# Minimal Linear Codes From Weakly Regular Plateaued Balanced Functions

Ahmet Sınak\*

May 12, 2020

#### Abstract

Linear codes have diverse applications in secret sharing schemes, secure two-party computation, association schemes, strongly regular graphs, authentication codes and communication. There are a large number of linear codes with few weights in the literature, but a little of them are minimal. In this paper, we are using for the first time weakly regular plateaued balanced functions over the finite fields of odd characteristic in the second generic construction method of linear codes. The main results of this paper are stated below. We first construct several three-weight and four-weight linear codes with flexible parameters from weakly regular plateaued balanced functions. It is worth noting that the (almost) optimal codes may be obtained from these functions. We next observe that all codes obtained in this paper are minimal, thereby they can be directly employed to construct secret sharing schemes with high democracy. Finally, the democratic secret sharing schemes are obtained from the dual codes of our minimal codes.

**Keywords** Linear code, minimal code, weakly regular plateaued function, balanced function, secret sharing scheme

### 1 Introduction

Let  $\mathbb{F}_{p^n}$  represent the finite field with  $p^n$  elements, where p is a prime number and n is a positive integer. The finite field  $\mathbb{F}_{p^n}$  can be seen as an n-dimensional vector space over  $\mathbb{F}_p$ , and denoted by  $\mathbb{F}_p^n$ . An  $[n, k, d]_p$  linear code  $\mathcal{C}$  over  $\mathbb{F}_p$  is a k-dimensional linear subspace of  $\mathbb{F}_p^n$  with length n, dimension k and minimum Hamming distance d. The Hamming weight of a codeword  $\mathbf{v} = (v_0, \ldots, v_{n-1}) \in \mathcal{C}$ , denoted by  $W_H(\mathbf{v})$ , is defined as the size of the set  $\mathrm{supp}(\mathbf{v}) = \{0 \leq i \leq n-1 : v_i \neq 0\}.$ 

<sup>\*</sup>Department of mathematics and computer science, Necmettin Erbakan University, 42090, Konya, Turkey and LAGA, Universities of Paris VIII and Paris XIII, CNRS, UMR 7539, Paris, France. Email: sinakahmet@gmail.com

Let  $A_{\omega}$  denote the number of codewords in  $\mathcal{C}$  with Hamming weight  $\omega$ . Then the sequence  $(1, A_1, \ldots, A_n)$  represents the *weight distribution* and the polynomial  $1 + A_1y + \cdots + A_ny^n$  shows the *weight enumerator* of the *n*-length code  $\mathcal{C}$ . The code  $\mathcal{C}$  is said to be a *t*-weight code if  $\#\{1 \leq \omega \leq n : A_{\omega} \neq 0\} = t$ . A generator matrix G of  $\mathcal{C}$  is a  $k \times n$  matrix whose rows form a basis for the code  $\mathcal{C}$ . The dual code of  $\mathcal{C}$  is defined as  $\mathcal{C}^{\perp} = \{\mathbf{u} \in \mathbb{F}_p^n : \mathbf{u} \cdot \mathbf{v} = \mathbf{0} \text{ for all } \mathbf{v} \in \mathcal{C}\}$  with length n and dimension n - k, where " $\cdot$ " is the standard inner product on  $\mathbb{F}_n^n$ .

For the codewords  $\mathbf{u}, \mathbf{v} \in \mathcal{C}$ , if  $\operatorname{supp}(\mathbf{u})$  includes  $\operatorname{supp}(\mathbf{v})$ , then it is said that  $\mathbf{u}$  covers  $\mathbf{v}$ . A nonzero codeword  $\mathbf{u}$  of  $\mathcal{C}$  is called *minimal* codeword if  $\mathbf{u}$  covers only the codeword  $i\mathbf{u}$  for all  $i \in \mathbb{F}_p$ . Indeed, a linear  $\mathcal{C}$  is called *minimal linear code* if every nonzero codeword of  $\mathcal{C}$  is minimal codeword. Minimal linear codes have an interesting application in secret sharing scheme (SSS). In SSS, a set of participants who can reconstruct the secret value s from their shares is said to be *an access set*. Besides, an access set is said to be *minimal access set* if none of its proper subset can reconstruct s from their shares. The *access structure* of a SSS is described as the set of all access sets. It is worth pointing out that we have a one-to-one match-up between the set of minimal codewords of the dual code  $\mathcal{C}^{\perp}$  and the set of minimal access sets of SSS based on  $\mathcal{C}$ .

Linear codes have diverse applications in secret sharing schemes, secure two-party computation, association schemes, strongly regular graphs, authentication codes, communication, data storage devices and consumer electronics. One of the well-known construction methods of linear codes is based on functions over finite fields. This construction method is an interesting problem in coding theory. In the literature, a larger number of linear codes with desirable parameters have been constructed from some special cryptographic functions such as quadratic functions [25], (weakly regular) bent functions [3, 7, 11, 12, 24, 26, 29], weakly regular plateaued functions [19, 23], almost bent functions [8], almost perfect nonlinear (APN) functions [17, 27] and perfect nonlinear functions [4]. Very recently, weakly regular plateaued unbalanced functions have been used in [23] to obtain minimal linear codes with flexible parameters. Within this framework, we benefit from weakly regular plateaued functions in order to construct further minimal linear codes with different parameters over the finite fields of odd characteristic.

The organization of the paper is given as follows. Section 2 gives some results on weakly regular plateaued balanced functions. In Section 3, we obtain three-weight and four-weight linear codes from these functions over the finite field of odd characteristic. It is remarkable that the punctured three-weight optimal codes are obtained in Examples 5 and 6. In Section 4, we first observe the constructed codes are minimal, and then define the access structures of the SSS based on their dual codes.

### 2 Weakly regular plateaued functions

This section introduces some useful results on exponential sums of weakly regular plateaued balanced functions.

#### 2.1 Some results on weakly regular plateaued functions

We first give a necessary background and some results on weakly regular plateaued functions. For a set S, #S represents the size of S and  $S^*$  denotes  $S \setminus \{0\}$ . The symbol  $\eta_0$  represents the quadratic character of  $\mathbb{F}_p^*$ , and  $\eta_0(-1)p$  is denoted by  $p^*$ . The set of all squares in  $\mathbb{F}_p^*$  is denoted by SQ and the set of all non-squares is denoted by NSQ. Throughout this paper, f is a function from  $\mathbb{F}_{p^m}$  to  $\mathbb{F}_p$  for an odd prime p and a positive integer m. The trace of  $\alpha \in \mathbb{F}_{p^m}$  over  $\mathbb{F}_p$  is defined by  $\operatorname{Tr}^m(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + \cdots + \alpha^{p^{m-1}}$ . The Walsh transform of f is defined by

$$\mathcal{W}_f(\omega) = \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{f(x) - \operatorname{Tr}^m(\omega x)},$$

where  $\zeta_p$  is a primitive *p*-th root of unity. A function *f* is said to be *balanced* over  $\mathbb{F}_p$  if  $\mathcal{W}_f(0) = 0$ ; otherwise, *f* is *unbalanced*.

The notion of plateaued Boolean functions was first introduced by Zheng and Zhang [28]. In characteristic p, a function f is called p-ary s-plateaued if  $|\mathcal{W}_f(\omega)|^2 \in \{0, p^{m+s}\}$  for every  $\omega \in \mathbb{F}_{p^m}$ , with  $0 \leq s \leq m$ . In particular, a 0-plateaued function is the *bent function*. The Walsh support of a plateaued f is defined as the set  $\mathcal{S}_f = \{\omega \in \mathbb{F}_{p^m} : |\mathcal{W}_f(\omega)|^2 = p^{m+s}\}$ . The absolute Walsh distribution of a plateaued function can be derived from the Parseval identity.

**Lemma 1.** If f is an s-plateaued function over  $\mathbb{F}_{p^m}$ , then for  $\omega \in \mathbb{F}_{p^m}$ ,  $|\mathcal{W}_f(\omega)|^2$  takes  $p^{m-s}$  times the value  $p^{m+s}$  and  $p^m - p^{m-s}$  times the value 0.

Recently, motivated by [16, Theorem 2], Mesnager et al. [20, 22] have defined the subclass of plateaued functions. An *s*-plateaued f is called *weakly regular* if

$$\mathcal{W}_f(\omega) \in \left\{0, up^{\frac{m+s}{2}} \zeta_p^{f^\star(\omega)}\right\}, \ \forall \omega \in \mathbb{F}_{p^m},\tag{1}$$

where  $u \in \{\pm 1, \pm i\}$  and  $f^*$  is a *p*-ary function over  $\mathbb{F}_{p^m}$  with  $f^*(\omega) = 0$  for all  $\omega \in \mathbb{F}_{p^m} \setminus S_f$ . We remark that f is said to be a *non-weakly regular plateaued function* when u in (1) depends on  $\omega$ . Notice that  $f^*(0) = 0$  if f is a plateaued balanced function.

**Lemma 2.** [22] If f is a weakly regular s-plateaued function over  $\mathbb{F}_{p^m}$ , then for every  $\omega \in S_f$ ,  $\mathcal{W}_f(\omega) = \epsilon \sqrt{p^*}^{m+s} \zeta_p^{f^*(\omega)}$ , where  $\epsilon \in \{\pm 1\}$  is the sign of  $\mathcal{W}_f$  and  $f^*$  is a p-ary function over  $S_f$ .

Very recently, Mesnager et al. [23] have denoted by WRP the set of weakly regular plateaued unbalanced functions with the following conditions. Within the same framework, we now assume that  $f : \mathbb{F}_{p^m} \to \mathbb{F}_p$  is a weakly regular s-plateaued balanced function, with  $0 \leq s \leq m$ , and we denote by WRPB the class of such functions satisfying the following two homogeneous conditions:

- f(0) = 0,
- $f(ax) = a^t f(x)$  for every  $a \in \mathbb{F}_p^*$  and  $x \in \mathbb{F}_{p^m}$ , where t is a positive even integer with gcd(t-1, p-1) = 1.

*Remark* 1. This paper uses for the first time the plateaued functions from the class *WRPB* to construct new minimal linear codes with flexible parameters.

We need in the subsequent section the following results that can be derived from [23, Lemma 6 and Proposition 2].

**Lemma 3.** Let  $\omega \in \mathbb{F}_{p^m}$  and  $f \in WRPB$  with  $\mathcal{W}_f(\omega) = \epsilon \sqrt{p^*}^{m+s} \zeta_p^{f^*(\omega)}$ . Then for every  $z \in \mathbb{F}_p^*$ , we have  $z\omega \in \mathcal{S}_f$  when  $\omega \in \mathcal{S}_f$ , and  $z\omega \in \mathbb{F}_{p^m} \setminus \mathcal{S}_f$ ; otherwise.

**Proposition 1.** Let  $f \in WRPB$  with  $W_f(\omega) = \epsilon \sqrt{p^*}^{m+s} \zeta_p^{f^*(\omega)}$  for every  $\omega \in S_f$ . Then, we have  $f^*(a\omega) = a^l f^*(\omega)$  for every  $a \in \mathbb{F}_p^*$  and  $\omega \in S_f$ , where l is a positive even integer with gcd(l-1, p-1) = 1.

We end this subsection with giving a brief introduction to the quadratic functions (see for example [14]). Recall that every quadratic function from  $\mathbb{F}_{p^m}$  to  $\mathbb{F}_p$  having no linear term can be represented by

$$Q(x) = \sum_{i=0}^{\lfloor m/2 \rfloor} \operatorname{Tr}^{m}(a_{i}x^{p^{i}+1}), \qquad (2)$$

where  $a_i \in \mathbb{F}_{p^m}$  for  $0 \leq i \leq \lfloor m/2 \rfloor$  and  $\lfloor x \rfloor$  represents the largest integer less than or equal to x. Let A be a corresponding  $m \times m$  symmetric matrix with  $Q(x) = x^T A x$  as in [14] and L be a corresponding linearized polynomial over  $\mathbb{F}_{p^m}$  defined as  $L(z) = \sum_{i=0}^l (a_i z^{p^i} + a_i^{p^{m-i}} z^{p^{m-i}})$ . The set of linear structures of quadratic function Q is the kernel of L, defined as

$$\ker_{\mathbb{F}_p}(L) = \{ z \in \mathbb{F}_{p^m} \colon Q(z+y) = Q(z) + Q(y), \forall y \in \mathbb{F}_{p^m} \},$$
(3)

which is an  $\mathbb{F}_p$ -linear subspace of  $\mathbb{F}_{p^m}$ . Let the dimension of  $\ker_{\mathbb{F}_p}(L)$  be s with  $0 \le s \le m$ . Notice that by [15, Proposition 2.1], the rank of A equals m - s. It was shown in [14] that a quadratic function Q is bent if and only if s = 0; equivalently, A is nonsingular, that is, A has full rank. Hence we have the following natural consequence (see [14, Proposition 2] and [21, Example 1]). **Proposition 2.** Any quadratic function Q is an s-plateaued if and only if the dimension of the kernel of L defined as in (3) equals s; equivalently, the rank of A equals m - s.

