Minimal binary linear codes - a general framework based on bent concatenation

Fengrong Zhang * Enes Pasalic† René Rodríguez‡ Yongzhuang Wei §

Abstract

Minimal codes are characterized by the property that none of the codewords is covered by some other linearly independent codeword. We first show that the use of a bent function g in the so-called direct sum of Boolean functions $h(x,y) = f(x) + g(y)$, where f is arbitrary, induces minimal codes. This approach gives an infinite class of minimal codes of length 2^n and dimension $n+1$ (assuming that $h : \mathbb{F}_2^n \to \mathbb{F}_2$), whose weight distribution is exactly specified for certain choices of f. To increase the dimension of these codes with respect to their length, we introduce the concept of *non-covering permutations* (referring to the property of minimality) used to construct a bent function g in s variables, which allows us to employ a suitable subspace of derivatives of g and generate minimal codes of dimension $s + s/2 + 1$ instead. Their exact weight distribution is also determined. In the second part of this article, we first provide an efficient method (with easily satisfied initial conditions) of generating minimal $[2^n, n+1]$ linear codes that cross the so-called Ashikhmin-Barg bound. This method is further extended for the purpose of generating minimal codes of larger dimension $n + s/2 + 2$, through the use of suitable derivatives along with the employment of non-covering permutations. To the best of our knowledge, the latter method is the most general framework for designing binary minimal linear codes that violate the Ashikhmin-Barg bound. More precisely, for a suitable choice of derivatives of $h(x,y) = f(x) + g(y)$, where g is a bent function and f satisfies certain minimality requirements, for any fixed f, one can derive a huge class of non-equivalent wide binary linear codes of the same length by varying the permutation ϕ when specifying the bent function $g(y_1, y_2) = \phi(y_2) \cdot y_1$ in the Maiorana-McFarland class. The weight distribution is given explicitly for any (suitable) f when ϕ is an almost bent permutation.

Keywords: Minimal linear codes, Ashikhmin-Barg's bound, Derivatives, Direct sum.

* State Key Laboratory of Integrated Services Networks, Xidian University, Xian, 710071, P.R. China, and School of Computer Science and Technology, China University of Mining and Technology, Xuzhou, Jiangsu 221116, P.R. China, e-mail: zhfl203@163.com

†University of Primorska, FAMNIT & IAM, Koper, Slovenia, and Guangxi Key Laboratory of Cryptography and Information Security, Guilin University of Electronic Technology, Guilin, P.R. China, e-mail: enes.pasalic6@gmail.com

‡University of Primorska, FAMNIT, Koper, Slovenia, e-mail: rene7ca@gmail.com

§Guangxi Key Laboratory of Cryptography and Information Security, Guilin University of Electronic Technology, Guilin, P.R. China, e-mail: walker_wyz@guet.edu.cn

1 Introduction

Error correcting codes have many applications in communication systems, data storage devices and consumer electronics. A special class of linear codes, called *minimal*, is characterized by the property that none of the (nonzero) codewords is covered by some other codeword. These codes are widely used in certain applications such as secret sharing schemes [6, 12, 23] and secure two-party computation in e.g., [8]. Ashikhmin and Barg [1] proved that a sufficient condition for a linear code over $\mathbb{F}_q$ to be minimal is that $w_{\min}/w_{\max} > \frac{q-1}{q}$, which in binary case means that $w_{\min}/w_{\max} > \frac{1}{2}$. Nevertheless, this condition is not necessary and there are several designs of binary minimal linear codes for which $w_{\min}/w_{\max} \leqslant \frac{1}{2}$ (intrinsically harder to specify); attributed as *wide* in this article. In their pioneering work, Chang and Hyun [7] constructed an infinite family of minimal binary linear codes satisfying $w_{\min}/w_{\max} \leqslant \frac{1}{2}$ and soon after that C. Ding *et al.* [11] provided three explicit classes of wide minimal linear codes over binary alphabet. In the same article [11], a useful relationship between the Walsh spectrum of the defining Boolean function and the weight distribution of the resulting code was derived. Recently, the problem of designing minimal linear codes was also considered using the notion of so-called cutting blocking sets [3] (generalized in [20]). It was shown in [3] that cutting blocking sets precisely capture the property of minimality and one explicit design example that employs homogenous functions was given. The main conclusion is that an infinite sequence of wide minimal codes could be specified using this particular class of functions (corresponding to a hypersurface of the affine space $\mathbb{A}(\mathbb{F}_q^n)$), see [3, Theorem 5.5]. Finally, we also mention a method that employs characteristic functions [16] for the purpose of designing wide minimal codes, which essentially generalizes the approach taken by Ding em et al. [11]. We notice that a lot of work has been done towards the design of minimal linear codes over non-binary alphabet and other related structures (e.g., over finite fields), see e.g., [2, 22, 13]. Nevertheless, since the topic of this article is the design of minimal binary linear codes, we do not discuss these methods in more detail.

In this article, we address the problem of specifying binary minimal linear codes mainly using the direct sum method for constructing Boolean functions (given in the form $h(x, y) = f(x) + g(y)$) and a suitable (predetermined) subspace of derivatives of bent functions. In brief, the use of the direct sum provides a simple method to specify minimal codes *without any initial conditions*. More precisely, selecting an arbitrary Boolean function f on $\mathbb{F}_2^r$ and a bent function g on $\mathbb{F}_2^s$ is sufficient to specify a minimal linear code of dimension $r + s + 1$ given as $\mathcal{C}_h = \{(ah(x, y) + \lambda \cdot x + \beta \cdot y)_{x\in\mathbb{F}_2^r, y\in\mathbb{F}_2^s} : a \in \mathbb{F}_2, \lambda \in \mathbb{F}_2^r, \beta \in \mathbb{F}_2^s\}$, see Theorem 2. The weight distribution of this family of minimal codes is specified exactly and for arbitrary f (whose Walsh spectrum is given), see Tables $1 - 4$. To accommodate a class of minimal linear codes having a larger dimension than $r + s + 1$, we show in Section 4 that a suitable subspace of derivatives of dimension $s/2$ of a bent function g can be added to the basis of $\mathcal{C}_g$ so that the resulting code of length 2^s whose dimension is $s + 1 + s/2$ (an increase by $s/2$ compared to Theorem 2). The minimality of this codes is strongly related to a novel concept of *non-covering permutations* $\{\phi\}$, used to define a bent function $g(y_1, y_2) = \phi(y_2) \cdot y_1$ in the Maiorana-McFarland class, see Theorem 3. We notice that this increase of dimension is not traded-off against stronger initial conditions which are once again absent (apart from selecting non-covering permutations to define a bent function g which turn out to be easily specified).

The weight distribution of this family of minimal codes (with increased dimension) is also given explicitly, see Corollary 2 and Table 5.

In the second part of this article, we first provide one efficient method (with easily satisfied initial conditions) of generating wide minimal codes, see Theorem 4. Then, we again consider the use of derivatives (along with the direct sum of the underlying Boolean function) for the purpose of defining another class of wide minimal codes. This approach essentially gives a very general framework for designing wide minimal codes which employs a (suitable) subspace of derivatives of $h(x, y) = f(x) + g(y)$, where g is a bent function again and f satisfies certain minimality requirements, see Theorem 5. This method generates wide minimal codes of length 2^n and of larger dimension $n + s/2 + 2$ compared to Theorem 4 (generating codes of dimension $n + 1$). Employing a bent function $g(y^{(1)}, y^{(2)}) = \phi(y^{(2)}) \cdot y^{(1)}$ in the Maiorana-McFarland class, one can derive a huge class (for a fixed suitable function f) of non-equivalent wide binary linear codes through different selections of a non-covering permutation ϕ. Thus, for any fixed (suitable) f, one can derive a huge class of non-equivalent wide binary linear codes of the same length by varying the permutation ϕ when specifying a bent function $g(y^{(1)}, y^{(2)}) = \phi(y^{(2)}) \cdot y^{(1)}$. The weight distribution is given explicitly for any (suitable) f when ϕ is an almost bent (AB) permutation.

This paper is organized as follows. In Section 2, we introduce some basic definitions and results related to Boolean functions, linear codes and, specifically, to minimal linear codes. The use of direct sum method for the purpose of constructing minimal linear codes is described in Section 3. Its extension, based on the use of a suitable subspace of derivatives and the so-called non-covering permutations, is presented in Section 4. In Section 5, two generic methods for constructing infinite sequences of (non-equivalent) wide binary linear codes are given. One general class of (wide) minimal codes is given in Section 6 (whose weight distribution is exactly specified), when the non-covering permutation is AB. Some concluding remarks are given in Section 7.

2 Preliminaries

Let $\mathbb{F}_2$ denote the finite field with two elements $\{0, 1\}$, and let $\mathbb{F}_2^n$ denote an n-dimensional vector space over $\mathbb{F}_2$. A Boolean function f is a map from the vector space $\mathbb{F}_2^n$ to the binary field $\mathbb{F}_2$, i.e., $f : \mathbb{F}_2^n \to \mathbb{F}_2$. The set of all Boolean functions in n variables is denoted by $\mathcal{B}_n$. Any Boolean function $f \in \mathcal{B}_n$ uniquely determines a sequence of output values (called truth table) given as

$$[f(0, \ldots, 0, 0), f(0, \ldots, 0, 1), \ldots, f(1, \ldots, 1, 1)],$$

which in turn can be viewed as a binary vector of length 2^n. We then treat a function $f \in \mathcal{B}_n$ and its truth table as the same object whenever there is no ambiguity. The Hamming weight of f, denoted by $wt(f)$, is the number of ones in its truth table. The Hamming distance $d(f, g)$ between f and g is the Hamming weight of $f + g$ (i.e., $d(f, g) = wt(f + g)$).

The Walsh transform of $f \in \mathcal{B}_n$ at a point $\lambda \in \mathbb{F}_2^n$ is defined as

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

where " $\cdot$ " denotes the standard inner (dot) product of two vectors, that is, $\lambda \cdot x = \lambda_1 x_1 + \cdots + \lambda_n x_n$. The nonlinearity of a Boolean function $f \in \mathcal{B}_n$ is the minimum Hamming distance between f and the set of all n-variable affine functions (denoted by $\mathcal{A}_n$), that is,

$$\mathcal{N}_f = \min_{g \in \mathcal{A}_n} d(f, g).$$

Furthermore, it is known that $\mathcal{N}_f$ is upper bounded by $2^{n-1} - 2^{n/2-1}$ in terms of Parseval's equation $\sum_{\lambda \in \mathbb{F}_2^n} (W_f(\lambda))^2 = 2^{2n}$ [14]. A Boolean function $f \in \mathcal{B}_n$ can attain the upper bound $2^{n-1} - 2^{n/2-1}$ on its nonlinearity only when n is even, in this case, f is called bent. The Walsh transform of f can be related to $\mathcal{N}_f$ using the equality

$$\mathcal{N}_f = 2^{n-1} - \frac{1}{2} \max_{\lambda \in \mathbb{F}_2^n} |W_f(\lambda)|.$$

Thus a Boolean function $f \in \mathcal{B}_n$ is bent if and only if $W_f(\lambda) = \pm 2^{\frac{n}{2}}$ for any $\lambda \in \mathbb{F}_2^n$.

The original Maiorana-McFarland class of bent functions [15], denoted by $\mathcal{MM}$, is the set of all bent functions on $\mathbb{F}_2^{2n} = \{(x, y) \mid x, y \in \mathbb{F}_2^n\}$ of the form:

$$f(x, y) = x \cdot \pi(y) + g(y), \tag{1}$$

where π is a permutation on $\mathbb{F}_2^n$ and $g \in \mathcal{B}_n$ is arbitrary.

The derivative of a Boolean function $f \in \mathcal{B}_n$ at direction $\gamma \in \mathbb{F}_2^n$ is defined as

$$D_\gamma f(x) = f(x + \gamma) + f(x). \tag{2}$$

Throughout this paper, we denote $(0, 0, \ldots, 0) \in \mathbb{F}_2^n$ by 0_n and $(1, 1, \ldots, 1) \in \mathbb{F}_2^n$ by 1_n. We reserve the double bar symbol to represent the cardinality of a set, i.e., $\|S\|$ represents the cardinality of the set S. For a vector $\upsilon = (\upsilon_1, \upsilon_2, \ldots, \upsilon_n) \in \mathbb{F}_2^n$, we define its support to be the set $\mathsf{supp}(\upsilon) = \{i \in \{1, 2, \ldots, n\} : v_i = 1\}$. Clearly, $wt(\upsilon) = ||\mathsf{supp}(\upsilon)||$. The same applies to vectors of length 2^n corresponding to truth tables of Boolean functions on $\mathbb{F}_2^n$.

2.1 Linear codes via Boolean functions

An $[m, k, d]$ linear code $\mathcal{C} \subseteq \mathbb{F}_p^m$ over the alphabet $\mathbb{F}_p$ is a k-dimensional linear subspace of $\mathbb{F}_p^m$, whose minimum distance (the minimum weight of its non-zero codewords) is d.

In general, for functions mapping from $\mathbb{F}_p^n$ to $\mathbb{F}_p$, where p is a prime number, there are two standard methods to define linear codes that stem from such functions [10]. The first generic method, which has been greatly explored in many works, specifies codes using a mapping $f : \mathbb{F}_p^n \to \mathbb{F}_p$. Namely, the linear code $\mathcal{C}_f$, as a linear subspace of $\mathbb{F}_p^{p^n}$, is defined by

$$\mathcal{C}_f = \{(af(x) + \lambda \cdot x)_{x \in \mathbb{F}_p^n} : a \in \mathbb{F}_p, \lambda \in \mathbb{F}_p^n\}. \tag{3}$$

The dimension of $\mathcal{C}_f$ is at most $n + 1$ and its length is p^n. If $f(0_n) = 0$, we may also consider the code obtained by puncturing the first coordinate in $\mathcal{C}_f$. In this case, the length is $p^n - 1$ while the dimension remains at most $n + 1$.

On the other hand, the second generic method specifies a code using a subset $S_f = \{s_1, s_2, \ldots, s_m\} \subseteq \mathbb{F}_p^n$, usually called the defining set, so that

$$\mathcal{C}_{S_f} = \{(s_1 \cdot x, s_2 \cdot x, \ldots, s_m \cdot x) : x \in \mathbb{F}_p^n\}. \tag{4}$$

Some good codes were derived [9, 10] using special classes of vectorial mappings from $\mathbb{F}_p^n$ to $\mathbb{F}_p^n$. In this article, we exclusively consider the binary case $p = 2$ although some notions are given in a more general context.

The weight distribution of binary linear codes is directly related to the Walsh spectrum of a given Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ through the following fundamental result.

