# A huge class of infinite sequences of minimal binary linear codes with or without crossing the Ashikhmin-Barg's bound

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

**Abstract**

A special class of linear codes, having important applications in secret sharing and secure two-party computation, called minimal is characterized by the property that none of the codewords is covered by some other codeword. Denoting by $w_{min}$ and $w_{max}$ the minimal and maximal weight of a binary linear code respectively, a sufficient but not necessary condition for achieving minimality is that $w_{min}/w_{max} > 1/2$ (called Ashikhmin-Barg's bound). Those minimal codes satisfying the condition $w_{min}/w_{max} \leq 1/2$ are called *wide* in this article (generally harder to construct), whereas codes satisfying $w_{min}/w_{max} > 1/2$ are called *narrow*. In this article, we first show that the so-called direct sum of Boolean functions of the form $h(x, y) = f(x) + g(y)$ induces narrow minimal codes whenever $g$ is a bent function. Then, we introduce the concept of non-covering permutations (referring to the property of minimality) which is shown to be sufficient for providing many infinite classes of minimal binary linear codes of larger dimension by employing a suitable subspace of derivatives of the bent function $g$. In the second part of this article, we first provide one efficient method (with easily satisfied initial conditions) of generating wide minimal codes. Then, we again consider the use of derivatives (along with the underlying Boolean function given as the direct sum) for the purpose of defining another class of wide minimal codes. To the best of our knowledge, the latter method is the most general framework for designing wide binary linear codes. It uses a (suitable) subspace of derivatives of $h(x, y) = f(x) + g(y)$, where $g$ is a bent function and $f$ satisfies certain minimality requirements. For a fixed suitable function $f$, one can derive a huge class of non-equivalent wide binary linear codes of the same length by varying the permutation $\phi$ when specifying the bent function $g(y_1, y_2) = \phi(y_2) \cdot y_1$ in the Maiorana-McFarland class.

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

*School of Computer Science and Technology, China University of Mining and Technology, Xuzhou, Jiangsu 221116, P.R. China, and State Key Laboratory of Integrated Services Networks, Xidian University, Xian, 710071, 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 [5, 12, 22] and secure two-party computation in e.g. [7]. 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 $w_{min}/w_{max} \leq \frac{1}{2}$ (intrinsically harder to specify); attributed as *wide* in this article. In their pioneering work, Chang and Hyun [6] constructed an infinite family of minimal binary linear codes satisfying $w_{min}/w_{max} \leq \frac{1}{2}$ and soon after that C. Ding *et al.* [10] provided three explicit classes of wide minimal linear codes over binary alphabet. In the same article [10], a useful relationship between Walsh spectrum of the defining Boolean function and the weight distribution of the resulting code was derived. Quite recently, the problem of designing minimal linear code 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. [10]. 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, 21, 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 using mainly 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 $\mathcal{C}_h = \{(ah(x, y) + \lambda \cdot x + \beta \cdot y)_{x\in\mathbb{F}_2^r, y\in\mathbb{F}_2^s} : a \in \mathbb{F}_2, \lambda \in \mathbb{F}_2^r, \beta \in \mathbb{F}_2^s\}$, cf. Theorem 2. To accommodate a class of minimal linear codes having a larger dimension than $r + s + 1$, we show that a suitable subspace of derivatives of $g$ of dimension $s/2$ can be added to the basis of $\mathcal{C}_h$ so that the resulting code is again minimal but of dimension $r + s + 1 + s/2$ instead. To achieve the minimality property a special class of *non-covering permutations* $\{\phi\}$ is introduced to define a bent function $g(y_1, y_2) = \phi(y_2) \cdot y_1$ in the Maiorana-McFarland class which is shown to be a sufficient condition for minimality, cf. Theorem 3. The 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 are easily specified). In the second part of this article, we first provide one efficient method (with easily satisfied initial conditions) of generating wide minimal codes. 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. Finally, to the best of our knowledge, we provide the most general framework for designing wide minimal codes which use a (suitable) subspace of derivatives of $h(x, y) = f(x) + g(y)$, where $g$ is a bent function again and $f$ give rise to minimal codes. 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 the permutation $\phi$. Concludingly, an extremely large family of infinite sequences of wide binary linear codes can be generated using this method since $g$ can be selected in many different ways.

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 without initial conditions is described in Section 3. Its extension, based on the use of a suitable subspace of derivatives, is presented in Section 3.1. In Section 4, two generic methods for constructing infinite sequences of (non-equivalent) wide binary linear codes are given. Some concluding remarks are given in Section 5.

## 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 identifies 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 codeword of length $2^n$. 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]. If a Boolean function $f \in \mathcal{B}_n$ attains the upper bound $2^{n-1} - 2^{n/2-1}$ on its nonlinearity, then the Boolean function $f$ is called bent. Obviously, bent functions exist only for an even number of variables. 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 $\pi$ is a permutation on $\mathbb{F}_2^n$ and $g \in \mathcal{B}_n$ is arbitrary.

A 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 codewords of length $2^n$ that belong to a linear code spanned by the truth tables of $f \in \mathcal{B}_n$ and linear functions on $\mathbb{F}_2^n$.

### 2.1 Linear codes via Boolean functions

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 [9]. 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 $\mathbb{F}_p^n$, 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 [8, 9] 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 $p = 2$, though 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** *[9] 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:*

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

## 2.2 Minimal Linear Codes

An $[n, k, d]$ linear code $\mathcal{C} \subseteq \mathbb{F}_q^n$ over the alphabet $\mathbb{F}_q$ is a $k$-dimensional linear subspace of $\mathbb{F}_q^n$, whose minimum distance (the minimum weight of its non-zero codewords) is $d$. For any $u, v \in \mathcal{C}$, we say that $u$ *covers* $v$ if and only if $\mathsf{supp}(v) \subseteq \mathsf{supp}(u)$. We denote this relation by $v \preceq u$. A codeword $u \in \mathcal{C}$ is called *minimal* if it only covers the elements in $\langle u \rangle$, i.e., for every $v \in \mathcal{C}$ if $v \preceq u$ then there exists $a \in \mathbb{F}_q$ such that $v = au$. The linear code $\mathcal{C}$ is said to be *minimal* if every element $c \in \mathcal{C}$ 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 $1 + A_1 z + \cdots + A_n z^n$.

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 $C$ be a linear code over $\mathbb{F}_q$. Denote by $w_{\min}$ and $w_{\max}$ the minimum and maximum nonzero Hamming weights in $C$, respectively. If it holds that $\frac{w_{\min}}{w_{\max}} > \frac{q-1}{q}$, then $C$ 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 minimal codes satisfying $w_{\min}/w_{\max} \leq 1/2$ are called *wide*.