One can derive from [14, Proposition 1] and [5, Theorem 4.3] the following reasonable fact.

**Proposition 3.** The sign of the Walsh transform of quadratic functions does not depend on inputs which means that every quadratic function is a weakly regular plateaued function. Namely, there is no quadratic non-weakly regular plateaued function.

*Remark* 2. All quadratic balanced functions are included in the class WRPB.

#### 2.2 Exponential sums from weakly regular plateaued functions

In this subsection, we give some results on exponential sums about weakly regular plateaued balanced functions.

**Lemma 4.** [23] Let  $f : \mathbb{F}_{p^m} \to \mathbb{F}_p$  be a weakly regular s-plateaued function with  $\mathcal{W}_f(\omega) = \epsilon \sqrt{p^*}^{m+s} \zeta_p^{f^*(\omega)}$  for  $\omega \in S_f$ , where  $f^*$  is a p-ary function over  $S_f$ . For  $a \in \mathbb{F}_p$ , define  $\mathcal{N}_{f^*}(a) = \#\{\omega \in S_f : f^*(\omega) = a\}$ . Then we have

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

when m - s is even; otherwise,

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

**Lemma 5.** Let  $f \in WRPB$ . For  $\omega \in \mathbb{F}_{p^m}^{\star}$ , define

$$A = \sum_{y,z \in \mathbb{F}_p^{\star}} \sum_{x \in \mathbb{F}_{p^m}} \zeta_p^{yf(x) - z \operatorname{Tr}^m(\omega x)}.$$

Then for every  $\omega \in \mathbb{F}_{p^m}^{\star} \setminus S_f$  we have A = 0, and for every  $\omega \in S_f$ 

$$A = \begin{cases} \epsilon(p-1)^2 \sqrt{p^{*}}^{m+s}, & \text{if } f^{*}(\omega) = 0, \\ -\epsilon(p-1)\sqrt{p^{*}}^{m+s}, & \text{if } f^{*}(\omega) \neq 0 \end{cases}$$

when m + s is even; otherwise,

$$A = \begin{cases} 0, & \text{if } f^{\star}(\omega) = 0, \\ \epsilon \eta_0(f^{\star}(\omega))(p-1)\sqrt{p^*}^{m+s+1}, & \text{if } f^{\star}(\omega) \neq 0. \end{cases}$$

*Proof.* The proof can proceed by using the same arguments of the proof of [23, Lemma 12].  $\Box$ 

**Lemma 6.** Let  $f \in WRPB$ . For  $\omega \in \mathbb{F}_{p^m}^{\star}$ , define  $\mathcal{N}_0(\omega) = \#\{x \in \mathbb{F}_{p^m}: f(x) = 0 \text{ and } \operatorname{Tr}^m(\omega x) = 0\}$ . Then for every  $\omega \in \mathbb{F}_{p^m}^{\star} \setminus S_f$  we have  $\mathcal{N}_0(\omega) = p^{m-2}$ , and for every  $\omega \in S_f$ ,

$$\mathcal{N}_{0}(\omega) = \begin{cases} p^{m-2} + \epsilon(p-1)^{2}\sqrt{p^{*}}^{m+s-4}, & \text{if } f^{*}(\omega) = 0, \\ p^{m-2} - \epsilon(p-1)\sqrt{p^{*}}^{m+s-4}, & \text{if } f^{*}(\omega) \neq 0 \end{cases}$$

when m + s is even; otherwise,

$$\mathcal{N}_{0}(\omega) = \begin{cases} p^{m-2}, & \text{if } f^{\star}(\omega) = 0, \\ p^{m-2} + \epsilon(p-1)\sqrt{p^{\star}}^{m+s-3}, & \text{if } f^{\star}(\omega) \in SQ, \\ p^{m-2} - \epsilon(p-1)\sqrt{p^{\star}}^{m+s-3}, & \text{if } f^{\star}(\omega) \in NSQ. \end{cases}$$

*Proof.* By the definition of  $\mathcal{N}_0(\omega)$  and the fact that f is balanced, we have

$$\mathcal{N}_0(\omega) = p^{m-2} + p^{-2} \sum_{y,z \in \mathbb{F}_p^*} \sum_{x \in \mathbb{F}_p^m} \zeta_p^{yf(x) - z\operatorname{Tr}^m(\omega x)}.$$

Then, the proof is ended from Lemma 5.

**Lemma 7.** Let  $f \in WRPB$ . For  $\omega \in \mathbb{F}_{p^m}^{\star}$ , define

$$A = \sum_{y,z \in \mathbb{F}_p^\star} \sum_{x \in \mathbb{F}_p^m} \zeta_p^{y^2 f(x) - z \operatorname{Tr}^m(\omega x)}.$$

Then for every  $\omega \in \mathbb{F}_{p^m}^{\star} \setminus \mathcal{S}_f$  we have A = 0, and for every  $\omega \in \mathcal{S}_f$ 

$$A = \begin{cases} \epsilon(p-1)^2 \sqrt{p^*}^{m+s}, & \text{if } f^*(\omega) = 0, \\ \epsilon(p-1) \sqrt{p^*}^{m+s} (\sqrt{p^*} - 1), & \text{if } f^*(\omega) \in SQ, \\ -\epsilon(p-1) \sqrt{p^*}^{m+s} (\sqrt{p^*} + 1), & \text{if } f^*(\omega) \in NSQ. \end{cases}$$

*Proof.* The proof can proceed by using the arguments used in the proof of [23, Lemma 15].  $\Box$ 

**Lemma 8.** Let  $f \in WRPB$ . For  $\omega \in \mathbb{F}_{p^m}^{\star}$ , define

$$\mathcal{N}_{sq}(\omega) = \#\{x \in \mathbb{F}_{p^m} \colon f(x) \in SQ \text{ and } \operatorname{Tr}^m(\omega x) = 0\},\$$
  
$$\mathcal{N}_{nsq}(\omega) = \#\{x \in \mathbb{F}_{p^m} \colon f(x) \in NSQ \text{ and } \operatorname{Tr}^m(\omega x) = 0\}.$$

-		

Then for every  $\omega \in \mathbb{F}_{p^m}^{\star} \setminus S_f$  we have  $\mathcal{N}_{sq}(\omega) = \mathcal{N}_{nsq}(\omega) = \frac{1}{2}(p-1)p^{m-2}$ . For every  $\omega \in S_f$ 

$$\mathcal{N}_{sq}(\omega) = \begin{cases} \frac{1}{2}(p-1)(p^{m-2} - \epsilon(p-1)\sqrt{p^{*m+s-4}}), & \text{if } f^{*}(\omega) = 0 \text{ or } f^{*}(\omega) \in NSQ, \\ \frac{1}{2}(p-1)(p^{m-2} + \epsilon(p+1)\sqrt{p^{*m+s-4}}), & \text{if } f^{*}(\omega) \in SQ, \end{cases}$$
$$\mathcal{N}_{nsq}(\omega) = \begin{cases} \frac{1}{2}(p-1)(p^{m-2} - \epsilon(p-1)\sqrt{p^{*m+s-4}}), & \text{if } f^{*}(\omega) = 0 \text{ or } f^{*}(\omega) \in SQ, \\ \frac{1}{2}(p-1)(p^{m-2} + \epsilon(p+1)\sqrt{p^{*m+s-4}}), & \text{if } f^{*}(\omega) \in NSQ \end{cases}$$

when m + s is even; otherwise,

$$\mathcal{N}_{sq}(\omega) = \begin{cases} \frac{1}{2}(p-1)(p^{m-2} + \epsilon\eta_0(-1)(p-1)\sqrt{p^*}^{m+s-3}), & \text{if } f^*(\omega) = 0, \\ \frac{1}{2}(p-1)(p^{m-2} - \epsilon\sqrt{p^*}^{m+s-3}(\eta_0(-1)+1)), & \text{if } f^*(\omega) \in SQ, \\ \frac{1}{2}(p-1)(p^{m-2} - \epsilon\sqrt{p^*}^{m+s-3}(\eta_0(-1)-1)), & \text{if } f^*(\omega) \in NSQ, \end{cases}$$
$$\mathcal{N}_{nsq}(\omega) = \begin{cases} \frac{1}{2}(p-1)(p^{m-2} - \epsilon\eta_0(-1)(p-1)\sqrt{p^*}^{m+s-3}), & \text{if } f^*(\omega) = 0, \\ \frac{1}{2}(p-1)(p^{m-2} + \epsilon\sqrt{p^*}^{m+s-3}(\eta_0(-1)-1)), & \text{if } f^*(\omega) \in SQ, \\ \frac{1}{2}(p-1)(p^{m-2} + \epsilon\sqrt{p^*}^{m+s-3}(\eta_0(-1)+1)), & \text{if } f^*(\omega) \in NSQ. \end{cases}$$

*Proof.* From the proof of [24, Lemma 14], recalling that f is balanced, we have

$$p^{2}\mathcal{N}_{0}(\omega) + p\sqrt{p^{*}}(\mathcal{N}_{sq}(\omega) - \mathcal{N}_{nsq}(\omega)) = p^{n} + \sum_{y,z \in \mathbb{F}_{p}^{*}} \sum_{x \in \mathbb{F}_{p}m} \zeta_{p}^{y^{2}f(x) - z\operatorname{Tr}^{n}(\omega x)},$$

where  $\mathcal{N}_0(\omega)$  is given in Lemma 6. We clearly have  $\mathcal{N}_0(\omega) + \mathcal{N}_{sq}(\omega) + \mathcal{N}_{nsq}(\omega) = p^{n-1}$ . Hence, combining these results, the proof is immediately completed from Lemmas 6 and 7.

The following lemma is a direct consequence of Lemma 8.

**Lemma 9.** Let  $f \in WRPB$ . For  $\omega \in \mathbb{F}_{p^m}^{\star}$ , define  $\mathcal{N}_1(\omega) = \#\{x \in \mathbb{F}_{p^m}: f(x) = 1 \text{ and } \operatorname{Tr}^m(\omega x) = 0\}$  and  $\mathcal{N}_2(\omega) = \#\{x \in \mathbb{F}_{p^m}: f(x) = 2 \text{ and } \operatorname{Tr}^m(\omega x) = 0\}$ . Then,

$$\mathcal{N}_1(\omega) = \frac{2\mathcal{N}_{sq}(\omega)}{(p-1)} \text{ and } \mathcal{N}_2(\omega) = \frac{2\mathcal{N}_{nsq}(\omega)}{(p-1)}.$$

The following lemma can be deduced from the combination of Lemmas 6 and 8.

