Minimal linear codes from weakly regular bent functions

Guangkui Xu*
Department of Mathematics
Huainan Normal University
Huainan, China
xuguangkuiy@163.com

Longjiang Qu†
College of Liberal Arts and Science
National University of Defense Technology
Changsha, China
ljqu_happy@hotmail.com

Gaojun Luo
Department of Mathematics
Nanjing University of Aeronautics and Astronautics
Nanjing, China
gjluo1990@163.com

Abstract

Minimal linear codes have received much attention in the past decades due to their important applications in secret sharing and secure two-party computation, etc. Recently, several classes of minimal linear codes with $w_{\min}/w_{\max} \leq (p-1)/p$ have been discovered, where $w_{\min}$ and $w_{\max}$ respectively denote the minimum and maximum nonzero weights in a code. In this paper, we investigate the minimality of a class of p-ary linear codes and obtain some sufficient conditions for this kind of linear codes to be minimal, which is a generalization of the recent results given by Xu et al. in (Finite Fields and Their Applications, vol. 65, 2020). This allows us to construct two new families of minimal linear codes with $w_{\min}/w_{\max} \leq (p-1)/p$ from weakly regular bent functions. The parameters of minimal linear codes presented in this paper are different from those known in literature.

1 Introduction

Throughout this paper, let p be an odd prime and m a positive integer. Let $\mathbb{F}_q$ denote the finite field with q elements, where $q = p^m$. An $[n, k, d]$ linear code $\mathcal{C}$ over $\mathbb{F}_p$ is a k-dimensional subspace of $\mathbb{F}_p^n$ with minimum Hamming distance d. The weight enumerator of $\mathcal{C}$ of length n is the polynomial $1 + A_1 z + A_2 z^2 + \cdots + A_n z^n$, where A_i is the number of

*First Author is supported by the NNSF of China (Grant No. 11601177) and Program for Innovative Research Team in Huainan Normal University (Grant No. XJTD202008).
†Second Author is supported by the NNSF of China (Grant No. 61722213).

codewords of weight i in $\mathcal{C}$. We generally denote the weight distribution of a linear code $\mathcal{C}$ by the sequence $(1, A_1, A_2, \cdots, A_n)$.

The support of a codeword $\mathbf{c} = (c_1, c_2, \cdots, c_n) \in \mathcal{C}$ is the set of coordinates with a non-zero entry, i.e., $\mathrm{Suppt}(\mathbf{c}) = \{i \in \{1, 2, \cdots, n\} : c_i \neq 0\}$. Clearly, the Hamming weight $\mathrm{wt}(\mathbf{c})$ of a codeword equals $|\mathrm{Suppt}(\mathbf{c})|$. If $\mathrm{Suppt}(\mathbf{c}') \subseteq \mathrm{Suppt}(\mathbf{c})$, we call $\mathbf{c}$ covers $\mathbf{c}'$ and write $\mathbf{c}' \preceq \mathbf{c}$. A codeword $\mathbf{c}$ is called minimal if it only covers the codewords $a\mathbf{c}$ for all $a \in \mathbb{F}_p$. Equivalently, the support of $\mathrm{wt}(\mathbf{c})$ does not contain the support of another linearly independent codeword. A linear code $\mathcal{C}$ is said to be minimal if every nonzero codeword of $\mathcal{C}$ is minimal.

Minimal linear codes play an important role in defining access structures in secret sharing schemes based on linear codes [6, 16]. In addition, they are used to ensure privacy in a protocol for secure two-party computation [4]. Ashikhmin and Barg [1] proved a useful criterion for a linear code to be minimal.

Theorem 1. *[1](Ashikhmin–Barg). A linear code $\mathcal{C}$ over $\mathbb{F}_p$ is minimal if $w_{\min}/w_{\max} > (p-1)/p$.*

Inspired by the works of [7, 8], several different families of optimal and minimal few-weight linear codes have been constructed in [11, 15, 23, 25, 26, 29, 31] by selecting a proper defining set D. In recent years, the notion of trace codes has been extended from finite fields to finite rings and more minimal linear codes with $w_{\min}/w_{\max} > (p-1)/p$ have been constructed in [20, 21, 22]. It should be noted that the condition in Theorem 1 is not necessary. Finding minimal linear codes with $w_{\min}/w_{\max} \leq (p-1)/p$ has been an interesting research topic since Chang and Hyun [5] constructed the first infinite family of minimal binary codes with $w_{\min}/w_{\max} \leq 1/2$. Ding, Heng and Zhou [9, 12] derived a new necessary and sufficient condition for a linear code to be minimal and obtained several classes of minimal linear codes with $w_{\min}/w_{\max} \leq (p-1)/p$. After that, several minimal linear codes with $w_{\min}/w_{\max} \leq (p-1)/p$ were constructed in [2, 14, 19, 27, 30]. In [3, 24], the authors studied the relationship between minimal linear codes and cutting blocking sets and gave some constructions of minimal linear codes not satisfying the Aschikhmin-Barg's condition.

Let U be a subset of $\mathbb{F}_p^s$, and let $g(x, y) = \phi(x) \cdot y$, where $\cdot$ denotes the standard inner product, $x \in \mathbb{F}_p^s$, $y \in \mathbb{F}_p^t$, $\phi(x)$ is an injection from U to $\mathbb{F}_p^t \setminus \{0\}$ and $\phi(x) = \mathbf{0}$ for any $x \in \mathbb{F}_p^s \setminus U$. Recently, Xu, Qu and Cao [28] studied the minimality of the following linear codes

$$\mathcal{C}_U = \{\mathbf{c}_{\alpha,\beta_1,\beta_2} = (\alpha g(x,y) - \beta_1 \cdot x - \beta_2 \cdot y)_{(x,y)\in\mathbb{F}_p^s\times\mathbb{F}_p^t\setminus\{(\mathbf{0},\mathbf{0})\}} : \alpha \in \mathbb{F}_p, \beta_1 \in \mathbb{F}_p^s, \beta_2 \in \mathbb{F}_p^t\}. \tag{1}$$

By selecting the suitable subset U of $\mathbb{F}_p^s$, they obtained two classes of minimal linear codes with $w_{\min}/w_{\max} < (p-1)/p$. Following the work of [28], this paper further study the construction of minimal linear codes not satisfying the Aschikhmin-Barg's condition. First, we give some sufficient conditions for linear codes in (1) to be minimal and determine their weight distributions. As applications, we present new minimal linear codes with $w_{\min}/w_{\max} < (p-1)/p$ from the subset of the preimage of weakly regular bent functions. The determination of the weight distributions of these linear codes are based on the technique in [23] to study the subset of the preimage of weakly regular bent functions.

