Minimal Binary Linear Codes

Cunsheng Ding, *Senior Member, IEEE*, Ziling Heng, and Zhengchun Zhou

***Abstract*— In addition to their applications in data communication and storage, linear codes also have nice applications in combinatorics and cryptography. Minimal linear codes, a special type of linear codes, are preferred in secret sharing. In this paper, a necessary and sufficient condition for a binary linear code to be minimal is derived. This condition enables us to obtain three infinite families of minimal binary linear codes with $w_{\min}/w_{\max} \leq 1/2$ from a generic construction, where $w_{\min}$ and $w_{\max}$, respectively, denote the minimum and maximum nonzero weights in a code. The weight distributions of all these minimal binary linear codes are also determined.**

***Index Terms*— Boolean function, linear code, binary code, minimal code, secret sharing.**

I. Introduction

LET q be a prime power. Let n, k, d be positive integers. An $[n, k, d]$ *linear code* $\mathcal{C}$ over GF(q) is a k-dimensional subspace of GF$(q)^n$ with minimum (Hamming) distance d. Let A_i denote the number of codewords with Hamming weight i in a code $\mathcal{C}$ of length n. The *weight enumerator* of $\mathcal{C}$ is defined by $1+A_1z+A_2z^2+\cdots+A_nz^n$. The sequence $(1, A_1, A_2, \cdots, A_n)$ is called the *weight distribution* of the code $\mathcal{C}$. A code $\mathcal{C}$ is said to be a t-weight code if the number of nonzero A_i in the sequence $(A_1, A_2, \cdots, A_n)$ is equal to t.

The support of a vector $v \in$ GF$(q)^n$, denoted by Suppt(v), is defined by

$$\text{Suppt}(v) = \{1 \leq i \leq n : v_i \neq 0\}.$$

The vector v is called the characteristic vector or the incidence vector of the set Suppt(v). A vector $u \in$ GF$(q)^n$ covers a vector $v \in$ GF$(q)^n$ if Suppt(u) contains Suppt(v). We write $v \preceq u$ if v is covered by u, and $v \prec u$ if Suppt(v) is a proper subset of Suppt(u). By definition, the Hamming weight $\mathtt{wt}(v)$ of v satisfies

$$\mathtt{wt}(v) = |\text{Suppt}(v)|. \quad (1)$$

A codeword u in a linear code $\mathcal{C}$ is said to be *minimal* if u covers only the codeword au for all $a \in$ GF(q), but no other codewords in $\mathcal{C}$. A linear code $\mathcal{C}$ is said to be *minimal* if every codeword in $\mathcal{C}$ is minimal.

Minimal linear codes could be decoded with the minimum distance decoding method [1], and have applications in secret sharing and secure two-party computation [5], [9], [10], [14], [17], [20]. Hence, constructing minimal linear codes is an interesting research problem. The following is a sufficient condition for a linear code to be minimal [1].

Lemma 1 (Aschikhmin-Barg): A linear code $\mathcal{C}$ over GF(q) is minimal if $w_{\min}/w_{\max} > (q-1)/q$. Herein and hereafter, $w_{\min}$ and $w_{\max}$ denote the minimum and maximum nonzero Hamming weights in $\mathcal{C}$, respectively.

In the literature many minimal linear codes satisfying the condition $w_{\min}/w_{\max} > (q-1)/q$ have been reported. However, no infinite family of minimal linear codes with $w_{\min}/w_{\max} \leq (q-1)/q$ was found until the recent breakthrough in [8], where an infinite family of such binary codes was discovered. The purpose of this paper is to derive a necessary and sufficient condition for a binary linear code to be minimal. This condition enables us to obtain three infinite families of minimal binary linear codes with $w_{\min}/w_{\max} \leq 1/2$ from a generic construction. To the best of our knowledge, only one infinite family of such minimal linear codes was reported in the literature [8]. As a byproduct, we establish the weight distributions of all the proposed minimal binary linear codes. Our work is inspired by the idea of [8], though our way of proving the minimality of binary linear codes is different.

The rest of paper is organized as follows. In Section II, we introduce basic results on Boolean functions and Krawtchouk polynomials which will be needed in the sequel. In Section III, we present general results about minimal binary linear codes, including a new sufficient and necessary condition for a binary linear code to be minimal. In Section IV, we introduce a general construction of linear codes from Boolean functions and use the Walsh transform of Boolean functions to characterize minimal binary linear codes. In Section V, we present three infinite families of minimal linear codes with $w_{\min}/w_{\max} \leq 1/2$ from some specific Boolean functions using the general construction. Finally, we conclude this paper and make some comments in Section VI.

II. Preliminaries

A. Boolean Functions and Walsh Transforms

A function f from GF$(2)^m$ to GF(2) is called a Boolean function. For a Boolean function f from GF$(2)^m$ to GF(2), its Walsh transform is defined by

$$\hat{f}(w) = \sum_{x \in \mathrm{GF}(2)^m} (-1)^{f(x)+w\cdot x},$$

Manuscript received December 18, 2017; accepted March 15, 2018. Date of publication March 26, 2018; date of current version September 13, 2018. C. Ding was supported by The Hong Kong Grants Council under Project 16300415. Z. Zhou was supported in part by the National Science Foundation of China under Grant 61672028 and in part by the Application Fundamental Research Plan Project of Sichuan Province under Grant 2018JY0046.

C. Ding is with the Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Hong Kong (e-mail: cding@ust.hk).

Z. Heng is with the Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Hong Kong (e-mail: zilingheng@163.com).

Z. Zhou is with the School of Mathematics, Southwest Jiaotong University, Chengdu 610031, China (e-mail: zzc@swjtu.edu.cn).

Communicated by S. Mesnager, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2018.2819196

where $w \in \mathrm{GF}(2)^m$ and $w \cdot x$ is the standard inner product of w and x. Another related Walsh transform of f is defined by

$$\tilde{f}(w) = \sum_{x \in \mathrm{GF}(2)^m} f(x)(-1)^{w \cdot x},$$

where $f(x)$ is viewed as a real-valued function taking on only 0 and 1.

The relation between the two kinds of Walsh spectra is well known and documented below.

Lemma 2: Let $f(x)$ be a Boolean function on $\mathrm{GF}(2)^m$. Then

$$\hat{f}(w) = \begin{cases} 2^m - 2\tilde{f}(\mathbf{0}) & \text{if } w = \mathbf{0}, \\ -2\tilde{f}(w) & \text{if } w \neq \mathbf{0}. \end{cases} \tag{2}$$

The support of a Boolean function $f(x)$ on $\mathrm{GF}(2)^m$ is defined by

$$\mathrm{Suppt}(f) = \{x \in \mathrm{GF}(2)^m : f(x) = 1\}.$$

For simplicity, let $n_f = |\mathrm{Suppt}(f)|$ throughout this paper.

B. Krawtchouk Polynomials and Their Properties

In this section, we introduce Krawchouk polynomials and summarize their properties, which will be needed in subsequent sections. A proof of these results could be found in [15, Ch. 2, Secs. 2 and 7].

Let m be a positive integer, and let x be a variable taking nonnegative values. The Krawtchouk polynomial is defined by

$$P_k(x, m) = \sum_{j=0}^{k} (-1)^j \binom{x}{j}\binom{m-x}{k-j} \tag{3}$$

where $0 \leq k \leq m$. We write $P_k(x) := P_k(x, m)$ for simplicity whenever there is no ambiguity. It is easily seen that

$$(1+z)^{m-x}(1-z)^x = \sum_{k=0}^{m} P_k(x) z^k.$$

Theorem 3: Let $u \in \mathrm{GF}(2)^m$ with Hamming weight $\mathtt{wt}(u) = i$. Then

$$\sum_{\mathtt{wt}(v)=k} (-1)^{u \cdot v} = P_k(i).$$

The next theorem documents further basic properties of the Krawtchouk polynomials.