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

**Lemma 2** *[10] 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* a *and* b *in $\mathcal{C}$,*

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

**Lemma 3** *[10] 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** *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*

$$2W_f(u_M) - W_f(u_m) \geq 2^n. \tag{8}$$

*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 $C \subseteq \mathbb{F}_2^n$ be an arbitrary binary linear code and $C_0 \subseteq C$ be any subcode of $C$. The following hold:*

- *(Narrowness is hereditary) If $C$ is narrow then so is $C_0$.*
- *(Minimality is hereditary) If $C$ is minimal then so is $C_0$, moreover, none of its subsets with two or more elements satisfies the covering property.*

## 3 Minimal linear codes from direct sum of Boolean functions

In this section, we describe a simple method to generate minimal linear codes using the so-called bent concatenation. We first notice that taking two nonlinear functions $h_1, h_2 \in \mathcal{B}_n$, whose sum is nonlinear as well, the construction in (3) can be extended to consider

$$\mathcal{C}_{h_1} \oplus \mathcal{C}_{h_2} := \{(ah_1(x) + bh_2(x) + v \cdot x)_{x\in\mathbb{F}_2^n} : a, b \in \mathbb{F}_2, v \in \mathbb{F}_2^n\}. \tag{9}$$

Note that $\mathcal{C}_{h_1}, \mathcal{C}_{h_2}$ are subcodes of $\mathcal{C}_{h_1} \oplus \mathcal{C}_{h_2}$ whose dimension is $n+2$. The notation $\mathcal{C}_{h_1} \oplus \mathcal{C}_{h_2}$, used for brevity, is slightly misleading since it does not refer to the direct sum of subspaces. We notice that $\mathcal{C}_{h_1} \cup \mathcal{C}_{h_2} \cup \mathcal{C}_{h_1+h_2} := \{(ah_1(x) + bh_2(x) + v \cdot x)_{x\in\mathbb{F}_2^n} : a, b \in \mathbb{F}_2, v \in \mathbb{F}_2^n\}$. A necessary and sufficient condition for $\mathcal{C}_{h_1} \oplus \mathcal{C}_{h_2}$ to be minimal is that $\mathcal{C}_{h_1}, \mathcal{C}_{h_2}, \mathcal{C}_{h_1+h_2}$ are minimal and additionally none of the codewords in $\mathcal{C}_{h_1}, \mathcal{C}_{h_2}$ or $\mathcal{C}_{h_1+h_2}$ is covered by some other codeword (cross terms), which appears to be quite difficult. One can easily extend this method and consider $\bigoplus_{i=1}^{k} \mathcal{C}_{h_i}$, which implies even harder restrictions on the choice of $h_i$.

On the other hand, these conditions can be significantly relaxed by considering the direct sum of the form $h(x, y) = f(x)+g(y)$, where $f$ and $g$ defined on disjoint variable spaces. The following result is a well-known property of this construction method.

**Lemma 5** *[18, 4] Let $r, s$ and $n$ be three positive integers such that $r + s = n$. Let $f \in \mathcal{B}_r$ and $g \in \mathcal{B}_s$, and define $h(x, y) = f(x) + g(y)$. Then, for any $\alpha \in \mathbb{F}_2^r, \beta \in \mathbb{F}_2^s$, we have*

*(i)*

$$W_h(\alpha, \beta) = W_f(\alpha)W_g(\beta). \tag{10}$$

*(ii) Let $v^x = (v_1, \ldots, v_r)$ and $v^y = (v_{r+1}, \ldots, v_n)$ so that $v = (v^x, v^y) \in \mathbb{F}_2^n$. Then,*

$$\begin{aligned} & wt\left((h(x, y) + (v^x, v^y) \cdot (x, y))_{(x,y)\in\mathbb{F}_2^n}\right) \\ = \; & 2^r wt\left((g(y) + v^y \cdot y)_{y\in\mathbb{F}_2^s}\right) + 2^s wt\left((f(x) + v^x \cdot x)_{x\in\mathbb{F}_2^r}\right) \\ & -2wt\left((f(x) + v^x \cdot x)_{x\in\mathbb{F}_2^r}\right) wt\left((g(y) + v^y \cdot y)_{y\in\mathbb{F}_2^s}\right). \end{aligned}$$

**Theorem 2** *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 and define $h(x, y) = f(x) + g(y)$. Then, the code $\mathcal{C}_h$ defined by (3) is a narrow binary linear code. Furthermore, $\mathcal{N}_h > 2^{n-2}$.*

*Proof.* It is well-known that $W_h(\alpha, \beta) = W_f(\alpha)W_g(\beta)$. Then, we have $W_h(v_M) = 2^{s/2}W_f(u_M)$ and $W_h(v_m) = 2^{s/2}W_f(u_m)$, where $u_M$ (resp. $u_m$) is such that $W_f(u_M)$ (resp. $W_f(u_m)$) is maximum (resp. minimum). Thus, we know that $v_M$ (resp. $v_m$) is such that $W_h(v_M)$ (resp. $W_h(v_m)$) is maximum (resp. minimum). Further,

$$2W_h(v_M) - W_h(v_m) = 2^{s/2}(2W_f(u_M) - W_f(u_m)) < 2^{s/2} \times 3 \times 2^r < 2^n,$$

for $s > 2$. From Lemma 4, we can conclude that the code $\mathcal{C}_h$ is narrow for $s > 2$.

Now, since $g$ is a bent function in $s$ variables, $|W_g(\beta)| = 2^{s/2}$. Then

$$\max_{(\alpha,\beta)\in\mathbb{F}_2^n} |W_h(\alpha, \beta)| = 2^{s/2} \max_{\alpha\in\mathbb{F}_2^r} |W_f(\alpha)| \leq 2^{r+s/2}. \tag{11}$$

Moreover, as $s > 2$ we have that $\frac{s}{2} < s - 1$ and therefore

$$r + \frac{s}{2} < r + s - 1 = n - 1.$$

Thus, $2^{r+s/2} < 2^{n-1}$ and $\max_{(\alpha,\beta)\in\mathbb{F}_2^n} |W_h(\alpha,\beta)| < 2^{n-1}$. We can finally compute $\mathcal{N}_h$ as

$$\mathcal{N}_h = 2^{n-1} - \frac{1}{2} \max_{(\alpha,\beta)\in\mathbb{F}_2^n} |W_h(\alpha,\beta)|$$

hence,

$$\mathcal{N}_h > 2^{n-1} - \frac{1}{2} \times 2^{n-1} = 2^{n-2}$$

by the previous observation. □

**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 the Walsh spectrum of $f$ is given in the table below.*

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

*The Walsh spectrum of the direct sum $h(x,y) = f(x)+h(y)$ can be computed using Lemma 5. 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.*

| $\lambda$ | $v_1$ | $v_2$ | $v_3$ | $v_4$ | $v_5$ | $v_6$ | $v_7$ | $v_8$ | $v_9$ | $v_{10}$ | $v_{11}$ | $v_{12}$ | $v_{13}$ | $v_{14}$ | $v_{15}$ | $v_{16}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $W_f(\lambda)$ | 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. The Walsh spectrum of the direct sum $h(x,y) = f(x) + h(y)$ can be computed using Lemma 5. 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.*

**Remark 1** *Note that the number of nonzero Walsh values of $h$ are directly related to the number of different nonzero values in the Walsh spectrum of $f$, namely, there are*

$$2||\{|W_f(\lambda)| \neq 0 : \lambda \in \mathbb{F}_2^n\}|| + 1$$

*nonzero weights in $\mathcal{C}_h$. Furthermore, the maximum Walsh value is $2^{s/2}W_f(\lambda_M)$ and therefore the minimum distance of $\mathcal{C}_h$ is $2^{n-1} - 2^{s/2-1}W_f(\lambda_M)$.*

### 3.1 Minimal linear codes through suitable derivatives

In this section, we extend the approach based on the direct sum 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 properties.

For our purpose, 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

$$g(y^{(1)}, y^{(2)}) = \phi(y^{(2)}) \cdot y^{(1)}, \tag{12}$$

where $\phi$ is a permutation on $\mathbb{F}_2^{s/2}$ without linear components.

The following lemma identifies certain useful non-covering properties of the codewords related to suitable derivatives of $g$.

