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

Ahmet Sınak[1,2]

[1] Department of Mathematics and Computer Science, Necmettin Erbakan University, 42090, Konya, Turkey
[2] LAGA, Universities of Paris VIII and Paris XIII, CNRS, UMR 7539, Paris, France
sinakahmet@gmail.com

Abstract. The construction of linear codes from functions over finite fields has been extensively studied in the literature since determining the parameters of linear codes based on functions is rather easy due to the nice structure of functions. In this paper, we derive 3-weight and 4-weight linear codes from weakly regular plateaued unbalanced functions in the recent construction method of linear codes over the finite fields of odd characteristics. The Hamming weights and their weight distributions for proposed codes are determined by using the Walsh transform values and Walsh distribution of the employed functions, respectively. We next 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 obtain association schemes. We also derive projective 2-weight and 3-weight subcodes with flexible dimensions from partially bent functions, and these subcodes can be employed to design strongly regular graphs. We finally show that all constructed codes are minimal, which approve that they can be employed to design high democratic secret sharing schemes.

Keywords: Linear code · minimal code · weight distribution · weakly regular plateaued function · unbalanced function

1 Introduction

Linear codes with few weights have a wide range of applications in practical systems. There are many construction methods for linear codes, one of them is derived from functions over finite fields. Constructing linear codes from functions is still a popular research topic in the literature although considerable progress has been done in this direction. A large number of linear codes have been constructed from popular cryptographic functions including quadratic functions [9,10,13,14,29,33], (weakly regular) bent functions [9,10,24,28,30,33], (almost) perfect nonlinear functions [6,20,31] and (weakly regular) plateaued functions [9,23,25,26]. Two generic (say, *first* and *second*) construction methods of linear codes from functions can be isolated from the others in the literature. In the past two decades, several linear codes with excellent parameters have been derived from cryptographic functions based on the first generic construction method (*e.g.* [6,10,24,25]) and the second generic construction method (*e.g.* [10,14,28,29,33]). Recently, weakly regular plateaued (especially, bent) functions have been employed to design (minimal) linear codes with a few weights over odd characteristic finite fields ([23,24,25,26,28,30]). In this paper, motivated by [19,30], we use some unbalanced weakly regular plateaued functions so that we can get new minimal linear codes with flexible parameters. It is worth noting that a very nice survey [21] written by Li and Mesnager is devoted to the construction methods of linear codes from cryptographic functions over finite fields.

The rest of this paper is structured 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. Section 4 is devoted to proposing subcodes and punctured codes for the constructed codes. We hereby obtain projective 2-weight and 3-weight codes with flexible parameters. In Section 5, we highlight that our codes are minimal, and so secret sharing schemes based on their dual codes have interesting access structures.

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 $q = p^n$ 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 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 $\sigma_a(\sqrt{p^*}^{\,n}) = {\eta_0}^n(a)\sqrt{p^*}^{\,n}$. The following lemma is frequently used in the subsequent proofs.

Lemma 1. *[22] Under the above notation, we have the following facts.*

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

2.1 Linear codes

An $[n, k, d]$ linear code $\mathcal{C}$ over $\mathbb{F}_p$ is a k-dimensional subspace of the n-dimensional 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 $\mathbf{v} = (v_1, \ldots, v_n) \in \mathbb{F}_p^n$, its Hamming weight $W_H(\mathbf{v})$ is the size of its support defined 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 elements (codewords) of $\mathcal{C}$. The *dual code* of $\mathcal{C}$ is defined to be the set

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

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 $(1,A_1,\ldots,A_n)$ and its *weight enumerator* is denoted by 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 $\{A_i\}_{i\geq 1}$ is equal to l, where l is an integer with $1\leq l\leq n$.

2.2 Weakly regular plateaued functions

Let $f:\mathbb{F}_q\longrightarrow\mathbb{F}_p$ 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; otherwise, f is said to be *unbalanced*. Note that f is balanced iff $\mathcal{W}_f(0)=0$.

A function f is called *bent* if $|\mathcal{W}_f(\beta)|^2=p^n$ for every $\beta\in\mathbb{F}_q$ (see [27] for Boolean bent and [18] 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 $0\leq s\leq n$, (see [32] for Boolean plateaued and [8] for p-ary plateaued). A plateaued function f is the *partially bent function* if $f(x+a)-f(x)$ is balanced or constant for all $a\in\mathbb{F}_{p^n}$. The notion of partially bent Boolean functions was firstly defined by Carlet [5]. In particular, a 0-plateaued function is the bent function. For an s-plateaued f, its *Walsh support* is described as the set $\mathcal{S}_f=\{\beta\in\mathbb{F}_q\colon\ |\mathcal{W}_f(\beta)|^2=p^{n+s}\}$. A plateaued function with affine Walsh support is trivially the partially bent function. From the Parseval identity, we have $\#\mathcal{S}_f=p^{n-s}$, and also its explicit Walsh distribution is given as follows.

Lemma 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. [25] have recently described the notion of weakly regular plateaued functions. An s-plateaued f is said to be *weakly regular* if we have

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

where $u\in\{\pm1,\pm i\}$, $f^\star$ 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 3. *[25] Let f be a weakly regular s-plateaued function. Then, we have*

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

for every $\beta \in \mathcal{S}_f$, where $\epsilon_f \in \{\pm 1\}$ 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 4. *[26] Let f be a weakly regular s-plateaued function. For $x \in \mathbb{F}_q$,*

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

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. *[26] Let f be a weakly regular s-plateaued function with $\mathcal{W}_f(\beta) = \epsilon_f \sqrt{p^*}^{\,n+s} \xi_p^{f^\star(\beta)}$ for every $\beta \in \mathcal{S}_f$, where $\epsilon_f = \pm 1$ is the sign of $\mathcal{W}_f$. For $j \in \mathbb{F}_p$, define $\mathcal{N}_{f^\star}(j) = \#\{\beta \in \mathcal{S}_f :\ f^\star(\beta) = j\}$. Then we have*

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

when $n - s$ is even; otherwise,

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

Mesnager et al. [26] have very recently introduced the subclass *WRP* of the class of weakly regular plateaued functions over odd characteristic finite fields. For an integer s_f with $0 \le s_f \le n$, *WRP* defines the set of weakly regular s_f-plateaued unbalanced functions $f : \mathbb{F}_q \to \mathbb{F}_p$ 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 a positive even integer with $\gcd(k_f - 1, p - 1) = 1$.

In this paper, to construct linear codes with new parameters, we use a large class *WRP* of functions in the recent construction method of [17,19,30] based on the second generic construction method. The class *WRP* is a non-trivial and non-empty set of functions since for example, all quadratic unbalanced functions belong to this class.

