Minimal linear codes with six-weights based on weakly regular plateaued balanced functions

Ahmet Sınak

Department of Mathematics and Computer Science, Necmettin Erbakan University, 42090 Konya, Turkey and LAGA, UMR 7539, CNRS, 93430 Villetaneuse, Paris, France
Corresponding Author: sinakahmet@gmail.com.tr

Research Paper Received: 20.08.2021 Revised: 26.09.2021 Accepted: 30.09.2021

Abstract—Constructing minimal linear codes has a great interest in coding theory since they have an important role in describing access structures in secret sharing schemes and they are employed to design secure two-party computation protocols. Many methods of constructing linear codes have been proposed in the literature, and the most famous one is based on functions over finite fields. Linear codes derived from cryptographic functions have desirable algebraic structures that are significant from the application point of view. We in this paper study the construction of these codes from special functions over the odd characteristic finite fields. We aim to construct new minimal codes by using a new type of function in the known construction method. To do this, we propose to use five different subsets of the preimages of weakly regular plateaued balanced functions. We then obtain five infinite classes of minimal linear codes with six-weights based on these functions over the odd characteristic finite fields.

Keywords—Balanced function, minimal code, weakly regular plateaued function, weight distribution

1. Introduction

Let n be a positive integer and p be an odd prime. The finite field with p^n elements is denoted by $\mathbb{F}_{p^n}$, and it can be viewed as an n-dimensional vector space $\mathbb{F}_p^n$ over $\mathbb{F}_p$. Then, a k-dimensional subspace of a vector space $\mathbb{F}_p^n$ is called linear code $\mathcal{C}$ with length n and dimension k over $\mathbb{F}_p$. The Hamming weight $wt(\mathbf{b})$ of a vector $\mathbf{b} = (b_0, \ldots, b_{n-1}) \in \mathbb{F}_p^n$ is the size of the set $\{0 \leq i \leq n-1 : b_i \neq 0\}$. The minimum nonzero Hamming weight in $\mathcal{C}$ is the minimum Hamming distance d of $\mathcal{C}$. Then, the code $\mathcal{C}$ is represented by $[n, k, d]_p$ over $\mathbb{F}_p$. The code $\mathcal{C}$ is said to be minimal if all nonzero codewords in $\mathcal{C}$ are minimal. Let A_w be the number of codewords $\mathbf{b}$ with the weight $wt(\mathbf{b}) = w$ in $\mathcal{C}$. The weight distribution of the code $\mathcal{C}$ is shown by $(1, A_1, \ldots, A_n)$, and its weight enumerator is represented by the polynomial $1 + A_1 y + \cdots + A_n y^n$. If the number of nonzero coefficients A_w in the polynomial equals t, then the code $\mathcal{C}$ is t-weight.

Linear codes have many applications in cryptography, design theory, graph theory, authentication codes, communication, data storage systems, and consumer electronics. Few-weight linear codes have many construction methods, one of them is based on functions over finite fields. Until now, a great number of few-weight linear codes have been obtained from functions such as bent functions ([16], [25]), plateaued functions ([17], [19], [20], [21], [24]), perfect nonlinear functions [3] and quadratic functions ([5], [6], [9]). The recent construction methods of linear codes from functions have been presented in [12]. Furthermore, Mesnager has published in [11] a recent survey on linear codes constructed from functions over finite fields.

An important subclass of linear codes is the minimal codes that have many practical applications such as secure two-party computation and sharing schemes. These codes have an important role in designing access structures in sharing schemes [8], [14], and they are employed to design new protocols for two-party computation. The following lemma proposes a sufficient condition for a linear code over finite fields to be minimal.

Lemma 1 [1] Let $\mathcal{C}$ be the linear code over $\mathbb{F}_p$. Let $w_{\max}$ and $w_{\min}$ denote the maximum and minimum weights of the nonzero codewords in $\mathcal{C}$. Then, the code $\mathcal{C}$ is minimal if

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

We remark that the sufficient condition (1) is not necessary for linear codes to be minimal. Recently, a new necessary-sufficient condition to be minimal has been introduced for a binary linear code by Chang et al. [4] and Ding et al. [7], independently. They have proposed binary minimal linear codes flouting (1) from Boolean functions. Immediately after, Heng et al. [10] have introduced a new necessary-sufficient condition for minimal linear codes over the odd characteristic finite fields, and they proposed minimal ternary codes flouting (1). Very recently, many minimal codes flouting (1) have been obtained in [2], [18], [19], [22], [26], [27], [28]. For instance, Mesnager et al. [18] have used characteristic functions to characterize minimal linear codes, and then Qi et al. [22] have generalized the recent results proposed in [18] over the odd characteristic finite fields. Very recently, Mesnager and Sınak [19] have proposed three different classes of minimal codes with six-weights based on weakly regular plateaued unbalanced functions. In this paper, inspired by the recent works [19], [27], [28], we aim to obtain new minimal linear codes based on weakly regular plateaued balanced functions from the construction method given in [28, Theorem 10].

The paper is scheduled as follows. We set a necessary background of the paper in Section 2. Section 3 presents some new results on the exponential sums of weakly regular plateaued balanced functions. Section 4 derives new classes of linear codes with six-weights from the subsets of the preimages of weakly regular plateaued balanced functions over $\mathbb{F}_p$.

2. Preliminaries

For any set K, $K^\star = K\setminus\{0\}$ and $\#K$ shows the size of K. The set of all non-square elements and square elements in $\mathbb{F}_p^\star$ is, respectively, denoted by NSQ and SQ. For simplicity, we use $p^* = \eta_0(-1)p$, where η_0 is the quadratic character of $\mathbb{F}_p^\star$. Let $\mathbb{Q}(\xi_p)$ be a cyclotomic field, where $\mathbb{Q}$ is the rational field and ξ_p is a primitive p-th root of unity. For $a \in \mathbb{F}_p^\star$, the automorphism σ_a of the cyclotomic field $\mathbb{Q}(\xi_p)$ is defined as $\sigma_a(\xi_p) = \xi_p^a$. For $b \in \mathbb{F}_p$, one can easily see that $\sigma_a(\xi_p^b) = \xi_p^{ab}$ and $\sigma_a(\sqrt{p^*}^{\,n}) = {\eta_0}^n(a)\sqrt{p^*}^{\,n}$.

