INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE
Mesnager et al., Vol.8, No.4, pp.77-87

Minimal Linear Codes with Few Weights and Their Secret Sharing

Sihem Mesnager[1], Ahmet Sınak[2], Oğuz Yayla[3]

[1]Department of Mathematics, University of Paris VIII, 93526 Saint-Denis, France, LAGA UMR 7539, CNRS, Sorbonne Paris Cité, University of Paris XIII, 93430 Villetaneuse, France and Telecom ParisTech, 91120 Palaiseau, France

[2]Department of Mathematics and Computer, Necmettin Erbakan University, 42090 Konya, Turkey and LAGA UMR 7539, CNRS, Sorbonne Paris Cité, University of Paris XIII, 93430 Villetaneuse, France

[3]Department of Mathematics, Hacettepe University, 06800 Ankara, Turkey

Corresponding Author: *asinak@erbakan.edu.tr*

ORCID iD: 0000-0003-4008-2031, 0000-0002-1071-765X, 0000-0001-8945-2780

Research Paper Received: 30.10.2019 Revised: 02.12.2019 Accepted: 11.12.2019

Abstract—Minimal linear codes with few weights have significant applications in secure two-party computation and secret sharing schemes. In this paper, we construct two-weight and three-weight minimal linear codes by using weakly regular plateaued functions in the well-known construction method based on the second generic construction. We also give punctured codes and subcodes for some constructed minimal codes. We finally obtain secret sharing schemes with high democracy from the dual codes of our minimal codes.

Keywords—Minimal linear code, weakly regular plateaued function, secret sharing scheme

1. Introduction

There are several applications of minimal linear codes such as secure two-party computation and secret sharing schemes (SSS). Constructing linear codes with perfect parameters is an attractive research topic in the literature. A number of construction methods for linear codes were proposed, one of them is based on some good functions over finite fields. Recently, some functions were used to obtain new linear codes with few weights in the second generic construction method (see [6], [7], [20], [21], [24]). Especially, bent functions (mostly, quadratic and weakly regular bent functions) were extensively employed to obtain linear codes with good parameters (see [7], [20], [24]). Very recently, weakly regular plateaued functions have been employed in [12], [14], [19] to construct minimal linear codes with few weights. In this paper, we construct further two- and three-weight minimal linear codes with good and flexible parameters. In addition to the codes constructed in [13], we here study the

The first version of this work [13] was presented at the 2IWCA'19.

subcodes of the constructed codes and obtain new classes of minimal codes with good parameters. We note that the dual of a subcode is expected to be more optimal as the dimension of the dual subcode is greater than that of the original dual code.

The content of the paper is organized as follows. The notation and some previous works related to plateaued functions are given in Section 2. Then, in Section 3, we construct two- and three-weight linear codes by using weakly regular plateaued functions in the second generic construction method. We also record the punctured codes and subcodes for some constructed codes. Section 4 shows that all constructed codes are minimal codes, which are used to construct the SSS with high democracy.

2. Preliminaries

Let p be a prime and n be a positive integer. We use $\mathbb{F}_{p^n}$ to denote the finite field with p^n elements. We sometimes see $\mathbb{F}_p^n$ as an n-dimensional vector space over $\mathbb{F}_p$. The *support* of a vector $\mathbf{a} = (a_0, \ldots, a_{n-1}) \in \mathbb{F}_p^n$ is described as $\mathrm{supp}(\mathbf{a}) = \{0 \leq i \leq n-1 : a_i \neq 0\}$. The Hamming weight of $\mathbf{a}$, symbolized by $wt(\mathbf{a})$, is defined as the size of $\mathrm{supp}(\mathbf{a})$. A k-dimensional linear subspace $\mathcal{C}$ of $\mathbb{F}_p^n$ is called *linear code*, and each of its element is called a *codeword*. The minimum Hamming weight of the nonzero codewords of $\mathcal{C}$ is said to be the minimum Hamming distance of $\mathcal{C}$. A linear code $\mathcal{C}$ over $\mathbb{F}_p$ with length n, dimension k and minimum Hamming distance d is represented by $[n, k, d]$, and its *dual code* $\mathcal{C}^\perp = \{\mathbf{b} \in \mathbb{F}_p^n : \mathbf{b} \cdot \mathbf{a} = \mathbf{0}$ for all $\mathbf{a} \in \mathcal{C}\}$ is denoted by $[n, n-k, d^\perp]$.

Let A_w denote the number of codewords with Hamming weight w in $\mathcal{C}$ of length n. Then, the *weight distribution* of $\mathcal{C}$ is $(1, A_1, \ldots, A_n)$ and its *weight enumerator* is the polynomial $W_{\mathcal{C}}(y) = 1 + A_1 y + \cdots + A_n y^n$. Besides, $\mathcal{C}$ is called a *t-weight code* if $W_{\mathcal{C}}$ has t nonzero coefficients. A $k \times n$ matrix G whose rows form a basis for $\mathcal{C}$ is said to be a *generator matrix* of $\mathcal{C}$. Note that a codeword $\mathbf{a}$ in $\mathcal{C}$ covers another codeword $\mathbf{b}$ in $\mathcal{C}$ if $\mathrm{supp}(\mathbf{b}) \subseteq \mathrm{supp}(\mathbf{a})$ holds. If a nonzero codeword $\mathbf{a} \in \mathcal{C}$ does not cover any element in $\mathcal{C} \setminus \{c_j = j\mathbf{a} : j \in \mathbb{F}_p\}$, then $\mathbf{a}$ is called the *minimal* codeword. A linear code $\mathcal{C}$ is called *minimal* linear code if all nonzero codewords of $\mathcal{C}$ are minimal. The class of such codes is a very special subclass of linear codes.