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

Proposition 1. *[26] If $f \in WRP$, 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 a positive even integer with $\gcd(l_f - 1, p - 1) = 1$.*

Lemma 6. *[26] If $f \in WRP$, then for every $\beta \in \mathcal{S}_f$ (resp., $\beta \in \mathbb{F}_q \setminus \mathcal{S}_f$), we have $z\beta \in \mathcal{S}_f$ (resp., $z\beta \in \mathbb{F}_q \setminus \mathcal{S}_f$) for every $z \in \mathbb{F}_p^\star$.*

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

In this section, weakly regular plateaued unbalanced 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 method of linear codes is given by

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

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

$$\mathcal{C}_D = \{(\mathrm{Tr}^n(ad_1), \ldots, \mathrm{Tr}^n(ad_m))\colon\ a \in \mathbb{F}_q\}, \tag{1}$$

whose length is m and dimension is at most n. The set D is called the *defining set* of $\mathcal{C}_D$, and the quality of $\mathcal{C}_D$ depends on the choice of D. The construction method of the form (1) has been initially studied by Ding et al. [11,12], and many linear codes have been proposed in [9,10,11,12,13,14]. Furthermore, new linear codes have been obtained from some cryptographic functions in this construction method (see *e.g.* [23,26,29,28,33]). Motivated by the method of the form (1), for a subset $\mathcal{D} = \{(x_1, y_1), \ldots, (x_m, y_m)\} \subseteq \mathbb{F}_q^2$, Li et al. [19] have defined the following linear code

$$\mathcal{C}_\mathcal{D} = \{\mathbf{c}_{(a,b)} = (\mathrm{Tr}^n(ax_1 + by_1), \ldots, \mathrm{Tr}^n(ax_m + by_m))\colon\ a, b \in \mathbb{F}_q\}, \tag{2}$$

whose length is m and dimension at most $2n$. They have then 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 $k, l \in \{1, 2, p^{n/2} + 1\}$. Recently, Jian et al. [17] have constructed further linear codes of the form (2) by using the defining set $\mathcal{D} = \{(x, y) \in \mathbb{F}_q^2 \setminus \{(0, 0)\}\colon\ \mathrm{Tr}^n(x^k + y^{p^u+1}) = 0\}$, where $k \in \{1, 2\}$. Very recently, Wu et al. [30] have constructed new linear codes of the form (2) based on the set

$$\mathcal{D} = \{(x, y) \in \mathbb{F}_q^2 \setminus \{(0, 0)\}\colon\ f(x) + g(y) = 0\} \subset \mathbb{F}_q^2, \tag{3}$$

where f and g are two weakly regular bent functions from $\mathbb{F}_q$ to $\mathbb{F}_p$. Motivated by the works [17,19,30], we in this paper construct minimal linear codes of the form (2) based on the set $\mathcal{D}$ of the form (3) for the following two cases:

1) $f(x) = \mathrm{Tr}^n(x)$ and $g(y) \in WRP$,
2) both $f(x) \in WRP$ and $g(y) \in WRP$.

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). From the definition of the code $\mathcal{C}_\mathcal{D}$ of the form (2), we define

$$\mathcal{N}(a,b) = \#\{(x,y) \in \mathbb{F}_q^2 \setminus \{(0,0)\} \colon f(x) + g(y) = 0 \text{ and } \mathrm{Tr}^n(ax+by) = 0\} \tag{4}$$

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

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

In this subsection, we construct the linear code $\mathcal{C}_\mathcal{D}$ of the form (2) for the defining set $\mathcal{D}$ of the form (3) when $f(x) = \mathrm{Tr}^n(x)$ and $g(y) \in WRP$, where g is an s_g-plateaued function with $0 \le s_g \le n$.

We introduce a couple of lemmas to find the Hamming weights of the code $\mathcal{C}_\mathcal{D}$. We first derive the following one from the proof of [30, Lemma 5].

Lemma 7. *[30] Let $\mathcal{N}(a,b)$ be defined as in (4) for $(a,b) \in (\mathbb{F}_q^2)^\star$. Then, $\mathcal{N}(a,b) = p^{2n-2} - 1 + \frac{A}{p^2}$, where*

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

Moreover, if $a \in \mathbb{F}_q \setminus \mathbb{F}_p^\star$ then we have $A = 0$, if $a \in \mathbb{F}_p^\star$ then

$$A = p^n \sum_{z_1 \in \mathbb{F}_p^\star} \sigma_{z_1}\left(\sum_{y \in \mathbb{F}_q} \xi_p^{g(y) - \mathrm{Tr}^n(\frac{b}{a}y)}\right). \tag{5}$$

The following lemma calculates the value A by using the Walsh spectrum of the employed function.

Lemma 8. *Let $g \in WRP$ and A be defined as in (5) for $a \in \mathbb{F}_p^\star$ and $b \in \mathbb{F}_q$. Then, for every $\frac{b}{a} \in \mathbb{F}_q \setminus \mathcal{S}_g$ we have $A = 0$, and for every $\frac{b}{a} \in \mathcal{S}_g$*

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

when $n + s_g$ is even; otherwise,

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

Proof. When $\frac{b}{a} \in \mathbb{F}_q \setminus \mathcal{S}_g$, we clearly get $A = 0$. When $\frac{b}{a} \in \mathcal{S}_g$, we have

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

where Lemma 3 is used in the second equality. The proof is completed from Lemma 1. □

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

Lemma 9. *Let $g \in WRP$ and $\mathcal{N}(a,b)$ be defined as in (4) for $(a,b) \in (\mathbb{F}_q^2)^\star$. Then, we have $\mathcal{N}(a,b) = p^{2n-2} - 1$ if $a \in \mathbb{F}_q \setminus \mathbb{F}_p^\star$ or if $\frac{b}{a} \notin \mathcal{S}_g$ for $a \in \mathbb{F}_p^\star$. For every $\frac{b}{a} \in \mathcal{S}_g$ for $a \in \mathbb{F}_p^\star$, we have*

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

when $n + s_g$ is even; otherwise,

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

Proof. The proof follows from the combination of Lemmas 7 and 8. □

The following theorem proposes the code $\mathcal{C}_\mathcal{D}$ of the form (2) based on the set

$$\mathcal{D} = \{(x,y) \in \mathbb{F}_q^2 \setminus \{(0,0)\} \colon \operatorname{Tr}^n(x) + g(y) = 0\}, \tag{6}$$

where $g(y) \in WRP$. We can calculate its size $\#\mathcal{D} = p^{2n-1} - 1$ from the orthogonality of exponential sums.

Theorem 1. *Let $\mathcal{D}$ be defined as in (6) and $g \in WRP$. Then, the code $\mathcal{C}_\mathcal{D}$ of the form (2) is a 3-weight linear $[p^{2n-1} - 1, 2n]$ code over $\mathbb{F}_p$. All parameters are listed in Tables 1 and 2 when $n + s_g$ is even and odd, respectively.*

Proof. From the definition of $\mathcal{C}_\mathcal{D}$, its length is the size of $\mathcal{D}$, and for every $(a,b) \in (\mathbb{F}_q^2)^\star$, its Hamming weight $W_H(\mathbf{c}_{(a,b)}) = \#\mathcal{D} - \mathcal{N}(a,b)$, where $\mathcal{N}(a,b)$ is defined as in (4). Then the Hamming weights can be obtained from Lemma 9. If $a \in \mathbb{F}_q \setminus \mathbb{F}_p^\star$ or if $\frac{b}{a} \notin \mathcal{S}_g$ for $a \in \mathbb{F}_p^\star$, then we have $W_H(\mathbf{c}_{(a,b)}) = (p-1)p^{2n-2}$, and its weight distribution is $p^{2n} - (p-1)p^{n-s_g} - 1$ by Lemma 2. Additionally, for every $\frac{b}{a} \in \mathcal{S}_g$ for $a \in \mathbb{F}_p^\star$, we have

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

when $n+s_g$ is even; otherwise,

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

In this case, the weight distribution of each weight is derived from Lemma 5. All Hamming weights and their weight distributions are given in Tables 1 and 2, completing the proof. □

We below give an example of the code $\mathcal{C}_{\mathcal{D}}$ constructed in Theorem 1, which is verified by MAGMA in [2].