Lemma 2 [13] Under the above notations,

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

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

Let $f:\mathbb{F}_q\to\mathbb{F}_p$ be a p-ary function, where $q=p^n$. f is called balanced function if it takes every element in $\mathbb{F}_p$ with p^{n-1} times; or else, it is called unbalanced function. A trace function $\mathrm{Tr}^n()$ is described as $\mathrm{Tr}^n(\alpha)=\alpha+\alpha^p+\alpha^{p^2}+\cdots+\alpha^{p^{n-1}}$ over $\mathbb{F}_p$ for $\alpha\in\mathbb{F}_{p^n}$. The Walsh transform $\widehat{f}$ of a function f is given as

$$\widehat{f}(\delta)=\sum_{x\in\mathbb{F}_{p^n}} \xi_p^{\,f(x)-\mathrm{Tr}^n(\delta x)},\ \delta\in\mathbb{F}_{p^n}.$$

Plateaued and bent functions were, respectively, introduced by Zheng and Zhang [29] and by Rothaus [23]. A function $f:\mathbb{F}_{p^n}\to\mathbb{F}_p$ is said to be s-plateaued if $|\widehat{f}(\delta)|^2\in\{0,p^{n+s}\}$, where s is an integer with $0\le s\le n$. It is obvious that a 0-plateaued function is the bent function. For a plateaued function f, the Walsh support of f is $\mathcal{S}_f=\{\delta\in\mathbb{F}_{p^n}: |\widehat{f}(\delta)|^2=p^{n+s}\}$. A plateaued function f is said to be weakly regular s-plateaued if

$$\widehat{f}(\delta)\in\left\{0, vp^{\frac{n+s}{2}}\xi_p^{f^\star(\delta)}\right\},\ \forall\delta\in\mathbb{F}_{p^n},$$

where $v\in\{\pm i,\pm1\}$ is a constant sign and $f^\star$ is a p-ary function over $\mathbb{F}_{p^n}$ with $f^\star(\delta)=0$ for all $\delta\in\mathbb{F}_{p^n}\setminus\mathcal{S}_f$. If the sign v changes depending on the value of δ, then we say that f is non-weakly regular plateaued function. For $1\le s\le n$, we have denoted by WRPB in [24] the set of weakly regular s-plateaued balanced functions f that hold the following conditions

- $f(0)=0$, and
- $f(bx)=b^if(x)$ for every $x\in\mathbb{F}_{p^n}$ and $b\in\mathbb{F}_p^\star$, where i is a positive even integer with $\gcd(i-1,p-1)=1$.

Lemma 3 [15] Let $f:\mathbb{F}_{p^n}\to\mathbb{F}_p$ be an s-plateaued function. For $\delta\in\mathbb{F}_q$, $|\widehat{f}(\delta)|^2$ has the value 0 and the value p^{n+s}, respectively, p^n-p^{n-s} times and p^{n-s} times.

Lemma 4 [17] Let $f:\mathbb{F}_{p^n}\to\mathbb{F}_p$. If f is weakly regular s-plateaued, then for every $\delta\in\mathcal{S}_f$,

$$\widehat{f}(\delta)=\epsilon\sqrt{p^*}^{\,n+s}\xi_p^{f^\star(\delta)},$$

where $\epsilon\in\{\pm1\}$ is the constant sign of $\widehat{f}$.

Lemma 5 [20] Let $f:\mathbb{F}_{p^n}\to\mathbb{F}_p$ be a weakly regular s-plateaued function. For $j\in\mathbb{F}_p$, we define $\mathcal{N}_{f^\star j}=\#\{\delta\in\mathcal{S}_f: f^\star(\delta)=j\}$. When $n-s$ is even,

$$\mathcal{N}_{f^\star j}=\begin{cases} p^k+\epsilon\eta_0^{n+1}(-1)\sqrt{p^*}^{\,k-1}(p-1), & \text{if } j=0 \\ p^k-\epsilon\eta_0^{n+1}(-1)\sqrt{p^*}^{\,k-1}, & \text{if } j\neq0 \end{cases}$$

otherwise,

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

where $k=n-s-1$.

3. Exponential sums of plateaued balanced functions

In this section, we provide new results on exponential sums of balanced plateaued functions.

Lemma 6 Let $f\in$ WRPB. For $i\in\mathbb{F}_p^\star$ and $\delta\in\mathbb{F}_q^\star$, we define

$$L(\delta,i)=\sum_{z,y\in\mathbb{F}_p^\star}\sum_{x\in\mathbb{F}_q}\xi_p^{yf(x)-z\mathrm{Tr}^n(\delta x)+zi}.$$

For all $\delta\in\mathbb{F}_q^\star\setminus\mathcal{S}_f$ we have $L(\delta,i)=0$, and for all $\delta\in\mathcal{S}_f$

$$L(\delta,i)=\begin{cases} -\epsilon\sqrt{p^*}^{\,n+s}(p-1), & \text{if } f^\star(\delta)=0, \\ \epsilon\sqrt{p^*}^{\,n+s}, & \text{if } f^\star(\delta)\neq0 \end{cases}$$

when $n+s$ is even; otherwise,

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

Proof: The proof proceeds from the techniques applied in the proof of [25, Lemma 10]. We provide its main parts. For $i\in\mathbb{F}_p^\star$ and $\delta\in\mathbb{F}_q^\star$, we can find that

$$L(\delta,i) = \sum_{y,z\in\mathbb{F}_p^\star}\sigma_y(\widehat{f}(z\delta))\sigma_y(\xi_p^{zi}).$$

When $\delta\in\mathbb{F}_q^\star\setminus\mathcal{S}_f$, we clearly have $L(\delta,i)=0$. When $\delta\in\mathcal{S}_f$, we have

$$\begin{aligned}L(\delta,i) &= \sum_{y,z\in\mathbb{F}_p^\star}\sigma_y(\epsilon\sqrt{p^*}^{n+s}\xi_p^{f^\star(z\delta)+zi})\\ &= \sum_{y,z\in\mathbb{F}_p^\star}\sigma_y(\epsilon\sqrt{p^*}^{n+s}\xi_p^{z^l f^\star(\delta)+zi})\\ &= \epsilon\sqrt{p^*}^{n+s}\sum_{y\in\mathbb{F}_p^\star}\eta_0^{n+s}(y)\sum_{z\in\mathbb{F}_p^\star}\sigma_y(\xi_p^{z^l f^\star(\delta)+zi})\\ &= -\epsilon\sqrt{p^*}^{n+s}\sum_{y\in\mathbb{F}_p^\star}\eta_0^{n+s}(y)\xi_p^{yf^\star(\delta)}.\end{aligned}$$

Hence, the proof is complete from Lemma 2. □

Lemma 7 Let $f\in$ WRPB. For $i\in\mathbb{F}_p^\star$ and $\delta\in\mathbb{F}_q^\star$, we define

$$\mathcal{N}_f(\delta,i)=\#\{x\in\mathbb{F}_q:\mathrm{Tr}^n(\delta x)=i \text{ and } f(x)=0\}.$$

Then, for all $\delta\in\mathbb{F}_q^\star\setminus\mathcal{S}_f$, we have $\mathcal{N}_f(\delta,i)=p^{n-2}$, and for all $\delta\in\mathcal{S}_f$,

$$\mathcal{N}_f(\delta,i) = \begin{cases}p^{n-2}-M(p-1), & \text{if } f^\star(\delta)=0,\\ p^{n-2}+M, & \text{if } f^\star(\delta)\neq 0,\end{cases}$$

when $n+s$ is even; otherwise,

$$\mathcal{N}_f(\delta,i) = \begin{cases}p^{n-2}, & \text{if } f^\star(\delta)=0,\\ p^{n-2}-N, & \text{if } f^\star(\delta)\in SQ,\\ p^{n-2}+N, & \text{if } f^\star(\delta)\in NSQ,\end{cases}$$

where $M=\epsilon\sqrt{p^*}^{n+s-4}$ and $N=\epsilon\sqrt{p^*}^{n+s-3}$.

