Minimal Linear Codes Constructed from Functions

Xia Wu\(^1\), Wei Lu\(^1\)\(^*\), Xiwang Cao\(^2\)

\(^1\)School of Mathematics, Southeast University, Nanjing 210096, China
\(^2\)Department of Math, Nanjing University of Aeronautics and Astronautics, Nanjing 211100, China

E-mail: wuxia80@seu.edu.cn, luwei1010@seu.edu.cn, xwcao@nuaa.edu.cn

\(^*\)Corresponding author. (Email: luwei1010@seu.edu.cn)

Abstract: In this paper, we consider minimal linear codes in a general construction of linear codes from q-ary functions. First, we give the sufficient and necessary condition for codewords to be minimal. Second, as an application, we present two constructions of minimal linear codes which contained some recent results as special cases.

Index Terms: Linear code, minimal code, q-ary function, secret sharing.

1. Introduction

Let \( q \) be a prime power and \( \mathbb{F}_q \) the finite field with \( q \) elements. Let \( n \) be a positive integer and \( \mathbb{F}_q^n \) the vector space with dimension \( n \) over \( \mathbb{F}_q \). In this paper, all vector spaces are over \( \mathbb{F}_q \) and all vectors are row vectors. For a vector \( \mathbf{v} = (v_1, \ldots, v_n) \in \mathbb{F}_q^n \), let \( \text{Suppt}(\mathbf{v}) := \{1 \leq i \leq n : v_i \neq 0\} \) be the support of \( \mathbf{v} \). For any two vectors \( \mathbf{u}, \mathbf{v} \in \mathbb{F}_q^n \), if \( \text{Suppt}(\mathbf{u}) \subseteq \text{Suppt}(\mathbf{v}) \), we say that \( \mathbf{v} \) covers \( \mathbf{u} \) (or \( \mathbf{u} \) is covered by \( \mathbf{v} \)) and write \( \mathbf{u} \preceq \mathbf{v} \). Clearly, \( a \mathbf{v} \preceq \mathbf{v} \) for all \( a \in \mathbb{F}_q \).

An \( [n, k]_q \) linear code \( \mathcal{C} \) over \( \mathbb{F}_q \) is a \( k \)-dimensional subspace of \( \mathbb{F}_q^n \). Vectors in \( \mathcal{C} \) are called codewords. A codeword \( \mathbf{c} \) in a linear code \( \mathcal{C} \) is called minimal if \( \mathbf{c} \) covers only the codewords \( a \mathbf{c} \) for all \( a \in \mathbb{F}_q \), but no other codewords in \( \mathcal{C} \). That is to say, if a codeword \( \mathbf{c} \) is minimal in \( \mathcal{C} \), then for any codeword \( \mathbf{b} \) in \( \mathcal{C} \), \( \mathbf{b} \preceq \mathbf{c} \) implies that \( \mathbf{b} = a \mathbf{c} \) for some \( a \in \mathbb{F}_q \). For an arbitrary linear code \( \mathcal{C} \), it is hard to determine the set of its minimal codewords.

If every codeword in \( \mathcal{C} \) is minimal, then \( \mathcal{C} \) is said to be a minimal linear code. Minimal linear codes have interesting applications in secret sharing [5, 6, 10, 18, 26] and secure two-party computation [2, 7], and could be decoded with a minimum distance decoding method [1]. Searching for minimal linear codes has been an interesting research topic in coding theory and cryptography.

The Hamming weight of a vector \( \mathbf{v} \) is \( \text{wt}(\mathbf{v}) := |\text{Suppt}(\mathbf{v})| \). In [1], Ashikhmin and Barg gave a sufficient condition on the minimum and maximum nonzero Hamming weights for a linear code to be minimal:

\*Supported by NSFC (Nos. 11971102, 11801070, 11771007)

MSC: 94B05, 94A62
Lemma 1.1. (Ashikhmin-Barg [1]) A linear code $\mathcal{C}$ over $\mathbb{F}_q$ is minimal if
\[ \frac{w_{\text{min}}}{w_{\text{max}}} > \frac{q-1}{q}, \]
where $w_{\text{min}}$ and $w_{\text{max}}$ denote the minimum and maximum nonzero Hamming weights in the code $\mathcal{C}$, respectively.

Inspired by Ding’s work [8, 9], many minimal linear codes with $\frac{w_{\text{min}}}{w_{\text{max}}} > \frac{q-1}{q}$ have been constructed by selecting the proper defining set or from functions over finite fields (see [12, 14, 17, 19, 20, 21, 22, 23, 24, 28]). Cohen et al. [7] provided an example to show that the condition $\frac{w_{\text{min}}}{w_{\text{max}}} > \frac{q-1}{q}$ in Lemma 1.1 is not necessary for a linear code to be minimal. Recently, Ding, Heng and Zhou [11, 13] generalized this sufficient condition and derived a sufficient and necessary condition on all Hamming weights for a given linear code to be minimal:

Lemma 1.2. (Ding-Heng-Zhou[11, 13]) A linear code $\mathcal{C}$ over $\mathbb{F}_q$ is minimal if and only if
\[ \sum_{c \in \mathbb{F}_q^*} \text{wt}(a + cb) \neq (q-1)\text{wt}(a) - \text{wt}(b) \]
for any $\mathbb{F}_q$-linearly independent codewords $a, b \in \mathcal{C}$.

Based on Lemma 1.2, Ding et al. presented three infinite families of minimal binary linear codes with $\frac{w_{\text{min}}}{w_{\text{max}}} \leq \frac{1}{2}$ in [11] and an infinite family of minimal ternary linear codes with $\frac{w_{\text{min}}}{w_{\text{max}}} < \frac{2}{3}$ in [13], respectively. In [27], Zhang et al. constructed four families of minimal binary linear codes with $\frac{w_{\text{min}}}{w_{\text{max}}} \leq \frac{1}{2}$ from Krawtchouk polynomials. Very recently, Bartoli and Bonini [3] provided infinite families of minimal linear codes; also in [25] Xu and Qu constructed three classes of minimal linear codes with $\frac{w_{\text{min}}}{w_{\text{max}}} < \frac{p-1}{p}$ for any odd prime $p$.

