Several classes of minimal binary linear codes violating the Aschikhmin-Barg's bound

E. Pasalic* R. Rodríguez† Fengrong Zhang ‡ Yongzhuang Wei §

Abstract

Minimal linear codes are a special class of codes which have important applications in secret sharing and secure two-party computation. These codes are characterized by the property that none of the codewords is covered by some other codeword. Denoting by w_{min} and w_{max} minimal and maximal weight of the codewords respectively, such codes are relatively easy to design when the ratio $w_{min}/w_{max} > 1/2$ (known as Aschikhmin-Barg's bound). On the other hand, there are few known classes of minimal codes violating this bound, hence having the property $w_{min}/w_{max} \leq 1/2$. In this article, we provide several *explicit* classes of minimal binary linear codes violating the Aschikhmin-Barg's bound, at the same time achieving a great variety of the ratio w_{min}/w_{max}. Our first generic method employs suitable characteristic functions of relatively low weight within the range $[n+1, 2^{n-2}]$. The second approach addresses a specification of characteristic functions covering the weights in $[2^{n-2}+1, 2^{n-2}+2^{n-3}-1]$ and containing a skewed (removing one element) affine subspace of dimension $n-2$. Finally, we also characterize an infinite family of such codes that utilize the class of so-called root Boolean functions of weight $2^{n-1}-(n-1)$, which are useful in certain hardware testing applications. Consequently, many infinite classes of minimal codes crossing the Aschikhmin-Barg's bound, with a wide range of the weight of their characteristic functions, are deduced. In certain cases we also completely specify the weight distribution of resulting codes.

Keywords: Minimal linear codes, Aschikhmin-Barg's bound, Characteristic functions, Root Boolean functions.

1 Introduction

Error correcting codes have many applications in communication systems, data storage devices and consumer electronics. The construction of linear codes with few weights has been widely studied, see e.g. [11, 13, 17, 20, 24], since these codes have many applications in

*University of Primorska, FAMNIT & IAM, Koper, Slovenia, e-mail: enes.pasalic6@gmail.com

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

‡School of Computer Science and Technology, China University of Mining and Technology, Xuzhou, Jiangsu 221116, China, and Mine Digitization Engineering Research Center of Minstry of Education, CUMT, Xuzhou, Jiangsu 221116, China, e-mail: zhfl203@cumt.edu.cn

§Guangxi Experiment Center of Information Science, Guilin University of Electronic Technology, Guilin, China, e-mail: walker_wyz@guet.edu.

consumer electronics, secret sharing schemes [5, 11, 22], authentication codes, communication, data storage system, association schemes, and strongly regular graphs. Recently, Ding [9] has published a valuable survey on the construction of binary linear codes from Boolean functions, in particular efficiently utilizing some well-known classes of Boolean functions such as bent and semi-bent functions.

On the other hand, apart from the standard properties of linear codes such as its length, dimension and minimum distance, linear codes may have additional properties that are useful in certain applications. In particular, *minimal linear codes* are characterized by the non-covering property which means that none of the (nonzero) codewords is covered by some other codeword. It was shown [2] by Aschikhmin and Barg that a sufficient condition for a linear code over $\mathbb{F}_q$ to be minimal is that $w_{min}/w_{max} > \frac{q-1}{q}$. Nevertheless, this condition is not necessary and the problem of designing minimal linear codes with the property $w_{min}/w_{max} \leq \frac{q-1}{q}$ appears to be much harder compared to only satisfying the Aschikhmin-Barg's ratio. The pioneering work in this direction was commenced by Ding *et al.* [10], where three classes of binary minimal linear codes were derived. These methods adjust standard construction techniques of designing cryptographic Boolean functions, such as the Maiorana-McFarland and partial spread method, for ensuring the desired properties of resulting codes.

This topic has later received attention in several works [6, 23, 19], where different approaches were considered for the same purpose. The use of non-binary alphabets, thus deriving minimal codes (satisfying $w_{min}/w_{max} > \frac{q-1}{q}$) from suitable mappings $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$, was addressed in [12] for the ternary case when $p = 3$. The design of minimal linear codes over finite fields $\mathbb{F}_{p^h}$ in odd characteristic (including the case of using mapping $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ since $h \geq 1$) is considered in [3] (extending the binary case by Ding *et al.* in [10]). Recently, the use of so-called cutting blocking sets [4, 18] and a method that employs characteristic functions [14] were considered. However, these methods primarily address the design of minimal codes without treating the extra condition on violating the Aschikhmin and Barg bound. In particular, the method based on cutting blocking sets [4] is quite general (since these induce minimality) but nevertheless specifying these sets is considered hard and Bonini and Borello in [4] only specified one family of minimal codes based on certain classes of homogenous polynomials (without considering the case when the bound of Aschikhmin and Barg is violated). We also mention some very recent contributions on this topic given in [1, 16].

In this article, we provide several classes of minimal binary linear codes with $w_{min}/w_{max} \leq 1/2$, which are for convenience called *wide minimal codes*. In general, employing an n-variable Boolean function f, a binary linear code can be defined as $\mathcal{C}_f = \{(af(x) \oplus \beta \cdot x)_{x \in \mathbb{F}_2^n} : a \in \mathbb{F}_2, \beta \in \mathbb{F}_2^n\}$. We show that the property of $\mathcal{C}_f$ being wide, referring to the condition $w_{min}/w_{max} \leq 1/2$, can be explicitly stated in terms of the Walsh spectral values of f. The derived condition, which is both necessary and sufficient, is quite simple and effective. Assuming that $\mathcal{C}_f$ is wide, we also show that the nonlinearity of an n-variable characteristic Boolean function cannot exceed $2^n/3$. To specify wide minimal codes, we firstly employ suitable characteristic functions of relatively low weight within the range $[n+1, 2^{n-2}]$. To increase the flexibility of using other weights of characteristic functions, we specify these supports of cardinality in $[2^{n-2}+1, 2^{n-2}+2^{n-3}-1]$ which all contain (skewed) affine subspace of dimension $n-2$ with one element removed. This skewed affine subspace is then enlarged through addition of a suitable set Γ so that such a characteristic function indeed specifies a

linear code which is both minimal and wide. In the special case, when the characteristic set is of cardinality $2^{n-2}+2$, we could specify the exact weight distribution of the resulting wide minimal codes. Such a specification is nevertheless not always possible, since there are many choices of the characteristic set and the relevant intersection estimates become hard to handle. Furthermore, we also provide an infinite family of such codes utilizing the class of so-called root Boolean functions of weight $2^{n-1}-(n-1)$ which are useful in certain hardware testing applications. To summarize, many infinite classes of minimal codes crossing the Aschikhmin-Barg's bound, with varying weight of characteristic functions and different ratio w_{min}/w_{max}, are deduced. In certain cases the weight distribution of resulting minimal (and wide) codes has also been specified. Essentially, using a direct connection between minimality and cutting blocking sets given in [4], we specify different families of cutting blocking sets with additional feature of satisfying the property of wideness which seems to be a non-trivial combinatorial problem. In this context, in the first place the results given in Theorem 3.3 and Theorem 3.4 give an elegant and specific solution for specifying these sets.

The rest of this article is organized as follows. In Section 2, we give some basic definitions related to Boolean functions and define linear codes that stem from these structures. Two constructions of wide minimal binary linear codes, having different weight of their characteristic functions are given in Section 3. In Section 4, we show that so-called root functions of maximal weight can be used as characteristic functions for specifying wide minimal binary linear codes. Some concluding remarks are given in Section 5.

2 Preliminaries

The vector space $\mathbb{F}_2^n$ is the space of all n-tuples $x=(x_1,\ldots,x_n)$, where $x_i\in\mathbb{F}_2$. For $x=(x_1,\ldots,x_n)$ and $y=(y_1,\ldots,y_n)$ in $\mathbb{F}_2^n$, the usual scalar (or dot) product over $\mathbb{F}_2$ is defined as $x\cdot y=x_1y_1\oplus\cdots\oplus x_ny_n$. The support of a vector x is defined by $\sup(x)=\{x_i : x_i=1\}$ and the Hamming weight of $x=(x_1,\ldots,x_n)\in\mathbb{F}_2^n$ is denoted and computed as $wt(x)=\sum_{i=1}^n x_i$. The cardinality of any set A is denoted by $||A||$, and in particular we sometimes use $||\sup(a)||=wt(a)$ to specify the number of nonzero coordinates of $a\in\mathbb{F}_2^n$. The distance between two vectors is then defined as $d(x,y)=wt(x\oplus y)$. By "$\sum$", we denote the integer sum (without modulo evaluation), whereas "$\bigoplus$" denotes the sum evaluated modulo two.

The set of all Boolean functions in n variables, which is the set of mappings from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, is denoted by $\mathcal{B}_n$. Especially, the set of affine functions in n variables is given by $\mathcal{A}_n=\{v\cdot x\oplus a \mid v\in\mathbb{F}_2^n,\ a\in\{0,1\}\}$, and similarly $\mathcal{L}_n=\{v\cdot x : v\in\mathbb{F}_2^n\}\subset\mathcal{A}_n$ denotes the set of linear functions. For every $v\in\mathbb{F}_2^n$, we will denote with H_v the support of linear function $v\cdot x$, that is, H_v represents the affine hyperplane $\sup(v\cdot x)=\{x\in\mathbb{F}_2^n : v\cdot x=1\}$. Additionally, for every $v\in\mathbb{F}_2^n$, $\overline{H}_v$ is the complement of H_v, i.e., $\overline{H}_v=\mathbb{F}_2^n\setminus H_v$ is the orthogonal complement of v.