Proof: According to the definition of $\mathcal{N}_f(\delta,i)$, as seen in the proof of [25, Lemma 11], one can derive from the exponential sum that

$$\mathcal{N}_f(\delta,i) = p^{n-2}+p^{-2}\sum_{y,z\in\mathbb{F}_p^\star}\sum_{x\in\mathbb{F}_q}\xi_p^{yf(x)-z(\mathrm{Tr}^n(\delta x)-i)}.$$

Hence, the results follow directly from Lemma 6. □

Lemma 8 Let $f\in$ WRPB. For $i\in\mathbb{F}_p^\star$ and $\delta\in\mathbb{F}_q^\star$, we define

$$S(\delta,i)=\sum_{z,y\in\mathbb{F}_p^\star}\sum_{x\in\mathbb{F}_q}\xi_p^{y^2f(x)-z(\mathrm{Tr}^n(\delta x)-i)}.$$

Then, for every $\delta\in\mathbb{F}_q^\star\setminus\mathcal{S}_f$ we have $S(\delta,i)=0$, and for every $\delta\in\mathcal{S}_f$

$$S(\delta,i)=\begin{cases}\epsilon(1-p)\sqrt{p^*}^{n+s}, & \text{if } f^\star(\delta)=0,\\ \epsilon(1-\sqrt{p^*})\sqrt{p^*}^{n+s}, & \text{if } f^\star(\delta)\in SQ,\\ \epsilon(1+\sqrt{p^*})\sqrt{p^*}^{n+s}, & \text{if } f^\star(\delta)\in NSQ.\end{cases}$$

Proof: The proof is the same as the proof of Lemma 6. Then, it completes from Lemma 2. □

Lemma 9 Let $f\in$ WRPB. For $i\in\mathbb{F}_p^\star$ and $\delta\in\mathbb{F}_q^\star$, we define the following sets

$$\begin{aligned}\mathcal{N}_{sq}(\delta,i) &= \#\{x\in\mathbb{F}_q:\mathrm{Tr}^n(\delta x)=i \text{ and } f(x)\in SQ\},\\ \mathcal{N}_{nsq}(\delta,i) &= \#\{x\in\mathbb{F}_q:\mathrm{Tr}^n(\delta x)=i \text{ and } f(x)\in NSQ\}.\end{aligned}$$

For every $\delta\in\mathbb{F}_q^\star\setminus\mathcal{S}_f$, we have

$$\mathcal{N}_{sq}(\delta,i)=\mathcal{N}_{nsq}(\delta,i)=(\frac{p-1}{2})p^{n-2}.$$

For every $\delta\in\mathcal{S}_f$,

$$\mathcal{N}_{sq}(\delta,i) = \begin{cases}A, & \text{if } f^\star(\delta)\in NSQ\cup\{0\},\\ B, & \text{if } f^\star(\delta)\in SQ,\end{cases}$$

$$\mathcal{N}_{nsq}(\delta,i) = \begin{cases}A, & \text{if } f^\star(\delta)\in SQ\cup\{0\},\\ B, & \text{if } f^\star(\delta)\in NSQ,\end{cases}$$

when $n+s$ is even; otherwise,

$$\mathcal{N}_{sq}(\delta,i) = \begin{cases} C, & \text{if } f^\star(\delta)=0,\\ D, & \text{if } f^\star(\delta)\in SQ,\\ E, & \text{if } f^\star(\delta)\in NSQ,\end{cases}$$

$$\mathcal{N}_{nsq}(\delta,i) = \begin{cases} F, & \text{if } f^\star(\delta)=0,\\ G, & \text{if } f^\star(\delta)\in SQ,\\ H, & \text{if } f^\star(\delta)\in NSQ,\end{cases}$$

where

$A = (\frac{p-1}{2})(p^{n-2} + \epsilon\sqrt{p^*}^{n+s-4})$,
$B = \frac{p-1}{2}p^{n-2} - \epsilon(\frac{p+1}{2})\sqrt{p^*}^{n+s-4}$,
$C = (\frac{p-1}{2})(p^{n-2} - \epsilon\frac{1}{p}\sqrt{p^*}^{n+s-1})$,
$D = (\frac{p-1}{2})p^{n-2} + \epsilon(\frac{\eta_0(-1)+1}{2})\sqrt{p^*}^{n+s-3}$,
$E = (\frac{p-1}{2})p^{n-2} + \epsilon(\frac{\eta_0(-1)-1}{2})\sqrt{p^*}^{n+s-3}$,
$F = (\frac{p-1}{2})(p^{n-2} + \epsilon\frac{1}{p}\sqrt{p^*}^{n+s-1})$,
$G = (\frac{p-1}{2})p^{n-2} - \epsilon(\frac{\eta_0(-1)-1}{2})\sqrt{p^*}^{n+s-3}$,
$H = (\frac{p-1}{2})p^{n-2} - \epsilon(\frac{\eta_0(-1)+1}{2})\sqrt{p^*}^{n+s-3}$.

Proof: For $i \in \mathbb{F}_p^\star$ and $\delta \in \mathbb{F}_q^\star$, we define

$$T(\delta,i) = \sum_{x\in\mathbb{F}_q}(\sum_{y\in\mathbb{F}_p}\xi_p^{y^2 f(x)})(\sum_{z\in\mathbb{F}_p}\xi_p^{-z(\mathrm{Tr}^n(\delta x)-i)}).$$

From Lemma 2, we have

$$\sum_{z\in\mathbb{F}_p}\xi_p^{-z(\mathrm{Tr}^n(\delta x)-i)} = \begin{cases} p, & \text{if } \mathrm{Tr}^n(\delta x)=i,\\ 0, & \text{if } \mathrm{Tr}^n(\delta x)\neq i,\end{cases}$$

and

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

They imply that

$$T(\delta,i) = p^2\mathcal{N}_f(\delta,i) + p\sqrt{p^*}(\mathcal{N}_{sq}(\delta,i) - \mathcal{N}_{nsq}(\delta,i)),$$

where $\mathcal{N}_f(\delta,i)$ is given in Lemma 7. We have also the fact that

$$\mathcal{N}_f(\delta,i) + \mathcal{N}_{sq}(\delta,i) + \mathcal{N}_{nsq}(\delta,i) = p^{n-1}.$$

