Infinite families of minimal binary codes via Krawtchouk polynomials

Xiaoni Du [*†‡] René Rodríguez [§¶] Hao Wu[*‖]

Abstract: Linear codes play a crucial role in various fields of engineering and mathematics, including data storage, communication, cryptography, and combinatorics. Minimal linear codes, a subset of linear codes, are particularly essential for designing effective secret sharing schemes. In this paper, we introduce several classes of minimal binary linear codes by carefully selecting appropriate Boolean functions. These functions belong to a renowned class of Boolean functions, the general Maiorana-McFarland class. We employ a method first proposed by Ding et al. [7] to construct minimal codes violating the Ashikhmin-Barg bound (wide minimal codes) by using Krawtchouk polynomials. The lengths, dimensions, and weight distributions of the obtained codes are determined using the Walsh spectrum distribution of the chosen Boolean functions. Our findings demonstrate that a vast majority of the newly constructed codes are wide minimal codes. Furthermore, our proposed codes exhibit a significantly larger minimum distance, in some cases, compared to some existing similar constructions. Finally, we address this method, based on Krawtchouk polynomials, more generally, and highlight certain generic properties related to it. This study provides insights into the scope of this method.

Keywords: Minimal binary linear codes; the Ashikhmin-Barg bound; Boolean functions; the general Maiorana-McFarland class; Krawtchouck polynomials.

1 Introduction

Due to their simple description, uninvolved algebraic structure and their associated cryptographic properties, linear codes have an ample range of applications in communication, data storage, information security and cryptography (e.g., McEliece cryptosystem [12]). In particu-

[*]The author is with College of Mathematics and Statistics, and also with Key Laboratory of Cryptography and Data Analytics, Northwest Normal University, Lanzhou, 730070, Gansu, China.

[†]The author is with Gansu Provincial Research Center for Basic Disciplines of Mathematics and Statistics, Lanzhou, 730070, Gansu, China.

[‡]e-mail: ymldxn@126.com

[§]The author is part of the Department of Mathematics at the University of Primorska and also part of the Andrej Marušič Institute, Koper, 6000, Slovenia.

[¶]e-mail: rene7ca@gmail.com (corresponding author)

[‖]e-mail: nwnuwh@126.com

lar, as a special class of linear codes, minimal linear codes play an important role in designing access structures for secret sharing schemes [1] and secure multi-party computation [14]. The weight distributions of linear codes give more information on their structures and properties. However, in general, it is difficult to determine the weight distributions of linear codes [5, 18, 19]. Therefore, the construction and full specification of new minimal linear codes have become an interesting topic in coding theory and cryptography over the past years.

In 1998, Ashikhmin and Barg [2] proved a sufficient condition for a linear code over a finite field with q elements to be minimal by using the maximum and minimum weight of the code, $w_{\max}$ and $w_{\min}$, namely, if $w_{\min}/w_{\max} > (q-1)/q$ then the code is minimal. This condition is called the Ashikhmin-Barg condition (or bound). Following the terminology introduced in [16, 17], linear codes satisfying the Ashikhmin-Barg condition are called narrow codes, and otherwise they are referred as wide codes.

Cohen et al. [6] presented the first example of a wide minimal code, and later, a necessary and sufficient condition for a linear code to be minimal was shown by Ding et al. [7, 9]. They used this condition to build the first examples of infinite families of wide minimal binary codes. As pointed out in [7], infinite families of wide minimal codes are in general harder to construct than their narrow counterpart.

Based on the conclusions of Ding et al. [7], Mesnager et al. [13] proposed a novel method using characteristic functions to construct minimal codes. More precisely, by applying the Fourier transform and properties of characteristic functions, they developed a coding scheme that achieves better error-correcting capabilities compared to conventional methods. In 2021, Zhang et al. [16] extended the results in [7] to construct several classes of wide binary minimal codes with larger minimum distances or higher dimensions. Very recently, with a similar idea as in [7], Du et al. [8] constructed two classes of wide minimal codes, and determined their weight distributions. Currently, there are many more constructions of infinite families of wide minimal codes based on a large range of techniques and mathematical objects, see for instance [3, 4, 10, 15].

Extending the work of Zhang et al. [16], we construct binary linear codes with larger minimum distances. To this end, we first specify the underlying Boolean function f that belongs to the so-called general Maiorana-McFarland class (GMM). It is important to highlight that the Boolean function f is different from the ones used in [7, 8, 16]. Then, we show that the resulting codes C_f derived from f are minimal and wide. To fully specify the weight distributions of the obtained codes, we use Krawtchouk polynomials and their good combinatorial properties. Using the method developed in [16, 17] and the code $C_{D_\gamma(f)}$ that is defined via a suitable derivative of the Boolean function $f \in$ GMM, we also construct a class of wide binary minimal codes and determine its weight distribution. Again, the function f used for $C_{D_\gamma(f)}$ is different from the one in [16]. Moreover, our codes $C_{D_\gamma(f)}$ possess a larger minimum distance than those in [16]. Finally,

the codewords in $C_{D_\gamma(f)}$ can be adjoined to C_f to increase the dimension of the resulting codes by one. In the second part of this paper, we study in greater detail the Krawtchouk-polynomials method to handle the general case of our constructions. It is noteworthy that this approach not only yields novel classes of linear codes but also produces a great variety of wide minimal codes. We also determine the general scope and limitations of our methods.

This article is structured as follows. In Section 2, we introduce all fundamental concepts related to Boolean functions, provide definitions and properties of minimal codes and set the notation that will be used throughout the paper. In Section 3, we provide the construction of classes of linear codes using certain functions (with an associated set) in the GMM class of Boolean functions, prove they are wide and minimal under certain conditions, and fully specify their weight distributions by employing the Krawtchouk method. Additionally, we present the derivative method [16, 17] for a suitable choice of f and its derivative $D_\gamma(f)$, and therewith we obtain wide minimal codes with better parameters than those in [16, 17]. The Krawtchouk method is analysed in depth in Section 4, where we address the general case for the choice of the associated set of Boolean functions in GMM. Finally, our research findings are summarized in Section 5.

2 Preliminaries

Let n be a positive integer, and $\mathbb{F}_2^n$ denote the n-dimensional vector space over the finite field $\mathbb{F}_2$. A binary $[n, k, d]$ linear code C is a k-dimensional subspace of $\mathbb{F}_2^n$ over $\mathbb{F}_2$ with minimum (Hamming) distance d. Each vector $\mathbf{c}$ in the code C is called a codeword. The number of codewords in C with (Hamming) weight i is denoted by A_i. The weight enumerator of C is the polynomial with integer coefficients, $1 + A_1 z + \cdots + A_n z^n$. Accordingly, the sequence $(1, A_1, A_2, \ldots, A_n)$ is called the weight distribution of C. A code C is said to be a t-weight code if the number of nonzero A_i in $(A_1, A_2, \cdots, A_n)$ is equal to t. The support of any $\mathbf{c} = (c_1, c_2, \ldots, c_n) \in C$ is defined as

$$\mathrm{supp}(\mathbf{c}) := \{i \in \{1, \ldots, n\} : c_i \neq 0\},$$

where $\{1, \ldots, n\}$ denotes the set of integers from 1 up to n (inclusive). If $|S|$ denotes the number of elements in a set S, then it is easy to see that the Hamming weight $wt(\mathbf{c})$ of a codeword $\mathbf{c}$ satisfies $wt(\mathbf{c}) = |\mathrm{supp}(\mathbf{c})|$. For any two vectors $\mathbf{u}, \mathbf{v} \in \mathbb{F}_2^n$, if $\mathrm{supp}(\mathbf{v}) \subseteq \mathrm{supp}(\mathbf{u})$, then we say $\mathbf{v}$ is covered by $\mathbf{u}$ (or $\mathbf{u}$ covers $\mathbf{v}$) and we write $\mathbf{v} \preceq \mathbf{u}$. For a code C over $\mathbb{F}_2$, a codeword $\mathbf{c} \in C$ is called minimal if in C it is covered only by itself.

Definition 1 A linear code C is called a minimal linear code (minimal code for short) if every nonzero codeword in C is minimal.

Lemma 1 (Ashikhmin–Barg [2]) Let $w_{\min}$ and $w_{\max}$ be the minimum and maximum nonzero weights of the linear code $\mathcal{C}$, respectively. If $w_{\min}/w_{\max} > 1/2$, then $\mathcal{C}$ is minimal.

Now, we introduce some basic facts about Krawtchouk polynomials [11] which will be extensively used for determining the Walsh transform of Boolean functions (which will be defined below). Let m be a positive integer and x be a variable taking non-negative integer values. The Krawtchouk polynomial is defined by

$$P_k(x,m) = \sum_{j=0}^{k} (-1)^j \binom{x}{j} \binom{m-x}{k-j}, \tag{2.1}$$

where $0 \le k \le m$. For the sake of simplicity, we write $P_k(x) := P_k(x,m)$ whenever there is no ambiguity. The properties of Krawtchouk polynomials [11] lead to the following symmetry property

$$P_k(i) = (-1)^i P_{m-k}(i), 0 \le i \le m, \tag{2.2}$$

and the following conclusion.

Lemma 2 [11] For any $\mathbf{u} \in \mathbb{F}_2^m$ with Hamming weight $wt(\mathbf{u}) = i$, $1 \le i \le m$, one has

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

To conclude this section, we present some fundamentals on Boolean functions and their connections to minimal linear codes. A mapping $f : \mathbb{F}_2^m \to \mathbb{F}_2$ is called an m-ary Boolean function. Denote by $\mathcal{B}_m$ the set of all m-ary Boolean functions. The Walsh transform of a function $f \in \mathcal{B}_m$ at $\mathbf{w} \in \mathbb{F}_2^m$ is defined by

$$W_f(\mathbf{w}) = \sum_{\mathbf{x}\in\mathbb{F}_2^m} (-1)^{f(\mathbf{x})+\mathbf{w}\cdot\mathbf{x}},$$

where $\mathbf{x} = (x_1, x_2, \ldots, x_m) \in \mathbb{F}_2^m$, $\mathbf{w} = (w_1, w_2, \ldots, w_m) \in \mathbb{F}_2^m$, and "$\cdot$" denotes the standard inner product of these two vectors, that is, $\mathbf{w}\cdot\mathbf{x} := \sum_{i=1}^{m} w_i x_i$. The support of f is defined to be

$$\mathrm{supp}(f) = \{\mathbf{x} \in \mathbb{F}_2^m : f(\mathbf{x}) = 1\}.$$

We denote $(0,0,\ldots,0) \in \mathbb{F}_2^m$ by $\mathbf{0}_m$ and $(1,1,\ldots,1) \in \mathbb{F}_2^m$ by $\mathbf{1}_m$.