Theorem 1 *[10] Let f be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Consider the linear code $\mathcal{C}_f$ defined in (3). If f is a nonlinear function (that is, for all $b \in \mathbb{F}_2^n$ it holds $f(x) \neq b \cdot x$), then $\mathcal{C}_f$ has dimension $m + 1$. Its weight distribution is given by the following multiset:*

$$\left\{\left\{2^{n-1} - \frac{1}{2}W_f(\lambda) : \lambda \in \mathbb{F}_{2^n}\right\}\right\} \cup \{\{\ 2^{n-1}\ \}\} \cup \{\ 0\ \}. \tag{5}$$

The code $\mathcal{C}_f$ associated to a non-affine Boolean function $\mathbb{F}_2^n$ to $\mathbb{F}_2$ (3) is constructed as the smallest linear subspace of $\mathbb{F}_2^{2^n}$ containing f and all linear functions. This construction can be readily generalized to deal with vectorial Boolean functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ simply considering the smallest linear subspace of $\mathbb{F}_2^{2^n}$ containing all linear functions and every coordinate function of F (hence every component of F), i.e.,

$$\mathcal{C}_F = \{(a(b \cdot F(x)) + \lambda \cdot x)_{x \in \mathbb{F}_2^n} : a \in \mathbb{F}_2, b \in (\mathbb{F}_2^n)^*, \lambda \in \mathbb{F}_2^n\}.$$

The dimension of $\mathcal{C}_F$ is at most $2n$ and its length is 2^n. If $F(0_n) = 0_n$, one may also consider the code obtained by puncturing the first coordinate of $\mathcal{C}_F$, in this case, the length is $2^n - 1$ and $\mathcal{C}_F$ can be used to characterize AB and APN functions [5].

2.2 Minimal Linear Codes

Consider an $[m, k, d]$-linear code $\mathcal{C} \subseteq \mathbb{F}_q^m$. For any $\mathbf{u}, \mathbf{v} \in \mathcal{C}$, we say that $\mathbf{u}$ *covers* $\mathbf{v}$ if and only if $\mathsf{supp}(\mathbf{v}) \subseteq \mathsf{supp}(\mathbf{u})$. We denote this relation by $\mathbf{v} \preceq \mathbf{u}$. A codeword $\mathbf{u} \in \mathcal{C}$ is called *minimal* if it only covers the elements in $\langle \mathbf{u} \rangle$, i.e., for every $\mathbf{v} \in \mathcal{C}$ if $\mathbf{v} \preceq \mathbf{u}$ then there exists $a \in \mathbb{F}_q$ such that $\mathbf{v} = a\mathbf{u}$. The linear code $\mathcal{C}$ is said to be *minimal* if every element $\mathbf{c} \in \mathcal{C}$ is minimal. Let A_i be the number of codewords with Hamming weight i in $\mathcal{C}$. The code $\mathcal{C}$ is fully specified by its weight enumerator, which is the polynomial $1 + A_1 z + \cdots + A_m z^m$.

Ashikhmin and Barg [1] gave a sufficient condition to obtain minimal linear codes over $\mathbb{F}_q$, namely, we have the following result.

Lemma 1 *Let $\mathcal{C}$ be a linear code over $\mathbb{F}_q$. Denote by $w_{\min}$ and $w_{\max}$ the minimum and maximum nonzero Hamming weights in $\mathcal{C}$, respectively. If it holds that $\frac{w_{\min}}{w_{\max}} > \frac{q-1}{q}$, then $\mathcal{C}$ is minimal.*

In the binary case, we will call a linear code *narrow* if it satisfies the condition of Lemma 1, namely, $w_{\min}/w_{\max} > 1/2$. However, the above condition is not necessary and the codes satisfying $w_{\min}/w_{\max} \leqslant 1/2$ are called *wide*.

The key observations, related to minimality, are given in the following two lemmas.

Lemma 2 *[11] Let $\mathcal{C} \subset \mathbb{F}_2^n$ be a binary linear code. The code $\mathcal{C}$ is minimal if and only if for each pair of distinct nonzero codewords $\mathbf{a}$ and $\mathbf{b}$ in $\mathcal{C}$,*

$$wt(\mathbf{a}+\mathbf{b}) \neq wt(\mathbf{a}) - wt(\mathbf{b}).$$

Lemma 3 *[11] Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function. Then, the code $\mathcal{C}_f$ in (3) is minimal if and only if for every pair of distinct $\lambda_1, \lambda_2 \in \mathbb{F}_2^n$, it holds that*

$$W_f(\lambda_1) + W_f(\lambda_2) \neq 2^n, \tag{6}$$

and

$$W_f(\lambda_1) - W_f(\lambda_2) \neq 2^n. \tag{7}$$

The following result is a quite straightforward consequence of the above lemmas and it provides a simple characterization of wideness.

Lemma 4 *[17] For a given non-affine Boolean function $f \in \mathcal{B}_n$, consider the code $\mathcal{C}_f$ given by (3). It holds that $\mathcal{C}_f$ is wide if and only if*

$$2W_f(u_M) - W_f(u_m) \geqslant 2^n, \tag{8}$$

where u_M (resp. u_m) is such that $W_f(u_M)$ (resp. $W_f(u_m)$) is maximum (resp. minimum).

Proposition 1 *Let $\mathcal{C} \subseteq \mathbb{F}_2^n$ be an arbitrary binary linear code and $\mathcal{C}_0 \subseteq \mathcal{C}$ be any subcode of $\mathcal{C}$. The following hold:*

- *(Narrowness is hereditary) If $\mathcal{C}$ is narrow, then so is $\mathcal{C}_0$.*
- *(Minimality is hereditary) If $\mathcal{C}$ is minimal, then so is $\mathcal{C}_0$, moreover, none of its subsets with two or more elements satisfies the covering property.*

For any subset $S \subset \{1, \ldots, m\}$, define the S-puncturing of an $[m, k, d]$-code $\mathcal{C} \subseteq \mathbb{F}_q^m$ as the function $p_S : \mathcal{C} \to \mathbb{F}_q^m$ given by

$$p_S(\mathbf{c})_i = \begin{cases} c_i & \text{if } i \notin S; \\ 0 & \text{otherwise,} \end{cases}$$

where subindexes i indicate the coordinates of the corresponding vector.

The following lemma, whose proof is omitted, is a slight rephrasing of the definition of minimality and it emphasizes that minimality is a local property that depends on each coordinate.

Lemma 5 *Let $\mathcal{C}$ be a binary linear code with parameters $[m, k, d]$. The code $\mathcal{C}$ is minimal if and only if for every two non-zero codewords $\mathbf{c}, \mathbf{c}' \in \mathcal{C}$, there exists $S \subset \{1, \ldots, m\}$ such that*

$$p_S(\mathbf{c}) \not\preceq p_S(\mathbf{c}'),$$

where p_S denotes the S-puncturing of $\mathcal{C}$.

The key idea for the first construction method given in (3), is to adjoin non-affine functions to the simplex code for the purpose of increasing the dimension of the resulting code. Adjoining two linearly independent non-affine functions whose sum is non-affine gives a $[2^n, n+2, d]$-code

$$\mathcal{C}_{f_1} \oplus \mathcal{C}_{f_2} := \{(a_1 f_1(x) + a_2 f_2(x) + \lambda \cdot x)_{x \in \mathbb{F}_2^n} : a_i \in \mathbb{F}_2, \lambda \in \mathbb{F}_2^n\} = \mathcal{C}_{f_1} \cup \mathcal{C}_{f_2} \cup \mathcal{C}_{f_1+f_2}.$$

The minimality of the code $\mathcal{C}_{f_1} \oplus \mathcal{C}_{f_2}$ can be expressed in terms of the minimality of each individual code and an additional non-covering property as stated in the following lemma.

Lemma 6 *Let f_1, f_2 be two distinct non-affine Boolean functions such that $f_1 + f_2$ is non-affine. Then, the code $\mathcal{C}_{f_1} \oplus \mathcal{C}_{f_2}$ is minimal if and only if $\mathcal{C}_{f_1}$, $\mathcal{C}_{f_2}, \mathcal{C}_{f_1+f_2}$ are minimal and the following condition holds:*
For every two vectors $\lambda_1, \lambda_2 \in \mathbb{F}_2^n$ and elements $\epsilon_1, \epsilon_2, \epsilon_3 \in \mathbb{F}_2$ such that $\epsilon_1 + \epsilon_2 + \epsilon_3 = 1$ (over $\mathbb{Z}$), we have

$$(-1)^{\epsilon_1} W_{f_1}(\lambda_1) + (-1)^{\epsilon_2} W_{f_2}(\lambda_2) + (-1)^{\epsilon_3} W_{f_1+f_2}(\lambda_1 + \lambda_2) \neq 2^n. \tag{9}$$

Proof. Let $\mathcal{C} := \mathcal{C}_{f_1} \oplus \mathcal{C}_{f_2}$. Suppose that $\mathcal{C}$ is minimal. Since $\mathcal{C}_{f_1}$, $\mathcal{C}_{f_2}, \mathcal{C}_{f_1+f_2}$ are subcodes of $\mathcal{C}$, they are minimal too. Let $\lambda_1, \lambda_2 \in \mathbb{F}_2^n$ be arbitrary. We show (9) only for the case $\epsilon_1 = 1, \epsilon_2 = \epsilon_3 = 0$, since the other two cases are similar (symmetric). Consider two distinct non-zero codewords $\mathbf{c}_1 = (f_1(x) + \lambda_1 \cdot x)_{x \in \mathbb{F}_2^n}$ and $\mathbf{c}_2 = (f_2(x) + \lambda_2 \cdot x)_{x \in \mathbb{F}_2^n}$. Since $\mathcal{C}$ is minimal, $\mathbf{c}_2 \not\preceq \mathbf{c}_1$. This implies that

$$wt(\mathbf{c}_1) - wt(\mathbf{c}_2) \neq wt(\mathbf{c}_1 + \mathbf{c}_2),$$

which is equivalent to

$$-W_{f_1}(\lambda_1) + W_{f_2}(\lambda_2) \neq 2^n - W_{f_1+f_2}(\lambda_1 + \lambda_2).$$

In other words, $-W_{f_1}(\lambda_1) + W_{f_2}(\lambda_2) + W_{f_1+f_2}(\lambda_1 + \lambda_2) \neq 2^n$. Conversely, suppose that $\mathcal{C}_{f_1}$, $\mathcal{C}_{f_2}, \mathcal{C}_{f_1+f_2}$ are minimal and (9) holds. It suffices to prove that the codewords stemming from different codes do not cover each other. There are several cases to consider but we only treat the case of (non-linear) $\mathbf{c}_1 \in \mathcal{C}_{f_1}$ and $\mathbf{c}_2 \in \mathcal{C}_{f_2}$, since the other cases are similar. Let $\mathbf{c}_1 = (f_1(x) + \lambda_1 \cdot x)_{x \in \mathbb{F}_2^n}$ and $\mathbf{c}_2 = (f_2(x) + \lambda_2 \cdot x)_{x \in \mathbb{F}_2^n}$. The statement $\mathbf{c}_2 \preceq \mathbf{c}_1$ is equivalent to

$$2^{n-1} - \frac{1}{2} W_{f_1}(\lambda_1) - 2^{n-1} + \frac{1}{2} W_{f_2}(\lambda_2) = 2^{n-1} - \frac{1}{2} W_{f_1+f_2}(\lambda_1 + \lambda_2),$$

which, in turn, is equivalent to

$$-W_{f_1}(\lambda_1) + W_{f_2}(\lambda_2) + W_{f_1+f_2}(\lambda_1 + \lambda_2) = 2^n.$$

Therefore $\mathbf{c}_2 \preceq \mathbf{c}_1$ is incompatible with (9). ∎

3 Minimal codes from the direct sum of Boolean functions

In this section, we describe a simple method to generate minimal linear codes using the so-called bent concatenation.

Theorem 2 *Let n, r, s be three integers such that $r+s=n$. Let $f \in \mathcal{B}_r$ be arbitrary and $g \in \mathcal{B}_s$ be a non-affine function such that $\mathcal{C}_g$ is minimal. Consider the direct sum $h(x,y) = f(x)+g(y)$. Then, the code $\mathcal{C}_h$, defined by (3), is a minimal binary linear code. Moreover, if we define*

$$\delta := \max\{W_f(v_M)W_g(u_M), W_f(v_m)W_g(u_m)\},$$

then the parameters of $\mathcal{C}_h$ are $[2^n, n+1, 2^{n-1} - \frac{1}{2}\delta]$, where u_M (resp. u_m) is such that $W_f(u_M)$ (resp. $W_f(u_m)$) is maximum (resp. minimum).

Proof. Consider the set $\{(0_r, y) : y \in \mathbb{F}_2^s\}$ ordered lexicographically. This set can be identified with a subset of $\{1, \ldots, 2^n\}$, call it S. The image of the S-puncturing p_S can be regarded as $\mathcal{C}_{g+f(0_r)}$. Since $\mathcal{C}_g$ is minimal, so is $\mathcal{C}_{g+f(0_r)}$. This implies that $p_S(\mathbf{c}) \not\preceq p_S(\mathbf{c}')$, for every pair of distinct non-zero codewords $\mathbf{c}, \mathbf{c}' \in \mathcal{C}_h$. Lemma 5 implies that $\mathcal{C}_h$ is minimal. The second part of the statement follows from the well-known fact [18, 4] that for every $(\lambda_1, \lambda_2) \in \mathbb{F}_2^r \times \mathbb{F}_2^s$, $W_h(\lambda_1, \lambda_2) = W_f(\lambda_1)W_g(\lambda_2)$. ∎

The Walsh spectrum of the direct sum of Boolean functions is well-understood [18, 4] and it entirely depends on the Walsh spectra of each summand. In particular, when $g \in \mathcal{B}_s$ is bent, the Walsh spectrum of the direct sum $h(x,y) = f(x) + g(y)$ can be completely determined using the Walsh spectrum of f. To make this statement more precise, consider the set (not multi-set) W_f^{abs} of distinct absolute values of nonzero elements in the Walsh spectrum $W_f = \{\{W_f(\lambda) : \lambda \in \mathbb{F}_2^r\}\}$ of an arbitrary Boolean function $f \in \mathcal{B}_r$, i.e.,

$$W_f^{\text{abs}} = \{|z| : z \in W_f, z \neq 0\} = \{|W_f(\lambda)| : \lambda \in \mathbb{F}_2^n, W_f(\lambda) \neq 0\}, \tag{10}$$

where $a \neq b$ for any $a, b \in W_f^{\text{abs}}$. For every element ρ in W_f^{abs}, define $\mathfrak{m}_\rho^+$ as the multiplicity of ρ in W_f and define $\mathfrak{m}_\rho^-$ as the multiplicity of $-\rho$ in W_f. Let also $\mathfrak{m}_0$ denote the multiplicity of 0 in W_f. We also recall that for any bent function $g \in \mathcal{B}_s$ there is a unique dual bent function $\tilde{g} \in \mathcal{B}_s$ determined through $(-1)^{\tilde{g}(\lambda)} = 2^{-s/2}W_g(\lambda)$, for any $\lambda \in \mathbb{F}_2^s$.