2 Preliminaries

In this section, we recall the basic notation and some results of weakly regular bent functions.

2.1 Weakly regular bent functions

Let $\mathrm{Tr}_1^m(x) = \sum_{i=0}^{m-1} x^{p^i}$ be the trace function from $\mathbb{F}_q$ to $\mathbb{F}_p$, where $q = p^m$. The Walsh transform of a p-ary function $f(x) : \mathbb{F}_q \to \mathbb{F}_p$ is defined as

$$\widehat{f}(\lambda) = \sum_{x \in \mathbb{F}_q} \zeta_p^{f(x) - \mathrm{Tr}_1^m(\lambda x)}, \lambda \in \mathbb{F}_q,$$

where $\zeta_p = e^{\frac{2\pi\sqrt{-1}}{p}}$ is a primitive p-th root of unity.

The inverse Walsh transform of a p-ary function f is given by

$$\zeta_p^{f(x)} = p^{-m} \sum_{\lambda \in \mathbb{F}_q} \widehat{f}(\lambda) \zeta_p^{\mathrm{Tr}_1^m(\lambda x)}.$$

A p-ary function f from $\mathbb{F}_q$ to $\mathbb{F}_p$ is *bent* if $|\widehat{f}(\lambda)| = p^{m/2}$ for any $\lambda \in \mathbb{F}_{p^m}$. A p-ary bent function $f(x)$ is called *regular* if for each $\lambda \in \mathbb{F}_{p^m}$, $\widehat{f}(\lambda) = p^{m/2}\zeta_p^{f^*(\lambda)}$ for some p-ary function f^* from $\mathbb{F}_{p^m}$ to $\mathbb{F}_p$. A p-ary bent function $f(x)$ is called *weakly regular* if there is a complex u with unit magnitude such that $\widehat{f}(\lambda) = up^{m/2}\omega^{f^*(\lambda)}$. The function $f^*(x)$ is called the dual of $f(x)$. It was shown in [10] that the Walsh transform of a weakly regular bent function satisfies

$$\widehat{f}(\lambda) = \varepsilon \sqrt{p^*}^m \zeta_p^{f^*(\lambda)}, \tag{2}$$

where $\varepsilon = \pm 1$ is called the sign of the Walsh transform of $f(x)$ and $p^* = \left(\frac{-1}{p}\right) p = (-1)^{\frac{p-1}{2}} p$. It is well known that the dual of a weakly regular bent function is also weakly regular bent. All known weakly regular bent functions over $\mathbb{F}_{p^m}$ with odd characteristic p can be found in [23, Table XI].

Let $f(x) \in \mathcal{R}_m$ be the set of weakly regular bent functions in m variables such that $f(0) = 0$ and $f(ax) = a^l f(x)$ for any $a \in \mathbb{F}_p^*$ and $x \in \mathbb{F}_q$ with $\gcd(l-1, p-1) = 1$. From [23], the dual $f^*(x)$ of the weakly bent function $f(x)$ in $\mathcal{R}_m$ also belongs to $\mathcal{R}_m$.

We need the following exponential sums, which are well known.

Lemma 2. *[13] Let η_0 be the quadratic character of $\mathbb{F}_p^*$. Then (i) $\sum_{a \in \mathbb{F}_p^*} \eta_0(a) = 0$; (ii) $\sum_{a \in \mathbb{F}_p^*} \eta_0(a)\zeta_p^a = \sqrt{p^*}$; (iii) $\sum_{a \in \mathbb{F}_p} \zeta_p^{ba^2} = \eta_0(b)\sqrt{p^*}$, for any $b \in \mathbb{F}_p^*$.*

Some well known results on the Galois group of the cyclotomic field $\mathbb{Q}(\zeta_p)$ are used in our proofs, where $\mathbb{Q}$ denotes the rational field. The Galois group of $\mathbb{Q}(\zeta_p)$ over $\mathbb{Q}$ is $\{\sigma_a : a \in \mathrm{GF}(p)^*\}$, where the automorphism σ_a of $\mathbb{Q}(\zeta_p)$ is defined by $\sigma_a(\zeta_p) = \zeta_p^a$. It is clear that $\sigma_a(\zeta_p^b) = \zeta_p^{ab}$ for any $a \in \mathbb{F}_p^*$ and $b \in \mathbb{F}_p$. The cyclotomic filed $\mathbb{Q}(\zeta_p)$ has a unique quadratic subfield $\mathbb{Q}(\sqrt{p^*})$.

By Lemma 2 (ii), we have $\sqrt{p^*} = \sum_{b\in\mathbb{F}_p^*} \eta_0(b)\zeta_p^b$, which implies that

$$\sigma_a(\sqrt{p^*}) = \sum_{b\in\mathbb{F}_p^*} \eta_0(b)\zeta_p^{ab} = \eta_0(a) \sum_{b\in\mathbb{F}_p^*} \eta_0(ab)\zeta_p^{ab} = \eta_0(a)\sqrt{p^*}. \tag{3}$$

2.2 A general construction of linear codes from functions

Let $g(x)$ be a p-ary function such that $g(\mathbf{0}) = 0$ and $g(x) \neq w \cdot x$ for any $w \in \mathbb{F}_p^k$. A general construction of linear codes from g is given by

$$\mathcal{C}_g = \{\mathbf{c}_{\alpha,\lambda} = (\alpha g(x) - \lambda \cdot x)_{x\in\mathbb{F}_p^k\setminus\{\mathbf{0}\}} : \alpha \in \mathbb{F}_p, \lambda \in \mathbb{F}_p^k\}. \tag{4}$$

It is well known that this construction can provide many interesting linear codes [3, 9, 12, 17, 18, 27]. With the automorphism of the cyclotomic field $\mathbb{Q}(\zeta_p)$, the Hamming weights of the codewords of $\mathcal{C}_g$ can be computed as follows.