Let $f \in \mathcal{B}_m$ be such that f is not affine, i.e., $f(\mathbf{x}) \ne \mathbf{v}\cdot\mathbf{x} + a$ for each $\mathbf{v} \in \mathbb{F}_2^m$ and $a \in \mathbb{F}_2$. Define the code C_f by

$$C_f = \left\{ (uf(\mathbf{x}) + \mathbf{v}\cdot\mathbf{x})_{\mathbf{x}\in\mathbb{F}_2^m} : u \in \mathbb{F}_2, \mathbf{v} \in \mathbb{F}_2^m \right\}. \tag{2.3}$$

The first lemma below presents the weight distribution of the linear code C_f constructed in Eq.(2.3) and the second one provides a necessary and sufficient condition to determine whether C_f is minimal via the Walsh transform of the function f.

Lemma 3 [7] The binary linear code defined by Eq.(2.3) has length 2^m, dimension $m+1$, and the weight distribution is given by the following multiset:

$$\left\{2^{m-1} - \frac{1}{2}W_f(\alpha) : \alpha \in \mathbb{F}_2^m\right\} \cup \left\{2^{m-1} : \alpha \in \mathbb{F}_2^{m*}\right\} \cup \{0\}.$$

Lemma 4 [7] The code C_f in Eq.(2.3) is minimal if and only if for every pair of distinct $\lambda_1, \lambda_2 \in \mathbb{F}_2^m$, it holds that

$$W_f(\lambda_1) \pm W_f(\lambda_2) \neq 2^m.$$

2.1 Notation

Throughout this paper, we adopt the following notation unless otherwise stated.

(1) We will work on the vector space $\mathbb{F}_2^r$, where r denotes an odd integer at least 7. We will always identify the Cartesian product of subspaces $\mathbb{F}_2^k \times \mathbb{F}_2^l$ with $\mathbb{F}_2^r$, where $k = (r+1)/2$ and $l = (r-1)/2$.

(2) The symbol $\mathbb{Z}^*$ is reserved for the ring of positive integers and $S_u = \{s^2 + u : s \in \mathbb{Z}^*\}$, where u is an odd integer.

(3) The function $\eta : \mathbb{C} \to \{0, 1\}$ is given by $\eta(a) = 1$ if $a \in \{1, \ldots, k\}$, and 0 otherwise.

(4) For a given integer i with $1 \leq i \leq k$ (equivalently, $i \in \{1, \ldots, k\}$), define the following:

(a)
$$\Gamma_i = \begin{cases} \{i, k+1-i\}, & k \text{ is odd}, \\ \{i\}, & \text{otherwise}. \end{cases} \tag{2.4}$$

(b) $a_{b,i}^{\pm} = \frac{(k+1) \pm \sqrt{4i(-i+1+k) - (k^2+b)}}{2}$, $b = -1, 3$.

(c) For a fixed $b \in \{-1, 3\}$,

$$\Delta_i = \begin{cases} \{a_{b,i}^+, a_{b,i}^-\}, & k \text{ is odd}, \ \eta(a_{b,i}^+) = 1, i \not\equiv a_{b,i}^+ \pmod 2, \\ \{a_{b,i}^v\}, & k \text{ is even}, \ \eta(a_{b,i}^v) = 1, i \not\equiv a_{b,i}^v \pmod 2, \\ \emptyset, & \text{otherwise}. \end{cases} \tag{2.5}$$

Note that Δ_i is well-defined as there is exactly one value "+" or "–" for v, since $a_{b,i}^+ \not\equiv a_{b,i}^- \pmod 2$ when k is even.

3 The construction of wide binary minimal codes

In this section, we will use the properties of the general Maiorana-McFarland class of Boolean functions and a derivative of a Boolean function to obtain two classes of wide minimal codes, that is, codes not satisfying the Ashikhmin-Barg condition.

Suppose that r, k, l are positive integers satisfying $r = k+l$. The general Maiorana-McFarland class of Boolean functions has the form

$$f(\mathbf{x}, \mathbf{y}) = \phi(\mathbf{x}) \cdot \mathbf{y} + g(\mathbf{x}), \tag{3.1}$$

where $\mathbf{x} \in \mathbb{F}_2^k, \mathbf{y} \in \mathbb{F}_2^l$, ϕ is an arbitrary mapping from $\mathbb{F}_2^k$ to $\mathbb{F}_2^l$ and $g \in \mathcal{B}_k$.

The derivative of $f \in \mathcal{B}_m$ at direction $\gamma \in \mathbb{F}_2^m$ is defined as

$$D_\gamma f(\mathbf{x}) = f(\mathbf{x} + \gamma) + f(\mathbf{x}). \tag{3.2}$$

Throughout this paper, we always use the symbol f to denote the Boolean function defined in Eq.(3.1) with $g \equiv 1$ (the constant one function), i.e.,

$$f(\mathbf{x}, \mathbf{y}) = \phi(\mathbf{x}) \cdot \mathbf{y} + 1. \tag{3.3}$$

For the specification of weight distributions in this section, we will need to study the following quadratic polynomial $A(x)$,

$$A(x) = 2x^2 - (2 + 2k)x + \frac{k(k+1)}{2} + 1, \tag{3.4}$$

where $1 \le x \le k$. It is clear that $A(x) = A(k + 1 - x)$.

3.1 Wide binary minimal codes derived from GMM class

Set r to be an odd integer with $r \ge 11$. To compute the sums in the Walsh transform of the proposed Boolean function, we will need the following lemma that shows the relation between $A(i)$ and the set U_0 of vectors with weight at most $k - 3$, i.e.,

$$U_0 = \left\{ \mathbf{x} \in \mathbb{F}_2^k : wt(\mathbf{x}) \le k - 3 \right\}. \tag{3.5}$$

Lemma 5 Let $k \ge 6$ and U_0 denote the set of vectors in $\mathbb{F}_2^k$ with weight at most $k - 3$ given in (3.5). Consider the quadratic polynomial $A(i)$ in (3.4). Then

$$\sum_{\mathbf{x} \in U_0} (-1)^{\mathbf{v}_1 \cdot \mathbf{x}} = \begin{cases} |U_0|, & \mathbf{v}_1 = \mathbf{0}_k, \\ (-1)^{i+1} A(i), & wt(\mathbf{v}_1) = i, \end{cases} \tag{3.6}$$

where $\mathbf{v}_1 \in \mathbb{F}_2^k$, $1 \le i \le k$.

Proof: If $\mathbf{v}_1 = \mathbf{0}_k$, then

$$\sum_{\mathbf{x}\in U_0}(-1)^{\mathbf{v}_1\cdot\mathbf{x}} = |U_0| = 2^k - \left(\binom{k}{k-2} + \binom{k}{k-1} + 1\right) = 2^k - \frac{k(k+1)}{2} - 1.$$

If $\mathbf{v}_1 \neq \mathbf{0}_k$ and $wt(\mathbf{v}_1) = i, i = 1, 2, \ldots, k$, according to Eqs.(2.1), (2.2) and Lemma 2, we have

$$\begin{aligned}\sum_{\mathbf{x}\in U_0}(-1)^{\mathbf{v}_1\cdot\mathbf{x}} &= \sum_{\mathbf{x}\in\mathbb{F}_2^k}(-1)^{\mathbf{v}_1\cdot\mathbf{x}} - \sum_{\mathbf{x}\in\mathbb{F}_2^k, wt(\mathbf{x})\geq k-2}(-1)^{\mathbf{v}_1\cdot\mathbf{x}}\\ &= 0 - (P_k(i) + P_{k-1}(i) + P_{k-2}(i))\\ &= (-1)^{i+1}\left(1 + k - 2i + \frac{(k-2i)^2 - k}{2}\right)\\ &= (-1)^{i+1}A(i).\end{aligned}$$

The proof is completed. □

By analyzing the behaviour of some quadratic equations, it is easy to derive the following properties of $A(i)$.

Lemma 6 The polynomial $A(x) = 2x^2 - (2+2k)x + \frac{k(k+1)}{2} + 1$ satisfies the following.

(1) $A(i) = 0$ if and only if $k = s^2 + 1 \in S_1$ and $i = \frac{s^2+2\pm s}{2}$.

(2) $A(i) = 1$ if and only if $k = s^2 - 1 \in S_{-1}$ and $i = \frac{s^2\pm s}{2}$.

(3) $A(i) = -1$ if and only if $k = s^2 + 3 \in S_3$ and $i = \frac{s^2+4\pm s}{2}$.

It follows from the relation between k and s given in Lemma 6(1)-(3) that $1 + k \pm s$ is always a positive even number smaller than $2k$, thus $\frac{1+k\pm s}{2}$ is a positive integer smaller than k.

The next lemma follows also from the definition of $A(i)$ by analyzing some quadratic equations derived therefrom, hence we omit its proof.

Lemma 7 Let $k \geq 6$. Let i, j be two distinct integers in $\{1, 2, \ldots, k\}$ and let $B(i) = (-1)^i A(i) = (-1)^i(2i^2 - 2(k+1)i + \frac{k^2+k+2}{2})$.

(1) If $i \equiv j \pmod 2$, then $B(i) = B(j)$ if and only if $i + j = k + 1$. In particular, this can only happen when k is odd.

(2) If $i \not\equiv j \pmod 2$, then $B(i) = B(j)$ if and only if $j = a_{3,i}^{\pm}$ (see Section 2.1).

(3) For every i, $|B(i)| \leq \frac{(k+1)(k-4)}{2} + 3$.

Observe that the sets S_1, S_3 and S_{-1} are mutually disjoint. For instance, $S_1 \cap S_3 = \emptyset$ since if $x = s^2 + 1 = t^2 + 3$ then $(s-t)(s+t) = 2$ so that either $s+t = 2$ and $s-t = 1$ or $s+t = 1$ and $s-t = 2$, which yields $s = 3/2$ and $t = \pm 1/2$. A contradiction to $s, t \in \mathbb{Z}^*$. Similarly, one can prove that $S_1 \cap S_{-1} = \emptyset$ and $S_{-1} \cap S_3 = \emptyset$. To simplify some notation, it will be convenient to define the function $\chi : \{1, \ldots, k\} \to \{0, 1\}$ given by $\chi(i) = 0$ if and only if i is even.

Now we are ready to present the fist class of wide minimal binary codes from the GMM class.