Recently, we gave a new sufficient and necessary condition for a given linear code to be minimal in [16]. In this paper, based on our sufficient and necessary condition, we give two constructions of minimal linear codes. Our results generalize the constructions in [11, 13, 3, 4]. These minimal linear codes are constructed from functions as follows. Let $f : \mathbb{F}_q^m \to \mathbb{F}_q$ be a function such that $f(x) \neq \omega \cdot x$ for any $\omega \in \mathbb{F}_q^m$. Let
\[ \mathcal{C}_f = \{ c(u, v) = (uf(x) + v \cdot x)_{x \in \mathbb{F}_q^m \setminus \{0\}} | \ u \in \mathbb{F}_q, v \in \mathbb{F}_q^m \}. \]
Then $\mathcal{C}_f$ is a $[q^m - 1, m + 1]_q$ linear codes. By the choices of the function $f$, many linear codes $\mathcal{C}_f$ can be minimal.

The rest of this paper is organized as follows. In Section 2, we give basic results on linear codes and our new sufficient and necessary condition. In Section 3, we present the new necessary and sufficient conditions for codewords in a general constructions of linear codes from $q$-ary functions to be minimal. In Section 4, we give the first construction of minimal linear code which generalize the constructions in [11, 13, 3]. In Section 5, we give the second
construction of minimal linear code which generalize the construction in [4]. In section 6, we conclude this paper.

2. Preliminaries

2.1. Inner product and dual. Let $k$ be a positive integer. For two vectors $\mathbf{x} = (x_1, x_2, ..., x_k)$, $\mathbf{y} = (y_1, y_2, ..., y_k) \in \mathbb{F}_q^k$, their Euclidean inner product is:

$$\mathbf{x} \cdot \mathbf{y} := \mathbf{x}^T = \sum_{i=1}^{k} x_i y_i,$$

where $T$ denotes the transpose operator.

For any subset $S \subseteq \mathbb{F}_q^k$, we define

$$S^\perp := \{ \mathbf{y} \in \mathbb{F}_q^k \mid \mathbf{y} \cdot \mathbf{x} = 0, \text{for any } \mathbf{x} \in S \}.$$ 

By the definition of $S^\perp$, the following two facts are immediate:

1. $S \subseteq (S^\perp)^\perp$;
2. If $S$ is a linear subspace of $\mathbb{F}_q^k$, then $\dim(S) + \dim(S^\perp) = k$.

2.2. Properties of covering.

**Lemma 2.1.** Let $\mathbf{u} = (u_1, u_n), \mathbf{v} = (v_1, v_n) \in \mathbb{F}_q^n$. Then the following conditions are equivalent:

1. $\mathbf{u} \preceq \mathbf{v}$ (i.e. $\text{Suppt}(\mathbf{u}) \subseteq \text{Suppt}(\mathbf{v})$);
2. for any $1 \leq i \leq n$, if $u_i \neq 0$, then $v_i \neq 0$;
3. for any $1 \leq i \leq n$, if $v_i = 0$, then $u_i = 0$;
4. $\text{Zero}(\mathbf{v}) \subseteq \text{Zero}(\mathbf{u})$, where $\text{Zero}(\mathbf{u}) := \{1 \leq i \leq n : u_i = 0 \} = [1, ..., n] \setminus \text{Suppt}(\mathbf{u})$.

2.3. A new sufficient and necessary condition for $q$-ary linear codes to be minimal.

This new sufficient and necessary condition is presented as a main result in [16], for easier reading, we list the results once more. To present the new sufficient and necessary condition in [16], some concepts are needed.

Let $k \leq n$ be two positive integers and $q$ a prime power. Let $D := \{\mathbf{d}_1, ..., \mathbf{d}_n\}$ be a multiset and $\text{rank}(D) = k$, where $\mathbf{d}_1, ..., \mathbf{d}_n \in \mathbb{F}_q^k$. Let

$$\mathcal{C} = \mathcal{C}(D) = \{\mathbf{c}(\mathbf{x}) = \mathbf{c}(\mathbf{x}; D) = (\mathbf{x}\mathbf{d}_1^T, ..., \mathbf{x}\mathbf{d}_n^T), \mathbf{x} \in \mathbb{F}_q^k \}.$$ 

Then $\mathcal{C}(D)$ is an $[n, k]_q$ linear code. For any $\mathbf{y} \in \mathbb{F}_q^k$, we define

$$H(\mathbf{y}) := \mathbf{y}^\perp = \{ \mathbf{x} \in \mathbb{F}_q^k \mid \mathbf{x}^T = 0 \},$$ 

$$H(\mathbf{y}, D) := D \cap H(\mathbf{y}) = \{ \mathbf{x} \in D \mid \mathbf{x}^T = 0 \},$$ 

$$V(\mathbf{y}, D) := \text{Span}(H(\mathbf{y}, D)).$$ 

It is obvious that $H(\mathbf{y}, D) \subseteq V(\mathbf{y}, D) \subseteq H(\mathbf{y})$. 

3
The following proposition is also needed.

**Proposition 2.1.** For any \( x, y \in \mathbb{F}_q^k \), \( c(x) \preceq c(y) \) if and only if \( H(y, D) \subseteq H(x, D) \).

**Proof.** By the definition of the linear code, we know that

\[
c(x) = (xd_1^T, ..., xd_n^T) \quad \text{and} \quad c(y) = (yd_1^T, ..., yd_n^T).
\]

It is easy to see \( i \in \text{Zero}(c(x)) \) if and only if \( d_i \in H(x, D) \). Similarly, \( i \in \text{Zero}(c(y)) \) if and only if \( d_i \in H(y, D) \). So \( \text{Zero}(c(y)) \subseteq \text{Zero}(c(x)) \) if and only if \( H(y, D) \subseteq H(x, D) \). By **Lemma 2.1**, we know \( \text{Zero}(c(y)) \subseteq \text{Zero}(c(x)) \) if and only if \( c(x) \preceq (c(y)) \), the result is immediate. \( \square \)

Now we give the new sufficient and necessary condition for a codeword \( c(y) \in C(D) \) to be minimal:

**Theorem 2.1.** Let \( y \in \mathbb{F}_q^k \setminus \{0\} \). Then the following three conditions are equivalent:

(1) \( c(y) \) is minimal in \( C(D) \);

(2) \( \dim(V(y, D)) = k - 1 \);

(3) \( V(y, D) = H(y) \).