For a set S, $\#S$ expresses the size of S and $S^\star = S\setminus\{0\}$. The symbols SQ and NSQ symbolize the set of all *squares* and *non-squares* in $\mathbb{F}_p^\star$, respectively. We denote by η_0 the *quadratic character* of $\mathbb{F}_p^\star$, and $p^* = \eta_0(-1)p$. The *trace* of $\beta \in \mathbb{F}_{p^n}$ over $\mathbb{F}_p$ is defined as $\mathrm{Tr}^n(\beta) = \beta + \beta^p + \beta^{p^2} + \cdots + \beta^{p^{n-1}}$. Given a function $f : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_p$, its *Walsh transform* is a function from $\mathbb{F}_{p^n}$ to $\mathbb{C}$ defined as

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

where $\xi_p = e^{2\pi i/p}$ is a *complex primitive p-th root of unity*. Note that f is *balanced* over $\mathbb{F}_p$ if $\widehat{\chi_f}(0) = 0$; otherwise, f is *unbalanced*.

The plateaued functions were first defined in 1999 by Zheng and Zhang [23]. For a prime p, f is called *p-ary s-plateaued* if $|\widehat{\chi_f}(\beta)|^2 \in \{0, p^{n+s}\}$ for all $\beta \in \mathbb{F}_{p^n}$, where s is an integer with $0 \leq s \leq n$. Then, its *Walsh support* is defined as $\mathcal{S}_f = \{\beta \in \mathbb{F}_{p^n} : |\widehat{\chi_f}(\beta)|^2 = p^{n+s}\}$, and $\#\mathcal{S}_f = p^{n-s}$ from the Parseval identity. Indeed, the Parseval identity implies the following lemma.

Lemma 1: Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be an s-plateaued function. Then, the square of its Walsh transform values takes p^{n-s} times the value p^{n+s} and $p^n - p^{n-s}$ times the value 0.

Very recently, Mesnager et al. [11], [12] introduced subclasses of plateaued functions. An s-plateaued f is said to be *weakly regular* if there exists a complex number u (indeed, $u \in \{\pm 1, \pm i\}$) and a p-ary function g over $\mathbb{F}_{p^n}$ with $g(\beta) = 0$ for all $\beta \in \mathbb{F}_{p^n} \setminus \mathcal{S}_f$ such that $\widehat{\chi_f}(\beta) \in \{0, up^{\frac{n+s}{2}} \xi_p^{g(\beta)}\}$ for all $\beta \in \mathbb{F}_{p^n}$. Otherwise, f is said to be *non-weakly regular*.

Lemma 2: [12] Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be a weakly regular s-plateaued function. Then for all $\beta \in \mathcal{S}_f$,

$$\widehat{\chi_f}(\beta) = \epsilon \sqrt{p^*}^{n+s} \xi_p^{g(\beta)},$$

where $\epsilon = \pm 1$ is the sign of $\widehat{\chi_f}$ and g is a p-ary function over $\mathcal{S}_f$.

Lemma 3: [14] Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be a weakly regular s-plateaued function. For $j \in \mathbb{F}_p$, we describe the set $\{\beta \in \mathcal{S}_f : g(\beta) = j\}$. Then, the size of this set is equal to

$$\begin{cases} p^{n-s-1} + \epsilon \eta_0^{n+1}(-1)(p-1)\sqrt{p^*}^{n-s-2}, & \text{if } j = 0, \\ p^{n-s-1} - \epsilon \eta_0^{n+1}(-1)\sqrt{p^*}^{n-s-2}, & \text{if } j \in \mathbb{F}_p^\star \end{cases}$$

when $n - s$ is even; otherwise,

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

3. Linear codes from weakly regular plateaued functions

In this section, we apply the construction method of binary linear codes from Boolean functions proposed by C. Ding [5], [6] for weakly regular plateaued functions in characteristic p.

Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$. The *support* of f is defined to be a set

$$D_f = \{x \in \mathbb{F}_{p^n} : f(x) \neq 0\}. \tag{1}$$

Assume $n_f = \#D_f$ and $D_f = \{d_1, d_2, \ldots, d_{n_f}\}$. A linear code involving D_f is defined as

$$\mathcal{C}_{D_f} = \{c_\beta = (\mathrm{Tr}^n(\beta d_1), \ldots, \mathrm{Tr}^n(\beta d_{n_f})) : \beta \in \mathbb{F}_{p^n}\}, \tag{2}$$

whose length is n_f and dimension is at most n. Here, the set D_f is called the *defining set* of the code $\mathcal{C}_{D_f}$.