Theorem 1 Let r be an odd integer with $r \geq 11$. Let $f : \mathbb{F}_2^k \times \mathbb{F}_2^l \to \mathbb{F}_2$ be the Boolean function in GMM defined by Eq.(3.3), where ϕ is an injection from $\mathbb{F}_2^k \backslash U_0$ to $\mathbb{F}_2^l \backslash \{\mathbf{0}_l\}$ and $\phi(\mathbf{x}) = \mathbf{0}_l$ for any $\mathbf{x} \in U_0$. The code C_f in Eq.(2.3) is a $[2^r, r+1, d]$ minimal code, where

$$d = \begin{cases} 2^{r-1} - 2^{l-2}(k^2 - 7k + 10), & k \text{ is odd}, \\ 2^{r-1} - 2^{l-2}(k^2 - 3k + 2), & k \text{ is even}. \end{cases}$$

Furthermore, if $r \geq 15$, then C_f is wide. The weight distributions are given in Table 1 and the relevant parameters related to k are given in Table 2 (see also Section 2.1).

Proof: First, we examine the Walsh transform of the function f in Eq.(3.3) at any $(\mathbf{v}_1, \mathbf{v}_2) \in \mathbb{F}_2^k \times \mathbb{F}_2^l$. According to Lemma 5, we have

$$\sum_{\mathbf{x} \in U_0} (-1)^{\mathbf{v}_1 \cdot \mathbf{x}} = \begin{cases} |U_0|, & \mathbf{v}_1 = \mathbf{0}_k, \\ -A(i)(-1)^i, & wt(\mathbf{v}_1) = i, \end{cases}$$

and then we can get

$$\begin{aligned} W_f(\mathbf{v}_1, \mathbf{v}_2) &= \sum_{\mathbf{x} \in \mathbb{F}_2^k} \sum_{\mathbf{y} \in \mathbb{F}_2^l} (-1)^{\phi(\mathbf{x}) \cdot \mathbf{y} + 1 + \mathbf{v}_1 \cdot \mathbf{x} + \mathbf{v}_2 \cdot \mathbf{y}} \\ &= \sum_{\mathbf{x} \in \left(\mathbb{F}_2^k \backslash U_0\right)} \sum_{\mathbf{y} \in \mathbb{F}_2^l} (-1)^{\phi(\mathbf{x}) \cdot \mathbf{y} + 1 + \mathbf{v}_1 \cdot \mathbf{x} + \mathbf{v}_2 \cdot \mathbf{y}} + \sum_{\mathbf{x} \in U_0} \sum_{\mathbf{y} \in \mathbb{F}_2^l} (-1)^{1 + \mathbf{v}_1 \cdot \mathbf{x} + \mathbf{v}_2 \cdot \mathbf{y}} \\ &= \begin{cases} -\left(2^k - \frac{k(k+1)}{2} - 1\right) 2^l, & \mathbf{v}_1 = \mathbf{0}_k, \mathbf{v}_2 = \mathbf{0}_l, \\ (-1)^i A(i) 2^l, & wt(\mathbf{v}_1) = i, \mathbf{v}_2 = \mathbf{0}_l, \\ -(-1)^{\mathbf{v}_1 \cdot \phi^{-1}(\mathbf{v}_2)} 2^l, & \mathbf{v}_2 \in \mathrm{Im}(\phi) \backslash \{\mathbf{0}_l\}, \\ 0, & \mathbf{v}_2 \notin \mathrm{Im}(\phi), \end{cases} \end{aligned} \tag{3.7}$$

where $i = 1, 2, \ldots, k$.

Furthermore, combining Lemma 3 and Eq.(3.7) together, we get that the length and dimension of C_f are 2^r and $r+1$, respectively.

Then, we will determine the weight distribution of the codes and it suffices to determine the frequency of $W_f(\mathbf{v}_1, \mathbf{v}_2)$, where $(\mathbf{v}_1, \mathbf{v}_2) \in \mathbb{F}_2^k \times \mathbb{F}_2^l$, since its corresponding weight can be easily obtained by Lemma 3.

It is clear that the multiplicity of $-\left(2^k - \frac{k(k+1)}{2} - 1\right) 2^l$ is 1. To derive the frequencies of other Walsh values in Eq.(3.7), it is necessary to consider the following cardinalities given in Eqs.(3.8)-(3.10) below.

$$|\{\mathbf{v}_1 \in \mathbb{F}_2^k : wt(\mathbf{v}_1) = i\}| = \binom{k}{i}, \tag{3.8}$$

$$|\{\mathbf{v}_2 \in \mathbb{F}_2^l : \mathbf{v}_2 \in \mathrm{Im}(\phi)\}| = |\mathbb{F}_2^k \backslash U_0| + 1 = 2 + \frac{k(k+1)}{2}, \tag{3.9}$$

$$|\{\mathbf{v}_2 \in \mathbb{F}_2^l : \mathbf{v}_2 \notin \mathrm{Im}(\phi)\}| = 2^l - 2 - \frac{k(k+1)}{2}. \tag{3.10}$$

The exact frequencies of weights in C_f depend on the values of k. We will only present two cases: when $k \notin S_1 \cup S_{-1} \cup S_3$ and the case when $k \in S_1$ and we will attempt to bring out the main differences between these two cases since other cases can be proved following similar ideas.

(1) Suppose that $k \notin S_1 \cup S_{-1} \cup S_3$. Lemma 6 implies that $A(i) \notin \{0, 1, -1\}$ for all $1 \leq i \leq k$. Hence, according to Eqs.(3.9) and (3.10), the multiplicities of 0 and $\pm 2^l$ are given by

$$\left|\left\{(\mathbf{v}_1, \mathbf{v}_2) : \mathbf{v}_1 \in \mathbb{F}_2^k, \mathbf{v}_2 \notin \mathrm{Im}(\phi)\right\}\right| = 2^k\left(2^l - 2 - \frac{k(k+1)}{2}\right),$$

$2^{k-2}k(k+1) + 2^{k-1}$, respectively. To prove, for instance, the latter, notice there are 2^{k-1} vectors $\mathbf{v}_1$ such that $\mathbf{v}_1 \cdot \phi^{-1}(\mathbf{v}_2) = 0$ for any choice of $\mathbf{v}_2$ in $\mathrm{Im}(\phi)\backslash\{\mathbf{0}_l\}$ (thus $\phi^{-1}(\mathbf{v}_2) \neq \mathbf{0}_k$), a set of size $\left|\mathbb{F}_2^k \backslash U_0\right| = \frac{k(k+1)}{2} + 1$.

On the other hand, Lemma 7 yields that the multiplicity of Walsh transform $(-1)^i A(i) 2^l$ in Eq.(3.7) is $\sum_{x \in \Gamma_i \cup \Delta_i} \binom{k}{x}$ where the sets Γ_i and Δ_i are given by Eqs.(2.4) and (2.5), respectively.

(2) Suppose now that $k \in S_1$ with $k = s^2 + 1$ for some integer s. On the one hand, it follows from Lemma 6 that $A(i) \neq \pm 1$ and thus the multiplicities of $\pm 2^l$ are $2^{k-2}k(k+1) + 2^{k-1}$ by Eq.(3.9). On the other hand, by Eqs.(3.8) and (3.10), one can deduce that the frequency of 0 is then given by

$$\begin{aligned}
&\left|\left\{(\mathbf{v}_1, \mathbf{0}_l) : wt(\mathbf{v}_1) = \frac{k+1 \pm s}{2}\right\}\right| + \left|\left\{(\mathbf{v}_1, \mathbf{v}_2) : \mathbf{v}_1 \in \mathbb{F}_2^k, \mathbf{v}_2 \notin \mathrm{Im}(\phi)\right\}\right| \\
=&\binom{k}{\frac{k+1+s}{2}} + \binom{k}{\frac{k+1-s}{2}} + 2^k\left(2^l - 2 - \frac{k(k+1)}{2}\right),
\end{aligned}$$

since $A(\frac{k+1\pm s}{2}) = 0$. The multiplicity of $(-1)^i A(i) 2^l$ for $i \neq \frac{k+1\pm s}{2}$ can be completed by using a similar approach as above.

Finally, we will examine the wideness and minimality of the code. It is an immediate result from Lemma 4 that C_f is minimal since Eq.(3.7) leads to

$$W_f(\mathbf{v}_1, \mathbf{v}_2) \pm W_f(\mathbf{w}_1, \mathbf{w}_2) \neq 2^r$$

for any pair of distinct $(\mathbf{v}_1, \mathbf{v}_2), (\mathbf{w}_1, \mathbf{w}_2) \in \mathbb{F}_2^k \times \mathbb{F}_2^l$.

It can be easily verified (see also Tables 1 and 2) that the maximum weight

$$w_{\max} = 2^{r-1} + 2^{l-1}(2^k - \frac{k(k+1)}{2} - 1), \tag{3.11}$$

corresponding to $wt(\mathbf{v}_1) = 0, wt(\mathbf{v}_2) = 0$. To compute the minimum weight, note that the quadratic function $A(x)$ has a critical point at $x = \frac{k+1}{2}$, thus the maximum attained at an integer i must lie near the endpoint (depending on the parity of i). Therefore, when k is odd, $(-1)^i A(i) \leq A(2) = A(k-1)$. On the other hand, when k is even, $(-1)^i A(i) \leq A(k)$. Thus, the minimum (nonzero) weight is achieved when $wt(\mathbf{v}_1) = k, wt(\mathbf{v}_2) = 0$ for k even and when $wt(\mathbf{v}_1) = 2, wt(\mathbf{v}_2) = 0$ for k odd, which gives

$$w_{\min} = 2^{r-1} - 2^{l-2}(k^2 - 3k + 2), \tag{3.12}$$

for even k and

$$w_{\min} = 2^{r-1} - 2^{l-2}(k^2 - 7k + 10), \tag{3.13}$$

for odd k. Therefore, combining Eqs.(3.11)-(3.13) together, we get $w_{\min}/w_{\max} \leq 1/2$ for $k \geq 8$, that is, C_f is a wide minimal code for $r \geq 13$. This completes the proof. □

Table 1: The weight distribution of C_f, where $1 \leq i \leq k$.

Weight	Multiplicity
$2^{r-1} + 2^{l-1}(2^k - \frac{k(k+1)}{2} - 1)$	1
$2^{r-1} + (-1)^{i+1}A(i)2^{l-1}$	$\sum_{x \in \Gamma_i \cup \Delta_i} \binom{k}{x}$ for $i \notin \Theta$
$2^{r-1} - 2^{l-1}$	$2^{k-2}k(k+1) + 2^{k-1} + N_1\binom{k}{\frac{1+k+s}{2}} + N_2\binom{k}{\frac{1+k-s}{2}}$
$2^{r-1} + 2^{l-1}$	$2^{k-2}k(k+1) + 2^{k-1} + N_3\binom{k}{\frac{1+k+s}{2}} + N_4\binom{k}{\frac{1+k-s}{2}}$
2^{r-1}	$2^r - 1 + 2^k(2^l - 2 - \frac{k(k+1)}{2}) + N_5\left(\binom{k}{\frac{1+k+s}{2}} + \binom{k}{\frac{1+k-s}{2}}\right)$
0	1

Table 2: Parameters in Table 1.