**Proof.** The equivalence of (2) and (3) is easy. Since \( V(y, D) \subseteq H(y) \) and \( \dim H(y) = k - 1 \), we get \( \dim(V(y, D)) = k - 1 \) if and only if \( V(y, D) = H(y) \).

Next, we prove that (1) and (3) are equivalent.

First, we prove that if \( V(y, D) = H(y) \), then \( c(y) \) is minimal.

Let \( x \in \mathbb{F}_q^k \setminus \{0\} \) and \( c(x) \preceq c(y) \). Then by **Proposition 2.1**, \( H(y, D) \subseteq H(x, D) \) and \( V(y, D) \subseteq V(x, D) \). Moreover, \( H(y) = V(y, D) \subseteq V(x, D) \subseteq H(x) \). Since \( \dim(H(y)) = k - 1 = \dim(H(x)) \), we get \( H(y) = H(x) \). So \( x \in H(x)^\perp = H(y)^\perp = \mathbb{F}_q y \), there exists \( a \in \mathbb{F}_q^* \) such that \( x = ay \) and \( c(x) = ac(y) \). Hence \( c(y) \) is minimal.

Next, we prove that if \( V(y, D) \neq H(y) \), then \( c(y) \) is not minimal.

Since \( V(y, D) \subseteq H(y) \) and \( V(y, D) \neq H(y) \), we get \( \dim(V(y, D)) < \dim(H(y)) = k - 1 \) and \( \dim(V(y, D))^\perp = k - \dim(V(y, D)) \geq 2 \). It follows that there exists \( x \in V(y, D)^\perp \setminus \{0\} \) satisfying \( x, y \) are linearly independent. For any \( d_i \in H(y, D) \subseteq V(y, D) \), since \( x \in V(y, D)^\perp \), we have \( x \cdot d_i = 0 \), and \( d_i \in H(x, D) \). Therefore \( H(y, D) \subseteq H(x, D) \), and by **Proposition 2.1**, we get \( c(x) \preceq c(y) \). Hence, \( c(y) \) is not minimal.

The proof is completed. \( \square \)

By **Theorem 2.1**, we can present a new sufficient and necessary condition for linear codes over \( \mathbb{F}_q \) to be minimal.

**Theorem 2.2.** The following three conditions are equivalent:

(1) \( C(D) \) is minimal ;
(2) for any $y \in \mathbb{F}_q^k \setminus \{0\}$, $\dim V(y, D) = k - 1$;
(3) for any $y \in \mathbb{F}_q^k \setminus \{0\}$, $V(y, D) = H(y)$.

3. The minimal codewords in a general construction of linear code from $q$-ary function

3.1. A general construction of linear code from $q$-ary function. Let $k \geq 2$ be a positive integer and $m := k - 1$. Let $f : \mathbb{F}_q^m \to \mathbb{F}_q$ be a function. Define

$$D = D_f := \{d_x = (f(x), x) : x \in \mathbb{F}_q^m \setminus \{0\}\},$$

and

$$C_f := C(D) = C(D_f) = \{c(u, v) := ((u, v) \cdot d_x)_{x \in \mathbb{F}_q^m \setminus \{0\}} = (uf(x) + v \cdot x)_{x \in \mathbb{F}_q^m \setminus \{0\}} : u \in \mathbb{F}_q, v \in \mathbb{F}_q^m\}.$$  

Let $r(D_f) = \text{rank}(D_f)$. Then $C(D_f)$ is a $[q^m - 1, r(D_f)]_q$ linear code. It is easy to see, $m \leq r(D_f) \leq m + 1$.

**Lemma 3.1.** $r(D_f) = m$ if and only if there exists $\omega \in \mathbb{F}_q^m$, such that $f(x) = \omega \cdot x$.

**Corollary 3.1.** $r(D_f) = m + 1$ if and only if for any given $\omega \in \mathbb{F}_q^m$, $f(x) \neq \omega \cdot x$.

In the rest of this paper, we assume that $f(x) \neq \omega \cdot x$ for any $\omega \in \mathbb{F}_q^m$, and then $C_f$ is a $[q^m - 1, m + 1]_q$ linear code.

3.2. The sufficient and necessary condition for codewords to be minimal. Let $y = (u, v)$, we discuss the following three cases respectively.

**Case 1:** When $u \neq 0$ and $v = 0$, we have the following proposition.

**Proposition 3.1.** When $u \neq 0$ and $v = 0$, then $c(u, v)$ is minimal if and only if there exist $\alpha_1, ..., \alpha_m$ which consists a basis of $\mathbb{F}_q^m$, such that $f(\alpha_1) = ... = f(\alpha_m) = 0$.

**Proof.** For $x \in \mathbb{F}_q^m \setminus \{0\}$,

$$d_x \in H(y, D) \iff uf(x) + v \cdot x = 0 \iff uf(x) = 0 \iff f(x) = 0.$$  

By **Theorem 2.1**, $c(u, v)$ is minimal if and only if there exist $\alpha_1, ..., \alpha_m \in \mathbb{F}_q^m$, such that $f(\alpha_1) = ... = f(\alpha_m) = 0$ and $d_{\alpha_1}, ..., d_{\alpha_m}$ are linearly independent over $\mathbb{F}_q$. It is equivalent to that $\{\alpha_1, ..., \alpha_m\}$ is a basis of $\mathbb{F}_q^m$ and $f(\alpha_1) = ... = f(\alpha_m) = 0$.

**Case 2:** When $u \neq 0$ and $v \neq 0$, we have the following proposition.

**Proposition 3.2.** When $u \neq 0$ and $v \neq 0$, let $\omega = -\frac{1}{u}v$. Then $c(u, v)$ is minimal if and only if there exist $\alpha_1, ..., \alpha_m \in \mathbb{F}_q^m$, such that for $1 \leq i \leq m$, $f(\alpha) = \omega \cdot \alpha$ and $d_{\alpha_1}, ..., d_{\alpha_m}$ are linearly independent over $\mathbb{F}_q$.  