Example 1. The function $g : \mathbb{F}_{3^4} \to \mathbb{F}_3$ defined as $g(x) = \mathrm{Tr}^4(2x^{92})$ is weakly regular 2-plateaued function from *WRP*, and $\mathcal{W}_g(\beta) \in \{0, \epsilon_g \eta_0^3(-1)3^3\xi_3^{g^\star(\beta)}\}$, where $\epsilon_g = 1$ and $g^\star$ is a function with $g^\star(0) = 0$. Then, $\mathcal{C}_{\mathcal{D}}$ is a 3-weight minimal ternary $[2186, 8, 1215]$ code with the weight enumerator $1 + 16y^{1215} + 6542y^{1458} + 2y^{1944}$.

Remark 1. When g is a weakly regular 0-plateaued (bent) function in Theorem 1, one can easily obtain the linear code given in [30, Theorem 3].

3.3 Three-weight and four-weight linear codes derived from $f(x), g(y) \in WRP$

In this subsection, we construct the linear code $\mathcal{C}_{\mathcal{D}}$ of the form (2) based on the set

$$\mathcal{D} = \{(x,y) \in \mathbb{F}_q^2 \setminus \{(0,0)\} \colon \; f(x) + g(y) = 0\}, \tag{7}$$

where $f, g \in WRP$ are s_f-plateaued and s_g-plateaued functions from $\mathbb{F}_q$ to $\mathbb{F}_p$, respectively, for $0 \le s_f, s_g \le n$.

We first introduce three lemmas by using the exponential sums and Walsh spectrum of a weakly regular plateaued function. They are needed to compute the lengths, weights, and weight distributions of codes.

We begin with finding the size of the set $\mathcal{D}$ of the form (7) by using the Walsh transform values of the functions at the zero points.

Lemma 10. *Let $\mathcal{D}$ be defined as in (7) and let $f, g \in WRP$. Then*

$$\#\mathcal{D} = \begin{cases} p^{2n-1} - 1, & \text{if } 2n + s_f + s_g \text{ is odd}, \\ p^{2n-1} - 1 + \epsilon_f \epsilon_g \frac{p-1}{p} \sqrt{p^*}^{2n+s_f+s_g}, & \text{if not.} \end{cases}$$

Proof. We can write $\mathcal{W}_f(0) = \epsilon_f \sqrt{p^*}^{\,n+s_f}$ and $\mathcal{W}_g(0) = \epsilon_g \sqrt{p^*}^{\,n+s_g}$ from Lemma 3, where $\epsilon_f, \epsilon_g \in \{\pm 1\}$, since we know $f^\star(0) = g^\star(0) = 0$ from Proposition 1. Hence, from the orthogonality of exponential sums, we have

$$
\begin{aligned}
\#\mathcal{D}+1 &= \tfrac{1}{p}\sum_{x,y\in\mathbb{F}_q}\sum_{z\in\mathbb{F}_p}\xi_p^{z(f(x)+g(y))}\\
&= \tfrac{1}{p}\left(p^{2n}+\sum_{z\in\mathbb{F}_p^\star}\sigma_z(\sum_{x\in\mathbb{F}_q}\xi_p^{f(x)}\sum_{y\in\mathbb{F}_q}\xi_p^{g(y)})\right)\\
&= \tfrac{1}{p}\left(p^{2n}+\sum_{z\in\mathbb{F}_p^\star}\sigma_z(\epsilon_f\epsilon_g\sqrt{p^*}^{2n+s_f+s_g})\right)\\
&= \tfrac{1}{p}\left(p^{2n}+\epsilon_f\epsilon_g\sqrt{p^*}^{2n+s_f+s_g}\sum_{z\in\mathbb{F}_p^\star}\eta_0^{2n+s_f+s_g}(z)\right)\\
&= \begin{cases} p^{2n-1}, & \text{if } 2n+s_f+s_g \text{ is odd},\\ p^{2n-1}+\epsilon_f\epsilon_g\frac{p-1}{p}\sqrt{p^*}^{2n+s_f+s_g}, & \text{if not,}\end{cases}
\end{aligned}
$$

where Lemma 1 is used in the last equality, thereby completing the proof. □

Lemma 11. *Let $f,g\in WRP$ and l_f,l_g be defined as in Proposition 1. For $(a,b)\in(\mathbb{F}_q^2)^\star$, define*

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

Then, we have $B=0$ for $(a,b)\notin\mathcal{S}_f\times\mathcal{S}_g$, and for $(a,b)\in\mathcal{S}_f\times\mathcal{S}_g$, we have two distinct cases.

- *When $2n+s_f+s_g$ is odd, we have*

$$B=\begin{cases}0, & \text{if } ab\neq 0 \text{ or } b=f^\star(a)=0 \text{ or } a=g^\star(b)=0,\\ \epsilon_f\epsilon_g(p-1)\sqrt{p^*}^{2n+s_f+s_g+1}, & \text{if } b=0 \text{ and } f^\star(a)\in SQ \text{ or } a=0 \text{ and } g^\star(b)\in SQ,\\ -\epsilon_f\epsilon_g(p-1)\sqrt{p^*}^{2n+s_f+s_g+1}, & \text{if } b=0 \text{ and } f^\star(a)\in NSQ \text{ or } a=0 \text{ and } g^\star(b)\in NSQ.\end{cases}$$

- *When $2n+s_f+s_g$ is even, we have for $l_f=l_g$*

$$B=\begin{cases}\epsilon_f\epsilon_g(p-1)^2\sqrt{p^*}^{2n+s_f+s_g}, & \text{if } C_1,\\ -\epsilon_f\epsilon_g(p-1)\sqrt{p^*}^{2n+s_f+s_g}, & \text{otherwise,}\end{cases}$$

  and for $l_f\neq l_g$

$$B=\begin{cases}\epsilon_f\epsilon_g(p-1)^2\sqrt{p^*}^{2n+s_f+s_g}, & \text{if } C_2,\\ \epsilon_f\epsilon_g(p+1)\sqrt{p^*}^{2n+s_f+s_g}, & \text{if } -\frac{f^\star(a)}{g^\star(b)}\in SQ,\\ -\epsilon_f\epsilon_g(p-1)\sqrt{p^*}^{2n+s_f+s_g}, & \text{otherwise,}\end{cases}$$

  where C_1 is the condition $a=g^\star(b)=0$ or $b=f^\star(a)=0$ or $f^\star(a)+g^\star(b)=0$ for $ab\neq 0$, and C_2 is the condition $a=g^\star(b)=0$ or $b=f^\star(a)=0$ or $f^\star(a)=g^\star(b)=0$ for $ab\neq 0$.

Proof. From the definition of B, we have

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

where we use the fact that $\frac{z_2}{z_1}$ runs all over $\mathbb{F}_p^\star$ for a fixed z_1 when z_2 runs through $\mathbb{F}_p^\star$ in the first equality. For every $(a,b)\notin\mathcal{S}_f\times\mathcal{S}_g$, i.e., $(z_2a,z_2b)\notin\mathcal{S}_f\times\mathcal{S}_g$ for every $z_2\in\mathbb{F}_p^\star$ by Lemma 6, we can see that $B=0$. For every $(a,b)\in\mathcal{S}_f\times\mathcal{S}_g$, i.e., $(z_2a,z_2b)\in\mathcal{S}_f\times\mathcal{S}_g$, 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

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

where we use Lemmas 3, 6 and Proposition 1 in the first and second equality, respectively. With the help of Lemma 1, we get

$$B=\begin{cases}0, & \text{if } g^\star(b)=0,\\ \epsilon_f\epsilon_g(p-1)\sqrt{p^*}^{2n+s_f+s_g+1}, & \text{if } g^\star(b)\in SQ,\\ -\epsilon_f\epsilon_g(p-1)\sqrt{p^*}^{2n+s_f+s_g+1}, & \text{if } g^\star(b)\in NSQ,\end{cases}$$

when $2n+s_f+s_g$ is odd; otherwise,

$$B=\begin{cases}\epsilon_f\epsilon_g(p-1)^2\sqrt{p^*}^{2n+s_f+s_g}, & \text{if } g^\star(b)=0,\\ -\epsilon_f\epsilon_g(p-1)\sqrt{p^*}^{2n+s_f+s_g}, & \text{if not.}\end{cases}$$

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

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

where we use Lemmas 3, 6 and Proposition 1 in the first and second equality, respectively. We hence compute B by using Lemma 1 and also some properties of the cyclotomic field and quadratic character η_0. When $2n+s_f+s_g$ is odd, we make that $B=0$. When $2n+s_f+s_g$ is even, we get for $l_f=l_g$

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

and for $l_f\neq l_g$

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

The proof is then complete. □

The following lemma helps to compute the weights and their weight distributions.