On the other part, expanding the expression of $T(\delta,i)$, as seen in the proof of [25, Lemma 14], one can verify that

$$T(\delta,i) = p^n + \sum_{y,z\in\mathbb{F}_p^\star}\sum_{x\in\mathbb{F}_q}\xi_p^{y^2 f(x) - z(\mathrm{Tr}^n(\delta x)-i)},$$

and by Lemma 8 we have

$$T(\delta,i) = \begin{cases} p^n, & \text{if } \delta\in\mathbb{F}_q^\star\setminus\mathcal{S}_f,\\ p^n - M(p-1), & \text{if } f^\star(\delta)=0,\\ p^n - M(\sqrt{p^*}-1), & \text{if } f^\star(\delta)\in SQ,\\ p^n + M(\sqrt{p^*}+1), & \text{if } f^\star(\delta)\in NSQ,\end{cases}$$

where $M = \epsilon\sqrt{p^*}^{n+s}$. Hence, the desired results can be obtained from the above results, thereby completing the proof. □

The character sum of a subset S of $\mathbb{F}_q$ in respect of $\delta \in \mathbb{F}_q^\star$ is given as

$$\chi_\delta(S) = \sum_{x\in S}\xi_p^{\mathrm{Tr}^n(\delta x)}. \tag{2}$$

We define the following subsets of $\mathbb{F}_{p^n}$ to construct linear codes based on these subsets.

$$\begin{aligned} D_0 &= \{x\in\mathbb{F}_{p^n} : f(x)=0\},\\ D_{sq} &= \{x\in\mathbb{F}_{p^n} : f(x)\in SQ\},\\ D_{nsq} &= \{x\in\mathbb{F}_{p^n} : f(x)\in NSQ\},\\ D_{sq,0} &= \{x\in\mathbb{F}_{p^n} : f(x)\in SQ\cup\{0\}\},\\ D_{nsq,0} &= \{x\in\mathbb{F}_{p^n} : f(x)\in NSQ\cup\{0\}\}.\end{aligned} \tag{3}$$

We now compute the character sums of these sets.

Lemma 10 Let $f \in$ WRPB and $\delta \in \mathbb{F}_q^\star$. Then the character sums of the sets of the form of (3) are given as follows. For every $\delta \in \mathbb{F}_q^\star \setminus \mathcal{S}_f$ we get $\chi_\delta(D_0) = \chi_\delta(D_{sq}) = \chi_\delta(D_{sq,0}) = \chi_\delta(D_{nsq}) = \chi_\delta(D_{nsq,0}) = 0$. For every $\delta \in \mathcal{S}_f$

$$\chi_\delta(D_0) = \begin{cases} 2A, & \text{if } f^\star(\delta)=0,\\ -2A/(p-1), & \text{if } f^\star(\delta)\neq 0,\end{cases}$$

$$\chi_\delta(D_{sq}) = \begin{cases} -A, & \text{if } f^\star(\delta)\in NSQ\cup\{0\},\\ B, & \text{if } f^\star(\delta)\in SQ,\end{cases}$$

$$\chi_\delta(D_{sq,0}) = \begin{cases} A, & \text{if } f^\star(\delta)\in SQ\cup\{0\},\\ -B, & \text{if } f^\star(\delta)\in NSQ,\end{cases}$$

$$\chi_\delta(D_{nsq}) = \begin{cases} -A, & \text{if } f^\star(\delta)\in SQ\cup\{0\},\\ B, & \text{if } f^\star(\delta)\in NSQ,\end{cases}$$

$$\chi_\delta(D_{nsq,0}) = \begin{cases} A, & \text{if } f^\star(\delta)\in NSQ\cup\{0\},\\ -B, & \text{if } f^\star(\delta)\in SQ,\end{cases}$$

when $n+s$ is even; otherwise,

$$\chi_\delta(D_0) = \begin{cases} 0, & \text{if } f^\star(\delta)=0, \\ \frac{\eta_0(-1)2C}{(p-1)}, & \text{if } f^\star(\delta)\in SQ, \\ -\frac{\eta_0(-1)2C}{(p-1)}, & \text{if } f^\star(\delta)\in NSQ, \end{cases}$$

$$\chi_\delta(D_{sq}) = \begin{cases} C, & \text{if } f^\star(\delta)=0, \\ -D, & \text{if } f^\star(\delta)\in SQ, \\ -E, & \text{if } f^\star(\delta)\in NSQ, \end{cases}$$

$$\chi_\delta(D_{sq,0}) = \begin{cases} C, & \text{if } f^\star(\delta)=0, \\ -E, & \text{if } f^\star(\delta)\in SQ, \\ -D, & \text{if } f^\star(\delta)\in NSQ, \end{cases}$$

$$\chi_\delta(D_{nsq}) = \begin{cases} -C, & \text{if } f^\star(\delta)=0, \\ E, & \text{if } f^\star(\delta)\in SQ, \\ D, & \text{if } f^\star(\delta)\in NSQ, \end{cases}$$

$$\chi_\delta(D_{nsq,0}) = \begin{cases} -C, & \text{if } f^\star(\delta)=0, \\ D, & \text{if } f^\star(\delta)\in SQ, \\ -E, & \text{if } f^\star(\delta)\in NSQ, \end{cases}$$

where

$$\begin{aligned} A &= \epsilon\frac{(p-1)}{2p}\sqrt{p^*}^{\,n+s}, \\ B &= \epsilon(\tfrac{p+1}{2p})\sqrt{p^*}^{\,n+s}, \\ C &= \epsilon(\tfrac{p-1}{2})\sqrt{p^*}^{\,n+s-1}, \\ D &= \epsilon(\tfrac{p^*+p}{2p^*})\sqrt{p^*}^{\,n+s-1}, \\ E &= \epsilon(\tfrac{p^*-p}{2p^*})\sqrt{p^*}^{\,n+s-1}. \end{aligned}$$

Proof: For the set D_0, from the definition of the character sum in (2), we have

$$\chi_\delta(D_0) = \sum_{x\in D_0}\xi_p^{\mathrm{Tr}^n(\delta x)} = \sum_{i=0}^{p-1}\mathcal{N}_f(\delta,i)\xi_p^i.$$

Then, by the fact that $\sum_{i=0}^{p-1}\xi_p^i=0$, the expected results can be derived from Lemma 7 and [24, Lemma 7]. For the sets D_{sq} and D_{nsq}, the results follow similarly from Lemma 9 and [24, Lemma 9]. Furthermore, for the sets $D_{sq,0}$ and $D_{nsq,0}$, they are derived from Lemmas 7, 9 and [24, Lemma 11]. □