Lemma 3. *[17] Let $\mathcal{C}_g$ be the linear code defined by (4). Then $\mathcal{C}_g$ is a $[p^k - 1, k + 1]$ code and the Hamming weight of $\mathbf{c}_{\alpha,\lambda}$ is given by*

$$\mathrm{wt}(\mathbf{c}_{\alpha,\lambda}) = \begin{cases} 0, & \text{if } \alpha = 0,\ \lambda = \mathbf{0}; \\ p^k - p^{k-1}, & \text{if } \alpha = 0,\ \lambda \neq \mathbf{0}; \\ p^k - p^{k-1} - \frac{1}{p}\sum_{\omega\in\mathbb{F}_p^*} \sigma_\omega(\sigma_\alpha(\widehat{\chi}_g(\alpha^{-1}\lambda))), & \text{if } \alpha \in \mathbb{F}_p^*,\ \lambda \in \mathbb{F}_p^k. \end{cases}$$

2.3 Exponential sums related to weakly regular bent functions

We now give some exponential sums related to weakly regular bent functions, which play a key role in constructing minimal linear codes with $w_{\min}/w_{\max} < (p-1)/p$. We denote SQ and NSQ by the set of all squares and nonsquares in $\mathbb{F}_p^*$, respectively.

Lemma 4. *[23] Let $f(x) \in \mathcal{R}_m$ with $\widehat{f}(0) = \varepsilon\sqrt{p^*}^m$, and $f^*(x)$ be the dual of $f(x)$, where $\varepsilon = \pm 1$. For $i \in \mathbb{F}_p$, define*

$$D_{f,i} = \{x \in \mathbb{F}_q : f(x) = i\} \text{ and } D_{f^*,i} = \{x \in \mathbb{F}_q : f^*(x) = i\}.$$

(i) If m is even, then

$$|D_{f,i}| = |D_{f^*,i}| = \begin{cases} p^{m-1} + \varepsilon(p-1)\eta_0^{m/2}(-1)p^{(m-2)/2}, & i = 0; \\ p^{m-1} - \varepsilon\eta_0^{m/2}(-1)p^{(m-2)/2}, & i \in \mathbb{F}_p^*. \end{cases}$$

(ii) If m is odd, then

$$|D_{f,i}| = \begin{cases} p^{m-1}, & i = 0; \\ p^{m-1} + \varepsilon\sqrt{p^*}^{m-1}, & i \in SQ; \\ p^{m-1} - \varepsilon\sqrt{p^*}^{m-1}, & i \in NSQ. \end{cases}$$

$$|D_{f^*,i}| = \begin{cases} p^{m-1}, & i = 0; \\ p^{m-1} + \varepsilon\eta_0(-1)\sqrt{p^*}^{m-1}, & i \in SQ; \\ p^{m-1} - \varepsilon\eta_0(-1)\sqrt{p^*}^{m-1}, & i \in NSQ. \end{cases}$$

In what follows, a series of auxiliary results are described, which are used to prove the minimality of linear codes presented in Section 3. For $\lambda \in \mathbb{F}_q^*$ and $j \in \mathbb{F}_p$, we define

$$D_{f,\lambda,j} = \{x \in \mathbb{F}_q : f(x) = 0 \text{ and } \mathrm{Tr}_1^m(\lambda x) = j\}.$$

Lemma 5. *Let $\lambda \in \mathbb{F}_q^*$, $j \in \mathbb{F}_p^*$ and $f(x) \in \mathcal{R}_m$ with $\widehat{f}(0) = \varepsilon\sqrt{p^*}^m$.*
(i) If m is even, then

$$\sum_{z\in\mathbb{F}_p^*}\sum_{y\in\mathbb{F}_p^*}\sum_{x\in\mathbb{F}_q} \zeta_p^{yf(x)-z(\mathrm{Tr}_1^m(\lambda x)-j)} = \begin{cases} -\varepsilon(p-1)\sqrt{p^*}^m, & f^*(\lambda) = 0; \\ \varepsilon\sqrt{p^*}^m, & f^*(\lambda) \neq 0; \end{cases}$$

(ii) If m is odd, then

$$\sum_{z\in\mathbb{F}_p^*}\sum_{y\in\mathbb{F}_p^*}\sum_{x\in\mathbb{F}_q} \zeta_p^{yf(x)-z(\mathrm{Tr}_1^m(\lambda x)-j)} = \begin{cases} 0, & f^*(\lambda) = 0; \\ -\varepsilon(-1)^{(p-1)(m+1)/4}p^{(m+1)/2}, & f^*(\lambda) \in SQ; \\ \varepsilon(-1)^{(p-1)(m+1)/4}p^{(m+1)/2}, & f^*(\lambda) \in NSQ. \end{cases}$$

Proof. The proof is similar to that of Lemma 10 in [23] and is omitted. □

From Lemma 5, and Lemmas 9 and 11 in [23], we have the following results.

Lemma 6. *For $\lambda \in \mathbb{F}_q^*$ and $f(x) \in \mathcal{R}_m$ with $\widehat{f}(0) = \varepsilon\sqrt{p^*}^m$.*
(i) If m is even, then

$$|D_{f,\lambda,0}| = \begin{cases} p^{m-2} + \varepsilon(p-1)\eta_0^{m/2}(-1)p^{(m-2)/2}, & f^*(\lambda) = 0; \\ p^{m-2}, & f^*(\lambda) \neq 0; \end{cases}$$

and

$$|D_{f,\lambda,j}| = \begin{cases} p^{m-2}, & f^*(\lambda) = 0; \\ p^{m-2} + \varepsilon\eta_0^{m/2}(-1)p^{(m-2)/2}, & f^*(\lambda) \neq 0; \end{cases}$$

for $j \in \mathbb{F}_p^*$.
(ii) If m is odd, then

$$|D_{f,\lambda,0}| = \begin{cases} p^{m-2}, & f^*(\lambda) = 0; \\ p^{m-2} + \varepsilon(p-1)(-1)^{(p-1)(m+1)/4}p^{(m-3)/2}, & f^*(\lambda) \in SQ; \\ p^{m-2} - \varepsilon(p-1)(-1)^{(p-1)(m+1)/4}p^{(m-3)/2}, & f^*(\lambda) \in NSQ; \end{cases}$$

and

$$|D_{f,\lambda,j}| = \begin{cases} p^{m-2}, & f^*(\lambda) = 0; \\ p^{m-2} - \varepsilon(-1)^{(p-1)(m+1)/4}p^{(m-3)/2}, & f^*(\lambda) \in SQ; \\ p^{m-2} + \varepsilon(-1)^{(p-1)(m+1)/4}p^{(m-3)/2}, & f^*(\lambda) \in NSQ; \end{cases}$$

for $j \in \mathbb{F}_p^*$.