Lemma 12. *Let $\mathcal{N}(a,b)$ be defined as in (4) for $(a,b)\in(\mathbb{F}_q^2)^\star$, and l_f,l_g be defined as in Proposition 1.*

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

$$\mathcal{N}(a,b)=\begin{cases}p^{2n-2}-1, & \text{if } ab\neq 0 \text{ or } b=f^\star(a)=0 \text{ or } a=g^\star(b)=0,\\ p^{2n-2}-1+E, & \text{if } b=0 \text{ and } f^\star(a)\in SQ \text{ or } a=0 \text{ and } g^\star(b)\in SQ,\\ p^{2n-2}-1-E, & \text{if } b=0 \text{ and } f^\star(a)\in NSQ \text{ or } a=0 \text{ and } g^\star(b)\in NSQ,\end{cases}$$

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

$$\mathcal{N}(a,b)=\begin{cases}p^{2n-2}-1+\epsilon_f\epsilon_g\frac{1}{p}(p-1)\sqrt{p^*}^{2n+s_f+s_g}, & \text{if } C_1,\\ p^{2n-2}-1, & \text{otherwise,}\end{cases}$$

and for $l_f\neq l_g$

$$\mathcal{N}(a,b)=\begin{cases}p^{2n-2}-1+\epsilon_f\epsilon_g\frac{1}{p}(p-1)\sqrt{p^*}^{2n+s_f+s_g}, & \text{if } C_2,\\ p^{2n-2}-1+\epsilon_f\epsilon_g\frac{2}{p}\sqrt{p^*}^{2n+s_f+s_g}, & \text{if } -\frac{f^\star(a)}{g^\star(b)}\in SQ,\\ p^{2n-2}-1, & \text{otherwise,}\end{cases}$$

where C_1 is the condition $a=g^\star(b)=0$ or $b=f^\star(a)=0$ or $f^\star(a)+g^\star(b)=0$ for $ab\neq 0$, and C_2 is the condition $a=g^\star(b)=0$ or $b=f^\star(a)=0$ or $f^\star(a)=g^\star(b)=0$ for $ab\neq 0$.

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

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

where

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

We clearly have $A=p(\#\mathcal{D}+1)-p^{2n}$ in the light of Lemma 10. The proof is then complete from Lemmas 10 and 11. □

We now construct the code $\mathcal{C}_\mathcal{D}$ of the form (2) when $2n+s_f+s_g$ is odd.

Theorem 2. *Let $\mathcal{D}$ be defined as in (7), and let $f,g\in$ WRP. Suppose that $n+s_f$ is odd and $n+s_g$ is even. Then, the code $\mathcal{C}_\mathcal{D}$ of the from (2) is a 3-weight linear $[p^{2n-1}-1,2n]$ code whose parameters are listed 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 $W_H(\mathbf{c}_{(a,b)})=\#\mathcal{D}-\mathcal{N}(a,b)$ for every $(a,b)\in(\mathbb{F}_q^2)^\star$, where $\mathcal{N}(a,b)$ is defined as in (4). By Lemma 10, we have $\#\mathcal{D}=p^{2n-1}-1$, and the Hamming weights can be derived from Lemma 12. 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. Additionally, for every $(a,b)\in\mathcal{S}_f\times\mathcal{S}_g$, we get

$$W_H(\mathbf{c}_{(a,b)})=\begin{cases}(p-1)p^{2n-2}, & A_1\text{ times},\\ (p-1)p^{2n-2}-\epsilon_f\epsilon_g\frac{1}{p^2}(p-1)\sqrt{p^*}^{2n+s_f+s_g+1}, & A_2\text{ times},\\ (p-1)p^{2n-2}+\epsilon_f\epsilon_g\frac{1}{p^2}(p-1)\sqrt{p^*}^{2n+s_f+s_g+1}, & A_3\text{ times},\end{cases}$$

whose weight distribution is determined by Lemmas 2, 5 and 12. Firstly, to compute A_1, we define the following three sets: $\{(a,b)\in\mathcal{S}_f^\star\times\mathcal{S}_g^\star\}$, $\{a\in\mathcal{S}_f^\star\colon\ f^\star(a)=0\}$ and $\{b\in\mathcal{S}_g^\star\colon\ g^\star(b)=0\}$. Here, A_1 can be expressed as the sum of the sizes of these sets, and hence by Lemmas 2 and 5, we get $A_1=p^{2n-s_f-s_g}-1-(p-1)(p^{n-s_f-1}+p^{n-s_g-1}-\epsilon_g\epsilon^{n+1}\sqrt{p^*}^{n-s_g-2})$. Similarly, A_2 and A_3 can be expressed as

$$A_2=\#\{a\in\mathcal{S}_f^\star\colon\ f^\star(a)\in SQ\}+\#\{b\in\mathcal{S}_g^\star\colon\ g^\star(b)\in SQ\},$$
$$A_3=\#\{a\in\mathcal{S}_f^\star\colon\ f^\star(a)\in NSQ\}+\#\{b\in\mathcal{S}_g^\star\colon\ g^\star(b)\in NSQ\}.$$

By Lemma 5, $A_2=(\frac{p-1}{2})(p^{n-s_f-1}+p^{n-s_g-1}+\epsilon_f\eta_0^n(-1)\sqrt{p^*}^{n-s_f-1}-\epsilon_g\eta_0^{n+1}(-1)\sqrt{p^*}^{n-s_g-2})$ and $A_3=(\frac{p-1}{2})(p^{n-s_f-1}+p^{n-s_g-1}-\epsilon_f\eta_0^n(-1)\sqrt{p^*}^{n-s_f-1}-\epsilon_g\eta_0^{n+1}(-1)\sqrt{p^*}^{n-s_g-2})$, thereby completing the proof. □

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

Example 2. Let $f, g : \mathbb{F}_{3^2} \to \mathbb{F}_3$ be defined as $f(x) = \mathrm{Tr}^2(\zeta x^4 + \zeta^8 x^2)$ and $g(x) = \mathrm{Tr}^2(x^{10})$, where ζ is a primitive element of $\mathbb{F}_{3^2}$. Then $f, g \in \mathit{WRP}$ with $s_f = 1, s_g = 0$ and $\epsilon_f = \epsilon_g = 1$, and hence $\mathcal{C}_{\mathcal{D}}$ is a 3-weight ternary $[26, 4, 12]$ code with the weight enumerator $1 + 4y^{12} + 70y^{18} + 6y^{24}$.