**Lemma 10.** Let  $f \in WRPB$ . For  $\omega \in \mathbb{F}_{p^m}^{\star}$ , define

$$\mathcal{N}_{(sq,0)}(\omega) = \#\{x \in \mathbb{F}_{p^m} \colon f(x) \in SQ \cup \{0\} \text{ and } \operatorname{Tr}^m(\omega x) = 0\},\\ \mathcal{N}_{(nsq,0)}(\omega) = \#\{x \in \mathbb{F}_{p^m} \colon f(x) \in NSQ \cup \{0\} \text{ and } \operatorname{Tr}^m(\omega x) = 0\}.$$

Then for every  $\omega \in \mathbb{F}_{p^m}^{\star} \setminus S_f$ , we have  $\mathcal{N}_{(sq,0)}(\omega) = \mathcal{N}_{(nsq,0)}(\omega) = \frac{1}{2}(p+1)p^{m-2}$ . For every  $\omega \in S_f$ ,

$$\mathcal{N}_{(sq,0)}(\omega) = \begin{cases} \frac{1}{2}(p+1)p^{m-2} + \epsilon \frac{1}{2}(p-1)^2 \sqrt{p^*}^{m+s-4}, & \text{if } f^*(\omega) = 0 \text{ or } f^*(\omega) \in SQ, \\ \frac{1}{2}(p+1)(p^{m-2} - \epsilon(p-1)\sqrt{p^*}^{m+s-4}), & \text{if } f^*(\omega) \in NSQ, \\ \frac{1}{2}(p+1)p^{m-2} + \epsilon \frac{1}{2}(p-1)^2 \sqrt{p^*}^{m+s-4}, & \text{if } f^*(\omega) = 0 \text{ or } f^*(\omega) \in NSQ, \\ \frac{1}{2}(p+1)(p^{m-2} - \epsilon(p-1)\sqrt{p^*}^{m+s-4}), & \text{if } f^*(\omega) \in SQ, \end{cases}$$

when m + s is even; otherwise,

$$\mathcal{N}_{(sq,0)}(\omega) = \begin{cases} \frac{1}{2}(p+1)p^{m-2} + \epsilon\eta_0(-1)\frac{1}{2}(p-1)^2\sqrt{p^*}^{m+s-3}, & \text{if } f^*(\omega) = 0, \\ \frac{1}{2}(p+1)p^{m-2} - \epsilon\frac{1}{2}(p-1)\sqrt{p^*}^{m+s-3}(\eta_0(-1)-1), & \text{if } f^*(\omega) \in SQ, \\ \frac{1}{2}(p+1)p^{m-2} - \epsilon\frac{1}{2}(p-1)\sqrt{p^*}^{m+s-3}(\eta_0(-1)+1), & \text{if } f^*(\omega) \in NSQ, \\ \frac{1}{2}(p+1)p^{m-2} - \epsilon\eta_0(-1)\frac{1}{2}(p-1)^2\sqrt{p^*}^{m+s-3}, & \text{if } f^*(\omega) = 0, \\ \frac{1}{2}(p+1)p^{m-2} + \epsilon\frac{1}{2}(p-1)\sqrt{p^*}^{m+s-3}(\eta_0(-1)+1), & \text{if } f^*(\omega) \in SQ, \\ \frac{1}{2}(p+1)p^{m-2} + \epsilon\frac{1}{2}(p-1)\sqrt{p^*}^{m+s-3}(\eta_0(-1)-1), & \text{if } f^*(\omega) \in SQ, \\ \frac{1}{2}(p+1)p^{m-2} + \epsilon\frac{1}{2}(p-1)\sqrt{p^*}^{m+s-3}(\eta_0(-1)-1), & \text{if } f^*(\omega) \in NSQ. \end{cases}$$

# 3 Linear codes from $f \in WRPB$

This section presents the flexible parameters of linear codes constructed from weakly regular plateaued balanced functions. In the literature, there are several construction methods of linear codes based on functions over finite fields. As stated by Ding in [8], we can distinguish two of them from the others, which are called the *first* and *second* generic construction methods based on functions. The first generic construction is defined over  $\mathbb{F}_p$  by

$$\mathcal{C}(F) = \{ \mathbf{c}_{(a,b)} = (\operatorname{Tr}^m(aF(x) + bx))_{x \in \mathbb{F}_{p^m}^*} \colon a, b \in \mathbb{F}_{p^m} \},\$$

where F is a polynomial over  $\mathbb{F}_{p^m}$ . The code  $\mathcal{C}(F)$  is a *p*-ary linear code of length  $p^m - 1$ and dimension at most 2m. The second generic construction of linear codes from functions is defined by assigning a subset  $D = \{d_1, \ldots, d_n\}$  of  $\mathbb{F}_{p^m}$ . A *p*-ary linear code involving Dis defined by

$$\mathcal{C}_D = \{ \mathbf{c}_\omega = (\mathrm{Tr}^m(\omega d_1), \dots, \mathrm{Tr}^m(\omega d_n)) \colon \omega \in \mathbb{F}_{p^m} \},$$
(4)

whose length equals n and dimension at most m. The subset D is usually called the *defining set* of  $C_D$ . The quality of the parameters depends on the selection of the defining set D. This method was first proposed by Ding et. al [6, 7, 9, 11, 12], and a large number of (minimal) linear codes with perfect parameters have been obtained in these papers. Furthermore, this method has been widely studied in the literature, and several (minimal) linear codes with few weights have been constructed from cryptographic functions over

finite fields (for example [8, 22, 23, 24, 25, 29]). We in this paper study the linear codes of the form (4) by selecting the following defining sets

$$D_{0} = \{x \in \mathbb{F}_{p^{m}}^{\star}: f(x) = 0\}, D_{1} = \{x \in \mathbb{F}_{p^{m}}: f(x) = 1\}, D_{2} = \{x \in \mathbb{F}_{p^{m}}: f(x) = 2\}, D_{(0,1)} = \{x \in \mathbb{F}_{p^{m}}^{\star}: f(x) \in \{0,1\}\}, D_{(0,2)} = \{x \in \mathbb{F}_{p^{m}}^{\star}: f(x) \in \{0,2\}\}, D_{(1,2)} = \{x \in \mathbb{F}_{p^{m}}: f(x) \in \{1,2\}\}, D_{sq} = \{x \in \mathbb{F}_{p^{m}}: f(x) \in SQ\}, D_{nsq} = \{x \in \mathbb{F}_{p^{m}}: f(x) \in NSQ\}, D_{(sq,0)} = \{x \in \mathbb{F}_{p^{m}}^{\star}: f(x) \in SQ \cup \{0\}\}, \\D_{(nsq,0)} = \{x \in \mathbb{F}_{p^{m}}^{\star}: f(x) \in NSQ \cup \{0\}\}, \end{cases}$$
(5)

where  $f \in WRPB$ . Since f is a balanced function with f(0) = 0, we have

$$#D_0 = p^{m-1} - 1, 
 #D_1 = #D_2 = p^{m-1}, 
 #D_{(0,1)} = #D_{(0,2)} = 2p^{m-1} - 1, 
 #D_{(1,2)} = 2p^{m-1}, 
 #D_{sq} = #D_{nsq} = p^{m-1}(p-1)/2, 
 #D_{(sq,0)} = #D_{(nsq,0)} = p^{m-1}(p+1)/2 - 1,$$
(6)

which are the lengths of the codes involving these sets. These different selections of the defining sets provide new parameters for the linear codes of the form (4), which discover several new classes of minimal linear codes with few weights. We first consider the defining set  $D_0$  of the form (5), and suppose  $D_0 = \{d_1, \ldots, d_n\}$ . Then a linear code involving  $D_0$  is defined by

$$\mathcal{C}_{D_0} = \{ \mathbf{c}_{\omega} = (\mathrm{Tr}^m(\omega d_1), \dots, \mathrm{Tr}^m(\omega d_n)) \colon \omega \in \mathbb{F}_{p^m} \},\$$

whose length  $n = p^{m-1} - 1$  and dimension at most m. For every  $\omega \in \mathbb{F}_{p^m}^{\star}$ , the Hamming weights  $W_H(\mathbf{c}_{\omega})$  can be derived from Lemma 6, and the weight distribution is determined by Lemmas 1 and 4.

**Theorem 1.** Let  $f \in WRPB$  and  $D_0$  be defined as in (5). When m + s is even, the set  $C_{D_0}$  is a three-weight linear  $[p^{m-1} - 1, m]$  code with weight distribution listed in Table 1.

Proof. From the definition of the code, for every  $\omega \in \mathbb{F}_{p^m}^{\star}$ , the Hamming weight of nonzero codeword  $\mathbf{c}_{\omega}$  is given as  $W_H(\mathbf{c}_{\omega}) = \#D_0 - \mathcal{N}_0(\omega) + 1$ , where  $\mathcal{N}_0(\omega)$  is defined as in Lemma 6. We can then find the Hamming weights by using Lemma 6. For every  $\omega \in \mathcal{S}_f$ ,

$$W_H(\mathbf{c}_{\omega}) = \begin{cases} (p-1)(p^{m-2} - \epsilon(p-1)\sqrt{p^*}^{m+s-4}), & \text{if } f^*(\omega) = 0, \\ (p-1)(p^{m-2} + \epsilon\sqrt{p^*}^{m+s-4}), & \text{if } f^*(\omega) \neq 0, \end{cases}$$

whose weight distribution is determined by Lemma 4. For every  $\omega \in \mathbb{F}_{p^m}^* \setminus S_f$ , we have  $W_H(\mathbf{c}_{\omega}) = (p-1)p^{m-2}$ , and the number of such codewords  $\mathbf{c}_{\omega}$  equals  $p^m - p^{m-s} - 1$  by Lemma 1. These parameters are listed in Table 1. Since  $W_H(\mathbf{c}_{\omega}) > 0$  for every  $\omega \in \mathbb{F}_{p^m}^*$ , the code  $\mathcal{C}_{D_0}$  has  $p^m$  different codewords, namely, its dimension equals m. The proof is then completed.

**Example 1.** For a quadratic 1-plateaued balanced function  $f : \mathbb{F}_{3^5} \to \mathbb{F}_3$ , the code  $\mathcal{C}_{D_0}$  is a three-weight ternary [80, 5, 48] code with weight enumerator  $1 + 60y^{48} + 161y^{54} + 21y^{66}$ . This code is almost optimal since the best known linear codes with length 80 and dimension 5 has d = 53 according to [13].

**Example 2.** For a quadratic 1-plateaued balanced function  $f : \mathbb{F}_{5^3} \to \mathbb{F}_5$ , the code  $\mathcal{C}_{D_0}$  is a three-weight [24, 3, 16] code with weight enumerator  $1 + 24y^{16} + 99y^{20} + 1y^{36}$ . This code is almost optimal by [13].

Remark 3. If m + s is odd, then the code  $C_{D_0}$  has the same parameters of  $C_{D_f}$  in [23, Theorem 1].

The following theorem constructs the code  $C_{D_1}$  of the form (4) involving the defining set  $D_1$ . We recall that

$$\eta_0(-1) = \begin{cases} 1 & \text{if and only if } p \equiv 1 \pmod{4}, \\ -1 & \text{if and only if } p \equiv 3 \pmod{4}. \end{cases}$$

**Theorem 2.** Let  $f \in WRPB$  and  $D_1$  be defined as in (5). Then, the set  $C_{D_1}$  is a threeweight linear  $[p^{m-1},m]$  code whose weight distribution is listed in Tables 2, 3 and 4.

*Proof.* We first state that the length of  $C_{D_1}$  is the size of the defining set  $D_1$ . From its definition, we can easily observe that  $W_H(\mathbf{c}_{\omega}) = \#D_1 - \mathcal{N}_1(\omega)$ , for every  $\omega \in \mathbb{F}_{p^m}^{\star}$ , where  $\mathcal{N}_1(\omega)$  is given in Lemma 9. This lemma is then able to compute the Hamming weights. Suppose that m + s is odd. For every  $\omega \in \mathbb{F}_{p^m}^{\star} \setminus S_f$ , we have  $W_H(\mathbf{c}_{\omega}) = p^{m-2}(p-1)$ ; otherwise,

$$W_{H}(\mathbf{c}_{\omega}) = \begin{cases} (p-1)(p^{m-2} - \epsilon\eta_{0}(-1)\sqrt{p^{*}}^{m+s-3}), & \text{if } f^{*}(\omega) = 0, \\ p^{m-2}(p-1) + \epsilon\sqrt{p^{*}}^{m+s-3}(\eta_{0}(-1)+1), & \text{if } f^{*}(\omega) \in SQ, \\ p^{m-2}(p-1) + \epsilon\sqrt{p^{*}}^{m+s-3}(\eta_{0}(-1)-1), & \text{if } f^{*}(\omega) \in NSQ. \end{cases}$$

The weight distribution is determined by Lemmas 1 and 4. Note that these parameters are listed in Tables 2 and 3 when  $p \equiv 1 \pmod{4}$  and  $p \equiv 3 \pmod{4}$ , respectively. When m + s is even, with the same method, we can find the corresponding parameters listed in Table 4, thereby completing the proof.