In the following subsections, we make use of some weakly regular plateaued functions in order to obtain linear codes, over the finite fields of characteristic p.

3.1. Linear codes from weakly regular plateaued unbalanced functions

We first consider weakly regular plateaued unbalanced functions in the second generic construction method. We recall from [14] that *WRP* denotes the set of weakly regular p-ary plateaued unbalanced functions satisfying the following two homogeneous conditions. For a function f

- $f(0) = 0$ and
- there exists a positive even integer t with $\gcd(t-1, p-1) = 1$ such that $f(ax) = a^t f(x)$ for every $a \in \mathbb{F}_p^\star$ and $x \in \mathbb{F}_{p^n}$.

The following lemma can be given as a natural consequence of [14, Lemma 9].

Lemma 4: Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be an unbalanced function with $\widehat{\chi_f}(0) = \epsilon \sqrt{p^*}^{n+s}$ where $\epsilon = \pm 1$, and let D_f be given in (1). Then we have

$$\#D_f = \begin{cases} A, & \text{if } n+s \text{ is even}, \\ (p-1)p^{n-1}, & \text{otherwise}, \end{cases}$$

where $A = (p-1)(p^{n-1} - \epsilon \eta_0(-1)\sqrt{p^*}^{n+s-2})$.

The following lemma can be directly derived from [14, Lemma 16].

Lemma 5: Let $f \in$ *WRP*. For $\beta \in \mathbb{F}_{p^n}^\star$, describe

$$\mathcal{N}_{f,\beta} = \#\{x \in \mathbb{F}_{p^n} : f(x) \neq 0 \text{ and } \mathrm{Tr}^n(\beta x) = 0\}.$$

Then for all $\beta \in \mathbb{F}_{p^n}^\star \setminus \mathcal{S}_f$, we have

$$\mathcal{N}_{f,\beta} = \begin{cases} (p-1)(p^{n-2} - \epsilon \sqrt{p^*}^{n+s-4}), & \text{if } n+s \text{ is even}, \\ (p-1)p^{n-2}, & \text{otherwise}. \end{cases}$$

For all $\beta \in \mathcal{S}_f$,

$$\mathcal{N}_{f,\beta} = \begin{cases} (p-1)(p^{n-2} - \epsilon\eta_0(-1)\sqrt{p^*}^{n+s-2}), & \text{if } g(\beta) = 0, \\ (p-1)p^{n-2}, & \text{if } g(\beta) \neq 0, \end{cases}$$

when $n+s$ is even; otherwise,

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

These lemmas help to find the Hamming weights of the codewords of $\mathcal{C}_{D_f}$, whose weight distribution follows from Lemmas 1 and 3. We collect its parameters in the following theorems.

Theorem 1: Let $f \in$ *WRP* and $\mathcal{C}_{D_f}$ be given in (2). Assume $n+s$ being an even integer. Then, $\mathcal{C}_{D_f}$ is a three-weight linear $[(p-1)(p^{n-1} - \epsilon\eta_0(-1)\sqrt{p^*}^{n+s-2}), n]$ code over $\mathbb{F}_p$. The Hamming weights are listed in Table 1.

Proof: By considering the definition of $\mathcal{C}_{D_f}$, we clearly see that the length of $\mathcal{C}_{D_f}$ is equal to n_f, which is given in Lemma 4. Similarly, the Hamming weight $wt(c_\beta)$ is equal to $n_f - \mathcal{N}_{f,\beta}$ for all $\beta \in \mathbb{F}_{p^n}^\star$, which are derived from Lemmas 4 and 5. We can easily compute them. For all $\beta \in \mathbb{F}_{p^n}^\star \setminus \mathcal{S}_f$, we get $wt(c_\beta) = (p-1)^2(p^{n-2} - \epsilon\sqrt{p^*}^{n+s-4})$, and the number of such codewords c_β follows from Lemma 1. For all $\beta \in \mathcal{S}_f$, we obtain

$$wt(c_\beta) = \begin{cases} (p-1)^2 p^{n-2}, & \text{if } g(\beta) = 0, \\ B, & \text{if } g(\beta) \neq 0, \end{cases}$$

where $B = (p-1)((p-1)p^{n-2} - \epsilon\eta_0(-1)\sqrt{p^*}^{n+s-2})$, and the number of c_β follows from Lemma 3. Finally, its dimension is a direct consequence of its weight distribution, completing the proof. □

Notice that Theorem 1 is a partial extension of [6, Corollaries 3 and 5] for weakly regular plateaued unbalanced functions in characteristic p.

The following remark states a necessary condition on the parameters of Theorem 1.

Remark 1: If $\epsilon\eta_0^{(n+s)/2}(-1) = -1$, then we have the condition $0 \leq s \leq n-4$, and $0 \leq s \leq n-2$ for $n \geq 3$, otherwise.

When the parameters of Theorem 1 fail the condition in Remark 1, $\mathcal{C}_{D_f}$ may be a two-weight code. For example, the following linear code has two-weight.