Proof. For $x \in \mathbb{F}_q^m \setminus \{0\}$,

$$d_x \in H(y, D) \iff uf(x) + v \cdot x = 0 \iff f(x) = -\frac{v}{u}x \iff f(x) = \omega \cdot x.$$ 

By Theorem 2.1, $c(u, v)$ is minimal if and only if there exist $\alpha_1, ..., \alpha_m \in \mathbb{F}_q^m$, such that for $1 \leq i \leq m$, $f(\alpha_i) = \omega \cdot \alpha_i$, and $d_{\alpha_1}, ..., d_{\alpha_m}$ are linearly independent over $\mathbb{F}_q$.

\[\square\]

Corollary 3.2. When $u \neq 0$ and $v \neq 0$, if there exists $\{\alpha_1, ..., \alpha_m\}$ which consists a basis of $\mathbb{F}_q^m$, such that $f(\alpha_i) = \omega \cdot \alpha_i$, then $c(u, v)$ is minimal.

Case 3: When $u = 0$ and $v \neq 0$, we have the following proposition.

Proposition 3.3. When $u = 0$ and $v \neq 0$, then $c(u, v)$ is minimal if and only if there exist $\alpha_1, ..., \alpha_m \in H(v)$, such that $d_{\alpha_1}, ..., d_{\alpha_m}$ are linearly independent over $\mathbb{F}_q$.

Proof. For $x \in \mathbb{F}_q^m \setminus \{0\}$,

$$d_x \in H(y, D) \iff uf(x) + v \cdot x = 0 \iff v \cdot x \iff x \in H(v).$$

By Theorem 2.1, $c(u, v)$ is minimal if and only if there exist $\alpha_1, ..., \alpha_m \in H(v)$, such that $d_{\alpha_1}, ..., d_{\alpha_m}$ are linearly independent over $\mathbb{F}_q$.

\[\square\]

4. The first construction of minimal linear codes

To construct the minimal linear codes, we need the following three lemmas.

Lemma 4.1. (1) If $q \geq 3$, then there exists $\{\alpha_1, ..., \alpha_m\}$ which is a basis of $\mathbb{F}_q^m$, such that $\text{wt}(\alpha_i) = m$, $1 \leq i \leq m$;

(2) If $q = 2$ and $m$ is even, then there exists $\{\alpha_1, ..., \alpha_m\}$ which is a basis of $\mathbb{F}_q^m$ such that $\text{wt}(\alpha_i) \geq m - 1$, $1 \leq i \leq m$;

(3) If $q = 2$ and $m$ is odd, then there exists $\{\alpha_1, ..., \alpha_m\}$ which is a basis of $\mathbb{F}_q^m$ such that $\text{wt}(\alpha_i) \geq m - 2$, $1 \leq i \leq m$.

Proof. Let $1 = (1, ..., 1)$ and $A = 1^T1 \in M_{m \times m}(\mathbb{F}_q)$.

(1) For any $b \in \mathbb{F}_q$ we set

$$bE_m - A = \begin{bmatrix} b-1 & -1 & \cdots & -1 \\ -1 & b-1 & \cdots & -1 \\ \vdots & \vdots & \ddots & \vdots \\ -1 & -1 & \cdots & -1 \end{bmatrix} = \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_m \end{bmatrix}.$$

It is easy to see,

$$|bE_m - A| = b^{m-1}(b - m) \in \mathbb{F}_q.$$
When $q > 3$, we can take $b \neq 0, 1, m$, then $\alpha_1, ..., \alpha_m$ are linearly independent over $\mathbb{F}_q$ and $\text{wt}(\alpha_i) = m, 1 \leq i \leq m$.

When $q = 3$ and $m \equiv 0, 1 \pmod{q}$, we can take $b = 2$ in (4.1), the result follows.

When $q = 3$ and $m \equiv 2 \pmod{q}$, we consider the following matrix:

$$2E_m - A - 2e_1^T e_1 = \begin{bmatrix} -1 & -1 & -1 & \ldots & -1 \\ -1 & 1 & -1 & \ldots & -1 \\ -1 & -1 & 1 & \ldots & -1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -1 & -1 & -1 & \ldots & 1 \end{bmatrix} = \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_m \end{bmatrix}. \tag{4.2}$$

It is easy to see

$$|2E_m - A - 2e_1^T e_1| = -2^{m-1} \neq 0.$$ Hence $\alpha_1, ..., \alpha_m$ are linearly independent over $\mathbb{F}_q$ and $\text{wt}(\alpha_i) = m, 1 \leq i \leq m$.

(2) When $q = 2$ and $m$ is even, we set

$$E_m - A = \begin{bmatrix} 0 & -1 & \ldots & -1 \\ -1 & 0 & \ldots & -1 \\ \vdots & \vdots & \ddots & \vdots \\ -1 & -1 & \ldots & 0 \end{bmatrix} = \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_m \end{bmatrix}. \tag{4.3}$$

It is easy to see,

$$|E_m - A| = 1 - m = 1 \neq 0.$$ Then $\alpha_1, ..., \alpha_m$ are linearly independent over $\mathbb{F}_q$ and $\text{wt}(\alpha_i) \geq m - 1, 1 \leq i \leq m$.

(3) When $q = 2$ and $m$ is odd, we set

$$B = \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} \begin{bmatrix} 1 & \ldots & 1 & 0 \\ \end{bmatrix} = \begin{bmatrix} 1 & \ldots & 1 & 0 \\ 1 & \ldots & 1 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 1 & \ldots & 1 & 0 \end{bmatrix}. \tag{4.4}$$

Then

$$E_m - B = \begin{bmatrix} 0 & 1 & \ldots & 1 & 0 \\ 1 & 0 & \ldots & 1 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 1 & \ldots & 1 & 1 \end{bmatrix} = \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_m \end{bmatrix}. \tag{4.5}$$

It is easy to see,

$$|E_m - B| = m = 1 \neq 0.$$ Then $\alpha_1, ..., \alpha_m$ are linearly independent over $\mathbb{F}_q$ and $\text{wt}(\alpha_i) \geq m - 2, 1 \leq i \leq m$.