	$k \in S_{-1}$	$k \in S_1$	$k \in S_3$	$k \notin S_1 \cup S_{-1} \cup S_3$
N_1	$1 - \chi(\frac{k+1+s}{2})$	0	$\chi(\frac{k+1+s}{2})$	0
N_2	$1 - \chi(\frac{k+1-s}{2})$	0	$\chi(\frac{k+1-s}{2})$	0
N_3	$\chi(\frac{k+1+s}{2})$	0	$1 - \chi(\frac{k+1+s}{2})$	0
N_4	$\chi(\frac{k+1-s}{2})$	0	$1 - \chi(\frac{k+1-s}{2})$	0
N_5	0	1	0	0
Θ	$\{\frac{k+1\pm s}{2}\}$	$\{\frac{k+1\pm s}{2}\}$	$\{\frac{k+1\pm s}{2}\}$	$\emptyset$

We now give some examples to illustrate the correctness of Theorem 1.

Example 1 *(1) Let $r = 11$, i.e., $k = 6, l = 5$, which implies that $k \notin S_1 \cup S_{-1} \cup S_3$. Then C_f described in Theorem 1 is a minimal $[2048, 12, 864]$ code, whose weight enumerator polynomial is $1+z^{864}+35^{992}+704z^{1008}+2623z^{1024}+704z^{1040}+21z^{1056}+6z^{1184}+z^{1696}$. Note that in this case, the only solution (i, j) of $j = \frac{(k+1)\pm\sqrt{4i(-i+1+k)-(k^2+3)}}{2}$ that is relevant for the computation of the weight distribution is $(3, 2)$ (minus sign) (the other solution $(3, 5)$ (plus sign) leads to $i \equiv j \pmod 2$).*

(2) Let $r = 13$, i.e., $k = 7 = 2^2 + 3 \in S_3, l = 6$. Then C_f described in Theorem 1 is a minimal $[8192, 14, 3936]$ code, whose weight enumerator polynomial is $1 + 28z^{3936} + 1912z^{4064} + 12543z^{4096} + 1856z^{4128} + 35z^{4192} + 8z^{4576} + z^{7264}$.

(3) Let $r = 15$, i.e., $k = 8 = 3^2 - 1 \in S_{-1}, l = 7$. Then C_f described in Theorem 1 is a wide minimal $[32768, 16, 15040]$ code, whose weight enumerator polynomial is $1 + z^{15040} + 28z^{15808} + 56z^{16192} + 4764z^{16320} + 55807z^{16384} + 4792z^{16448} + 70z^{16576} + 8z^{16960} + 8z^{17728} + z^{30400}$. Observe that indeed $\frac{15040}{30400} = \frac{47}{95} < \frac{1}{2}$.

3.2 Wide binary minimal codes from the derivative of a Boolean function

In what follows, we first show that a different characteristic set, i.e., $U_1 = \{\mathbf{x} \in \mathbb{F}_2^k : wt(\mathbf{x}) \geq 3\}$, can actually give rise to wide minimal codes if a suitable derivative $D_\gamma(f)$ of f defined in Eq.(3.3) is used. Then, we combine the codewords of $C_{D_\gamma(f)}$ and of C_f to increase the dimension of the resulting wide minimal codes.

From Eqs.(2.3) and (3.2), the code $C_{D_\gamma(f)}$ is defined by

$$C_{D_\gamma(f)} = \left\{(u(f(\mathbf{x}) + f(\mathbf{x}+\gamma)) + \mathbf{v}\cdot\mathbf{x})_{\mathbf{x}\in\mathbb{F}_2^m} : u \in \mathbb{F}_2, \mathbf{v} \in \mathbb{F}_2^m\right\}, \tag{3.14}$$

where $f(\mathbf{x}) \neq \mathbf{v}\cdot\mathbf{x} + a$. For the choice of U_1, we will study the polynomial

$$B(i) = A(i) + (-1)^i A(i) = \begin{cases} 4i^2 - 4(k+1)i + k^2 + k + 2, & i \text{ is even}, \\ 0, & i \text{ is odd}, \end{cases} \tag{3.15}$$

for $1 \leq i \leq k$.

Lemma 8 Consider the polynomial $B(i)$ defined in (3.15). The following statements hold for $k \geq 6$.

(1) $B(i) = 0$ if and only if i is odd or i is even and $k = s^2 + 1 \in S_1$ and $i = \frac{s^2+2\pm s}{2}$.

(2) $B(i) = -2$ if and only if i is even and $k = s^2 + 3 \in S_3$ and $i = \frac{s^2+4\pm s}{2}$.

(3) $B(i) = 2$ if and only if i is even and $k = s^2 - 1 \in S_{-1}$ and $i = \frac{s^2\pm s}{2}$.

Similarly as in Sect 3.1, one can deduce that $\frac{1+k\pm s}{2}$ is a positive integer smaller than k and we also have the following lemma.

Lemma 9 Let i, j be two distinct even integers in $\{1, 2, \cdots, k\}$ and B be defined in (3.15). Then $B(i) = B(j)$ if and only if $i + j = k + 1$. In particular, this can only happen when k is odd.

For the code $C_{D_\gamma(f)}$ in Eq.(3.14), we have the following.

Theorem 2 Let $r \geq 11$ be an odd integer, $U_1 = \{\mathbf{x} \in \mathbb{F}_2^k : wt(\mathbf{x}) \geq 3\}$ and ϕ be a mapping such that it is an injection from $\mathbb{F}_2^k \backslash U_1$ to $\mathbb{F}_2^l \backslash \{\mathbf{0}_l\}$ and $\phi(\mathbf{x}) = \mathbf{0}_l$ for any $\mathbf{x} \in U_1$. Consider $\gamma = (\mathbf{1}_k, \mathbf{0}_l) \in \mathbb{F}_2^r$. Then the derivative code $C_{D_\gamma(f)}$ in Eq.(3.14) is a $\left[2^r, r+1, 2^{l-1}\left(k^2+k+2\right)\right]$ minimal code. Furthermore, if $r \geq 13$, then $C_{D_\gamma(f)}$ is wide. The weight distribution is displayed in Table 3 and the parameters related to k are given in Table 4, where $\Lambda = \{1 \leq j \leq k | j \text{ is even}\} \cap \{\frac{1+k\pm s}{2}\}$, $\Omega = \{1 \leq j \leq k | j \text{ is odd}\} \cup \{\frac{1+k\pm s}{2}\}$.

Proof: Similar as the proof of Theorem 1, we first determine the Walsh transform of the function $D_\gamma(f)$ given in Eq.(3.2). Note that $U_0 = U_1 + \mathbf{1}_k$. It is easy to prove (see also [8, Lemma 6])

$$\sum_{\mathbf{x} \in U_1} (-1)^{\mathbf{v}_1 \cdot \mathbf{x}} = \begin{cases} |U_1|, & \mathbf{v}_1 = \mathbf{0}_k, \\ -A(i), & wt(\mathbf{v}_1) = i, \end{cases} \tag{3.16}$$

where $|U_1| = |U_0| = 2^k - \frac{k(k+1)}{2} - 1$ and $A(i)$ is given by Eq.(3.4).

According to Lemma 5 and Eq.(3.16), we get

$$\begin{aligned} W_{D_\gamma(f)}(\mathbf{v}_1, \mathbf{v}_2) &= \sum_{\mathbf{x} \in \mathbb{F}_2^k} \sum_{\mathbf{y} \in \mathbb{F}_2^l} (-1)^{\phi(\mathbf{x}) \cdot \mathbf{y} + \phi(\mathbf{x}+\mathbf{1}_k) \cdot \mathbf{y} + \mathbf{v}_1 \cdot \mathbf{x} + \mathbf{v}_2 \cdot \mathbf{y}} \\ &= \sum_{\mathbf{x} \in (\mathbb{F}_2^k \backslash U_1)} \sum_{\mathbf{y} \in \mathbb{F}_2^l} (-1)^{\phi(\mathbf{x}) \cdot \mathbf{y} + \mathbf{v}_1 \cdot \mathbf{x} + \mathbf{v}_2 \cdot \mathbf{y}} + \sum_{\mathbf{x} \in (\mathbb{F}_2^k \backslash U_0)} \sum_{\mathbf{y} \in \mathbb{F}_2^l} (-1)^{\phi(\mathbf{x}+\mathbf{1}_k) \cdot \mathbf{y} + \mathbf{v}_1 \cdot \mathbf{x} + \mathbf{v}_2 \cdot \mathbf{y}} \\ &\quad + \sum_{\mathbf{x} \in (U_1 \cap U_0)} \sum_{\mathbf{y} \in \mathbb{F}_2^l} (-1)^{\mathbf{v}_1 \cdot \mathbf{x} + \mathbf{v}_2 \cdot \mathbf{y}} \\ &= \begin{cases} \left(2^k - k(k+1) - 2\right) 2^l, & \mathbf{v}_1 = \mathbf{0}_k, \mathbf{v}_2 = \mathbf{0}_l, \\ -\left(A(i) + (-1)^i A(i)\right) 2^l, & wt(\mathbf{v}_1) = i, \mathbf{v}_2 = \mathbf{0}_l, \\ \left(1 + (-1)^{\mathbf{v}_1 \cdot \mathbf{1}_k}\right) (-1)^{\mathbf{v}_1 \cdot \phi^{-1}(\mathbf{v}_2)} 2^l, & \mathbf{v}_2 \in \mathrm{Im}(\phi) \backslash \{\mathbf{0}_l\}, \\ 0, & \mathbf{v}_2 \notin \mathrm{Im}(\phi), \end{cases} \end{aligned} \tag{3.17}$$

where $i = 1, 2, \ldots, k$.

Now, we are ready to determine the frequencies in the Walsh spectrum of the values given in Eq.(3.17). Although the specification of the weight distribution of the code is similar to that of Theorem 1, we will provide some details for the reader's convenience. We only present the case when k is of the form $s^2 + 1$ since the other cases can be proved with the same idea.

Note that the function $-B(i)$ has a maximum at $\frac{k+1}{2}$. Thus the Walsh value $(2^k - k^2 - k - 2)2^l$ in Eq.(3.17) is attained only once and it corresponds to the minimum weight in $C_{D_\gamma(f)}$. The number of balanced codewords corresponds to the number of linear functions plus the frequency of the zero Walsh values in Eq.(3.17), which includes the following four possibilities.

(i) $\mathbf{v}_2 \in \mathbb{F}_2^l$ and $\mathbf{v}_2 \notin \mathrm{Im}(\phi)$ gives $2^k(2^l - \frac{k^2+k}{2} - 2)$ occurrences.