Remark 7. Evaluating the complete weight enumerator of a given linear code is not an easy task in general. Notice that Lemma 6 can be used to determine the complete weight enumerators of some linear codes presented in [23].

For a subset D of $\mathbb{F}_q$, the character sum $\chi_\lambda(D)$ of D with respect to $\lambda \in \mathbb{F}_q^*$ is defined by $\chi_\lambda(D) = \sum_{x\in D} \zeta_p^{\mathrm{Tr}_1^m(\lambda x)}$.

Lemma 8. *Let $\lambda \in \mathbb{F}_q^*$ and $f(x) \in \mathcal{R}_m$ with $\widehat{f}(0) = \varepsilon\sqrt{p^*}^m$. Let $D_{f,0} = \{x \in \mathbb{F}_q : f(x) = 0\}$.*

(i) If m is even, then

$$\chi_\lambda(D_{f,0}) = \begin{cases} \varepsilon\eta_0^{m/2}(-1)(p-1)p^{(m-2)/2}, & f^*(\lambda) = 0; \\ -\varepsilon\eta_0^{m/2}(-1)p^{(m-2)/2}, & f^*(\lambda) \neq 0. \end{cases}$$

(ii) If m is odd, then

$$\chi_\lambda(D_{f,0}) = \begin{cases} 0, & f^*(\lambda) = 0; \\ \varepsilon(-1)^{(p-1)(m+1)/4}p^{(m-1)/2}, & f^*(\lambda) \in SQ; \\ -\varepsilon(-1)^{(p-1)(m+1)/4}p^{(m-1)/2}, & f^*(\lambda) \in NSQ. \end{cases}$$

Proof. By the definition of $\chi_\lambda(D_{f,0})$, we have

$$\chi_\lambda(D_{f,0}) = \sum_{x\in D} \zeta_p^{\mathrm{Tr}_1^m(\lambda x)} = \sum_{j=0}^{p-1} |D_{f,\lambda,j}|\zeta_p^j.$$

The assertion then follows from the fact that $\sum_{j=0}^{p-1} \zeta_p^j = 0$ and Lemma 6. □

3 Minimal linear codes violating the Ashikhmin-Barg's condition from weakly regular bent functions

In this section, we present two families of p-ary minimal linear codes violating the Ashikhmin-Barg's condition with a generalization of our construction in [28, Theorem 3.1]. We begin with a lemma about the Walsh transform of a function $g(x, y)$ defined over $\mathbb{F}_p^s \times \mathbb{F}_p^t$.

Lemma 9. *Let U be a subset of $\mathbb{F}_p^s$. For $(x, y) \in \mathbb{F}_p^s \times \mathbb{F}_p^t$, define $g(x, y) = \phi(x) \cdot y$, where $\phi(x)$ is a mapping from $\mathbb{F}_p^s$ to $\mathbb{F}_p^t$ such that $\phi(x)$ is an injection from U to $\mathbb{F}_p^t \setminus \{\mathbf{0}\}$ and $\phi(x) = \mathbf{0}$ for any $x \in \mathbb{F}_p^s \setminus U$. For any $(\lambda_1, \lambda_2) \in \mathbb{F}_p^s \times \mathbb{F}_p^t$,*

$$\widehat{g}(\lambda_1, \lambda_2) = \begin{cases} p^t \sum\limits_{x\in\mathbb{F}_p^s\setminus U} \zeta_p^{-\lambda_1\cdot x}, & \text{if } \lambda_2 = \mathbf{0}; \\ p^t\zeta_p^{-\lambda_1\cdot\phi^{-1}(\lambda_2)}, & \text{if } \lambda_2 \in \mathrm{Im}\phi \setminus \{\mathbf{0}\}; \\ 0, & \text{if } \lambda_2 \notin \mathrm{Im}\phi, \end{cases}$$

where $\mathrm{Im}\phi$ *denotes the image of* $\phi(x)$.

Proof. By the definition of Walsh transform, we have

$$\begin{aligned}\widehat{g}(\lambda_1,\lambda_2) &= \sum_{x\in\mathbb{F}_p^s}\sum_{y\in\mathbb{F}_p^t}\zeta_p^{\phi(x)\cdot y-\lambda_1\cdot x-\lambda_2\cdot y} = \sum_{x\in\mathbb{F}_p^s}\zeta_p^{-\lambda_1\cdot x}\sum_{y\in\mathbb{F}_p^t}\zeta_p^{(\phi(x)-\lambda_2)\cdot y}\\ &= \begin{cases} p^t\sum\limits_{x\in\phi^{-1}(\lambda_2)}\zeta_p^{-\lambda_1\cdot x}, & \text{if } \lambda_2\in \mathrm{Im}\phi;\\ 0, & \text{if } \lambda_2\notin \mathrm{Im}\phi.\end{cases}\end{aligned}$$

The desired results follow from the assumption that $\phi(x)$ is an injection from U to $\mathbb{F}_p^t\setminus\{\mathbf{0}\}$ and $\phi(x)=\mathbf{0}$ for any $x\in\mathbb{F}_p^s\setminus U$. □

Now we are going to give a further characterization of the minimality linear code defined in (1).