$\square$

**Lemma 4.2.** For any $\omega \in \mathbb{F}^m_q \setminus \{0\}$, there exists $\{\beta_1, ..., \beta_m\}$ which is a basis of $\mathbb{F}^m_q$, such that $1 \leq \text{wt}(\beta_i) \leq 2$ and $\omega \cdot \beta_i = 1, 1 \leq i \leq m$. 7
Proof. Let $\omega = (w_1, \ldots, w_m)$. Since $\omega \neq 0$, there exists $w_{i_0} \neq 0$. Let

$$\beta_i := \begin{cases} w_{i_0}^{-1}e_{i_0}, & \text{if } i = i_0; \\ e_i + w_{i_0}^{-1}(1 - w_i)e_{i_0}, & \text{if } i \neq i_0. \end{cases}$$

Then $1 \leq \text{wt}(\beta_i) \leq 2$ and $\omega \cdot \beta_i = 1$.

It is easy to see that $\beta_1, \ldots, \beta_m$ are linearly independent and they constitute a basis of $\mathbb{F}_q^m$.

Lemma 4.3. For any $v \in \mathbb{F}_q^n \setminus \{0\}$, there exists $\{\alpha_1, \ldots, \alpha_{m-1}\}$ which is a basis of $H(v)$, such that $1 \leq \text{wt}(\alpha_i) \leq 2$, $1 \leq i \leq m - 1$.

Proof. Let $v = (v_1, \ldots, v_m)$. Since $v \neq 0$, there exists $v_{i_0} \neq 0$. For $i \neq i_0$, let

$$\beta_i = e_i - v_{i_0}^{-1}v_i e_{i_0}.$$ 

Then $\beta_i \in H(v)$ and $1 \leq \text{wt}(\beta_i) \leq 2$. It is easy to see $\{\beta_i : i \neq i_0\}$ are linearly independent. For $1 \leq i \leq m - 1$, let

$$\alpha_i := \begin{cases} \beta_i, & \text{if } i < i_0; \\ \beta_{i+1}, & \text{if } i \geq i_0. \end{cases}$$

Then $\{\alpha_1, \ldots, \alpha_{m-1}\}$ is a basis of $H(v)$ and $1 \leq \text{wt}(\alpha_i) \leq 2$, $1 \leq i \leq m - 1$.

Now we start to construct the minimal linear codes.

Theorem 4.1. Let $q > 2$, $m \geq 3$ and $f : \mathbb{F}_q^m \to \mathbb{F}_q$ be a function. If $f(x)$ satisfies the following two conditions:

1. if $1 \leq \text{wt}(x) \leq 2$, then for any $a \in \mathbb{F}_q^*$, $f(ax) = f(x) \neq 0$;
2. if $\text{wt}(x) = m$, then $f(x) = 0$,

then $C_f = C(D_f)$ is minimal.

Proof. By condition (1) in this theorem, it is easy to see $f(x) \neq \omega \cdot x$ for any $\omega \in \mathbb{F}_q^m$, then by Corollary 3.1, $C_f$ is a $[q^m - 1, m + 1]_q$ linear code.

Case 1: When $u \neq 0$ and $v = 0$, by Lemma 4.1(1), there exists $\{\alpha_1, \ldots, \alpha_m\}$ which is a basis of $\mathbb{F}_q^m$ such that $\text{wt}(\alpha_i) = m$, $1 \leq i \leq m$. By condition (2), we can get $f(\alpha_i) = 0$, $1 \leq i \leq m$. Then by Proposition 3.1, $c(u, v)$ is minimal.

Case 2: When $u \neq 0$ and $v \neq 0$, let $\omega = -\frac{1}{u}v$. By Lemma 4.2, there exist $\{\beta_1, \ldots, \beta_m\}$ which is a basis of $\mathbb{F}_q^m$, such that $1 \leq \text{wt}(\beta_i) \leq 2$ and $\omega \cdot \beta_i = 1$, $1 \leq i \leq m$. Let $\alpha_i = f(\beta_i)\beta_i$. By condition (1), we have $f(\beta_i) \neq 0$, then $1 \leq \text{wt}(\alpha_i) \leq 2$ and $\alpha_1, \ldots, \alpha_m$ is a basis of $\mathbb{F}_q^m$. Thus by condition (1) in this theorem, we have $f(\alpha_i) = f(\beta_i) = f(\beta_i)(\omega \cdot \beta_i) = \omega \cdot (f(\beta_i)\beta_i) = \omega \cdot \alpha_i$. By Corollary 3.2, $c(u, v)$ is minimal.
Case 3: When \( u = 0 \) and \( v \neq 0 \), by Lemma 4.3, there exists \( \{\alpha_1, \ldots, \alpha_{m-1}\} \) which is a basis of \( H(v) \), such that \( 1 \leq \text{wt}(\alpha_i) \leq 2, 1 \leq i \leq m - 1 \). Let \( \alpha_m = a\alpha_1, a \in \mathbb{F}_q \setminus \{0,1\} \). Then \( \alpha_m \in H(v) \). Now we prove that \( d_{\alpha_1}, \ldots, d_{\alpha_m} \) are linearly independent. Let \( \sum^m_{i=1} k_i d_{\alpha_i} = 0 \). It is equivalent to \( (\sum^m_{i=1} k_i f(\alpha_i), \sum^m_{i=1} k_i \alpha_i) = (0, 0) \). We get
\[
0 = \sum^m_{i=1} k_i \alpha_i = \sum^{m-1}_{i=2} k_i \alpha_i + (k_1 + ak_m) \alpha_1.
\]
Since \( \alpha_1, \ldots, \alpha_{m-1} \) are linearly independent, \( k_i = 0, i = 2, \ldots, m - 1 \) and \( k_1 + ak_m = 0 \). Then
\[
0 = \sum^m_{i=1} k_i f(\alpha_i) = k_1 f(\alpha_1) + k_m f(\alpha_m) = k_1 f(\alpha_1) + k_m f(a\alpha_1).
\]
Since \( 1 \leq \text{wt}(\alpha_1) \leq 2 \) and \( a \neq 0 \), by condition (1), we get \( f(a\alpha_1) = f(\alpha_1) \), and then
\[
0 = k_1 f(\alpha_1) + k_m f(\alpha_1) = k_m(1 - a)f(\alpha_1)
\]
Since \( a \neq 1 \) and \( f(\alpha_1) \neq 0 \), we get \( k_m = 0 \) and \( k_1 = 0 \). Thus \( d_{\alpha_1}, \ldots, d_{\alpha_m} \) are linearly independent. By Proposition 3.3, \( c(u, v) \) is minimal.