**Example 3.** For a quadratic 1-plateaued balanced function  $f : \mathbb{F}_{5^3} \to \mathbb{F}_5$ , the code  $\mathcal{C}_{D_1}$  is a three-weight [25, 3, 16] code with weight enumerator  $1 + 13y^{16} + 99y^{20} + 12y^{26}$ . This code is almost optimal by [13].

The following theorem constructs the code  $\mathcal{C}_{D_{(0,1)}}$  of the form (4) involving the set  $D_{(0,1)}$ .

**Theorem 3.** Let  $f \in WRPB$  and  $D_{(0,1)}$  be defined as in (5). Then, the set  $C_{D_{(0,1)}}$  is a four-weight linear  $[2p^{m-1} - 1, m]$  code with weight distribution listed in Tables 5 and 6.

Proof. We proceed the proof only when m + s is odd. For every  $\omega \in \mathbb{F}_{p^m}^{\star}$ , the Hamming weight  $W_H(\mathbf{c}_{\omega}) = \#D_{(0,1)} - \mathcal{N}_0(\omega) - \mathcal{N}_1(\omega) + 1$  can be found by using Lemmas 6 and 9. For every  $\omega \in \mathbb{F}_{p^m}^{\star} \setminus S_f$ , we have  $W_H(\mathbf{c}_{\omega}) = 2(p-1)p^{m-2}$ ; otherwise,

$$W_{H}(\mathbf{c}_{\omega}) = \begin{cases} 2(p-1)p^{m-2} - \epsilon\eta_{0}(-1)(p-1)\sqrt{p^{*}}^{m+s-3}, & \text{if } f^{*}(\omega) = 0, \\ 2(p-1)p^{m-2} - \epsilon(p-2-\eta_{0}(-1))\sqrt{p^{*}}^{m+s-3} & \text{if } f^{*}(\omega) \in SQ, \\ 2(p-1)p^{m-2} + \epsilon(p-2+\eta_{0}(-1))\sqrt{p^{*}}^{m+s-3} & \text{if } f^{*}(\omega) \in NSQ. \end{cases}$$

The weight distribution is determined by Lemmas 1 and 4. When m + s is even, with the same method, we can clearly find the corresponding parameters listed in Table 6. Hence the proof is complete.

We point out that the code  $C_{D_{(0,1)}}$  in Theorem 3 is the three-weight ternary code when p = 3. As an example, we give the following code.

**Example 4.** For a quadratic 1-plateaued balanced function  $f : \mathbb{F}_{3^4} \to \mathbb{F}_3$ , the code  $\mathcal{C}_{D_{(0,1)}}$  is a three-weight ternary [53, 4, 30] code with weight enumerator  $1 + 9y^{30} + 65y^{36} + 6y^{42}$ . This code is almost optimal since the best known linear code has d = 35 by [13].

We next use the defining set  $D_2$  from (5) to define the code  $C_{D_2}$  of the form (4), whose parameters are collected in the following theorem.

**Theorem 4.** Let  $f \in WRPB$  and  $D_2$  be defined as in (5). When m + s is odd, the set  $C_{D_2}$  is a three-weight linear  $[p^{m-1}, m]$  code with weight distribution given in Tables 7 and 8.

*Proof.* For every  $\omega \in \mathbb{F}_{p^m}^{\star}$ , we have  $W_H(\mathbf{c}_{\omega}) = \#D_2 - \mathcal{N}_2(\omega)$ , where  $\mathcal{N}_2(\omega)$  is given in Lemma 9. It follows then from Lemma 9 that we have  $W_H(\mathbf{c}_{\omega}) = (p-1)p^{m-2}$  if  $\omega \in \mathbb{F}_{p^m}^{\star} \setminus \mathcal{S}_f$ ; otherwise,

$$W_{H}(\mathbf{c}_{\omega}) = \begin{cases} (p-1)(p^{m-2} + \epsilon\eta_{0}(-1)\sqrt{p^{*}}^{m+s-3}), & \text{if } f^{*}(\omega) = 0, \\ p^{m-2}(p-1) - \epsilon\sqrt{p^{*}}^{m+s-3}(\eta_{0}(-1) - 1), & \text{if } f^{*}(\omega) \in SQ, \\ p^{m-2}(p-1) - \epsilon\sqrt{p^{*}}^{m+s-3}(\eta_{0}(-1) + 1), & \text{if } f^{*}(\omega) \in NSQ. \end{cases}$$

The weight distribution is determined by Lemmas 1 and 4. The parameters are listed in Tables 7 and 8 when  $p \equiv 1 \pmod{4}$  and  $p \equiv 3 \pmod{4}$ , respectively, thereby completing the proof.

Remark 4. If m + s is even, then the code  $C_{D_2}$  has the same parameters of  $C_{D_1}$  in Theorem 2.

We further study the code  $C_{D_{(0,2)}}$  of the form (4) involving  $D_{(0,2)}$ . The following theorem collects its parameters.

**Theorem 5.** Let  $f \in WRPB$  and  $D_{(0,2)}$  be defined as in (5). When m + s is odd, the set  $\mathcal{C}_{D_{(0,2)}}$  is a four-weight linear  $[2p^{m-1} - 1, m]$  code with weight distribution given in Table 9. Proof. For every  $\omega \in \mathbb{F}_{p^m}^{\star}$ , the Hamming weight  $W_H(\mathbf{c}_{\omega}) = \#D_{(0,2)} - \mathcal{N}_0(\omega) - \mathcal{N}_2(\omega) + 1$  can be found by considering Lemmas 6 and 9. Then we have  $W_H(\mathbf{c}_{\omega}) = 2(p-1)p^{m-2}$  if  $\omega \in \mathbb{F}_{p^m}^{\star} \setminus \mathcal{S}_f$ ; otherwise,

$$W_{H}(\mathbf{c}_{\omega}) = \begin{cases} 2(p-1)p^{m-2} + \epsilon \eta_{0}(-1)(p-1)\sqrt{p^{*}}^{m+s-3}, & \text{if } f^{*}(\omega) = 0, \\ 2(p-1)p^{m-2} - \epsilon(p-2+\eta_{0}(-1))\sqrt{p^{*}}^{m+s-3} & \text{if } f^{*}(\omega) \in SQ, \\ 2(p-1)p^{m-2} + \epsilon(p-2-\eta_{0}(-1))\sqrt{p^{*}}^{m+s-3} & \text{if } f^{*}(\omega) \in NSQ, \end{cases}$$

whose weight distributions are, respectively, determined by Lemmas 1 and 4. Hence the proof is completed.  $\hfill \Box$ 

The following theorem constructs the code  $\mathcal{C}_{D_{(1,2)}}$  of the form (4) involving  $D_{(1,2)}$ .

**Theorem 6.** Let  $f \in WRPB$  and  $D_{(1,2)}$  be defined as in (5). Then, the set  $C_{D_{(1,2)}}$  is a three-weight linear  $[2p^{m-1}, m]$  code with weight distribution given in Tables 10 and 11.

Proof. For every  $\omega \in \mathbb{F}_{p^m}^{\star}$ , the Hamming weight  $W_H(\mathbf{c}_{\omega}) = \#D_{(1,2)} - \mathcal{N}_1(\omega) - \mathcal{N}_2(\omega)$  can be computed by using Lemma 9. Suppose that m + s is odd. We then have  $W_H(\mathbf{c}_{\omega}) = 2(p-1)p^{m-2}$  if  $\omega \in \mathbb{F}_{p^m}^{\star} \setminus \mathcal{S}_f$ ; otherwise,

$$W_{H}(\mathbf{c}_{\omega}) = \begin{cases} 2(p-1)p^{m-2}, & \text{if } f^{\star}(\omega) = 0, \\ 2(p-1)p^{m-2} + 2\epsilon\sqrt{p^{\star}}^{m+s-3} & \text{if } f^{\star}(\omega) \in SQ, \\ 2(p-1)p^{m-2} - 2\epsilon\sqrt{p^{\star}}^{m+s-3}, & \text{if } f^{\star}(\omega) \in NSQ, \end{cases}$$

whose weight distributions are, respectively, determined by Lemmas 1 and 4. We do not proceed the case of m + s is even since the corresponding parameters listed in Table 11 can be easily obtained with the same method. The proof hence is complete.

The following theorem considers the code  $\mathcal{C}_{D_{sq}}$  of the form (4) involving  $D_{sq}$ .

**Theorem 7.** Let  $f \in WRPB$  and  $D_{sq}$  be defined as in (5). Then, the set  $C_{D_{sq}}$  is a threeweight linear  $[p^{m-1}(p-1)/2, m]$  code whose weight distribution is given in Tables 12, 13 and 14.

Proof. For every  $\omega \in \mathbb{F}_{p^m}^{\star}$ , the Hamming weight  $W_H(\mathbf{c}_{\omega}) = \#D_{sq} - \mathcal{N}_{sq}(\omega)$  follows from Lemma 8. We proceed the proof only when m + s is odd. If  $\omega \in \mathbb{F}_{p^m}^{\star} \setminus S_f$ , then we have  $W_H(\mathbf{c}_{\omega}) = p^{m-2}(p-1)^2/2$ ; otherwise,

$$W_{H}(\mathbf{c}_{\omega}) = \begin{cases} \frac{1}{2}(p-1)^{2}(p^{m-2}-\epsilon\eta_{0}(-1)\sqrt{p^{*}}^{m+s-3}), & \text{if } f^{*}(\omega) = 0, \\ p^{m-2}(p-1)^{2}/2 + \epsilon\frac{1}{2}(p-1)\sqrt{p^{*}}^{m+s-3}(\eta_{0}(-1)+1), & \text{if } f^{*}(\omega) \in SQ, \\ p^{m-2}(p-1)^{2}/2 + \epsilon\frac{1}{2}(p-1)\sqrt{p^{*}}^{m+s-3}(\eta_{0}(-1)-1), & \text{if } f^{*}(\omega) \in NSQ. \end{cases}$$

The weight distribution can be determined by using Lemmas 1 and 4. The parameters are listed in Tables 12 and 13 when  $p \equiv 1 \pmod{4}$  and  $p \equiv 3 \pmod{4}$ , respectively. When m + s is even, we immediately obtain the corresponding parameters listed in Table 14, completing the proof.

We use the defining set  $D_{(sq,0)}$  from (5) to define the code  $\mathcal{C}_{D_{(sq,0)}}$  of the form (4), whose parameters are collected in the following theorem.

**Theorem 8.** Let  $f \in WRPB$  and  $D_{(sq,0)}$  be defined as in (5). Then, the set  $C_{D_{(sq,0)}}$  is a three-weight linear  $[p^{m-1}(p+1)/2 - 1, m]$  code whose weight distribution is documented in Tables 15, 16 and 17.

*Proof.* For every  $\omega \in \mathbb{F}_{p^m}^{\star}$ ,  $W_H(\mathbf{c}_{\omega}) = \#D_{(sq,0)} - \mathcal{N}_{(sq,0)}(\omega) + 1$  follows from Lemma 8. When m + s is odd, we have  $W_H(\mathbf{c}_{\omega}) = p^{m-2}(p^2 - 1)/2$  if  $\omega \in \mathbb{F}_{p^m}^{\star} \setminus \mathcal{S}_f$ ; otherwise,

$$W_{H}(\mathbf{c}_{\omega}) = \begin{cases} p^{m-2}(p^{2}-1)/2 - \epsilon\eta_{0}(-1)\frac{1}{2}(p-1)^{2}\sqrt{p^{*}}^{m+s-3}, & \text{if } f^{*}(\omega) = 0, \\ p^{m-2}(p^{2}-1)/2 + \epsilon\frac{1}{2}(p-1)\sqrt{p^{*}}^{m+s-3}(\eta_{0}(-1)-1), & \text{if } f^{*}(\omega) \in SQ, \\ p^{m-2}(p^{2}-1)/2 + \epsilon\frac{1}{2}(p-1)\sqrt{p^{*}}^{m+s-3}(\eta_{0}(-1)+1), & \text{if } f^{*}(\omega) \in NSQ, \end{cases}$$

which are listed in Tables 15 and 16 when  $p \equiv 1 \pmod{4}$  and  $p \equiv 3 \pmod{4}$ , respectively. When m + s is even, it is easy to get the corresponding parameters listed in Table 17. Finally, the weight distribution is determined by using Lemmas 1 and 4, completing the proof.