Example 1: The function $f : \mathbb{F}_{3^4} \to \mathbb{F}_3$ defined as $f(x) = \mathrm{Tr}^4(\zeta^4 x^{92})$ is 2-plateaued in the class *WRP*, where ζ is a primitive element of $\mathbb{F}_{3^4}$. Then, we have $\widehat{\chi_f}(\beta) \in \{0, \epsilon\eta_0^3(-1)3^3\xi_3^{g(\beta)}\}$, where $\epsilon = 1$. Thus, $\mathcal{C}_{D_f}$ is a two-weight $[72, 4, 48]_3$ code with $W_\mathcal{C}(y) = 1 + 72y^{48} + 8y^{54}$, verified by MAGMA.

The case when $n+s$ is odd can be similarly proven.

Theorem 2: Let $f \in$ *WRP* and $\mathcal{C}_{D_f}$ be given in (2). Assume $n+s$ being an odd integer. Then, $\mathcal{C}_{D_f}$ is a three-weight linear $[(p-1)p^{n-1}, n]$ code over $\mathbb{F}_p$. The Hamming weights are tabulated in Table 2.

3.2. Linear codes from weakly regular plateaued balanced functions

In this subsection, we obtain further linear codes by using plateaued balanced functions from the class *WRPB*, introduced in [19]. The class *WRPB* consists of weakly regular p-ary plateaued balanced functions satisfying the following two homogeneous conditions. For a function f,

- $f(0) = 0$ and
- there exists a positive even integer t with $\gcd(t-1, p-1) = 1$ such that $f(ax) = a^t f(x)$ for every $a \in \mathbb{F}_p^\star$ and $x \in \mathbb{F}_{p^n}$.

As a consequence of [19, Lemma 9], we have the following lemma.

Lemma 6: Let $f \in$ *WRPB*. For $\beta \in \mathbb{F}_{p^n}^\star$, describe

$$\mathcal{N}_{f,\beta} = \#\{x \in \mathbb{F}_{p^n} : f(x) \neq 0 \text{ and } \mathrm{Tr}^n(\beta x) = 0\}.$$

Assume $n+s$ being an even integer. Then for all $\beta \in \mathbb{F}_{p^n}^{\star} \setminus \mathcal{S}_f$, we have $\mathcal{N}_{f,\beta} = (p-1)p^{n-2}$, and for all $\beta \in \mathcal{S}_f$

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

Remark 2: When $n+s$ is odd, $\mathcal{N}_{f,\beta}$, defined in Lemma 6, is equal to that of Lemma 5.

Remark 3: If $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is a balanced function, then $n_f = \#D_f = (p-1)p^{n-1}$.

The following theorem collects the parameters of the code $\mathcal{C}_{D_f}$.

Theorem 3: Let $f \in$ *WRPB* and $\mathcal{C}_{D_f}$ be given in (2). Assume $n+s$ being an even integer. Then, $\mathcal{C}_{D_f}$ is a three-weight linear $[(p-1)p^{n-1}, n]$ code over $\mathbb{F}_p$. The Hamming weights are listed in Table 3.

Proof: The length of $\mathcal{C}_{D_f}$ is given in Remark 3. From the definition of $\mathcal{C}_{D_f}$, the Hamming weights are $wt(c_\beta) = n_f - \mathcal{N}_{f,\beta}$, derived from Remark 3 and Lemma 6. For all $\beta \in \mathbb{F}_{p^n}^{\star} \setminus \mathcal{S}_f$, we compute $wt(c_\beta) = (p-1)^2 p^{n-2}$, and the number of such codewords c_β is equal to $p^n - p^{n-s} - 1$ by Lemma 1. For all $\beta \in \mathcal{S}_f$, the Hamming weight of c_β is

$$\begin{cases} (p-1)^2(p^{n-2} + \epsilon\sqrt{p^*}^{n+s-4}), & \text{if } g(\beta)=0, \\ (p-1)((p-1)p^{n-2} - \epsilon\sqrt{p^*}^{n+s-4}), & \text{if } g(\beta)\neq 0, \end{cases}$$

and the number of such codewords c_β follows from Lemma 3. Finally, its dimension is a direct consequence of its weight distribution, completing the proof. □

Notice that Theorem 3 is a partial extension of [6, Corollary 5] for weakly regular plateaued balanced functions in characteristic p.

Remark 4: When $n+s$ is odd, $\mathcal{C}_{D_f}$ has the same parameters given in Theorem 2.

3.3. Punctured codes and subcodes

In this subsection, we present the punctured versions and subcodes for constructed codes.

We first consider a *punctured code* for each code constructed above. The dimension of the punctured code is the same as that of the original code while its length and minimum Hamming distance are smaller than the original ones. So they may be optimal codes, and also they are used to construct the democratic SSS.