This completes the proof.

\[\square\]

Theorem 4.2. Let \( q = 2, m \geq 4 \) and \( f : \mathbb{F}_q^m \rightarrow \mathbb{F}_q \) be a function. If \( f(x) \) satisfies the following two conditions:
(1) when \( 1 \leq \text{wt}(x) \leq 2 \), \( f(x) \neq 0 \), i.e. \( f(x) = 1 \);
(2) when \( m \) is even and \( \text{wt}(x) \geq m - 1 \) or when \( m \) is odd and \( \text{wt}(x) \geq m - 2 \), \( f(x) = 0 \), then \( C_f = C(D_f) \) is minimal.

Proof.

Case 1: When \( u \neq 0 \) and \( v = 0 \). If \( m \) is even, by Lemma 4.1(2), there exists \( \{\alpha_1, \ldots, \alpha_m\} \) which is a basis of \( \mathbb{F}_q^m \) satisfy \( \text{wt}(\alpha_i) \geq m - 1, 1 \leq i \leq m \). By condition (2), we can get \( f(\alpha_i) = 0, 1 \leq i \leq m \). Then by Proposition 3.1, \( c(u, v) \) is minimal.

Case 2: When \( u \neq 0 \) and \( v \neq 0 \), let \( \omega = -\frac{1}{u}v \). By Lemma 4.2, there exists \( \{\alpha_1, \ldots, \alpha_m\} \) which is a basis of \( \mathbb{F}_q^m \) such that \( 1 \leq \text{wt}(\alpha_i) \leq 2 \) and \( \omega \cdot \alpha_i = 1, 1 \leq i \leq m \). By condition (1), we have \( f(\alpha_i) = 1 = \omega \cdot \alpha_i, 1 \leq i \leq m \), then by corollary 3.2, \( c(u, v) \) is minimal.

Case 3: When \( u = 0 \) and \( v \neq 0 \). Let \( v = (v_1, \ldots, v_m) \). Then there exists \( \nu_0 \neq 0 \). For \( i \neq i_0 \), let
\[
\alpha_i = e_i - v^{-1}_{i_0} v_i e_{i_0}.
\]
Then \( \{\alpha_i : i \neq i_0\} \) is a basis of \( H(v) \) and \( 1 \leq \text{wt}(\alpha_i) \leq 2 \).

When \( m \) is even, let \( \alpha_{i_0} = \sum_{i \neq i_0} \alpha_i \). Then \( \alpha_{i_0} \in H(v) \) and \( \text{wt}(\alpha_{i_0}) \geq m - 1 \). By condition (2), \( f(\alpha_{i_0}) = 0 \). Now we prove that \( d_{\alpha_1}, \ldots, d_{\alpha_m} \) are linearly independent. Let \( \sum^m_{i=1} k_i d_{\alpha_i} = 0 \).
It is equivalent to \((\sum_{i=1}^{m} k_i f(\alpha_i), \sum_{i=1}^{m} k_i \alpha_i) = (0, 0)\). We get
\[
0 = \sum_{i=1}^{m} k_i \alpha_i = \sum_{i \neq i_0}(k_i + k_{i_0})\alpha_i.
\]
Since \(\{\alpha_i : i \neq i_0\}\) are linearly independent, \(k_i = -k_{i_0} = k_{i_0}\), for \(i \neq i_0\). Since
\[
f(\alpha_i) = \begin{cases} 
0, & \text{if } i = i_0; \\
1, & \text{if } i \neq i_0,
\end{cases}
\]
\[
0 = \sum_{i=1}^{m} k_i f(\alpha_i) = \sum_{i \neq i_0} k_i f(\alpha_i) + k_{i_0} f(\alpha_{i_0}) = (m - 1)k_{i_0} = k_{i_0}.
\]
Thus for all \(i, k_i = k_{i_0} = 0, d_{\alpha_1}, ..., d_{\alpha_m}\) are linearly independent. By Proposition 3.3, \(c(u, v)\) is minimal.

When \(m\) is odd, let \(i_1 \neq i_0\) and \(\alpha_{i_0} = \sum_{i \neq i_0, i_1} \alpha_i\). Then \(\alpha_{i_0} \in H(v)\) and \(\text{wt}(\alpha_{i_0}) \geq m - 2\). By condition (2), \(f(\alpha_{i_0}) = 0\). Now we prove that \(d_{\alpha_1}, ..., d_{\alpha_m}\) are linearly independent. Let
\[
\sum_{i=1}^{m} k_i d_{\alpha_i} = 0,
\]
it is equivalent to \((\sum_{i=1}^{m} k_i f(\alpha_i), \sum_{i=1}^{m} k_i \alpha_i) = (0, 0)\). We get
\[
0 = \sum_{i=1}^{m} k_i \alpha_i = \sum_{i \neq i_0, i_1} (k_i + k_{i_0})\alpha_i + k_{i_1} \alpha_{i_1}.
\]
Since \(\{\alpha_i : i \neq i_0\}\) are linearly independent, for \(i \neq i_1, k_i = -k_{i_0} = k_{i_0}\), and \(k_{i_1} = 0\). Since
\[
f(\alpha_i) = \begin{cases} 
0, & \text{if } i = i_0; \\
1, & \text{if } i \neq i_0,
\end{cases}
\]
\[
0 = \sum_{i=1}^{m} k_i f(\alpha_i) = \sum_{i \neq i_0, i_1} k_i f(\alpha_i) + k_{i_0} f(\alpha_{i_0}) + k_{i_1} f(\alpha_{i_1}) = (m - 2)k_{i_0} = k_{i_0}.
\]
Thus \(k_i = 0, 1 \leq i \leq m, d_{\alpha_1}, ..., d_{\alpha_m}\) are linearly independent. By Proposition 3.3, \(c(u, v)\) is minimal.

This completes the proof.

As the special cases of Theorem 4.1 and 4.2, we have the following corollaries.

**Corollary 4.1.** Let \(m, t\) be integers with \(m \geq 7\) and \(2 \leq t \leq \left\lfloor \frac{m - 3}{2} \right\rfloor\). Assume that \(f : \mathbb{F}_2^m \to \mathbb{F}_2\) is a function defined as follows:
\[
f(x) = \begin{cases} 
1, & 1 \leq \text{wt}(x) \leq t, \\
0, & \text{wt}(x) > t.
\end{cases}
\]
Then \(C_f\) is minimal.