**Lemma 6** *Let $g$ be a bent function on $\mathbb{F}_2^s$ ($s$ even) in the $\mathcal{MM}$ class, as specified in (12). Then we have*

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

$$D_\alpha g(y) \neq D_\beta g(y), \tag{14}$$

*for any two different vectors $\alpha, \beta \in \mathbb{F}_2^{s/2} \times \{0_{s/2}\}$. Furthermore, for every $v \in \mathbb{F}_2^s$, $\gamma \in \mathbb{F}_2^{s/2} \times \{0_{s/2}\}$ and $\epsilon \in \mathbb{F}_2$ it holds*

$$wt(D_\gamma g(y) + v \cdot y + \epsilon) \in \{2^{s/2}k : k \in \{0, 2, \ldots, 2^{s/2} - 2, 2^{s/2}\}\}. \tag{15}$$

*Proof.* For every $y = (y^{(1)}, y^{(2)}) \in \mathbb{F}_2^{s/2} \times \mathbb{F}_2^{s/2}$, denoting $\alpha = (\alpha^{(1)}, 0_{s/2}), \beta = (\beta^{(1)}, 0_{s/2})$, we have

$$\begin{aligned} D_\alpha g(y) + D_\beta g(y) &= \phi(y^{(2)}) \cdot (y^{(1)}) + \phi(y^{(2)}) \cdot (y^{(1)} + \alpha) + \phi(y^{(2)}) \cdot (y^{(1)}) + \phi(y^{(2)}) \cdot (y^{(1)} + \beta) \\ &= \phi(y^{(2)}) \cdot (\alpha + \beta) = \phi(y^{(2)}) \cdot (y^{(1)}) + \phi(y^{(2)}) \cdot (y^{(1)} + \alpha + \beta) \\ &= D_{(\alpha+\beta)} g(y). \end{aligned}$$

Thus, equation (13) holds. Since $g$ is bent, $D_{(\alpha+\beta)}g$ is a balanced function and hence (14) follows.

In (15), $k = 0$ and $k = 2^{s/2}$ correspond to the trivial cases when $\gamma = 0_s, v = 0_s, \epsilon = 0$ (the zero function) and $\gamma = 0_s, v = 0_s, \epsilon = 1$ (the constant one function), respectively. We then

assume that the considered functions are non-constant. Now, let $v \in \mathbb{F}_2^s$, $\gamma \in \mathbb{F}_2^{s/2} \times \{0_{s/2}\}$ and $\epsilon \in \mathbb{F}_2$ be arbitrary vectors. Since $\gamma = (\gamma^{(1)}, \gamma^{(2)}) \in \mathbb{F}_2^{s/2} \times \{0_{s/2}\}$, we have that

$$D_\gamma g(y) = \phi(y^{(2)}) \cdot \gamma^{(1)},$$

so the derivative $D_\gamma g(y)$ only depends on the coordinate $y^{(2)}$. We also notice that since $\phi$ is a permutation then $D_\gamma g(y)$ is balanced, for any nonzero $\gamma \in \mathbb{F}_2^s$. The function $v \cdot y + \epsilon$ can be viewed as $a \cdot y^{(1)} + b \cdot y^{(2)} + \epsilon$ for some $a, b \in \mathbb{F}_2^{s/2}$.

To show (15), we consider the different cases w.r.t. $v = (a, b)$:
*i*) When $a \neq 0_{s/2}$ then $D_\gamma g(y) + a \cdot y^{(1)} + b \cdot y^{(2)} + \epsilon$ involves (canonical) linear functions from the variable space $y^{(1)}$ and is therefore balanced since $D_\gamma g(y)$ only depends on $y^{(2)}$. The balancedness of $D_\gamma g(y) + v \cdot y + \epsilon$ clearly remains when $\gamma = 0_s$.
*ii*) When $a = 0_{s/2}$, then the codewords are of the form $D_\gamma g(y) + b \cdot y^{(2)} + \epsilon = \phi(y^{(2)}) \cdot \gamma^{(1)} + b \cdot y^{(2)} + \epsilon$. Assuming additionally that $b = 0_{s/2}$ gives again balanced codewords due to the term $D_\gamma g(y) = \phi(y^{(2)}) \cdot \gamma^{(1)}$. On the other hand, when $b \neq 0_{s/2}$ then summing over all $y^{(2)}$ the expression $\phi(y^{(2)}) \cdot \gamma^{(1)} + b \cdot y^{(2)}$ corresponds to computing $W_\phi(b)$. Since both $\phi(y^{(2)}) \cdot \gamma^{(1)}$ and $b \cdot y^{(2)}$ have a balanced Hamming weight, the fact that $\phi(y^{(2)}) \cdot \gamma^{(1)}$ is not linear implies that

$$wt(D_\gamma g(y) + v \cdot y + \epsilon) \in \{2^{s/2}k : k \in \{2, \ldots, 2^{s/2} - 2, \}\},$$

where the factor $2^{s/2}$ is due to the missing variables of $y^{(1)}$. Summarizing all the cases, we conclude that (15) indeed specifies the possible weights of $D_\gamma g(y) + v \cdot y + \epsilon)$. ∎

The following result specifies the non-covering property of certain codewords that stem form the bent function $g$.

**Lemma 7** *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 $\epsilon \in \mathbb{F}_2$, the following hold:*

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

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

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

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

*(iii) If $\alpha \neq 0_s$ or $v \cdot y \neq 0$ then*

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

*Proof.* The statements are proved separately.

(i) Consider the codewords

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

Since $g$ is a bent function, we have

$$wt(\mathbf{c}_2) - wt(\mathbf{c}_1) = \pm 2^{s/2} \quad or \quad 0.$$

On the other hand,

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

Using Lemma 6, 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 $v \cdot y = u \cdot y + \epsilon$.

(ii) Now, consider the vectors

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

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

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

hence

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

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

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

By Lemma 6, $wt(\mathbf{c}_2) \neq 2^s - 2^{s/2}$. Hence, if $\mathbf{c}_1 \preceq \mathbf{c}_2$ then $\mathbf{c}_2$ is the constant one vector which gives $\beta = 0_s$ and $u \cdot y + \epsilon = 1$.

(iii) Finally, consider the vectors

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

Similarly as in the previous case, the functions corresponding to $\mathbf{c}_2$ and $\mathbf{c}_1 + \mathbf{c}_2$ are the sum of a bent function and an affine function, specifically,

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

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

$$wt(\mathbf{c}_2) - wt(\mathbf{c}_2 + \mathbf{c}_1) = \pm 2^{s/2} \quad or \quad 0.$$

By Lemma 6, $wt(\mathbf{c}_1) \neq 2^{s/2}$. Hence if $\mathbf{c}_1 \preceq \mathbf{c}_2$, then $\mathbf{c}_1$ is the all-zero vector which gives $\alpha = 0_s$ and $v \cdot y = 0$. □

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 $i$th position ) and define the functions $g_0(y) = g(y)$ and $g_i(y) = g(y + e_i)$. The previous lemma suggests that the linear code

$$\bigoplus_{i \in I} \mathcal{C}_{g_i} \tag{16}$$

is potentially a minimal code, where $I = \{0, \ldots, \frac{s}{2}\}$. Unfortunately, this is not true in general since the covering property in Lemma 7 does not necessarily hold for the derivatives of $g$. Notice that Lemma 7 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 $\phi$ over $\mathbb{F}_2^m$ that allows us to prove the minimality of the aforementioned code.