Theorem 10. *Let $k=s+t$ be a positive integer, where s and t are two positive integers. Let U be a subset of $\mathbb{F}_p^s$ with $\mathbf{0}\in U$. Let $g(x,y)=\phi(x)\cdot y$, where $\phi(x)$ is a mapping from $\mathbb{F}_p^s$ to $\mathbb{F}_p^t$ such that $\phi(x)$ is an injection from U to $\mathbb{F}_p^t\setminus\{\mathbf{0}\}$ and $\phi(x)=\mathbf{0}$ for any $x\in\mathbb{F}_p^s\setminus U$. If the set U satisfies the following three conditions:*

(i) $p-1<|U|<(p-1)p^{s-1}$,

(ii) $|\{x\in U\mid \lambda_1\cdot x\neq 0\}|\geq 2$ *for any* $\lambda_1\in\mathbb{F}_p^s\setminus\{\mathbf{0}\}$,

(iii) $\max_{\lambda_1\in\mathbb{F}_p^s\setminus\{\mathbf{0}\}}|\{x\in U\mid \lambda_1\cdot x=i\}|<(p-1)p^{s-2}$ *for any* $i\in\mathbb{F}_p$,

then the code $\mathcal{C}_U$ defined in (1) is a minimal linear code with $w_{\min}/w_{\max}<(p-1)/p$. Moreover, the Hamming weights of the codewords of $\mathcal{C}_U$ are given in Table 1.

Table 1: The Hamming weights of $\mathcal{C}_U$ in Theorem 10

Weight w	No.of codewords A_w
0	1
$p^{t-1}(p-1)\lvert U\rvert$	$p-1$
$p^k-p^{k-1}-p^{t-1}\sum_{\omega\in\mathbb{F}_p^*}\sigma_\omega(\sum\limits_{x\in\mathbb{F}_p^s\setminus U}\zeta_p^{-\lambda_1\cdot x})$, $\lambda_1\in\mathbb{F}_p^s\setminus\{\mathbf{0}\}$	$(p^s-1)(p-1))$
$p^k-p^{k-1}-p^{t-1}(p-1)$	$(p-1)(\lvert U\rvert+p-1)p^{s-1}$
p^k-p^{k-1}	$p^k-1+p^s(p^t-\lvert U\rvert-1)(p-1)$
$p^k-p^{k-1}+p^{t-1}$	$(p-1)(\lvert U\rvert-1)(p^s-p^{s-1})$

Proof. The minimality of $\mathcal{C}_U$ is proved by using the similar argument given in the proof of [28, Lemma 3.1 and Theorem 3.1].

We now compute the Hamming weights of the codewords of $\mathcal{C}_U$. Clearly, when $\alpha=0$ and $(\lambda_1,\lambda_2)\neq(\mathbf{0},\mathbf{0})$, we have $\mathrm{wt}(\mathbf{c}_{0,\beta_1,\beta_2})=p^k-p^{k-1}$ from Lemma 3.

Below we consider the case of $\alpha\neq 0$. By Lemma 3 again,

$$\mathrm{wt}(\mathbf{c}_{\alpha,\lambda_1,\lambda_2})=p^k-p^{k-1}-\frac{1}{p}\sum_{\omega\in\mathbb{F}_p^*}\sigma_\omega(\sigma_\alpha(\widehat{g}(\alpha^{-1}\lambda_1,\alpha^{-1}\lambda_2))). \tag{5}$$

Case 1: Let $\alpha \neq 0$ and $(\lambda_1, \lambda_2) = (\mathbf{0}, \mathbf{0})$. It is clear that $(\alpha^{-1}\lambda_1, \alpha^{-1}\lambda_2) = (\mathbf{0}, \mathbf{0})$. It follows from Lemma 9 and (5) that

$$\mathrm{wt}(\mathbf{c}_{\alpha,\mathbf{0},\mathbf{0}}) = p^k - p^{k-1} - (p-1)p^{t-1}(p^s - |U|) = p^{t-1}(p-1)|U|.$$

Case 2: Let $\alpha \neq 0$, $\lambda_1 \neq \mathbf{0}$ and $\lambda_2 = \mathbf{0}$. It is clear that $\alpha^{-1}\lambda_1 \neq \mathbf{0}$ and $\alpha^{-1}\lambda_2 = \mathbf{0}$. It follows from Lemma 9 and (5) that

$$\mathrm{wt}(\mathbf{c}_{\alpha,\lambda_1,\mathbf{0}}) = p^k - p^{k-1} - p^{t-1}\sum_{\omega\in\mathbb{F}_p^*}\sigma_\omega\Big(\sum_{x\in\mathbb{F}_p^s\setminus U}\zeta_p^{-\lambda_1\cdot x}\Big).$$

Case 3: Let $\alpha \neq 0$ and $\alpha^{-1}\lambda_2 \in \mathrm{Im}\phi \setminus \{\mathbf{0}\}$. By Lemma 9 and (5), we have

$$\begin{aligned}\mathrm{wt}(\mathbf{c}_{\alpha,\lambda_1,\lambda_2}) &= p^k - p^{k-1} - \frac{1}{p}\sum_{\omega\in\mathbb{F}_p^*}\sigma_\omega(\sigma_\alpha(\widehat{g}(\alpha^{-1}\lambda_1, \alpha^{-1}\lambda_2)))\\ &= p^k - p^{k-1} - p^{t-1}\sum_{\omega\in\mathbb{F}_p^*}\zeta_p^{-\omega\lambda_1\cdot\phi^{-1}(\alpha^{-1}\lambda_2)}.\end{aligned}$$

Note that $\phi(x)$ is a mapping from $\mathbb{F}_p^s$ to $\mathbb{F}_p^t$ such that $\phi(x)$ is an injection from U to $\mathbb{F}_p^t \setminus \{\mathbf{0}\}$.

Subcase 3.1: Let $\phi^{-1}(\alpha^{-1}\lambda_2) = \mathbf{0}$. Then $\mathrm{wt}(\mathbf{c}_{\alpha,\lambda_1,\lambda_2}) = p^k - p^{k-1} - p^{t-1}(p-1)$ for any $\lambda_1 \in \mathbb{F}_p^s$.