Example 3. Let $f, g : \mathbb{F}_{3^3} \to \mathbb{F}_3$ be defined as $f(x) = \mathrm{Tr}^3(x^{10})$ and $g(x) = \mathrm{Tr}^3(\zeta x^4 + \zeta^8 x^2)$, where ζ is a primitive element of $\mathbb{F}_{3^3}$. Then $f, g \in \mathit{WRP}$ with $s_f = 0, s_g = 1$ and $\epsilon_f = \epsilon_g = 1$, and hence $\mathcal{C}_{\mathcal{D}}$ is a 3-weight minimal ternary $[242, 6, 144]$ code with $1 + 14y^{144} + 706y^{162} + 8y^{180}$. It is worth noting that this code is better than the code $[242, 6, 135]_3$, which is obtained in [30, Example 6] only from quadratic weakly regular bent $f(x) = \mathrm{Tr}^3(x^{10})$.

The following lemma is needed to determine the weight distribution.

Lemma 13. *Let $f, g \in \mathit{WRP}$, and define $S_{f,g} = \#\{(a, b) \in \mathcal{S}_f \times \mathcal{S}_g \colon\ f^\star(a) + g^\star(b) = 0\}$. Then,*

$$S_{f,g} = \begin{cases} p^{2n-s_f-s_g-1}, & \text{if } 2n - s_f - s_g \text{ odd,} \\ p^{2n-s_f-s_g-1} + \epsilon_f\epsilon_g \frac{p-1}{p} \sqrt{p^*}^{2n-s_f-s_g}, & \text{if not.} \end{cases}$$

Proof. From the orthogonality of exponential sums, we have

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

where Lemma 4 is used in the last equality. The proof is hence complete by Lemma 1. □

We below construct the code $\mathcal{C}_{\mathcal{D}}$ of the form (2) when $2n + s_f + s_g$ is even.

Theorem 3. *Let $\mathcal{D}$ be defined as in (7), and let $f, g \in \mathit{WRP}$. Suppose that $2n + s_f + s_g$ is even and l_f, l_g are defined as in Proposition 1. Then, the code $\mathcal{C}_{\mathcal{D}}$ of the form (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 a 3-weight linear p-ary code over $\mathbb{F}_p$ when $l_f = l_g$,*
- *is a 4-weight linear p-ary code over $\mathbb{F}_p$ for $p > 3$ when $l_f \neq l_g$, in particular, it is a 3-weight ternary code for $p = 3$.*

The Hamming weights are listed in Tables 4 and 5 when $l_f = l_g$ and $l_f \neq l_g$, respectively.

Proof. The length of the code $\mathcal{C}_{\mathcal{D}}$ follows from Lemma 10, and for every $(a, b) \in (\mathbb{F}_q^2)^\star$, the weight $W_H(\mathbf{c}_{(a,b)}) = \#\mathcal{D} - \mathcal{N}(a, b)$ can be obtained from Lemmas 10 and 12. To be more precise, when $(a, b) \notin \mathcal{S}_f \times \mathcal{S}_g$, we have

$$W_H(\mathbf{c}_{(a,b)}) = (p-1)(p^{2n-2} + \epsilon_f\epsilon_g \frac{1}{p^2}(p-1)\sqrt{p^*}^{2n+s_f+s_g}),$$

whose weight distribution is $p^{2n} - p^{2n-s_f-s_g}$ from Lemma 2. In addition, when $(a, b) \in \mathcal{S}_f \times \mathcal{S}_g$, there are two distinct cases.

– When $l_f = l_g$,

$$W_H(\mathbf{c}_{(a,b)}) = \begin{cases} (p-1)p^{2n-2}, & A_1 \text{ times},\\ (p-1)(p^{2n-2} + \epsilon_f\epsilon_g \frac{1}{p}\sqrt{p^*}^{2n+s_f+s_g}), & A_2 \text{ times}, \end{cases}$$

whose weight distribution can be determined from Lemma 12. To compute A_1, we define the following three sets by using the condition C_1 given in Lemma 12, and so A_1 can be expressed as

$$A_1 = \#\{(a,b) \in \mathcal{S}_f^\star \times \mathcal{S}_g^\star\colon\ f^\star(a) + g^\star(b) = 0\}$$
$$+\#\{a \in \mathcal{S}_f^\star\colon\ f^\star(a) = 0\} + \#\{b \in \mathcal{S}_g^\star\colon\ g^\star(b) = 0\}.$$

We hence conclude that $A_1 = S_{f,g} - 1$, where $S_{f,g}$ is defined as in Lemma 13. We clearly have $A_2 = p^{2n-s_f-s_g} - S_{f,g}$ due to the fact that the dimension is $2n$. The Hamming weights and their weight distributions are given in Table 4.

– When $l_f \neq l_g$,

$$W_H(\mathbf{c}_{(a,b)}) = \begin{cases} (p-1)p^{2n-2}, & A_{\omega_1} \text{ times},\\ (p-1)p^{2n-2} + \epsilon_f\epsilon_g \frac{(p-3)}{p}\sqrt{p^*}^{2n+s_f+s_g}, & A_{\omega_2} \text{ times},\\ (p-1)(p^{2n-2} + \epsilon_f\epsilon_g \frac{1}{p}\sqrt{p^*}^{2n+s_f+s_g}), & A_{\omega_3} \text{ times}. \end{cases}$$

In this case, to determine the weight distribution, we define the following four sets by using the condition C_2 given in Lemma 12. A_{ω_1} and A_{ω_2} can be written as

$$\begin{aligned} A_{\omega_1} &= \#\{(a,b) \in \mathcal{S}_f^\star \times \mathcal{S}_g^\star\colon\ f^\star(a) = g^\star(b) = 0\} + \#\{a \in \mathcal{S}_f^\star\colon\ f^\star(a) = 0\}\\ &\quad +\#\{b \in \mathcal{S}_g^\star\colon\ g^\star(b) = 0\} = \#\{(a,b) \in \mathcal{S}_f \times \mathcal{S}_g\colon\ f^\star(a) = g^\star(b) = 0\} - 1\\ &= \mathcal{N}_{f^\star}(0) * \mathcal{N}_{g^\star}(0) - 1,\\ A_{\omega_2} &= \#\{(a,b) \in \mathcal{S}_f^\star \times \mathcal{S}_g^\star\colon\ -\tfrac{f^\star(a)}{g^\star(b)} \in SQ\} = \tfrac{(p-1)^2}{4}\mathcal{N}_{f^\star}(i) * \mathcal{N}_{g^\star}(j), \end{aligned}$$

where $i, j \in SQ$. 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 they are given in Lemma 5. Additionally, we have $A_{\omega_3} = p^{2n-s_f-s_g} - 1 - A_{\omega_1} - A_{\omega_2}$ due to the fact that the dimension is $2n$. Hence, the weight distribution follows from Lemma 5 for each case, and the Hamming weights are given in Table 5.

The proof of this theorem is finally complete. □

We end this subsection giving a numerical example for the code $\mathcal{C}_{\mathcal{D}}$ constructed in Theorem 3, verified by MAGMA in [2].

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

Remark 2. When f and g are two weakly regular 0-plateaued (bent) functions in Theorem 3, we have the same linear code given in [30, Theorem 4].

4 Punctured codes and Subcodes of the constructed codes

In this section, we derive punctured codes and subcodes with flexible parameters from the linear codes constructed in Section 3.

4.1 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 $\mathcal{D}$ of the form (7). Such a code is said to be a *punctured code* of the original code. The minimum distance and length of a punctured code are rather smaller than the original ones while its dimension is the same as the original one.