For an arbitrary function $f\in\mathcal{B}_n$, the set of its values on $\mathbb{F}_2^n$ (*the truth table*) is defined as $T_f=(f(0,\ldots,0,0),f(0,\ldots,0,1),f(0,\ldots,1,0),\ldots,f(1,\ldots,1,1))$. The Walsh-Hadamard

transform of $f \in \mathcal{B}_n$, at any point $\beta \in \mathbb{F}_2^n$, is defined by

$$W_f(\beta) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus \beta \cdot x}. \tag{1}$$

The multiset $\{W_f(\beta) : \beta \in \mathbb{F}_2^n\}$, whose elements are Walsh coefficients, is called *Walsh spectrum* of f. The nonlinearity of a Boolean function $f \in \mathcal{B}_n$ (measuring the distance to the set of all affine functions), denoted by $nl(f)$, can be determined as

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{u \in \mathbb{F}_2^n} |W_f(u)|. \tag{2}$$

In general, there are two standard methods to define linear codes using mappings from $\mathbb{F}_p^n$ to $\mathbb{F}_p$ [9]. The first generic method, which has been greatly explored in many works, specifies a code $\mathcal{C}_f$ using a mapping $f : \mathbb{F}_p^n \to \mathbb{F}_p$ as:

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

where p is any prime. The dimension of this code is at most $n+1$ and its length is p^n. The dual of $\mathcal{C}_f$ has dimension at least $p^n - n - 1$.

On the other hand, the second generic method specifies a code by a subset $D_f = \{d_1, d_2, \ldots, d_m\} \subseteq \mathbb{F}_p^n$ so that it has a variable length m and the properties of such a code entirely depend on the choice of D_f. More precisely, one can define

$$\mathcal{C}_{D_f} = \{(d_1 \cdot x), (d_2 \cdot x), \ldots, (d_m \cdot x)) : x \in \mathbb{F}_p^n\}. \tag{4}$$

The set D_f is called the defining set of code $\mathcal{C}_{D_f}$ whose dimension is at most n. Some good codes (achieving the optimality of relevant parameters in certain cases) were derived in [8, 9] using suitable classes of vectorial mappings from $\mathbb{F}_p^n$ to $\mathbb{F}_p^n$. In particular, when Boolean functions are considered so that $f : \mathbb{F}_2^n \to \mathbb{F}_2$, this method gives some excellent codes when bent and semi-bent functions are employed.

The weight distribution of such 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 two fundamental results.

Theorem 2.1 *[9] Let f be a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Consider the linear code $\mathcal{C}_f$ defined by (3). If f is a nonlinear function (that is, for all $v \in \mathbb{F}_2^n$ it holds $f(x) \neq v \cdot x$), then $\mathcal{C}_f$ has dimension $m+1$. Its weight distribution is given by the following multiset:*

$$\left\{ 2^{n-1} - \frac{W_f(\beta)}{2} : \beta \in \mathbb{F}_2^n \right\} \cup \left\{ 2^{n-1},\ 0 \right\}, \tag{5}$$

Theorem 2.2 *[8, 9] Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ and denote $n_f = ||supp(f)||$, where $supp(f) = \{x \in \mathbb{F}_2^n : f(x) = 1\}$. If $2n_f + W_f(\beta) \neq 0$ for all $\beta \in \mathbb{F}_2^{n*}$, then $\mathcal{C}_{D_f}$ given by (4), where $D_f = \sup(f)$, is a binary linear code with length n_f and dimension n. Its weight distribution is given by the following multiset:*

$$\left\{ \left\{ \frac{2n_f + W_f(\beta)}{4} : \beta \in (\mathbb{F}_2^n)^* \right\} \right\} \cup \left\{ \{ \{0\} \} \right\}, \tag{6}$$

It was later noticed [9, Theorem 2] that a slightly more precise statement related to the dimension and weight distribution can be deduced.

3 Minimal Linear Codes

Minimal linear codes are an important type of codes due to their applications in data communication, storage, coding theory and cryptography. They have been successfully employed in secret sharing and secure two-party computations.

Consider a linear code $C \subseteq \mathbb{F}_q^n$ over the alphabet $\mathbb{F}_q$. For any given $u, v \in C$, we say that u *covers* v if and only if $\sup(v) \subseteq \sup(u)$. We denote this relation by $v \preceq u$. A codeword u is called *minimal* if u covers only the elements in $\langle u \rangle$, i.e., for every $v \in C$ if $v \preceq u$ then there exists $a \in \mathbb{F}_q$ such that $v = au$. The linear code C is said to be *minimal* if every element $c \in C$ is minimal.

Ashikhmin and Barg [2] gave a sufficient condition to obtain minimal linear codes over $\mathbb{F}_q$ through the following result.

Lemma 3.1 *[2] 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*

$$\frac{w_{\min}}{w_{\max}} > \frac{q-1}{q}, \tag{7}$$

then C is minimal.

There are plenty of examples of minimal linear codes constructed using Ashikhmin and Barg's condition ([5, 7, 8, 9, 13]), whereas some infinite families of minimal binary linear codes satisfying $w_{\min}/w_{\max} \leq 1/2$ can be found in [10, 12, 3, 23, 21]. Certain characterizations of minimality have been given when considering binary codes. We will say that a binary linear code is *narrow* if it satisfies the condition of Lemma 3.1, namely, $w_{\min}/w_{\max} > 1/2$. Otherwise, the code is said to be *wide*.

3.1 Wide linear codes

Recently, three infinite families of wide minimal binary linear codes were constructed using suitable Boolean functions in [10], where the code $\mathcal{C}_f$ is defined by means of (3). The property of minimality is characterized through the following results of Ding.

Proposition 3.1 *[10] Let $\mathcal{C} \subset \mathbb{F}_2^n$ be a binary linear code. Then, $\mathcal{C}$ is minimal if and only if for each pair of distinct nonzero codewords* a *and* b *in $\mathcal{C}$,*

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

Theorem 3.1 *[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 $\beta_1, \beta_2 \in \mathbb{F}_2^n$ it holds that*

$$W_f(\beta_1) + W_f(\beta_2) \neq 2^n, \tag{8}$$

and

$$W_f(\beta_1) - W_f(\beta_2) \neq 2^n. \tag{9}$$

The following fact is a quite straightforward consequence of the above results and it provides a simple characterization of the property of being "wide".

Proposition 3.2 *For a given non-affine Boolean function $f \in \mathcal{B}_n$, consider the code $\mathcal{C}_f$ given by (3). Then, $\mathcal{C}_f$ is wide if and only if*

$$2W_f(u_M) - W_f(u_m) \geq 2^n, \tag{10}$$

where u_M (resp. u_m) is such that $W_f(u_M)$ (resp. $W_f(u_m)$) is maximal (resp. minimal).

Proof. Since f is non-affine, then its Walsh spectrum contains at least one positive value and at least one negative value, which implies that $W_f(u_M) > 0$ and $W_f(u_m) < 0$. The existence of both positive and negative values in the Walsh spectrum can be easily confirmed using Titsworth theorem, which states that $\sum_{u\in\mathbb{F}_2^n} W_f(u)W(u+s) = 0$ for any $s \in \mathbb{F}_2^{n*}$. Therefore, using (5), we have

$$w_{\min} = 2^{n-1} - \frac{W_f(u_M)}{2} \quad \text{and} \quad w_{\max} = 2^{n-1} - \frac{W_f(u_m)}{2}. \tag{11}$$

Further,

$$\begin{aligned} \tfrac{w_{\min}}{w_{\max}} \leq \tfrac{1}{2} &\iff 2w_{\min} \leq w_{\max} \\ &\iff 2(2^{n-1} - \tfrac{W_f(u_M)}{2}) \leq 2^{n-1} - \tfrac{W_f(u_m)}{2}. \end{aligned}$$

Hence, we have

$$\frac{w_{\min}}{w_{\max}} \leq \frac{1}{2} \iff 2^n \leq 2W_f(u_M) - W_f(u_m).$$

□

Remark 3.1 *Throughout this article we use $W_f(u_M)$ and $W_f(u_m)$ to denote, respectively, the maximal and minimal values in the Walsh spectrum of a given Boolean function $f \in \mathcal{B}_n$.*

The property of minimality of a code $\mathcal{C}_f$, characterized by Theorem 3.1, can alternatively be stated using only extremal Walsh spectral values of f.

Corollary 1 *Consider the code $\mathcal{C}_f$, where $f \in \mathcal{B}_n$ is non-affine. If f satisfies*

$$W_f(u_M) - W_f(u_m) < 2^n \quad \textit{and} \quad W_f(u_M) < 2^{n-1}, \tag{12}$$

then $\mathcal{C}_f$ is minimal.

Proof. Let $\beta_1, \beta_2 \in \mathbb{F}_2^n$. Since $W_f(u_M) \geq W_f(\beta_1)$ and $W_f(u_M) \geq W_f(\beta_2)$, then

$$W_f(\beta_1) + W_f(\beta_2) \leq 2W_f(u_M) < 2^n. \tag{13}$$

Now, as $W_f(\beta_2) \geq W_f(u_m)$ we have

$$W_f(\beta_1) - W_f(\beta_2) \leq W_f(u_M) - W_f(u_m) < 2^n, \tag{14}$$

using the first condition in (12) in the last inequality. The minimality then follows easily from Theorem 3.1 and equations (13) and (14). □

The following result gives an upper bound on the nonlinearity of a Boolean function $f \in \mathcal{B}_n$ in the case the resulting linear code $\mathcal{C}_f$ is wide.