Corollary 1 *Let n, r, s be three integers such that $s > 2$ is even and $r + s = n$. Let $f \in \mathcal{B}_r$ be arbitrary and $g \in \mathcal{B}_s$ be bent. Consider $h(x,y) = f(x) + g(y)$. The code $\mathcal{C}_h$, defined by (3), is a minimal binary linear code with parameters $[2^n, n+1, \mathcal{N}_h]$ and it has $2||W_f^{\text{abs}}|| + 1$ different non-zero weights, where W_f^{abs} is given by (10). The weight distributions of $\mathcal{C}_h$, depending on the weight of the dual $\tilde{g}$, are displayed in Table 1 and Table 2.*

Proof. Since $g \in \mathcal{B}_s$ is bent, the code $\mathcal{C}_g$ is minimal. Theorem 2 implies that $\mathcal{C}_h$ is minimal with parameters $[2^n, n+1, 2^{n-1} - \frac{1}{2}\delta]$, where $\delta = \max\{W_g(u_M)W_f(v_M), W_g(u_m)W_f(v_m)\}$. Now,

$$\max\{W_g(u_M)W_f(v_M), W_g(u_m)W_f(v_m)\} = 2^{s/2}\max\{W_f(v_M), -W_f(v_m)\} = 2^{s/2}\max_{w \in \mathbb{F}_2^r}|W_f(w)|.$$

From here, we conclude that the minimum distance of $\mathcal{C}_h$ equals

$$\mathcal{N}_h = 2^{n-1} - 2^{s/2-1} \max_{w \in \mathbb{F}_2^r} |W_f(w)|.$$

Now, for every $\lambda = (\lambda_1, \lambda_2) \in \mathbb{F}_2^n$, the weight of the codeword corresponding to $h(x,y) + (\lambda_1, \lambda_2) \cdot (x,y)$ equals

$$2^{n-1} - \frac{1}{2} W_f(\lambda_1) W_g(\lambda_2) = 2^{n-1} \pm 2^{s/2-1} W_f(\lambda_1).$$

By definition, the dual $\tilde{g}$ of g has weight $2^{s-1} - 2^{s/2-1}$ when $||\{w \in \mathbb{F}_2^s : W_g(w) = -2^{s/2}\}|| = 2^{s-1} - 2^{s/2-1}$. For every $\rho \in W_f^{\text{abs}}$, the weight $2^{n-1} - 2^{s/2-1}\rho$ of $\mathcal{C}_h$ is attained

$$(2^{s-1} + 2^{s/2-1})\mathfrak{m}_\rho^+ + (2^{s-1} - 2^{s/2-1})\mathfrak{m}_\rho^- \text{ times},$$

since it is attained by the pair of Walsh values $(2^{s/2}, \rho)$ or by the pair $(-2^{s/2}, -\rho)$. Similarly, the weight $2^{n-1} + 2^{s/2-1}\rho$ is attained

$$(2^{s-1} - 2^{s/2-1})\mathfrak{m}_\rho^+ + (2^{s-1} + 2^{s/2-1})\mathfrak{m}_\rho^- \text{ times}.$$

A similar analysis can be done when the dual of g has weight $2^{s-1} + 2^{s/2-1}$. Finally, note that for every $\rho \in W_f^{\text{abs}}$, either $\mathfrak{m}_\rho^+ \neq 0$ or $\mathfrak{m}_\rho^- \neq 0$, this implies that both weights $2^{n-1} - 2^{s/2-1}\rho$ and $2^{n-1} + 2^{s/2-1}\rho$ are always attained. Additionally, distinct values in W_f^{abs} yield distinct values of the corresponding weights, thus there are $2||W_f^{\text{abs}}|| + 1$ non-zero weights including the weight 2^{n-1}. □

Table 1: Weight distribution of $\mathcal{C}_h$ when f is an arbitrary Boolean function and g is a bent function whose dual has weight $2^{s-1} - 2^{s/2-1}$ and $h(x,y) = f(x) + g(y)$, where ρ runs over the set W_f^{abs}.

Weight w	Number of codewords A_w
$2^{n-1} - 2^{s/2-1}\rho$	$(2^{s-1} + 2^{s/2-1})\mathfrak{m}_\rho^+ + (2^{s-1} - 2^{s/2-1})\mathfrak{m}_\rho^-$
$2^{n-1} + 2^{s/2-1}\rho$	$(2^{s-1} - 2^{s/2-1})\mathfrak{m}_\rho^+ + (2^{s-1} + 2^{s/2-1})\mathfrak{m}_\rho^-$
2^{n-1}	$2^n + 2^s\mathfrak{m}_0 - 1$
0	1

Table 2: Weight distribution of $\mathcal{C}_h$ when f is an arbitrary Boolean function and g is a bent function whose dual has weight $2^{s-1}+2^{s/2-1}$ and $h(x,y)=f(x)+g(y)$, where ρ runs over the set W_f^{abs}.

Weight w	Number of codewords A_w
$2^{n-1}-2^{s/2-1}\rho$	$(2^{s-1}-2^{s/2-1})\mathfrak{m}_\rho^+ + (2^{s-1}+2^{s/2-1})\mathfrak{m}_\rho^-$
$2^{n-1}+2^{s/2-1}\rho$	$(2^{s-1}+2^{s/2-1})\mathfrak{m}_\rho^+ + (2^{s-1}-2^{s/2-1})\mathfrak{m}_\rho^-$
2^{n-1}	$2^n+2^s\mathfrak{m}_0-1$
0	1

Once we know the Walsh spectrum of f, the weight distribution of the code $\mathcal{C}_h$ is easily obtained. For instance, if r is odd and f is a semi-bent Boolean function with $f(0_r)=0$, then the weight distributions of $\mathcal{C}_h$ are displayed in Tables 3 and 4.

Table 3: Weight distribution of $\mathcal{C}_h$ when f is semi-bent, g is a bent function whose dual has weight $2^{s-1}-2^{s/2-1}$ and $h(x,y)=f(x)+g(y)$.

Weight w	Number of codewords A_w
$2^{n-1}-2^{s/2-1}2^{(r+1)/2}$	$(2^{s-1}+2^{s/2-1})(2^{r-2}+2^{\frac{r-3}{2}})+(2^{s-1}-2^{s/2-1})(2^{r-2}-2^{\frac{r-3}{2}})$
$2^{n-1}+2^{s/2-1}2^{(r+1)/2}$	$(2^{s-1}+2^{s/2-1})(2^{r-2}-2^{\frac{r-3}{2}})+(2^{s-1}-2^{s/2-1})(2^{r-2}+2^{\frac{r-3}{2}})$
2^{n-1}	$2^n+2^{n-1}-1$
0	1

Table 4: Weight distribution of $\mathcal{C}_h$ when f is semi-bent, g is a bent function whose dual has weight $2^{s-1}+2^{s/2-1}$ and $h(x,y)=f(x)+g(y)$.

Weight w	Number of codewords A_w
$2^{n-1}-2^{s/2-1}2^{(r+1)/2}$	$(2^{s-1}-2^{s/2-1})(2^{r-2}+2^{\frac{r-3}{2}})+(2^{s-1}+2^{s/2-1})(2^{r-2}-2^{\frac{r-3}{2}})$
$2^{n-1}+2^{s/2-1}2^{(r+1)/2}$	$(2^{s-1}-2^{s/2-1})(2^{r-2}-2^{\frac{r-3}{2}})+(2^{s-1}+2^{s/2-1})(2^{r-2}+2^{\frac{r-3}{2}})$
2^{n-1}	$2^n+2^{n-1}-1$
0	1

Example 1 *For $r=3, s=4$ consider the functions $f\in\mathcal{B}_3$ and $g\in\mathcal{B}_4$ given by*

$$f(x_1,x_2,x_3)=x_1x_2+x_3 \text{ and } g(y_1,y_2,y_3,y_4)=y_1y_3+y_2y_4.$$

The function g is a bent function and f is a semi-bent function with Walsh spectrum given in the table below.

λ	$(0,0,0)$	$(0,0,1)$	$(0,1,0)$	$(0,1,1)$	$(1,0,0)$	$(1,0,1)$	$(1,1,0)$	$(1,1,1)$
$W_f(\lambda)$	0	4	0	4	0	4	0	-4

By computer simulations, we have verified that the linear code $\mathcal{C}_h$ is a minimal code with minimum weight $w_{\min} = \mathcal{N}_h = 56$ and $w_{\max} = 72$. It is a $[128, 8, 56]$-code. Moreover, its weight enumerator is

$$1 + 36z^{56} + 191z^{64} + 28z^{72},$$

i.e., $\mathcal{C}_h$ is a three-weight code.

Example 2 *For $r = 4, s = 4$ consider the functions $f \in \mathcal{B}_4$ and $g \in \mathcal{B}_4$ given by*

$$f(x_1, x_2, x_3, x_4) = x_1x_2x_3 + x_4 \text{ and } g(y_1, y_2, y_3, y_4) = y_1y_3 + y_2y_4 + 1.$$

The function g is a bent function and the Walsh spectrum of f is displayed in the table below.

λ	v_1	v_2	v_3	v_4	v_5	v_6	v_7	v_8	v_9	v_{10}	v_{11}	v_{12}	v_{13}	v_{14}	v_{15}	v_{16}
$W_f(\lambda)$	0	12	0	4	0	4	0	-4	0	4	0	-4	0	-4	0	4

where we consider $\mathbb{F}_2^4 = \{v_1, \ldots, v_{16}\}$ ordered lexicographically. It can be verified that the linear code $\mathcal{C}_h$ is a minimal $[256, 9, 104]$-code with $w_{\min} = \mathcal{N}_h = 104$ and $w_{\max} = 152$. Moreover, its weight enumerator is

$$1 + 6z^{104} + 54z^{120} + 383z^{128} + 58z^{136} + 10z^{152},$$

i.e., $\mathcal{C}_h$ is a five-weight code.

4 Minimal linear codes through suitable derivatives

In this section, we propose a different approach to obtaining (wide) minimal codes by employing a suitable subspace of derivatives of a bent function g which is taken from the $\mathcal{MM}$ class of bent functions. To achieve the minimality of the resulting codes, it will be required that a permutation used to define a bent function g in the $\mathcal{MM}$ class satisfies certain covering properties.

For our purposes, we will focus on the simplest bent functions in the $\mathcal{MM}$ class. Namely, for s even and $y = (y^{(1)}, y^{(2)}) \in \mathbb{F}_2^{s/2} \times \mathbb{F}_2^{s/2}$, consider g to be a bent function in the $\mathcal{MM}$ class defined as

$$g(y^{(1)}, y^{(2)}) = \phi(y^{(2)}) \cdot y^{(1)}, \tag{11}$$

where ϕ is a permutation on $\mathbb{F}_2^{s/2}$ such that $\deg(a \cdot \phi) > 1$ for every $a \in (\mathbb{F}_2^{s/2})^*$.

The following lemmas identify useful non-covering properties of the codewords related to suitable derivatives of g.

Lemma 7 *Let g be a bent function on $\mathbb{F}_2^s$ (s even) in the $\mathcal{MM}$ class, as specified in (11). Then we have*

$$D_\alpha g(y) + D_\beta g(y) = D_{(\alpha+\beta)} g(y), \tag{12}$$

$$D_\alpha g(y) \neq D_\beta g(y), \tag{13}$$

for any two different vectors $\alpha, \beta \in \mathbb{F}_2^{s/2} \times \{0_{s/2}\}$. *Moreover, for every non-zero* $v = (v^{(1)}, v^{(2)}) \in \mathbb{F}_2^{s/2} \times \mathbb{F}_2^{s/2}, \gamma \in \mathbb{F}_2^{s/2}$ *and* $\epsilon \in \mathbb{F}_2$,

$$wt(D_{(\gamma,0_{s/2})}g(y) + v \cdot y + \epsilon) = \begin{cases} 2^{s-1} - 2^{s/2-1}(-1)^{\epsilon} W_{\gamma\cdot\phi}(v^{(2)}) & \text{if } \gamma \neq 0_{s/2}, v^{(1)} = 0_{s/2} \\ 2^{s-1} & \text{otherwise.} \end{cases} \quad (14)$$

Proof. Note that for every $y = (y^{(1)}, y^{(2)}) \in \mathbb{F}_2^{s/2} \times \mathbb{F}_2^{s/2}$ and $\gamma \in \mathbb{F}_2^{s/2}$, we have

$$D_{(\gamma,0_{s/2})}g(y) = \phi(y^{(2)}) \cdot y^{(1)} + \phi(y^{(2)}) \cdot (y^{(1)} + \gamma) = \phi(y^{(2)}) \cdot \gamma.$$

Consider a pair of vectors $\alpha = (\alpha^{(1)}, 0_{s/2}), \beta = (\beta^{(1)}, 0_{s/2}) \in \mathbb{F}_2^{s/2} \times \{0_{s/2}\}$, then

$$D_\alpha g(y) + D_\beta g(y) = \phi(y^{(2)}) \cdot \alpha + \phi(y^{(2)}) \cdot \beta = \phi(y^{(2)}) \cdot (\alpha + \beta) = D_{\alpha+\beta}g(y),$$

for every $y \in \mathbb{F}_2^s$. Thus, equation (12) holds. Since g is bent, $D_{(\alpha+\beta)}g$ is a balanced function and hence (13) follows.

To prove (14), suppose first that $\gamma \neq 0_{s/2}$ and $v^{(1)} = 0_{s/2}$. In this case, the function $D_{(\gamma,0_{s/2})}g(y) + v \cdot y + \epsilon$ becomes $\phi(y^{(2)}) \cdot \gamma + v^{(2)} \cdot y^{(2)} + \epsilon$ (viewed over $\mathbb{F}_2^s$), thus it has weight

$$2^{s/2}(2^{s/2-1} - \frac{1}{2}(-1)^{\epsilon} W_{\gamma\cdot\phi}(v^{(2)})).$$

Now, if either $\gamma = 0_{s/2}$ or $v^{(1)} \neq 0_{s/2}$, then the function $D_{(\gamma,0_{s/2})}g(y) + v \cdot y + \epsilon$ is either affine (non-constant) or equals $\phi(y^{(2)}) \cdot \gamma + v^{(2)} \cdot y^{(2)} + v^{(1)} \cdot y^{(1)} + \epsilon$, in both cases, we get a balanced function, i.e.,

$$wt(D_{(\gamma,0_{s/2})}g(y) + v \cdot y + \epsilon) = 2^{s-1}.$$

□

The following result specifies the non-covering property among the codewords that stem from a bent function g.