We below introduce the parameters of the code  $C_{D_{nsq}}$  of the form (4) involving  $D_{nsq}$ .

**Theorem 9.** Let  $f \in WRPB$  and  $D_{nsq}$  be defined as in (5). When m + s is odd, the set  $C_{D_{nsq}}$  is a three-weight linear  $[p^{m-1}(p-1)/2, m]$  code with weight distribution given in Tables 18 and 19.

Proof. For every  $\omega \in \mathbb{F}_{p^m}^{\star}$ , the Hamming weight  $W_H(\mathbf{c}_{\omega}) = \#D_{nsq} - \mathcal{N}_{nsq}(\omega)$  follows from Lemma 8. We then have  $W_H(\mathbf{c}_{\omega}) = \frac{1}{2}(p-1)^2 p^{m-2}$  if  $\omega \in \mathbb{F}_{p^m}^{\star} \setminus \mathcal{S}_f$ ; otherwise,

$$W_{H}(\mathbf{c}_{\omega}) = \begin{cases} \frac{1}{2}(p-1)^{2}(p^{m-2}+\epsilon\eta_{0}(-1)\sqrt{p^{*}}^{m+s-3}), & \text{if } f^{*}(\omega) = 0, \\ p^{m-2}(p-1)^{2}/2 - \epsilon\frac{1}{2}(p-1)\sqrt{p^{*}}^{m+s-3}(\eta_{0}(-1)-1), & \text{if } f^{*}(\omega) \in SQ, \\ p^{m-2}(p-1)^{2}/2 - \epsilon\frac{1}{2}(p-1)\sqrt{p^{*}}^{m+s-3}(\eta_{0}(-1)+1), & \text{if } f^{*}(\omega) \in NSQ. \end{cases}$$

The weight distribution is determined with the help of Lemmas 1 and 4, completing the proof.  $\hfill \Box$ 

Remark 5. If m+s is even, then the code  $\mathcal{C}_{D_{nsq}}$  has the same parameters of  $\mathcal{C}_{D_{sq}}$  in Theorem 7.

We finally use the defining set  $D_{(nsq,0)}$  from (5) to define the code  $\mathcal{C}_{D_{(nsq,0)}}$  of the form (4), whose parameters are listed in the following theorem.

**Theorem 10.** Let  $f \in WRPB$  and  $D_{(nsq,0)}$  be defined as in (5). When m + s is odd, the set  $C_{D_{(nsq,0)}}$  is a three-weight  $[p^{m-1}(p+1)/2 - 1, m]$  code with weight distribution listed in Tables 20 and 21.

*Proof.* For every  $\omega \in \mathbb{F}_{p^m}^{\star}$ ,  $W_H(\mathbf{c}_{\omega}) = \#D_{(nsq,0)} - \mathcal{N}_{(nsq,0)}(\omega) + 1$  follows from Lemma 8. Then we have  $W_H(\mathbf{c}_{\omega}) = p^{m-2}(p^2 - 1)/2$  if  $\omega \in \mathbb{F}_{p^m}^{\star} \setminus \mathcal{S}_f$ ; otherwise,

$$W_{H}(\mathbf{c}_{\omega}) = \begin{cases} p^{m-2}(p^{2}-1)/2 + \epsilon \eta_{0}(-1)\frac{1}{2}(p-1)^{2}\sqrt{p^{*}}^{m+s-3}, & \text{if } f^{*}(\omega) = 0, \\ p^{m-2}(p^{2}-1)/2 - \epsilon\frac{1}{2}(p-1)\sqrt{p^{*}}^{m+s-3}(\eta_{0}(-1)+1), & \text{if } f^{*}(\omega) \in SQ, \\ p^{m-2}(p^{2}-1)/2 - \epsilon\frac{1}{2}(p-1)\sqrt{p^{*}}^{m+s-3}(\eta_{0}(-1)-1), & \text{if } f^{*}(\omega) \in NSQ. \end{cases}$$

The weight distribution is determined by Lemmas 1 and 4, thereby completing the proof.  $\hfill \Box$ 

Remark 6. If m + s is even, then  $\mathcal{C}_{D_{(nsq,0)}}$  has the same parameters of  $\mathcal{C}_{D_{(sq,0)}}$  in Theorem 8.

*Remark* 7. The length and dimension of each constructed code follows, respectively, from (6) and its weight distribution.

We end this section by proposing a shorter linear code, which is called *punctured code*, for the code  $C_{D_0}$  defined as in (4). For  $f \in WRPB$ , we have that f(x) = 0 if and only if f(ax) = 0 for every  $x \in \mathbb{F}_{p^m}$  and  $a \in \mathbb{F}_p^*$ . Then we select a subset  $\overline{D}_0$  of the defining set  $D_0$  of  $C_{D_0}$  such that  $\bigcup_{a \in \mathbb{F}_p^*} a\overline{D}_0$  is a partition of  $D_0$ , namely,

$$D_0 = \mathbb{F}_p^{\star} \overline{D}_0 = \{ a \bar{d} \colon a \in \mathbb{F}_p^{\star} \text{ and } \bar{d} \in \overline{D}_0 \},$$
(7)

where we have  $\frac{\overline{d_1}}{d_2} \notin \mathbb{F}_p^{\star}$  for every  $\overline{d_1}, \overline{d_2} \in \overline{D}_0$ . Notice that for every  $\omega \in \mathbb{F}_{p^m}^{\star}$ , we have  $\#\{x \in D_0: f(x) = 0 \text{ and } \operatorname{Tr}^m(\omega x) = 0\} = (p-1)\#\{x \in \overline{D}_0: f(x) = 0 \text{ and } \operatorname{Tr}^m(\omega x) = 0\}$ . Hence, the code  $\mathcal{C}_{D_0}$  can be punctured into a shorter linear code  $\mathcal{C}_{\overline{D}_0}$  involving the defining set  $\overline{D}_0$ . This method decreases the minimum Hamming distance and length of the original code while its dimension does not change. The punctured codes then may be optimal codes by [13]. The parameters of the punctured code  $\mathcal{C}_{\overline{D}_0}$  are collected in the following corollary.

**Corollary 1.** The punctured code  $C_{\overline{D}_0}$  of the code  $C_{D_0}$  in Theorem 1 is a three-weight linear  $[(p^{m-1}-1)/(p-1),m]$  code with weight distribution listed in Table 22.

**Example 5.** The punctured version  $C_{\overline{D}_0}$  of Example 1 is a three-weight ternary [40, 5, 24] code with weight enumerator  $1 + 60y^{24} + 161y^{27} + 21y^{33}$ . This code is optimal by [13].

**Example 6.** The punctured version  $C_{\overline{D}_0}$  of Example 2 is a three-weight [12, 3, 8] code over  $\mathbb{F}_5$  with weight enumerator  $1 + 24y^8 + 99y^{10} + 1y^{18}$ . This code is optimal by [13].

*Remark* 8. The projective three-weight punctured code of Corollary 1 provides an association scheme given in [2].

When p = 3, the code  $C_{D_{(1,2)}}$  in Theorem 6 can be punctured into a shorter linear code  $C_{\overline{D}_{(1,2)}}$  involving the defining set  $\overline{D}_{(1,2)}$  defined as in (7)

**Corollary 2.** The punctured code  $C_{\overline{D}_{(1,2)}}$  of Theorem 6 is a three-weight ternary linear  $[3^{m-1},m]$  code over  $\mathbb{F}_3$  with weight distribution given in Tables 23 and 24, when p = 3.

**Example 7.** For a quadratic 1-plateaued balanced function  $f : \mathbb{F}_{3^3} \to \mathbb{F}_3$ , the punctured code  $\mathcal{C}_{\overline{D}_{(1,2)}}$  is a three-weight ternary [9, 3, 5] code with weight enumerator  $1 + 4y^5 + 17y^6 + 5y^8$ . This code is almost optimal owing to the Griesmer bound.

### 4 Application of the constructed codes in secret sharing

In this section, we study an application of the constructed codes in secret sharing.

We first recall the the following sufficient condition for minimal codes introduced by Ashikhmin et al. [1]. Let  $\mathcal{C}$  be a linear code over  $\mathbb{F}_p$  and denote by  $w_{\min}$  and  $w_{\max}$  the minimum and maximum Hamming weights of its nonzero codewords, respectively. Then,  $\mathcal{C}$  is a minimal code if

$$\frac{p-1}{p} < \frac{w_{\min}}{w_{\max}}.$$
(8)

With the help of the condition in (8), we observe that our codes are minimal, thereby they have an interesting application in secret sharing.

We recall that  $f : \mathbb{F}_{p^m} \to \mathbb{F}_p$  is an *s*-plateaued balanced function from the class *WRPB*, where  $s \in \{1, \ldots, m\}$ . We now see that the code  $\mathcal{C}_{D_0}$  in Theorem 1 is minimal for  $s \in \{1, \ldots, m-4\}$ , and similarly the others can be easily seen by putting a necessary bound on  $s \in \{1, \ldots, m\}$ . We provide the parameters of our minimal codes in the following propositions. Suppose that the sign  $\epsilon \eta_0^{(m+s)/2}(-1)$  and  $\epsilon \eta_0^{(m+s-3)/2}(-1)$  is, respectively, denoted by  $\epsilon_0$  and  $\epsilon_1$ .

**Proposition 4.** The code  $C_{D_0}$  in Theorem 1 is minimal over  $\mathbb{F}_p$  for  $1 \leq s \leq m-4$  with parameters  $[p^{m-1}-1, m, (p-1)(p^{m-2}-(p-1)\sqrt{p^{m+s-4}})]$  if  $\epsilon_0 = 1$ , and  $[p^{m-1}-1, m, (p-1)(p^{m-2}-\sqrt{p^{m+s-4}})]$ ; otherwise.

Proof. If  $\epsilon_0 = 1$ , then we have  $w_{\min} = (p-1)(p^{m-2} - (p-1)\sqrt{p}^{m+s-4})$  and  $w_{\max} = (p-1)(p^{m-2} + \sqrt{p}^{m+s-4})$ . Otherwise,  $w_{\min} = (p-1)(p^{m-2} - \sqrt{p}^{m+s-4})$  and  $w_{\max} = (p-1)(p^{m-2} + (p-1)\sqrt{p}^{m+s-4})$ . For both cases, the sufficient condition in (8) is satisfied when  $1 \le s \le m-4$ . Hence, this observation completes the proof.

**Proposition 5.** The code  $C_{D_1}$  in Theorem 2 is minimal over  $\mathbb{F}_p$ . When m + s is odd with  $1 \leq s \leq m-5$ , we have  $[p^{m-1}, m, (p-1)(p^{m-2} - \sqrt{p}^{m+s-3})]$  if  $\epsilon = 1$  when  $p \equiv 1 \pmod{4}$  and  $\epsilon_1 = -1$  when  $p \equiv 3 \pmod{4}$ . Otherwise,  $[p^{m-1}, m, (p-1)p^{m-2} - 2\sqrt{p}^{m+s-3}]$ . When m + s is even with  $1 \leq s \leq m-4$ , we have  $[p^{m-1}, m, (p-1)p^{m-2} - (p+1)\sqrt{p}^{m+s-4}]$  if  $\epsilon_0 = 1$ , and  $[p^{m-1}, m, (p-1)(p^{m-2} - \sqrt{p}^{m+s-4})]$ ; otherwise.

**Proposition 6.** The code  $C_{D_{(0,1)}}$  in Theorem 3 is minimal over  $\mathbb{F}_p$ . When m + s is odd with  $1 \leq s \leq m-3$ , we have  $[2p^{m-1} - 1, m, (p-1)(2p^{m-2} - \sqrt{p}^{m+s-3})]$ . When m + s is even with  $1 \leq s \leq m-4$ , we have  $[2p^{m-1} - 1, m, (p-1)(2p^{m-2} - (p-2)\sqrt{p}^{m+s-4})]$  if  $\epsilon_0 = 1$ , and  $[2p^{m-1} - 1, m, 2(p-1)(p^{m-2} - \sqrt{p}^{m+s-4})]$ ; otherwise.