The code $\mathcal{C}_{D_f}$ given in (2) can be punctured into a shorter code since the Hamming weights of its nonzero codewords have a common divisor $p-1$. We assume that $f \in$ *WRP*. For all $x \in \mathbb{F}_{p^n}$, $f(x) = 0$ if and only if $f(ax) = 0$, for any $a \in \mathbb{F}_p^{\star}$. We now take a subset $\overline{D}_f$ of the defining set D_f given in (1) such that $\bigcup_{a \in \mathbb{F}_p^{\star}} a\overline{D}_f$ is a partition of D_f,

$$D_f = \mathbb{F}_p^{\star}\overline{D}_f = \{a\bar{d} : a \in \mathbb{F}_p^{\star} \text{ and } \bar{d} \in \overline{D}_f\}, \quad (3)$$

where we have $\frac{\bar{d}_1}{\bar{d}_2} \notin \mathbb{F}_p^{\star}$ for each pair of distinct elements $\bar{d}_1, \bar{d}_2 \in \overline{D}_f$. Clearly, $\#D_f = (p-1)\#\overline{D}_f$. Hence, $\mathcal{C}_{D_f}$ is punctured into a shorter code, $\mathcal{C}_{\overline{D}_f}$, which can be defined as in (2) for the defining set $\overline{D}_f$. Hence, the parameters of Corollaries 1 and 2 are directly obtained from Theorems 1 and 2, respectively.

Corollary 1: The punctured code $\mathcal{C}_{\overline{D}_f}$ of Theorem 1 is a three-weight $[p^{n-1} - \epsilon\eta_0(-1)\sqrt{p^*}^{n+s-2}, n]$ code, whose Hamming weights are documented in Table 4.

Corollary 2: The punctured code $\mathcal{C}_{\overline{D}_f}$ of Theorem 2 is a three-weight $[p^{n-1}, n]$ code, whose Hamming weights are documented in Table 5.

With the same definition above, the punctured code of Theorem 3 can be given as follows.

Corollary 3: The punctured code $\mathcal{C}_{\overline{D}_f}$ of Theorem 3 is a three-weight $[p^{n-1}, n]$ code, whose Hamming weights are listed in Table 6.

We next present subcodes for some constructed codes by limiting an element from finite field to the Walsh support of function. To define a subcode of

$\mathcal{C}_{D_f}$, we are using an element of the Walsh support $\mathcal{S}_f$ with order p^{n-s} for $f \in$ *WRP* and so consider a linear code involving D_f defined as

$$\overline{\mathcal{C}}_{D_f} = \{\mathbf{c}_\beta = (\mathrm{Tr}^n(\beta d_1), \ldots, \mathrm{Tr}^n(\beta d_{n_f})) : \beta \in \mathcal{S}_f\},$$

which has length n_f and dimension at most $n-s$. We collect the parameters of $\overline{\mathcal{C}}_{D_f}$, which are directly derived from the corresponding original code $\mathcal{C}_{D_f}$ in the following corollaries.

Corollary 4: The subcode $\overline{\mathcal{C}}_{D_f}$ of Theorem 1 is a two-weight $[(p-1)(p^{n-1}-\epsilon\eta_0(-1)\sqrt{p^*}^{n+s-2}), n-s]$ code, whose Hamming weights are given in Table 7.

Corollary 5: The subcode $\overline{\mathcal{C}}_{D_f}$ of Theorem 2 is a three-weight $[(p-1)p^{n-1}, n-s]$ code, whose Hamming weights follow from Table 2.

Similarly, subcodes for the punctured codes in Corollaries 1 and 2 can be given as follows.

Corollary 6: The subcode $\overline{\mathcal{C}}_{\overline{D}_f}$ of the punctured code $\mathcal{C}_{\overline{D}_f}$ in Corollary 1 is a two-weight $[p^{n-1} - \epsilon\eta_0(-1)\sqrt{p^*}^{n+s-2}, n-s]$ code, whose Hamming weights are given in Table 8.

Corollary 7: The subcode $\overline{\mathcal{C}}_{\overline{D}_f}$ of the punctured code $\mathcal{C}_{\overline{D}_f}$ in Corollary 2 is a three-weight $[p^{n-1}, n-s]$ code, whose Hamming weights follow from Table 5.

We remark that the dimension of a subcode is smaller than that of the original code while its length and minimum Hamming distance are the same as that of the original code. Hence, the minimum Hamming distance of the dual subcode does not change much while its dimension is greater than that of the original dual code. So, the dual subcodes may be more optimal codes.

We lastly find the minimum Hamming distance of the dual codes. Clearly, the minimum Hamming distance $d^\perp$ of the dual code $\mathcal{C}_{D_f}^\perp$ is greater than 1 because $0 \notin D_f$. We know that $d^\perp$ is equal to 2 if and only if there are two distinct elements $d_i, d_j \in D_f$ and two elements $a_i, a_j \in \mathbb{F}_p^\star$ such that

$$a_i\mathrm{Tr}^n(xd_i) + a_j\mathrm{Tr}^n(xd_j) = 0 \qquad (4)$$

for all $x \in \mathbb{F}_{p^n}$. For $d_i \in D_f$, we have $-d_i \in D_f$ since $f(x) = f(-x)$ for all $x \in \mathbb{F}_{p^n}$. Notice that $d_i \neq -d_i$ since p is an odd prime. For $d_j = -d_i$ and $a_i = a_j = 1$, (4) holds for all $x \in \mathbb{F}_{p^n}$. Hence, we have $d^\perp = 2$ for the dual codes of the codes in Theorems 1, 2, 3 and Corollaries 4, 5.