4. Linear (minimal) codes from weakly regular plateaued balanced functions

For a subset U of $\mathbb{F}_{p^n}$, we define a function

$$g(x,y) = \mathrm{Tr}^n(\phi(x)y) \tag{4}$$

from $\mathbb{F}_{p^{2n}}$ to $\mathbb{F}_p$, where ϕ is a polynomial from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$ such that ϕ is an injection from U to $\mathbb{F}_{p^n}^\star$ and $\phi(x)=0$ for any $x\in\mathbb{F}_{p^n}\setminus U$. The linear code $\mathcal{C}_U$ associated with the set U is defined as

$$\mathcal{C}_U = \{c_{\alpha,\delta_1,\delta_2} \mid \alpha\in\mathbb{F}_p, \delta_1\in\mathbb{F}_{p^n}, \delta_2\in\mathbb{F}_{p^n}\}, \tag{5}$$

where

$$c_{\alpha,\delta_1,\delta_2} = (\alpha g(x,y) - \mathrm{Tr}^n(\delta_1 x) - \mathrm{Tr}^n(\delta_2 y))_{(x,y)\in\mathbb{F}_{p^{2n}}^\star}.$$

From the definition of the code $\mathcal{C}_U$, its length is $p^{2n}-1$ and dimension is $2n+1$. The Hamming weights in $\mathcal{C}_U$ can be obtained from [16, Section 5] by considering the Walsh spectrum of a function g.

Lemma 11 [16] Let $\mathcal{C}_U$ be the code of the form of (5). Then

$$wt(c_{\alpha,\delta_1,\delta_2}) = \begin{cases} 0, & \text{if } \alpha=\delta_1=\delta_2=0, \\ A, & \text{if } \alpha=0,\ (\delta_1,\delta_2)\neq(0,0), \\ B, & \text{if } \alpha\in\mathbb{F}_p^\star, \delta_1\in\mathbb{F}_{p^n}, \delta_2\in\mathbb{F}_{p^n}, \end{cases}$$

where $A=p^{2n}-p^{2n-1}$ and

$$B = p^{2n}-p^{2n-1}-\frac{1}{p}\sum_{\omega\in\mathbb{F}_p^\star}\sigma_\omega\left(\sigma_\alpha(\widehat{g}(\alpha^{-1}\delta_1,\alpha^{-1}\delta_2))\right).$$

Lemma 12 [28] For $(x,y)\in\mathbb{F}_{p^n}\times\mathbb{F}_{p^n}$, let $g(x,y)=\mathrm{Tr}^n(\phi(x)y)$ be the function of the form of (4). For $(\delta_1,\delta_2)\in\mathbb{F}_{p^n}\times\mathbb{F}_{p^n}$,

$$\widehat{g}(\delta_1,\delta_2) = \begin{cases} p^n\displaystyle\sum_{x\in\mathbb{F}_{p^n}\setminus U}\xi_p^{-\mathrm{Tr}^n(\delta_1 x)}, & \text{if } \delta_2=0, \\ p^n\xi_p^{-\mathrm{Tr}^n(\delta_1\phi^{-1}(\delta_2))}, & \text{if } \delta_2\in Im(\phi)^\star, \\ 0, & \text{if } \delta_2\notin Im(\phi), \end{cases}$$

where $Im(\phi)$ denotes the image of ϕ.

For any $\delta_1 \in \mathbb{F}_{p^n}^\star$, one can verify that

$$\sum_{x \in \mathbb{F}_{p^n} \setminus U} \xi_p^{-\mathrm{Tr}^n(\delta_1 x)} = -\chi_{\delta_1}(U).$$

The following proposition describes the minimality conditions of the code $\mathcal{C}_U$ in (5) for a given subset U of $\mathbb{F}_q$.

Proposition 1 [28] If a subset U of $\mathbb{F}_q$ holds the following conditions:

1. $(p-1) < \#U < p^{n-1}(p-1)$,
2. $\#\{x \in U : \mathrm{Tr}^n(\delta_1 x) \neq 0\} \geq 2$ for $\delta_1 \in \mathbb{F}_{p^n}^\star$,
3. $\max\limits_{\delta_1 \in \mathbb{F}_{p^n}^\star} \#\{x \in U : \mathrm{Tr}^n(\delta_1 x) = i\} < (p-1)p^{n-2}$ for $i \in \mathbb{F}_p$,

then $\mathcal{C}_U$ of the form of (5) is minimal code.

Xu et al.[27] have initially provided the construction method of minimal linear codes in [27, Theorem 3.1]. They have proposed two classes of minimal codes $\mathcal{C}_U$ of the form of (5) by choosing the suitable subsets U of $\mathbb{F}_{p^n}$ in the proposed method. Later, Xu et al. have generalized this construction method in [28, Theorem 10] for a new type of function. They have selected the set $U = D_0 = \{x \in \mathbb{F}_q : f(x) = 0\}$, where f is weakly regular bent and they obtained a class of minimal codes based on this set. Very recently, Mesnager and Sınak [19] have generalized this method by using weakly regular plateaued unbalanced function f in the subsets D_0, D_{sq} and D_{nsq}. Then, they have obtained three infinite classes of minimal codes with six-weights from these subsets. In this paper, within this framework, we use weakly regular plateaued balanced functions in the subsets defined in (3) so that we can obtain new linear codes $\mathcal{C}_U$ of the form (5). This enables us to obtain new classes of minimal codes with six-weights over $\mathbb{F}_p$. One can easily find the sizes of these subsets since f is balanced function. Clearly we have

$$\begin{aligned}
\#D_0 &= p^{n-1}, \\
\#D_{sq} &= \#D_{nsq} = \tfrac{(p-1)}{2} p^{n-1}, \\
\#D_{sq,0} &= \#D_{nsq,0} = \tfrac{(p+1)}{2} p^{n-1}.
\end{aligned}$$

We first construct minimal codes based on the set D_0.

Theorem 1 Let $n+s$ be even with $1 \leq s \leq n-2$, and $f \in$ WRPB. Let D_0 be the set given in (3). Then, the six-weight code $\mathcal{C}_{D_0}$ in (5) has the parameters $[p^{2n}-1, 2n+1]_p$ and Hamming weights presented in Table 1. Furthermore, it is minimal when $s+4 \leq n$.

Proof: The Hamming weights of nonzero codewords in $\mathcal{C}_{D_0}$ can be computed from Lemmas 10 and 11. For $\alpha = 0$ and $(\delta_1, \delta_2) \neq (0,0)$, we clearly have $wt(c_{0,\delta_1,\delta_2}) = p^{2n} - p^{2n-1}$. We focus on computing the Hamming weights $wt(c_{\alpha,\delta_1,\delta_2})$ when $\alpha \in \mathbb{F}_p^\star$ and $\delta_1, \delta_2 \in \mathbb{F}_{p^n}$.