**Proposition 7.** The code  $C_{D_2}$  in Theorem 4 is minimal over  $\mathbb{F}_p$  for  $1 \le s \le m-5$ . If  $\epsilon = 1$  when  $p \equiv 1 \pmod{4}$  and  $\epsilon_1 = -1$  when  $p \equiv 3 \pmod{4}$ , then we have  $[p^{m-1}, m, p^{m-2}(p-1) - 2\sqrt{p^{m+s-3}}]$ , and  $[p^{m-1}, m, (p-1)(p^{m-2} - \sqrt{p^{m+s-3}})]$ ; otherwise.

**Proposition 8.** The code  $C_{D_{(0,2)}}$  in Theorem 5 is the minimal  $[2p^{m-1}-1, m, (p-1)(2p^{m-2}-\sqrt{p^{m+s-3}})]$  code over  $\mathbb{F}_p$  for  $1 \leq s \leq m-3$ .

**Proposition 9.** The code  $C_{D_{(1,2)}}$  in Theorem 6 is minimal over  $\mathbb{F}_p$ . When m + s is odd with  $1 \leq s \leq m-3$ , we have  $[2p^{m-1}, m, 2(p-1)p^{m-2} - 2\sqrt{p}^{m+s-3}]$ . When m+s is even, we have  $[2p^{m-1}, m, 2(p-1)p^{m-2} - 2\sqrt{p}^{m+s-4}]$  if  $\epsilon_0 = 1$ ; otherwise,  $[2p^{m-1}, m, 2(p-1)(p^{m-2} - \sqrt{p}^{m+s-4})]$ , for  $1 \leq s \leq m-2$  and  $1 \leq s \leq m-4$ , respectively.

**Proposition 10.** The code  $C_{D_{sq}}$  in Theorem 7 is minimal over  $\mathbb{F}_p$ . When m + s is odd with  $1 \leq s \leq m-5$ , if  $\epsilon = 1$  when  $p \equiv 1 \pmod{4}$  and  $\epsilon_1 = -1$  when  $p \equiv 3 \pmod{4}$ , we have  $[p^{m-1}(p-1)/2, m, (p-1)^2(p^{m-2} - \sqrt{p^{m+s-3}})/2]$ ; otherwise,  $[p^{m-1}(p-1)/2, m, (p-1)(p^{m-2}(p-1)/2 - \sqrt{p^{m+s-3}})]$ . When m + s is even with  $1 \leq s \leq m-4$ , we have  $[p^{m-1}(p-1)/2, m, \frac{1}{2}(p-1)((p-1)p^{m-2} - (p+1)\sqrt{p^{m+s-4}})]$  if  $\epsilon_0 = 1$ , and  $[p^{m-1}(p-1)/2, m, \frac{1}{2}(p-1)^2(p^{m-2} - \sqrt{p^{m+s-4}})]$ ; otherwise.

**Proposition 11.** The code  $C_{D_{(sq,0)}}$  in Theorem 8 is minimal over  $\mathbb{F}_p$ . When m + s is odd with  $1 \leq s \leq m-3$ , if  $\epsilon = 1$  when  $p \equiv 1 \pmod{4}$  and  $\epsilon_1 = -1$  when  $p \equiv 3 \pmod{4}$ , we have  $[p^{m-1}(p+1)/2 - 1, m, \frac{1}{2}(p-1)(p^{m-2}(p+1) - (p-1)\sqrt{p^{m+s-3}})]$ ; otherwise,  $[p^{m-1}(p+1)/2 - 1, m, p^{m-2}(p^2 - 1)/2 - (p-1)\sqrt{p^{m+s-3}}]$ . When m + s is even with  $1 \leq s \leq m-4$ , we have  $[p^{m-1}(p+1)/2 - 1, m, \frac{1}{2}(p-1)((p+1)p^{m-2} - (p-1)\sqrt{p^{m+s-4}})]$  if  $\epsilon_0 = 1$ , and  $[p^{m-1}(p+1)/2 - 1, m, \frac{1}{2}(p^2 - 1)(p^{m-2} - \sqrt{p^{m+s-4}})]$ ; otherwise.

**Proposition 12.** The code  $C_{D_{nsq}}$  in Theorem 9 is minimal over  $\mathbb{F}_p$  for  $1 \le s \le m-5$ . If  $\epsilon = 1$  when  $p \equiv 1 \pmod{4}$  and  $\epsilon_1 = -1$  when  $p \equiv 3 \pmod{4}$ , then we have  $[p^{m-1}(p-1)/2, m, (p-1)(p^{m-2}(p-1)/2 - \sqrt{p^{m+s-3}})]$ ; otherwise,  $[p^{m-1}(p-1)/2, m, \frac{1}{2}(p-1)^2(p^{m-2} - \sqrt{p^{m+s-3}})]$ .

**Proposition 13.** The code  $C_{D_{(nsq,0)}}$  in Theorem 10 is minimal over  $\mathbb{F}_p$  for  $1 \leq s \leq m-3$ . If  $\epsilon = 1$  when  $p \equiv 1 \pmod{4}$  and  $\epsilon_1 = -1$  when  $p \equiv 3 \pmod{4}$ , then we have  $[p^{m-1}(p+1)/2 - 1, m, (p-1)(p^{m-2}(p+1)/2 - \sqrt{p}^{m+s-3})];$  otherwise,  $[p^{m-1}(p+1)/2 - 1, m, \frac{1}{2}(p-1)(p^{m-2}(p+1) - (p-1)\sqrt{p}^{m+s-3})].$ 

As the constructed codes are all minimal codes, secret sharing schemes based on their dual codes have high democracy introduced in the following theorem.

**Theorem 11.** [4, 10] Let C be a minimal linear [n, k, d] code over  $\mathbb{F}_p$  with the generator matrix  $G = [\mathbf{g}_0, \mathbf{g}_1, \ldots, \mathbf{g}_{n-1}]$ , and let  $d^{\perp}$  represent the minimum Hamming distance of its dual code  $C^{\perp}$ . Then in the SSS based on  $C^{\perp}$ , the number of participants equals n - 1, and the number of minimal access sets equals  $p^{k-1}$ .

- For d<sup>⊥</sup> = 2, if g<sub>i</sub>, 1 ≤ i ≤ n − 1, is a multiple of g<sub>0</sub>, then a participant P<sub>i</sub> is in every minimal access set; else, P<sub>i</sub> is in (p − 1)p<sup>k−2</sup> minimal access sets.
- For  $d^{\perp} \geq 3$ , for each fixed  $1 \leq l \leq \min\{k-1, d^{\perp}-2\}$ , every set of l participants is involved in  $(p-1)^l p^{k-(l+1)}$  minimal access sets.

To describe the access structures of SSS based on the dual codes of our minimal codes, we are first interested in the minimum Hamming distance of the dual code. By *the MacWilliams identity* (F. J. MacWilliams, 1963), the weight enumerator (and hence minimum Hamming distance) of the dual code is obtained from that of the original code.

**Theorem 12.** [18, Theorem 3.5.3] Let  $\mathcal{C}$  be a linear [n,k] code over  $\mathbb{F}_q$  with weight enumerator A(z). The weight enumerator of  $\mathcal{C}^{\perp}$  is denoted by  $A^{\perp}(z)$ . Then

$$A^{\perp}(z) = q^{-k} (1 + (q-1)z)^n A\left(\frac{1-z}{1+(q-1)z}\right).$$

With the help of Theorem 12, one can find the weight enumerator and minimum Hamming distance of the dual code of each code constructed in this paper. However, we prefer to use the following simple method in order to find  $d^{\perp}$ . It is a well known fact that two elements of each codeword are dependent if and only if the minimum Hamming distance of the dual code is 2. In our framework, the dual code  $C_{D_0}^{\perp}$  of Theorem 1 has  $d^{\perp} = 2$  if and only if for any two different elements  $d_i, d_j \in D_0$  and two elements  $c_i, c_j \in \mathbb{F}_p^{\star}$ , we have

$$c_i \operatorname{Tr}^n(xd_i) + c_j \operatorname{Tr}^n(xd_j) = 0$$

for every  $x \in \mathbb{F}_{p^m}$ , which holds when  $d_j = -d_i$  and  $c_i = c_j = 1$ . This result confirms  $d^{\perp} = 2$ . With the same reason, the dual codes of Theorems 2, 3, 4, 5, 6, 7, 8, 9, 10 have  $d^{\perp} = 2$ . Hence, one can give the SSS based on the dual codes of these minimal codes by considering Theorem 11. As an example, we deal with the following one.

**Corollary 3.** Let  $C_{D_{(0,1)}}$  be the minimal  $[2p^{m-1} - 1, m, (p-1)(2p^{m-2} - (p-2)\sqrt{p}^{m+s-4})]$ code in Theorem 3 with  $G = [\mathbf{g}_0, \mathbf{g}_1, \dots, \mathbf{g}_{2p^{m-1}-2}]$ . Then in the SSS based on  $C_{D_{(0,1)}}^{\perp}$  with  $d^{\perp} = 2$ , the number of participants is  $2p^{m-1} - 2$  and the number of minimal access sets is  $p^{m-1}$ . Besides,  $P_i$  must be in all minimal access sets if  $\mathbf{g}_i$ ,  $i \neq 0$ , is a multiple of  $\mathbf{g}_0$ ; otherwise, in  $(p-1)p^{m-2}$  minimal access sets.

We finally see that  $d^{\perp}$  of the dual code  $\mathcal{C}_{\overline{D}_0}^{\perp}$  of Corollary 1 is at least 3. From (7), we have  $D_0 = \mathbb{F}_p^{\star}\overline{D}_0$ . Clearly,  $d^{\perp} = 2$  if and only if for any two different elements  $\bar{d}_i, \bar{d}_j \in \overline{D}_0$  and two elements  $a_i, a_j \in \mathbb{F}_p^{\star}$ , we have  $\operatorname{Tr}^n(x(a_i\bar{d}_i + a_j\bar{d}_j)) = 0$  for every  $x \in \mathbb{F}_{p^m}$ ; that is,  $a_i\bar{d}_i + a_j\bar{d}_j = 0$ , which contradicts  $\frac{\bar{d}_i}{d_i} \notin \mathbb{F}_p^{\star}$ . This observation says  $d^{\perp} \geq 3$ .

**Corollary 4.** Let  $C_{\overline{D}_0}$  be the minimal  $[(p^{m-1}-1)/(p-1),m]$  code in Corollary 1. Then in the SSS based on  $C_{\overline{D}_0}^{\perp}$  with  $d^{\perp} \geq 3$ , the number of participants is  $(p^{m-1}-1)/(p-1)-1$ and the number of minimal access sets is  $p^{m-1}$ . For each fixed  $1 \leq l \leq \min\{m-1, d^{\perp}-2\}$ , every set of l participants is involved in  $(p-1)^l p^{m-(l+1)}$  minimal access sets.

**Example 8.** Let  $C_{\overline{D}_0}$  be the three-weight ternary minimal [40, 5, 24] code in Example 5. Then in the SSS based on  $C_{\overline{D}_0}^{\perp}$  with  $d^{\perp} \geq 3$ , the number of participants and minimal access sets is, respectively, 39 and 81. For l = 1, each participant is a member of 54 minimal access sets.

## 5 Conclusion

The main objectives of the paper are twofold: to construct minimal linear codes from functions and to give their application in secret sharing. To do this, we first pushed the use of weakly regular plateaued balanced functions over the finite fields of odd characteristic, introduced recently by Mesnager et al. [20, 22]. We then obtained several classes of threeweight and four-weight minimal linear codes from these functions with some homogeneous conditions. This paper provides the first construction of minimal linear codes with few weights from such balanced functions based on the second generic construction. To the best of our knowledge, the constructed minimal codes are inequivalent to the known ones in the literature. We finally derived secret sharing schemes with nice access structures from the dual codes of our minimal codes.