Theorem 4: Let symbols and notation be as before. Then we have the following.

- $\sum_{k=0}^{m} \binom{m-k}{m-j} P_k(x) = 2^j \binom{m-x}{j}$.
- $P_k(i) = (-1)^i P_{m-k}(i)$, $0 \leq i \leq m$.
- $P_m(k) = (-1)^k$.
- $P_k(1) = \frac{m-2k}{m}\binom{m}{k}$.
- $P_k(0) = \binom{m}{k}$.

Theorem 5: Let symbols and notation be as before. We have

$$P_k(x) = (-1)^k P_k(m-x).$$

An upper bound on the absolute value of Krawtchouk polynomials is presented as follows.

Theorem 6: [6, Lemma 4] Let $1 \leq k \leq \lfloor \frac{m-1}{2} \rfloor$ and $1 \leq i \leq m-1$. Then

$$|P_k(i)| \leq P_k(1).$$

Theorem 7: [6, Lemma 1] Let i, m, k be integers such that $i, m \geq 1$ and $0 \leq k \leq m$. Then

$$\sum_{j=0}^{k} P_j(i, m) = P_k(i-1, m-1).$$

Combining Theorems 4, 5, 6, 7 directly yields the following.

Corollary 8: Let $1 \leq k \leq \lfloor \frac{m-3}{2} \rfloor$ and $2 \leq i \leq m-1$. Then we have the following.

- $\left|\sum_{j=1}^{k} P_j(i)\right| \leq 1 + \frac{m-1-2k}{m-1}\binom{m-1}{k}$.
- $\sum_{j=1}^{k} P_j(1) = \sum_{j=1}^{k} \frac{m-2j}{m}\binom{m}{j}$.
- $\sum_{j=1}^{k} P_j(m) = \sum_{j=1}^{k} (-1)^j \binom{m}{j}$.

III. Minimal Binary Linear Codes

In this section, we will derive some general results on minimal binary linear codes. We first prove the following.

Lemma 9: Let $a \in \mathrm{GF}(2)^n$ and $b \in \mathrm{GF}(2)^n$. Then $a \preceq b$ if and only if

$$\mathtt{wt}(a+b) = \mathtt{wt}(b) - wt(a). \tag{4}$$

Proof: By definition, the symmetric difference of $\mathrm{Suppt}(a)$ and $\mathrm{Suppt}(b)$ is given by

$$\begin{aligned} &\mathrm{Suppt}(a)\Delta\mathrm{Suppt}(b) \\ &\quad = [\mathrm{Suppt}(a) \setminus \mathrm{Suppt}(b)] \cup [\mathrm{Suppt}(b) \setminus \mathrm{Suppt}(a)]. \end{aligned}$$

Note that

$$\mathtt{wt}(a+b) = |\mathrm{Suppt}(a)\Delta\mathrm{Suppt}(b)|.$$

By definition, $a \preceq b$ if and only if

$$\mathrm{Suppt}(a) \subseteq \mathrm{Suppt}(b),$$

which is equivalent to

$$\mathrm{Suppt}(a)\Delta\mathrm{Suppt}(b) = \mathrm{Suppt}(b) \setminus \mathrm{Suppt}(a).$$

The desired conclusion then follows from Equation (1). ■

As a consequence of Lemma 9, we deduce the following.

Theorem 10: Let $\mathcal{C} \subset \mathrm{GF}(2)^n$ be a binary linear code. Then $\mathcal{C}$ is minimal if and only if for each pair of distinct nonzero codewords a and b in $\mathcal{C}$,

$$\mathtt{wt}(a+b) \neq \mathtt{wt}(a) - \mathtt{wt}(b). \tag{5}$$

For two-weight linear codes, we have the following simple but useful result.

Theorem 11: Let $\mathcal{C}$ be a two-weight binary linear code with length n and weights w_1 and w_2, where $0 < w_1 < w_2 < n$. Then the following statements hold.

(1) If $w_2 \neq 2w_1$, then $\mathcal{C}$ is minimal.

(2) If $\mathcal{C}$ is minimal and w_1 is odd, then $w_2 \neq 2w_1$.

Proof: Let a and b be two codewords with weight w_1 and w_2, respectively. Note that $a+b$ is a nonzero codeword of $\mathcal{C}$. Obviously,

$$\mathtt{wt}(a+b) = \mathtt{wt}(a) + \mathtt{wt}(b) - 2|\mathrm{Suppt}(a) \cap \mathrm{Suppt}(b)|. \tag{6}$$

(1) Assume that $w_2 \neq 2w_1$. If $a \prec b$, then

$$|\mathrm{Suppt}(a) \cap \mathrm{Suppt}(b)| = |\mathrm{Suppt}(a)| = \mathtt{wt}(a).$$

It then follows from Equation (6) that

$$\mathtt{wt}(a+b) = \mathtt{wt}(b) - \mathtt{wt}(a) = w_2 - w_1.$$

Clearly, $\mathtt{wt}(a+b) \neq w_2$. Otherwise, $w_1 = 0$. Consequently, $\mathtt{wt}(a+b) = w_1$. We then deduce that $w_2 = 2w_1$, which is contrary to our assumption. Hence every codeword in $\mathcal{C}$ is minimal.

(2) Assume that $\mathcal{C}$ is minimal and w_1 is odd. Since $\mathrm{Suppt}(a) \cap \mathrm{Suppt}(b) \subseteq \mathrm{Suppt}(a)$, by Equation (6), we deduce

$$\mathtt{wt}(a+b) \geq \mathtt{wt}(b) - \mathtt{wt}(a).$$

The equality holds if and only if $a \prec b$. If $w_2 = 2w_1$, then $\mathtt{wt}(a+b) \geq w_1$ which implies $\mathtt{wt}(a+b) = w_1$ or $\mathtt{wt}(a+b) = w_2$. Due to Equation (6) and that w_1 is odd, $\mathtt{wt}(a+b) = w_2$ is impossible. Then $\mathtt{wt}(a+b) = \mathtt{wt}(b) - \mathtt{wt}(a) = w_1$ and $a \prec b$, which is contrary to our assumption. Hence $w_2 \neq 2w_1$. ■

For three-weight codes, we have the following.

Theorem 12: Let $\mathcal{C}$ be a three-weight binary linear code with length n and weights w_1, w_2 and w_3, where $0 < w_1 < w_2 < w_3 < n$. Then $\mathcal{C}$ is minimal provided that

$$w_2 \neq 2w_1, \;\; w_3 \neq 2w_1, \;\; w_3 \neq 2w_2 \text{ and } \;\; w_3 \neq w_2 + w_1. \quad (7)$$

Proof: Suppose that

$$\mathtt{wt}(a+b) + \mathtt{wt}(b) = \mathtt{wt}(a) \quad (8)$$

for two distinct nonzero codewords a and b in $\mathcal{C}$. In this case, $\mathtt{wt}(a) \neq \mathtt{wt}(b)$. Otherwise, $\mathtt{wt}(a+b) = 0$ and consequently, $a = b$, which is contrary to our assumption that $a \neq b$. Note that $\mathtt{wt}(b) \neq 0$ and $\mathtt{wt}(a) \neq 0$. It then follows that $\mathtt{wt}(a+b) < \mathtt{wt}(a)$ and $\mathtt{wt}(b) < \mathtt{wt}(a)$.

By (8), $\mathtt{wt}(a)$ cannot be w_1. If $\mathtt{wt}(a) = w_2$, Then $\mathtt{wt}(a+b) = \mathtt{wt}(b) = w_1$. In this case, $w_2 = 2w_1$, which is contrary to one of the conditions in (7). If $\mathtt{wt}(a) = w_3$, then there are two possibilities. The first case is that $\mathtt{wt}(a+b) = \mathtt{wt}(b)$. In this case, we have either $w_3 = 2w_1$ or $w_3 = 2w_2$, which is contrary to one of the conditions in (7). The second case is that $\mathtt{wt}(a+b) \neq \mathtt{wt}(b)$. In this case, we arrive at the conclusion that $w_3 = w_2 + w_1$, which is contrary to one of the conditions in (7).