Proposition 3.3 *Let $f \in \mathcal{B}_n$ be any non-affine Boolean function and $\mathcal{C}_f$ its associated code defined by (3). Then $nl(f) = \min\{w_{\min}, 2^n - w_{\max}\}$. Moreover, if $\mathcal{C}_f$ is wide then $nl(f) \leq \frac{2^n}{3}$.*

Proof. Notice that either $W_f(u_m)$ or $W_f(u_M)$ achieves the maximum absolute value in the Walsh spectrum of f. Then, using $nl(f) = 2^{n-1} - \frac{1}{2}\max_{u\in\mathbb{F}_2^n}|W_f(u)|$, we have that either

$$nl(f) = 2^{n-1} + \frac{1}{2}W_f(u_m)$$

or

$$nl(f) = 2^{n-1} - \frac{1}{2}W_f(u_M).$$

Employing (11), this gives that $nl(f) = 2^n - w_{\max}$ or $nl(f) = w_{\min}$, respectively. We conclude that $nl(f) = \min\{w_{\min}, 2^n - w_{\max}\}$.

If $\mathcal{C}_f$ is wide, then $2nl(f) \leq 2w_{\min} \leq w_{\max} \leq 2^n - nl(f)$. Thus, $nl(f) \leq \frac{2^n}{3}$. ∎

Remark 3.2 *According to the above results, we can observe that certain Boolean functions f cannot be used when constructing wide minimal (binary) linear codes. For instance, assume that $(W_f(u_m), W_f(u_M)) = (2^{-l}, 2^l)$ for $l \in \{\frac{n}{2}, \ldots, n-2, n-1\}$. If $l = n-1$, then $\mathcal{C}_f$ is clearly not minimal since $W_f(u_M) + W_f(u_m) = 2^n$. On the other hand, when $l \leq n-2$ we have $2W_f(u_M) - W_f(u_m) = 3 \cdot 2^l \leq 3 \cdot 2^{n-2} < 2^n$ and using Proposition 3.2 we conclude that $\mathcal{C}_f$ is narrow (hence minimal). Notice that some well-known classes of Boolean functions such as bent and semi-bent (characterized by $W_f \in \{\pm 2^{n/2}\}$ and $W_f \in \{0, \pm 2^{(n+1)/2}\}$ respectively) cannot give rise to wide codes (this can also be inferred from the bound $nl(f) \leq 2^n/3$).*

Very recently, a geometric approach for minimal codes was introduced in the literature [4] using vectorial blocking sets. The authors showed a strong connection between these two apparently non-related objects. We will not need to define these concepts in a general way rather we will use the following very particular instances.

A set $\mathcal{BS} \subseteq \mathbb{F}_2^n$ is a vectorial blocking set if it intersects nontrivially all $(n-1)$-dimensional subspaces $\overline{H}_u$, i.e. $\mathcal{BS}^* \cap \overline{H}_u \neq \emptyset$. A vectorial blocking set $\mathcal{BS} \subseteq \mathbb{F}_2^n$ is said to be d-dimensional if its span is d-dimensional, that is, $\dim(\langle \mathcal{BS} \rangle) = d$. A vectorial blocking set $\mathcal{BS} \subseteq \mathbb{F}_2^n$ is called a vectorial $(1, n-1)$-blocking set if $\mathcal{BS}$ does not contain any $(n-1)$-dimensional subspace $\overline{H}_u$. A vectorial blocking set $\mathcal{BS}$ is cutting if the intersection between $\mathcal{B}$ and every $(n-1)$-dimensional subspace is not contained in any other $(n-1)$-dimensional subspace.

Lemma 3.2 *[4] Let $\mathcal{BS} \subseteq \mathbb{F}_2^n$. The set $\mathcal{BS}$ is an n-dimensional cutting vectorial $(1, n-1)$-blocking set if and only if the following two conditions hold*

- *For every pair of distinct $u, u' \in (\mathbb{F}_2^n)^*$, it holds that $\mathcal{BS}^* \cap \overline{H}_u \not\subseteq \overline{H}_{u'}$.*
- *For every $u \in (\mathbb{F}_2^n)^*$ we have $\overline{H}_u \not\subseteq \mathcal{BS}$.*

The previous lemma is a straightforward rephrasing of the definitions, however, it somewhat simplifies them and that is why it will be extremely useful in the sequel. Following [4], given any Boolean function $f : \mathbb{F}_2^n \to F_2$, we will denote the set of zeros of f as $V(f)$, i.e.

$$V(f) = \{x \in \mathbb{F}_2^n : f(x) = 0\}.$$

The following theorem provides the aforementioned connection between minimal codes and vectorial blocking sets. More precisely, it gives a sufficient condition for the linear code $\mathcal{C}_f$ to be minimal in terms of the geometry of $V(f)$.

Theorem 3.2 *[4] If $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is a Boolean function such that:*

1) $V(f)$ is an n-dimensional cutting vectorial $(1, n-1)$-blocking set;

2) For every nonzero $u \in \mathbb{F}_2^n$, $\overline{H}_u \cup V(f) \neq \mathbb{F}_2^n$,

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

Remark 3.3 *A full characterization of minimality using vectorial blocking sets has been given in [18] (cf. Theorem 13). Every minimal code induces a vectorial cutting blocking set and vice versa, thus in principle one can track down the vectorial blocking set from any minimal code and one can create a minimal code from certain vectorial blocking sets.*

Let us recall that for every subset Δ of $\mathbb{F}_2^n$, the characteristic function f of Δ is the Boolean function defined as

$$f(x) = \begin{cases} 1, & x \in \Delta, \\ 0, & x \in \mathbb{F}_2^n \setminus \Delta. \end{cases} \tag{15}$$

When f is the characteristic function of Δ its set of zeros $V(f)$ equals the complement of Δ, i.e. $V(f) = \mathbb{F}_2^n \setminus \Delta$. This simple observation allows us to deduce the following corollary which will be more suitable for our purposes.

Corollary 2 *Let Δ be a subset of $\mathbb{F}_2^n$. If for every $u \neq u' \in (\mathbb{F}_2^n)^*$ the following properties hold:*

1) $H_u \cap \Delta \neq \emptyset$;

2) $\overline{H}_u \cap \Delta \neq \emptyset$,

3) $H_u \setminus H_{u'} \not\subseteq \Delta \setminus H_{u'}$;

then the code $\mathcal{C}_f$ given by (3), where f is the characteristic function of Δ, is a minimal binary code.

Proof. The three conditions imply the hypotheses in Theorem 3.2 simply by considering the complementary statements. Note that the statement "for every nonzero $u \in \mathbb{F}_2^n$, $H_u \cap \Delta \neq \emptyset$" is equivalent to "for every nonzero $u \in \mathbb{F}_2^n$, $\overline{H}_u \cup V(f) \neq \mathbb{F}_2^n$" thus the first condition in Corollary 2 is equivalent to the second condition in Theorem 3.2. Now we prove that $V(f)$

is an n-dimensional cutting vectorial $(1, n-1)$-blocking set. Indeed, suppose there is a hyperplane $\overline{H}_{u'}$ where $u' \neq 0_n$, such that the intersection $V(f)^* \cap \overline{H}_{u'}$ is contained in $\overline{H}_u$ for some $u \in (\mathbb{F}_2^n)^*$. Taking complements we have

$$H_u \subseteq \Delta \cup \{0_n\} \cup H_{u'}$$

which implies

$$H_u \setminus H_{u'} \subseteq \Delta \setminus H_{u'},$$

contradicting 3). This shows that $V(f)$ is an n-dimensional cutting vectorial blocking set. Finally observe that $V(f)$ cannot contain any hyperplane $\overline{H}_v$, otherwise

$$\Delta \subseteq H_u,$$

a contradiction to 2). We conclude that $V(f)$ is an n-dimensional cutting vectorial $(1, n-1)$-blocking set. ∎

3.2 Minimal codes from suitable characteristic functions of weight $\leq 2^{n-2}$

In what follows, based on Corollary 2 we give a general construction regarding the choice of support of f which ensures both minimality and wideness of the resulting codes. Most notably, this design of wide minimal linear codes only requires the inclusion of (any) basis vectors of $\mathbb{F}_2^n$ and at least one element in its span for defining the support of $f \in \mathcal{B}_n$.

Theorem 3.3 *Let $n \geq 5$ be a poitive integer. If $\Delta \subset \mathbb{F}_2^n$, used to specify $f \in \mathcal{B}_n$ through (15), satisfies the following conditions:*

a) $n + 1 \leq ||\Delta|| \leq 2^{n-2}$*;*

b) Δ *includes at least one basis* $\{a^{(1)}, \ldots, a^{(n)}\}$ *of* $\mathbb{F}_2^n$ *(with* $a^{(i)} \in \mathbb{F}_2^n$*) and at least one vector* $\tau_1 a^{(1)} \oplus \cdots \oplus \tau_n a^{(n)}$*, where* $(\tau_1, \ldots, \tau_n) \in \mathbb{F}_2^n$ *and* $wt(\tau_1, \ldots, \tau_n)$ *is even;*

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

Proof. We first claim that for every nonzero $u \in \mathbb{F}_2^n$ we have $H_u \cap \Delta \neq \emptyset$ and $\overline{H}_u \cap \Delta \neq \emptyset$, i.e. there exist $x^{(1)}, x^{(2)} \in \Delta$ such that $u \cdot x^{(2)} = 1$ $u \cdot x^{(1)} = 0$. For any $u \in \mathbb{F}_2^{n*}$, there are two possibilities to consider.

i) If there exists one vector $a^{(i)} \in \{a^{(1)}, \ldots, a^{(n)}\}$ such that $u \cdot a^{(i)} = 0$, then there must exist $a^{(j)} \in \{a^{(1)}, \ldots, a^{(n)}\} \subseteq \Delta$ such that $u \cdot a^{(j)} = 1$ since the dimension of the dual (orthogonal) space of u equals $n - 1$.

ii) If $u \cdot a^{(i)} = 1$ for all $i \in \{1, \ldots, n\}$, then we can define $x^{(2)} = \tau_1 a^{(1)} \oplus \cdots \oplus \tau_n a^{(n)} \in \Delta$. Consequently $u \cdot x^{(2)} = 0$, since $wt(\tau_1, \ldots, \tau_n)$ is even.