**Definition 1** *A permutation $\phi$ 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*

$$W_{b\cdot\phi}(a_1) \pm W_{b\cdot\phi}(a_2) \neq 2^m, \tag{17}$$

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

$$W_{b_1\cdot\phi}(a_1) - W_{b_2\cdot\phi}(a_2) + W_{(b_1+b_2)\cdot\phi}(a_1 + a_2) \neq 2^m. \tag{18}$$

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 $\phi$ satisfies

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

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

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

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

**Remark 2** *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 $\phi$ is a non-covering permutation. Hence, non-covering permutations are easily obtained.*

**Example 3** *The monomial $\phi(y) = y^{30}$ on $\mathbb{F}_{2^5}$ is a non-covering permutation. Namely, for every $a, b \in \mathbb{F}_2^5$ we have*

$$W_{b\cdot\phi}(a) \in \{-12, -4, -8, 0, 4, 8\}.$$

*Moreover, the spectral value $-12$ appears exactly once, thus*

$$W_{b\cdot\phi}(a_1) \pm W_{b\cdot\phi}(a_2) \leq 8 + 12 = 20 < 32,$$

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

$$W_{b_1 \cdot \phi}(a_1) - W_{b_2 \cdot \phi}(a_2) + W_{(b_1+b_2)\cdot\phi}(a_1 + a_2) \leq 8 - (-12) + 8 = 28 < 32,$$

*for* $(a_1, b_1) \neq (a_2, b_2) \in \mathbb{F}_2^m \times (\mathbb{F}_2^m)^*$.

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 (12) and assume that $\phi$ 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 (12).

**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 $\mathcal{B}_s$, as specified by (12). 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 $\mathbf{c}_1 \neq \mathbf{c}_2$. We have that $\mathbf{c}_1 \not\preceq \mathbf{c}_2$, 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

$$wt(\mathbf{c}_2') - wt(\mathbf{c}_1') = wt(\mathbf{c}_1' + \mathbf{c}_2'). \tag{19}$$

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 (19) 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 (18) 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 (19) we obtain

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

which contradicts (17) 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 possibilty is that $\alpha^{(1)} = 0_{s/2}$. Finally, using similar arguments and the fact that $\mathbf{c}_2$ is not the constant one vector of $\mathbb{F}_2^s$, 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 all-zero codeword. □

Now, we can claim the minimality of the linear code in (16) using a bent function $g$ defined by (12) and its suitable derivatives in accordance to Lemma 8.

**Theorem 3** *Let $s > 2$ be an even integer. Consider the canonical basis $E = \{e_1, \ldots, e_{s/2}\}$ of $\mathbb{F}_2^{s/2}$. If $g$ is a bent function as in (12), then assigning $g_0 = g$ and $g_i(y) = g(y + e_i)$ for $i = 1, \ldots, s/2$ the linear code*

$$C = \bigoplus_{i\in\{0,\ldots,\frac{s}{2}\}} \mathcal{C}_{g_i}, \tag{20}$$

*is a $[2^s, s + \frac{s}{2} + 1, d]$ code with $d \geq 2^{s/2+1}$. Moreover, if $\phi$ is non-covering then $C$ is minimal.*

*Proof.* We already know that the length of $C$ is $2^s$ and its dimension is $s + \frac{s}{2} + 1$ since the set $\{g_i\}$ is linearly independent. The minimum distance can be deduced using Lemma 6 and expressing any codeword $\mathbf{c} \in C$ in the form

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

where $k$ is a non-negative integer, $\mu \in \mathbb{F}_2$ and $v \in \mathbb{F}_2^s$. Let us now consider $\mathbf{c}_1, \mathbf{c}_2 \in C$, whose parameters are indexed accordingly so that $k_i$ and $\mu_i$ correspond to $\mathbf{c}_i$, for $i = 1, 2$. Suppose that $\mathbf{c}_1 \preceq \mathbf{c}_2$. Lemma 7 implies that $\mathbf{c}_1$ is the zero codeword when $\mu_1 = 0$ or $\mu_2 = 0$. If $\mu_1 = \mu_2 = 1$, then Lemma 8 (due to the choice of derivatives) implies that $\mathbf{c}_1$ is the zero codeword. Therefore, $C$ is minimal. □

**Corollary 1** *Let the notation of Theorem 3 hold. If $\phi$ is an AB permutation over $\mathbb{F}_2^{s/2}$, then $C$ defined by (20) for $s \equiv 2 \mod 4$ 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 1.*

Table 1: Weight distribution of $C$ in Corollary 1.

| 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 3** *Note that when $\phi$ is an AB permutation, the minimality of $C$ follows 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 $s > 2$. Moreover, we mention that AB functions were used in [19] to provide linear codes with good parameters (in certain cases optimal codes) but without the request on minimality or wideness.*

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

**Example 4** *Set $s = 10$. Let $\phi$ be the permutation on $\mathbb{F}_2^5$ given by $\phi(y) = y^{2^5-2} = y^{30}$. We noted before that $\phi$ 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*

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

*is an eight-valued minimal code with parameters $[1024, 16, 320]$. Moreover, $C$ 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 in certain cases yields wide binary linear codes, in what follows we specify generic methods that ensure wideness of the resulting codes.

# 4 Explicit non-trivial constructions of wide minimal codes

In this section, we provide several classes of wide minimal binary linear codes. Out first method connects the result from the previous section, thus specifying a function $f \in \mathcal{B}_r$ such that both $\mathcal{C}_f$ and $\mathcal{C}_{D_\gamma(f)}$ are minimal codes and $\frac{w_{\min(D_\gamma(f))}}{w_{\max(D_\gamma(f))}} \leq \frac{1}{2}$, where $\gamma \in \mathbb{F}_2^r \setminus \{0_r\}$. These codes can be potentially used in a more general framework based on the direct sum method, described in Section 4.1, for constructing wide minimal codes from those Boolean functions whose associated derivative code $\mathcal{C}_{D_\gamma(f)}$ is wide. We provide several examples of embedding these wide linear codes described by Theorem 4 into a broader framework given by Theorem 5, for the purpose of providing many infinite classes of wide minimal codes. Due to a large number of possibilities of selecting a bent function $g$ in Theorem 5, for a fixed suitable $f \in \mathcal{B}_r$, we essentially exhibit a great variety of non-equivalent wide linear codes on the same variable space.

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

$$f(x) = \begin{cases} 1, & x \in \Delta, \\ 0, & x \in \mathbb{F}_2^r \setminus \Delta. \end{cases} \tag{21}$$

**Lemma 9** *[17] If $\Delta \subset \mathbb{F}_2^r$, $f \in \mathcal{B}_r$ given by (21), satisfies the following conditions:*

1. $r + 1 \leq |\Delta| \leq 2^{r-2}$;
2. *$\Delta$ includes at least one basis $\{a^{(1)}, \ldots, a^{(r)}\}$ of $\mathbb{F}_2^r$ and at least one nonzero vector $\tau_1 a^{(1)} + \cdots + \tau_r a^{(r)}$, where $(\tau_1, \ldots, \tau_r) \in \mathbb{F}_2^r \setminus \{0_r\}$ and $wt(\tau_1, \ldots, \tau_r)$ is even,*

*then the code $\mathcal{C}_f$ given by (3) is a wide binary linear code.*

**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 $||S|| \leq 2^{r-3} - r$, and let $f \in \mathcal{B}_r$ be the indicator function of $\Delta$ as in (21). 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 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 minimal binary 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 minimal binary linear code.*

*Proof.* $(i)$ The statement follows directly from Lemma 9.
$(ii)$ 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 $||S|| \leq 2^{r-3} - r$, we have $||\mathsf{supp}(D_\gamma f)|| \leq 2^{r-2}$. 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 9, 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 $||S|| \leq 2^{r-3} - r$, we have $||\mathsf{supp}(D_\gamma f)|| \leq 2^{r-2}$. 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 9, we conclude that the code $\mathcal{C}_{D_\gamma f}$ is a wide binary linear code. □