Summarizing the conclusions in all the cases above, we see that (8) is impossible. The desired conclusion follows from Theorem 10. ■

Clearly, Lemma 1 for $q = 2$ is a direct consequence of Theorem 10. It has been the tool for proving that a binary linear code is minimal in the literature. However, it will be shown later that the condition $w_{\min}/w_{\max} > 1/2$ is too strong. Some binary codes are indeed minimal, but do not satisfy this condition.

IV. A General Construction of Minimal Binary Linear Codes From Boolean Functions

A. The General Construction of Binary Linear Codes From Boolean Functions

In this section, we introduce a construction of binary codes from Boolean functions, which was considered in [4], [8], [18], and [19]. Though the construction is simple, interesting codes could be obtained.

Let $f(x)$ be a Boolean function from $\mathrm{GF}(2)^m$ to $\mathrm{GF}(2)$ such that $f(\mathbf{0}) = 0$ but $f(b) = 1$ for at least one $b \in \mathrm{GF}(2)^m$. We now define a linear code by

$$\mathcal{C}_f = \left\{ (uf(x) + v \cdot x)_{x \in \mathrm{GF}(2)^m \setminus \{\mathbf{0}\}} : \begin{array}{c} u \in \mathrm{GF}(2) \\ v \in \mathrm{GF}(2)^m \end{array} \right\}. \quad (9)$$

The following theorem should be well known [4], [8], [18], [19]. However, for completeness we will sketch a proof of it.

Theorem 13: The binary code $\mathcal{C}_f$ in (9) has length $2^m - 1$ and dimension $m+1$ if $f(x) \neq w \cdot x$ for all $w \in \mathrm{GF}(2)^m$. In addition, the weight distribution of $\mathcal{C}_f$ is given by the following multiset union:

$$\begin{aligned} &\{2^{m-1} + \tilde{f}(w) : w \in \mathrm{GF}(2)^m \setminus \{\mathbf{0}\}\} \cup \{\tilde{f}(\mathbf{0})\} \cup \\ &\{2^{m-1} : w \in \mathrm{GF}(2)^m \setminus \{\mathbf{0}\}\} \cup \{0\} \\ &\quad = \{(2^m - \hat{f}(w))/2 : w \in \mathrm{GF}(2)^m\} \cup \\ &\qquad \{2^{m-1} : w \in \mathrm{GF}(2)^m \setminus \{\mathbf{0}\}\} \cup \{0\}. \end{aligned}$$

Proof: By Lemma 2,

$$\begin{aligned} \hat{f}(w) &= \sum_{x \in \mathrm{GF}(2)^m} (-1)^{f(x) + w \cdot x} \\ &= \begin{cases} 2^m - 2\tilde{f}(\mathbf{0}) & \text{if } w = \mathbf{0}, \\ -2\tilde{f}(w) & \text{if } w \neq \mathbf{0}. \end{cases} \end{aligned}$$

On the other hand,

$$\begin{aligned} \hat{f}(w) &= \sum_{x \in \mathrm{GF}(2)^m} (-1)^{f(x) + w \cdot x} \\ &= 2^m - 2|\{x \in \mathrm{GF}(2)^m \setminus \{\mathbf{0}\} : f(x) + w \cdot x = 1\}|. \end{aligned}$$

Combining the two equations above and the definition of the Hamming weight of a codeword yields the desired conclusion on the weight distribution. Since f is not a linear function, the dimension of the code $\mathcal{C}_f$ must be $m+1$. ■

Let $f(x)$ be a Boolean function from $\mathrm{GF}(2^m)$ to $\mathrm{GF}(2)$ such that $f(0) = 0$ but $f(b) = 1$ for at least one $b \in \mathrm{GF}(2^m)$. We now define a linear code by

$$\mathcal{C}_f = \left\{ (uf(x) + \mathrm{Tr}(vx))_{x \in \mathrm{GF}(2^m) \setminus \{\mathbf{0}\}} : \begin{array}{c} u \in \mathrm{GF}(2) \\ v \in \mathrm{GF}(2^m) \end{array} \right\}. \quad (10)$$

One can similarly prove the following.

Theorem 14: The binary code $\mathcal{C}_f$ in (10) has length $2^m - 1$ and dimension $m+1$ if $f(x) \neq \mathrm{Tr}(wx)$ for all $w \in \mathrm{GF}(2^m)$. In addition, the weight distribution of $\mathcal{C}_f$ is given by the following multiset union:

$$\begin{aligned} &\{2^{m-1} + \tilde{f}(w) : w \in \mathrm{GF}(2^m)^*\} \cup \{\tilde{f}(\mathbf{0})\} \cup \\ &\{2^{m-1} : w \in \mathrm{GF}(2^m)^*\} \cup \{0\} \\ &\quad = \{(2^m - \hat{f}(w))/2 : w \in \mathrm{GF}(2^m)\} \cup \\ &\qquad \{2^{m-1} : w \in \mathrm{GF}(2^m)^*\} \cup \{0\}. \end{aligned}$$

B. When Are These Codes Minimal?

One main result of this paper is stated in the next theorem.

Theorem 15: Let $\mathcal{C}_f$ be the code of Theorem 13. Then $\mathcal{C}_f$ is minimal if and only if

$$\hat{f}(h) + \hat{f}(\ell) \neq 2^m \quad (11)$$

and

$$\hat{f}(h) - \hat{f}(\ell) \neq 2^m \tag{12}$$

for every pair of distinct vectors h and ℓ in GF$(2)^m$.

Proof: Denote $(\mathrm{GF}(2)^m)^* = \mathrm{GF}(2)^m \backslash \{\mathbf{0}\}$. We define the following linear code

$$\mathcal{S}_m = \{(u \cdot x)_{x \in (\mathrm{GF}(2)^m)^*} : u \in \mathrm{GF}(2)^m\}.$$

This code is the Simplex code with parameters $[2^m - 1, m, 2^{m-1}]$. Clearly, every nonzero codeword in $\mathcal{S}_m$ has weight 2^{m-1}.

Let the vector $\mathbf{f}$ be defined as

$$\mathbf{f} = (f(x))_{x \in (\mathrm{GF}(2)^m)^*}.$$

By definition, every codeword a in $\mathcal{C}_f$ can be expressed as

$$a = u_a \mathbf{f} + s_a,$$

where $u_a \in \{0, 1\}$ and s_a is a codeword in $\mathcal{S}_m$. We next consider the coverage of codewords in C_f by distinguishing the following cases.

Case I: Let a and b be two distinct nonzero codewords in $\mathcal{S}_m$. Since $\mathtt{wt}(a) = \mathtt{wt}(b) = 2^{m-1}$. Consequently, one cannot cover the other.

Case II: Let $a = \mathbf{f} + s_a$ and $b = \mathbf{f} + s_b$, where s_a and s_b are two distinct codewords in $\mathcal{S}_m$. Note that $a + b = s_a + s_b$ is a nonzero codeword in $\mathcal{S}_m$. It then follows from Lemma 9 that

$$a \preceq b \iff \mathtt{wt}(b) - \mathtt{wt}(a) = 2^{m-1}$$

and

$$b \preceq a \iff \mathtt{wt}(a) - \mathtt{wt}(b) = 2^{m-1}.$$

Case III: Let $a = \mathbf{f} + s_a$ and let b be a nonzero codeword in $\mathcal{S}_m$, where s_a is a codeword in $\mathcal{S}_m$. In this case, $a + b = \mathbf{f} + s_a + b$ which is not a codeword in $\mathcal{S}_m$. It then follows from Lemma 9 that

$$a \preceq b \iff \mathtt{wt}(\mathbf{f} + s_a + b) = 2^{m-1} - \mathtt{wt}(\mathbf{f} + s_a)$$

and

$$b \preceq a \iff \mathtt{wt}(\mathbf{f} + s_a + b) = \mathtt{wt}(\mathbf{f} + s_a) - 2^{m-1}.$$

Combining the discussions in the three cases above and the proof of Theorem 13 proves the desired conclusion. ■

V. Three Families of Minimal Binary Linear Codes From the Generic Construction

In this section, we shall present three families of minimal binary linear codes with $w_{\min}/w_{\max} \leq 1/2$ from some specific Boolean functions using the general construction documented above.