Lemma 8 *Let* s *be even and* $y = (y^{(1)}, y^{(2)}) \in \mathbb{F}_2^{s/2} \times \mathbb{F}_2^{s/2}$. *Let* $g(y^{(1)}, y^{(2)}) = \phi(y^{(2)}) \cdot y^{(1)}$ *be a bent function in* $\mathcal{B}_s$. *For* $\alpha, \beta \in \mathbb{F}_2^{s/2} \times \{0_{s/2}\}$, $u, v \in \mathbb{F}_2^s$ *and* $\epsilon_1, \epsilon_2 \in \mathbb{F}_2$, *the following hold:*

(i) If $\alpha \neq \beta$ *or* $v \cdot y + \epsilon_1 \neq u \cdot y + \epsilon_2$ *then*

$$(g(y + \alpha) + v \cdot y + \epsilon_1)_{y \in \mathbb{F}_2^s} \not\preceq (g(y + \beta) + u \cdot y + \epsilon_2)_{y \in \mathbb{F}_2^s}.$$

(ii) If $\beta \neq 0_s$ *or* $u \cdot y + \epsilon_2 \neq 1$ *then*

$$(g(y + \alpha) + v \cdot y + \epsilon_1)_{y \in \mathbb{F}_2^s} \not\preceq (g(y) + g(y + \beta) + u \cdot y + \epsilon_2)_{y \in \mathbb{F}_2^s}.$$

Proof. The statements are proved separately.

(i) Consider the codewords

$$\mathbf{c}_1 := (g(y+\alpha) + v \cdot y + \epsilon_1)_{y \in \mathbb{F}_2^s} \text{ and } \mathbf{c}_2 := (g(y+\beta) + u \cdot y + \epsilon_2)_{y \in \mathbb{F}_2^s}.$$

Since g is a bent function, we have $wt(\mathbf{c}_2) - wt(\mathbf{c}_1) = \pm 2^{s/2}$ *or* 0. On the other hand,

$$\mathbf{c}_1 + \mathbf{c}_2 = (D_{\alpha+\beta} g(y) + (v+u) \cdot y + \epsilon_1 + \epsilon_2)_{y \in \mathbb{F}_2^s}.$$

Using Lemma 7, we have $wt(\mathbf{c}_1 + \mathbf{c}_2) \neq 2^{s/2}$. Hence, if $\mathbf{c}_1 \preceq \mathbf{c}_2$ then $\mathbf{c}_1 = \mathbf{c}_2$. Equivalently, $\alpha = \beta$ and $v \cdot y + \epsilon_1 = u \cdot y + \epsilon_2$.

(ii) Let now the codewords $\mathbf{c}_1$ and $\mathbf{c}_2$ be of the form:

$$\mathbf{c}_1 := (g(y+\alpha) + v \cdot y + \epsilon_1)_{y \in \mathbb{F}_2^s} \text{ and } \mathbf{c}_2 := (g(y) + g(y+\beta) + u \cdot y + \epsilon_2)_{y \in \mathbb{F}_2^s}.$$

Note that the function corresponding to $\mathbf{c}_1$ and $\mathbf{c}_1 + \mathbf{c}_2$ is the sum of a bent function and an affine function. Specifically, using the definition of g, we have

$$g(y+\alpha) + g(y) + g(y+\beta) = \phi(y^2) \cdot (y^{(1)} + \alpha^{(1)}) + \phi(y^2) \cdot (\beta^{(1)}),$$

and therefore

$$\mathbf{c}_1 + \mathbf{c}_2 = (g(y+\alpha+\beta) + (v+u) \cdot y + \epsilon_1 + \epsilon_2)_{y \in \mathbb{F}_2^s}.$$

From this, we have that $wt(\mathbf{c}_1) = 2^{s-1} \pm 2^{s/2-1}$ and $wt(\mathbf{c}_1 + \mathbf{c}_2) = 2^{s-1} \pm 2^{s/2-1}$, thus

$$wt(\mathbf{c}_2 + \mathbf{c}_1) + wt(\mathbf{c}_1) = 2^s + 2^{s/2} \quad or \quad 2^s - 2^{s/2} \quad or \quad 2^s.$$

If $\mathbf{c}_1 \preceq \mathbf{c}_2$, then $wt(\mathbf{c}_2) = wt(\mathbf{c}_2 + \mathbf{c}_1) + wt(\mathbf{c}_1)$, which implies that $wt(\mathbf{c}_2)$ must be equal to either $2^s - 2^{s/2}$ or 2^s (the weight of a vector cannot be larger than 2^s). By Lemma 7, $wt(\mathbf{c}_2) \neq 2^s - 2^{s/2}$. Hence, if $\mathbf{c}_1 \preceq \mathbf{c}_2$ then $\mathbf{c}_2$ is the constant one vector, in other words, $\beta = 0_s$ and $u \cdot y + \epsilon_2 = 1$. □

Let us now consider the canonical basis $E = \{e_1, \ldots, e_{s/2}\}$ for $\mathbb{F}_2^{s/2}$ ($e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ with "1" at the ith position) and define the functions $g_0(y) = g(y)$ and $g_i(y) = g(y + (e_i, 0_{s/2}))$. The previous lemma suggests that the linear code

$$\bigoplus_{i \in I} \mathcal{C}_{g_i}, \tag{15}$$

where $I = \{0, \ldots, \frac{s}{2}\}$, is potentially a minimal code. Unfortunately, this is not true in general since the covering property in Lemma 8 does not necessarily hold for the derivatives of g. Notice that Lemma 8 does not address the covering property of two codewords that both stem from the derivative of g.

To resolve this issue, we will consider a special subclass of permutations ϕ over $\mathbb{F}_2^m$ that allows us to prove the minimality of the aforementioned code.

Definition 1 *A permutation ϕ on $\mathbb{F}_2^m$ such that $\phi(0_m) = 0_m$ will be called a* non-covering permutation *if for every $(a_1, b) \neq (a_2, b) \in \mathbb{F}_2^m \times (\mathbb{F}_2^m)^*$ we have*

$$W_{b\cdot\phi}(a_1) \pm W_{b\cdot\phi}(a_2) \neq 2^m, \tag{16}$$

and furthermore for every pair $(a_1, b_1), (a_2, b_2) \in \mathbb{F}_2^m \times (\mathbb{F}_2^m)^*$ with $b_1 \neq b_2$, the following is satisfied

$$W_{b_1\cdot\phi}(a_1) - W_{b_2\cdot\phi}(a_2) + W_{(b_1+b_2)\cdot\phi}(a_1 + a_2) \neq 2^m. \tag{17}$$

Definition 1 implies that $\deg(a \cdot \phi) \geqslant 2$, for any $a \in \mathbb{F}_2^{m*}$, thus a non-covering permutation has no affine components. A particular class of non-covering permutations is given by the so-called *almost bent* (AB) permutations. Recall that if m is odd, a vectorial Boolean function $\phi : \mathbb{F}_2^m \to \mathbb{F}_2^m$ is called an AB function if $W_{b\cdot\phi}(a) \in \{0, \pm 2^{\frac{m+1}{2}}\}$ for every pair $(a, b) \in \mathbb{F}_2^m \times (\mathbb{F}_2^m)^*$. For odd $m > 3$, any AB permutation ϕ satisfies

$$W_{b\cdot\phi}(a_1) \pm W_{b\cdot\phi}(a_2) \leqslant 2 \cdot 2^{\frac{m+1}{2}} < 2^m,$$

for $(a_1, b) \neq (a_2, b) \in \mathbb{F}_2^m \times (\mathbb{F}_2^m)^*$ and

$$W_{b_1\cdot\phi}(a_1) - W_{b_2\cdot\phi}(a_2) + W_{(b_1+b_2)\cdot\phi}(a_1 + a_2) \leqslant 3 \cdot 2^{\frac{m+1}{2}} < 2^m,$$

for $(a_1, b_1), (a_2, b_2) \in \mathbb{F}_2^m \times (\mathbb{F}_2^m)^*$ such that $b_1 \neq b_2$. Therefore, an AB permutation ϕ is non-covering for odd $m > 3$.

Similarly, another class of non-covering permutations is the multiplicative inverse $\phi(y) = y^{-1}$ on $\mathbb{F}_{2^m}$ (with convention $\phi(0) = 0$), as shown in the following lemma.

Lemma 9 *Let m be any integer such that $m \geqslant 5$. The multiplicative inverse permutation $\phi(y) = y^{2^m-2}$ is a covering permutation on $\mathbb{F}_2^m$.*

Proof. For this proof, we identify the space $\mathbb{F}_2^m$ with $\mathbb{F}_{2^m}$. It is well-known [21] that the Walsh values of any component $\phi_b := \mathrm{Tr}(by^{2^m-2})$ of $\phi(y)$ (where 'Tr$(\cdot)$' denotes the absolute trace function), for $b \in \mathbb{F}_{2^m}^*$, are given by the integers congruent to 0 mod 4 in the interval $[-2^{m/2+1}, 2^{m/2+1}]$. This implies $|W_{\phi_b}| \leqslant 2^{m/2+1}$, for any $b \in \mathbb{F}_{2^m}^*$. For $m \geqslant 5$, we then have

$$W_{\phi_b}(a_1) \pm W_{\phi_b}(a_2) \leqslant 2 \cdot 2^{m/2+1} < 2^m,$$

for $(a_1, b) \neq (a_2, b) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}^*$. This shows that (16) is satisfied. For $m > 5$, we also have

$$W_{\phi_{b_1}}(a_1) - W_{\phi_{b_2}}(a_2) + W_{\phi_{b_1+b_2}}(a_1 + a_2) \leqslant 3 \cdot 2^{\frac{m+1}{2}} < 2^m,$$

for $(a_1, b_1), (a_2, b_2) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}^*$ with $b_1 \neq b_2$. Hence (17) is satisfied for $m > 5$. The equation (17) holds also for $m = 5$, which can be confirmed by computer simulations. ∎

Remark 1 *In general, if a mapping $\phi : \mathbb{F}_2^m \to \mathbb{F}_2^m$ satisfies $\max_{(a,b)\in\mathbb{F}_2^m\times(\mathbb{F}_2^m)^*} |W_{b\cdot\phi(a)}| < 2^m/3$, then ϕ is a non-covering permutation. Hence, non-covering permutations are easily obtained.*

Similarly as before, let s be even and $y = (y^{(1)}, y^{(2)}) \in \mathbb{F}_2^{s/2} \times \mathbb{F}_2^{s/2}$. We again consider g in the $\mathcal{MM}$ class defined by (11) and assume that ϕ is a non-covering permutation on $\mathbb{F}_2^{s/2}$. The following lemma shows that the covering property applies to codewords that stem from suitable derivatives of g defined by (11).

Lemma 10 *Let s be even and $y = (y^{(1)}, y^{(2)}) \in \mathbb{F}_2^{s/2} \times \mathbb{F}_2^{s/2}$. Let $g(y^{(1)}, y^{(2)}) = \phi(y^{(2)}) \cdot y^{(1)}$ be a bent function in $\mathcal{B}_s$, where ϕ is a non-covering permutation. For $\alpha, \beta \in \mathbb{F}_2^{s/2} \times \{0_{s/2}\}$, $u, v \in \mathbb{F}_2^s$ and $\epsilon \in \mathbb{F}_2$, consider the vectors*

$$\mathbf{c}_1 := (g(y) + g(y+\alpha) + v \cdot y)_{y \in \mathbb{F}_2^s} \text{ and } \mathbf{c}_2 := (g(y) + g(y+\beta) + u \cdot y + \epsilon)_{y \in \mathbb{F}_2^s}.$$

Suppose that $\mathbf{c}_1 \neq \mathbf{c}_2$. Then, $\mathbf{c}_1 \not\preceq \mathbf{c}_2$, unless $\mathbf{c}_1$ is the zero vector or $\mathbf{c}_2$ is the constant one vector.

Proof. Using the definition of g, we have that

$$g(y) + g(y+\alpha) + g(y) + g(y+\beta) = \phi(y^{(2)}) \cdot (\alpha^{(1)} + \beta^{(1)}) = g(y) + g(y+\alpha+\beta),$$

hence

$$\mathbf{c}_1 + \mathbf{c}_2 = (g(y) + g(y+\alpha+\beta) + (v+u) \cdot y + \epsilon)_{y \in \mathbb{F}_2^s}.$$

Assume that $\mathbf{c}_2$ is not the constant one vector. If either $\mathbf{c}_1$ or $\mathbf{c}_2$ depend on $y^{(1)}$, then exactly two vectors amongst $\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_1 + \mathbf{c}_2$ are balanced since the only terms that depend on $y^{(1)}$ are affine. In this case $\mathbf{c}_1 \not\preceq \mathbf{c}_2$ unless $\mathbf{c}_1$ is the zero vector.

Suppose that none of $\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_1 + \mathbf{c}_2$ depend on $y^{(1)}$ and $\mathbf{c}_1 \preceq \mathbf{c}_2$, i.e.,

$$wt(\mathbf{c}_2) - wt(\mathbf{c}_1) = wt(\mathbf{c}_1 + \mathbf{c}_2).$$

In this case,

$$2^{s/2} w(\mathbf{c}_2') - 2^{s/2} w(\mathbf{c}_1') = 2^{s/2} wt(\mathbf{c}_1' + \mathbf{c}_2'),$$

where $\mathbf{c}_i'$ denotes the restriction of $\mathbf{c}_i$ to the coordinate $y^{(2)}$. This gives

$$wt(\mathbf{c}_2') - wt(\mathbf{c}_1') = wt(\mathbf{c}_1' + \mathbf{c}_2'). \tag{18}$$

Let us represent with a superindex (i) the restriction of an element in $\mathbb{F}_2^{s/2} \times \mathbb{F}_2^{s/2}$ to the coordinate $y^{(i)}$ where $i \in \{1, 2\}$, e.g., $v^{(2)}$ is the restriction of v to the coordinate $y^{(2)}$. Note that

$$\mathbf{c}_1' = (\phi(y^{(2)}) \cdot \alpha^{(1)} + v^{(2)} \cdot y^{(2)})_{y^{(2)} \in \mathbb{F}_2^{s/2}}, \quad \mathbf{c}_2' = (\phi(y^{(2)}) \cdot \beta^{(1)} + u^{(2)} \cdot y^{(2)} + \epsilon)_{y^{(2)} \in \mathbb{F}_2^{s/2}}.$$

If $\alpha^{(1)} \neq 0_{s/2}, \beta^{(1)} \neq 0_{s/2}$ and $\alpha^{(1)} \neq \beta^{(1)}$, then

$$wt(\mathbf{c}_1') = 2^{s/2-1} - \frac{1}{2} W_{\alpha^{(1)} \cdot \phi}(v^{(2)}), \quad wt(\mathbf{c}_2') = 2^{s/2-1} - \frac{1}{2}(-1)^{\epsilon} W_{\beta^{(1)} \cdot \phi}(u^{(2)}),$$

and

$$wt(\mathbf{c}_1' + \mathbf{c}_2') = 2^{s/2-1} - \frac{1}{2}(-1)^{\epsilon} W_{(\alpha^{(1)} + \beta^{(1)}) \cdot \phi}(v^{(2)} + u^{(2)}).$$

Using (18), we obtain

$$W_{\alpha^{(1)}\cdot\phi}(v^{(2)}) - (-1)^{\epsilon}W_{\beta^{(1)}\cdot\phi}(u^{(2)}) + (-1)^{\epsilon}W_{(\alpha^{(1)}+\beta^{(1)})\cdot\phi}(v^{(2)}+u^{(2)}) = 2^{s/2},$$

which contradicts (17) in the definition of a non-covering permutation.