(ii) $B(i) = 0$, $1 \le i \le k$, which yields $2^{k-1} + \sum_{x\in\Lambda} \binom{k}{x}$ codewords according to Lemma 8, where

$$\Lambda = \{j \in \{1, \ldots, k\} | j \text{ is even}\} \cap \left\{ \frac{s^2 \pm s + 2}{2} \right\}.$$

(iii) $\mathbf{v}_2 \in \mathrm{Im}(\phi) \backslash \{\mathbf{0}_l\}$ and $1 + (-1)^{\mathbf{v}_1 \cdot \mathbf{1}_k} = 0$, i.e., $\mathbf{v}_1$ has odd weight.

(iv) The case $u = 0$ which corresponds to $2^r - 1$ codewords.

Thus the total number of balanced codewords is

$$2^r - 1 + 2^k(2^l - \frac{k(k+1)}{2} - 2) + 2^{k-1} + \sum_{x\in\Lambda} \binom{k}{x} + 2^{k-1}\left(\frac{k(k+1)}{2} + 1\right).$$

To count the frequency of 2^{l+1}, note that $\left(1 + (-1)^{\mathbf{v}_1 \cdot \mathbf{1}_k}\right)(-1)^{\mathbf{v}_1 \cdot \phi^{-1}(\mathbf{v}_2)}$ equals 2 when $\mathbf{v}_1$ has even weight and $\mathbf{v_1}$ is orthogonal to $\phi^{-1}(\mathbf{v}_2)$ for $\mathbf{v}_2 \in \mathrm{Im}(\phi) \backslash \{\mathbf{0}_l\}$. That is, there are $2^{k-3}k(k+1) + 2^{k-1}$ such values. Similarly, the frequency of -2^{l+1} equals $2^{k-2}(\frac{k(k+1)}{2})$.

When $B(i) \notin \{0, 2, -2\}$, the values $-\left(A(i) + (-1)^i A(i)\right) 2^l$ are different from each other for even i with $1 \le i \le k$, when k is even, thus its multiplicity is $\binom{k}{i}$. Otherwise, if k is odd, its multiplicity equals $\sum_{x\in\{i,k+1-i\}} \binom{k}{x}$ by Lemma 9. This completes the description of the weight distribution.

Next, we show $C_{D_\gamma(f)}$ is minimal and wide. From Eq.(3.17), we see that

$$W_{D_\gamma(f)}(\mathbf{v}_1, \mathbf{v}_2) \pm W_{D_\gamma(f)}(\mathbf{w}_1, \mathbf{w}_2) \neq 2^r$$

for any pair of distinct $(\mathbf{v}_1, \mathbf{v}_2), (\mathbf{w}_1, \mathbf{w}_2) \in \mathbb{F}_2^k \times \mathbb{F}_2^l$. It follows from Lemma 4 that $C_{D_\gamma(f)}$ is minimal. Note that the minimum weight is clearly

$$w_{\min} = 2^{l-1}(k^2 + k + 2), \tag{3.18}$$

corresponding to $wt(\mathbf{v}_1) = 0, wt(\mathbf{v}_2) = 0$. The maximum weight corresponds to the vectors $wt(\mathbf{v}_1) = k, wt(\mathbf{v}_2) = 0$, when k is even, and $wt(\mathbf{v}_1) = 2, wt(\mathbf{v}_2) = 0$, when k is odd. Thus,

$$w_{\max} = \begin{cases} 2^{r-1} + 2^{l-1}(k^2 - 3k + 2), & k \text{ is even}, \\ 2^{r-1} + 2^{l-1}(k^2 - 7k + 10), & k \text{ is odd}. \end{cases} \tag{3.19}$$

Therefore, combining Eqs.(3.18) and (3.19) together, we get $w_{\min}/w_{\max} \le 1/2$ for $k \ge 7$, i.e., $\mathcal{C}_{D_\gamma(f)}$ is wide minimal. This completes the proof. □

Table 3: The weight distribution of $\mathcal{C}_{D_\gamma(f)}$, where $1 \le i \le k$.

Weight	Multiplicity
$2^{l-1}\left(k^2+k+2\right)$	1
$2^{r-1}+B(i)2^l$	$\sum_{x\in\Gamma_i}\binom{k}{x}$ for $i \notin \Theta$
$2^{r-1}+2^l$	$2^{k-3}k(k+1)+N_1\sum_{x\in\Lambda}\binom{k}{x}$
$2^{r-1}-2^l$	$2^{k-1}+2^{k-3}k(k+1)+N_2\sum_{x\in\Lambda}\binom{k}{x}$
2^{r-1}	$2^r-1+2^k(2^l-2-\frac{k(k+1)}{2})+N_3\sum_{x\in\Lambda}\binom{k}{x}$ $+2^{k-1}(\frac{k(k+1)}{2}+2)$
0	1

Table 4: Parameters in Table 3.

	$k\in S_{-1}$	$k\in S_1$	$k\in S_3$	$k\notin S_1\cup S_{-1}\cup S_3$
N_1	1	0	0	0
N_2	0	0	1	0
N_3	0	1	0	0
Θ	Ω	Ω	Ω	$\{1\le j\le k \mid j \text{ is odd}\}$

Example 2 *(1) Let $r=11$, i.e., $k=6\notin S_1\cup S_{-1}\cup S_3, l=5$. Then $\mathcal{C}_{D_\gamma(f)}$ described in Theorem 2 is a minimal $[2048,12,704]$ code, whose weight enumerator polynomial is $1+z^{704}+15z^{960}+368z^{992}+3359z^{1024}+336z^{1056}+15z^{1088}+z^{1344}$.*

(2) Let $r=13$, i.e., $k=7\in S_3, l=6$ and $k\pm s\equiv 1 \pmod 4$. Then $\mathcal{C}_{D_\gamma(f)}$ described in Theorem 2 is a wide minimal $[8192,14,1856]$ code, whose weight enumerator polynomial is $1+z^{1856}+35z^{3904}+960z^{4032}+14463z^{4096}+896z^{4160}+28z^{4416}$.

Now, we use the codewords of the codes specified in Theorem 1 together with those given in Theorem 2 to increase the dimension of the resulting codes by one. Precisely, we define $C_f\oplus C_{D_\gamma(f)}$ as

$$C_f\oplus C_{D_\gamma(f)} := \left\{(af(\mathbf{x})+bD_\gamma f(\mathbf{x})+\mathbf{v}\cdot\mathbf{x})_{\mathbf{x}\in\mathbb{F}_2^n} : a,b\in\mathbb{F}_2, \mathbf{v}\in\mathbb{F}_2^n\right\}. \tag{3.20}$$

From the results of [8, Theorem 1], Theorems 1 and 2, we can similarly obtain the following theorem. Its proof is lengthy and similar to that of [16, Theorem 5], thus we omit it.

Theorem 3 Let the symbols be given as above. Then the code $C_f\oplus C_{D_\gamma(f)}$ given by Eq.(3.20), is a $\left[2^r, r+2, 2^{l-1}\left(k^2+k+2\right)\right]$ wide binary minimal code.

Remark 1 *The codes $C_{D_\gamma(f)}$ and $C_f\oplus C_{D_\gamma(f)}$, presented in Th.2 and Th.3, respectively, attain a larger minimum distance than the ones introduced in [16], obtained using the same method, i.e., Th.4 and Th.5 in [16]. Namely, the number $2^{l-1}\left(k^2+k+2\right)$ is always larger than $2^l(k+1)$.*

4 The general case

In this section, we present the general construction of (wide) minimal codes using the previously described form. For $I \subseteq \{1, \ldots, n\}$, define the subset $\mathcal{U}_I$ of $\mathbb{F}_2^m$ as

$$\mathcal{U}_I := \{\mathbf{v} \in \mathbb{F}_2^m : wt(\mathbf{v}) \notin I\}. \tag{4.1}$$

For instance, in $\mathbb{F}_2^k$, the sets defined in the previous sections are a special case of this definition, namely, $\mathcal{U}_{\{0,1,2\}} = U_1$ and $\mathcal{U}_{\{k-2,k-1,k\}} = U_0$. Since $\mathcal{U}_I$ contains every vector whose weight is not in I, then we get the following result.

Lemma 10 Let m be any positive integer and $I \subseteq \{1, \ldots, m\}$. Consider the subset $\mathcal{U}_I$ given in (4.1). The following holds

$$\sum_{\mathbf{x} \in \mathcal{U}_I} (-1)^{\mathbf{v}\cdot\mathbf{x}} = \begin{cases} |\mathcal{U}_I| = 2^m - \sum_{i \in I} \binom{m}{i}, & \mathbf{v} = \mathbf{0}_m, \\ -\sum_{j \in I} P_j(i), & wt\,(\mathbf{v}) = i, \end{cases} \tag{4.2}$$

for any $\mathbf{v} \in \mathbb{F}_2^m$.

For suitable choices of I, one can explicitly obtain the values in the previous sum. For our purposes, it will be enough to consider subsets I for which $|\mathcal{U}_I| > 2^{k-1}$. Moreover, since the Krawtchouck polynomials satisfy Eq.(2.2), we will restrict to cases when $I \subseteq \{0, 1, 2\} \cup \{k-2, k-1, k\}$. Our previous discussion together with [7, 8, 13, 16] essentially cover the cases when I equals $\{0, 1\}, \{k-1, k\}, \{0, 1, 2\}, \{k-2, k-1, k\}$ as it will become obvious after the following lemma.

Lemma 11 Let r be an odd integer with $r \geq 7$. Let $I \subseteq \{0, 2, \ldots, k\}$. Consider the function f defined in Eq.(3.3), where ϕ is an injective mapping from $\mathbb{F}_2^k \backslash \mathcal{U}_I$ to $\mathbb{F}_2^l \backslash \{\mathbf{0}_l\}$ and $\phi(\mathbf{x}) = \mathbf{0}_l$ for any $\mathbf{x} \in \mathcal{U}_I$. Then, the Walsh transform of f takes the following values

$$W_f\,(\mathbf{v}_1, \mathbf{v}_2) = \begin{cases} -2^l |\mathcal{U}_I|, & \mathbf{v}_1 = \mathbf{0}_k, \mathbf{v}_2 = \mathbf{0}_l, \\ 2^l \sum_{j \in I} P_j(i), & wt\,(\mathbf{v}_1) = i, \mathbf{v}_2 = \mathbf{0}_l, \\ -(-1)^{\mathbf{v}_1 \cdot \phi^{-1}(\mathbf{v}_2)} 2^l, & \mathbf{v}_2 \in \mathrm{Im}(\phi) \backslash \{\mathbf{0}_l\}, \\ 0, & \mathbf{v}_2 \notin \mathrm{Im}(\phi), \end{cases}$$

where $i = 1, 2, \ldots, k$.