We also show that the minimum Hamming distance of each dual punctured code is at least 3. To see this, we first recall from (3) that $D_f = \mathbb{F}_p^\star\overline{D}_f$. We know that $d^\perp = 2$ if and only if there are two distinct elements $\bar{d}_i, \bar{d}_j \in \overline{D}_f$ and two elements $a_i, a_j \in \mathbb{F}_p^\star$ such that $\mathrm{Tr}^n(x(a_i\bar{d}_i + a_j\bar{d}_j)) = 0$ for all $x \in \mathbb{F}_{p^n}$; equivalently, $a_i\bar{d}_i + a_j\bar{d}_j = 0$, which contradicts to $\frac{\bar{d}_i}{\bar{d}_j} \notin \mathbb{F}_p^\star$. This says that $d^\perp$ is greater than or equal to 3. Hence, the dual codes of the codes in Corollaries 1, 2, 3, 6 and 7 have minimum Hamming distance at least 3.

We note that the projective two-weight code in Corollary 6 can be employed to obtain strongly regular graphs in [4] and the projective three-weight punctured codes in Corollaries 1, 2, 3 and 7 can be used to obtain association schemes given in [3].

4. Secret sharing schemes

In this section, we first show that all codes constructed in Section 3 are minimal codes, and then introduce the SSS by using the dual codes of our minimal codes.

4.1. Minimal linear codes

We start with the following lemma, which states that all nonzero codewords of the code $\mathcal{C}$ are minimal if their Hamming weights are too close to each other.

Lemma 7: (Ashikhmin-Barg) [1] A linear code $\mathcal{C}$ over $\mathbb{F}_p$ is minimal if

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

where $w_{\min}$ and $w_{\max}$ represent the minimum and maximum weights of nonzero codewords in $\mathcal{C}$, respectively.

Lemma 7 implies that our constructed codes are minimal codes, which are explicitly expressed as follows.

Proposition 1: Let $n+s$ be an even integer with $0 \leq s \leq n-4$ and $f \in$ *WRP*. Then, the code $\mathcal{C}_{D_f}$ in Theorem 1 is minimal code with the following parameters $[(p-1)(p^{n-1} - p^{(n+s-2)/2}), n, (p-1)((p-1)p^{n-2} - p^{(n+s-2)/2})]$ if $\epsilon\eta_0^{(n+s)/2}(-1) = 1$; otherwise, $\left[(p-1)(p^{n-1} + p^{(n+s-2)/2}), n, (p-1)^2 p^{n-2})\right]$.

Proposition 2: Let $n+s$ be an odd integer with $0 \leq s \leq n-3$ and $f \in$ *WRP*. Then, the code $\mathcal{C}_{D_f}$ in Theorem 2 is minimal code with the following parameters $\left[(p-1)p^{n-1}, n, (p-1)((p-1)p^{n-2} - p^{(n+s-3)/2})\right]$.

Proposition 3: Let $n+s$ be an even integer with $1 \leq s \leq n-4$ and $f \in$ *WRPB*. Then, the code $\mathcal{C}_{D_f}$ in Theorem 3 is minimal code with the following parameters $[(p-1)p^{n-1}, n, (p-1)((p-1)p^{n-2} - p^{(n+s-4)/2})]$ if $\epsilon\eta_0^{(n+s)/2}(-1) = 1$; otherwise, $\left[(p-1)p^{n-1}, n, (p-1)^2(p^{n-2} - p^{(n+s-4)/2})\right]$.

Remark 5: The punctured codes and subcodes given in Corollaries 1, 2, 3, 4, 5, 6 and 7 are also minimal codes for almost all cases.

4.2. Secret sharing schemes from the constructed minimal codes

In this subsection, we consider the construction of SSS from linear codes. There are a lot of methods to construct the SSS from linear codes (see [9], [10], [15], [16]). Here we see the one described in [9].

Let $\mathcal{C}$ be a linear $[n,k,d]$ code with a $k \times n$ generator matrix $G = [g_0, g_1, \ldots, g_{n-1}]$. A secret $s \in \mathbb{F}_p$ is shared among n group members as follows. A dealer, one of the group members, chooses a random $u \in \mathbb{F}_{p^k}$ such that $s = ug_0$, and obtains the shares $t = (t_0, \ldots, t_{n-1})$ by getting the codeword corresponding to u as $t = uG$. Each components of t are distributed to group members, and t_i is called the secret shares. The secret can be only recovered by a set of secret shares $(t_{i_1}, \ldots, t_{i_m})$, where g_0 is a linear combination of rows $(g_{i_1}, \ldots, g_{i_m})$ of G. In other words, if there is a codeword in $\mathcal{C}^\perp$ starting by 1 and nonzero at $(i_1, \ldots, i_m)$, then one can recover s easily. Indeed, if one can find the vector $(x_1, \ldots, x_m)$ by solving $\sum_{j=1}^m x_j g_{i_j} = g_0$, then $s = \sum_{j=1}^m x_j t_{i_j}$.