Note that for every other u', the set $H_u \setminus H_{u'}$ cannot be contained in $\Delta \setminus H_{u'}$ since $||H_u \setminus H_{u'}|| = 2^{n-2}$ and $||\Delta \setminus H_{u'}|| < 2^{n-2}$. Using Corollary 2, we conclude that $\mathcal{C}_f$ is a minimal code.

Finally, it is obvious that $w_{\max} \geq 2^{n-1}$ since the Hamming weight of any linear function equals 2^{n-1}. We also know that $||\sup(f)|| = ||\Delta|| \leq 2^{n-2}$, that is, $w_{\min} \leq ||\Delta|| \leq 2^{n-2}$. Thus $\frac{w_{\min}}{w_{\max}} \leq \frac{1}{2}$. ∎

Remark 3.4 *The weights of the codes constructed using the previous theorem have a very irregular distribution, nevertheless, their values rely completely on the cardinality of* Δ *thus we can prove that the maximum value in the Walsh spectrum of* f *is* $2^n - 2||\Delta||$ *and the other Walsh values belong to the set* $\{2||\Delta|| - 4, 2||\Delta|| - 8, \ldots, 2||\Delta|| - 4(||\Delta|| - 1)\}$.

Example 3.1 *Set* $n = 6$. *Consider the canonical basis* $\mathcal{E} = \{e_1, \ldots, e_6\}$ *and* $\tau = (1, 0, 1, 1, 1, 0)$. *Selecting* $\Delta = \mathcal{E} \cup \{\tau\}$ *we have* $||\Delta|| = 7$. *The code* $\mathcal{C}_f$ *is wide and minimal with weight enumerator given by*

$$1 + z^7 + 5z^{27} + 10z^{29} + 15z^{31} + 63z^{32} + 20z^{33} + 11z^{35} + 2z^{37},$$

thus its minimum distance is 7 *and the maximum distance is* 37, *in other words,* $\mathcal{C}_f$ *is an* 8*-valued code with parameters* $[64, 7, 7]$.

If we select 9 additional random vectors, say, $v_1, \ldots, v_9$ *such that* $\Delta = \mathcal{E} \cup \{\tau, v_1, \ldots, v_9\}$ *then we obtain a wide minimal code with parameters* $[64, 7, 16]$.

3.3 Minimal codes from suitable characteristic functions of weight $> 2^{n-2}$

In this section, we extend the approach presented above by specifying f, whose support has cardinality greater than 2^{n-2}, suitable for constructing wide minimal binary linear codes.

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 $||A \ominus B|| = ||A|| + ||B|| - 2||A \cap B||$. We recall a well-known result concerning the dimension of intersection of affine subspaces.

Lemma 3.3 *Let* $A = a \oplus V$ *and* $B = b \oplus W$ *be two affine subspaces of* $\mathbb{F}_2^n$ *whose dimension is in the range* $[1, n-1]$. *Then either*

- $A \cap B = \emptyset$, *or,*
- $A \cap B$ *is an affine subspace and* $\dim(A \cap B) \geq \dim(A) + \dim(B) - n$.

Remark 3.5 *Lemma 3.3 is an easy consequence of the well-known similar result on the intersection of linear subspaces. The bound is quite loose, giving no additional information about the mentioned intersection when* $\dim(A) + \dim(B) \leq n$. *When* $\dim(A) + \dim(B) > n$, *which will be considered in our main theorem, the intersection bound becomes non-trivial.*

The following lemma is useful for specifying wide minimal linear codes from characteristic functions that contain an $(n-2)$-dimensional affine subspace.

Lemma 3.4 *Let* V *be an* $(n-2)$*-dimensional linear subspace of* $\mathbb{F}_2^n$. *Let* $a \notin V$ *and* $A = a \oplus V$ *be an* $(n-2)$*-dimensional affine space. There exists a unique* $u_0 \in \mathbb{F}_2^{n*}$ *such that* $A \cap H_{u_0} = \emptyset$, *where* H_{u_0} *represents the affine hyperplane* $\sup(u_0 \cdot x) = \{x \in \mathbb{F}_2^n : u_0 \cdot x = 1\}$.

Proof. Let $\mathcal{V} = \{v_1, \ldots, v_{n-2}\}$ be a basis of V. Since $a \notin V$, we have that $\mathcal{V} \cup \{a\}$ is a linearly independent set, therefore $U = \langle \mathcal{V} \cup \{a\} \rangle$ is an $(n-1)$-dimensional subspace. This implies that $U = \overline{H}_{u_0}$, for a $u_0 \in \mathbb{F}_2^n$. Now, taking any $a \oplus v \in A$ we have $u_0 \cdot (a \oplus v) = 0$ which also implies $A \subseteq \overline{H}_{u_0}$. In other words, $A \cap H_{u_0} = \emptyset$ since $H_{u_0} \cup \overline{H}_{u_0} = \mathbb{F}_2^n$. Note that u_0 is unique because if there were another $u' \in \mathbb{F}_2^n$ such that $H_{u'} \cap A = \emptyset$ then $A \subseteq (\overline{H}_{u_0} \cap \overline{H}_{u'}) \setminus \{0_n\}$ which is impossible as $||(\overline{H}_{u_0} \cap \overline{H}_{u'}) \setminus \{0_n\}|| = 2^{n-2} - 1$. ∎

In what follows, we will use an $(n-2)$-dimensional affine subspace $A = a \oplus V$ of $\mathbb{F}_2^n$ and select an element $p_0 \in A$, so that $S = A \setminus \{p_0\}$ can be considered as a punctured affine subspace of dimension $n-2$. Adjoining a suitable disjoint set $\Gamma \subset \mathbb{F}_2^n$ to S, we will define characteristic functions that give rise to linear codes which are both minimal and wide.

Theorem 3.4 *Let $n \geq 4$ be a positive integer and $A = a \oplus V$ be an $(n-2)$-dimensional affine subspace of $\mathbb{F}_2^n$. Furthermore, fix an element $p_0 \in A$ and consider $S = A \setminus \{p_0\}$. Suppose that there is a set $\Gamma \subseteq \mathbb{F}_2^n \setminus (A \cup \{0_n\})$ of cardinality $0 < ||\Gamma|| < 2^{n-3}$ with the property:*

($\star$) $\Gamma \cap H_{u_0} \neq \emptyset$, where u_0 is the unique element of $\mathbb{F}_2^{n*}$ such that $A \cap H_{u_0} = \emptyset$.

Let $\Delta = S \cup \Gamma \cup \{0_n\}$ and define $f \in \mathcal{B}_n$ to be the characteristic function of Δ. Then, $\mathcal{C}_f$ given by (3) is a minimal binary linear code of length 2^n, dimension $n+1$ and minimum distance $d \in \{2^{n-2} - ||\Gamma|| + 2, \ldots, 2^{n-2} + ||\Gamma||\}$. Moreover, if $||\Gamma \cap H_{u_0}|| \leq 2^{n-3} - \frac{||\Gamma||}{2}$ then $\mathcal{C}_f$ is wide.

Proof. According to Lemma 3.3, for every $u \in (\mathbb{F}_2^n)^*$ different from $u \neq u_0$ it must be that either $A \in H_u$ or $||A \cap H_u|| = 2^{n-3}$. We will now verify the three conditions in Corollary 2 taking into account these possibilities. The condition ($\star$) guarantees that $\Delta \cap H_{u_0} \neq \emptyset$. Note that the difference $A \setminus \Delta$ equals $\{p_0\}$, hence $H_u \cap \Delta$ contains at least $2^{n-3} - 1$ elements. Given that $n \geq 4$, we see that for every $u \in \mathbb{F}_2^n$ it holds $H_u \cap \Delta \neq \emptyset$. The second condition in Corollary 2 readily holds since $0_n \in \overline{H}_u \cap \Delta$.

Now we prove the third condition in Corollary 2, so that for every pair of distinct $u, u' \in (\mathbb{F}_2^n)^*$ we have $H_u \setminus H_{u'} \not\subseteq \Delta \setminus H_{u'}$. Suppose that $H_u \setminus H_{u'} \subseteq \Delta \setminus H_{u'}$ for some $u \neq u' \in (\mathbb{F}_2^n)^*$. Recall that $||H_u \setminus H_{u'}|| = 2^{n-2}$. We now consider the following three cases:

1) Consider the case when $H_{u'} \cap A = \emptyset$, that is, $u' = u_0$. In this case either

$$||A \cap (H_u \setminus H_{u_0})|| = 2^{n-3} \text{ or } ||A \cap (H_u \setminus H_{u_0})|| = 2^{n-2}.$$

In the latter, $p_0 \in H_u \setminus H_{u_0}$ while $p_0 \notin \Delta$. In the former, we have

$$H_u \setminus H_{u_0} \subseteq (\Delta \cap H_u) \setminus H_{u_0}.$$

However, $||(\Delta \cap H_u) \setminus H_{u_0}|| < 2^{n-2}$ and $||H_u \setminus H_{u_0}|| = 2^{n-2}$, a contradiction. Therefore $H_u \setminus H_{u_0} \not\subseteq \Delta \setminus H_{u_0}$.