Proof: The result follows immediately from Lemma 10. □

Comparing the previous result with Lemma 5 and Theorem 1, one can see that the key for the results in Sect.3 is that the polynomial $(-1)^i A(i) = P_k(i) + P_{k-1}(i) + P_{k-2}(i)$ has degree two, which implies that it is easy to find the critical points for $A(i) = \pm 1$ or $A(i) = 0$, thus allowing

us to fully describe the weight distribution of the codes. In the following, we will illustrate this general method by considering simple subsets I that yield polynomials of low degree (denoted by $A_I(i)$), namely, we will select I to be $\{0, k-2, k-1\}$, $\{0, 1, k-1\}$ and $\{0, 1, k\}$. Other similar choices of I can be handled analogously and are left as an exercise to the interested reader.

4.1 The case $I = \{0, k-1, k-2\}$.

Throughout this section, set $I = \{0, k-1, k-2\}$. The associated polynomial is now the quadratic polynomial

$$A_I(i) = (-1)^i(2i^2 - 2i(k+1) + \frac{k(k+1)}{2}) + 1,$$

where $1 \leq i \leq k$. Similar to Lemma 6, we can easily derive the following properties of $A_I(i)$.

Lemma 12 For $1 \leq i \leq k$, we have,

(1) $A_I(i) = 0$ if and only if $k = s^2 - 3 \in S_{-3}$, $i = \frac{s^2-2\pm s}{2}$ is odd, or $k = s^2 + 1 \in S_1$ and $i = \frac{s^2+2\pm s}{2}$ is even.

(2) $A_I(i) = -1$ if and only if $k = s^2 - 5 \in S_{-5}$ and $i = \frac{s^2-4\pm s}{2}$ is odd, or $k = s^2 + 3 \in S_3$ and $i = \frac{s^2+4\pm s}{2}$ is even.

(3) $A_I(i) = 1$ if and only if $k = s^2 - 1 \in S_{-1}$ and $i = \frac{s^2\pm s}{2}$ is odd, or $k = s^2 - 1 \in S_{-1}$ and $i = \frac{s^2\pm s}{2}$ is even.

Observe that the sets S_u are almost always mutually disjoint with the unique exception $k = 4 \in S_3 \cap S_{-5}$ giving $i = 2$, $j = 1$ and $A_I(i) = A_I(j) = -1$. This implies that the conditions are almost always mutually exclusive.

A result similar to Lemma 7 can now be derived.

Lemma 13 Let $i \neq j$ be two integers in $\{1, \ldots, k\}$.

(1) If $i \equiv j \pmod 2$, then $A_I(i) = A_I(j)$ if and only if $i + j = k + 1$. In particular, this can only happen when k is odd.

(2) If $i \not\equiv j \pmod 2$, then $A_I(i) = A_I(j)$ if and only if $j = a^{\pm}_{-1,i}$.

We now have all the ingredients to state and prove the following.

Theorem 4 Let r be an odd integer with $r \geq 7$. Let $I = \{0, k-1, k-2\}$. Consider the function f defined in Eq.(3.3) where ϕ is an injective mapping from $\mathbb{F}_2^k \backslash \mathcal{U}_I$ to $\mathbb{F}_2^l \backslash \{\mathbf{0}_l\}$ and $\phi(\mathbf{x}) = \mathbf{0}_l$ for any $\mathbf{x} \in \mathcal{U}_I$. Then the code C_f in Eq.(2.3) is a $[2^r, r+1, d]$ minimal code, where

$$d = \begin{cases} 2^{r-1} - 2^{l-2}(k^2 - 7k + 10), & k \text{ is odd}, \\ 2^{r-1} - 2^{l-2}(k^2 - 3k + 2), & k \text{ is even}. \end{cases}$$

Furthermore, if $r \geq 15$, then C_f is wide. The weight distributions are given in Table 5, whose parameters related to k and the set Λ_s are shown in Tables 6 and 7, respectively.

Proof: The proof is similar to that of Theorem 1, so we only present a sketch here. Lemma 11 implies that

$$W_f(\mathbf{v}_1, \mathbf{v}_2) = \begin{cases} -\left(2^k - \frac{k(k+1)}{2} - 1\right) 2^l, & \mathbf{v}_1 = \mathbf{0}_k, \mathbf{v}_2 = \mathbf{0}_l, \\ 2^l A_I(i), & wt(\mathbf{v}_1) = i, \mathbf{v}_2 = \mathbf{0}_l, \\ -(-1)^{\mathbf{v}_1 \cdot \phi^{-1}(\mathbf{v}_2)} 2^l, & \mathbf{v}_2 \in \mathrm{Im}(\phi) \backslash \{\mathbf{0}_l\}, \\ 0, & \mathbf{v}_2 \notin \mathrm{Im}(\phi), \end{cases} \tag{4.3}$$

for $i = 1, 2, \ldots, k$.

The exact frequencies of weights in C_f depend on the values of k. We will describe the case when $k \notin \cup_{j \in \{\pm 1, \pm 3, -5\}} S_j$ and when $k \in S_{-3}$ since the other cases can be proved using a similar reasoning.

(1) Suppose that $k \notin \cup_{j \in \{\pm 1, \pm 3, -5\}} S_j$. Lemma 12 implies that there is no solution for $A_I(i) = 0, 1, -1$. Hence the multiplicities of $0, 2^l$, and -2^l are given by $2^k\left(2^l - 2 - \frac{k(k+1)}{2}\right)$, $2^{k-2}k(k+1)$ and $2^{k-2}k(k+1) + 2^k$, respectively. Lemma 13, Eq.(2.4) and Eq.(2.5) yield the frequency of $2^l A_I(i)$ in Eq.(4.3) to be $\sum_{x \in \Gamma_i \cup \Delta_i} \binom{k}{x}$.

(2) If $k \in S_{-3}$ with $k = s^2 - 3$, then by Lemma 12, $A_I(i) \neq \pm 1$. This implies that the multiplicities of 2^l and -2^l are $2^{k-2}k(k+1)$ and $2^{k-2}k(k+1) + 2^k$, respectively. Now, to compute the frequency of 0, we define

$$\Lambda_s := \begin{cases} \{\frac{s^2 \pm s - 2}{2}\}, & s \equiv 0 \pmod 4, \\ \{\frac{s^2 - s - 2}{2}\}, & s \equiv 1 \pmod 4, \\ \emptyset, & s \equiv 2 \pmod 4, \\ \{\frac{s^2 + s - 2}{2}\}, & s \equiv -1 \pmod 4. \end{cases}$$

Thus, the multiplicity of 0 in the Walsh spectrum is given by $\sum_{\rho \in \Lambda_s} \binom{k}{\rho} + 2^k\left(2^l - 2 - \frac{k(k+1)}{2}\right)$. Finally, the multiplicity of $A_I(i)2^l$ for $i \notin \Lambda_s$ is attained $\sum_{j \in \Gamma_i \cup \Delta_i} \binom{k}{j}$ times.

Following the same reasoning as in the proof of Theorem 1, we can obtain that C_f is minimal using the equation below

$$W_f(\mathbf{v}_1, \mathbf{v}_2) \pm W_f(\mathbf{w}_1, \mathbf{w}_2) \neq 2^r, (\mathbf{v}_1, \mathbf{v}_2) \neq (\mathbf{w}_1, \mathbf{w}_2) \in \mathbb{F}_2^k \times \mathbb{F}_2^l.$$

Clearly, the maximum weight is

$$w_{\max} = 2^{r-1} + 2^{l-1}(2^k - \frac{k(k+1)}{2} - 1).$$

If $wt(\mathbf{v}_1) = k$ is even and $wt(\mathbf{v}_2) = 0$, we have

$$w_{\min} = 2^{r-1} - 2^{l-2}(k^2 - 3k + 2).$$

If k is odd and $wt(\mathbf{v}_1) = 2, wt(\mathbf{v}_2) = 0$, we have

$$w_{\min} = 2^{r-1} - 2^{l-2}(k^2 - 7k + 10).$$

Thus, the code is wide and minimal for $k \geq 8$. □

Table 5: The weight distribution of C_f, where $1 \leq i \leq k$.

Weight	Multiplicity
$2^{r-1} + 2^{l-1}(2^k - \frac{k(k+1)}{2} - 1)$	1
$2^{r-1} - 2^l A_I(i)$	$\sum_{j\in\Gamma_i\cup\Delta_i} \binom{k}{j}$ for $i \notin \Theta$
$2^{r-1} - 2^{l-1}$	$2^{k-2}k(k+1) + N_1$
$2^{r-1} + 2^{l-1}$	$2^{k-2}k(k+1) + 2^k + N_2$
2^{r-1}	$2^{r+1} - 1 - 2^{k-1}(k(k+1)+4) + N_3$
0	1

Table 6: Parameters in Table 5.

	$k \in S_1 \cup S_{-3}$	$k \in S_{-5} \cup S_3$	$k \in S_{-1}$	$k \notin \cup_{j\in\{\pm1,\pm3,-5\}} S_j$
N_1	0	0	$\binom{k}{\frac{s^2-s}{2}} + \binom{k}{\frac{s^2+s}{2}}$	0
N_2	0	$\sum_{j\in\Lambda_s} \binom{k}{j}$	0	0
N_3	$\sum_{j\in\Lambda_s} \binom{k}{j}$	0	0	0
Θ	Λ_s	Λ_s	Λ_s	$\emptyset$

Table 7: The values of the set Λ_s in Table 6.

	$k \in S_{-3}$	$k \in S_1$	$k \in S_{-5}$	$k \in S_3$	$k \in S_{-1}$
$s \equiv 0 \pmod 4$	$\{\frac{s^2\pm s-2}{2}\}$	$\emptyset$	$\emptyset$	$\{\frac{s^2\pm s+4}{2}\}$	$\{\frac{s^2\pm s}{2}\}$
$s \equiv 1 \pmod 4$	$\{\frac{s^2-s-2}{2}\}$	$\{\frac{s^2+s+2}{2}\}$	$\{\frac{s^2-s-4}{2}\}$	$\{\frac{s^2-s+4}{2}\}$	$\{\frac{s^2\pm s}{2}\}$
$s \equiv 2 \pmod 4$	$\emptyset$	$\{\frac{s^2\pm s+2}{2}\}$	$\{\frac{s^2\pm s-4}{2}\}$	$\emptyset$	$\{\frac{s^2\pm s}{2}\}$
$s \equiv -1 \pmod 4$	$\{\frac{s^2+s-2}{2}\}$	$\{\frac{s^2-s+2}{2}\}$	$\{\frac{s^2+s-4}{2}\}$	$\{\frac{s^2+s+4}{2}\}$	$\{\frac{s^2\pm s}{2}\}$

Example 3 *(1) Let $r = 11$, i.e., $k = 6 = 3^2 - 3 \in S_{-3}, l = 5$. Then C_f described in Theorem 4 is a wide minimal $[2048, 12, 864]$ code, whose weight enumerator polynomial is $1 + z^{864} + 20z^{960} + 15z^{992} + 672z^{1008} + 2629^{1024} + 736z^{1040} + 15z^{1056} + 6z^{1152} + z^{696}$.*

(2) Let $r = 13$, *i.e.,* $k = 7 = 2^2 + 3 \in S_3, l = 6$. *Then* C_f *described in Theorem 4 is a minimal* $[8192, 14, 3936]$ *code, whose weight enumerator polynomial is* $1 + 28z^{3936} + 56z^{4000} + 1792z^{4064} + 12543^{4096} + 1920^{4128} + 35z^{4192} + 8z^{4512} + z^{7264}$.

