no two of the vectors are dependent. This means that the punctured codes are projective minimal codes. The proposed projective 3-weight codes can be employed to design association schemes introduced in [3]. Additionally, they can be employed to design democratic secret sharing schemes as introduced in [4, Theorem 17].

4. Conclusion

In this paper, motivated by the works of [14, 17, 28], to construct minimal codes, we consider weakly regular plateaued functions in the recent construction method of linear codes. In conclusion, the main results of the paper can be summarized as follows.

- We construct new infinite classes of 3-weight and 4-weight linear codes from the classes *WRP* and *WRPB* of plateaued functions over $\mathbb{F}_p$. To find the Hamming weights of nonzero codewords, we benefit from the exponential sums and Walsh spectrum of the employed functions. To determine the weight distributions of the proposed codes, we use the exponential sums and Walsh distributions of functions f, g as well as the sizes of the pre-image sets of the associated functions $f^{\star}$ and $g^{\star}$ on the Walsh supports $\mathcal{S}_f$ and $\mathcal{S}_g$.

- We derive 3-weight punctured codes from the constructed codes, by deleting some special coordinates in the defining set. Note that they contain almost optimal codes due to the Griesmer bound.

- We show that our obtained codes are minimal, which says that they can be used to design high democratic secret sharing schemes with new parameters under the framework introduced in [10, Proposition 2].

- We lastly consider the minimum distances of the dual codes of our minimal codes. We conclude that the proposed 3-weight punctured codes are projective, and, hence, they can be used to design association schemes in [3].

References

[1] Ashikhmin A, Barg A. Minimal vectors in linear codes. IEEE Transactions on Information Theory 1998; 44 (5): 2010-2017.

[2] Bosma W, Cannon J, Playoust C. The Magma algebra system I: The user language Journal of Symbolic Computation 1997; 24 (3): 235-265.

[3] Calderbank A, Goethals J. Three-weight codes and association schemes. Philips Journal of Research 1984; 39 (4-5): 143-152.

[4] Carlet C, Ding C, Yuan J. Linear codes from perfect nonlinear mappings and their secret sharing schemes. IEEE Transactions on Information Theory 2005; 51 (6): 2089-2102.

[5] Çeşmelioğlu A, Meidl W. A construction of bent functions from plateaued functions. Designs, Codes and Cryptography 2013; 66 (1): 231-242.

[6] Cheng Y, Cao X. Linear codes with few weights from weakly regular plateaued functions. Discrete Mathematics 2021; 344 (12): 112597.

[7] Ding, C. Linear codes from some 2-designs. IEEE Transactions on Information Theory 2015; 61 (6): 3265-3275.

[8] Ding C. A construction of binary linear codes from Boolean functions. Discrete mathematics 2016; 339 (9): 2288-2303.

[9] Ding C, Niederreiter H. Cyclotomic Linear Codes of Order 3. IEEE Transactions on Information Theory 2007; 53 (6): 2274-2277.

[10] Ding C, Yuan J. Covering and secret sharing with linear codes. In: International Conference on Discrete Mathematics and Theoretical Computer Science (DMTCS); Dijon, France; 2003. pp. 11-25.

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

[12] Ding K, Ding C. A class of two-weight and three-weight codes and their applications in secret sharing. IEEE Transactions on Information Theory 2015; 61 (11): 5835-5842.

[13] Grassl M. Bounds on the minimum distance of linear codes and quantum codes. www.codetables.de (2019), Accessed April 2021.

[14] Jian G, Lin Z, Feng R. Two-weight and three-weight linear codes based on Weil sums. Finite Fields and Their Applications 2019; 57: 92-107.

[15] Kumar P, Scholtz R, Welch L. Generalized bent functions and their properties. Journal of Combinatorial Theory Series A 1985; 40 (1): 90-107.

[16] Li C, Li N, Helleseth T, Ding C. The weight distributions of several classes of cyclic codes from APN monomials. IEEE Transactions on Information Theory 2014; 60 (8): 4710-4721.

[17] Li C, Yue Q, Fu FW. A construction of several classes of two-weight and three-weight linear codes. Applicable Algebra in Engineering, Communication and Computing 2017; 28 (1): 11-30.

[18] Li N, Mesnager S. Recent results and problems on constructions of linear codes from cryptographic functions. Cryptography and Communications 2020; 12: 965-986.

[19] Lidl R, Niederreiter H. Finite fields. 2nd Edition. Cambridge, UK: Cambridge University Press, 1997.

[20] Mesnager S. Linear codes from functions. In: Huffman WC, Kim JL, Solé P (editors). A Concise Encyclopedia of Coding Theory 2021. Chapman and Hall/CRC Press Taylor and Francis Group, London, New York 2021, pp. 463-526.

[21] Mesnager S. Linear codes with few weights from weakly regular bent functions based on a generic construction. Cryptography and Communications 2017; 9 (1): 71-84.

[22] Mesnager S, Özbudak F, Sınak A. Linear codes from weakly regular plateaued functions and their secret sharing schemes. Designs, Codes and Cryptography 2019; 87 (2-3): 463-480.

[23] Mesnager S, Sınak A. Several Classes of Minimal Linear Codes With Few Weights From Weakly Regular Plateaued Functions. IEEE Transactions on Information Theory 2020; 66 (4): 2296-2310.

[24] Rothaus, O. On "bent" functions. Journal of Combinatorial Theory Series A 1976; 20 (3): 300-305.

[25] Sınak A. Minimal linear codes from weakly regular plateaued balanced functions. Discrete Mathematics 2021; 344 (3): 112215.

[26] 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 2016; 62 (3): 1166-1176.

[27] Tang C, Xiang C, Feng K. Linear codes with few weights from inhomogeneous quadratic functions. Designs, Codes and Cryptography 2017; 83 (3): 691-714.

[28] Wu Y, Li N, Zeng X. Linear codes with few weights from cyclotomic classes and weakly regular bent functions. Designs, Codes and Cryptography 2020; 88: 1255-1272.

[29] Zeng X, Shan J, Hu L. A triple-error-correcting cyclic code from the Gold and Kasami–Welch APN power functions. Finite Fields and Their Applications 2012; 18 (1): 70-92.

[30] Zheng Y, Zhang XM. On plateaued functions. IEEE Transactions on Information Theory 2001; 47 (3): 1215-1223.

[31] Zhou Z, Li N, Fan C, Helleseth T. Linear codes with two or three weights from quadratic bent functions. Designs, Codes and Cryptography 2016; 81 (2): 283–295.