New characterizations and construction methods of bent and hyper-bent Boolean functions

Sihem Mesnager, B. Mandal, C. Tang

Version of Record: https://www.sciencedirect.com/science/article/pii/S0012365X20302673
Manuscript_572ab0cbe53d4b81e8a6d53862f383ad

New characterizations and construction methods of bent and hyper-bent Boolean functions

Sihem Mesnager[1], Bimal Mandal[2] and Chunming Tang[3]

[1]Department of Mathematics, University of Paris VIII, F-93526 Saint-Denis,
Laboratoire de Géométrie, Analyse et Applications, LAGA,
University Sorbonne Paris Nord, CNRS, UMR 7539, F-93430, Villetaneuse, France,
and Telecom ParisTech, 91120 Palaiseau, France.
Email: **smesnager@univ-paris8.fr**
[2]CARAMBA, INRIA Nancy - Grand Est., France
Email: **bimal.mandal@inria.fr**
[3]China West Normal University, Nanchong, Sichuan, 637002, China,
and Department of Computer Science and Engineering,
The Hong Kong University of Science and Technology,
Clear Water Bay, Kowloon, Hong Kong, China.
Email: **tangchunmingmath@163.com**

July 23, 2020

Abstract

In this paper, we first derive a necessary and sufficient condition for a bent Boolean function by analyzing their support set. Next, using this condition and the Pless power moment identities, we propose a construction method of bent functions of $2k$ variables by a suitable choice of $2k$-dimension subspace of $\mathbb{F}_2^{2^{2k-1}-2^{k-1}}$. Further, we extend our results to the so-called hyper-bent functions.

Keywords: Boolean function, Walsh-Hadamard transform, bent function, hyper-bent function, Pless power moment identity.
MSC 2010: 05A05, 06E30, 11T55, 94C10

1 Introduction

Boolean functions are used in many domains such as sequence theory, cryptography, and design theory. Boolean functions that are used as cryptographic primitives must resist affine approximation, which is achieved by having high nonlinearity. A Boolean function defined on an even number of variables having maximum nonlinearity is called a bent function. Such a function offers maximum resistance to affine approximation. Although, bent functions are not directly used as cryptographic primitives to design a secure cryptosystem due to their unbalancedness and since they are not of optimal algebraic degree. Several classes of bent functions were constructed by Rothaus [17],

Dillon [10, 11], Dobbertin [12], McFarland [15] and Carlet [1]. Till the constructions and characterizations of bent functions hold interest among researchers since they have maximum Hamming distance from the set of all affine Boolean functions and have very nice combinatorial properties, which are important for designing good Boolean functions. There are many cryptographic significant Boolean functions that are constructed by modifying bent functions [12, 18, 19]. Bent functions are used as a primitive in some ciphers like CAST [23], Grain [14] and hash function HAVAL [22].

For more details about bent Boolean functions, we refer to [2, 3, 5, 6, 4, 16, 20]. In this paper, we characterize the support set of a bent function and provide a necessary and sufficient condition for bentness.

Youssef and Gong [21] introduced a new class of Boolean functions which are subclasses of bent functions, so-called *hyper-bent functions*. A Boolean function f in n variables is called hyper-bent if $f(x^i)$ is bent for any i coprime to $2^n - 1$. In [13], Golomb and Gong proposed a new criterion to design a good Sbox that Sboxes should not be approximated by a monomial permutation. For that, they have defined the extended Walsh-Hadamard transform (see (1)). Hyper-bent functions can be completely characterized in terms of the extended Walsh-Hadamard transform. In fact, a Boolean function defined over $\mathbb{F}_{2^n}$ (n even) is hyper-bent if and only if its extended Walsh-Hadamard transform takes only the values $\pm 2^{\frac{n}{2}}$. Till now, all the know hyper-bent functions [7] belong to $\mathcal{PS}_{ap}$, which is a subclass of partial spread introduced by Dillon [10], and hyper-bentness mainly depends on the Kloosterman sums. In this paper, we also derive a necessary and sufficient condition for bent and hyper-bent functions which is based on their support sets. Next, using the Pless power moment identities from coding theory, we succeed in proposing new construction methods for bent and hyper-bent functions.