A. The First Family of Minimal Binary Linear Codes

In this subsection, we assume that m is a positive even integer with $m \geq 6$ and we let $t = \frac{m}{2}$. A partial spread of order s (an s-spread) in GF$(2)^m$ is a set of s t-dimensional subspaces $E_1, E_2, \cdots, E_s$ of GF$(2)^m$ such that $E_i \cap E_j = \{\mathbf{0}\}$ for all $1 \leq i < j \leq s$. Clearly, the order of a partial spread is less than or equal to $2^t + 1$. Let $\{E_1, E_2, \cdots, E_s\}$ be an s-spread in GF$(2)^m$. It is well-known that partial spreads can be used to construct Bent functions [11]. In the sequel, we shall use partial spreads to obtain a class of Boolean functions which can generate a family of minimal binary linear codes with $w_{\min}/w_{\max} \leq 1/2$.

Let $f_i : \mathrm{GF}(2)^m \to \mathrm{GF}(2)$ be the Boolean function with support $E_i \setminus \{\mathbf{0}\}$, i.e.,

$$f_i(x) = \begin{cases} 1, & \text{if } x \in E_i \setminus \{\mathbf{0}\}, \\ 0, & \text{otherwise.} \end{cases}$$

Lemma 16: Let f be the Boolean function over GF$(2)^m$ defined by

$$f = \sum_{i=1}^{s} f_i. \tag{13}$$

Then

$$\hat{f}(w) = \begin{cases} 2^m - 2s(2^t - 1), & 1 \text{ time}, \\ 2s, & (2^t + 1 - s)(2^t - 1) \text{ times}, \\ -2^{t+1} + 2s, & s(2^t - 1) \text{ times}. \end{cases}$$

Proof: It is easily verified from the definitions of f and f_i that

$$\tilde{f}(w) = \begin{cases} s(2^t - 1), \text{ if } w = \mathbf{0}, \\ -s, \text{ if } w \notin E_i^{\perp} \text{ for all } 1 \leq i \leq s, \\ 2^t - s, \text{ if } w \neq \mathbf{0} \text{ and } w \in E_i^{\perp} \text{ for some } 1 \leq i \leq s, \end{cases} \tag{14}$$

where $E_i^{\perp}$ denotes the dual space of E_i. The conclusion then follows from Equations (2) and (14) and the definitions of E_i's. ■

Lemma 17: Let s be any integer with $1 \leq s \leq 2^t + 1$, and f be the Boolean function defined in Equation (13). When $s \notin \{1, 2^t, 2^t + 1\}$, we have

$$\hat{f}(h) + \hat{f}(\ell) \neq 2^m$$

and

$$\hat{f}(h) - \hat{f}(\ell) \neq 2^m$$

for every pair of distinct vectors h and ℓ in GF$(2)^m$.

Proof: The conclusions follow directly from Lemma 16. ■

Theorem 18: Let s be any integer with $1 \leq s \leq 2^t + 1$ and $s \notin \{1, 2^t, 2^t + 1\}$, and f be the Boolean function defined in Equation (13). Then the code $\mathcal{C}_f$ in Equation (9) is a $[2^m - 1, m + 1]$ minimal linear code with the weight distribution in Table I. Furthermore,

$$\frac{w_{\min}}{w_{\max}} \leq \frac{1}{2}$$

provided that $s \leq 2^{t-2}$.

TABLE I
THE WEIGHT DISTRIBUTION OF $\mathcal{C}_f$ IN THEOREM 18

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

Proof: The conclusions follow directly by combining Theorem 13, Lemmas 16 and 17. ■

Remark 19: It can be seen from Table I that the code $\mathcal{C}_f$ in Theorem 18 has at most four weights. It is easy to check that $\mathcal{C}_f$ is a three-weight linear code when $s \in \{2^{t-1}, 2^{t-1}+1\}$, and otherwise a four-weight linear code.

The following numerical data is consistent with the conclusions of Theorem 18.

Example 20: Let $m = 6$ and $s = 2$. Then the set $\mathcal{C}_f$ in Theorem 18 is a minimal code with parameters $[63, 7, 14]$ and weight enumerator

$$1 + z^{14} + 49z^{30} + 63\, z^{32} + 14\, z^{38}.$$

Obviously, $w_{\min}/w_{\max} = 14/38 < 1/2$.

Example 21: Let $m = 8$ and $s = 4$. Then the set $\mathcal{C}_f$ in Theorem 18 is a minimal code with parameters $[255, 9, 60]$ and weight enumerator

$$1 + z^{60} + 195z^{124} + 255\, z^{128} + 60\, z^{140}.$$

Clearly, $w_{\min}/w_{\max} = 60/140 < 1/2$.

B. The Second Family of Minimal Binary Linear Codes

In this section, we propose a family of minimal binary linear codes with $w_{\min}/w_{\max} \le 1/2$ from the Boolean functions belonging to the general Maiorana-McFarland class. Let m be an arbitrary positive integer and s, t be two positive integers such that $s + t = m$. The function in this class has the form

$$f(x, y) = \phi(x) \cdot y + g(x), \tag{15}$$

where $x \in \mathrm{GF}(2)^s$, $y \in \mathrm{GF}(2)^t$, ϕ is an arbitrary mapping from $\mathrm{GF}(2)^s$ to $\mathrm{GF}(2)^t$, and g is an arbitrary Boolean function in s variables. It is known that the construction in (15) has been widely used to generate Boolean functions with interesting cryptographic properties (see [3], [7], [11], and [16] for more details).

For the Boolean function defined by (15), it is easy to verify that

$$\hat{f}(h_1, h_2) = \begin{cases} 2^t \displaystyle\sum_{x \in \phi^{-1}(h_2)} (-1)^{g(x)+h_1\cdot x}, & h_2 \in \mathrm{Im}\phi, \\ 0, & h_2 \notin \mathrm{Im}\phi, \end{cases} \tag{16}$$

for any $(h_1, h_2) \in \mathrm{GF}(2)^s \times \mathrm{GF}(2)^t$.

TABLE II
THE WEIGHT DISTRIBUTION OF $\mathcal{C}_f$ IN THEOREM 23 FOR ODD s

Weight w	No. of codewords A_w
0	1
2^{m-1}	$2^m - 1 + 2^s(2^t - s - 2) + \binom{s}{(1+s)/2}$
$2^{m-1}+2^{t-1}$	$s2^{s-1}$
$2^{m-1}-2^{t-1}$	$2^s + s2^{s-1}$
$2^{m-1}-2^{t-1}(1+s-2i)$ for $1 \le i \le s$ & $i \ne \frac{1+s}{2}$	$\binom{s}{i}$
$2^{m-1}+2^{t-1}(2^s-s-1)$	1

TABLE III
THE WEIGHT DISTRIBUTION OF $\mathcal{C}_f$ IN THEOREM 23 FOR EVEN s

Weight w	No. of codewords A_w
0	1
2^{m-1}	$2^m - 1 + 2^s(2^t - s - 2)$
$2^{m-1}+2^{t-1}$	$s2^{s-1} + \binom{s}{(s+2)/2}$
$2^{m-1}-2^{t-1}$	$2^s + s2^{s-1} + \binom{s}{s/2}$
$2^{m-1}-2^{t-1}(1+s-2i)$ for $1 \le i \le s$ and $i \notin \{\frac{s}{2}, \frac{s+2}{2}\}$	$\binom{s}{i}$
$2^{m-1}+2^{t-1}(2^s-s-1)$	1