We deal with the code $\mathcal{C}_{\mathcal{D}}$ of the form (2) for the defining set $\mathcal{D}$ of the form (7). In Theorems 2 and 3, the length and Hamming weights of $\mathcal{C}_{\mathcal{D}}$ 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 $f, g \in WRP$ with $k_f = k_g$. For every $x, y \in \mathbb{F}_q$, $f(ax) + g(ay) = 0$ iff $f(x) + g(y) = 0$ for every $a \in \mathbb{F}_p^\star$ because $f(ax) + g(ay) = a^{k_f}(f(x) + g(y))$. We can then choose a subset $\overline{\mathcal{D}}$ of $\mathcal{D}$ such that $\bigcup_{a\in\mathbb{F}_p^\star} a\overline{\mathcal{D}}$ is a partition of $\mathcal{D}$:

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

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 1. *Let $\mathcal{D}$ be defined as in (7), where $f, g \in WRP$, and suppose $k_f = k_g$. Let $\mathcal{C}_{\mathcal{D}}$ be the 3-weight code proposed in Theorem 2. Then, its punctured code $\mathcal{C}_{\overline{\mathcal{D}}}$ is a 3-weight $[(p^{2n-1}-1)/(p-1), 2n]$ code whose parameters are documented in Table 6.*

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

Example 5. The punctured code $\mathcal{C}_{\overline{\mathcal{D}}}$ of the code given in Example 2 is a 3-weight ternary $[13, 4, 6]$ code with $1 + 4y^6 + 70y^9 + 6y^{12}$. This punctured code is almost optimal ternary code because the best ternary code with length 13 and dimension 4 has $d = 7$ in [15].

Example 6. The punctured code $\mathcal{C}_{\overline{\mathcal{D}}}$ of the code given in Example 3 is a 3-weight ternary $[121, 6, 72]$ minimal code with $1 + 14y^{72} + 706y^{81} + 8y^{90}$. Note that $d = 78$ for the best ternary code with length 121 and dimension 6 in [15].

Corollary 2. *Let $\mathcal{D}$ be defined as in (7), where $f, g \in WRP$, and suppose that $k_f = k_g$ and $l_f = l_g$. Let $\mathcal{C}_{\mathcal{D}}$ be the 3-weight code proposed in Theorem 3 when $l_f = l_g$. Then, its punctured code $\mathcal{C}_{\overline{\mathcal{D}}}$ is a 3-weight $[(p^{2n-1}-1)/(p-1) + \epsilon_f\epsilon_g\frac{1}{p}\sqrt{p^*}^{2n+s_f+s_g}, 2n]$ code whose parameters are listed in Table 7.*

4.2 Two-weight and three-weight subcodes from partially bent functions

There are several ways to obtain subcodes from the known linear codes over finite fields. To obtain subcodes from our constructed codes, we restrict the element of the finite field to an affine Walsh support of a partially bent function over a finite field.

We notice that the Walsh support of a plateaued function is in general not necessarily a vector space. If it is a vector space, then such a plateaued function is said to be a trivial plateaued function that essentially corresponds to a partially bent function (see [5,7,16]). Hence, the Walsh support of any partially bent function over $\mathbb{F}_q$ is an affine subspace of $\mathbb{F}_q$. It is well-known that the Walsh support of any partially bent function (and also, quadratic function) over $\mathbb{F}_q$ is a certain coset of the orthogonal complement of an affine subspace of its linear structures in $\mathbb{F}_q$. We remark that all quadratic unbalanced functions and some partially bent unbalanced functions belong to this class *WRP*. For any partially bent function $g \in WRP$, there exists an integer s_g with $0 < s_g \leq n$ such that the vector space of its linear structures has dimension s_g, and so its affine Walsh support has dimension $n - s_g$.

To define a subcode of the code $\mathcal{C}_{\mathcal{D}}$ constructed in Theorem 1, we restrict an element b from $\mathbb{F}_{p^n}$ to an $(n - s_g)$-dimensional affine Walsh support $\mathcal{S}_g$ of a function $g \in WRP$. We define a subcode

$$\overline{\mathcal{C}}_{\mathcal{D}} = \{\mathbf{c}_{(a,b)} = (\mathrm{Tr}^n(ax_1 + by_1), \ldots, \mathrm{Tr}^n(ax_m + by_m)) \colon\ a \in \mathbb{F}_{p^n} \text{ and } b \in \mathcal{S}_g\}$$

based on the defining set $\mathcal{D}$ of the form (6). The length of $\overline{\mathcal{C}}_{\mathcal{D}}$ is m and its dimension is $2n - s_g$. The following corollary presents the parameters of this subcode $\overline{\mathcal{C}}_{\mathcal{D}}$ for $\mathcal{C}_{\mathcal{D}}$ proposed in Theorem 1.

Corollary 3. *Let $\mathcal{D}$ be defined as in (6) and $g \in WRP$. Let $\mathcal{C}_{\mathcal{D}}$ be the 3-weight code proposed in Theorem 1. Then, its subcode $\overline{\mathcal{C}}_{\mathcal{D}}$ is a 3-weight $[p^{2n-1} - 1, 2n - s_g]$ code whose parameters follow from Tables 1 and 2 when $n + s_g$ is even and odd, respectively.*

For the codes $\mathcal{C}_{\mathcal{D}}$ proposed in Theorems 2 and 3, we restrict an element (a, b) from $\mathbb{F}_q^2$ to its affine subspace $\mathcal{S}_f \times \mathcal{S}_g$, where $\mathcal{S}_f$ and $\mathcal{S}_g$ are the affine Walsh supports of $f, g \in WRP$ with order p^{n-s_f} and p^{n-s_g}, respectively. We then define a subcode

$$\overline{\mathcal{C}}_{\mathcal{D}} = \{\mathbf{c}_{(a,b)} = (\mathrm{Tr}^n(ax_1 + by_1), \ldots, \mathrm{Tr}^n(ax_m + by_m)) :\ (a, b) \in \mathcal{S}_f \times \mathcal{S}_g\} \qquad (8)$$

based on the defining set $\mathcal{D}$ of the form (7). It is clear that the length of $\overline{\mathcal{C}}_{\mathcal{D}}$ is m and its dimension is $2n - s_f - s_g$.

The following corollaries introduce the parameters of the subcodes of the form (8), which follow from that of the corresponding original codes.

Corollary 4. *Let $\mathcal{D}$ be defined as in (7), and let $f, g \in WRP$. Let $\mathcal{C}_{\mathcal{D}}$ be the 3-weight code proposed in Theorem 2. Then, its subcode $\overline{\mathcal{C}}_{\mathcal{D}}$ of the form (8) is a 3-weight $[p^{2n-1} - 1, 2n - s_f - s_g]$ code whose parameters follow from Table 3.*

Corollary 5. *Let $\mathcal{D}$ be defined as in (7), and let $f, g \in WRP$. Let $\mathcal{C}_{\mathcal{D}}$ be the code proposed in Theorem 3. Then, its subcode $\overline{\mathcal{C}}_{\mathcal{D}}$ of the form (8) with $[p^{2n-1} - 1 + \epsilon_f \epsilon_g \frac{1}{p}(p - 1)\sqrt{p^*}^{2n+s_f+s_g}, 2n - s_f - s_g]$ is a p-ary subcode over $\mathbb{F}_p$*

- *with 2-weights when* $l_f = l_g$,
- *with 3-weights for* $p > 3$ *when* $l_f \neq l_g$, *in particular, it is a 2-weight ternary subcode for* $p = 3$.

The parameters of this subcode are given in Tables 8 and 9.