We have fully derived similar approaches for $I = \{0, 1, k\}$ and $I = \{0, 1, k-1\}$. These theorems can be handled in a similar fashion as for the cases above. They are lengthy but simpler, thus we present such detailed proofs in the appendix.

4.2 The case $I = \{0, 1, k\}$.

We now study the case $I = \{0, 1, k\}$, where the associated polynomial $A_I(i)$ is the linear polynomial $-2i + k + (-1)^i + 1$ and $A_I(0) = 2^k - |\mathcal{U}_I|$.

Theorem 5 Let r be an odd integer with $r \geq 7$. Let $I = \{0, 1, k\}$. Consider the function f defined in Eq.(3.3), where ϕ is an injective mapping from $\mathbb{F}_2^k \backslash \mathcal{U}_I$ to $\mathbb{F}_2^l \backslash \{\mathbf{0}_l\}$ and $\phi(\mathbf{x}) = \mathbf{0}_l$ for any $\mathbf{x} \in \mathcal{U}_I$. Then the code C_f in Eq.(2.3) is a $[2^r, r+1, 2^{r-1} - 2^{l-1}(k-2)]$ minimal code. Furthermore, if $r \geq 11$, then C_f is wide. The weight distributions are displayed in Table 8, where the parameters related to k are given in Table 9.

Table 8: The weight distribution of C_f, where $1 \leq i \leq k-1$ is odd.

Weight	Multiplicity
$2^{r-1} + 2^{l-1}(2^k - k - 2)$	1
$2^{r-1} - 2^{l-1}(k - 2i)$	$\binom{k}{i} + \binom{k}{i+1}$ for $i \notin \Theta$
$2^{r-1} - 2^{l-1}$	$2^{k-1}(k+1) + N_1$
$2^{r-1} + 2^{l-1}$	$2^{k-1}(k+1) + 2^k + N_2$
2^{r-1}	$2^r - 1 + 2^k(2^l - k - 3) + N_3$
0	1

Table 9: Parameters in Table 8.

	$k \equiv 0 \pmod 4$	$k \equiv 1 \pmod 4$	$k \equiv 2 \pmod 4$	$k \equiv -1 \pmod 4$
N_1	0	0	0	$\binom{k}{\frac{k-1}{2}} + \binom{k}{\frac{k+1}{2}}$
N_2	0	$\binom{k}{\frac{k+1}{2}} + \binom{k}{\frac{k+3}{2}}$	0	0
N_3	0	0	$\binom{k}{\frac{k+2}{2}} + \binom{k}{\frac{k}{2}}$	0
Θ	$\emptyset$	$\{\frac{k+1}{2}\}$	$\{\frac{k}{2}\}$	$\{\frac{k-1}{2}\}$

Example 4 *(1) Let $r = 7$, i.e., $k = 4 \equiv 0 \pmod 4, l = 3$. Then C_f described in Theorem 5 is a minimal $[128, 8, 56]$ code, whose weight enumerator polynomial is $1 + 10z^{56} + 40z^{60} + 143z^{64} + 56z^{68} + 5z^{72} + z^{104}$.*

(2) Let $r = 9$, i.e., $k = 5 \equiv 1 \pmod 4, l = 4$. Then C_f described in Theorem 5 is a minimal $[512, 10, 232]$ code, whose weight enumerator polynomial is $1+15z^{232}+96z^{248}+767z^{256}+143z^{264}+z^{296} + z^{456}$.

(3) Let $r = 11$, i.e., $k = 6 \equiv 2 \pmod 4, l = 5$. Then C_f described in Theorem 5 is a wide minimal $[2048, 12, 960]$ code, whose weight enumerator polynomial is $1 + 21z^{960} + 224^{1008} + 3554z^{1024} + 288z^{1040} + 7z^{1088} + z^{1920}$. Note that indeed C_f is wide as $\frac{960}{1920} = \frac{1}{2}$.

(4) Let $r = 13$, i.e., $k = 7 \equiv -1 \pmod 4, l = 6$. Then C_f described in Theorem 5 is a minimal $[8192, 14, 3936]$ code, whose weight enumerator polynomial is $1 + 28z^{3936} + 582^{4064} + 15103^{4096} + 640z^{4128} + 28z^{4192} + z^{4320} + z^{7904}$.

4.3 The case $I = \{0, 1, k-1\}$.

Consider $I = \{0, 1, k-1\}$. This case is similar to the one described in the previous section, however, some care must be taken when specifying all details. The associated polynomial $A_I(i)$ is the linear polynomial $((-1)^i + 1)(-2i + k) + 1$ and, again, $A_I(0) = 2^k - |\mathcal{U}_I|$.

Theorem 6 Let r be an odd integer with $r \geq 9$. Let $I = \{0, 1, k-1\}$. Consider the function f defined in Eq.(3.3), where ϕ is an injective mapping from $\mathbb{F}_2^k \backslash \mathcal{U}_I$ to $\mathbb{F}_2^l \backslash \{\mathbf{0}_l\}$ and $\phi(\mathbf{x}) = \mathbf{0}_l$ for any $\mathbf{x} \in \mathcal{U}_I$,. Then the code C_f in Eq.(2.3) is a $[2^r, r+1, 2^{r-1} - 2^{l-1}(2k-7)]$ minimal code. Furthermore, if $r \geq 15$, then C_f is wide. Its weight distribution is given in Table 10, where the parameters related to k are given in Table 11.

Table 10: The weight distribution of C_f, where $1 \leq i \leq k$ is even.

Weight	Multiplicity
$2^{r-1} + 2^{l-1}(2^k - 2k - 1)$	1
$2^{r-1} - 2^{l-1}(-4i + 2k + 1)$	$\binom{k}{i}$ for $i \notin \Theta$
$2^{r-1} - 2^{l-1}$	$2^k k + 2^{k-1} + N_1$
$2^{r-1} + 2^{l-1}$	$2^k(k+1) + N_2$
2^{r-1}	$2^r - 1 + 2^k(2^l - 2k - 2)$
0	1

Table 11: Parameters in Table 10.

	$k \equiv 0 \pmod 4$	$k \equiv -1 \pmod 4$	$k \equiv 1 \pmod 4$ or $k \equiv 2 \pmod 4$
N_1	$\binom{k}{\frac{k}{2}}$	0	0
N_2	0	$\binom{k}{\frac{k+1}{2}}$	0
Θ	$\{\frac{k}{2}\}$	$\{\frac{k+1}{2}\}$	$\emptyset$

Example 5 *(1) Let $r = 9$, $k = 5 \equiv 1 \pmod 4, l = 4$. Then C_f described in Theorem 6 is a minimal $[512, 10, 232]$ code, whose weight enumerator polynomial is $1 + 10z^{232} + 176z^{248} + 639z^{256} + 192z^{264} + 5z^{296} + z^{424}$.*

(2) Let $r = 11$, $k = 6 \equiv 2 \pmod 4, l = 5$. Then C_f described in Theorem 6 is a wide minimal $[2048, 12, 944]$ code, whose weight enumerator polynomial $1 + 15z^{944} + 416z^{1008} + 3199z^{1024} + 448z^{1040} + 15z^{1072} + z^{1200} + z^{1840}$.

(3) Let $r = 13$, i.e., $k = 7 \equiv -1 \pmod 4, l = 6$. Then C_f described in Theorem 6 is a minimal $[8192, 14, 3872]$-code, whose weight enumerator polynomial is $1 + 21z^{3872} + 960^{4064} + 14335z^{4096} + 1059z^{4128} + 7z^{4384} + z^{7712}$.

(4) Let $r = 15$, i.e., $k = 8 \equiv 0 \pmod 4, l = 7$. Then C_f described in Theorem 6 is a wide minimal $[32768, 16, 15808]$ code, whose weight enumerator polynomial is $1 + 28z^{15808} + 2246z^{16320} + 60927z^{16384} + 2304z^{16448} + 28z^{16832} + z^{17344} + z^{31680}$. Note that indeed $\frac{15808}{31680} = \frac{247}{495} < \frac{1}{2}$.

Remark 2 *The code C_f in Theorem 5 has the largest minimum distance (for the given parameters), i.e., $2^{r-1} - 2^{l-1}(k-2)$, among the explicit binary codes constructed using the method of Krawtchouk polynomials ([7, 8, 13, 16]) except for $U = \{k, k-1\}$ when k is even, which yields a minimum distance of $2^{r-1} - 2^{l-1}(k-3)$ [Theorem 2, [16]].*

5 Conclusion

In this paper, we have constructed several classes of new wide binary minimal codes by selecting appropriate Boolean functions in the GMM class. The methods used in this paper are based on [7, 8, 16], namely, we employed Krawtchouk polynomials to compute the Walsh distributions of the chosen Boolean functions. The lengths, dimensions and weight distributions of these codes have been determined. The results show that some of the new codes achieve a larger minimum distance than those in [16]. Furthermore, we used the derivative method devised in [16] to increase the dimension of our codes. To deepen the understanding of the Krawtchouk-polynomials method, we have studied the general case by using suitable choices for subsets in $\{1, \ldots, k\}$. We have described some feasible choices for which we were able to study the minimality and wideness properties of such codes. While these subsets of $\{1, \ldots, k\}$ give simple descriptions of the codes, other more involved selections may give rise to possibly better codes

(e.g., having a larger minimum distance). However, the difficulty lies in the analysis of specific cubic or quartic polynomials. We leave this as a research challenge.

6 Declarations

6.1 Ethical Approval and Consent to participate

There are no ethical issues concerning the submitted article since its topic is coding theory and cryptography and therefore it does not include a study on humans or animals.

6.2 Consent for publication

The authors give their consent for possible publication of the submitted material.

6.3 Availability of supporting data

There is no supporting data related to the submitted article.

6.4 Competing interests

There are no competing interests with other researchers or scientific institutions.