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

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

*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 $C_f \oplus \mathcal{C}_{D_\gamma f}$ is also a wide minimal code with parameters $[128, 9, 16]$ and $w_{max} = 80$, so that $w_{min}/w_{max} = 1/5$.*

**Example 6** *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* $C_f \oplus \mathcal{C}_{D_\gamma f}$ *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** *The codes constructed using Theorem 4 do not necessarily have the property that* $\mathcal{C}_f \oplus \mathcal{C}_{D_\gamma f}$ *is minimal. For instance, the problem arises when* $wt(D_\gamma f) = 2wt(f)$ *in which case the codeword coming from* $D_\gamma f$ *covers both codewords related to* $f$ *and* $f(x+\gamma)$ *since they have the same weight. Nevertheless, suitable choices for* $f$ *and* $\gamma$ *can ensure the minimality of* $\mathcal{C}_f \oplus \mathcal{C}_{D_\gamma f}$, *as illustrated in Examples 5 and 6.*

### 4.1 Wide minimal linear codes through derivative subspaces

In what follows, we extend the construction based on the use of direct sum of $f(x) + g(y) := h(x,y)$ for the purpose of increasing the dimension of the resulting codes. To achieve 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 will be achieved using suitable derivatives of $h$.

Let us define the following set

$$\mathcal{C}_h^{(\gamma)} = \left\{ (uh(x,y) + h(x+\alpha, y+\beta) + v \cdot (x,y))_{(x,y)\in\mathbb{F}_2^r \times \mathbb{F}_2^s} : \begin{array}{l} \beta \in \mathbb{F}_2^{s/2} \times \{0_{\frac{s}{2}}\}, u \in \mathbb{F}_2, \\ \alpha \in \{0_r, \gamma\}, v \in \mathbb{F}_2^n \end{array} \right\}. \tag{22}$$

**Lemma 10** *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 (12), where* $\phi$ *is a non-covering permutation on* $\mathbb{F}_2^{s/2}$ *by means of Definition* 1. *If* $h(x,y) = f(x) + g(y)$, *then the set* $\mathcal{C}_h^{(\gamma)}$ *defined in (22) 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

$$f(x+\alpha^{(1)}) + f(x+\alpha^{(2)}) = f(x) + f(x+\alpha^{(1)}+\alpha^{(2)}). \tag{23}$$

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 $\mathbb{F}_2^{2^n}$.

By Theorem 2, we know that $\mathcal{N}_h > 2^{n-2}$ thus $h$ is non-affine. In general, for arbitrary $\alpha \in \{0_r, \gamma\}$ and $\beta \in \mathbb{F}_2^{s/2} \times \{0_{\frac{s}{2}}\}$,

$$h(x,y) + h(x+\alpha, y+\beta) \text{ is linear if and only if } \alpha = 0_r \text{ and } \beta = 0_s. \tag{24}$$

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 $\phi$ 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 (24) 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 $\phi$ 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 (22), 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 10, we know $\mathcal{C}_h^{(\gamma)}$ is a linear binary code with parameters $[2^n, n+\frac{s}{2}+2]$. Now we prove $\mathcal{C}_h^{(\gamma)}$ is minimal. Define the following sets

$$A = \left\{(h(x+\alpha, y+\beta) + v\cdot(x,y))_{(x,y)\in\mathbb{F}_2^n} : \alpha \in \{0_r, \gamma\}, \beta \in \mathbb{F}_2^{s/2}\times\{0_{s/2}\}, v \in \mathbb{F}_2^n\right\},$$
$$B = \left\{(h(x,y) + h(x+\alpha, y+\beta) + v\cdot(x,y))_{(x,y)\in\mathbb{F}_2^n} : \alpha \in \{0_r, \gamma\}, \beta \in \mathbb{F}_2^{s/2}\times\{0_{s/2}\}, v \in \mathbb{F}_2^n\right\},$$

where $h(x,y) = f(x) + g(y)$. From the definition of $\mathcal{C}_h^{(\gamma)}$, the sets $A$ and $B$ correspond to $u = 0, u = 1$ respectively. Additionally, these sets form a partition of $\mathcal{C}_h^{(\gamma)}$.

Suppose $\mathcal{C}_h^{(\gamma)}$ is not a minimal linear code, that is, assume that there exist

$$u_1, u_2 \in \mathbb{F}_2, \alpha^{(1)}, \alpha^{(2)} \in \{0_r, \gamma\}, \beta^{(1)}, \beta^{(2)} \in \mathbb{F}_2^{s/2}\times\{0_{s/2}\} \text{ and } v^{(1)}, v^{(2)} \in \mathbb{F}_2^n$$

not all of them pairwise (referring to same symbols) equal to each other such that

$$(u_1h(x,y)+h(x+\alpha^{(1)}, y+\beta^{(1)})+v^{(1)}\cdot(x,y))_{(x,y)\in\mathbb{F}_2^n} \preceq (u_2h(x,y)+h(x+\alpha^{(2)}, y+\beta^{(2)})+v^{(2)}\cdot(x,y))_{(x,y)\in\mathbb{F}_2^n}.$$

Let us denote by $\mathbf{c}_1, \mathbf{c}_2$ these two codewords in $\mathcal{C}_h^{(\gamma)}$, thus we assume $\mathbf{c}_1 \preceq \mathbf{c}_2$ and $\mathbf{c}_1 \neq \mathbf{c}_2$. We will prove that $\mathbf{c}_1$ is the zero codeword. There are four cases to consider according to the possible values of $(u_1, u_2) \in \mathbb{F}_2 \times \mathbb{F}_2$. We only provide the proof when $u_1 = u_2 = 0$ and for convenience of the reader the remaining (similar) cases are given in Appendix.

By definition of $\phi$, 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.

1. Assume that $\mathbf{c}_1, \mathbf{c}_2 \in A$, i.e., $u_1 = u_2 = 0$. There are two cases to be considered.

   (a) Suppose that
   $$\beta^{(1)} \neq \beta^{(2)} \text{ or } v^{(1)}\cdot(0_r, y) \neq v^{(2)}\cdot(0_r, y).$$
   Restricting these codewords to $(0_r, 0_s)$ we see that $f(\alpha^{(1)}) \neq 1$ or $f(\alpha^{(2)}) \neq 0$. The restriction of $\mathcal{C}_h^{(\gamma)}$ to the $y$-coordinates would give
   $$(g(y+\beta^{(1)})+v^{(1)}\cdot(0_r,y)+f(\alpha^{(1)}))_{y\in\mathbb{F}_2^s} \preceq (g(y+\beta^{(2)})+v^{(2)}\cdot(0_r,y)+f(\alpha^{(2)}))_{y\in\mathbb{F}_2^s}.$$
   A contradiction to (i) in Lemma 7.

   (b) Suppose that
   $$\beta^{(1)} = \beta^{(2)} \text{ and } v^{(1)}\cdot(0_r, y) = v^{(2)}\cdot(0_r, y).$$
   We then have that
   $$f(x+\alpha^{(1)}) + v^{(1)}\cdot(x, 0_s) \neq f(x+\alpha^{(2)}) + v^{(2)}\cdot(x, 0_s)$$
   and
   $$(f(x+\alpha^{(1)}) + v^{(1)}\cdot(x, 0_s))_{x\in\mathbb{F}_2^r} \preceq (f(x+\alpha^{(2)}) + v^{(2)}\cdot(x, 0_s))_{x\in\mathbb{F}_2^r}.$$
   These two non-zero different codewords belong to $\mathcal{C}_f \oplus \mathcal{C}_{D_\gamma f}$ and they cover each other. This contradicts the minimality of $\mathcal{C}_f \oplus \mathcal{C}_{D_\gamma f}$.