Subcase 3.2: Let $\phi^{-1}(\alpha^{-1}\lambda_2) \neq \mathbf{0}$. For a fixed $\phi^{-1}(\alpha^{-1}\lambda_2) \in \mathbb{F}_p^s \setminus \{\mathbf{0}\}$, there exist p^{s-1} elements $\lambda_1 \in \mathbb{F}_p^s$ such that $\lambda_1 \cdot \phi^{-1}(\alpha^{-1}\lambda_2) = 0$ and $(p-1)p^{s-1}$ elements $\lambda_1 \in \mathbb{F}_p^s$ such that $\lambda_1 \cdot \phi^{-1}(\alpha^{-1}\lambda_2) \neq 0$. If $\lambda_1 \cdot \phi^{-1}(\alpha^{-1}\lambda_2) = 0$, then $\mathrm{wt}(\mathbf{c}_{\alpha,\lambda_1,\lambda_2}) = p^k - p^{k-1} - p^{t-1}(p-1)$. If $\lambda_1 \cdot \phi^{-1}(\alpha^{-1}\lambda_2) \neq 0$, then $\mathrm{wt}(\mathbf{c}_{\alpha,\lambda_1,\lambda_2}) = p^k - p^{k-1} + p^{t-1}$.

Case 4: Let $\alpha \neq 0$ and $\alpha^{-1}\lambda_2 \notin \mathrm{Im}\phi$. It follows from Lemma 9 that $\widehat{g}(\alpha^{-1}\lambda_1, \alpha^{-1}\lambda_2) = 0$, which implies that $\mathrm{wt}(\mathbf{c}_{\alpha,\lambda_1,\lambda_2}) = p^k - p^{k-1}$.

Let $w_1 = p^{t-1}(p-1)|U|$ and $w_2 = p^k - p^{k-1}$. It is easily verified that

$$\frac{w_{\min}}{w_{\max}} \leq \frac{w_1}{w_2} = \frac{|U|}{p^s} < \frac{p-1}{p}$$

since $|U| < (p-1)p^{s-1}$. □

Remark 11. When $|U| < (p-1)p^{s-2}$, it is easy to see that the condition $\max_{\lambda_1\in\mathbb{F}_p^s\setminus\{\mathbf{0}\}}|\{x \in U \mid \lambda_1 \cdot x = i\}| < (p-1)p^{s-2}$ always holds for any $i \in \mathbb{F}_p$. Hence, the sufficient conditions for $\mathcal{C}_U$ to be minimal in Theorem 10 generalizes the results of [28, Theorem 3.1]. What's more, with the increase of the cardinality of the set U, it is helpful to improve the minimum distance of $\mathcal{C}_U$ defined by (1).

Remark 12. From Table 1, the parameters of $\mathcal{C}_U$ are closely related to the property of the set U. It is important to find a subset of $\mathbb{F}_p^s$ suitable for constructing of minimal linear codes in Theorem 10.

In what follows, we will use Theorem 10 to construct new minimal linear codes with $w_{\min}/w_{\max} < (p-1)/p$ from weakly regular bent functions.

Let $U = D_{f,0} = \{x \in \mathbb{F}_q : f(x) = 0\}$, where $f(x) \in \mathcal{R}_m$ with $\widehat{f}(0) = \varepsilon\sqrt{p^*}^m$. We consider p-ary function $g(x,y)$ defined over $\mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$ by $g(x,y) = \mathrm{Tr}_1^m(\phi(x)y)$, where $(x,y) \in \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$, $\phi(x)$ is a mapping from $\mathbb{F}_{p^m}$ to $\mathbb{F}_{p^m}$ such that $\phi(x)$ is an injection from U to $\mathbb{F}_{p^m}^*$ and $\phi(x) = 0$ for any $x \in \mathbb{F}_{p^m} \setminus U$. Define a linear code by

$$\mathcal{C}_U = \{\mathbf{c}_{\alpha,\lambda_1,\lambda_2} = (\alpha g(x,y) - \mathrm{Tr}_1^m(\lambda_1 x) - \mathrm{Tr}_1^m(\lambda_2 y))_{(x,y)\in\mathbb{F}_{p^m}\times\mathbb{F}_{p^m}\setminus\{(0,0)\}} : \alpha \in \mathbb{F}_p, \lambda_1 \in \mathbb{F}_{p^m}, \lambda_2 \in \mathbb{F}_{p^m}\}. \quad (6)$$

Theorem 13. *Let m be an even positive integer with $m \geq 4$, and let $f(x) \in \mathcal{R}_m$ with $\widehat{f}(0) = \varepsilon\sqrt{p^*}^m$. Define $U = D_{f,0} = \{x \in \mathbb{F}_q : f(x) = 0\}$. Then $\mathcal{C}_U$ defined by (6) is a $[p^{2m}-1, 2m+1]$ minimal linear code with $w_{\min}/w_{\max} < (p-1)/p$ and its weight distribution is listed in Table 2, where $A = \varepsilon\eta_0^{m/2}(-1)p^{(m-2)/2}$.*

Table 2: The weight distribution of $\mathcal{C}_U$ in Theorem 13

Weight w	No.of codewords A_w
0	1
$p^{m-1}(p-1)(p^{m-1}+(p-1)A)$	$p-1$
$p^{2m}-p^{2m-1}+(p-1)^2p^{m-1}A$	$(p-1)(p^{m-1}+(p-1)A-1)$
$p^{2m}-p^{2m-1}-(p-1)p^{m-1}A$	$(p-1)^2(p^{m-1}-A)$
$p^{2m}-p^{2m-1}-p^{m-1}(p-1)$	$(p-1)p^{m-1}(p^{m-1}+(p-1)A+p-1)$
$p^{2m}-p^{2m-1}$	$p^{2m}-1+p^m(p^m-p^{m-1}-(p-1)A-1)(p-1)$
$p^{2m}-p^{2m-1}+p^{m-1}$	$(p-1)(p^{m-1}+(p-1)A-1)(p^m-p^{m-1})$

Proof. To investigate the minimality of $\mathcal{C}_U$, it is sufficient to show that the set U satisfies three conditions of Theorem 10. It follows from Lemmas 4 and 6 that the set U satisfies Conditions (i), (ii) and (iii) of Theorem 10.