2) When $A \in H_{u'}$ we have that $||\Delta \setminus H_{u'}|| < 2^{n-3}$ since $S \subset H_{u'}$. Hence $H_u \setminus H_{u'}$ cannot be contained in $\Delta \setminus H_{u'}$.

3) Now consider $u' \in (\mathbb{F}_2^n)^*$ such that $||A \cap H_{u'}|| = 2^{n-3}$. Observe that $||\Delta \setminus H_{u'}|| < 2^{n-3} + 2^{n-3} = 2^{n-2}$ since S can only contribute with at most 2^{n-3} elements to this difference. Therefore $H_u \setminus H_{u'}$ cannot be contained in $\Delta \setminus H_{u'}$.

These three cases show that for every pair of distinct $u, u' \in (\mathbb{F}_2^n)^*$ we have $H_u \setminus H_{u'} \not\subseteq \Delta \setminus H_{u'}$. We have verified the conditions in Corollary 2 which establish the minimality of $\mathcal{C}_f$.

We finally show that $\mathcal{C}_f$ is wide. By hypothesis, we have $||\Gamma \cap H_{u_0}|| \leq 2^{n-3} - \frac{||\Gamma||}{2}$. Letting $\kappa = ||\Gamma \cap H_{u_0}||$, we have $||\Gamma|| \leq 2^{n-2} - 2\kappa$.
Notice that $||\Delta \setminus H_{u_0}|| = 2^{n-2} + ||\Gamma|| - \kappa$ and $||H_{u_0} \setminus \Delta|| = 2^{n-1} - \kappa$. Thus, the codeword $T_{f(x)\oplus u_0 \cdot x}$ has weight

$$2^{n-1} + 2^{n-2} + ||\Gamma|| - 2\kappa,$$

so that $w_{max} \geq 2^{n-1} + 2^{n-2} + ||\Gamma|| - 2\kappa$. We also know that $w_{min} \leq 2^{n-2} + ||\Gamma||$, since $||\Delta|| = 2^{n-2} + ||\Gamma||$. Thus, we deduce

$$2w_{min} \leq 2^{n-1} + 2||\Gamma|| \leq 2^{n-1} + ||\Gamma|| + 2^{n-2} - 2\kappa \leq w_{max},$$

which means that $\frac{w_{\min}}{w_{\max}} \leq \frac{1}{2}$. □

A special case of this method, which applies when $||\Gamma|| \in \{1, 2\}$, is given below.

Corollary 3 *Let $n \geq 4$ and $\mathcal{B} = \{a^{(1)}, \ldots, a^{(n)}\}$, with $a^{(i)} \in \mathbb{F}_2^n$, be a basis of $\mathbb{F}_2^n$ such that $a^{(n)}$ is of odd weight and orthogonal to all $a^{(i)}$, i.e, $a^{(n)} \cdot a^{(i)} = 0$ for $1 \leq i \leq n-1$. Define $V = \langle a^{(1)}, \ldots, a^{(n-2)} \rangle$ and assign $A = a^{(n-1)} \oplus V$. Let $S = A \setminus \{p_0\}$ for some $p_0 \in A$. Fix any $(\tau_1, \ldots, \tau_{n-1}) \in \mathbb{F}_2^{n-1} \setminus \{0_{n-1}\}$ and define Γ as follows:*

$$\Gamma = \begin{cases} \{a^{(n)}\} & \text{if } n = 4, \\ \{a^{(n)}, a^{(n)} \oplus \tau_{n-1} a^{(n-1)} \oplus \cdots \oplus \tau_1 a^{(1)}\} & \text{if } n > 4. \end{cases}$$

Suppose Δ and f are defined as in Theorem 3.4. Then $\mathcal{C}_f$ is a wide minimal code.

Proof. To prove minimality of $\mathcal{C}_f$ it is sufficient to verify the condition $(\star)$, for Γ specified above. We now show that the unique hyperplane disjoint to A is $H_{a^{(n)}}$, thus $a^{(n)} = u_0$ in the context of Lemma 3.4. Indeed, since $a^{(n)} \cdot a^{(i)} = 0$ for every i with $1 \leq i \leq n-1$, it holds that

$$\langle a^{(1)}, \ldots, a^{(n-1)} \rangle \cap H_{a^{(n)}} = \emptyset,$$

which implies that $A \cap H_{a^{(n)}} = \emptyset$. Since the weight of $a^{(n)}$ is odd by hypothesis, we have that $a^{(n)} \in H_{a^{(n)}}$. Therefore, $\Gamma \cap H_{a^{(n)}} \neq \emptyset$ and $(\star)$ is satisfied, thus the code $\mathcal{C}_f$ is minimal.

The property of being wide can also be confirmed using Theorem 3.4, thus verifying that

$$||\Gamma \cap H_{a^{(n)}}|| \leq 2^{n-3} - \frac{||\Gamma||}{2}.$$

For $n = 4$, we easily confirm that $||\Gamma \cap H_{a^{(n)}}|| = 1 < \frac{3}{2} = 2 - \frac{1}{2}$, thus the code $\mathcal{C}_f$ is wide in this case. For $n \geq 5$, observe that $a^{(n)} \oplus \tau_{n-1} a^{(n-1)} \oplus \cdots \oplus \tau_1 a^{(1)} \in H_{a^{(n)}}$, since $a^{(n)} \cdot a^{(i)} = 0$ for every i smaller than n and $a^{(n)} \cdot a^{(n)} = 1$ (because the weight of $a^{(n)}$ is odd). Clearly, the latter equality implies that $a^{(n)} \in H_{a^{(n)}}$. Hence,

$$||\Gamma \cap H_{a^{(n)}}|| = 2 < 2^{n-3} - 1 \quad \text{for } n \geq 5,$$

and therefore $\mathcal{C}_f$ is wide. □

The minimum distance d depends on the intersection of $(n-2)$-dimensional affine subspace A with affine hyperplanes of the form H_u. The following examples illustrate this dependency.

Example 3.2 *Let $n = 5$ and assume $||\Gamma|| = 2$. Consider the linear subspace*

$$V = \langle (1,1,0,0,0), (1,0,1,0,1), (0,0,1,0,1) \rangle$$

and define $A = (1,1,1,1,1) \oplus V$. Let $p_0 = (1,1,1,1,1) \oplus (1,1,0,0,0) = (0,0,1,1,1)$ and define $S = A \setminus \{p_0\}$ and $\Gamma = \{(0,0,1,1,0), (1,1,0,1,1)\}$. Suppose Δ and f are defined as in Theorem 3.4. Then, by using computer simulations, one can confirm that $\mathcal{C}_f$ is a wide minimal code with $w_{min} = 8$ and $w_{max} = 22$. Indeed, the set $U = \sup((0,0,1,0,1) \cdot x)$ is (the unique) affine hyperplane disjoint to A and $\Gamma \subseteq U$.

Example 3.3 *Let again $n = 5$ and $||\Gamma|| = 2$. Consider the linear subspace*

$$V = \langle (1,1,1,1,1), (1,1,0,1,0), (1,1,0,1,1) \rangle$$

and define $A = (1,0,1,1,0) \oplus V$. Let $p_0 = (1,0,1,1,0) \oplus (1,1,1,1,1) = (0,1,0,0,1)$ and define $S = A \setminus \{p_0\}$ and $\Gamma = \{(0,0,1,0,1), (0,0,1,1,0)\}$. Again specifying Δ and f as in Theorem 3.4 one can verify that $\mathcal{C}_f$ is a wide minimal code with $w_{min} = 10$ (which is different from Example 3.2) and $w_{max} = 24$. In this case, the set $U = \sup((1,0,0,1,0) \cdot x)$ is (the unique) affine hyperplane disjoint to A and $||\Gamma \cap U|| = ||\{(0,0,1,1,0)\}|| = 1$.

When $||\Gamma|| = 2$, there are a few possibilities for the cardinality of intersection $\Gamma \cap H_u$. Consequently, we can specify the weight distribution of the code described in Corollary 3 because their values only depend on the choice of the vector $(\tau_1, \ldots, \tau_{n-1})$. The weight distributions are listed in descending order in Tables 1, 2 and 3.

Weight w	Number of codewords A_w
$2^{n-1} + 2^{n-2} - 2$	1
$2^{n-1} + 2$	$2^n - 2^{n-2} - 3$
2^{n-1}	$2^n - 1$
$2^{n-1} - 2$	$2^{n-2} - 1$
$2^{n-2} + 2$	3

Table 1: Weights of 5-valued wide minimal codes $\mathcal{C}_f$ when $(\tau_1, \ldots, \tau_{n-1}) = (0, 0, \ldots, 0, 1)$.