6.5 Funding

Xiaoni Du is partially supported by the National Natural Science Foundation of China (Grant No.62172337) and the Key Project of Gansu Natural Science Foundation (Grant No.23JRRA685). René Rodríguez is partly supported by the Slovenian Research Agency (research projects J1-4084, J1-2451 and N1-0159).

6.6 Authors' contributions

All authors have contributed equally.

6.7 Acknowledgments

The authors would like to thank the anonymous reviewers and the Associate Editor for their helpful comments that greatly improved the presentation and quality of this paper.

References

[1] Alkavur, S.: A study on Multisecret-Sharing schemes based on linear codes. Emerging Science Journal, vol. 4, no. 4, 263-271 (2020)

[2] Ashikhmin, A., Barg, A.: Minimal vectors in linear codes. IEEE Transactions on Information Theory, vol. 44, no. 5, 2010-2017 (1998)

[3] Bonini, M., Borello, M.: Minimal linear codes arising from blocking sets. Journal of Algebraic Combinatorics, vol. 53, 327-341 (2021)

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

[5] Choi, S. T., Kim, J. Y., No, J. S., Chung, H.: Weight distribution of some cyclic codes. 2012 IEEE International Symposium on Information Theory Proceedings, 2901-2903 (2012)

[6] Cohen, G. D., Mesnager, S., Patey, A.: On minimal and quasi-minimal linear codes. IMA International Conference on Cryptography and Coding. Springer, Berlin, Heidelberg, 85-98 (2013)

[7] Ding, C., Heng, Z., Zhou, Z.: Minimal binary linear codes. IEEE Transactions on Information Theory, vol. 64, no. 10, 6536-6545 (2018)

[8] Du, X., Hu, J., Jin, W., Sun, Y.: Construction of two classes of minimal binary linear codes. Journal of Electronics and Information Technology, vol. 44, no. 10, 7 (2022)

[9] Heng, Z., Ding, C., Zhou, Z.: Minimal linear codes over finite fields. Finite Fields and Their Applications, vol. 54, 176-196 (2018)

[10] Li, X., Yue, Q.: Four classes of minimal binary linear codes with $w_{min}/w_{max} < 1/2$ derived from Boolean functions. Designs, Codes and Cryptography, vol. 88, 257-271 (2020)

[11] MacWilliams, F. J., Sloane, N. J. A.: The theory of error-correcting codes. Elsevier, vol.16 (1977)

[12] McEliece, R. J.: A public-key cryptosystem based on algebraic coding theory. DSN Progress, Report. 44, 114-116 (1978)

[13] Mesnager, S., Qi, Y., Ru, H., Tang, C.: Minimal linear codes from characteristic functions. IEEE Transactions on Information Theory, vol. 66, no. 9, 5404-5413 (2020)

[14] Nieminen, R., Jarvinen, K.: Practical privacy-preserving indoor localization based on secure two-party computation. IEEE Transactions on Mobile Computing, vol. 20, no. 9, 2877-2890 (2020)

[15] Pasalic, E., Rodríguez, R., Zhang, F., Wei, Y.: Several classes of minimal binary linear codes violating the Aschikhmin-Barg bound. Cryptography and Communications, vol. 13, 637-659 (2021)

[16] Zhang, F., Pasalic, E., Rodríguez, R., Wei, Y.: Wide minimal binary linear codes from the general Maiorana-McFarland class. Designs, Codes and Cryptography, vol. 89, no. 7, 1485-1507 (2021)

[17] Zhang, F., Pasalic, E., Rodríguez, R., Wei, Y.: Minimal binary linear codes: a general framework based on bent concatenation. Designs, Codes and Cryptography, vol. 90, 1289-1318 (2022)

[18] Zheng, D., Wang, X., Yu, L., Liu, H.: The weight enumerators of several classes of p-ary cyclic codes. Discrete Mathematics, vol. 338, no. 7, 1264-1276 (2015)

[19] Zhou, Z., Ding, C.: A class of three-weight cyclic codes. Finite Fields and Their Applications, vol. 25, no. 1, 79-93 (2014)

Appendix A

A.1 Proof of Theorem 5

Proof: From Lemma 11, we have

$$W_f(\mathbf{v}_1,\mathbf{v}_2)=\begin{cases}-\left(2^k-k-2\right)2^l, & \mathbf{v}_1=\mathbf{0}_k,\mathbf{v}_2=\mathbf{0}_l,\\ 2^l((-1)^i-2i+k+1), & wt(\mathbf{v}_1)=i,\mathbf{v}_2=\mathbf{0}_l,\\ -(-1)^{\mathbf{v}_1\cdot\phi^{-1}(\mathbf{v}_2)}2^l, & \mathbf{v}_2\in \mathrm{Im}(\phi)\backslash\{\mathbf{0}_l\},\\ 0, & \mathbf{v}_2\notin \mathrm{Im}(\phi),\end{cases} \tag{-1}$$

for $i=1,2,\ldots,k$.

We now turn to provide the full description of the weight distribution of the code.

For k even and any $1\le i\le k$, $-2i+k+1+(-1)^i$ is even, thus -2^l and 2^l are attained $2^{k-1}(k+1)+2^k$ and $2^{k-1}(k+1)$ times, respectively. Moreover, $-2i+k+1+(-1)^i=0$ if and only if $i=\frac{k+1+(-1)^i}{2}$. In other words, when $k\equiv 2 \pmod 4$ and $i=\frac{k+2}{2}$ or $i=\frac{k}{2}$. However, when $k\equiv 0 \pmod 4$ there is no solution i to this equation. Hence, for $k\equiv 2 \pmod 4$, the value 0 has multiplicity $2^k(2^l-k-3)+\binom{k}{\frac{k+2}{2}}+\binom{k}{\frac{k}{2}}$ and the (non-zero) values $2^l(-2i+k+2)$ and $2^l(-2i+k)$ are both attained $\binom{k}{i}$ times, where $i\neq\frac{k+2}{2}$ and $i\neq\frac{k}{2}$, respectively. Whereas for $k\equiv 0 \pmod 4$, the value 0 is attained $2^k(2^l-k-3)$ times and there is no restriction for $2^l(-2i+k+2)$ and $2^l(-2i+k)$ that are both attained $\binom{k}{i}$ times.

Similarly, for odd k, $-2i+k+1+(-1)^i$ cannot be even, so that 0 is attained $2^k(2^l-k-3)$ times. The polynomial $-2i+k+1+(-1)^i=\pm 1$ has a solution if and only if $i=\frac{k+1+(-1)^i\mp 1}{2}$, that is, when either $k\equiv 1 \pmod 4$ and $i\in\left\{\frac{k+1}{2},\frac{k+3}{2}\right\}$ or $k\equiv -1 \pmod 4$ and $i\in\left\{\frac{k-1}{2},\frac{k+1}{2}\right\}$. Hence, for $k\equiv 1 \pmod 4$, -2^l has multiplicity $2^{k-1}(k+1)+2^k+\binom{k}{\frac{k+1}{2}}+\binom{k}{\frac{k+3}{2}}$ and 2^l has multiplicity $2^{k-1}(k+1)$. For $k\equiv -1 \pmod 4$, 2^l has multiplicity $2^{k-1}(k+1)+\binom{k}{\frac{k-1}{2}}+\binom{k}{\frac{k+1}{2}}$ and -2^l has multiplicity $2^{k-1}(k+1)+2^k$. The values $2^l(-2i+k+2)$, i even, and $2^l(-2i+k)$, i odd, for which $-2i+k+2\neq\pm 1$ are attained $\binom{k}{i}$ times.

From Eq.(-1), we see that C_f is minimal by Lemma 4. Note that the minimum (nonzero) weight is achieved when $wt(\mathbf{v}_1)=1, wt(\mathbf{v}_2)=0$, that is, $w_{\min}=2^{r-1}-2^{l-1}(k-2)$ and the maximum weight is $w_{\max}=2^{r-1}+2^{l-1}(2^k-k-2)$ corresponding to $wt(\mathbf{v}_1)=0, wt(\mathbf{v}_2)=0$. Hence, $w_{\min}/w_{\max}\le 1/2$ when $k\ge 6$. □

A.2 Proof of Theorem 6

Proof: Lemma 11 implies that

$$W_f(\mathbf{v}_1,\mathbf{v}_2)=\begin{cases}-\left(2^k-2k-1\right)2^l, & \mathbf{v}_1=\mathbf{0}_k,\mathbf{v}_2=\mathbf{0}_l,\\ 2^l(((-1)^i+1)(-2i+k)+1), & wt(\mathbf{v}_1)=i,\mathbf{v}_2=\mathbf{0}_l,\\ -(-1)^{\mathbf{v}_1\cdot\phi^{-1}(\mathbf{v}_2)}2^l, & \mathbf{v}_2\in \mathrm{Im}(\phi)\backslash\{\mathbf{0}_l\},\\ 0, & \mathbf{v}_2\notin \mathrm{Im}(\phi),\end{cases} \tag{-2}$$

for $i = 1, 2, \ldots, k$.

Observe that the polynomial $((-1)^i + 1)(-2i + k) + 1$ has no integer roots i, thus 0 has multiplicity $2^k(2^l - 2k - 2)$. Moreover, $((-1)^i + 1)(-2i + k) + 1 = 1$ has an integer solution i if and only if i is odd or i is even and $k \equiv 0 \pmod 4$. Similarly, $((-1)^i + 1)(-2i + k) + 1 = -1$ has a solution i if and only if i is even and $k \equiv -1 \pmod 4$. Therefore, for $k \equiv 0 \pmod 4$, 2^l is attained $2^k k + \binom{k}{\frac{k}{2}} + 2^{k-1}$ times and -2^l is attained $2^k(k + 1)$ times. The Walsh coefficient $2^l(((-1)^i + 1)(-2i + k) + 1)$ for even i and $i \neq \frac{k}{2}$ is attained $\binom{k}{i}$ times. Similarly, for $k \equiv -1 \pmod 4$, 2^l is attained $2^k k + 2^{k-1}$ times and -2^l is attained $2^k(k + 1) + \binom{k}{\frac{k+1}{2}}$ times. Finally, $2^l(((-1)^i + 1)(-2i + k) + 1)$ for even i and $i \neq \frac{k+1}{2}$ has frequency $\binom{k}{i}$.

Eq.(-2) yields minimality of C_f. The minimal (nonzero) weight is achieved when $wt(\mathbf{v}_1) = 2, wt(\mathbf{v}_2) = 0$, that is, $w_{\min} = 2^{r-1} - 2^{l-1}(-8 + 2k + 1) = 2^{r-1} - 2^{l-1}(2k - 7)$ and the maximal weight is $w_{\max} = 2^{r-1} + 2^{l-1}(2^k - 2k - 1)$. Hence, the code C_f is wide when $k \geq 8$. □