Thus, assuming $\mathbf{c}_1, \mathbf{c}_2 \in A$ (when $u_1 = u_2 = 0$) we have that $\mathbf{c}_1 \preceq \mathbf{c}_2$ implies that $\mathbf{c}_1 = \mathbf{0}$.

It remains to show the wideness of $\mathcal{C}_h^{(\gamma)}$ assuming that $\mathcal{C}_{D_\gamma(f)}$ is wide. When $\beta = 0_s$, we have $h(x,y)+h(x+\gamma,y) = f(x)+f(x+\gamma)$. We know $w_{\min}\mathcal{C}_{D_\gamma(f)} = wt(f(x)+f(x+\gamma)+l^*(x))$, for some $l^*(x) \in \mathcal{B}_r$. The upper bound on $w_{\min}\mathcal{C}_h^{(\gamma)}$ satisfies

$$w_{\min}\mathcal{C}_h^{(\gamma)} \leq wt(f(x) + f(x+\gamma) + l^*(x)) = 2^s w_{\min}\mathcal{C}_{D_\gamma(f)}, \tag{25}$$

where $l^*(x) \in \mathcal{B}_n$ and also $f(x) + f(x+\gamma) + l^*(x) \in \mathcal{B}_n$. Similarly, there exists at least one $l'(x) \in B_r$ such that $w_{\max}\mathcal{C}_{D_\gamma(f)} = wt(f(x) + f(x+\gamma) + l'(x))$. Then,

$$wt(f(x) + f(x+\gamma) + l'(x)) = 2^s w_{\max(D_\gamma(f))} \leq w_{\max}\mathcal{C}_h^{(\gamma)} \tag{26}$$

for $l'(x) \in \mathcal{B}_n$. From (25) and (26), we have

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

□

### 4.2 Applications of Theorem 5

The importance of the above result lies in the fact that the initial conditions in Theorem 5 are entirely related to the function $f$ and the bent function $g$ in the $\mathcal{MM}$ class is selected using a non-covering permutation $\phi$. This gives a huge class of wide binary linear codes, which are not necessarily equivalent since one can for instance employ permutations $\phi$ (when defining $g$) of different algebraic degree. The following example exactly illustrates a possibility of getting non-equivalent codes using different permutations $\phi$.

**Example 7** *Let $r = 6, s = 10$. Consider the bent function $g \in \mathcal{B}_{10}$ as in (12) whose underlying permutation is the cubic AB permutation $\phi : \mathbb{F}_2^5 \to \mathbb{F}_2^5$ given by $\phi(y) = y^7$. Let us identify the integers in the interval $[0, \ldots, 63]$ with their binary representation (lexicographically ordered) which can be seen as a vector in $\mathbb{F}_2^6$, e.g. $(0,0,0,0,0,1)$ is identified with 1. Consider $f \in \mathcal{B}_6$ whose support is given by*

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

*Take $\gamma = (1,0,1,1,0,1)$. Using computer simulations, we could conclude that $\mathcal{C}_f \oplus \mathcal{C}_{D_\gamma f}$ is a wide linear code. Theorem 5 implies that $\mathcal{C}_h^{(\gamma)}$ is also wide. Moreover, its minimum distance $w_{min}$ equals $24576 = 3 \cdot 2^{13}$ and $w_{max} = 49152 = 3 \cdot 2^{14}$; thus $\mathcal{C}_h^{(\gamma)}$ has parameters $[2^{16}, 23, 3 \cdot 2^{13}]$ and ratio $w_{min}/w_{max} = 1/2$.*

*Let us now consider the bent function $g \in \mathcal{B}_{10}$ as in (12) whose defining non-covering permutation $\phi : \mathbb{F}_2^5 \to \mathbb{F}_2^5$ given by $\phi(y) = y^{30}$ is not AB. Let $f \in \mathcal{B}_6$ and $\gamma$ be defined as in the paragraph above. Again, Theorem 5 ensures the wideness of $\mathcal{C}_h^{(\gamma)}$. Furthermore, $w_{min} = 20480 = 5 \cdot 2^{12}$ and $w_{max} = 49152 = 3 \cdot 2^{14}$ which implies that $\mathcal{C}_h^{(\gamma)}$ is a wide linear code with parameters $[2^{16}, 23, 5 \cdot 2^{12}]$ and ratio $w_{min}/w_{max} = 5/12$.*

**Remark 5** *The initial conditions of Theorem 5 may be hard to satisfy but essentially the result given in Theorem 4 almost provides classes of Boolean functions suitable for this purpose. Example 5 and 6 illustrate exactly the existence of $f$ satisfying the conditions of Theorem 4 which can be utilized as initial functions in Theorem 5.*

To further emphasize a wide range of possibilities of employing the result of Theorem 5 we consider the use of function $f$ in Example 5 more specifically.

**Proposition 2** *Let $f \in \mathcal{B}_7$ be specified as in Example 5. Let $s = 10$ and define a bent function $g(y_1, y_2) = \phi(y_2) \cdot y_1$, with $(y_1, y_2) \in \mathbb{F}_2^5 \times \mathbb{F}_2^5$, where $\phi$ is a non-covering permutation on $\mathbb{F}_2^5$ without affine components. For $h(x, y) = f(x) + g(y)$, where $y = (y_1, y_2)$, define the code $\mathcal{C}_h^{(\gamma)}$ by means of (22). Then, $\mathcal{C}_h^{(\gamma)}$ is a $[2^{17}, 24]$ wide linear code for any non-covering permutation $\phi$ without affine components.*

**Remark 6** *Using simple Walsh spectrum arguments and known bounds on the nonlinearity of $\phi$, one can show that there are no non-covering permutations $\phi$ over $\mathbb{F}_2^n$ for $n \leq 4$. However, there are $32!$ permutations over $\mathbb{F}_2^5$ and many of these permutations are non-covering and do not have affine components. Employing the function $f \in \mathcal{B}_7$ in Example 5, each of these permutations specifies a wide linear $[2^{17}, 24]$ code $\mathcal{C}_h^{(\gamma)}$ among which there are many non-equivalent codes.*

**Example 8** *Set $r = 6$. Similarly to Example 7 we identify the integers in the interval $[0, \ldots, 63]$ with their binary representation. Consider $f \in \mathcal{B}_6$ whose support is given by*

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

*Take $\gamma = (0, 1, 1, 0, 1, 0)$. 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 $b \in \mathbb{F}_2^6$. Using computer simulations, we could conclude that $\mathcal{C}_f \oplus \mathcal{C}_{D_\gamma f}$ is wide linear code. From Theorem 5 we know that $\mathcal{C}_h^{(\gamma)}$ is also wide, where $h(x, y) = f(x) + g(y)$ and $g$ is a bent function of the form $g(y) = \phi(y^{(2)}) \cdot y^{(1)}$ such that $\phi$ is a non-covering permutation without affine components. The weight distribution of $\mathcal{C}_h^{(\gamma)}$ for an arbitrary $AB$ permutation $\phi$ over $\mathbb{F}_2^{s/2}$ and specifically over $\mathbb{F}_2^5$ are given in Table 2 and Table 3, respectively.*