Weight w	Number of codewords A_w
$2^{n-1}+2^{n-2}-2$	1
$2^{n-1}+4$	2^{n-3}
$2^{n-1}+2$	$2^n-5\cdot 2^{n-3}-3$
2^{n-1}	$2^n-1+3\cdot 2^{n-3}$
$2^{n-1}-2$	$2^{n-3}-1$
$2^{n-2}+2$	3

Table 2: Weights of 6-valued wide minimal codes $\mathcal{C}_f$ when $(\tau_1,\ldots,\tau_{n-1})$ is such that $\tau_{n-1}=1$ and $(\tau_1,\ldots,\tau_{n-2})$ is nonzero.

Weight w	Number of codewords A_w
$2^{n-1}+2^{n-2}-2$	1
$2^{n-1}+4$	$2^{n-3}-1$
$2^{n-1}+2$	$2^n-2^{n-3}-3$
2^{n-1}	$2^n+2^n-2^{n-3}-4$
$2^{n-1}-2$	$2^{n-3}-1$
$2^{n-2}+4$	1
$2^{n-2}+2$	1
2^{n-2}	1

Table 3: Weights of 8-valued wide minimal codes $\mathcal{C}_f$ when $(\tau_1,\ldots,\tau_{n-1})$ is such that $\tau_{n-1}=0$ and $(\tau_1,\ldots,\tau_{n-2})$ is nonzero.

4 Minimal linear codes from root functions

In this section we employ the so-called root functions analyzed in [15], useful for hardware circuits testing, to derive minimal codes with the property that $w_{min}/w_{max}\leq 1/2$. Firstly, we will derive two general results similar to Theorem 3.4. The main difference is essentially the cardinality of support, which is given as $||\Delta||=2^{n-1}-||\Gamma||+1$ for a suitably chosen Γ with $||\Gamma||\leq 2^{n-2}$. Afterwards, we will use root functions to construct associated linear codes. It is worth mentioning that the minimality of the codes constructed in this section is not a consequence of Corollary 2.

Theorem 4.1 *Let $n\geq 4$ be a positive integer. Fix $u_0\in\mathbb{F}_2^{n*}$ and select a point $p_0\in H_{u_0}$. Specify a nonempty set $\Gamma\subseteq\overline{H}_{u_0}$ satisfying the following two properties:*

- $||\Gamma||\leq 2^{n-2}$.
- *For every $v\in\mathbb{F}_2^{n*}$, with $v\neq u_0$ and such that $p_0\in H_v$, we have $\Gamma\cap H_v\neq\emptyset$.*

Let now $\Delta=(\overline{H}_{u_0}\setminus\Gamma)\cup\{p_0\}$ and consider the code $\mathcal{C}_f$ given by (3), where f is the characteristic function of Δ. Then, $w_{min}=||\Delta||=2^{n-1}-||\Gamma||+1$ and $w_{max}=2^n-||\Gamma||-1$. Furthermore, the code $\mathcal{C}_f$ is wide and minimal.

Proof. Recall that the weight of a codeword $\boldsymbol{c}_{a,v} = af(x)+v\cdot x$ in $\mathcal{C}_f$ is given by $||\sup(\boldsymbol{c}_{a,v})||$ where

$$\sup(\boldsymbol{c}_{a,v}) = \begin{cases} \Delta \ominus H_v & \text{if } a \neq 0 \\ H_v & \text{otherwise.} \end{cases}.$$

We will estimate the possible values for $||\sup(\boldsymbol{c}_{a,v})||$. Since $||\sup(\boldsymbol{c}_{0,v})|| = 2^{n-1}$ for every $v \in \mathbb{F}_2^{n*}$, we assume that $a = 1$ and denote $\boldsymbol{c}_{1,v}$ as $\boldsymbol{c}_v$. There are three cases to be considered.

(i) When $v = 0_n$ it holds that $\sup(\boldsymbol{c}_{0_n}) = \Delta$ and $||\Delta|| = 2^{n-1} - ||\Gamma|| + 1$.

(ii) If $v = u_0$, then $H_{u_0} \cap \Delta = \{p_0\}$ and consequently

$$wt(\boldsymbol{c}_{u_0}) = ||\Delta \ominus H_{u_0}|| = ||\Delta|| + ||H_{u_0}|| - 2 = 2^n - ||\Gamma|| - 1.$$

(iii) Finally, suppose $v \neq 0_n$ and $v \neq u_0$. We know that $||\overline{H}_{u_0} \cap H_v|| = 2^{n-2}$, therewith we will estimate the cardinality of $\Delta \cap H_v$. This cardinality completely depends on the way $\Gamma \cup \{p_0\}$ intersects H_v. It attains the smallest value when Γ is a subset of H_v and $p_0 \notin H_v$, then $||\Delta \cap H_v|| \geq 2^{n-2} - ||\Gamma||$. On the other hand, by the definition of Γ, we cannot have simultaneously that Γ is disjoint to H_v and $p_0 \in H_v$. Therefore, $||\Delta \cap H_v|| \leq 2^{n-2}$ so that

$$2^{n-2} - ||\Gamma|| \leq ||\Delta \cap H_v|| \leq 2^{n-2}.$$

Since $wt(\boldsymbol{c}_v) = ||\Delta \ominus H_v|| = ||\Delta|| + ||H_v|| - 2||\Delta \cap H_v||$, we can now bound the weight $wt(\boldsymbol{c}_v)$ as follows,

$$2^{n-1} - ||\Gamma|| + 1 \leq wt(\boldsymbol{c}_v) \leq 2^{n-1} + ||\Gamma|| + 1.$$

Considering $wt(\boldsymbol{c}_v)$ for different $v \in \mathbb{F}_2^n$, we conclude that $w_{min} = ||\Delta|| = 2^{n-1} - ||\Gamma|| + 1$. Now, $||\Gamma|| \leq 2^{n-2}$ if and only if $2^{n-1} + ||\Gamma|| + 1 \leq 2^n - ||\Gamma|| - 1$, and therefore $w_{max} = 2^n - ||\Gamma|| - 1$.

To show the minimality and wideness of $\mathcal{C}_f$, we use the expressions for w_{min} and w_{max}. Since

$$2w_{min} = 2^n - 2||\Gamma|| + 2 \leq 2^n - ||\Gamma|| - 1 = w_{max},$$

we have $\frac{w_{min}}{w_{max}} \leq \frac{1}{2}$ and $\mathcal{C}_f$ is wide. To prove the minimality of $\mathcal{C}_f$, we compute the maximum and minimum Walsh values as

$$W(u_m) = 2^n - 2w_{max} = -2^n + 2||\Gamma|| + 2$$

and

$$W(u_M) = 2^n - 2w_{min} = 2||\Gamma|| - 2.$$

Since $||\Gamma|| \leq 2^{n-2}$ then $W(u_M) = 2||\Gamma|| - 2 < 2^{n-1}$. Similarly, one easily deduces that

$$W(u_M) - W(u_m) = (2||\Gamma|| - 2) - (-2^n + 2||\Gamma|| + 2) = 2^n - 4 < 2^n.$$

By applying Corollary 1, we conclude that $\mathcal{C}_f$ is minimal as well. ∎

The results similar to Theorem 4.1 can be proved using the same lines of reasoning in a *complementary* setting. This particularly means that the selection of p_0 and Γ can be performed using orthogonal complements of the relevant hyperplanes. Observe that the method described below is indeed almost verbatim compared to Theorem 4.1 .

Theorem 4.2 *Let $n \geq 4$ be a positive integer. Fix $u_0 \in \mathbb{F}_2^{n*}$ and select a point $p_0 \in \overline{H}_{u_0}$. Specify a nonempty set $\Gamma \subseteq H_{u_0}$ satisfying the following three properties:*

- $n \leq ||\Gamma|| < 2^{n-2}$.
- *For every $v \in \mathbb{F}_2^{n*}$, where $v \neq u_0$, if $p_0 \in H_v$ then we have $\Gamma \cap H_v \neq \emptyset$.*
- *For every $v \in \mathbb{F}_2^{n*}$, where $v \neq u_0$, if $p_0 \notin H_v$ then we have $\Gamma \cap \overline{H}_v \neq \emptyset$.*

Let $\Delta = (H_{u_0} \setminus \Gamma) \cup \{p_0\}$ and consider the code $\mathcal{C}_f$ given by (3), where f is the characteristic function of Δ. Then, $w_{min} = ||\Gamma|| + 1$ and $w_{max} \leq 2^{n-1} + ||\Gamma|| - 1$ for the code $\mathcal{C}_f$. Furthermore, the code $\mathcal{C}_f$ is wide and minimal.

Proof. Similarly to the proof of Theorem 4.1, we estimate $||\sup(\boldsymbol{c}_{a,v})||$ for different $v \in \mathbb{F}_2^n$. We again assume that $a = 1$ and consider three cases.

(i) When $v = 0_n$, it holds that $\sup(\boldsymbol{c}_{0_n}) = \Delta$ and $||\Delta|| = 2^{n-1} - ||\Gamma|| + 1$.