Lemma 22: Let U and V respectively be subsets of $\mathrm{GF}(2)^s$ and $\mathrm{GF}(2)^t$ such that $2^s - |U| \le 2^t - |V|$. Let ϕ be an injection from $\mathrm{GF}(2)^s \setminus U$ to $\mathrm{GF}(2)^t \setminus V$. Then, for the Boolean function in Equation (15),

$$\hat{f}(h_1, h_2) = \begin{cases} 2^t \displaystyle\sum_{x \in \phi^{-1}(h_2)} (-1)^{g(x)+h_1\cdot x}, & h_2 \in \mathrm{Im}\phi \cap V, \\ 2^t(-1)^{g(\phi^{-1}(h_2))+h_1\cdot\phi^{-1}(h_2)}, & h_2 \in \mathrm{Im}\phi \setminus V, \\ 0, & h_2 \notin \mathrm{Im}\phi. \end{cases} \tag{17}$$

Proof: The conclusion follows directly from Equation (16). ■

Theorem 23: Let $m \ge 7$ be an odd integer, $s = (m+1)/2$, and $t = (m-1)/2$. Let $U = \{x \in \mathrm{GF}(2)^s : \mathrm{wt}(x) \ge 2\}$ and $V = \{0\}$. Let f be the Boolean function defined in Equation (15), where $g \equiv 1$, and ϕ is an injection from $\mathrm{GF}(2)^s \setminus U$ to $\mathrm{GF}(2)^t \setminus V$ and $\phi(x) = \mathbf{0}$ for any $x \in U$. Then the code $\mathcal{C}_f$ in Equation (9) is a $[2^m-1, m+1, 2^{m-1}-2^{t-1}(s-1)]$ binary minimal code with

$$w_{\min}/w_{\max} \le 1/2.$$

Furthermore, the weight distribution of $\mathcal{C}_f$ is given by Table II when s is odd and Table III when s is even.

Proof: According to Theorem 3 and the fact that $|U| = 2^s - s - 1$, we have

$$\sum_{x \in U} (-1)^{h_1 \cdot x} = \begin{cases} 2^s - s - 1, & \text{if } h_1 = \mathbf{0}, \\ -(P_1(i) + 1), & \text{if } \mathtt{wt}(h_1) = i, \end{cases}$$

where $P_1(i) = P_1(i, s) = s - 2i$ due to Equation (3). It then follows from Equation (17) in Lemma 22 that

$$\hat{f}(h_1, h_2) = \begin{cases} -2^t(2^s - s - 1), \text{ if } h_1 = \mathbf{0} \text{ and } h_2 = \mathbf{0}, \\ 2^t(s + 1 - 2i), \text{ if } h_1 \ne \mathbf{0}, \mathtt{wt}(h_1) = i \text{ and } h_2 = \mathbf{0}, \\ -2^t(-1)^{h_1\cdot\phi^{-1}(h_2)}, \text{ if } h_2 \in \mathrm{Im}\phi \setminus \{\mathbf{0}\}, \\ 0, \text{ if } h_2 \notin \mathrm{Im}\phi, \end{cases} \tag{18}$$

where i runs from 1 to s. It is clear from Equation (18) that $\hat{f}(h_1, h_2) \pm \hat{f}(\ell_1, \ell_2) \ne 2^m$ for any pair of distinct

TABLE IV
WEIGHT DISTRIBUTION

Weight w	No. of codewords A_w
0	1
$2^{m-1}+\sum_{j=1}^{k} P_j(i)$	$\binom{m}{i}$ $1 \le i \le m$
$\sum_{j=1}^{k}\binom{m}{j}$	1
2^{m-1}	$2^m - 1$

$(h_1, h_2), (\ell_1, \ell_2) \in \mathrm{GF}(2)^s \times \mathrm{GF}(2)^t$. By Theorem 15, $\mathcal{C}_f$ is minimal. The parameters and weight distribution of $\mathcal{C}_f$ then follow by combining Theorem 13, Equation (18), and the facts that $|\mathrm{Im}\phi| = s + 2$ and $\phi^{-1}(h_2) \neq \mathbf{0}$ for any $h_2 \in \mathrm{Im}\phi \setminus \{\mathbf{0}\}$. From the weight distribution of $\mathcal{C}_f$, we know that $w_{\min} = 2^{m-1} - 2^{t-1}(s-1)$ and $w_{\max} = 2^{m-1} + 2^{t-1}(2^s - s - 1)$. It is clear that $w_{\min}/w_{\max} \le 1/2$. This completes the proof of this theorem. ■

The results above tell us that minimal binary linear codes with $w_{\min}/w_{\max} \le 1/2$ can be obtained if the subsets U and V are suitably chosen. It would be possible to construct more minimal binary linear codes with $w_{\min}/w_{\max} \le 1/2$ from other subsets U and V.

The following numerical data is consistent with the conclusion of Theorem 23.

Example 24: Let $m = 7$. Then the set $\mathcal{C}_f$ in Theorem 23 is a minimal code with parameters [127, 8, 52] and weight enumerator

$$1 + 4z^{52} + 54z^{60} + 159\, z^{64} + 36\, z^{68} + z^{76} + z^{108}.$$

Obviously, $w_{\min}/w_{\max} = 52/108 < 1/2$.

Example 25: Let $m = 9$. Then the set $\mathcal{C}_f$ in Theorem 23 is a minimal code with parameters [511, 10, 224] and weight enumerator

$$1 + 5z^{224} + 10z^{240} + 112\, z^{248} + 809\, z^{256} + 80z^{264} + 5z^{272} + z^{288} + z^{464}.$$

It is clear that $w_{\min}/w_{\max} = 224/464 < 1/2$.

C. The Third Family of Minimal Binary Linear Codes

For a positive integer k with $1 \le k \le m$, let $S(m, k)$ denote the set of all vectors in $\mathrm{GF}(2)^m$ with Hamming weight at least 1 and at most k. Let $g_{(m,k)}$ be the Boolean function of m variables with support $S(m, k)$. In the following, we consider the linear code $\mathcal{C}_{g_{(m,k)}}$ in Equation (9).

Theorem 26: The code $\mathcal{C}_{g_{(m,k)}}$ has length $2^m - 1$, dimension $m + 1$, and the weight distribution in Table IV.

Proof: Let $w \in \mathrm{GF}(2)^m$ with Hamming weight i. By definition and Theorem 3,

$$\tilde{g}_{(m,k)}(w) = \sum_{x \in S(m,k)} (-1)^{w \cdot x} = \sum_{j=1}^{k} P_j(i). \tag{19}$$

The desired conclusions then follow from Theorem 13. ■

Theorem 27: Let $1 \le k \le m$. Then $\mathcal{C}_{g_{(m,k)}}$ is minimal if and only if

$$\sum_{j=1}^{k} P_j(i_1) + \sum_{j=1}^{k} P_j(i_2) \neq -2^{m-1} \text{ and}$$
$$\sum_{j=1}^{k} P_j(i_1) - \sum_{j=1}^{k} P_j(i_2) \neq 2^{m-1} \tag{20}$$

for all pairs (i_1, i_2) with $1 \le i_1 \le m$ and $1 \le i_2 \le m$, and

$$\sum_{j=1}^{k} P_j(i) \neq \pm \sum_{j=1}^{k} \binom{m}{j} \tag{21}$$

for all $1 \le i \le m$.

Proof: By Equations (2), (19) and Theorem 4, we deduce

$$\hat{f}(w) = \begin{cases} 2^m - 2\sum_{j=1}^{k}\binom{m}{j} & \text{if } w = 0, \\ -2\sum_{j=1}^{k} P_j(i) & \text{if } w \neq 0, \end{cases}$$

where $w \in \mathrm{GF}(2)^m$ has Hamming weight i. Then the desired conclusion follows from Theorem 15. ■

Before giving a class of minimal linear codes with $w_{\min}/w_{\max} \le 1/2$, we firstly present a few lemmas below.