Table 2: Weight distribution of $\mathcal{C}_h^{(\gamma)}$ in Example 8 for any $AB$ permutation $\phi : \mathbb{F}_2^{s/2} \to \mathbb{F}_2^{s/2}$

| Weight $w$ | Number of codewords $A_w$ |
|---|---|
| $2^{n-1} - 2^{r+s/2-1} + 2^{s/2}w$ | $2^{s+s/2+1}A_w^{(f)}$ when $w \notin \{0, w_{min}^{(f)}, 32, w_{max}^{(f)}\}$ |
| $2^{n-1} - 2^{r+s/2-1} + 2^{s/2}w$ | $2^{s/2+1}(2^{s-1} + 2^{s/2-1})A_w^{(f)}$ when $w \in \{w_{min}^{(f)}, w_{max}^{(f)}\}$ |
| $2^{n-1} + 2^{r+s/2-1} - 2^{s/2}w$ | $2^{s/2+1}(2^{s-1} - 2^{s/2-1})A_w^{(f)}$ when $w \in \{w_{min}^{(f)}, w_{max}^{(f)}\}$ |
| $2^{n-1} + w'(2^{\frac{s+s/2-1}{2}+1})$ $-2^{\frac{s+s/2-1}{2}+r}$ | $(2^{s/2}-1)((2^{s/2-2} + 2^{(s/2-3)/2})A_{w'}^{(D_\gamma f)} +$ $(2^{s/2-2} - 2^{(s/2-3)/2})A_{64-w'}^{(D_\gamma f)})$ if $w' \notin \{0, 32\}$ |
| $2^s w'$ | $A_{w'}^{(D_\gamma f)}$ if $w' \notin \{0, 32\}$ |
| $2^{n-1} - 2^{\frac{s+s/2-1}{2}+r}$ | $(2^{s/2}-1)((2^{s/2-2} + 2^{(s/2-3)/2})$ |
| $2^{n-1} + 2^{\frac{s+s/2-1}{2}+r}$ | $(2^{s/2}-1)((2^{s/2-2} - 2^{(s/2-3)/2})$ |
| $2^{n-1}$ | $2^n - 2^r + 33 \cdot 2^{s/2-1} - 161 \cdot 2^{s-1}$ $+47 \cdot 2^{(3s)/2+1} + 2^{(3s)/2+r} + 31$ |
| 0 | 1 |

When considering an arbitrary $AB$ permutation $\phi$ on $\mathbb{F}_2^{s/2}$, the weight distribution of $\mathcal{C}_h^{(\gamma)}$ in Table 2 can be described using the weight distributions of $\mathcal{C}_f$ and $\mathcal{C}_{D_\gamma f}$. Namely, if $A_w^{(f)}$ and $A_{w'}^{(D_\gamma f)}$ denote the frequency of the weight $w$ in $\mathcal{C}_f$ and the weight $w'$ in $\mathcal{C}_{D_\gamma f}$ respectively, then we can compute the weights of $\mathcal{C}_h^{(\gamma)}$ accordingly as shown in Table 2. The symbols $w_{max}^{(f)}, w_{max}^{(f)}$ represent the maximum and minimum weight of $\mathcal{C}_f$ and the variables $w, w'$ take values among the possible weights of $\mathcal{C}_f, \mathcal{C}_{D_\gamma f}$, respectively.

Table 3: Weight distribution of $\mathcal{C}_h^{(\gamma)}$ in Example 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 |

# 5 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 does not involve any initial conditions and therefore our approach based is 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 minimality of both $\mathcal{C}_f$ and of $\mathcal{C}_f \oplus \mathcal{C}_{D_\gamma f}$ one can construct a huge family of non-equivalent codes by using different 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 $\phi$) such families of non-equivalent wide binary linear codes of length $2^n$ can be designed for any $n \geq 7$. It is an interesting research problem to consider subcodes 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), and in the part by the Fundamental Research Funds for

the Central Universities (2019XKQYMS86). 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] A. E. Ashikhmin and A. Barg. Minimal vectors in linear codes. *IEEE Trans. on Inf. Theory*, vol. 44, no. 5, 2010–2017, 1998.

[2] D. Bartoli and M. Bonini. Minimal linear codes in odd characteristic. *IEEE Trans. on Inf. Theory*, vol. 65, no. 7, pp. 4152–4155, 2019.

[3] M. Bonini and M. Borello. Minimal linear codes arising from blocking sets. *Journal of Algebraic Combinatorics*, 2020, 115.

[4] C. Carlet. Boolean models and methods in mathematics, computer science, and engineering. *Encyclopedia of Mathematics and its Applications (No. 134) - Cambridge University Press*, pp. 398 – 469, 2013.

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

[6] S. Chang and J. Hyun. Linear codes from simplicial complexes. *Designs, Codes and Cryptography* vol. 86, pp. 2167–2181, 2018.

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

[8] C. Ding. Linear codes from some2-designs. *IEEE Trans. on Inf. Theory*, vol. 61, no. 6, pp. 3265–3275, 2015.

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

[10] C. Ding, Z. Heng and Z. Zhou. Minimal binary linear codes. *IEEE Trans. on Inf. Theory*, vol. 64, no. 10, pp. 6536–6545, 2018.

[11] K. Ding and C. Ding. A class of two-weight and three-weight codes and their applications in secret sharing. *IEEE Trans. on Inf. Theory*, vol. 64, no. 11, pp. 5835–5842, 2015.

[12] C. Ding and J. Yuan. Covering and secret sharing with linear codes. In: *Discrete Mathematics and Theoretical Computer Science*, Lecture Notes in Computer Science, vol. 2731, Springer Verlag, pp. 11–25, 2003.

[13] Z. Heng, C. Ding and Z. Zhou. Minimal Linear Codes over Finite Fields. *Finite Fields Appl.*, vol. 54, pp. 176–196, 2018.

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

[15] R. L. McFarland. A family of noncyclic difference sets. *J. Combin. Theory, Ser. A,* vol. 15, pp.1–10, 1973.

[16] S. Mesnager, Y. Qi, H. Ru and C. Thang. Minimal linear codes from characteristic functions. *IEEE Trans. on Inf. Theory*, vol. 66, no. 9, pp. 5404–5413, 2020.

[17] E. Pasalic, F. Zhang, R. Rodriguez and Y. Wei. Several classes of minimal binary linear codes violating the Ashikhmin-Barg's bound. Available at https://eprint.iacr.org/2020/1131.

[18] O. S. Rothaus. On bent functions. *J. Combin. Theory, Ser. A*, vol. 20, pp. 300–305, May 1976.

[19] D. Tang, C. Carlet and Z. Zhou. Binary linear codes from vectorial Boolean functions and their weight distribution. *Discrete Mathematics*, Vol. 340, Issue 12, pp. 3055–3072, 2017.

[20] C. Tang, Y. Qiu, Q. Liao, Z. Zhou. Full characterization of minimal linear codes as cutting blocking sets. Available at https://arxiv.org/abs/1911.09867.

[21] G. Xu, L. Qu Three classes of minimal linear codes over the finite fields of odd characteristic. *IEEE Trans. on Inf. Theory*, vol. 65, no. 11, pp. 7067–7078, 2019.

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

# Appendix

*Proof.* (**Theorem 5**, the remaining cases are proved assuming that $\mathbf{c}_1 \preceq \mathbf{c}_2$ and showing that necessarily $\mathbf{c}_1 = \mathbf{0}$)

2. Consider the case when $\mathbf{c}_1, \mathbf{c}_2$ belong to $B$, i.e., $u_1 = u_2 = 1$. There are two cases to be considered:

(a) Suppose that $\beta^{(1)} \neq \beta^{(2)}$ or $v^{(1)} \cdot (0_r, y) \neq v^{(2)} \cdot (0_r, y)$. Restricting $\mathbf{c}_1, \mathbf{c}_2 \in \mathcal{C}_h^{(\gamma)}$ to $(0_r, 0_s)$ (assuming $\mathbf{c}_1 \preceq \mathbf{c}_2$) we get $f(0_r) + f(\alpha^{(1)}) \neq 1$ or $f(0_r) + f(\alpha^{(2)}) \neq 0$. Now, restricting to the $y$-coordinates gives that the codeword

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

is covered by

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

Lemma 8 implies that $g(y) + g(y + \beta^{(1)}) + v^{(1)} \cdot (0_r, y) = 0$, for all $y \in \mathbb{F}_2^s$. This gives that $\beta^{(1)} = 0_s$ and $v^{(1)} \cdot (0_r, y)$ is zero.