Now, if $\alpha^{(1)} \neq 0_{s/2}, \beta^{(1)} \neq 0_{s/2}$ and $\alpha^{(1)} = \beta^{(1)}$, then

$$wt(\mathbf{c}_1') = 2^{s/2-1} - \frac{1}{2}W_{\alpha^{(1)}\cdot\phi}(v^{(2)}), \quad wt(\mathbf{c}_2') = 2^{s/2-1} - \frac{1}{2}(-1)^{\epsilon}W_{\alpha^{(1)}\cdot\phi}(u^{(2)}),$$

and $wt(\mathbf{c}_1' + \mathbf{c}_2') = 2^{s/2-1}$. Using (18), we obtain

$$W_{\alpha^{(1)}\cdot\phi}(v^{(2)}) - (-1)^{\epsilon}W_{\alpha^{(1)}\cdot\phi}(u^{(2)}) = 2^{s/2},$$

which contradicts (16) in the definition of a non-covering permutation. A similar argument rules out the possibility that $\alpha^{(1)} \neq 0_{s/2}, \beta^{(1)} = 0_{s/2}$. The only possibility is that $\alpha^{(1)} = 0_{s/2}$. Finally, using similar arguments and the fact that $\mathbf{c}_2$ is not the constant one vector in $\mathbb{F}_2^s$, we get $v^{(2)} = 0_{s/2}$. Therefore $\mathbf{c}_1' = 0$. Thus $v = 0_s$ and $\alpha = (0_{s/2}, 0_{s/2})$, in other words, $\mathbf{c}_1$ is the zero codeword. □

Now, we can claim the minimality of the linear code in (15) using a bent function g defined by (11) and its suitable derivatives in accordance to Lemma 10.

Theorem 3 *Let $s > 2$ be an even integer. Let $E = \{e_1, \ldots, e_{s/2}\}$ be the canonical basis of $\mathbb{F}_2^{s/2}$. Let $g(y^{(1)}, y^{(2)}) = \phi(y^{(2)}) \cdot y^{(1)}$ be a bent function on $\mathbb{F}_2^s$ defined as in (11). Then, assigning $g_0 = g$ and $g_i(y) = g(y + (e_i, 0_{s/2}))$ for $i = 1, \ldots, s/2$, the linear code*

$$\mathcal{C} = \bigoplus_{i\in\{0,\ldots,\frac{s}{2}\}} \mathcal{C}_{g_i}, \tag{19}$$

is a $[2^s, s + \frac{s}{2} + 1, 2^{s/2}\theta]$ code with $\theta \geqslant \mathcal{N}_\phi$. Moreover, if ϕ is non-covering, then $\mathcal{C}$ is minimal.

Proof. Clearly, the length of $\mathcal{C}$ is 2^s and its dimension is $s+\frac{s}{2}+1$ since the set $\{g_0, g_1, \ldots, g_{s/2}\}$ is linearly independent. The minimum distance can be deduced using Lemma 7 and expressing any codeword $\mathbf{c} \in \mathcal{C}$ in the form

$$\mathbf{c} = (\mu g(y)+g(y+e_{i_1})+\cdots+g(y+e_{i_k})+v\cdot y)_{y\in\mathbb{F}_2^s} = ((\mu+\delta)g(y)+g(y+e_{i_0}+\cdots+e_{i_k})+v\cdot y)_{y\in\mathbb{F}_2^s},$$

where k is a non-negative integer such that $k \leqslant s/2$, $\mu \in \mathbb{F}_2, v \in \mathbb{F}_2^s$ and δ is equal to $k \pmod 2$. Let us now consider two distinct codewords $\mathbf{c}_1, \mathbf{c}_2 \in \mathcal{C}$, whose parameters are indexed accordingly, so that k_i, μ_i, δ_i correspond to $\mathbf{c}_i$, for $i = 1, 2$. Suppose that $\mathbf{c}_1 \preceq \mathbf{c}_2$. Lemma 8 implies that $\mathbf{c}_1$ is the zero codeword when $\mu_1 + \delta_1 = 0$ or $\mu_2 + \delta_2 = 0$. If $\mu_1 + \delta_1 = \mu_2 + \delta_2 = 1$, then Lemma 10 implies that $\mathbf{c}_1$ is the zero codeword since ϕ is non-covering. Therefore, $\mathcal{C}$ is minimal. □

Corollary 2 *Let the notation of Theorem 3 hold. Suppose that $s \equiv 2 \pmod 4$ and $s/2 > 3$. If ϕ is an AB permutation over $\mathbb{F}_2^{s/2}$ with $\phi(0_{s/2}) = 0_{s/2}$, then $\mathcal{C}$, defined by (19), is a five-valued minimal code with parameters $[2^s, s + \frac{s}{2} + 1, 2^{s-1} - 2^{\frac{s+s/2-1}{2}}]$, whose weight distribution is displayed in Table 5.*

Proof. Theorem 3 implies that the code $\mathcal{C}$ has parameters $[2^n, s+s/2+1, d]$, where

$$d \geqslant 2^{s/2}\mathcal{N}_\phi = 2^{s/2}(2^{s/2-1} - 2^{\frac{s/2-1}{2}}).$$

Minimality of $\mathcal{C}$ can also be inferred from Theorem 3, as AB functions are non-covering for $s/2 > 3$. For any $\beta \in (\mathbb{F}_2^{s/2})^*, \lambda \in \mathbb{F}_2^{s/2}$ such that $W_{\beta\cdot\phi}(\lambda) = 2^{\frac{s/2+1}{2}}$, the codeword corresponding to the function $D_{(\beta,0_{s/2})}g(y)+(\lambda,0_{s/2})\cdot y$ has weight $2^{s/2}(2^{s/2-1}-2^{(s/2-1)/2})$. This implies that $d = 2^{s/2}(2^{s/2-1}-2^{(s/2-1)/2})$. Since ϕ is an AB permutation with $\phi(0_{s/2}) = 0_{s/2}$, the number of occurrences of $2^{\frac{s/2+1}{2}}$ in the Walsh spectra of every component $\beta\cdot\phi$ is $2^{s/2-2}+2^{(s/2-3)/2}$. This means that there are $(2^{s/2}-1)(2^{s/2-2}+2^{(s/2-3)/2})$ codewords of minimum weight. In a similar fashion, regarding the other weights, we can obtain the weight distribution of $\mathcal{C}$ displayed in Table 5. ∎

Table 5: Weight distribution of $\mathcal{C}$ in Corollary 2.

Weight w	Number of codewords A_w
$2^{s-1} - 2^{\frac{s+s/2-1}{2}}$	$(2^{s/2}-1)(2^{s/2-2}+2^{(s/2-3)/2})$
$2^{s-1} - 2^{s/2-1}$	$2^{s/2}(2^{s-1}+2^{s/2-1})$
2^{s-1}	$2^{s/2-1}(2^{s/2}-1)+(2^s-2^{s/2})(2^{s/2}-1)+(2^s-1)$
$2^{s-1}+2^{s/2-1}$	$2^{s/2}(2^{s-1}-2^{s/2-1})$
$2^{s-1}+2^{\frac{s+s/2-1}{2}}$	$(2^{s/2}-1)(2^{s/2-2}-2^{(s/2-3)/2})$
0	1

Remark 2 *Note that when ϕ is an AB permutation, the minimality of $\mathcal{C}$ follows also from the fact that the ratio*

$$\frac{w_{\min}}{w_{\max}} = \frac{2^{s-1} - 2^{\frac{s+s/2-1}{2}}}{2^{s-1} + 2^{\frac{s+s/2-1}{2}}}$$

is larger than $1/2$ when $s/2 > 3$. Moreover, we mention that AB functions were used in [19] to provide linear codes with good parameters (optimal codes in certain cases) but without the requirement on minimality or wideness.

On the other hand, the use of a non-covering permutation ϕ which is not AB may give rise to wide minimal codes, thus violating the Ashikhmin-Barg bound.

Corollary 3 *Let the notation of Theorem 3 hold. Suppose that $s/2 \geqslant 5$ and let ϕ be the inverse permutation $\phi(y) = y^{2^{s/2}-2}$ over $\mathbb{F}_2^{s/2}$. Then, $\mathcal{C}$ defined by (19) is an $(s-2)$-weighted minimal code with parameters $[2^s, s+\frac{s}{2}+1, 2^{s/2}\theta]$, where $\theta = 2^{s/2}(2^{s/2-1}-2^{s/4})$ when $s/2$ is even and θ equals the highest even integer bounded above by $2^{s/2-1}-2^{s/4}$ when $s/2$ is odd.*

Proof. It is well-known [21] that $\mathcal{N}_\phi = \min_{b\in\mathbb{F}_{2^s}^*}\mathcal{N}_{Tr(b\phi(y))}$ is equal to $\theta = (2^{s/2-1}-2^{s/4})$ when $s/2$ is even, and θ equals the highest even integer bounded above by $2^{s/2-1}-2^{s/4}$ when $s/2$ is

odd. Theorem 3 implies that the code $\mathcal{C}$ has parameters $[2^n, s+s/2+1, d]$, where $d \geqslant 2^{s/2}\theta$. Minimality of $\mathcal{C}$ follows from Theorem 3, as the inverse permutations are non-covering for $s/2 \geqslant 5$. Since the Walsh spectrum of any component of ϕ is given by the integers congruent to 0 mod 4 in the (real) range $[-2^{s/4+1}+1, 2^{s/4+1}+1]$, selecting $\beta \in (\mathbb{F}_2^{s/2})^*, \lambda \in \mathbb{F}_2^{s/2}$ such that $2^{s/2-1} - \frac{1}{2}W_{\beta\cdot\phi}(\lambda) = \mathcal{N}_\phi$ yields a codeword of weight $2^{s/2}\mathcal{N}_\phi$. This then implies that $d = 2^{s/2}\mathcal{N}_\phi$. □

Example 3 *Set $s = 10$. Let ϕ be the multiplicative inverse permutation on $\mathbb{F}_2^5$ given by $\phi(y) = y^{2^5-2} = y^{30}$. We noted before that ϕ is a (non-AB) non-covering permutation, thus the bent function $g(y^{(1)}, y^{(2)}) = \phi(y^{(2)}) \cdot y^{(1)}$ satisfies the hypotheses of Theorem 3, therefore*

$$\mathcal{C} = \bigoplus_{i\in\{0,\ldots,5\}} \mathcal{C}_{g_i}$$

is an eight-valued minimal code with parameters $[1024, 16, 320]$. Moreover, $\mathcal{C}$ is a wide code whose nonzero weights belong to the set

$$\{320, 384, 448, 496, 512, 528, 576, 640\}$$

and its weight enumerator is given by

$$1 + 31z^{320} + 155z^{384} + 310z^{448} + 16896z^{496} + 31961z^{512} + 15872z^{528} + 155z^{576} + 155z^{640}.$$

In this case $w_{\min}/w_{\max} = \frac{1}{2}$.

Even though this approach yields wide binary linear codes sometimes, in what follows, we specify generic methods that ensure wideness of the resulting codes.

5 Explicit non-trivial constructions of wide minimal codes

In this section, we present two generic methods for constructing wide minimal binary linear codes. The first method, connecting the results from the previous section, specifies functions $f \in \mathcal{B}_r$ such that both $\mathcal{C}_f$ and $\mathcal{C}_{D_\gamma(f)}$ are wide minimal codes. These codes can be potentially used in a more general framework, given in Theorem 5 in Section 5.1, for constructing wide minimal codes of larger dimension.

Recall that the symmetric difference of two sets A and B is defined as $(A \cup B) \setminus (A \cap B)$, equivalently, it can be defined as $(A \setminus B) \cup (B \setminus A)$, where the union is disjoint. We will denote the symmetric difference of A and B by $A \ominus B$. Observe that $||A \ominus B|| = ||A|| + ||B|| - 2||A \cap B||$.

Let r be a positive integer. Let Δ be a subset of $\mathbb{F}_2^r$ and consider the characteristic function $f \in \mathcal{B}_r$ of Δ, i. e., the Boolean function defined as

$$f(x) = \begin{cases} 1, & x \in \Delta, \\ 0, & x \in \mathbb{F}_2^r \setminus \Delta. \end{cases} \tag{20}$$

Lemma 11 *[17] If $\Delta \subset \mathbb{F}_2^r$, $f \in \mathcal{B}_r$ given by (20), satisfies the following conditions:*

1. $r+1 \leqslant |\Delta| \leqslant 2^{r-2}$;

2. Δ *includes at least one basis* $\{a^{(1)}, \ldots, a^{(r)}\}$ *of* $\mathbb{F}_2^r$ *and at least one vector* $\tau_1 a^{(1)} + \cdots + \tau_r a^{(r)}$, *where* $(\tau_1, \ldots, \tau_r) \in \mathbb{F}_2^r$ *and* $wt(\tau_1, \ldots, \tau_r)$ *is even,*

then the code $\mathcal{C}_f$ *given by (3) is a wide binary linear code with parameters* $[2^r, r+1, \Delta]$.