Lemma 28: The following equations hold.

(1) For $1 \le k \le \lfloor \frac{m-3}{2} \rfloor$,

$$\sum_{j=1}^{k} \binom{m}{j} = 2^{m-1} - 1 - \sum_{j=k}^{m-k-2} \binom{m-1}{j}.$$

(2) If m is odd, then

$$\sum_{j=1}^{\frac{m-1}{2}} \binom{m}{j} = 2^{m-1} - 1.$$

(3) If m is even, then

$$\sum_{j=1}^{\frac{m-2}{2}} \binom{m}{j} = 2^{m-1} - 1 - \binom{m-1}{\frac{m-2}{2}}.$$

Proof: (1) Note that

$$\begin{aligned}
&\sum_{j=1}^{k} \binom{m}{j} \\
&= \sum_{j=1}^{k} \left(\binom{m-1}{j-1} + \binom{m-1}{j} \right) \\
&= \sum_{j=0}^{k-1} \binom{m-1}{j} + \sum_{j=1}^{k} \binom{m-1}{m-1-j} \\
&= \sum_{j=0}^{k-1} \binom{m-1}{j} + \sum_{j=m-k-1}^{m-2} \binom{m-1}{j} \\
&= \sum_{j=0}^{m-1} \binom{m-1}{j} - \binom{m-1}{m-1} - \sum_{j=k}^{m-k-2} \binom{m-1}{j} \\
&= 2^{m-1} - 1 - \sum_{j=k}^{m-k-2} \binom{m-1}{j}.
\end{aligned}$$

The proof is then completed.

(2) If m is odd, then

$$\begin{aligned}\sum_{j=1}^{\frac{m-1}{2}}\binom{m}{j} &= \sum_{j=1}^{\frac{m-1}{2}}\left(\binom{m-1}{j-1}+\binom{m-1}{j}\right)\\ &= \sum_{j=0}^{\frac{m-3}{2}}\binom{m-1}{j}+\sum_{j=1}^{\frac{m-1}{2}}\binom{m-1}{m-1-j}\\ &= \sum_{j=0}^{\frac{m-3}{2}}\binom{m-1}{j}+\sum_{j=\frac{m-1}{2}}^{m-2}\binom{m-1}{j}\\ &= \sum_{j=0}^{m-1}\binom{m-1}{j}-\binom{m-1}{m-1}\\ &= 2^{m-1}-1.\end{aligned}$$

(3) The proof is similar to that of (2) above, and is omitted. ■

Lemma 29: Let $2 \leq k \leq \lfloor\frac{m-3}{2}\rfloor$ and $m \geq 7$. Then we have the followings.

(1) The equation

$$\sum_{j=1}^{k}\frac{m-2j}{m}\binom{m}{j} = \binom{m-1}{k}-1$$

holds.

(2) If k is even, then

$$\sum_{j=1}^{k}(-1)^j\binom{m}{j} = \binom{m-1}{k}-1.$$

If k is odd, then

$$\sum_{j=1}^{k}(-1)^j\binom{m}{j} = -\binom{m-1}{k}-1.$$

Proof: (1) The proof is completed by noting that

$$\begin{aligned}&\sum_{j=1}^{k}\frac{m-2j}{m}\binom{m}{j}\\ &= \sum_{j=1}^{k}\binom{m}{j}-2\sum_{j=1}^{k}\frac{j}{m}\binom{m}{j}\\ &= \sum_{j=1}^{k}\binom{m}{j}-2\sum_{j=1}^{k}\binom{m-1}{j-1}\\ &= \sum_{j=1}^{k}\left(\binom{m-1}{j}+\binom{m-1}{j-1}\right)-2\sum_{j=1}^{k}\binom{m-1}{j-1}\\ &= \sum_{j=1}^{k}\binom{m-1}{j}-\sum_{j=1}^{k}\binom{m-1}{j-1}\\ &= \binom{m-1}{k}-1.\end{aligned}$$

(2) Note that

$$\begin{aligned}&\sum_{j=1}^{k}(-1)^j\binom{m}{j}\\ &= \sum_{j=1}^{k}(-1)^j\left(\binom{m-1}{j-1}+\binom{m-1}{j}\right)\\ &= -\left(\binom{m-1}{0}+\binom{m-1}{1}\right)+\\ &\quad\left(\binom{m-1}{1}+\binom{m-1}{2}\right)+\cdots+\\ &\quad(-1)^{k-1}\left(\binom{m-1}{k-2}+\binom{k-1}{j}\right)+\\ &\quad(-1)^{k}\left(\binom{m-1}{k-1}+\binom{m-1}{k}\right)\\ &= \begin{cases}\binom{m-1}{k}-1 & \text{if } k \text{ is even,}\\ -\binom{m-1}{k}-1 & \text{if } k \text{ is odd.}\end{cases}\end{aligned}$$

Then we complete the proof. ■

Lemma 30: Let $2 \leq k \leq \lfloor\frac{m-3}{2}\rfloor$ and $m \geq 7$. For any $1 \leq i \leq m$, then

$$\left|\sum_{j=1}^{k}P_j(i)\right| \leq \binom{m-1}{k}+1.$$

Proof: By Corollary 8, we have

$$\begin{cases}\left|\sum_{j=1}^{k}P_j(i)\right| \leq 1+\frac{m-1-2k}{m-1}\binom{m-1}{k} \text{ if } 2 \leq i \leq m-1,\\ \sum_{j=1}^{k}P_j(i) = \sum_{j=1}^{k}\frac{m-2j}{m}\binom{m}{j} \text{ if } i=1,\\ \sum_{j=1}^{k}P_j(i) = \sum_{j=1}^{k}(-1)^j\binom{m}{j} \text{ if } i=m.\end{cases} \quad (22)$$

Due to Lemma 29, if k is even, then

$$\sum_{j=1}^{k}P_j(m) = \sum_{j=1}^{k}P_j(1) = \binom{m-1}{k}-1 > 0;$$

if k is odd, then

$$\sum_{j=1}^{k}P_j(m) = -\binom{m-1}{k}-1$$

and

$$\begin{aligned}\left|\sum_{j=1}^{k}P_j(m)\right| &= 1+\binom{m-1}{k}\\ &> \left|\sum_{j=1}^{k}P_j(1)\right| = \binom{m-1}{k}-1.\end{aligned}$$

From (22), it is clear that

$$\left|\sum_{j=1}^{k}P_j(i)\right| \leq 1+\frac{m-1-2k}{m-1}\binom{m-1}{k} < 1+\binom{m-1}{k}$$

for any $2 \leq i \leq m-1$. From the discussions above, we deduce that

$$\left|\sum_{j=1}^{k}P_j(i)\right| \leq \binom{m-1}{k}+1$$

for any $1 \leq i \leq m$, which completes the proof. ■

The following theorem describes an infinite class of minimal codes satisfying $w_{\min}/w_{\max} \leq 1/2$ under certain conditions.

Theorem 31: Let $2 \leq k \leq \lfloor \frac{m-3}{2} \rfloor$ and $m \geq 7$. Then the set $\mathcal{C}_{g_{(m,k)}}$ in Theorem 27 is a minimal code with parameters

$$\left[2^m - 1,\ m+1,\ \sum_{j=1}^{k} \binom{m}{j}\right].$$

Furthermore, $w_{\min}/w_{\max} \leq 1/2$ if and only if

$$1 + 2\sum_{j=1}^{k} \binom{m}{j} \leq 2^{m-1} + \binom{m-1}{k}.$$

Proof: If $k = 1$, then by Theorem 27 we deduce that $\mathcal{C}_{g_{(m,k)}}$ is not minimal as $P_1(m) = -P_1(0) = -\binom{m}{1}$. In the following, we assume that $2 \leq k \leq \lfloor \frac{m-3}{2} \rfloor$.