(ii) Suppose $v = u_0$. In this case, using the fact that $\Gamma \subseteq H_{u_0}$ and definition of Δ, we have

$$||H_{u_0} \cap \Delta|| = 2^{n-1} - ||\Gamma||,$$

and thus

$$wt(\boldsymbol{c}_{u_0}) = ||\Delta \ominus H_{u_0}|| = ||\Gamma|| + 1.$$

(iii) Now, assume $v \neq 0_n$ and $v \neq u_0$. Using that $||H_{u_0} \cap H_v|| = 2^{n-2}$, we will estimate the cardinality of $\Delta \cap H_v$. The cardinality of this intersection is determined by the way $\Gamma \cup \{p_0\}$ intersects H_v. By the third property of Γ, it is impossible that Γ is a subset of H_v and $p_0 \notin H_v$ at the same time, therefore it holds that

$$||\Delta \cap H_v|| \geq 2^{n-2} - ||\Gamma|| + 1.$$

On the other hand, by the second property of Γ, we cannot have simultaneously that Γ is disjoint to H_v and $p_0 \in H_v$. Therefore, $||\Delta \cap H_v|| \leq 2^{n-2}$ implying that

$$2^{n-2} - ||\Gamma|| + 1 \leq ||\Delta \cap H_v|| \leq 2^{n-2}.$$

As before, since $wt(\boldsymbol{c}_v) = ||\Delta \ominus H_v|| = ||\Delta|| + ||H_v|| - 2||\Delta \cap H_v||$ we can bound the weight $wt(\boldsymbol{c}_v)$ as follows,

$$2^{n-1} - ||\Gamma|| + 1 \leq wt(\boldsymbol{c}_v) \leq 2^{n-1} + ||\Gamma|| - 1.$$

Obviously, $w_{max} \leq 2^{n-1} + ||\Gamma|| - 1$. Now, $||\Gamma|| + 1$ is the minimum weight of the code $\mathcal{C}_f$ because $||\Gamma|| + 1 < 2^{n-1} - ||\Gamma|| + 1$ if and only if $||\Gamma|| < 2^{n-2}$.

To show the minimality and wideness we notice that $2^{n-1} \leq w_{max} \leq 2^{n-1} + ||\Gamma|| - 1$ and $w_{min} = ||\Gamma|| + 1$. Since $2w_{min} = 2||\Gamma|| + 2 \leq 2^{n-1} \leq w_{max}$, we have $\frac{w_{min}}{w_{max}} \leq \frac{1}{2}$ and therefore $\mathcal{C}_f$ is wide. Now, we will prove minimality of $\mathcal{C}_f$. Theorem 4.2 and equation (11) give

$$W_f(u_m) = 2^n - 2w_{max} \geq -2||\Gamma|| + 2$$

and

$$W_f(u_M) = 2^n - 2w_{min} = 2^n - 2||\Gamma|| - 2.$$

In this case one cannot apply Corollary 1, since $W_f(u_M)$ is always larger or equal than 2^{n-1}. Instead, we will prove it using a different approach that uses the second largest Walsh coefficient as well.

From the proof of Theorem 4.2, we can observe that the minimum weight is attained by a single codeword and the next weight (in increasing order) is $2^{n-1} - ||\Gamma|| + 1$. Hence, the largest Walsh value is attained once and the second one is $W_f(u_M^{(2)}) := 2||\Gamma|| - 2$ (again using (11)). Notice that

$$W_f(u_M) + W_f(u_M^{(2)}) = 2^n - 2||\Gamma|| - 2 + 2||\Gamma|| - 2 = 2^n - 4 < 2^n.$$

Since $W_f(u_M)$ for $\mathcal{C}_f$ is attained exactly once, for every distinct $u, v \in \mathbb{F}_2^{n*}$ it holds that

$$W_f(u) + W_f(v) \leq W_f(u_M) + W_f(u_M^{(2)}) < 2^n,$$

and

$$W_f(u) - W_f(v) \leq W_f(u_M) - W_f(u_m) \leq (2^n - 2||\Gamma|| - 2) - (-2||\Gamma|| + 2) = 2^n - 4 < 2^n.$$

According to Theorem 3.1, $\mathcal{C}_f$ is minimal. □

4.1 Root functions and derived linear codes

A Boolean function $f \in \mathcal{B}_n$ is called a *root function* if for every $x \in \mathbb{F}_2^n$ we have that $f(x) = 0$ if and only if there is a $y \in \mathbb{F}_2^n$ such that $f(y) = 1$ and $d(x, y) = 1$. A family of non-affine root functions of maximal weight was constructed in [15] using the following procedure.

Construction A

- Consider the affine function $l_n(x) = x_n \oplus \cdots \oplus x_1 \oplus \epsilon$, where $\epsilon \in \mathbb{F}_2$. It is readily seen that l_n is a root function of weight 2^{n-1}.
- Select $p_0 \notin \sup(l_n)$ and flip up the value of l_n at p_0, i.e., define $l_n^{(1)}$ such that for every $x \neq p_0$ it holds $l_n^{(1)}(x) = l_n(x)$ and $l_n^{(1)}(p_0) = 1$.
- Define a function $r_n^{\epsilon}(x)$ characterized by the property that: for every $x \in \mathbb{F}_2^n$ such that $d(x, p_0) = 1$, we have $r_n^{\epsilon}(x) = 0$; and $r_n^{\epsilon}(x) = l_n^{(1)}(x)$ otherwise.

Theorem 4.3 *[15] The function $r_n^\epsilon(x) \in \mathcal{B}_n$ described above is a root function of weight $2^{n-1} - n + 1$. For $n > 3$, there are exactly 2^n root functions having this weight, and when $n = 3$, there are 2^{n-1} such functions.*

Theorem 4.4 *Let $n \geq 4$ and consider the root function r_n^ϵ with weight $2^{n-1} - n + 1$ described in Construction A, where $\epsilon \in \mathbb{F}_2$. The code $\mathcal{C}_{r_n^\epsilon}$ is a wide minimal code.*

Proof. Denote with Δ the support of r_n^ϵ. The construction of r_n^ϵ gives that

$$\Delta = (\sup(l_n) \setminus \{x \in \mathbb{F}_2^n : d(x, p_0) = 1\}) \cup \{p_0\}.$$

We consider two cases according to the values of ϵ.

(i) Suppose $\epsilon = 1$. In this case, by setting $u_0 = 1_n$ we have $\sup(l_n) = \overline{H}_{u_0}$ and $p_0 \in H_{u_0}$. Define $\Gamma = \{x \in \mathbb{F}_2^n : d(x, p_0) = 1\}$ and observe that $\Gamma \subseteq \overline{H}_{u_0}$ and $||\Gamma|| = n \leq 2^{n-2}$. With this notation, we can write $\Delta = (\overline{H}_{u_0} \setminus \Gamma) \cup \{p_0\}$. Therefore, in order to apply Theorem 4.1, it is enough to show that for every $v \in \mathbb{F}_2^{n*}$ (with $v \neq u_0$) such that $p_0 \in H_v$, we have $\Gamma \cap H_v \neq \emptyset$. In fact, we will prove the stronger statement that $\Gamma \cap H_v \neq \emptyset$, for every $v \in \mathbb{F}_2^{n*}$ such that $v \neq u_0$.
Choose an ordering of the elements in Γ, say $\Gamma = \{x^{(1)}, \ldots, x^{(n)}\}$, in such a way that $x^{(1)}, \ldots, x^{(wt(p_0))}$ have weight equal to $wt(p_0) - 1$ and $x^{(wt(p_0)+1)}, \ldots, x^{(n)}$ have weight $wt(p_0) + 1$. Moreover, if $0_n \in \Gamma$ we set $x^{(1)} = 0_n$. Since $wt(p_0)$ is odd (recall that $p_0 \notin \sup(l_n)$), the set $\{x^{(2)}, \ldots, x^{(n)}\}$ is linearly independent over $\mathbb{F}_2$. Thus, we have $n-1$ linearly independent vectors in $\overline{H}_{u_0}$, which is a space of dimension $n-1$, implying that

$$\langle x^{(2)}, \ldots, x^{(n)} \rangle = \overline{H}_{u_0}.$$

Let now $v \in \mathbb{F}_2^{n*}$ with $v \neq u_0$. If $\Gamma \cap H_v = \emptyset$, then $\langle x_2, \ldots, x_n \rangle \cap H_v = \emptyset$ which contradicts the fact that $||\overline{H}_{u_0} \cap H_v|| = 2^{n-2}$. Using Theorem 4.1, we conclude that $\mathcal{C}_{r_n^1}$ is a wide minimal code.

(ii) Suppose $\epsilon = 0$. This case is similar to (i) with the only difference that we apply Theorem 4.2. By setting $u_0 = 1_n$ we have $\sup(l_n) = H_{u_0}$ and $p_0 \in \overline{H}_{u_0}$. Define $\Gamma = \{x \in \mathbb{F}_2^n : d(x, p_0) = 1\}$ and observe that $\Gamma \subseteq H_{u_0}$ and $||\Gamma|| = n < 2^{n-2}$. With this notation we can write $\Delta = (H_{u_0} \setminus \Gamma) \cup \{p_0\}$. In order to apply Theorem 4.2, we must prove two conditions, namely,

- For every $v \in \mathbb{F}_2^{n*}$ with $v \neq u_0$, if $p_0 \in H_v$ then we have $\Gamma \cap H_v \neq \emptyset$,
- For every $v \in \mathbb{F}_2^{n*}$ with $v \neq u_0$, if $p_0 \in \overline{H}_v$ then we have $\Gamma \cap \overline{H}_v \neq \emptyset$.

In fact, we will prove the stronger statement that Γ intersects every affine hyperplane H_v and every $(n-1)$-dimensional subspace $\overline{H}_v$, for $v \in \mathbb{F}_2^{n*}$ different from u_0. To show this, notice that the elements of Γ are linearly independent since $wt(p_0)$ is even now, hence we have a basis of $\mathbb{F}_2^n$ consisting of elements of H_{u_0}.