Theorem 4 *Let* $\mathcal{F} = \{a^{(1)}, \ldots, a^{(r)}\}$ *be a basis of* $\mathbb{F}_2^r$ *and define*

$$E = \{\ e \in \mathbb{F}_2^r \mid e = \tau \cdot (a^{(1)}, \ldots, a^{(r)}), wt(\tau) \text{ is even}, \tau \in \mathbb{F}_2^r\ \}.$$

Consider $\Delta = \mathcal{F} \cup S$, *where* $S \subseteq E$ *such that* $S \neq \emptyset$ *and* $||S|| \leqslant 2^{r-3} - r$, *and let* $f \in \mathcal{B}_r$ *be the indicator function of* Δ *as in (20). Take* $\tau' \in (\mathbb{F}_2^r)^*$ *and define* $\gamma = \tau' \cdot (a^{(1)}, \ldots, a^{(r)})$. *The following is true:*

(i) The code $\mathcal{C}_f$ *given by (3) is a wide binary* $[2^r, r+1, \Delta]$ *linear code.*

(ii) If $wt(\tau') > 2$ *is even and* $S \ominus (\gamma + S) \neq \emptyset$, *then the code* $\mathcal{C}_{D_\gamma f}$ *given by (3) is also a wide binary* $[2^r, r+1]$ *linear code.*

(iii) If $wt(\tau') > 2$ *is odd and* $\mathcal{F} \cap (\gamma + S) = \emptyset$, *then the code* $\mathcal{C}_{D_\gamma f}$ *given by (3) is also a wide binary* $[2^r, r+1]$ *linear code.*

Proof. (i) The statement follows directly from Lemma 11.
(ii) Suppose that $wt(\tau') > 2$ is even. We have that $(\gamma + \mathcal{F}) \cap \mathcal{F} = \emptyset$ since $wt(\tau') > 2$. Observe that

$$\mathsf{supp}(D_\gamma f) = (\gamma + \mathcal{F}) \cup \mathcal{F} \cup (S \ominus (\gamma + S)).$$

Since $||S|| \leqslant 2^{r-3} - r$, we have $||\mathsf{supp}(D_\gamma f)|| \leqslant 2^{r-2}$. Now, the fact that $wt(\tau')$ is even and $S \ominus (\gamma + S) \neq \emptyset$ imply that $\mathsf{supp}(D_\gamma f)$ contains at least one element of the form $\tau \cdot (a^{(1)}, \ldots, a^{(r)})$ with $wt(\tau)$ even. By Lemma 11, we conclude that the code $\mathcal{C}_{D_{\tau' f}}$ is a wide binary linear code.
(iii) Suppose that $wt(\tau') > 2$ is odd and $\mathcal{F} \cap (\gamma + S) = \emptyset$. Again, $(\gamma + \mathcal{F}) \cap \mathcal{F} = \emptyset$ since $wt(\tau') > 2$. We also have $(\gamma + S) \cap S = \emptyset$ since $wt(\tau')$ is odd. Observe that

$$\mathsf{supp}(D_\gamma f) = (\gamma + \mathcal{F}) \cup \mathcal{F} \cup (\gamma + S) \cup S.$$

As before, since $||S|| \leqslant 2^{r-3} - r$, we have $||\mathsf{supp}(D_\gamma f)|| \leqslant 2^{r-2}$. Note that $(\gamma + \mathcal{F}) \cap E \neq \emptyset$ thus $\mathsf{supp}(D_\gamma f)$ contains at least one element of the form $\tau \cdot (a^{(1)}, \ldots, a^{(r)})$ with $wt(\tau)$ even. By Lemma 11, we conclude that the code $\mathcal{C}_{D_\gamma f}$ is a wide binary linear code. In all the cases, the codes are of length 2^r and dimension $r+1$. ∎

Remark 3 *According to Theorem 4, for any non-empty subset* $S \subseteq E$ *with* $||S|| = 2^{r-3} - r$ *and* $\tau' \in (\mathbb{F}_2^r)^*$ *with even weight larger than two such that* $\gamma = \tau' \cdot (a^{(1)}, \ldots, a^{(r)}) \notin S + S$, *the code* $\mathcal{C}_{D_\gamma f}$ *is a wide binary linear code with parameters* $[2^r, r+1, 2^{r-2}]$. *Similarly, for any non-empty subset* $S \subseteq E$ *with* $||S|| = 2^{r-3} - r$ *and* $\tau' \in (\mathbb{F}_2^r)^*$ *with odd weight larger than two such that* $\gamma = \tau' \cdot (a^{(1)}, \ldots, a^{(r)}) \notin \mathcal{F} + S$ *the code* $\mathcal{C}_{D_\gamma f}$ *is a wide binary linear code with parameters* $[2^r, r+1, 2^{r-2}]$.

Example 4 *Set $r = 7$. Consider the basis $\mathcal{F} \subseteq \mathbb{F}_2^7$ with elements*

$$a^{(1)} = e_3 + e_5 + e_6; \quad a^{(2)} = e_2 + e_5 + e_6; a^{(3)} = e_1 + e_2 + e_3 + e_4 + e_6; \quad a^{(4)} = e_4 + e_6,$$
$$a^{(5)} = e_1 + e_4 + e_6 + e_7; \quad a^{(6)} = e_1 + e_6; \quad a^{(7)} = e_1 + e_5 + e_6 + e_7;$$

where e_i represents the vectors in the canonical base. Define $S \subseteq E$ with elements

$$s^{(1)} = a^{(1)} + a^{(3)} + a^{(4)} + a^{(6)}; \quad s^{(2)} = a^{(3)} + a^{(4)} + a^{(5)} + a^{(7)}; \quad s^{(3)} = a^{(1)} + a^{(4)};$$
$$s^{(4)} = a^{(1)} + a^{(2)} + a^{(4)} + a^{(5)} + a^{(6)} + a^{(7)}; \quad s^{(5)} = a^{(2)} + a^{(3)} + a^{(5)} + a^{(6)};$$
$$s^{(6)} = a^{(1)} + a^{(2)} + a^{(3)} + a^{(7)}; \quad s^{(7)} = a^{(1)} + a^{(2)} + a^{(5)} + a^{(6)},$$

and take $\gamma = a^{(2)} + a^{(4)} + a^{(6)} + a^{(7)}$. Note that $\tau' = (0, 1, 0, 1, 0, 1, 1)$, $wt(\tau') = 4$ and $||S|| = 7 < 9 = 2^{7-3} - 7$. By computer simulations, $||S \ominus (\gamma + S)|| = 10$ and the code $\mathcal{C}_{D_\gamma f}$ is a wide linear code, where f is the indicator function of $\Delta = \mathcal{F} \cup S$. This is a $[128, 8, 24]$ code with $w_{\max} = 80$, so that $w_{\min}/w_{\max} = 1/3$. This confirms the validity of (ii) in Theorem 4. Moreover, the code $\mathcal{C}_f \oplus \mathcal{C}_{D_\gamma f}$ is also a wide minimal code with parameters $[128, 9, 16]$ and $w_{\max} = 80$, so that $w_{\min}/w_{\max} = 1/5$.

Example 5 *Set $r = 7$. Consider the basis $\mathcal{F} \subseteq \mathbb{F}_2^7$ with elements*

$$a^{(1)} = e_1 + e_2 + e_5 + e_6; \quad a^{(2)} = e_1 + e_3 + e_6; \quad a^{(3)} = e_4 + e_7; \quad a^{(4)} = e_1 + e_4;$$
$$a^{(5)} = e_4 + e_5; \quad a^{(6)} = e_3 + e_5 + e_7; a^{(7)} = e_1 + e_2 + e_5;$$

where e_i represents the vectors in the canonical base. Define $S \subseteq E$ with elements

$$s^{(1)} = a^{(1)} + a^{(4)} + a^{(5)} + a^{(7)}; \quad s^{(2)} = a^{(1)} + a^{(2)} + a^{(5)} + a^{(6)}; \quad s^{(3)} = a^{(1)} + a^{(2)} + a^{(4)} + a^{(7)};$$
$$s^{(4)} = a^{(2)} + a^{(3)} + a^{(4)} + a^{(5)}; \quad s^{(5)} = a^{(1)} + a^{(2)} + a^{(5)} + a^{(7)}; \quad s^{(6)} = a^{(4)} + a^{(7)};$$
$$s^{(7)} = a^{(1)} + a^{(2)} + a^{(3)} + a^{(5)} + a^{(6)} + a^{(7)}; \quad s^{(8)} = 0_7; \quad s^{(9)} = a^{(4)} + a^{(6)},$$

and take $\gamma = a^{(2)} + a^{(5)} + a^{(7)}$. Note that $\tau' = (0, 1, 0, 0, 1, 0, 1)$, $wt(\tau') = 3$, and $||S|| = 9 = 2^{7-3} - 7$. One can verify that $\mathcal{C}_{D_\gamma f}$ is a wide $[128, 8, 28]$ linear code, where f is the indicator function of $\Delta = \mathcal{F} \cup S$. Furthermore, $w_{\max} = 74$, so that $w_{\min}/w_{\max} = 8/37$. This is in accordance with (iii) in Theorem 4. Moreover, the code $\mathcal{C}_f \oplus \mathcal{C}_{D_\gamma f}$ is also a wide linear code with parameters $[128, 9, 16]$ and $w_{\max} = 80$, so that $w_{\min}/w_{\max} = 1/5$.

Remark 4 *According to Examples 4 and 5, the codes constructed using Theorem 4 may have the property that $\mathcal{C}_f \oplus \mathcal{C}_{D_\gamma f}$ is minimal. However, this is not always true. For instance, the problem arises when $wt(D_\gamma f) = 2wt(f)$ in which case the codeword corresponding to $D_\gamma f$ covers the codewords stemming from f and $f(x + \gamma)$ since they have the same weight.*

5.1 Wide minimal linear codes through derivative subspaces

In what follows, we extend the construction that uses direct sum of $f(x) + g(y) := h(x, y)$ for the purpose of increasing the dimension of the resulting codes (at the cost of increasing the length, too). To achieve the minimality of $\mathcal{C}_h$, the function $f \in \mathcal{B}_r$ will be selected so that it

has at least one nonaffine derivative $D_\gamma f$ such that $\mathcal{C}_f \oplus \mathcal{C}_{D_\gamma f}$ is a minimal code. The increase in dimension is a consequence of additionally employing (suitable) derivatives of h.

Let us define the following set

$$\mathcal{C}_h^{(\gamma)} = \left\{ (uh(x,y) + h(x+\alpha, y+\beta) + v \cdot (x,y))_{(x,y)\in\mathbb{F}_2^r\times\mathbb{F}_2^s} : \begin{array}{l} \beta \in \mathbb{F}_2^{s/2} \times \{0_{\frac{s}{2}}\}, u \in \mathbb{F}_2, \\ \alpha \in \{0_r, \gamma\}, v \in \mathbb{F}_2^n \end{array} \right\}. \tag{21}$$

Lemma 12 *Let $f \in \mathcal{B}_r$ be a nonaffine function and $\gamma \in \mathbb{F}_2^r \setminus \{0_r\}$ such that $D_\gamma f$ is nonaffine. Let $g(y^{(1)}, y^{(2)}) = \phi(y^{(2)}) \cdot y^{(1)}$ be a bent function in $\mathcal{B}_s$ defined by (11), where ϕ is a permutation on $\mathbb{F}_2^{s/2}$ without affine components. If $h(x,y) = f(x) + g(y)$, then the set $\mathcal{C}_h^{(\gamma)}$ defined in (21) is a linear binary code with parameters $[2^n, n + \frac{s}{2} + 2]$.*

Proof. We first prove that $\mathcal{C}_h^{(\gamma)}$ is a linear subspace of $\mathbb{F}_2^{2^n}$. Take two different vectors in $\mathcal{C}_h^{(\gamma)}$, say,

$$(u^{(1)}h(x,y) + h(x+\alpha^{(1)}, y+\beta^{(1)}) + v^{(1)} \cdot (x,y))_{(x,y)\in\mathbb{F}_2^n} \in \mathcal{C}_h^{(\gamma)}$$

and

$$(u^{(2)}h(x,y) + h(x+\alpha^{(2)}, y+\beta^{(2)}) + v^{(2)} \cdot (x,y))_{(x,y)\in\mathbb{F}_2^n} \in \mathcal{C}_h^{(\gamma)}.$$

Using the definition of g, we have

$$g(y+\beta^{(1)}) + g(y+\beta^{(2)}) = g(y) + g(y+\beta^{(1)}+\beta^{(2)}).$$

Moreover, given that $\alpha^{(1)}, \alpha^{(2)} \in \{0_r, \gamma\}$, we have

$$f(x+\alpha^{(1)}) + f(x+\alpha^{(2)}) = f(x) + f(x+\alpha^{(1)}+\alpha^{(2)}). \tag{22}$$

These two facts imply that for $h(x,y) = f(x) + g(y)$ we have

$$h(x+\alpha^{(1)}, y+\beta^{(1)}) + h(x+\alpha^{(2)}, y+\beta^{(2)}) = f(x) + g(y) + f(x+\alpha^{(1)}+\alpha^{(2)}) + g(y+\beta^{(1)}+\beta^{(2)}),$$

thus

$$h(x+\alpha^{(1)}, y+\beta^{(1)}) + h(x+\alpha^{(2)}, y+\beta^{(2)}) = h(x,y) + h(x+\alpha^{(1)}+\alpha^{(2)}, y+\beta^{(1)}+\beta^{(2)}).$$

From the last equality, we get that the sum of the functions

$$u^{(1)}h(x,y) + h(x+\alpha^{(1)}, y+\beta^{(1)}) + v^{(1)} \cdot (x,y)$$

and

$$u^{(2)}h(x,y) + h(x+\alpha^{(2)}, y+\beta^{(2)}) + v^{(2)} \cdot (x,y)$$

is equal to

$$(u^{(1)} + u^{(2)} + 1)h(x,y) + h(x+\alpha^{(1)}+\alpha^{(2)}, y+\beta^{(1)}+\beta^{(2)}) + (v^{(1)} + v^{(2)}) \cdot (x,y).$$

Hence, the sum of the corresponding vectors belongs to $\mathcal{C}_h^{(\gamma)}$, thus $\mathcal{C}_h^{(\gamma)}$ is a linear subspace of $\mathbb{F}_2^{2^n}$.

The function $h(x,y)$ is non-affine since it is the direct sum of non-affine functions. In general, for arbitrary $\alpha \in \{0_r, \gamma\}$ and $\beta \in \mathbb{F}_2^{s/2} \times \{0_{\frac{s}{2}}\}$,

$$h(x,y) + h(x+\alpha, y+\beta) \text{ is linear if and only if } \alpha = 0_r \text{ and } \beta = 0_s. \tag{23}$$

To prove this, note that $h(x,y) + h(x+\alpha, y+\beta) = f(x) + f(x+\alpha) + g(y) + g(y+\beta)$, hence it is linear if and only if both $f(x) + f(x+\alpha)$ and $g(y) + g(y+\beta)$ are linear. Since $D_\gamma f$ is non-affine by hypothesis and $D_\beta g = \phi(y^{(2)}) \cdot \beta$ is a non-affine Boolean function as ϕ does not have affine components, the only possible way that these two functions are linear, arises when $\alpha = 0_r$ and $\beta = 0_s$.
Considering again the sum of two elements in $\mathcal{C}_h^{(\gamma)}$ and applying (23) to $\alpha = \alpha^{(1)} + \alpha^{(2)}, \beta = \beta^{(1)} + \beta^{(2)}$, we conclude that

$$(u^{(1)} + u^{(2)} + 1)h(x,y) + h(x + \alpha^{(1)} + \alpha^{(2)}, y + \beta^{(1)} + \beta^{(2)}) + (v^{(1)} + v^{(2)}) \cdot (x,y)$$

is the zero function if and only if $u^{(1)} + u^{(2)} = 0$, $\alpha^{(1)} + \alpha^{(2)} = 0_r$, $\beta^{(1)} + \beta^{(2)} = 0_s$ and $v^{(1)} + v^{(2)} = 0_n$. Thus, we have $2^{n+\frac{s}{2}+2}$ different elements, i.e., $\dim(\mathcal{C}_h^{(\gamma)}) = n + \frac{s}{2} + 2$. □

Theorem 5 *Let n, r, s be three integers such that $s(>2)$ is even and $r + s = n$. Let f be a non-affine r-variable function and $\gamma \in \mathbb{F}_2^r \setminus \{0_r\}$ with $D_\gamma f$ non-affine such that*

$$\mathcal{C}_f \oplus \mathcal{C}_{D_\gamma f} := \{(af(x) + b(f(x) + f(x+\gamma)) + v \cdot x)_{x \in \mathbb{F}_2^n} : a, b \in \mathbb{F}_2, v \in \mathbb{F}_2^n\}$$

is a minimal code. Let $g(y^{(1)}, y^{(2)}) = \phi(y^{(2)}) \cdot y^{(1)}$, with $(y^{(1)}, y^{(2)}) \in \mathbb{F}_2^{s/2} \times \mathbb{F}_2^{s/2}$, be a bent function where ϕ is a non-covering permutation on $\mathbb{F}_2^{s/2}$ as in Definition 1. Then, the code $\mathcal{C}_h^{(\gamma)}$ defined as in (21), with $h(x,y) = f(x) + g(y)$, is a minimal linear code with parameters $[2^n, n + \frac{s}{2} + 2]$. Further, if $\mathcal{C}_{D_\gamma(f)}$ is wide, then $\mathcal{C}_h^{(\gamma)}$ is also wide.