**Remark:** The \(C_f\) in Corollary 4.1 is the one in [11, Theorem 3.1].
Corollary 4.2. Let $m$, $t$ be integers with $m \geq 5$ and $2 \leq t \leq \left\lfloor \frac{m-1}{2} \right\rfloor$. Assume that $f : \mathbb{F}_3^m \rightarrow \mathbb{F}_3$ is a function defined as follows:

$$f(x) = \begin{cases} 1, & \text{if } 1 \leq \text{wt}(x) \leq t, \\ 0, & \text{if } \text{wt}(x) > t. \end{cases}$$

Then $C_f$ is minimal.

Remark: The $C_f$ in Corollary 4.2 is the one in [13, Theorem 18].

Corollary 4.3. Let $m$, $t$ be integers with $m > 3$ and $2 \leq t \leq m - 2$. Assume that $f : \mathbb{F}_q^m \rightarrow \mathbb{F}_q$ is a function defined as follows:

$$f(x) = \begin{cases} a_i \neq 0, & \text{if } \text{wt}(x) = i \leq t, \\ 0, & \text{if } \text{wt}(x) > t. \end{cases}$$

Then $C_f$ is minimal.

Remark: The $C_f$ in Corollary 4.3 is the one in [3, Theorem III 2].

It is easy to see that our constructions contain the above three constructions in [11, 13, 3] as special cases, and our constructions are more general than theirs.

5. The second onstruction of minimal linear codes

Theorem 5.1. Let $f : \mathbb{F}_q^m \rightarrow \mathbb{F}_q$ be a function. If $f(x)$ satisfies the following two conditions:

1. when $1 \leq \text{wt}(x) \leq 2$, $f(x) = 0$;
2. when $\text{wt}(x) \geq m - 1$, then for any $a \in \mathbb{F}_q^*$, $f(ax) = f(x) \neq 0$,

then $C_f = C(D_f)$ is minimal.

Proof. It is easy to see $f(x) \neq \omega \cdot x$ for any $\omega \in \mathbb{F}_q^m$, then by Corollary 3.1, $C_f$ is a $[m-1,m+1]_q$ linear code.

Case 1: By condition (1), we get $f(e_i) = 0, 1 \leq i \leq m$. Then $\{e_1, \ldots, e_m\}$ is a basis of $\mathbb{F}_q^m$ and $f(e_1) = \ldots = f(e_m) = 0$. By Proposition 3.1, $c(u,v)$ is minimal.

Case 2: When $u \neq 0$ and $v \neq 0$, let $\omega = -\frac{1}{u}v = (w_1, \ldots, w_m)$. Then there exists $w_{i_0} \neq 0$. For $i \neq i_0$, let $\alpha_i = e_i - w_i w_{i_0}^{-1} e_{i_0}$. It is easy to see $\{\alpha_i, i \neq i_0\}$ is a basis of $H(\omega), \omega \cdot \alpha_i = 0$ and $1 \leq \text{wt}(\alpha_i) \leq 2$. By condition (1), $f(\alpha_i) = 0 = \omega \cdot \alpha_i$.

Let $\beta_{i_0} = \Sigma_{i \neq i_0} \alpha_i + w_{i_0}^{-1} e_{i_0}$. Then $\omega \cdot \beta_{i_0} = 1$ and $\text{wt}(\beta_{i_0}) \geq m - 1$. By condition (2) of this theorem, we get $f(\beta_{i_0}) \neq 0$. Let $\alpha_{i_0} = f(\beta_{i_0}) \beta_{i_0}$. By condition (2), we get $f(\alpha_{i_0}) = f(f(\beta_{i_0}) \beta_{i_0}) = f(\beta_{i_0}) = f(\beta_{i_0}) (\omega \cdot \beta_{i_0}) = \omega \cdot (f(\beta_{i_0}) \beta_{i_0}) = \omega \cdot \alpha_{i_0}$. It is easy to see $\alpha_1, \ldots, \alpha_m$ are linearly independent. Thus we find that $\{\alpha_1, \ldots, \alpha_m\}$ is a basis of $\mathbb{F}_q^m$, and $f(\alpha_i) = \omega \cdot \alpha_i$. By Corollary 3.2, $c(u,v)$ is minimal.

Case 3: When $u = 0$ and $v \neq 0$, let $v = (v_1, \ldots, v_m)$. Then there exists $v_{i_0} \neq 0$. For $i \neq i_0$, let $\alpha_i = e_i - v_i v_{i_0}^{-1} e_{i_0}$. Then $\{\alpha_i : i \neq i_0\}$ is a basis of $H(v)$ and $1 \leq \text{wt}(\alpha_i) \leq 2$. By
condition (1) of this theorem, we get $f(\alpha_i) = 0$. Let $\alpha_{i_0} = \sum_{i \neq i_0} \alpha_i$. Then $\alpha_{i_0} \in H(v)$ and $\text{wt}(\alpha_{i_0}) \geq m - 1$. By condition(2), we get $f(\alpha_i) \neq 0$. Thus it is easy to see $\alpha_i \in H(v)$, $1 \leq i \leq m$ and $d_{\alpha_1}, ..., d_{\alpha_m}$ are linearly independent. By Proposition 3.3, $c(u,v)$ is minimal.

This completes the proof.

As a special case of Theorem 5.1, we have the following corollary.

**Corollary 5.1.** Let $m$, $t$ be integers with $m > 3$ and $2 \leq t \leq m - 2$. Assume that $f : \mathbb{F}_2^m \rightarrow \mathbb{F}_2$ is a function defined as follows:

$$
f(x) = \begin{cases} 
0, & \text{wt}(x) = i \leq t, \\
1, & \text{wt}(x) > t.
\end{cases}
$$

Then $C_f$ is minimal.

**Remark:** The $C_f$ in Corollary 4.3 is the one in [4, Theorem 3.6].

It is to see, our construction contains [4, Theorem 3.6] as a special case, and our construction is more general.

6. Concluding remarks

In this paper, we first give the sufficient and necessary condition for codewords in a general construction of linear codes from $q$-ary functions to be minimal. Based on this sufficient and necessary condition, we give two constructions of minimal linear codes and we contain the constructions in [11, 13, 3, 4] as special cases. Because of our new sufficient and necessary condition, the choices of $f$ are much flexible, and it is easy to prove that the linear codes we presented are minimal. We expect that based on our sufficient and necessary condition, more minimal linear codes can be constructed from the functions.