By Lemma 30, for any $1 \leq i \leq m$, we have

$$\begin{aligned}\left|\sum_{j=1}^{k} P_j(i)\right| &\leq \binom{m-1}{k} + 1 \\ &< \binom{m}{k} + 1 < \sum_{j=1}^{k} \binom{m}{j}.\end{aligned}$$

Thus Inequality (21) holds. On the other hand, for any $1 \leq i \leq m$, we have

$$-\binom{m-1}{k} - 1 \leq \sum_{j=1}^{k} P_j(i) \leq \binom{m-1}{k} + 1.$$

Hence, for any pair (i_1, i_2) satisfying $1 \leq i_1 \leq m$ and $1 \leq i_2 \leq m$, one obtains

$$\sum_{j=1}^{k} P_j(i_1) + \sum_{j=1}^{k} P_j(i_2) \geq -2\binom{m-1}{k} - 2$$

and

$$\sum_{j=1}^{k} P_j(i_1) - \sum_{j=1}^{k} P_j(i_2) \leq 2\binom{m-1}{k} + 2.$$

Note that

$$\begin{aligned}2\binom{m-1}{k} + 2 &= 2\left(\binom{m-1}{k} + 1\right) \\ &= 2\left(\binom{m-2}{k} + \binom{m-2}{k-1} + 1\right) \\ &< 2\sum_{j=0}^{m-2} \binom{m-2}{j} = 2^{m-1}.\end{aligned}$$

This implies that the inequalities in (20) hold. We then deduce that $\mathcal{C}_{g_{(m,k)}}$ is minimal by Theorem 27.

By Table IV and Corollary 8, we derive that all the nonzero Hamming weights of $\mathcal{C}_{g_{(m,k)}}$ are

$$\begin{cases} w_1 = \sum_{j=1}^{k} \binom{m}{j}, \\ w_2 = 2^{m-1}, \\ w_3 = 2^{m-1} + \sum_{j=1}^{k} (-1)^j \binom{m}{j}, \\ w_4 = 2^{m-1} + \sum_{j=1}^{k} \frac{m-2j}{m} \binom{m}{j}, \\ w(i) = 2^{m-1} + \sum_{j=1}^{k} P_j(i) \text{ for } 2 \leq i \leq m-1, \end{cases}$$

where $\left|\sum_{j=1}^{k} P_j(i)\right| \leq 1 + \frac{m-1-2k}{m-1}\binom{m-1}{k}$ for $2 \leq i \leq m-1$ and $2 \leq k \leq \lfloor \frac{m-3}{2} \rfloor$. Hence, for $2 \leq i \leq m-1$,

$$\begin{aligned}2^{m-1} - 1 - \frac{m-1-2k}{m-1}\binom{m-1}{k} &\\ \leq w(i) &\\ \leq 2^{m-1} + 1 + \frac{m-1-2k}{m-1}\binom{m-1}{k}&.\end{aligned} \tag{23}$$

Since $2 \leq k \leq \lfloor \frac{m-3}{2} \rfloor$, we have $w_1 = \sum_{j=1}^{k} \binom{m}{j} < 2^{m-1} = w_2$ by Lemma 28. It is clear that $w_2 < w_4$. By Lemma 29, we deduce $w_4 \geq w_3$. Since

$$\begin{aligned}\sum_{j=1}^{k} \binom{m}{j} - \sum_{j=1}^{k} (-1)^j \binom{m}{j} &= \sum_{j=1}^{k} (1 - (-1)^j) \binom{m}{j} \\ &= \sum_{\substack{j \text{ is odd}, \\ 1 \leq j \leq k}} 2\binom{m}{j} \\ &< \sum_{j=1}^{k+1} \binom{m}{j} < 2^{m-1},\end{aligned}$$

by Lemma 28 we deduce that

$$w_1 = \sum_{j=1}^{k} \binom{m}{j} < 2^{m-1} + \sum_{j=1}^{k} (-1)^j \binom{m}{j} = w_3.$$

Note that

$$\begin{aligned}\sum_{j=1}^{k} \binom{m}{j} &+ 1 + \frac{m-1-2k}{m-1}\binom{m-1}{k} \\ &= \sum_{j=0}^{k} \binom{m}{j} + \frac{m-1-2k}{m-1}\binom{m-1}{k} \\ &< \sum_{j=0}^{k} \binom{m}{j} + \binom{m-1}{k} \\ &< \sum_{j=0}^{k} \binom{m}{j} + \binom{m-1}{k} + \binom{m-1}{k+1} \\ &= \sum_{j=0}^{k+1} \binom{m}{j}.\end{aligned}$$

Due to $k \leq \lfloor \frac{m-3}{2} \rfloor$, we then obtain that

$$\begin{aligned}\sum_{j=1}^{k} \binom{m}{j} + 1 + \frac{m-1-2k}{m-1}\binom{m-1}{k}& \\ < \sum_{j=0}^{\frac{m-1}{2}} \binom{m}{j} < 2^{m-1} &\text{ for odd } m\end{aligned}$$

and

$$\begin{aligned}\sum_{j=1}^{k} \binom{m}{j} + 1 + \frac{m-1-2k}{m-1}\binom{m-1}{k}& \\ < \sum_{j=0}^{\frac{m-2}{2}} \binom{m}{j} < 2^{m-1} &\text{ for even } m\end{aligned}$$

by Lemma 28. Then by Inequality (23), we have

$$w_1 < w(i) \text{ for any } 2 \le i \le m-1.$$

In the following, we shall prove that

$$w_4 > w(i) \text{ for any } 2 \le i \le m-1.$$

Due to Inequality (23), it suffices to prove that

$$\begin{aligned} w_4 &= 2^{m-1} + \sum_{j=1}^{k} \frac{m-2j}{m}\binom{m}{j} \\ &> 2^{m-1} + 1 + \frac{m-1-2k}{m-1}\binom{m-1}{k}, \end{aligned}$$

that is,

$$\sum_{j=1}^{k} \frac{m-2j}{m}\binom{m}{j} > 1 + \frac{m-1-2k}{m-1}\binom{m-1}{k}. \tag{24}$$

By Lemma 29, we have

$$\begin{aligned} \sum_{j=1}^{k} \frac{m-2j}{m}\binom{m}{j} &= \binom{m-1}{k} - 1 \\ &> \binom{m-1}{k} + 1 - 2\binom{m-2}{k-1} \\ &= \binom{m-1}{k} + 1 - \frac{2k}{m-1}\binom{m-1}{k} \\ &= 1 + \frac{m-1-2k}{m-1}\binom{m-1}{k}. \end{aligned}$$

Thus Inequality (24) holds and

$$w_4 > w(i) \text{ for any } 2 \le i \le m-1.$$

From the discussions above, we deduce that

$$w_{\min} = w_1 = \sum_{j=1}^{k}\binom{m}{j}$$

and

$$w_{\max} = w_4 = 2^{m-1} + \binom{m-1}{k} - 1.$$

Then $\frac{w_{\min}}{w_{\max}} \le \frac{1}{2}$ if and only if

$$1 + 2\sum_{j=1}^{k}\binom{m}{j} \le 2^{m-1} + \binom{m-1}{k},$$

which completes the proof. ■

As corollaries of Theorem 31, we have the following.

Corollary 32: Let $m \ge 7$. Then $\mathcal{C}_{g_{(m,2)}}$ in Theorem 27 is a minimal code with parameters

$$\left[2^m - 1,\ m+1,\ \sum_{j=1}^{2}\binom{m}{j}\right].$$

Furthermore, $w_{\min}/w_{\max} < 1/2$.

Example 33: The set $\mathcal{C}_{g_{(7,2)}}$ in Theorem 27 is a minimal code with parameters [127, 8, 28] and weight enumerator

$$1 + z^{28} + 35z^{60} + 56z^{62} + 127z^{64} + 28\ z^{68} + 8z^{78}.$$

Furthermore, $w_{\min}/w_{\max} = 14/39 < 1/2$. Note that some weights in Table IV may be the same in certain cases. Hence the code has at most $m+2$ weights. This example shows that the code has in fact 6 (rather than 9) weights.