# Acknowledgment

The author is very grateful to the Prof. Dr. Sihem Mesnager for her valuable scientific comments and suggestions that improved the quality of the paper. This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

### References

- A. Ashikhmin, A. Barg, Minimal vectors in linear codes, IEEE Transactions on Information Theory 44 (5) ((1998)) 2010–2017.
- [2] A. Calderbank, J. Goethals, Three-weight codes and association schemes, Philips J. Res 39 (4-5) (1984) 143–152.
- [3] C. Carlet, P. Charpin, V. Zinoviev, Codes, bent functions and permutations suitable for des-like cryptosystems, Designs, Codes and Cryptography 15 (2) (1998) 125–156.

- [4] C. Carlet, C. Ding, J. Yuan, Linear codes from perfect nonlinear mappings and their secret sharing schemes, IEEE Transactions on Information Theory 51 (6) (2005) 2089– 2102.
- [5] A. Çeşmelioğlu, G. McGuire, W. Meidl, A construction of weakly and non-weakly regular bent functions, Journal of Combinatorial Theory, Series A 119 (2) (2012) 420– 429.
- [6] C. Ding, A class of three-weight and four-weight codes, in: International Conference on Coding and Cryptology, Springer, 2009, pp. 34–42.
- [7] C. Ding, Linear codes from some 2-designs, IEEE Transactions on information theory 61 (6) (2015) 3265–3275.
- [8] C. Ding, A construction of binary linear codes from boolean functions, Discrete mathematics 339 (9) (2016) 2288–2303.
- [9] C. Ding, H. Niederreiter, Cyclotomic linear codes of order 3, IEEE transactions on information theory 53 (6) (2007) 2274–2277.
- [10] C. Ding, J. Yuan, Covering and secret sharing with linear codes, DMTCS 2731 (2003) 11–25.
- [11] K. Ding, C. Ding, Binary linear codes with three weights, IEEE Communications Letters 18 (11) (2014) 1879–1882.
- [12] K. Ding, C. Ding, A class of two-weight and three-weight codes and their applications in secret sharing, IEEE Transactions on Information Theory 61 (11) (2015) 5835–5842.
- [13] M. Grassl, Bounds on the minimum distance of linear codes, http://www.codetables.de.
- [14] T. Helleseth, A. Kholosha, Monomial and quadratic bent functions over the finite fields of odd characteristic, IEEE Transactions on Information Theory 52 (5) (2006) 2018–2032.
- [15] X.-d. Hou, Solution to a problem of s. payne, Proceedings of the American Mathematical Society 132 (1) (2004) 1–6.
- [16] J. Y. Hyun, J. Lee, Y. Lee, Explicit criteria for construction of plateaued functions, IEEE Transactions on Information Theory 62 (12) (2016) 7555–7565.
- [17] C. Li, N. Li, T. Helleseth, C. Ding, The weight distributions of several classes of cyclic codes from apn monomials, IEEE transactions on information theory 60 (8) (2014) 4710–4721.

- [18] J. v. Lint, Introduction to coding theory, Springer, 1999.
- [19] S. Mesnager, Linear codes with few weights from weakly regular bent functions based on a generic construction, Cryptography and Communications 9 (1) (2017) 71–84.
- [20] S. Mesnager, F. Ozbudak, A. Sınak, A new class of three-weight linear codes from weakly regular plateaued functions, in: Proceedings of the Tenth International Workshop on Coding and Cryptography (WCC) 2017.
- [21] S. Mesnager, F. Ozbudak, A. Sınak, Results on characterizations of plateaued functions in arbitrary characteristic, in: International Conference on Cryptography and Information Security in the Balkans, Springer, 2015, pp. 17–30.
- [22] S. Mesnager, F. Özbudak, A. Sınak, Linear codes from weakly regular plateaued functions and their secret sharing schemes, Designs, Codes and Cryptography 87 (2-3) (2019) 463–480.
- [23] S. Mesnager, A. Sınak, Several classes of minimal linear codes with few weights from weakly regular plateaued functions, IEEE Transactions on Information Theory 66 (4) (2020) 2296–2310.
- [24] C. Tang, N. Li, Y. Qi, Z. Zhou, T. Helleseth, Linear codes with two or three weights from weakly regular bent functions, IEEE Transactions on Information Theory 62 (3) (2016) 1166–1176.
- [25] C. Tang, C. Xiang, K. Feng, Linear codes with few weights from inhomogeneous quadratic functions, Designs, Codes and Cryptography 83 (3) (2017) 691–714.
- [26] Y. Wu, N. Li, X. Zeng, Linear codes with few weights from cyclotomic classes and weakly regular bent functions, Designs, Codes and Cryptography (2020) 1–18.
- [27] X. Zeng, J. Shan, L. Hu, A triple-error-correcting cyclic code from the gold and kasami–welch app power functions, Finite Fields and Their Applications 18 (1) (2012) 70–92.
- [28] Y. Zheng, X.-M. Zhang, Plateaued functions, in: ICICS, Vol. 99, Springer, 1999, pp. 284–300.
- [29] Z. Zhou, N. Li, C. Fan, T. Helleseth, Linear codes with two or three weights from quadratic bent functions, Designs, Codes and Cryptography 81 (2) (2016) 283–295.

# Appendix

The Hamming weights and weight distributions of the codes constructed in Section 3 are presented in Tables 1-24.

Hamming weight $\omega$	Multiplicity $A_{\omega}$
0	1
$(p-1)p^{m-2}$	$p^m - p^{m-s} - 1$
$(p^m - \epsilon(p-1)\sqrt{p^*}^{m+s})(p-1)/p^2$	$p^{m-s-1} + \epsilon \eta_0^{m+1} (-1)(p-1)\sqrt{p^*}^{m-s-2}$
$(p^m + \epsilon \sqrt{p^*}^{m+s})(p-1)/p^2$	$(p-1)(p^{m-s-1}-\epsilon\eta_0^{m+1}(-1)\sqrt{p^*}^{m-s-2})$

Table 1: The weight distribution of  $C_{D_0}$  in Theorem 1 when m + s is even

Hamming weight $w$	Multiplicity $A_w$
0	1
$(p-1)(p^{m-2} - \epsilon \sqrt{p}^{m+s-3})$	$p^{m-s-1}$
$(p-1)p^{m-2} + \epsilon 2\sqrt{p}^{m+s-3}$	$(p^{m-s-1} + \epsilon \sqrt{p^{m-s-1}})(p-1)/2$
$(p-1)p^{m-2}$	$p^m - p^{m-s} - 1 + (p^{m-s-1} - \epsilon \sqrt{p}^{m-s-1})(p-1)/2$

Table 2: The weight distribution of  $\mathcal{C}_{D_1}$  when  $p \equiv 1 \pmod{4}$  and m + s is odd

Hamming weight $w$	Multiplicity $A_w$
0	1
$(p-1)(p^{m-2} + \epsilon \sqrt{p^*}^{m+s-3})$	$p^{m-s-1}$
$(p-1)p^{m-2}$	$p^{m} - p^{m-s} - 1 + (p^{m-s-1} + \epsilon(-1)^{m}\sqrt{p^{*}}^{m-s-1})(p-1)/2$
$(p-1)p^{m-2} - \epsilon 2\sqrt{p^*}^{m+s-3}$	$(p^{m-s-1} - \epsilon(-1)^m \sqrt{p^*}^{m-s-1})(p-1)/2$

Table 3: The weight distribution of  $\mathcal{C}_{D_1}$  when  $p \equiv 3 \pmod{4}$  and m + s is odd

Hamming weight $w$	Multiplicity $A_w$
0	1
$(p-1)p^{m-2}$	$p^m - p^{m-s} - 1$
$(p^m + \epsilon \sqrt{p^*}^{m+s})(p-1)/p^2$	$p^{m-s-1} + (p^{m-s-1} + \epsilon \eta_0^{m+1} (-1)\sqrt{p^*}^{m-s-2})(p-1)/2$
$((p-1)p^m - \epsilon(p+1)\sqrt{p^*}^{m+s})/p^2$	$(p^{m-s-1} - \epsilon \eta_0^{m+1}(-1)\sqrt{p^*}^{m-s-2})(p-1)/2$

Table 4: The weight distribution of  $C_{D_1}$  when m + s is even

Hamming weight $\omega$	Multiplicity $A_{\omega}$
0	1
$2(p-1)p^{m-2}$	$p^m - p^{m-s} - 1$
$(p-1)(2p^{m-2}-\epsilon\eta_0(-1)\sqrt{p^*}^{m+s-3})$	$p^{m-s-1}$
$2(p-1)p^{m-2} - \epsilon(p-2 - \eta_0(-1))\sqrt{p^*}^{m+s-3}$	$(p^{m-s-1} + \epsilon \eta_0^m (-1) \sqrt{p^*}^{m-s-1})(p-1)/2$
$2(p-1)p^{m-2} + \epsilon(p-2+\eta_0(-1))\sqrt{p^*}^{m+s-3}$	$(p^{m-s-1} - \epsilon \eta_0^m (-1) \sqrt{p^*}^{m-s-1})(p-1)/2$

Table 5: The weight distribution of  $\mathcal{C}_{D_{(0,1)}}$  when m + s is odd

Hamming weight $\omega$	Multiplicity $A_{\omega}$
0	1
$2(p-1)p^{m-2}$	$p^m - p^{m-s} - 1$
$(2p^m - \epsilon(p-2)\sqrt{p^{*}}^{m+s})(p-1)/p^2$	$p^{m-s-1} + \epsilon \eta_0^{m+1} (-1)(p-1)\sqrt{p^*}^{m-s-2}$
$2((p-1)p^m - \epsilon\sqrt{p^*}^{m+s})/p^2$	$(p^{m-s-1} - \epsilon \eta_0^{m+1}(-1)\sqrt{p^*}^{m-s-2})(p-1)/2$
$2(p^m + \epsilon \sqrt{p^*}^{m+s})(p-1)/p^2$	$(p^{m-s-1} - \epsilon \eta_0^{m+1} (-1) \sqrt{p^*}^{m-s-2})(p-1)/2$

Table 6: The weight distribution of  $\mathcal{C}_{D_{(0,1)}}$  when m + s is even

Hamming weight $w$	Multiplicity $A_w$
0	1
$(p-1)(p^{m-2} + \epsilon \sqrt{p}^{m+s-3})$	$p^{m-s-1}$
$(p-1)p^{m-2}$	$p^m - p^{m-s} - 1 + (p^{m-s-1} + \epsilon \sqrt{p}^{m-s-1})(p-1)/2$
$(p-1)p^{m-2} - \epsilon 2\sqrt{p}^{m+s-3}$	$(p^{m-s-1} - \epsilon \sqrt{p}^{m-s-1})(p-1)/2$

Table 7: The weight distribution of  $\mathcal{C}_{D_2}$  when  $p \equiv 1 \pmod{4}$  and m + s is odd

Hamming weight $w$	Multiplicity $A_w$
0	1
$(p-1)(p^{m-2} - \epsilon \sqrt{p^*}^{m+s-3})$	$p^{m-s-1}$
$(p-1)p^{m-2} + \epsilon 2\sqrt{p^*}^{m+s-3}$	$(p^{m-s-1} + \epsilon(-1)^m \sqrt{p^*}^{m-s-1})(p-1)/2$
$(p-1)p^{m-2}$	$p^{m} - p^{m-s} - 1 + (p^{m-s-1} - \epsilon(-1)^{m} \sqrt{p^{*}}^{m-s-1})(p-1)/2$

Table 8: The weight distribution of  $\mathcal{C}_{D_2}$  when  $p \equiv 3 \pmod{4}$  and m + s is odd

Hamming weight $\omega$	Multiplicity $A_{\omega}$
0	1
$2(p-1)p^{m-2}$	$p^m - p^{m-s} - 1$
$(p-1)(2p^{m-2}+\epsilon\eta_0(-1)\sqrt{p^*}^{m+s-3})$	$p^{m-s-1}$
$2(p-1)p^{m-2} - \epsilon(p-2+\eta_0(-1))\sqrt{p^*}^{m+s-3}$	$(p^{m-s-1} + \epsilon \eta_0^m (-1) \sqrt{p^*}^{m-s-1})(p-1)/2$
$2(p-1)p^{m-2} + \epsilon(p-2 - \eta_0(-1))\sqrt{p^{*^{m+s-3}}}$	$(p^{m-s-1} - \epsilon \eta_0^m (-1) \sqrt{p^*}^{m-s-1})(p-1)/2$