Note that $\sum_{x\in\mathbb{F}_{p^m}} \zeta_p^{\mathrm{Tr}_1^m(-\lambda_1 x)} = 0$ for any $\lambda_1 \in \mathbb{F}_{p^m}^*$. Since $f(x) \in \mathcal{R}_m$, $f^*(-\lambda_1) = f^*(\lambda_1)$ for any $\lambda_1 \in \mathbb{F}_{p^m}^*$. From Lemma 8 (i), we have

$$\sum_{x\in\mathbb{F}_{p^m}\setminus U} \zeta_p^{-\mathrm{Tr}_1^m(\lambda_1 x)} = -\chi_\lambda(D_{f,0}) = \begin{cases} -\varepsilon\eta_0^{m/2}(-1)(p-1)p^{(m-2)/2}, & f^*(\lambda) = 0; \\ \varepsilon\eta_0^{m/2}(-1)p^{(m-2)/2}, & f^*(\lambda) \neq 0. \end{cases}$$

By Table 1, for $\alpha \neq 0$, $\lambda_1 \in \mathbb{F}_{p^m}^*$ and $\lambda_2 = 0$,

$$\begin{aligned} \mathrm{wt}(\mathbf{c}_{\alpha,\lambda_1,\mathbf{0}}) &= p^{2m} - p^{2m-1} - p^{m-1}\sum_{\omega\in\mathbb{F}_p^*} \sigma_\omega\Big(\sum_{x\in\mathbb{F}_{p^m}\setminus U} \zeta_p^{-\lambda_1\cdot x}\Big) \\ &= \begin{cases} p^{2m} - p^{2m-1} + (p-1)^2p^{m-1}\varepsilon\eta_0^{m/2}(-1)p^{(m-2)/2}, & f^*(\lambda) = 0; \\ p^{2m} - p^{2m-1} - (p-1)p^{m-1}\varepsilon\eta_0^{m/2}(-1)p^{(m-2)/2}, & f^*(\lambda) \neq 0. \end{cases} \end{aligned}$$

By Lemma 4 (i), the number of codewords $\mathbf{c}_{\alpha,\lambda_1,\lambda_2}$ with the Hamming weight $p^{2m} - p^{2m-1}+(p-1)^2p^{m-1}\varepsilon\eta_0^{m/2}(-1)p^{(m-2)/2}$ (resp. $p^{2m}-p^{2m-1}-(p-1)p^{m-1}\varepsilon\eta_0^{m/2}(-1)p^{(m-2)/2}$) is equal to $(p-1)(p^{m-1}+(p-1)\varepsilon\eta_0^{m/2}(-1)p^{(m-2)/2}-1)$ (resp. $(p-1)^2(p^{m-1}-\varepsilon\eta_0^{m/2}(-1)p^{(m-2)/2})$).

Then the desired results follow from Theorem 10. □

Example 14. Let $p = 3$, $m = 4$ and $f(x) = \mathrm{Tr}_1^4(\xi x^2)$, where ξ is a generator of $\mathbb{F}_{3^4}^*$. The sign ε of the Walsh transform of $f(x)$ is equal to 1. Then $\mathcal{C}_U$ is a minimal ternary code with parameters [6560,9,1782] and its weight enumerator is $1 + 2z^{1782} + 96z^{4212} + 1890z^{4320} + 14174z^{4374} + 3456z^{4401} + 64z^{4698}$, which is verified by Magma. It is clear that $w_{\min}/w_{\max} = 1782/4698 < 2/3$.

Example 15. Let $p = 3$, $m = 4$ and $f(x) = \mathrm{Tr}_1^4(x^{34} + x^2)$. The sign ε of the Walsh transform of $f(x)$ is equal to -1. Then $\mathcal{C}_U$ is a minimal ternary code with parameters [6560,9,1134] and its weight enumerator is $1 + 2z^{1134} + 40z^{4050} + 1242z^{4320} + 16118z^{4374} + 2160z^{4401} + 120z^{4536}$, which is verified by Magma. It is clear that $w_{\min}/w_{\max} = 1134/4536 < 2/3$.

Theorem 16. *Let m be an odd positive integer with $m \geq 3$, and let $f(x) \in \mathcal{R}_m$ with $\widehat{f}(0) = \varepsilon\sqrt{p^*}^m$. Define $U = D_{f,0} = \{x \in \mathbb{F}_q : f(x) = 0\}$. Then $\mathcal{C}_U$ defined by (6) is a $[p^{2m}-1, 2m+1]$ minimal linear code with $w_{\min}/w_{\max} < (p-1)/p$ and its weight distribution is listed in Table 3, where $B = \varepsilon\eta_0^{(m+1)/2}(-1)p^{(m-1)/2}$.*

Table 3: The weight distribution of $\mathcal{C}_U$ in Theorem 16

Weight w	No.of codewords A_w
0	1
$p^{2m-2}(p-1)$	$p-1$
$p^{2m} - p^{2m-1} + (p-1)p^{m-1}B$	$\frac{(p-1)^2}{2}(p^{m-1} + B)$
$p^{2m} - p^{2m-1} - (p-1)p^{m-1}B$	$\frac{(p-1)^2}{2}(p^{m-1} - B)$
$p^{2m} - p^{2m-1} - p^{m-1}(p-1)$	$(p-1)p^{m-1}(p^{m-1} + p - 1)$
$p^{2m} - p^{2m-1}$	$p^{2m} - 1 + (p-1)(p^{m-1} - 1 + p^m(p^m - p^{m-1} - 1))$
$p^{2m} - p^{2m-1} + p^{m-1}$	$(p-1)(p^{m-1} - 1)(p^m - p^{m-1})$

Proof. From Lemma 8 (ii) and Lemma 4 (ii), the proof is similar to that of Theorem 13 and we omit it here. □

Example 17. Let $p = 3$, $m = 3$ and $f(x) = \mathrm{Tr}_1^3(\xi x^4)$, where ξ is a generator of $\mathbb{F}_{3^3}^*$. The sign ε of the Walsh transform of $f(x)$ is equal to -1. Then $\mathcal{C}_U$ is a minimal ternary code with parameters [728,7,162] and its weight enumerator is $1 + 2z^{162} + 12z^{432} + 198z^{468} + 1662z^{486} + 288z^{495} + 24z^{540}$, which is verified by Magma. It is clear that $w_{\min}/w_{\max} = 162/540 < 2/3$.