Now, if $f(x) + f(x + \alpha^{(1)}) + v^{(1)} \cdot (x, 0_s)$ is non-zero, then there exists $x_0 \in \mathbb{F}_2^r$ such that

$$f(x_0) + f(x_0 + \alpha^{(1)}) + v^{(1)} \cdot (x_0, 0_s) = 1. \tag{27}$$

Also, the assumption $\mathbf{c}_1 \preceq \mathbf{c}_2$ applied to the projection onto the $x$-coordinates gives

$$f(x_0) + f(x_0 + \alpha^{(2)}) + v^{(2)} \cdot (x_0, 0_s) = 1. \tag{28}$$

Select $y_0 \in \mathbb{F}_2^s$ such that

$$g(y_0) + g(y_0 + \beta^{(2)}) + v^{(2)} \cdot (0_r, y_0) = 1, \tag{29}$$

which is possible since $g(y) + g(y + \beta^{(2)}) + v^{(2)} \cdot (0_r, y)$ is non-constant. Combining (27), (28) and (29), we obtain

$$\mathbf{c}_1(x_0, y_0) = f(x_0) + f(x_0 + \alpha^{(1)}) + v^{(1)} \cdot (x_0, 0_s) = 1$$

and

$$\mathbf{c}_2(x_0, y_0) = f(x_0) + g(y_0) + f(x_0 + \alpha^{(2)}) + g(y_0 + \beta^{(2)}) + v^{(2)} \cdot (x_0, y_0) = 0.$$

A contradiction to $\mathbf{c}_1 \preceq \mathbf{c}_2$. Hence $f(x) + f(x + \alpha^{(1)}) + v^{(1)} \cdot (x, 0_s) = \underline{0}$. Thus $\mathbf{c}_1$ is the zero codeword.

(b) Suppose that

$$\beta^{(1)} = \beta^{(2)} \text{ and } v^{(1)} \cdot (0_r, y) = v^{(2)} \cdot (0_r, y).$$

We then have that

$$f(x) + f(x + \alpha^{(1)}) + v^{(1)} \cdot (x, 0_s) \neq f(x) + f(x + \alpha^{(2)}) + v^{(2)} \cdot (x, 0_s)$$

and

$$(f(x) + f(x + \alpha^{(1)}) + v^{(1)} \cdot (x, 0_s))_{x \in \mathbb{F}_2^r}$$

is covered by

$$(f(x) + f(x + \alpha^{(2)}) + v^{(2)} \cdot (x, 0_s))_{x \in \mathbb{F}_2^r}.$$

We then get two different codewords in $\mathcal{C}_{D_\gamma f}$ covering each other hence $f(x) + f(x + \alpha^{(1)}) + v^{(1)} \cdot (x, 0_s) = 0$, for all $x \in \mathbb{F}_2^r$, since $\mathcal{C}_{D_\gamma f}$ is minimal. Thus, $\alpha^{(1)} = 0_r, v^{(1)} \cdot (x, 0_s) = 0$. Note that $f(x) + f(x + \alpha^{(2)}) + v^{(2)} \cdot (x, 0_s) \neq 0$ because $\mathbf{c}_1 \neq \mathbf{c}_2$. Hence, there exists $x_0 \in \mathbb{F}_2^r$ such that

$$f(x_0) + f(x_0 + \alpha^{(2)}) + v^{(2)} \cdot (x_0, 0_s) = 1. \tag{30}$$

Now, if

$$g(y) + g(y + \beta^{(1)}) + v^{(1)} \cdot (0_r, y) = g(y) + g(y + \beta^{(2)}) + v^{(2)} \cdot (0_r, y) \neq 0$$

then there is $y_0 \in \mathbb{F}_2^s$ such that

$$g(y_0) + g(y_0 + \beta^{(1)}) + v^{(1)} \cdot (0_r, y_0) = g(y_0) + g(y_0 + \beta^{(2)}) + v^{(2)} \cdot (0_r, y_0) = 1. \quad (31)$$

Combining the equations (30) and (31) we get

$$\mathbf{c}_1(x_0, y_0) = g(y_0) + g(y_0 + \alpha^{(1)}) + v^{(1)} \cdot (0_r, y_0) = 1$$

and

$$\mathbf{c}_2(x_0, y_0) = f(x_0) + g(y_0) + f(x_0 + \alpha^{(2)}) + g(y_0 + \beta^{(2)}) + v^{(2)} \cdot (x_0, y_0) = 0.$$

This contradicts $\mathbf{c}_1 \preceq \mathbf{c}_2$, hence

$$g(y) + g(y + \beta^{(1)}) + v^{(1)} \cdot (0_r, y) = 0, \ \forall y \in \mathbb{F}_2^s.$$

Therefore, $\mathbf{c}_1$ is the zero codeword.

3. We now consider $u^{(1)} = 0$ and $u^{(2)} = 1$ so that $\mathbf{c}_1 \in A$ and $\mathbf{c}_2 \in B$.

(a) Suppose that

$$\beta^{(1)} \neq \beta^{(2)} \text{ or } v^{(1)} \cdot (0_r, y) \neq v^{(2)} \cdot (0_r, y).$$

The restriction of $\mathbf{c}_1, \mathbf{c}_2 \in \mathcal{C}_h^{(\gamma)}$ to $(0_r, 0_s)$ (assuming $\mathbf{c}_1 \preceq \mathbf{c}_2$) implies $f(\alpha^{(1)}) \neq 1$ or $f(0_r) + f(\alpha^{(2)}) \neq 0$. Now, the restriction of $\mathcal{C}_h^{(\gamma)}$ to the $y$-coordinates gives that the codeword

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

is covered by

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

A contradiction to (ii) in Lemma 7.

(b) Suppose that

$$\beta^{(1)} = \beta^{(2)} \text{ and } v^{(1)} \cdot (0_r, y) = v^{(2)} \cdot (0_r, y).$$

Since $f$ is non-affine, we have that

$$f(x + \alpha^{(1)}) + v^{(1)} \cdot (x, 0_s) \neq f(x) + f(x + \alpha^{(2)}) + v^{(2)} \cdot (x, 0_s).$$

Assuming that $\mathbf{c}_1 \preceq \mathbf{c}_2$ then

$$(f(x + \alpha^{(1)}) + v^{(1)} \cdot (x, 0_s))_{x \in \mathbb{F}_2^r}$$

is covered by

$$(f(x) + f(x + \alpha^{(2)}) + v^{(2)} \cdot (x, 0_s))_{x \in \mathbb{F}_2^r}.$$

We have two different non-zero codewords in $\mathcal{C}_f \oplus \mathcal{C}_{D_\gamma f}$ covering each other, a contradiction to the minimality of $\mathcal{C}_f \oplus \mathcal{C}_{D_\gamma f}$.

4. Finally, the case when $u^{(1)} = 1$ and $u^{(2)} = 0$ ($\mathbf{c}_2 \in A$ and $\mathbf{c}_1 \in B$) can be reduced to the first case since the sum of an element in $B$ and an element in $A$ belongs to $A$.