Table 9: The weight distribution of  $\mathcal{C}_{D_{(0,2)}}$  when m+s is odd

Hamming weight $\omega$	Multiplicity $A_{\omega}$
0	1
$2(p-1)p^{m-2}$	$p^{m-s-1} + p^m - p^{m-s} - 1$
$2(p-1)p^{m-2} + \epsilon 2\sqrt{p^*}^{m+s-3}$	$(p^{m-s-1} + \epsilon \eta_0^m (-1) \sqrt{p^*}^{m-s-1})(p-1)/2$
$2(p-1)p^{m-2} - \epsilon 2\sqrt{p^*}^{m+s-3}$	$(p^{m-s-1} - \epsilon \eta_0^m (-1) \sqrt{p^{*m-s-1}})(p-1)/2$

Table 10: The weight distribution of  $\mathcal{C}_{D_{(1,2)}}$  when m + s is odd

Hamming weight $\omega$	Multiplicity $A_{\omega}$
0	1
$2(p-1)p^{m-2}$	$p^m - p^{m-s} - 1$
$2(p-1)(p^m + \epsilon \sqrt{p^*}^{m+s})/p^2$	$p^{m-s-1} + \epsilon \eta_0^{m+1} (-1)(p-1) \sqrt{p^*}^{m-s-2}$
$2((p-1)p^m - \epsilon \sqrt{p^*}^{m+s})/p^2$	$(p-1)(p^{m-s-1} - \epsilon \eta_0^{m+1}(-1)\sqrt{p^*}^{m-s-2})$

Table 11: The weight distribution of  $\mathcal{C}_{D_{(1,2)}}$  when m+s is even

Hamming weight $\omega$	Multiplicity $A_{\omega}$
0	1
$(p^{m-2} - \epsilon \sqrt{p^{m+s-3}})(p-1)^2/2$	$p^{m-s-1}$
$(p-1)(p^{m-2}(p-1)/2 + \epsilon\sqrt{p}^{m+s-3})$	$(p^{m-s-1} + \epsilon \sqrt{p^{m-s-1}})(p-1)/2$
$p^{m-2}(p-1)^2/2$	$p^{m} - p^{m-s} - 1 + (p^{m-s-1} - \epsilon \sqrt{p^{m-s-1}})(p-1)/2$

Table 12: The weight distribution of  $\mathcal{C}_{D_{sq}}$  when  $p \equiv 1 \pmod{4}$  and m + s is odd

Hamming weight $\omega$	Multiplicity $A_{\omega}$
0	1
$(p^{m-2} + \epsilon \sqrt{p^*}^{m+s-3})(p-1)^2/2$	$p^{m-s-1}$
$p^{m-2}(p-1)^2/2$	$p^{m} - p^{m-s} - 1 + (p^{m-s-1} + \epsilon(-1)^{m}\sqrt{p^{*m-s-1}})(p-1)/2$
$(p-1)(p^{m-2}(p-1)/2 - \epsilon \sqrt{p^*}^{m+s-3})$	$(p^{m-s-1} - \epsilon(-1)^m \sqrt{p^*}^{m-s-1})(p-1)/2$

Table 13: The weight distribution of  $\mathcal{C}_{D_{sq}}$  when  $p \equiv 3 \pmod{4}$  and m + s is odd

Hamming weight $\omega$	Multiplicity $A_{\omega}$
0	1
$p^m(p-1)^2/2p^2$	$p^m - p^{m-s} - 1$
$(p^m + \epsilon \sqrt{p^*}^{m+s})(p-1)^2/2p^2$	$p^{m-s-1} + (p^{m-s-1} + \epsilon \eta_0^{m+1} (-1) \sqrt{p^*}^{m-s-2})(p-1)/2$
$((p-1)p^m - \epsilon(p+1)\sqrt{p^*}^{m+s})(p-1)/2p^2$	$(p^{m-s-1} - \epsilon \eta_0^{m+1} (-1) \sqrt{p^*}^{m-s-2})(p-1)/2$

Table 14: The weight distribution of  $C_{D_{sq}}$  when m + s is even

Hamming weight $w$	Multiplicity $A_w$
0	1
$p^{m-2}(p^2-1)/2 - \epsilon \sqrt{p}^{m+s-3}(p-1)^2/2$	$p^{m-s-1}$
$p^{m-2}(p^2-1)/2$	$p^m - p^{m-s} - 1 + (p^{m-s-1} + \epsilon \sqrt{p^{m-s-1}})(p-1)/2$
$p^{m-2}(p^2-1)/2 + \epsilon(p-1)\sqrt{p}^{m+s-3}$	$(p^{m-s-1} - \epsilon \sqrt{p}^{m-s-1})(p-1)/2$

Table 15: The weight distribution of  $\mathcal{C}_{D_{(sq,0)}}$  when  $p \equiv 1 \pmod{4}$  and m + s is odd

Hamming weight $w$	Multiplicity $A_w$
0	1
$p^{m-2}(p^2-1)/2 + \epsilon \sqrt{p^*}^{m+s-3}(p-1)^2/2$	$p^{m-s-1}$
$p^{m-2}(p^2-1)/2 - \epsilon(p-1)\sqrt{p^*}^{m+s-3}$	$(p^{m-s-1} + \epsilon(-1)^m \sqrt{p^*}^{m-s-1})(p-1)/2$
$p^{m-2}(p^2-1)/2$	$p^{m} - p^{m-s} - 1 + (p^{m-s-1} - \epsilon(-1)^{m}\sqrt{p^{*}}^{m-s-1})(p-1)/2$

Table 16: The weight distribution of  $\mathcal{C}_{D_{(sq,0)}}$  when  $p \equiv 3 \pmod{4}$  and m + s is odd

Hamming weight $w$	Multiplicity $A_w$
0	1
$p^m(p^2-1)/2p^2$	$p^m - p^{m-s} - 1$
$((p+1)p^m - \epsilon(p-1)\sqrt{p^*}^{m+s})(p-1)/2p^2$	$p^{m-s-1} + \frac{1}{2}(p-1)(p^{m-s-1} + \epsilon \eta_0^{m+1}(-1)\sqrt{p^*}^{m-s-2})$
$(p^m + \epsilon \sqrt{p^*}^{m+s})(p^2 - 1)/2p^2$	$\frac{1}{2}(p-1)(p^{m-s-1}-\epsilon\eta_0^{m+1}(-1)\sqrt{p^{*}}^{m-s-2})$

Table 17: The weight distribution of  $\mathcal{C}_{D_{(sq,0)}}$  when m + s is even

Hamming weight $\omega$	Multiplicity $A_{\omega}$
0	1
$(p^{m-2} + \epsilon \sqrt{p^{m+s-3}})(p-1)^2/2$	$p^{m-s-1}$
$p^{m-2}(p-1)^2/2$	$p^m - p^{m-s} - 1 + (p^{m-s-1} + \epsilon \sqrt{p}^{m-s-1})(p-1)/2$
$(p-1)(p^{m-2}(p-1)/2 - \epsilon\sqrt{p}^{m+s-3})$	$(p^{m-s-1} - \epsilon \sqrt{p}^{m-s-1})(p-1)/2$

Table 18: The weight distribution of  $C_{D_{nsq}}$  when  $p \equiv 1 \pmod{4}$  and m + s is odd

Hamming weight $\omega$	Multiplicity $A_{\omega}$
0	1
$(p^{m-2} - \epsilon \sqrt{p^*}^{m+s-3})(p-1)^2/2$	$p^{m-s-1}$
$(p-1)(p^{m-2}(p-1)/2 + \epsilon \sqrt{p^*}^{m+s-3})$	$(p^{m-s-1} + \epsilon(-1)^m \sqrt{p^*}^{m-s-1})(p-1)/2$
$p^{m-2}(p-1)^2/2$	$p^{m} - p^{m-s} - 1 + (p^{m-s-1} - \epsilon(-1)^{m} \sqrt{p^{*}}^{m-s-1})(p-1)/2$

Table 19: The weight distribution of  $\mathcal{C}_{D_{nsq}}$  when  $p \equiv 3 \pmod{4}$  and m + s is odd

Hamming weight $w$	Multiplicity $A_w$
0	1
$p^{m-2}(p^2-1)/2 + \epsilon \sqrt{p}^{m+s-3}(p-1)^2/2$	$p^{m-s-1}$
$p^{m-2}(p^2-1)/2 - \epsilon(p-1)\sqrt{p}^{m+s-3}$	$(p^{m-s-1} + \epsilon \sqrt{p^{m-s-1}})(p-1)/2$
$p^{m-2}(p^2-1)/2$	$p^{m} - p^{m-s} - 1 + (p^{m-s-1} - \epsilon \sqrt{p^{m-s-1}})(p-1)/2$

Table 20: The weight distribution of  $\mathcal{C}_{D_{(nsq,0)}}$  when  $p \equiv 1 \pmod{4}$  and m + s is odd

Hamming weight $w$	Multiplicity $A_w$
0	1
$p^{m-2}(p^2-1)/2 - \epsilon \sqrt{p^*}^{m+s-3}(p-1)^2/2$	$p^{m-s-1}$
$p^{m-2}(p^2-1)/2$	$p^{m} - p^{m-s} - 1 + (p^{m-s-1} + \epsilon(-1)^{m}\sqrt{p^{*}}^{m-s-1})(p-1)/2$
$p^{m-2}(p^2-1)/2 + \epsilon(p-1)\sqrt{p^*}^{m+s-3}$	$(p^{m-s-1} - \epsilon(-1)^m \sqrt{p^*}^{m-s-1})(p-1)/2$

Table 21: The weight distribution of  $\mathcal{C}_{D_{(nsq,0)}}$  when  $p \equiv 3 \pmod{4}$  and m + s is odd

Hamming weight $\omega$	Multiplicity $A_{\omega}$
0	1
$p^{m-2}$	$p^m - p^{m-s} - 1$
$p^{m-2} - \epsilon(p-1)\sqrt{p^*}^{m+s-4}$	$p^{m-s-1} + \epsilon \eta_0^{m+1} (-1)(p-1) \sqrt{p^*}^{m-s-2}$
$p^{m-2} + \epsilon \sqrt{p^*}^{m+s-4}$	$(p-1)(p^{m-s-1}-\epsilon\eta_0^{m+1}(-1)\sqrt{p^*}^{m-s-2})$

Table 2	22: The weight distri	bution of $\mathcal{C}_{\overline{D}_0}$ when $m + s$	is even
	Hamming weight $\omega$	Multiplicity $A_{\omega}$	
	0	1	
	$2 \cdot 3^{m-2}$	$3^{m-s-1} + 3^m - 3^{m-s} - 1$	
	$2 \cdot 3^{m-2} + \epsilon \sqrt{-3}^{m+s-3}$	$3^{m-s-1} + \epsilon(-1)^m \sqrt{-3}^{m-s-1}$	
	$2 \cdot 3^{m-2} - \epsilon \sqrt{-3}^{m+s-3}$	$3^{m-s-1} - \epsilon(-1)^m \sqrt{-3}^{m-s-1}$	

Table 23: The weight distribution of  $\mathcal{C}_{\overline{D}_{(1,2)}}$  when p = 3 and m + s is odd

	(1,2)
Hamming weight $\omega$	Multiplicity $A_{\omega}$
0	1
$2 \cdot 3^{m-2}$	$3^m - 3^{m-s} - 1$
$2(3^{m-2} + \epsilon \sqrt{-3}^{m+s-4})$	$3^{m-s-1} + \epsilon(-1)^{m+1} 2\sqrt{-3}^{m-s-2}$
$2 \cdot 3^{m-2} - \epsilon \sqrt{-3}^{m+s-4}$	$2(3^{m-s-1} - \epsilon(-1)^{m+1}\sqrt{-3}^{m-s-2})$

Table 24: The weight distribution of  $\mathcal{C}_{\overline{D}_{(1,2)}}$  when p = 3 and m + s is even