Proof. From Lemma 12, we know $\mathcal{C}_h^{(\gamma)}$ is a linear binary code with parameters $[2^n, n + \frac{s}{2} + 2]$. By definition of ϕ, we know that $\phi(0_{s/2}) = 0_{s/2}$. This implies that for every $\beta \in \mathbb{F}_2^{s/2} \times \{0_{s/2}\}$, we have $g(\beta) = 0$. We will use this fact throughout the proof without further mentioning it. For functions $\mathfrak{h} : \mathbb{F}_2^n \to \mathbb{F}_2$, corresponding to codewords in $\mathcal{C}_h^{(\gamma)}$, let $A_\mathfrak{h} : \mathbb{F}_2^r \to \mathbb{F}_2$ and $B_\mathfrak{h} : \mathbb{F}_2^s \to \mathbb{F}_2$ denote the restrictions of $\mathfrak{h}$ to the x and y coordinates, respectively. That is, for a function

$$\mathfrak{h}(x,y) = uh(x,y) + h(x+\alpha, y+\beta) + v \cdot (x,y),$$

$A_\mathfrak{h}(x) = uf(x) + f(x+\alpha) + v \cdot (x,0)$ and $B_\mathfrak{h}(y) = ug(y) + g(y+\beta) + v \cdot (0,y)$. Consider two non-zero distinct codewords in $\mathcal{C}_h^{(\gamma)}$, say,

$$\mathbf{c}_1 := (\mathfrak{h}_1(x,y))_{(x,y) \in \mathbb{F}_2^n} = (u_1 h(x,y) + h(x + \alpha^{(1)}, y + \beta^{(1)}) + v^{(1)} \cdot (x,y))_{(x,y) \in \mathbb{F}_2^n}$$

and

$$\mathbf{c}_2 := (\mathfrak{h}_2(x,y))_{(x,y) \in \mathbb{F}_2^n} = (u_2 h(x,y) + h(x + \alpha^{(2)}, y + \beta^{(2)}) + v^{(2)} \cdot (x,y))_{(x,y) \in \mathbb{F}_2^n}.$$

If $A_{\mathfrak{h}_1}$ and $A_{\mathfrak{h}_2}$ are non-zero and distinct, then puncturing the x coordinates gives two non-zero distinct codewords in $\mathcal{C}_f \oplus \mathcal{C}_{D_\gamma f}$, which is minimal by hypothesis. Thus, neither $\mathbf{c}_1 \preceq \mathbf{c}_2$ nor $\mathbf{c}_2 \preceq \mathbf{c}_1$. Similarly, if $B_{\mathfrak{h}_1}$ and $B_{\mathfrak{h}_2}$ are non-zero and distinct, then puncturing of the y coordinates yields non-zero distinct vectors of the form

$$(u_1 g(x) + g(y + \beta^{(1)}) + v^{(1)} \cdot (0_r, y) + u_1 f(0_r) + f(\alpha^{(1)}))_{y \in \mathbb{F}_2^s}$$

and

$$(u_2 g(x) + g(y + \beta^{(2)}) + v^{(2)} \cdot (0_r, y) + u_2 f(0_r) + f(\alpha^{(2)}))_{y \in \mathbb{F}_2^s}.$$

The fact that $\phi(y)$ is a non-covering permutation implies that these (nonzero) vectors do not cover each other by Lemmas 8 and 10. Thus, neither $\mathbf{c}_1 \preceq \mathbf{c}_2$ nor $\mathbf{c}_2 \preceq \mathbf{c}_1$, in this case.

Using the assumption that $\mathbf{c}_1, \mathbf{c}_2$ are distinct non-zero codewords and the above paragraph, we only need to consider the following cases:

- $A_{\mathfrak{h}_1} = A_{\mathfrak{h}_2}$ (non-zero), $B_{\mathfrak{h}_i} = \underline{0}$ and $B_{\mathfrak{h}_{(i \bmod 2)+1}} \neq \underline{0}$ for exactly one $i \in \{1, 2\}$, or
- $B_{\mathfrak{h}_1} = B_{\mathfrak{h}_2}$ (non-zero), $A_{\mathfrak{h}_i} = \underline{0}$ and $A_{\mathfrak{h}_{(i \bmod 2)+1}} \neq \underline{0}$ for exactly one $i \in \{1, 2\}$.

Let us prove the first item only since the other case can be proved *mutatis mutandis*. Suppose then that $A_{\mathfrak{h}_1} = A_{\mathfrak{h}_2}$ with $A_{\mathfrak{h}_1} \neq \underline{0}$, $B_{\mathfrak{h}_i} = \underline{0}$ and $B_{\mathfrak{h}_{(i \bmod 2)+1}} \neq \underline{0}$ for exactly one $i \in \{1, 2\}$. Without loss of generality, assume that $i = 1$. Take $x_0, x_0' \in \mathbb{F}_2^r$ and $y_0 \in \mathbb{F}_2^s$ with $A_{\mathfrak{h}_1}(x_0) = 1$, $A_{\mathfrak{h}_1}(x_0') = 0$ and $B_{\mathfrak{h}_2}(y_0) = 1$, which exist as $A_{\mathfrak{h}_1}, B_{\mathfrak{h}_2}$ are non-constant. Now, the (x_0, y_0) coordinate of $\mathbf{c}_1$ equals

$$A_{\mathfrak{h}_1}(x_0) + B_{\mathfrak{h}_1}(y_0) = A_{\mathfrak{h}_1}(x_0) = 1$$

whereas the (x_0, y_0) coordinate of $\mathbf{c}_2$ equals

$$A_{\mathfrak{h}_1}(x_0) + B_{\mathfrak{h}_2}(y_0) = 0,$$

this gives $\mathbf{c}_1 \not\preceq \mathbf{c}_2$. The (x_0', y_0) coordinate of $\mathbf{c}_1$ equals

$$A_{\mathfrak{h}_1}(x_0') + B_{\mathfrak{h}_1}(y_0) = A_{\mathfrak{h}_1}(x_0') = 0$$

whereas the (x_0', y_0) coordinate of $\mathbf{c}_2$ equals

$$A_{\mathfrak{h}_1}(x_0') + B_{\mathfrak{h}_2}(y_0) = 1.$$

This means that $\mathbf{c}_2 \not\preceq \mathbf{c}_1$. We have proved that distinct non-zero codewords in $\mathcal{C}_h^{(\gamma)}$ do not cover each other, i.e., $\mathcal{C}_h^{(\gamma)}$ is minimal.

To show the wideness of $\mathcal{C}_h^{(\gamma)}$, assuming that $\mathcal{C}_{D_\gamma(f)}$ is wide, we note that a codeword corresponding to the function

$$\mathfrak{h}(x, y) = uh(x, y) + h(x + \alpha, y + \beta) + v \cdot (x, y),$$

where additionally $B_{\mathfrak{h}}(y)$ is the zero function, has weight $2^s wt(A_{\mathfrak{h}}(x))$. Moreover, there is a natural correspondence between the codewords of $\mathcal{C}_{D_\gamma f}$ and the codewords of $\mathcal{C}_h^{(\gamma)}$ with $u \neq 0$ and $B_{\mathfrak{h}}(y)$ zero. Since $\mathcal{C}_{D_\gamma f}$ is wide, we have

$$\frac{w_{\min}\mathcal{C}_h^{(\gamma)}}{w_{\max}\mathcal{C}_h^{(\gamma)}} \leqslant \frac{2^s w_{\min}\mathcal{C}_{D_\gamma(f)}}{2^s w_{\max}\mathcal{C}_{D_\gamma(f)}} \leqslant \frac{1}{2}.$$

□

6 Applications of Theorem 5 - explicit wide minimal codes

In this section, we study the existence of functions that serve as building blocks for the construction in Theorem 5, namely, we analyse the existence of suitable Boolean functions f and their corresponding derivatives as well as the specification of non-covering permutations.

Remark 5 *The initial conditions of Theorem 5 may seem hard to satisfy, however, the results given in Theorem 4 essentially provide classes of Boolean functions suitable for this purpose. Example 4 and 5 illustrate the existence of f and $\gamma \in (\mathbb{F}_2^r)^*$ satisfying the conditions of Theorem 4. More importantly, these functions can be used as initial functions in Theorem 5 since $\mathcal{C}_f \oplus \mathcal{C}_{D_\gamma f}$ is a minimal code and $\mathcal{C}_{D_\gamma f}$ is wide.*

The importance of Theorem 5 lies in the fact that once we have suitable functions f and $D_\gamma f$, we can define a bent function g in the $\mathcal{MM}$ class using arbitrary non-covering permutation ϕ. Therefore, a huge class of wide binary linear codes can be derived from single f. These codes are not necessarily equivalent since one can, for instance, employ permutations ϕ of different algebraic degree (or Walsh spectrum). The following example illustrates the possibility of getting non-equivalent codes using different permutations ϕ.

For a fixed positive integer r, let us identify the vectors in $\mathbb{F}_2^r$ with the integers $0, \ldots, 2^r - 1$, via their binary representation (lexicographically ordered), e.g., for $r = 6$, $(0, 0, 0, 0, 0, 1) \in \mathbb{F}_2^6$ is identified with 1.

Fact 1 The function f in $\mathcal{B}_6$, whose support is given by

$$\Delta = \{4, 7, 8, 18, 21, 22, 24, 28, 35, 36, 42, 51, 54, 60\},$$

together with its derivative $D_\gamma f$ at direction $\gamma = (1, 0, 1, 1, 0, 1)$ have the property that $\mathcal{C}_f \oplus \mathcal{C}_{D_\gamma f}$ is minimal and $\mathcal{C}_{D_\gamma f}$ is wide.

Theorem 6 *Let $f \in \mathcal{B}_6$ and its derivative $D_\gamma f$ be as in Fact 1. Consider any bent function $g \in \mathcal{B}_{10}$ of the form (11) whose underlying permutation ϕ is non-covering. Then, the associated code $\mathcal{C}_h^{(\gamma)}$, defined by (21), is a wide minimal linear code with parameters $[2^{16}, 23]$.*

Proof. The result follows immediately from Theorem 5. ∎

Example 6 *In Theorem 6, if we consider the cubic AB permutation $\phi : \mathbb{F}_2^5 \to \mathbb{F}_2^5$ given by $\phi(y) = y^7$ as the underlying permutation for g, then $\mathcal{C}_h^{(\gamma)}$ is a wide minimal code with minimum distance $w_{\min} = 24576 = 3 \cdot 2^{13}$ and $w_{\max} = 49152 = 3 \cdot 2^{14}$. Thus, $\mathcal{C}_h^{(\gamma)}$ has parameters $[2^{16}, 23, 3 \cdot 2^{13}]$ and ratio $w_{\min}/w_{\max} = 1/2$. On the other hand, if we consider the inverse permutation $\phi : \mathbb{F}_2^5 \to \mathbb{F}_2^5$ given by $\phi(y) = y^{30}$, used to define g, then $\mathcal{C}_h^{(\gamma)}$ is a wide minimal linear code with parameters $[2^{16}, 23, 5 \cdot 2^{12}]$, $w_{\max} = 49152 = 3 \cdot 2^{14}$ and ratio $w_{\min}/w_{\max} = 5/12$.*

Since AB permutations (m odd) and the inverse permutations are non-covering permutations for $m \geqslant 5$, we see that non-covering permutations exist for every integer m with $m \geqslant 5$. Moreover, one can observe that there are no non-covering permutations when $m \leqslant 4$.

Remark 6 *Using simple Walsh spectrum arguments and known bounds on the nonlinearity of ϕ, one can show that there are no non-covering permutations ϕ over $\mathbb{F}_2^m$ for $m \leqslant 4$. However, there are 32! permutations over $\mathbb{F}_2^5$ and many of these permutations are non-covering. Employing a fixed function $f \in \mathcal{B}_r$ and a fixed derivative $D_\gamma f$ such that $\mathcal{C}_f \oplus \mathcal{C}_{D_\gamma f}$ is minimal and $\mathcal{C}_{D_\gamma f}$ is wide (e.g., the functions in Example 4, Example 5, Fact 1, or, Fact 2 below), each of these permutations specifies a wide minimal $[2^{r+10}, 17+r]$ linear code $\mathcal{C}_h^{(\gamma)}$.*

If the non-covering permutation ϕ has a simple Walsh spectrum (e.g., AB permutations), then the weight distribution of $\mathcal{C}_h^{(\gamma)}$ can be obtained once we know the Walsh spectra of the underlying functions f and $D_\gamma f$. To precisely describe it, we will use the notation introduced for describing the weight distributions of the direct-sum approach presented in Section 3, namely, the notation introduced in (10) and the paragraph following it.

Since we will be dealing with two Walsh spectra, corresponding to f and $D_\gamma f$, we will reserve the symbols W_f, W_f^{abs}, $\mathfrak{m}_\rho^+$, $\mathfrak{m}_\rho^-$ and $\mathfrak{m}_0$, to refer to the values associated to f and the symbols $W_{D_\gamma f}$, $W_{D_\gamma f}^{\text{abs}}$, $\mathfrak{n}_{\rho'}^+$, $\mathfrak{n}_{\rho'}^-$ and $\mathfrak{n}_0$, to refer to the values attached to $D_\gamma f$.