Now, for every nonzero $v \in \mathbb{F}_2^n$ we must have $\Gamma \cap H_v \neq \emptyset$, as otherwise we would have $\Gamma \subseteq \overline{H}_v$ and then $\langle \Gamma \rangle \subseteq \overline{H}_v$. This contradicts the fact that $\langle \Gamma \rangle = \mathbb{F}_2^n$.

Furthermore, for every nonzero $v \in \mathbb{F}_2^n$, with $v \neq u_0$, we must have $\Gamma \cap \overline{H}_v \neq \emptyset$. Suppose on the contrary, there is a $v \in \mathbb{F}_2^{n*}$ such that $\Gamma \subseteq H_v$. Let $\Gamma = \{\gamma_1, \ldots, \gamma_n\}$ and select a point $x_0 \in H_{u_0} \setminus H_v$. Since Γ is a basis for $\mathbb{F}_2^n$, there exist a positive integer k and $\gamma_{i_1}, \ldots, \gamma_{i_k} \in \Gamma$ such that $x_0 = \gamma_{i_1} \oplus \cdots \oplus \gamma_{i_k}$. By selection of x_0, we know that $u_0 \cdot x_0 = 1$ and $v \cdot x_0 = 0$. On the one hand, we have that

$$1 = u_0 \cdot x_0 = u_0 \cdot (\gamma_{i_1} \oplus \cdots \oplus \gamma_{i_k}) = (u_0 \cdot \gamma_{i_1}) \oplus \cdots \oplus (u_0 \cdot \gamma_{i_k}). \tag{16}$$

From equation (16), we deduce that k must be odd since $\Gamma \subseteq H_{u_0}$. On the other hand, we have that

$$0 = v \cdot x_0 = v \cdot (\gamma_{i_1} \oplus \cdots \oplus \gamma_{i_k}) = (v \cdot \gamma_{i_1}) \oplus \cdots \oplus (v \cdot \gamma_{i_k}). \tag{17}$$

Therefore, k must be even since $\Gamma \subseteq H_v$. This is a contradiction which establishes the result. □

4.2 Weight distribution and asymptotic behaviour

For every $n \geq 4$, we have seen the code $\mathcal{C}_{r_n^\epsilon}$ is wide and minimal. The asymptotic behaviour of the ratio $\frac{w_{min}}{w_{max}}$ can be easily established.

Corollary 4 *Let $\mathcal{C}_{r_n^\epsilon}$ be the linear code described in Theorem 4.4. Denoting by $a_n^\epsilon = \frac{w_{min}}{w_{max}}$, where $\epsilon \in \{0, 1\}$, we have*

$$\lim_{n\to\infty} a_n^1 = \frac{1}{2} \qquad \text{and} \qquad \lim_{n\to\infty} a_n^0 = 0.$$

Proof. When $\epsilon = 1$, we have $w_{min} = 2^{n-1} - n + 1$ and $w_{max} = 2^n - n - 1$. Thus,

$$\lim_{n\to\infty} a_n^1 = \frac{2^{n-1} - n + 1}{2^n - n - 1} = \frac{1}{2}.$$

Similarly, for $\epsilon = 0$, we have $w_{min} = n + 1$ and $w_{max} = 2^{n-1} + n - 1$ and therefore

$$\lim_{n\to\infty} a_n^0 = \lim_{n\to\infty} \frac{n+1}{2^{n-1} + n - 1} = 0.$$

□

The weight distribution, directly related to the Walsh spectrum of root functions of maximal weight, is given in Tables 4–7 below.

Case	Walsh spectrum
n even	$\pm 2, \pm 6, \pm 10, \ldots, \pm 2n-2, -2^n + 2n + 2$
n odd	$0, \pm 4, \pm 8, \ldots, \pm 2n-2, -2^n + 2n + 2$

Table 4: Walsh spectral values of r_n^1 w.r.t. the parity of n.

Case	Weights
n even	$2^{n-1} \pm (n-1), 2^{n-1} \pm (n-2), \ldots, 2^{n-1} \pm 1, 2^{n-1}, 2^n - (n+1)$
n odd	$2^{n-1} \pm (n-1), 2^{n-1} \pm (n-2), \ldots, 2^{n-1} \pm 2, 2^{n-1}, 2^n - (n+1)$

Table 5: Nonzero weights of codewords of $\mathcal{C}_{r_n^1}$.

Case	Walsh spectrum
n even	$\pm 2, \pm 6, \pm 10, \ldots, \pm(2n-2)$, $2^n - 2n - 2$
n odd	$0, \pm 4, \pm 8, \ldots, \pm(2n-2)$, $2^n - 2n - 2$

Table 6: Walsh spectral values of r_n^0 w.r.t. the parity of n.

Case	Weights
n even	$2^{n-1} \pm (n-1), 2^{n-1} \pm (n-2), \ldots, 2^{n-1} \pm 1, 2^{n-1}, n+1$
n odd	$2^{n-1} \pm (n-1), 2^{n-1} \pm (n-2), \ldots, 2^{n-1} \pm 2, 2^{n-1}, n+1$

Table 7: Nonzero weights of codewords of $\mathcal{C}_{r_n^0}$.

5 Conclusions

In this article, three different classes of binary minimal codes satisfying the inequality $\frac{w_{min}}{w_{max}} \leq \frac{1}{2}$ have been presented. Our methods cover a wide range of the weight of characteristic functions used and in many cases the exact specification of linear codes and their relevant parameters could be provided. Nevertheless, the employment of more sophisticated choices of the set Γ, with respect to its intersection with affine hyperplanes H_u, might provide further explicit classes of wide minimal linear codes. Another interesting research challenge is to possibly extend the approaches in this article to nonbinary alphabets.

Acknowledgment: Enes Pasalic is partly supported by the Slovenian Research Agency (research program P1-0404 and research projects J1-9108, J1-1694). Fengrong Zhang is supported in part by the Natural Science Foundation of China (No. 61972400) and in the part by the Jiangsu Natural Science Foundation (No. BK20181352). 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] G. N. Alfarano, M. Borello and A. Neri. A geometric characterization of minimal codes and their asymptotic performance. Available at

https://arxiv.org/abs/1911.11738v2

[2] A. Ashikhmin and A. Barg. Minimal vectors in linear codes. *IEEE Transactions on Information Theory*, vol. 44, no. 5, pp. 2010-2017, Sept. 1998.

[3] D. Bartoli and M. Bonini. Minimal linear codes in odd characteristic. *IEEE Transactions on Information Theory*, vol. 65, no. 7, pp. 4152-4155, July 2019.

[4] M. Bonini and M. Borello. Minimal linear codes arising from blocking sets. Available at https://arxiv.org/abs/1907.04626v2

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

[6] S. Chang and J. Hyun. Linear codes from simplicial complexes. *Designs, Codes and Cryptography 86*, 2167-2181, Oct. 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 some 2-designs. *IEEE Transactions on Information Theory*, vol. 61, no. 6, pp. 3265–3275, June 2015.

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

[10] C. Ding, Z. Heng and Z. Zhou. Minimal binary linear codes. *IEEE Transactions on Information Theory*, vol. 64, issue 10, pp. 6536–6545, Oct. 2018.

[11] K. Ding and C. Ding. A class of two-weight and three-weight codes and their applications in secret sharing. *IEEE Transactions on Information Theory*, vol. 64, issue 11, pp. 5835–5842, Nov. 2015.

[12] Z. Heng, C. Ding, and Z. Zhou. Minimal linear codes over finite fields. *Finite Fields and their Applications*, vol. 54, pp. 176–196, March 2018.

[13] S. Mesnager. Linear codes with few weights from weakly regular bent functions based on a generic construction. *Cryptography and Communications*, vol. 9, pp. 71–84, Jan. 2017.

[14] S. Mesnager, Y. Qi, H. Ru, and C. Tang. Minimal linear codes from characteristic functions. To appear in *IEEE Transactions on Information Theory*, 2020.

[15] E. Pasalic, A. Chattopadhyay and D. Chowdhury. An analysis of root functions—a subclass of the impossible class of faulty functions (ICFF). *Discrete Applied Mathematics*, vol. 222, pp 1-13, Feb. 2017.

[16] J. Sorci. Minimal codes from characteristic functions not satisfying the Ashikhmin-Barg condition. Available at https://arxiv.org/abs/1912.12769

[17] C. Tang., N. Li., Y. Qi., Z. Zhou. and T. Helleseth. Linear codes with two or three weights from weakly regular bent functions. *IEEE Transactions on Information Theory*, Vol. 62, Issue 3, pp. 1166–1176, March 2016.

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

[19] X. Wu, W. Lu and X. Cao. Minimal linear codes constructed from functions. Available at https://arxiv.org/abs/1911.11632v1

[20] G. Xu, X. Cao and S. Xu. Several classes of Boolean functions with few Walsh transform values. *Applicable Algebra in Engineering, Communication and Computing*, vol. 28, no. 2, pp. 155–176, March 2017.

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

[22] J. Yuan and C. Ding. Secret sharing schemes from three classes of linear codes. *IEEE Transactions on Information Theory*, vol. 52, issue 1, pp. 206–212, Jan. 2006.

[23] W. Zhang, H. Yan and H. Wei. Four families of minimal binary linear codes with $w_{min}/w_{max} \leq 1/2$. *Applicable Algebra in Engineering, Communication and Computing*, vol. 30, pp. 175–184, March 2019.

[24] Z. Zhou., N. Li., C. Fan. and T. Helleseth. Linear codes with two or three weights from quadratic bent functions. *Designs, Codes and Cryptography*, vol. 81, issue 2, pp. 283–295, Nov. 2016.