Corollary 6. *Let* $\mathcal{D}$ *be defined as in (7), where* $f, g \in$ *WRP, and suppose* $k_f = k_g$. *Let* $\mathcal{C}_{\overline{\mathcal{D}}}$ *be the 3-weight punctured code obtained in Corollary 1. Then, its subcode* $\overline{\mathcal{C}}_{\overline{\mathcal{D}}}$ *of the form (8) is a 3-weight* $[(p^{2n-1}-1)/(p-1), 2n - s_f - s_g]$ *code whose parameters follow readily from Table 6.*

Example 7. The subcode $\mathcal{C}_{\overline{\mathcal{D}}}$ of Example 6 is a 3-weight minimal ternary $[121, 5, 72]$ code with $1 + 14y^{72} + 220y^{81} + 8y^{90}$.

Corollary 7. *Let* $\mathcal{D}$ *be defined as in (7), where* $f, g \in$ *WRP, and suppose that* $k_f = k_g$ *and* $l_f = l_g$. *Let* $\mathcal{C}_{\overline{\mathcal{D}}}$ *be the 3-weight punctured code given in Corollary 2. Then, its subcode* $\overline{\mathcal{C}}_{\overline{\mathcal{D}}}$ *of the form (8) is a 2-weight*

$$[(p^{2n-1}-1)/(p-1) + \epsilon_f \epsilon_g \frac{1}{p} \sqrt{p^*}^{2n+s_f+s_g}, 2n - s_f - s_g]$$

code whose parameters are listed in Table 10.

The method proposed above for obtaining subcodes decreases the dimension of the original code while its length does not change. Also, this method does not change the minimum distances of our codes although it may usually change that of a linear code. Consequently, the dimension of a dual subcode is rather greater than that of the original dual code. This suggests that the obtained subcodes may be used to construct more flexible secret sharing schemes with high democracy.

5 Minimality of the constructed codes

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

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

Lemma 14. *(Ashikhmin-Barg,1998) [1] Let* $\mathcal{C}$ *be a linear code over* $\mathbb{F}_p$, *and let* $w_{\min}$ *and* $w_{\max}$ *represent the minimum and maximum Hamming weights of* $\mathcal{C}$, *respectively. Then,* $\mathcal{C}$ *is minimal if*

$$\frac{p-1}{p} < \frac{w_{\min}}{w_{\max}}. \tag{9}$$

By (9), our linear codes are minimal codes for almost all integers s_f and s_g with $0 \leq s_f, s_g \leq n$. The following proposition finds the bounds on the integers s_f and s_g that make the associated codes are minimal.

Proposition 2. *Let $f, g \in WRP$, and let s_f and s_g be two integers with $0 \leq s_f, s_g \leq n$. We have the following bounds on the parameters.*

i.) The code $\mathcal{C}_{\mathcal{D}}$ in Theorem 1 is minimal for $0 \leq s_g \leq n-3$ if $n+s_g$ is even; otherwise, it is minimal for $0 \leq s_g \leq n-2$ and $4 \leq n$.
ii.) The code $\mathcal{C}_{\mathcal{D}}$ in Theorem 2 is minimal when $0 \leq s_f + s_g \leq 2n-4$ and $3 \leq n$.
iii.) The code $\mathcal{C}_{\mathcal{D}}$ in Theorem 3 is minimal for $0 \leq s_f+s_g \leq 2n-4$ if $\epsilon_f \epsilon_g \eta_0^{(2n+s_f+s_g+1)/2}(-1) = 1$; otherwise, it is minimal for $0 \leq s_f + s_g \leq 2n-6$ and $3 \leq n$.

Remark 3. Our punctured codes and subcodes 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 [6, 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 1, 2 and 3, 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. Moreover, for each subcode $\overline{\mathcal{C}}_{\mathcal{D}}$ proposed in Corollaries 3, 4 and 5, its dual code $\overline{\mathcal{C}}_{\mathcal{D}}^{\perp}$ has $d^{\perp} = 2$ due to the same fact. Hence, these minimal codes can be used to design high democratic secret sharing schemes with good access structures as introduced in [6, Theorem 17] (developed in [12, Proposition 2]).

On the other hand, for the punctured codes $\mathcal{C}_{\overline{\mathcal{D}}}$ given in Corollaries 1 and 2 (and also for their subcodes $\overline{\mathcal{C}}_{\overline{\mathcal{D}}}$ given in Corollaries 6 and 7), the minimum distances of their dual codes are at least 3 since no two of the vectors are dependent. As a consequence, the punctured codes and their subcodes are projective minimal codes. The projective 3-weight codes given in Corollaries 1, 2 and 6 can be employed to obtain association schemes introduced in [3], and projective 2-weight codes given in Corollary 7 can be used in strongly regular graphs defined in [4]. Additionally, they can be employed to design democratic secret sharing schemes as introduced in [6, Theorem 17].

6 Conclusion

In this paper, motivated by the work of [17,19,30], to construct minimal codes, we consider weakly regular plateaued unbalanced functions in the recent construction method of linear codes. As far as we search, our minimal codes have new parameters since we for the first time use a new class *WRP* of functions in the recent construction method proposed in [17,19,30]. In conclusion, the main contributions of the paper are given as follows.

- We construct new infinite classes of 3-weight and 4-weight linear codes from the class *WRP* of plateaued functions over $\mathbb{F}_p$. To find the Hamming weights, we benefit from the exponential sums and Walsh spectrums of the employed functions $f, g \in WRP$. To determine the weight distributions, we use the exponential sums and Walsh distributions of $f, g \in WRP$ as well as the numbers of the pre-images 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 also derive 2-weight and 3-weight subcodes with flexible dimensions from partially bent functions f and g by considering their affine Walsh supports $\mathcal{S}_f$ and $\mathcal{S}_g$ instead of the finite field $\mathbb{F}_q$ in the construction method of the form (2). As a result of this technique, the dimension of the dual subcode is rather greater than that of the original dual code, which implies that the subcode produces a more flexible secret sharing scheme with new parameters.
– 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 [12, Proposition 2].
– We finally consider the minimum Hamming distances of the dual codes of our minimal codes. We conclude that the proposed punctured codes and their subcodes are projective. Hence, the proposed projective 2-weight and 3-weight codes can be used to obtain strongly regular graphs in [4] and association schemes in [3], respectively.

References

1. Ashikhmin, A., Barg, A.: Minimal vectors in linear codes. IEEE Transactions on Information Theory **44**(5), 2010–2017 (1998)
2. Bosma, W., Cannon, J., Playoust, C.: The magma algebra system i: The user language. Journal of Symbolic Computation **24**(3), 235–265 (1997)
3. Calderbank, A., Goethals, J.: Three-weight codes and association schemes. Philips J. Res **39**(4-5), 143–152 (1984)
4. Calderbank, R., Kantor, W.: The geometry of two-weight codes. Bulletin of the London Mathematical Society **18**(2), 97–122 (1986)
5. Carlet, C.: Partially-bent functions. Designs, Codes and Cryptography **3**(2), 135–145 (1993)
6. Carlet, C., Ding, C., Yuan, J.: Linear codes from perfect nonlinear mappings and their secret sharing schemes. IEEE Transactions on Information Theory **51**(6), 2089–2102 (2005)
7. Çeşmelioğlu, A., McGuire, G., Meidl, W.: A construction of weakly and non-weakly regular bent functions. Journal of Combinatorial Theory, Series A **119**(2), 420–429 (2012)
8. Çeşmelioğlu, A., Meidl, W.: A construction of bent functions from plateaued functions. Designs, codes and cryptography **66**(1), 231–242 (2013)
9. Ding, C.: Linear codes from some 2-designs. IEEE Transactions on information theory **61**(6), 3265–3275 (2015)
10. Ding, C.: A construction of binary linear codes from Boolean functions. Discrete mathematics **339**(9), 2288–2303 (2016)
11. Ding, C., Niederreiter, H.: Cyclotomic linear codes of order 3. IEEE transactions on information theory **53**(6), 2274–2277 (2007)
12. Ding, C., Yuan, J.: Covering and secret sharing with linear codes. DMTCS **2731**, 11–25 (2003)
13. Ding, K., Ding, C.: Binary linear codes with three weights. IEEE Communications Letters **18**(11), 1879–1882 (2014)
14. Ding, K., Ding, C.: A class of two-weight and three-weight codes and their applications in secret sharing. IEEE Transactions on Information Theory **61**(11), 5835–5842 (2015)
15. Grassl, M.: Bounds on the minimum distance of linear codes and quantum codes. Online available at `http://www.codetables.de` (2007), accessed on 2020-08-02
16. Hodžić, S., Pasalic, E., Wei, Y., Zhang, F.: Designing plateaued boolean functions in spectral domain and their classification. IEEE transactions on information theory **65**(9), 5865–5879 (2019)
17. Jian, G., Lin, Z., Feng, R.: Two-weight and three-weight linear codes based on weil sums. Finite Fields and Their Applications **57**, 92–107 (2019)