- When $\alpha \neq 0$ and $(\delta_1, \delta_2) = (0,0)$, we have $wt(c_{\alpha,0,0}) = p^{n-1}(p-1)\#D_0$.
- When $\alpha \neq 0$, $\delta_1 \neq 0$ and $\delta_2 = 0$, by considering Lemma 10, the Hamming weight $wt(c_{\alpha,\delta_1,0})$ is

$$\begin{aligned}
& p^{2n} - p^{2n-1} + p^{n-1} \sum_{\omega \in \mathbb{F}_p^\star} \sigma_\omega(\chi_{\delta_1}(D_0)) \\
&= \begin{cases} p^{2n-1}(p-1), & \text{if } \delta_1 \in \mathbb{F}_q^\star \setminus \mathcal{S}_f, \\ (p^{2n-1} + A)(p-1), & \text{if } f^\star(\delta_1) = 0, \\ p^{2n-1}(p-1) - A, & \text{if } f^\star(\delta_1) \neq 0, \end{cases}
\end{aligned}$$

  where $A = \epsilon p^{n-2}(p-1)\sqrt{p^*}^{\,n+s}$.
- When $\alpha \neq 0$ and $\alpha^{-1}\delta_2 \in Im(\phi)^\star$, the Hamming weight $wt(c_{\alpha,\delta_1,\delta_2})$ is

$$p^{2n} - p^{2n-1} - p^{n-1} \sum_{\omega \in \mathbb{F}_p^\star} \xi_p^{-\omega \mathrm{Tr}^n(\delta_1 \phi^{-1}(\alpha^{-1}\delta_2))}.$$

  - For $\phi^{-1}(\alpha^{-1}\delta_2) = 0$, then we have $wt(c_{\alpha,\delta_1,\delta_2}) = p^{2n} - p^{2n-1} - (p-1)p^{n-1}$.
  - For $\phi^{-1}(\alpha^{-1}\delta_2) \neq 0$, we have two cases.

  - * If $\mathrm{Tr}^n(\delta_1\phi^{-1}(\alpha^{-1}\delta_2)) = 0$, we have $wt(c_{\alpha,\delta_1,\delta_2}) = p^{2n} - p^{2n-1} - (p-1)p^{n-1}$.
  - * If $\mathrm{Tr}^n(\delta_1\phi^{-1}(\alpha^{-1}\delta_2)) \neq 0$, we have $wt(c_{\alpha,\delta_1,\delta_2}) = p^{2n} - p^{2n-1} + p^{n-1}$.
- When $\alpha \neq 0$ and $\alpha^{-1}\delta_2 \notin Im(\phi)$, we have $wt(c_{\alpha,\delta_1,\delta_2}) = p^{2n} - p^{2n-1}$.

Besides, the weight distributions of such codewords are completely obtained from Lemmas 3, 5 and 12. By Proposition 1, the code is minimal, thereby completing the proof. □

Example 1 Let $p = 5$ and $n = 5$. Let $f \in$ WRPB with $s = 1$ and $\epsilon = 1$. The code $\mathcal{C}_{D_0}$ in Theorem 1 is a six-weight minimal $[9765624, 11, 1562500]_5$ code over $\mathbb{F}_5$ with $1 + 4y^{1562500} + 580y^{8062500} + 1920y^{7750000} + 1572500y^{7810000} + 41013120y^{7812500} + 6240000y^{7813125}$.

Remark 1 When $n + s$ is odd in Theorem 1, the code $\mathcal{C}_{D_0}$ has the same parameters of the code $\mathcal{C}_{D_{f,0}}$ in [19, Theorem 2].

Theorem 2 Let $f \in$ WRPB and D_{sq} be the set given in (3). Then, the code $\mathcal{C}_{D_{sq}}$ in (5) is a six-weight $[p^{2n} - 1, 2n + 1]_p$ code over $\mathbb{F}_p$. The parameters of $\mathcal{C}_{D_{sq}}$ are presented in

- Table 2 if $n + s$ is even with $1 \leq s \leq n - 2$,
- Table 3 if $n + s$ is odd with $1 \leq s \leq n - 1$.

Furthermore, it is minimal for $s + 3 \leq n$.

Proof: The Hamming weights of nonzero codewords in $\mathcal{C}_{D_{sq}}$ can be obtained from Lemmas 10 and 11. We compute them for each case in the following.

- For $\alpha = 0$ and $(\delta_1, \delta_2) \neq (0, 0)$, we have $wt(c_{0,\delta_1,\delta_2}) = p^{2n} - p^{2n-1}$.
- For $\alpha \neq 0$ and $(\delta_1, \delta_2) = (0, 0)$, we have $wt(c_{\alpha,0,0}) = p^{n-1}(p-1)\#D_{sq}$.
- For $\alpha \in \mathbb{F}_p^\star$, $\delta_1 \in \mathbb{F}_{p^n}^\star$ and $\delta_2 = 0$, by considering Lemma 10, we obtain

$$wt(c_{\alpha,\delta_1,0}) = \begin{cases} A, & \text{if } \delta_1 \in \mathbb{F}_q^\star \setminus \mathcal{S}_f, \\ B, & \text{if } f^\star(\delta) \in NSQ \cup \{0\}, \\ C, & \text{if } f^\star(\delta) \in SQ \end{cases}$$

when $n + s$ is even; otherwise,

$$wt(c_{\alpha,\delta_1,0}) = \begin{cases} A, & \text{if } \delta_1 \in \mathbb{F}_q^\star \setminus \mathcal{S}_f, \\ D, & \text{if } f^\star(\delta) = 0, \\ E, & \text{if } f^\star(\delta) \in SQ, \\ F, & \text{if } f^\star(\delta) \in NSQ, \end{cases}$$

where

$$\begin{aligned} A &= (p-1)p^{2n-1}, \\ B &= (p-1)(p^{2n-1} - \epsilon\tfrac{(p-1)}{2}p^{n-2}\sqrt{p^*}^{\,n+s}), \\ C &= (p-1)(p^{2n-1} + \epsilon\tfrac{(p+1)}{2}p^{n-2}\sqrt{p^*}^{\,n+s}), \\ D &= (p-1)(p^{2n-1} + \epsilon\tfrac{(p-1)}{2}p^{n-1}\sqrt{p^*}^{\,n+s-1}), \\ E &= (p-1)(p^{2n-1} - \epsilon\tfrac{(p^*+p)}{2p^*}p^{n-1}\sqrt{p^*}^{\,n+s-1}), \\ F &= (p-1)(p^{2n-1} - \epsilon\tfrac{(p^*-p)}{2p^*}p^{n-1}\sqrt{p^*}^{\,n+s-1}). \end{aligned}$$

- For $\alpha \neq 0$ and $\alpha^{-1}\delta_2 \in Im(\phi) \setminus \{0\}$, we get $\phi^{-1}(\alpha^{-1}\delta_2) \neq 0$ since $0 \notin D_{sq}$. Then we have the following two cases:
  - If $\mathrm{Tr}^n(\delta_1\phi^{-1}(\alpha^{-1}\delta_2)) = 0$, we have $wt(c_{\alpha,\delta_1,\delta_2}) = p^{2n} - p^{2n-1} - (p-1)p^{n-1}$.
  - If $\mathrm{Tr}^n(\delta_1\phi^{-1}(\alpha^{-1}\delta_2)) \neq 0$, we have $wt(c_{\alpha,\delta_1,\delta_2}) = p^{2n} - p^{2n-1} + p^{n-1}$.
- For $\alpha \neq 0$ and $\alpha^{-1}\delta_2 \notin Im(\phi)$, we have $wt(c_{\alpha,\delta_1,\delta_2}) = p^{2n} - p^{2n-1}$.