**References**

[1] A. Ashikhmin, A. Barg, “Minimal vectors in linear codes,” IEEE Trans. Inf. Theory, vol. 44, no. 5, pp. 2010-2017, sep. 1998.

[2] A. Ashikhmin, A. Barg, G. Cohen, L. Huguet, “Variations on minimal codewords in linear codes,” in: Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, (AAECC-11), (Lecture Notes in Computer Science, vol. 948), G. Cohen, M. Giusti, and T. Mora, Eds. Berlin: Springer-Verlag, pp. 96-105, 1995.

[3] D. Bartoli and M. Bonini, “Minimal linear codes in odd characteristic,” IEEE Trans. Inf. Theory, to be published. doi: 10.1109/TIT.2019.2891992.

[4] S. Mesnager, Y. F. Qi, H. M. Ru, C. M. Tang, Minimal linear codes from characteristic functions, aixiv:1908.01650

[5] C. Carlet, C. Ding, J. Yuan, “Linear codes from highly nonlinear functions and their secret sharing schemes,” IEEE Trans. Inf. Theory, vol. 51, no. 6, pp. 2089-2102, May. 2005.
[6] H. Chabanne, G. Cohen, and A. Patey, “Towards secure two-party computation from the wire-tap channel,” in: Proceedings of ICISC 2013(Lecture Notes in Computer Science, vol. 8565), H.-S. Lee and D.-G. Han Eds. Berlin: Springer-Verlag, pp. 34-46, 2014.
[7] G. D. Cohen, S. Mesnager, A. Patey, “On minimal and quasi-minimal linear codes,” in: Proceedings of IMACC (Lecture Notes in Computer Science, vol. 8308), M. Stam, Eds. Berlin: Springer-Verlag, pp. 85-98, 2003.
[8] C. Ding, “Linear codes from some 2-designs,” IEEE Trans. Inf. Theory, vol. 61, no. 6, pp. 3265-3275, Jun. 2015.
[9] C. Ding, “A construction of binary linear codes from Boolean functions,” Discrete Mathematics, vol. 339, no. 9, pp. 2288-2303, Sep. 2016.
[10] C. Ding and J. Yuan, “Covering and secret sharing with linear codes,” in Discrete Mathematics and Theoretical Computer Science (Lecture Notes in Computer Science), vol. 2731, Springer-Verlag, pp. 11-25, 2003.
[11] C. Ding, Z. Heng, and Z. Zhou, “Minimal binary linear codes,” IEEE Trans. Inf. Theory, vol. 64, no. 10, pp. 6536 - 6545, Oct. 2018.
[12] K. Ding and C. Ding, “A class of two-weight and three-weight codes and their applications in secret sharing,” IEEE Trans. Inf. Theory, vol. 61, no. 11, pp. 5835-5842, Nov. 2015.
[13] Z. Heng, C. Ding, and Z. Zhou, “Minimal linear codes over finite fields,” Finite Fields Appl., vol. 54, pp. 176-196, Nov. 2018.
[14] Z. Heng and Q. Yue, “Two classes of two-weight linear codes,” Finite Fields Appl., vol. 38, pp. 72-92, Mar. 2016.
[15] X. Li and Q. Yue, “Four classes of minimal binary linear codes with derived from Boolean functions,” Des. Codes Cryptogr., DOI: https://doi.org/10.1007/s10623-019-00682-1.
[16] W. Lu and X. Wu, “The Parameters of Minimal Linear Codes,” arxiv: 1911.07648.
[17] G. Luo, X. Cao, S. Xu, and J. Mi, “Binary linear codes with two or three weights from niho exponents,” Cryptogr. Commun., vol. 10, no. 2, pp. 301-318, Mar. 2018.
[18] J. L. Massey, “Minimal codewords and secret sharing,” in: Proc. 6th Joint Swedish-Russian Workshop on Information Theory (M¨olle, Sweden, 1993), pp. 246-249.
[19] M. Shi, Y. Liu, and Patrick Solé, “Optimal two weight codes from trace codes over $\mathbb{F}_p + u\mathbb{F}_p$,” IEEE Commun. Lett, vol. 20, no. 12, pp. 2346-2349, Dec. 2016.
[20] M. Shi, Y. Guan, and Patrick Solé, “Two new families of two-weight codes,” IEEE Trans. Inf. Theory, vol. 63, no. 10, pp. 6240-6246, Oct. 2017.
[21] C. Tang, N. Li, F. Qi, Z. Zhou, and T. Helleseth, “Linear codes with two or three weights from weakly regular bent functions,” IEEE Trans. Inf. Theory, vol. 62, no. 3, pp. 1166-1176, Mar. 2016.
[22] Q. Wang, K. Ding, and R. Xue, “Binary linear sodes with two weights,” IEEE Commun. Lett, vol. 19, no. 7, pp. 1097-1100, Jul. 2015.
[23] C. Xiang, “Linear codes from a generic construction,” Cryptogr. Commun., vol. 8, no. 4, pp. 525-539, Oct. 2016.
[24] S. Yang and Z. Yao, “Complete weight enumerators of a family of three-weight linear codes,” Des. Codes Cryptogr., vol. 82, no. 3, pp. 663-674, Mar. 2017.
[25] G. K. Xu and L. J. Qu, “Three classes of minimal linear codes over the finite fields of odd characteristic,” IEEE Trans. Inf. Theory, vol. 65, no. 11, pp. 7067-7078, Nov. 2017.
[26] J. Yuan, C. Ding, “Secret sharing schemes from three classes of linear codes,” IEEE Trans. Inf. Theory, vol. 52, no. 1, pp. 206-212, 2006.
[27] W. Zhang, H. Yan, and H. Wei, “Four families of minimal binary linear codes with \( \frac{w_{\text{min}}}{w_{\text{max}}} \leq \frac{1}{2} \),” Appl. Algebra Eng. Comm. Comput., to be published. DOI: https://doi.org/10.1007/s00200

[28] Z. Zhou, N. Li, C. Fan and T. Helleseth, “Linear codes with two or three weights from quadratic bent functions,” Des. Codes Cryptogr., vol. 81, no. 2, pp. 283-295, Nov. 2016.