A set of group members is called *minimal access set* if they can recover the secret; however, any of its proper subsets can not. From the discussion above we express that minimal codewords of $\mathcal{C}^\perp$ starting with 1 gives the minimal access sets. And so, the minimum Hamming distance d of $\mathcal{C}$ gives a lower bound on the size of a minimal access set. On the other hand, $d^\perp$ determines the extent of democracy of SSS. It is a well-known fact that $d + d^\perp \leq n+2$. Then there is a tradeoff between the size of a minimal access set and the number of minimal access sets. Indeed, it is hold only for maximum distance separable (MDS) codes. Hence, the SSS from MDS codes are interesting [15].

The dual codes of our minimal codes propose the SSS with high democracy, described in [7, Theorem 12]. As an example, we construct the SSS from the codes given in Theorem 1 and Corollary 2.

Proposition 4: Let $\mathcal{C}_{D_f}$ be the code $[m, n, (p-1)((p-1)p^{n-2} - p^{(n+s-2)/2})]$ in Theorem 1 with $G = [g_0, g_1, \ldots, g_{m-1}]$, where $m = (p-1)(p^{n-1} - p^{(n+s-2)/2})$. Then in SSS based on $\mathcal{C}_{D_f}^\perp$ with $d^\perp = 2$, the number of members is $m-1$ and there are p^{n-1}

minimal access sets.

- A member P_i is in all minimal access sets if g_i, $i \neq 0$, is a multiple of g_0, and P_i is in $(p-1)p^{n-2}$ minimal access sets, otherwise.

Note that some P_i's are in all minimal access sets, and such P_i is called a *dictatorial member*.

Proposition 5: Let $\mathcal{C}_{\overline{D}_f}$ be the code $[p^{n-1}, n]$ in Corollary 2 with $G = [g_0, g_1, \ldots, g_{p^{n-1}-1}]$. Then in SSS based on $\mathcal{C}^{\perp}_{\overline{D}_f}$ with $d^{\perp} \geq 3$, the number of members is equal to $p^{n-1} - 1$ and there are p^{n-1} minimal access sets.

- Every group of t members is involved in $(p-1)^t p^{n-t-1}$ minimal access sets for any fixed $t \leq \min(n-1, d^{\perp} - 2)$.

We remark that each P_i in SSS constructed in Proposition 5 is counted in the same number of minimal access sets, and so this scheme is called *democratic*.

From an application point of view, SSS is practically used in many areas. First of all, it can be used in cryptography for secretly sharing an encryption key [2], [18]. Second, it is used in cloud computing, where the encryption key is secretly shared among servers [22]. Third application is in secure multiparty computation, where computation is based on the secret sharing of all inputs of the corresponding parties [8]. Another application of SSS is decentralized electronic voting systems, where the vote of each party is split into different vote-counters, i.e. sharing secret among vote-counters [17]. One of the very recent application of SSS is in blockchain technology, where data in blockchain is altered by a group having enough number of secret shares [25].

5. Conclusion

The main aim of this paper is to present minimal linear codes with good and flexible parameters. To do this, we constructed some classes of minimal linear codes by using weakly regular plateaued functions in the second generic construction method. We next obtained the SSS with nice access structures from the dual codes of our codes. Such SSS have a number of applications in the industry including cryptography, cloud computing, secure multiparty computation, electronic voting systems and blockchain technology. To the best of our knowledge, the minimal codes constructed in this paper are inequivalent to the previous codes in the literature.

Acknowledgment

The authors would like to thank to Assoc. Prof. Dr. Sedat Akleylek and the anonymous reviewers of the IJISS for their valuable comments, which have enhanced the quality of the paper.

Appendix

The appendix presents in Tables 1-8 the Hamming weights of the codewords and weight distributions of the codes constructed in this paper.

References

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

[2] G. R. Blakley et al. Safeguarding cryptographic keys. In *Proceedings of the national computer conference*, volume 48, pages 313–317, 1979.

[3] A. Calderbank and J. Goethals. Three-weight codes and association schemes. *Philips J. Res*, 39(4-5):143–152, 1984.

[4] R. Calderbank and W. Kantor. The geometry of two-weight codes. *Bulletin of the London Mathematical Society*, 18(2):97–122, 1986.

[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] 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.

[8] O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game. In *Proceedings of the nineteenth annual ACM symposium on Theory of computing*, pages 218–229. ACM, 1987.

[9] 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.

[10] R. J. McEliece and D. V. Sarwate. On sharing secrets and reed-solomon codes. *Communications of the ACM*, 24(9):583–584, 1981.

[11] S. Mesnager, F. Özbudak, and 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.*

[12] 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.

[13] S. Mesnager, A. Sınak, and O. Yayla. Three-weight minimal linear codes and their applications. In *Proceedings of the Second International Workshop on Cryptography and its Applications (2IWCA'19), pages 216-220, 19-20 June 2019, Oran, Algeria*.

[14] S. Mesnager and A. Sınak. Several classes of minimal linear codes with few weights from weakly regular plateaued functions. *IEEE Transaction on Information Theory, DOI: 10.1109/TIT.2019.2956130*, 2019.