Besides, the weight distributions of these codewords can be derived from Lemmas 3, 5 and 11. By Proposition 1, the code is minimal. The proof is hence complete. □

Example 2 Let $p = 5$ and $n = 6$. Let $f \in$ WRPB with $s = 2$ and the sign $\epsilon = 1$. The code $\mathcal{C}_{D_{sq}}$ in Theorem 2 is a six-weight minimal $[244140624, 13, 78125000]_5$ code over $\mathbb{F}_5$ with $1 + 4y^{78125000} + 1540y^{192187500} + 960y^{200000000} + 78125000y^{195300000} + 830075620y^{195312500} + 312500000y^{195315625}$.

Theorem 3 Let $f \in$ WRPB and $D_{sq,0}$ be the set given in (3). Then, the code $\mathcal{C}_{D_{sq,0}}$ in (5) is a six-weight $[p^{2n}-1, 2n+1]_p$ code over $\mathbb{F}_p$. The parameters of $\mathcal{C}_{D_{sq,0}}$ are presented in

- Table 4 if $n+s$ is even with $1 \leq s \leq n-2$,
- Table 5 if $n+s$ is odd with $1 \leq s \leq n-1$.

Furthermore, it is minimal for $p > 3$ and $s+3 \leq n$.

Proof: It is similar to the proof of Theorem 1. □

Example 3 Let $p = 5$ and $n = 5$. Let $f \in$ WRPB with $s = 2$ and the sign $\epsilon = 1$. The code $\mathcal{C}_{D_{sq,0}}$ in Theorem 3 is a six-weight minimal $[9765624, 11,]_5$ code over $\mathbb{F}_5$ with the weight enumerator $1 + 4y^{4687500} + 100y^{8437500} + 25390360y^{7812500} + 160y^{7500000} + 4697500y^{7810000} + 18740000y^{7813125}$.

Theorem 4 Let $n+s$ be odd with $1 \leq s \leq n-1$, and $f \in$ WRPB. Let D_{nsq} be the set defined as in (3). Then, the six-weight code $\mathcal{C}_{D_{nsq}}$ in (5) has the parameters $[p^{2n}-1, 2n+1]_p$ and the Hamming weights presented in Table 6. Furthermore, it is minimal for $s+3 \leq n$.

Proof: It is similar to the proof of Theorem 2. □

Example 4 Let $p = 3$ and $n = 4$. Let $f \in$ WRPB with $s = 1$ and the sign $\epsilon = 1$. The code $\mathcal{C}_{D_{nsq}}$ in Theorem 4 is a six-weight ternary minimal $[6560, 9, 1458]_3$ code over $\mathbb{F}_3$ with the weight enumerator $1+2y^{1458}+18y^{3888}+12y^{4860}+15276y^{4374}+1458y^{4320}+2916y^{4401}$.

Theorem 5 Let $n+s$ is odd with $1 \leq s \leq n-1$, and $f \in$ WRPB. Let $D_{nsq,0}$ be the set given in (3). Then, the six-weight code $\mathcal{C}_{D_{nsq,0}}$ in (5) has the parameters $[p^{2n}-1, 2n+1]_p$ and the Hamming weights presented in Table 7. Furthermore, it is minimal for $p > 3$ and $s+3 \leq n$.

Proof: It is similar to the proof of Theorem 1. □

Remark 2 When $n+s$ is even, both $\mathcal{C}_{D_{sq}}$ and $\mathcal{C}_{D_{nsq}}$ are the same code, and similarly both $\mathcal{C}_{D_{sq,0}}$ and $\mathcal{C}_{D_{nsq,0}}$ are the same code.

5. Conclusion

Motivated by the previous works [19], [27], [28], we constructed six-weight minimal linear codes by considering a new type of functions over $\mathbb{F}_p$ and new subsets of $\mathbb{F}_q$. We proposed five classes of minimal codes by using five different subsets of the preimages of weakly regular plateaued balanced functions. The Hamming weights in the constructed codes follow from the Walsh spectrum of the function $f \in$ WRPB and the function g of the form of (4). The weight distributions of the proposed codes follow from the subsets of the preimages of $f \in$ WRPB. As far as we know, the six-weight minimal linear codes proposed in this paper are new codes since for the first time we employed weakly regular plateaued balanced functions in the construction method proposed in [28].

One of the interesting research problems on the construction method proposed in [27], [28] is to determine the best proper subset U of $\mathbb{F}_q$ that defines the best code over $\mathbb{F}_p$.

It is a well-known fact that minimal codes can be applied to obtain secret sharing schemes with perfect access structures. The constructed minimal codes contribute to the design of secret sharing schemes with high democracy as in [8, Proposition 2].

Acknowledgments

The author thanks the anonymous reviewers for their valuable comments that have improved the organization of the paper.

Appendix A

This section presents the Hamming weights in $\mathcal{C}_U$ and its weight distributions in Tables 1-7.

References

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

[2] D. Bartoli and M. Bonini. Minimal linear codes in odd characteristic. IEEE Transactions on Information Theory, 65(7):4152–4155, 2019.

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

[4] S. Chang and J. Y. Hyun. Linear codes from simplicial complexes. Designs, Codes and Cryptography, 86(10):2167–2181, 2018.

[5] C. Ding. Linear codes from some 2-designs. IEEE Transactions on information theory, 61(6):3265–3275, 2015.

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

[7] C. Ding, Z. Heng, and Z. Zhou. Minimal binary linear codes. IEEE Transactions on Information Theory, 64(10):6536–6545, 2018.

[8] C. Ding and J. Yuan. Covering and secret sharing with linear codes. DMTCS, 2731:11–25, 2003.

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

[10] Z. Heng, C. Ding, and Z. Zhou. Minimal linear codes over finite fields. Finite Fields and Their Applications, 54:176–196, 2018.

[11] W. C. Huffman, J.-L. Kim, and P. Solé. Linear codes from functions in Chapter 20 of Concise Encyclopedia of Coding Theory. Chapman and Hall/CRC, 2021.

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

[13] R. Lidl and H. Niederreiter. Finite fields, volume 20. Cambridge university press, 1997.

[14] J. L. Massey. Minimal codewords and secret sharing. In Proceedings of the 6th joint Swedish-Russian international workshop on information theory, pages 276–279, 1993.