Example 18. Let $p = 5$, $m = 3$ and $f(x) = \mathrm{Tr}_1^3(x^2)$. The sign ε of the Walsh transform of $f(x)$ is equal to 1. Then $\mathcal{C}_U$ is a minimal code with parameters [15624,7,2500] and its weight enumerator is $1+4z^{2500}+160z^{12000}+2900z^{12400}+65220z^{12500}+9600z^{12525}+240z^{13000}$, which is verified by Magma. It is clear that $w_{\min}/w_{\max} = 2500/13000 < 4/5$.

Remark 19. It should be noted that the weight distributions of minimal linear codes with $w_{\min}/w_{\max} < (p-1)/p$ presented in this paper are new by comparing with known minimal linear codes with $w_{\min}/w_{\max} < (p-1)/p$ in the literatures [2, 3, 5, 9, 12, 19, 27, 28].

References

[1] A. Ashikhmin, A. Barg, Minimal vectors in linear codes, IEEE Trans. Inform. Theory 44 (5) (1998) 2010–2017.

[2] D. Bartoli, M. Bonini, Minimal linear codes in odd characteristic, IEEE Trans. Inf. Theory 65 (7) (2019) 4152-4155.

[3] M. Bonini, M. Borello, Minimal linear codes arising from blocking sets, arXiv preprint arXiv:1907.04626, 2019.

[4] H. Chabanne, G. Cohen, A. Patey, Towards secure two-party computation from the wire-tap channel, in: Proceedings of ICISC 2013, LNCS, vol. 8565, Springer, Heidelberg, 2014, pp. 34-46.

[5] S. Chang, J. Y. Hyun, Linear codes from simplicial complexes, Des. Codes Cryptogr. 86 (10) (2018) 2167-2181.

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

[7] C. Ding, Linear codes from some 2-designs, IEEE Trans. Inf. Theory 61 (6) (2015) 3265-3275.

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

[9] C. Ding, Z. Heng, Z. Zhou, Minimal binary linear codes, IEEE Trans. Inf. Theory 64 (10) (2018) 6536-6545.

[10] T. Helleseth, A. Kholosha, Monomial and quadratic bent functions over the finite fields of odd characteristic. IEEE Trans. Inf. Theory 52 (5) (2006) 2018-2032.

[11] Z. Heng, Q. Yue, Two classes of two-weight linear codes, Finite Fields Appl. 38 (2016) 72-92.

[12] Z. Heng, C. Ding, Z. Zhou, Minimal linear codes over finite fields, Finite Fields Appl. 54 (2018) 176-196.

[13] R. Lidl, H. Niederreiter, Finite fields, in Encyclopedia of Mathematics, vol. 20. Cambridge, U.K.: Cambridge Univ. Press, 1983.

[14] W. Lu, X. Wu, X. Cao, The parameters of minimal linear codes, arXiv preprint arXiv:1911.07648, 2019.

[15] G. Luo, X. Cao, Five classes of optimal two-weight linear codes, Cryptogr. Commun. 10 (6) (2018) 1119-1135.

[16] J. L. Massey, Minimal codewords and secret sharing, In: Proc. 6th Joint Swedish-Russian Int. Workshop on Info. Theory, 276-279, 1993.

[17] S. Mesnager, Linear codes with few weights from weakly regular bent functions based on a generic construction, Cryptogr. Commun. 9 (1) (2017) 71-84.

[18] S. Mesnager, F. özbudak, A. Sinak, Linear codes from weakly regular plateaued functions and their secret sharing schemes, Des. Codes Cryptogr. 87 (2-3) (2019) 463-480.

[19] S. Mesnager, Y. Qi, H. Ru, C. Tang, Minimal linear codes from characteristic functions, IEEE Trans. on Inform. Theory 2020 doi: 10.1109/TIT.2020.2978387.

[20] M. Shi, Yan Liu, Patrick Solé, Optimal two weight codes from trace codes over $\mathbb{F}_2 + u\mathbb{F}_2$, IEEE Communication Letters 20 (2016) 2346-2349.

[21] M. Shi, Y.Guan, P. Solé, Two New Families of Two-Weight Codes, IEEE Trans. on Inform. Theory 63 (2017) 6240–6246.

[22] M. Shi, Y. Liu, P. Solé, Optimal binary codes from trace codes over a non-chain ring, Discrete Applied Mathematics 219 (2017) 176–181.

[23] C. Tang, N. Li, F. Qi, Z. Zhou, T. Helleseth, Linear codes with two or three weights from weakly regular bent functions, IEEE Trans. Inf. Theory 62 (3) (2016) 1166-1176.

[24] C. Tang, Y. Qiu, Q. Liao, Z.Zhou, Full characterization of minimal linear codes as cutting blocking Sets, 2019, http://arxiv.org/abs/1911.09867v1.

[25] Q. Wang, K. Ding, R. Xue, Binary linear sodes with two weights, IEEE Commun. Lett 19 (7) (2015) 1097-1100.

[26] C. Xiang, Linear codes from a generic construction, Cryptogr. Commun. 8 (4) (2016) 525-539.

[27] G. Xu, L. Qu, Three classes of minimal linear codes over the finite fields of odd characteristic, IEEE Trans. Inf. Theory 65 (11) (2019) 7067-7078.

[28] G. Xu, L. Qu, X. Cao, Minimal linear codes from Maiorana-McFarland functions, Finite Fields Appl. 65 (2020) https://doi.org/10.1016/j.ffa.2020.101688.

[29] S. Yang, Z. Yao, Complete weight enumerators of a family of three-weight linear codes, Des. Codes Cryptogr. 82 (3) (2017) 663-674.

[30] W. Zhang, H. Yan, H. Wei, Four families of minimal binary linear codes with $w_{\min}/w_{\max} \leq 1/2$, Appl. Algebra Eng. Commun. Comput. 30 (2) (2019) 175-184.

[31] Z. Zhou, N. Li, C. Fan, T. Helleseth, Linear codes with two or three weights from quadratic bent functions, Des. Codes Cryptogr. 81 (2) (2016) 283-295.