Corollary 34: Let $m \ge 9$. Then $\mathcal{C}_{g_{(m,3)}}$ in Theorem 27 is a minimal code with parameters

$$\left[2^m - 1,\ m+1,\ \sum_{j=1}^{3}\binom{m}{j}\right].$$

Furthermore, $w_{\min}/w_{\max} < 1/2$.

Example 35: The set $\mathcal{C}_{g_{(9,3)}}$ in Theorem 27 is a minimal code with parameters [511, 10, 129] and weight enumerator

$$\begin{aligned} &1 + z^{129} + z^{199} + 9\ z^{241} + 126^{249} + 84z^{251} + 126^{255} \\ &\quad +511\ z^{256} + 36z^{259} + 84z^{261} + 36z^{269} + 9z^{311}. \end{aligned}$$

Furthermore, $w_{\min}/w_{\max} = 129/311 < 1/2$.

VI. Summary and Concluding Remarks

The main contributions of this paper are the following:

- A necessary and sufficient condition for a binary linear code to be minimal (Theorem 15).
- A necessary and sufficient condition for a two-weight binary linear code to be minimal (Theorem 11).
- A set of sufficient conditions for a three-weight binary linear code to be minimal (Theorem 12).
- Three infinite families of minimal binary linear codes with $w_{\min}/w_{\max} < 1/2$ (Theorems 18, 23, and 31).

We remark that constructing infinite families of minimal binary linear codes with $w_{\min}/w_{\max} \le 1/2$ is a hard problem in general. It would be nice if more infinite families of such codes could be found. Another construction of binary linear codes was surveyed in [12] and [13], which may contain more infinite families of such binary codes. To the best of our knowledge, no infinite family of minimal linear codes over GF(q) with $w_{\min}/w_{\max} < (q-1)/q$ for $q > 2$ is reported in the literature, though a specific example of such code was presented in [10].

It should be noted that linear codes employed for secret sharing are preferred to be minimal, in order to make the access structure of the secret sharing scheme to be special [14], [20]. Such codes may not have very good error-correcting capability. The minimal binary codes presented in this paper are for secret sharing, not for error correction.

Acknowledgements

The authors are very grateful to the reviewers and the Associate Editor, Prof. Sihem Mesnager, for their comments and suggestions that improved the quality and presentation of this paper.

References

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

[3] C. Carlet, "Boolean functions for cryptography and error correcting codes," in *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, Y. Crama and P. L. Hammer, Eds. Cambridge, U.K.: Cambridge Univ. Press, 2010, pp. 257–397.

[4] C. Carlet and C. Ding, "Nonlinearities of S-boxes," *Finite Fields Appl.*, vol. 13, no. 1, pp. 121–135, 2007.

[5] C. Carlet, C. Ding, and J. Yuan, "Linear codes from perfect nonlinear mappings and their secret sharing schemes," *IEEE Trans. Inf. Theory*, vol. 51, no. 6, pp. 2089–2102, Jun. 2005.

[6] C. Carlet, X. Zeng, C. Li, and L. Hu, "Further properties of several classes of Boolean functions with optimum algebraic immunity," *Des., Codes Cryptogr.*, vol. 52, no. 3, pp. 303–338, 2009.

[7] C. Carlet and S. Mesnager, "Four decades of research on bent functions," *Des., Codes Cryptogr.*, vol. 78, no. 1, pp. 5–50, Jan. 2016.

[8] S. Chang and J. Y. Hyun, "Linear codes from simplicial complexes," in *Designs, Codes and Cryptography*, pp. 1–15, Nov. 2017. [Online]. Available: https://doi.org/10.1007/s10623-017-0442-5

[9] H. Chabanne, G. Cohen, and A. Patey, "Towards secure two-party computation from the wire-tap channel," in *Information Security and Cryptology* (Lecture Notes in Computer Science), vol. 8565, H.-S. Lee and D.-G. Han, Eds. Berlin, Germany: Springer-Verlag, 2014, pp. 34–46.

[10] G. Cohen, S. Mesnager, and A. Patey, "On minimal and quasi-minimal linear codes," in *Cryptography and Coding* (Lecture Notes in Computer Science), vol. 8308, M. Stam, Eds. Berlin, Germany: Springer-Verlag, 2003, pp. 85–98.

[11] J. F. Dillon, "Elementary Hadamard difference sets," Ph.D. dissertation, Dept. Math., Univ. Maryland, College Park, MD, USA, 1974.

[12] C. Ding, "Linear codes from some 2-designs," *IEEE Trans. Inf. Theory*, vol. 60, no. 6, pp. 3265–3275, Jun. 2015.

[13] C. Ding, "A construction of binary linear codes from Boolean functions," *Discrete Math.*, vol. 339, no. 9, pp. 2288–2303, 2016.

[14] 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, Jun. 2003, pp. 11–25.

[15] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. The Netherlands, Amsterdam: North Holland, 1977.

[16] R. L. McFarland, "A family of difference sets in non-cyclic groups," *J. Combinat. Theory A*, vol. 15, no. 1, pp. 1–10, Jul. 1973.

[17] J. L. Massey, "Minimal codewords and secret sharing," in *Proc. 6th Joint Swedish-Russian Int. Workshop Inf. Theory*, Mölle, Sweden, 1993, pp. 246–249.

[18] S. Mesnager, "Linear codes with few weights from weakly regular bent functions based on a generic construction," *Cryptogr. Commun.*, vol. 9, no. 1, pp. 71–84, 2017.

[19] T. Wadayama, T. Hada, K. Wakasugi, and M. Kasahara, "Upper and lower bounds on maximum nonlinearity of n-input m-output Boolean function," *Des., Codes Cryptograph.*, vol. 23, no. 1, pp. 23–33, 2001.

[20] J. Yuan and C. Ding, "Secret sharing schemes from three classes of linear codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 1, pp. 206–212, Jan. 2006.

Cunsheng Ding (M'98–SM'05) was born in 1962 in Shaanxi, China. He received the M.Sc. degree in 1988 from the Northwestern Telecommunications Engineering Institute, Xian, China; and the Ph.D. in 1997 from the University of Turku, Turku, Finland.

From 1988 to 1992 he was a Lecturer of Mathematics at Xidian University, China. Before joining the Hong Kong University of Science and Technology in 2000, where he is currently a Professor of Computer Science and Engineering, he was an Assistant Professor of Computer Science at the National University of Singapore.

His research fields are combinatorial designs, cryptography and coding theory. He has coauthored four research monographs, and served as a guest editor or editor for ten journals. Dr. Ding co-received the State Natural Science Award of China in 1989.

Ziling Heng received the B.Sci. degree in mathematics from Henan Normal University, Xinxiang, China, and the Ph.D. in mathematics at the Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2012 and 2017, respectively. From 2017 to 2018, he was a postdoctoral fellow at the Department of Computer Science and Engineering, the Hong Kong University of Science and Technology. His research interests include coding theory and sequences.

Zhengchun Zhou received the B.S. and M.S. degrees in mathematics and the Ph.D. degree in information security from Southwest Jiaotong University, Chengdu, China, in 2001, 2004, and 2010, respectively. From 2012 to 2013, he was a postdoctoral member in the Department of Computer Science and Engineering, the Hong Kong University of Science and Technology. From 2013 to 2014, he was a research associate in the Department of Computer Science and Engineering, the Hong Kong University of Science and Technology. Since 2001, he has been in the Department of Mathematics, Southwest Jiaotong University, where he is currently a professor. His research interests include sequence design, Boolean function, coding theory, and compressed sensing. Dr. Zhou was the recipient of the National excellent Doctoral Dissertation award in 2013 (China).