18. Kumar, P.V., Scholtz, R.A., Welch, L.R.: Generalized bent functions and their properties. Journal of Combinatorial Theory, Series A **40**(1), 90–107 (1985)
19. Li, C., Yue, Q., Fu, F.W.: A construction of several classes of two-weight and three-weight linear codes. Applicable Algebra in Engineering, Communication and Computing **28**(1), 11–30 (2017)
20. 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 **60**(8), 4710–4721 (2014)
21. Li, N., Mesnager, S.: Recent results and problems on constructions of linear codes from cryptographic functions. Cryptography and Communications **12**, 965–986 (2020)
22. Lidl, R., Niederreiter, H.: Finite fields, vol. 20. Cambridge university press (1997)
23. Mesnager, S., Sınak, A., Yayla, O.: Minimal linear codes with few weights and their secret sharing. International Journal of Information Security Science **8**(4), 77–87 (2019)
24. 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)
25. Mesnager, S., Özbudak, F., Sınak, A.: Linear codes from weakly regular plateaued functions and their secret sharing schemes. Designs, Codes and Cryptography **87**(2-3), 463–480 (2019)
26. 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)
27. Rothaus, O.S.: On "bent" functions. Journal of Combinatorial Theory, Series A **20**(3), 300–305 (1976)
28. Tang, C., Li, N., Qi, Y., Zhou, Z., Helleseth, T.: Linear codes with two or three weights from weakly regular bent functions. IEEE Transactions on Information Theory **62**(3), 1166–1176 (2016)
29. Tang, C., Xiang, C., Feng, K.: Linear codes with few weights from inhomogeneous quadratic functions. Designs, Codes and Cryptography **83**(3), 691–714 (2017)
30. Wu, Y., Li, N., Zeng, X.: Linear codes with few weights from cyclotomic classes and weakly regular bent functions. Designs, Codes and Cryptography **88**, 1255–1272 (2020)
31. 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 **18**(1), 70–92 (2012)
32. Zheng, Y., Zhang, X.M.: Plateaued functions. In: ICICS. vol. 99, pp. 284–300. Springer (1999)
33. Zhou, Z., Li, N., Fan, C., Helleseth, T.: Linear codes with two or three weights from quadratic bent functions. Designs, Codes and Cryptography **81**(2), 283–295 (2016)

7 Appendix

The appendix presents the Hamming weights and weight distributions of the minimal codes obtained in this paper.

Table 1. The Hamming weights of $\mathcal{C}_{\mathcal{D}}$ in Theorem 1 when $n + s_g$ is even

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

Table 2. The Hamming weights of $\mathcal{C}_{\mathcal{D}}$ in Theorem 1 when $n+s_g$ is odd

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

Table 3. The Hamming weights of $\mathcal{C}_{\mathcal{D}}$ in Theorem 2 when $n+s_f$ is odd and $n+s_g$ is even

Hamming weight ω	Multiplicity A_ω
0	1
$(p-1)p^{2n-2}$	$p^{2n}-p^{2n-s_f-s_g}+A_1$
$(p-1)(p^{2n-2}-\epsilon_f\epsilon_g\frac{1}{p^2}\sqrt{p^*}^{2n+s_f+s_g+1})$	A_2
$(p-1)(p^{2n-2}+\epsilon_f\epsilon_g\frac{1}{p^2}\sqrt{p^*}^{2n+s_f+s_g+1})$	A_3

Table 4. The Hamming weights of $\mathcal{C}_{\mathcal{D}}$ in Theorem 3 when $2n+s_f+s_g$ is even and $l_f=l_g$

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

Table 5. The Hamming weights of $\mathcal{C}_{\mathcal{D}}$ in Theorem 3 when $2n+s_f+s_g$ is even and $l_f\neq l_g$

Hamming weight ω	Multiplicity A_ω
0	1
$(p-1)(p^{2n-2}+\epsilon_f\epsilon_g\frac{1}{p^2}(p-1)\sqrt{p^*}^{2n+s_f+s_g})$	$p^{2n}-p^{2n-s_f-s_g}$
$(p-1)p^{2n-2}$	A_{ω_1}
$(p-1)p^{2n-2}+\epsilon_f\epsilon_g\frac{(p-3)}{p}\sqrt{p^*}^{2n+s_f+s_g}$	A_{ω_2}
$(p-1)(p^{2n-2}+\epsilon_f\epsilon_g\frac{1}{p}\sqrt{p^*}^{2n+s_f+s_g})$	A_{ω_3}

Table 6. The Hamming weights of $\mathcal{C}_{\overline{\mathcal{D}}}$ in Corollary 1 when $2n+s_f+s_g$ is odd and $k_f=k_g$

Hamming weight ω	Multiplicity A_ω
0	1
p^{2n-2}	$p^{2n}-p^{2n-s_f-s_g}+A_1$
$p^{2n-2}-\epsilon_f\epsilon_g\frac{1}{p^2}\sqrt{p^*}^{2n+s_f+s_g+1}$	A_2
$p^{2n-2}+\epsilon_f\epsilon_g\frac{1}{p^2}\sqrt{p^*}^{2n+s_f+s_g+1}$	A_3

Table 7. The Hamming weights of $\mathcal{C}_{\overline{\mathcal{D}}}$ in Corollary 2 when $2n+s_f+s_g$ is even, $k_f=k_g$ and $l_f=l_g$

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

Table 8. The Hamming weights of $\overline{\mathcal{C}}_{\mathcal{D}}$ in Corollary 5 when $2n+s_f+s_g$ is even and $l_f=l_g$

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

Table 9. The Hamming weights of $\overline{\mathcal{C}}_{\mathcal{D}}$ in Corollary 5 when $2n+s_f+s_g$ is even and $l_f\neq l_g$

Hamming weight ω	Multiplicity A_ω
0	1
$(p-1)p^{2n-2}$	A_{ω_1}
$(p-1)p^{2n-2}+\epsilon_f\epsilon_g\frac{(p-3)}{p}\sqrt{p^*}^{2n+s_f+s_g}$	A_{ω_2}
$(p-1)(p^{2n-2}+\epsilon_f\epsilon_g\frac{1}{p}\sqrt{p^*}^{2n+s_f+s_g})$	A_{ω_3}

Table 10. The Hamming weights of $\overline{\mathcal{C}}_{\overline{\mathcal{D}}}$ in Corollary 7 when $2n+s_f+s_g$ is even, $k_f=k_g$ and $l_f=l_g$

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