Theorem 7 *Use the same notation as in Theorem 5. Suppose that $s/2$ is an odd integer and $\phi : \mathbb{F}_2^{s/2} \to \mathbb{F}_2^{s/2}$ is an AB permutation. If $W_{D_\gamma f}(u_M) \geqslant 2^{(2r-s/2+1)/2}$, then the minimum distance of $\mathcal{C}_h^{(\gamma)}$ is equal to $2^s w_{\min}^\gamma$, where $w_{\min}^\gamma$ is the minimum weight in $\mathcal{C}_{D_\gamma f}$. In particular, if $\mathcal{C}_f \oplus \mathcal{C}_{D_\gamma f}$ is minimal and $\mathcal{C}_{D_\gamma f}$ is wide, then the code $\mathcal{C}_h^{(\gamma)}$ is also a wide minimal linear code with parameters $[2^n, n+s/2+2, 2^s w_{min}^\gamma]$.*

Proof. We will only consider codewords in $\mathcal{C}_h^{(\gamma)}$ whose underlying Boolean function is not linear. Note that every such codeword $(uh(x,y)+h(x+\alpha,y+\beta)+v\cdot(x,y))_{(x,y)\in\mathbb{F}_2^n}$ corresponds to any of the following four types:

$$u=1, \beta=0_s, \alpha\neq 0_s;\ u=1, \beta\neq 0_s, \alpha=0_s;\ u=1, \beta\neq 0_s, \alpha\neq 0_r;\ u=0.$$

The weight of each of these types of codewords can be easily computed using known properties of the direct sum. The weights of these codewords belong, respectively, to the sets

$$\{2^{n-1}\pm 2^{s-1}w : w\in W_{D_\gamma f}\}, \{2^{n-1}\pm 2^{\frac{s+s/2-1}{2}+r}\}, \{2^{n-1}\pm 2^{\frac{s+s/2-1}{2}}\rho' : \rho'\in W_{D_\gamma f}^{\text{abs}}\}, \{2^{n-1}\pm 2^{\frac{s}{2}-1}\rho : \rho\in W_f^{\text{abs}}\}.$$

Now, within these sets, consider the elements smaller than 2^{n-1}, that is, $2^{n-1}-2^{\frac{s+s/2-1}{2}+r}$ together with

$$2^{n-1}-2^{s-1}w,\ 2^{n-1}-2^{\frac{s+s/2-1}{2}}\rho',\ 2^{n-1}-2^{s/2-1}\rho,$$

for each positive element $w\in W_{D_\gamma f}$, $\rho\in W_f^{\text{abs}}$ and $\rho'\in W_{D_\gamma f}^{\text{abs}}$. Since ρ,ρ' are both smaller than 2^r, we have that for every $\rho\in W_f^{\text{abs}}$ and $\rho'\in W_{D_\gamma f}^{\text{abs}}$

$$2^{s/2-1}\rho < 2^{s/2-1+r} < 2^{(s+s/2-1)/2+r} \text{ and } 2^{(s+s/2-1)/2}\rho' < 2^{(s+s/2-1)/2+r}.$$

Now, $2^{(s+s/2-1)/2+r} \leqslant 2^{s-1}W_{D_\gamma f}(u_M)$ by hypothesis. This readily implies that the minimum weight of $\mathcal{C}_h^{(\gamma)}$ is $2^{n-1}-2^{s-1}W_{D_\gamma f}(u_M) = 2^s w_{\min}^\gamma$. The last part of the statement follows directly from Theorem 5. ∎

Remark 7 *The weight distribution of the code $\mathcal{C}_h^{(\gamma)}$ in Theorem 7 can be specified knowing that the possible values of weights are distinct from each other (otherwise, frequencies of the repeated entries in the left column in Table 6 must be summed). That is, if for every $w \in W_{D_\gamma f}, \rho' \in W_{D_\gamma f}^{\mathrm{abs}}$, $\rho \in W_f^{\mathrm{abs}}$ we have $2^{(s/2-1)/2}w \neq \rho'$, $\rho' \neq 2^{(2r-s/2+1)/2}$, $2^{(s/2+1)/2}\rho' \neq \rho$ and $\rho \neq 2^{s/2}w$, then the weight distribution of the code $\mathcal{C}_h^{(\gamma)}$ can be fully determined and is given in Table 6.*

Table 6: Weight distribution of $\mathcal{C}_h^{(\gamma)}$ in Theorem 7 for $s/2$ odd and an AB permutation $\phi : \mathbb{F}_2^{s/2} \to \mathbb{F}_2^{s/2}$, where ρ runs over W_f^{abs} and ρ' runs over $W_{D_\gamma f}^{\mathrm{abs}}$.

Weight w	Number of codewords
$2^{n-1} - 2^{s-1}\rho'$	$\mathfrak{n}_{\rho'}^{+}$
$2^{n-1} - 2^{\frac{s+s/2-1}{2}+r}$	$(2^{s/2}-1)(2^{s/2-2} + 2^{(s/2-3)/2})$
$2^{n-1} - 2^{\frac{s+s/2-1}{2}}\rho'$	$(2^{s/2}-1)((2^{s/2-2} + 2^{(s/2-3)/2})\mathfrak{n}_{\rho'}^{+} + (2^{s/2-2} - 2^{(s/2-3)/2})\mathfrak{n}_{\rho'}^{-})$
$2^{n-1} - 2^{s/2-1}\rho$	$2^{s/2+1}((2^{s-1} + 2^{s/2-1})\mathfrak{m}_{\rho}^{+} + (2^{s-1} - 2^{s/2-1})\mathfrak{m}_{\rho}^{-})$
2^{n-1}	$2^n + 2^{n-1} + 2^{s/2+1}\mathfrak{m}_0 + (2^{s/2}-1)2^{s/2-1} + (2^{s/2-1}+1)\mathfrak{n}_0 - 1$
$2^{n-1} + 2^{s/2-1}\rho$	$2^{s/2+1}((2^{s-1} - 2^{s/2-1})\mathfrak{m}_{\rho}^{+} + (2^{s-1} + 2^{s/2-1})\mathfrak{m}_{\rho}^{-})$
$2^{n-1} + 2^{\frac{s+s/2-1}{2}}\rho'$	$(2^{s/2}-1)((2^{s/2-2} - 2^{(s/2-3)/2})\mathfrak{n}_{\rho'}^{+} + (2^{s/2-2} + 2^{(s/2-3)/2})\mathfrak{n}_{\rho'}^{-})$
$2^{n-1} + 2^{\frac{s+s/2-1}{2}+r}$	$(2^{s/2}-1)(2^{s/2-2} - 2^{(s/2-3)/2})$
$2^{n-1} + 2^{s-1}\rho'$	$\mathfrak{n}_{\rho'}^{-}$
0	1

Note that the number of non-zero weights given in Table 6 (the left column) depends on the cardinalities of W_f^{abs} and $W_{D_\gamma f}^{\mathrm{abs}}$. In particular, the code $\mathcal{C}_h^{(\gamma)}$ in Theorem 7 has at most $4||W_{D_\gamma f}^{\mathrm{abs}}|| + 2||W_f^{\mathrm{abs}}|| + 3$ non-zero weights.

Fact 2 The function $f \in \mathcal{B}_6$ whose support is given by

$$\Delta = \{3, 5, 7, 11, 12, 24, 27, 31, 34, 37, 51, 52\}$$

and its derivative $D_\gamma f$ at direction $\gamma = (0, 1, 1, 0, 1, 0)$, will induce both the minimality and wideness of the associated codes $\mathcal{C}_{D_\gamma f}$ and $\mathcal{C}_f \oplus \mathcal{C}_{D_\gamma f}$. Moreover, the Walsh spectra of f and $D_\gamma f$ satisfy

$$W_f(b) \in \{-16, -12, -8, -4, 0, 4, 8, 12, 40\}, W_{D_\gamma f}(b) \in \{-24, -8, 0, 8, 24\},$$

for every $b \in \mathbb{F}_2^6$.

Theorem 8 *Let $f \in \mathcal{B}_6$ and $D_\gamma f$ be as in Fact 2. Consider any bent function $g \in \mathcal{B}_{10}$ as in (11) whose underlying permutation is non-covering. The code $\mathcal{C}_h^{(\gamma)}$ is a wide minimal linear code with parameters $[2^{16}, 23]$. Moreover, if ϕ is an AB permutation on $\mathbb{F}_2^5$, then $\mathcal{C}_h^{(\gamma)}$ has parameters $[2^{16}, 23, 2^{10} \cdot 20]$ and its weight distribution is displayed in Table 7.*

Proof. The result follows immediately from Theorem 5, Theorem 7 and Table 6. □

Table 7: Weight distribution of $\mathcal{C}_h^{(\gamma)}$ in Theorem 8 for any AB permutation $\phi : \mathbb{F}_2^5 \to \mathbb{F}_2^5$.

Weight w	Number of codewords A_w
$2^{15} - 2^{10} + 2^5 \cdot 26$	$2^{16} \cdot 3$
$2^{15} - 2^{10} + 2^5 \cdot 28$	$2^{16} \cdot 10$
$2^{15} - 2^{10} + 2^5 \cdot 30$	$2^{16} \cdot 13$
$2^{15} - 2^{10} + 2^5 \cdot 34$	$2^{16} \cdot 13$
$2^{15} - 2^{10} + 2^5 \cdot 36$	$2^{16} \cdot 5$
$2^{15} - 2^{10} + 2^5 \cdot 38$	$2^{16} \cdot 3$
$2^{15} - 2^{10} + 2^5 \cdot 12$	$2^6(2^9 + 2^4)$
$2^{15} - 2^{10} + 2^5 \cdot 40$	$2^6(2^9 + 2^4)$
$2^{15} + 2^{10} - 2^5 \cdot 12$	$2^6(2^9 - 2^4)$
$2^{15} + 2^{10} - 2^5 \cdot 40$	$2^6(2^9 - 2^4)$
$2^{15} + 2^8 \cdot 20 - 2^{13}$	$(2^5 - 1)((2^3 + 2) + (2^3 - 2) \cdot 3)$
$2^{15} + 2^8 \cdot 28 - 2^{13}$	$(2^5 - 1)((2^3 + 2) \cdot 21 + (2^3 - 2) \cdot 7)$
$2^{15} + 2^8 \cdot 36 - 2^{13}$	$(2^5 - 1)((2^3 + 2) \cdot 7 + (2^3 - 2) \cdot 21)$
$2^{15} + 2^8 \cdot 44 - 2^{13}$	$(2^5 - 1)((2^3 + 2) \cdot 3 + (2^3 - 2))$
$2^{10} \cdot 20$	1
$2^{10} \cdot 28$	21
$2^{10} \cdot 36$	7
$2^{10} \cdot 44$	3
$2^{15} - 2^{13}$	$(2^5 - 1)(2^3 + 2)$
$2^{15} + 2^{13}$	$(2^5 - 1)(2^3 - 2)$
2^{15}	5160943
0	1

Note that for the function f in Fact 2, the cardinalities of $W_{D_\gamma f}^{\text{abs}}$ and W_f^{abs} are 2 and 5, respectively. Thus, there are at most $4||W_{D_\gamma f}^{\text{abs}}|| + 2||W_f^{\text{abs}}|| + 3 = 21$ distinct weights in $\mathcal{C}_h^{(\gamma)}$ when ϕ is an AB on $\mathbb{F}_2^5$. In this case, all of these weights are distinct (see Remark 7) so there are exactly 21 non-zero weights, which is in accordance with Table 7.

7 Conclusion

In this article, we have presented several generic methods of constructing (wide) minimal binary linear codes. Most notably, the design of minimal binary linear codes involves some weak initial conditions and therefore our approaches are quite general. Two generic methods for constructing wide binary linear codes are also given and their initial conditions are easily satisfied. Moreover, given a single Boolean function f which induces the minimality of both $\mathcal{C}_f$

and of $\mathcal{C}_f \oplus \mathcal{C}_{D_\gamma f}$, one can generate a huge family of non-equivalent codes by using different (non-covering) permutations on a suitable variable space. In this case, since the choice of a bent function in the $\mathcal{MM}$ used in the direct sum is arbitrary (up to the non-covering property of permutation ϕ) such families of non-equivalent wide binary linear codes of length 2^n can be easily designed. It is an interesting research problem to consider shortenings of these codes for the purpose of deriving optimal codes.

Acknowledgment: Fengrong Zhang is supported in part by the Natural Science Foundation of China (No. 61972400). Enes Pasalic is partly supported by the Slovenian Research Agency (research program P1-0404 and research projects J1-9108, J1-1694). Yongzhuang Wei (corresponding author) is supported in part by the Natural Science Foundation of China (No. 61872103), in part by the Guangxi Natural Science Foundation (No. 2019GXNSFGA245004), and in part by the Guangxi Science and Technology Foundation (Guike AB18281019).

References

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

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

[3] Bonini, M., Borello, M.: Minimal linear codes arising from blocking sets. Journal of Algebraic Combinatorics (2021). https://doi.org/10.1007/s10801-019-00930-6

[4] Carlet, C.: Boolean models and methods in mathematics, computer science, and engineering. In: Crama, Y., Hammer, P. (eds.) Encyclopedia of Mathematics and its Applications, pp. 398–468. Cambridge University Press, Cambridge (2010)

[5] Carlet, C., Charpin, P., Zinoviev, V.: Codes, bent functions and permutations suitable for DES-like cryptosystems. Des. Codes Cryptogr. 15, 125–156 (1998). https://doi.org/10.1023/A:1008344232130

[6] Carlet, C., Ding, C., Yuan, J.: Linear codes from highly nonlinear functions and their secret sharing schemes. IEEE Trans. Inf. Theory 51 (6), 2089–2102 (2005)

[7] Chang, S., Hyun, J.: Linear codes from simplicial complexes. Des. Codes Cryptogr. 86, 2167–2181 (2018)

[8] Cohen, G., Mesnager, S., Patey, A.: On minimal and quasi-minimal linear codes. In: Stam, M. (eds.) Proceedings of IMACC (Lecture Notes in Computer Science, vol. 8308), pp. 85–98. Springer-Verlag, Berlin (2013)

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

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

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

[12] Ding C., Yuan, J.: Covering and secret sharing with linear codes. In: Calude, C., Dinneen M., Vajnovszki V. (eds) Discrete Mathematics and Theoretical Computer Science (Lecture Notes in Computer Science, vol. 2731), pp. 11–25. Springer, Berlin, Heidelberg (2003)

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

[14] MacWilliams, F., Sloane, N.: The theory of error-correcting codes. North Holland, Amsterdam (1977)

[15] McFarland, R.: A family of difference sets in non-cyclic groups. Journal of Combinatorial Theory (series A) 15, 1–10 (1973)

[16] Mesnager, S., Qi, Y., Ru, H., Tang, C.: Minimal linear codes from characteristic functions. IEEE Trans. Inf. Theory 66 (9), 5404–5413 (2020)

[17] Pasalic, E., Rodríguez, R., Zhang, F., Wei, Y.: Several classes of minimal binary linear codes violating the Aschikhmin-Barg bound. Cryptogr. Commun. (2021). https://doi.org/10.1007/s12095-021-00491-1

[18] Rothaus, O.: On bent functions. Journal of Combinatorial Theory (series A) 20, 300–305 (1976)

[19] Tang, D., Carlet, C., Zhou, Z.: Binary linear codes from vectorial Boolean functions and their weight distribution. Discrete Math. 340 (12), 3055–3072 (2017)

[20] Tang, C., Qiu, Y., Liao, Q., Zhou, Z.: Full characterization of minimal linear codes as cutting blocking sets. IEEE Trans. Inf. Theory (2021). https://doi.org/10.1109/TIT.2021.3070377

[21] Wolfmann, J.: The weights of the orthogonal of certainc cyclic codes or extended Goppa codes. In: Mora T. (eds) Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. AAECC 1988 (Lecture Notes in Computer Science, vol 357), pp. 476–480. Springer, Berlin, Heidelberg (1989). https://doi.org/10.1007/3-540-51083-4_84

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

[23] Yuan, J., Ding, C.: Secret sharing schemes from three classes of linear codes. IEEE Trans. Inf. Theory 52 (1), 206–212 (2006)