[15] J. Pieprzyk and X. Zhang. Ideal secret sharing schemes from mds codes. In *Proc. 5th Int. Conf. Information Security and Cryptology (ICISC 2002)*, pages 269–279, 2002.

[16] A. Renvall and C. Ding. The access structure of some secret-sharing schemes. In *Information Security and Privacy*, pages 67–78. Springer, 1996.

[17] B. Schoenmakers. A simple publicly verifiable secret sharing scheme and its application to electronic voting. In *Annual International Cryptology Conference*, pages 148–164. Springer, 1999.

[18] A. Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.

[19] A. Sınak. Three-weight and four-weight minimal linear codes and their secret sharing schemes. *Submitted to the international journal*, 2019.

[20] 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.

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

[22] C.-N. Yang and J.-B. Lai. Protecting data privacy and security for cloud computing based on secret sharing. In *2013 International Symposium on Biometrics and Security Technologies*, pages 259–266. IEEE, 2013.

[23] Y. Zheng and X.-M. Zhang. Plateaued functions. In *ICICS*, volume 99, pages 284–300. Springer, 1999.

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

[25] G. Zyskind, O. Nathan, et al. Decentralizing privacy: Using blockchain to protect personal data. In *2015 IEEE Security and Privacy Workshops*, pages 180–184. IEEE, 2015.

Table 1
The Hamming weights of $\mathcal{C}_{D_f}$ if $n+s$ is even and $f \in$ *WRP*

Hamming weight w	Multiplicity A_w
0	1
$(p-1)^2(p^{n-2} - \epsilon\sqrt{p^*}^{n+s-4})$	$p^n - p^{n-s}$
$(p-1)^2 p^{n-2}$	$p^{n-s-1} + \epsilon\eta_0^{n+1}(-1)(p-1)\sqrt{p^*}^{n-s-2} - 1$
$(p-1)((p-1)p^{n-2} - \epsilon\eta_0(-1)\sqrt{p^*}^{n+s-2})$	$(p-1)(p^{n-s-1} - \epsilon\eta_0^{n+1}(-1)\sqrt{p^*}^{n-s-2})$

Table 2
The Hamming weights of $\mathcal{C}_{D_f}$ if $n+s$ is odd and $f \in$ *WRP*

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

Table 3
The Hamming weights of $\mathcal{C}_{D_f}$ if $n+s$ is even and $f \in$ *WRPB*

Hamming weight w	Multiplicity A_w
0	1
$(p-1)^2 p^{n-2}$	$p^n - p^{n-s} - 1$
$(p-1)^2(p^{n-2} + \epsilon\sqrt{p^*}^{n+s-4})$	$p^{n-s-1} + \epsilon\eta_0^{n+1}(-1)(p-1)\sqrt{p^*}^{n-s-2}$
$(p-1)((p-1)p^{n-2} - \epsilon\sqrt{p^*}^{n+s-4})$	$(p-1)(p^{n-s-1} - \epsilon\eta_0^{n+1}(-1)\sqrt{p^*}^{n-s-2})$

Table 4
The Hamming weights of punctured code $\mathcal{C}_{\overline{D}_f}$ if $n+s$ is even and $f \in$ *WRP*

Hamming weight w	Multiplicity A_w
0	1
$(p-1)(p^{n-2} - \epsilon\sqrt{p^*}^{n+s-4})$	$p^n - p^{n-s}$
$(p-1)p^{n-2}$	$p^{n-s-1} + \epsilon\eta_0^{n+1}(-1)(p-1)\sqrt{p^*}^{n-s-2} - 1$
$(p-1)p^{n-2} - \epsilon\eta_0(-1)\sqrt{p^*}^{n+s-2}$	$(p-1)(p^{n-s-1} - \epsilon\eta_0^{n+1}(-1)\sqrt{p^*}^{n-s-2})$

Table 5
The Hamming weights of punctured code $\mathcal{C}_{\overline{D}_f}$ if $n+s$ is odd and $f \in$ *WRP*

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

Table 6
The Hamming weights of punctured code $\mathcal{C}_{\overline{D}_f}$ if $n+s$ is even and $f \in$ *WRPB*

Hamming weight w	Multiplicity A_w
0	1
$(p-1)p^{n-2}$	$p^n - p^{n-s} - 1$
$(p-1)(p^{n-2} + \epsilon\sqrt{p^*}^{n+s-4})$	$p^{n-s-1} + \epsilon\eta_0^{n+1}(-1)(p-1)\sqrt{p^*}^{n-s-2}$
$(p-1)p^{n-2} - \epsilon\sqrt{p^*}^{n+s-4}$	$(p-1)(p^{n-s-1} - \epsilon\eta_0^{n+1}(-1)\sqrt{p^*}^{n-s-2})$

Table 7
The Hamming weights of subcode $\overline{\mathcal{C}}_{D_f}$ if $n+s$ is even and $f \in$ *WRP*

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

Table 8
The Hamming weights of subcode $\overline{\mathcal{C}}_{\overline{D}_f}$ if $n+s$ is even and $f \in$ *WRP*

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