[15] S. Mesnager. Characterizations of plateaued and bent functions in characteristic p. In International Conference on Sequences and Their Applications, pages 72–82. Springer, 2014.

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

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

[18] S. Mesnager, Y. Qi, H. Ru, and C. Tang. Minimal linear codes from characteristic functions. IEEE Transactions on Information Theory, 2020.

[19] S. Mesnager and A. Sınak. Infinite classes of six-weight linear codes derived from weakly regular plateaued functions. In 2020 International Conference on Information Security and Cryptology (ISCTURKEY), pages 93–100. IEEE, 2020.

[20] S. Mesnager and A. Sınak. Several classes of minimal linear codes with few weights from weakly regular plateaued functions. IEEE Transactions on Information Theory, 66(4):2296–2310, 2020.

[21] S. Mesnager, A. Sınak, and O. Yayla. Minimal linear codes with few weights and their secret sharing. International Journal of Information Security Science, 8(4):77–87, 2019.

[22] Y. Qi, T. Yang, and B. Dai. Minimal linear codes from vectors with given weights. IEEE Communications Letters, 24(12):2674–2677, 2020.

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

[24] A. Sınak. Minimal linear codes from weakly regular plateaued balanced functions. Discrete Mathematics, 2020.

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

[26] G. Xu and L. Qu. Three classes of minimal linear codes over the finite fields of odd characteristic. IEEE Transactions on Information Theory, 65(11):7067–7078, 2019.

[27] G. Xu, L. Qu, and X. Cao. Minimal linear codes from maiorana-mcfarland functions. Finite Fields and Their Applications, 65:101688, 2020.

[28] G. Xu, L. Qu, and G. Luo. Minimal linear codes from weakly regular bent functions. The 11th International

Conference on Sequences and Their Applications (SETA 2020).
[29] Y. Zheng and X.-M. Zhang. Plateaued functions. In ICICS, volume 99, pages 284–300. Springer, 1999.

Table 1: The Hamming weights in $\mathcal{C}_{D_0}$ in Theorem 1

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

Table 2: The Hamming weights in $\mathcal{C}_{D_{sq}}$ when $n+s$ is even in Theorem 2

Hamming weight w	Multiplicity A_w
0	1
$\frac{1}{2}p^{2n-2}(p-1)^2$	$p-1$
$(p-1)(p^{2n-1}-\epsilon\frac{1}{2}(p-1)p^{n-2}\sqrt{p^*}^{\,n+s})$	$\frac{1}{2}(p-1)((p+1)p^{n-s-1}+\epsilon\eta_0^{n+1}(-1)(p-1)\sqrt{p^*}^{\,n-s-2})$
$(p-1)(p^{2n-1}+\epsilon\frac{1}{2}(p+1)p^{n-2}\sqrt{p^*}^{\,n+s})$,	$\frac{1}{2}(p-1)^2(p^{n-s-1}-\epsilon\eta_0^{n+1}(-1)\sqrt{p^*}^{\,n-s-2})$
$(p-1)(p^n-1)p^{n-1}$	$\frac{1}{2}p^{2n-2}(p-1)^2$
$(p-1)p^{2n-1}$	$p^{2n}-1+(p-1)(p^{2n}-p^{n-s}-p^{2n-1}(p-1)/2-1)$
$(p-1)p^{2n-1}+p^{n-1}$	$\frac{1}{2}(p-1)^3p^{2n-2}$

Table 3: The Hamming weights in $\mathcal{C}_{D_{sq}}$ when $n+s$ is odd in Theorem 2

Hamming weight w	Multiplicity A_w
0	1
$\frac{1}{2}(p-1)^2p^{2n-2}$	$p-1$
$(p-1)(p^{2n-1}+\epsilon\frac{1}{2}(p-1)p^{n-1}\sqrt{p^*}^{\,n+s-1})$	$(p-1)p^{n-s-1}$
$(p-1)(p^{2n-1}-\epsilon\frac{(p+p^*)}{2p^*}p^{n-1}\sqrt{p^*}^{\,n+s-1})$	$\frac{1}{2}(p-1)^2(p^{n-s-1}+\epsilon\eta_0^{n}(-1)\sqrt{p^*}^{\,n-s-1})$
$(p-1)(p^{2n-1}-\epsilon\frac{(p^*-p)}{2p^*}p^{n-1}\sqrt{p^*}^{\,n+s-1})$	$\frac{1}{2}(p-1)^2(p^{n-s-1}-\epsilon\eta_0^{n}(-1)\sqrt{p^*}^{\,n-s-1})$
$(p-1)(p^n-1)p^{n-1}$	$\frac{1}{2}(p-1)^2p^{2n-2}$
$(p-1)p^{2n-1}$	$p^{2n}-1+(p-1)(p^{2n}-p^{n-s}-p^{2n-1}(p-1)/2-1)$
$(p-1)p^{2n-1}+p^{n-1}$	$\frac{1}{2}(p-1)^3p^{2n-2}$

Table 4: The Hamming weights in $\mathcal{C}_{D_{sq,0}}$ when $n+s$ is even in Theorem 3

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

Table 5: The Hamming weights in $\mathcal{C}_{D_{sq,0}}$ when $n+s$ is odd in Theorem 3

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

Table 6: The Hamming weights in $\mathcal{C}_{D_{nsq}}$ in Theorem 4

Hamming weight w	Multiplicity A_w
0	1
$\frac{1}{2}(p-1)^2p^{2n-2}$	$p-1$
$(p-1)(p^{2n-1}-\epsilon\frac{1}{2}(p-1)p^{n-1}\sqrt{p^*}^{\,n+s-1})$	$(p-1)p^{n-s-1}$
$(p-1)(p^{2n-1}+\epsilon\frac{(p^*-p)}{2p^*}p^{n-1}\sqrt{p^*}^{\,n+s-1})$	$\frac{1}{2}(p-1)^2(p^{n-s-1}+\epsilon\eta_0^{n}(-1)\sqrt{p^*}^{\,n-s-1})$
$(p-1)(p^{2n-1}+\epsilon\frac{(p+p^*)}{2p^*}p^{n-1}\sqrt{p^*}^{\,n+s-1})$	$\frac{1}{2}(p-1)^2(p^{n-s-1}-\epsilon\eta_0^{n}(-1)\sqrt{p^*}^{\,n-s-1})$
$(p-1)(p^n-1)p^{n-1}$	$\frac{1}{2}(p-1)^2p^{2n-2}$
$(p-1)p^{2n-1}$	$p^{2n}-1+(p-1)(p^{2n}-p^{n-s}-p^{2n-1}(p-1)/2-1)$
$(p-1)p^{2n-1}+p^{n-1}$	$\frac{1}{2}(p-1)^3p^{2n-2}$

Table 7: The Hamming weights in $\mathcal{C}_{D_{nsq,0}}$ in Theorem 5

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