The paper is organized as follows. In Section 2, some basic definitions and known results are described. In Section 3, we characterize the bent functions by means of their support set and derive a construction method for bent functions by using the Pless power moment identities. In Section 4, we extend our results to hyper-bent functions.

2 Preliminaries and notation

Let $\mathbb{F}_2$ and $\mathbb{F}_2^n$ be the prime field of characteristic 2 and the n-dimensional vector space over $\mathbb{F}_2$, respectively. Any element $\mathbf{x}$ in $\mathbb{F}_2^n$ can be written $\mathbf{x} = (x_1, x_2, \ldots, x_n)$, where $x_i \in \mathbb{F}_2,\ 1 \leq i \leq n$. The addition over $\mathbb{F}_2$ is denoted by $\oplus$. Let $\mathbb{F}_{2^n}$ be the extension field of $\mathbb{F}_2$ of degree n and α be a primitive element of $\mathbb{F}_{2^n}$. Any element $x \in \mathbb{F}_{2^n}$ can be written as $x = \bigoplus_{i=0}^{n-1} x_{i+1}\alpha^i$, where $x_{i+1} \in \mathbb{F}_2,\ 0 \leq i \leq n-1$. So, for the fixed basis $\{\alpha^0, \alpha^1, \ldots, \alpha^{n-1}\}$ of $\mathbb{F}_{2^n}$, there is a vector isomorphism between $\mathbb{F}_{2^n}$ and $\mathbb{F}_2^n$, and any element $x \in \mathbb{F}_{2^n}$ can be identified with an n-bit binary string $\mathbf{x} \in \mathbb{F}_2^n$ of the form $\mathbf{x} = (x_1, x_2, \ldots, x_n)$. The trace function $\mathrm{Tr}_1^n : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is defined by $\mathrm{Tr}_1^n(x) = \bigoplus_{i=0}^{n-1} x^{2^i}$ and the inner product between two elements $x, y \in \mathbb{F}_{2^n}$ is defined by $\mathrm{Tr}_1^n(xy)$. Let $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$. The addition and inner product of $\mathbf{x}$ and $\mathbf{y}$ are defined as $\mathbf{x} \oplus \mathbf{y} = (x_1 \oplus y_1, x_2 \oplus y_2, \ldots, x_n \oplus y_n)$ and $\mathbf{x} \cdot \mathbf{y} = x_1y_1 \oplus x_2y_2 \oplus \cdots \oplus x_ny_n$, respectively. The weight of an element $\mathbf{x} \in \mathbb{F}_2^n$ is defined as $wt(\mathbf{x}) = \sum_{i=1}^{n} x_i$, the sum is over the set of integers. The cardinality of a set S is denoted by $\#S$, defined as the number of

elements in S.

Any function from $\mathbb{F}_2^n$ (or $\mathbb{F}_{2^n}$) to $\mathbb{F}_2$ is called a Boolean function in n variables. The set of n-variable Boolean functions is denoted by $\mathcal{B}_n$. Any function $f \in \mathcal{B}_n$ can be uniquely written as a multivariate polynomial of the form

$$f(\mathbf{x}) = \bigoplus_{\mathbf{a} \in \mathbb{F}_2^n} \mu_{\mathbf{a}} x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n},$$

where $\mu_{\mathbf{a}} \in \mathbb{F}_2$. Its polynomial form of f is called *algebraic normal form*. The algebraic degree of $f \in \mathcal{B}_n$ is defined as $deg(f) = \max_{\mathbf{a} \in \mathbb{F}_2^n}\{wt(\mathbf{a}) : \ \mu_{\mathbf{a}} \neq 0\}$. The support of $f \in \mathcal{B}_n$, denoted by $supp(f)$, is the set of all nonzero inputs, i.e., $supp(f) = \{\mathbf{x} \in \mathbb{F}_2^n : \ f(\mathbf{x}) = 1\}$. The cardinality of the support of a Boolean function f is called the Hamming weight of f, i.e., $wt(f) = \#supp(f)$. If the weight of an n-variable Boolean function f is $wt(f) = 2^{n-1}$, then f is called *balanced*. If the algebraic degree of a Boolean function is at most 1, then it is called an *affine function*. The set of all n-variable affine functions is denoted by $\mathcal{AF}_n$. Any affine function can be written as $l_{\mathbf{a},\varepsilon}(\mathbf{x}) = \mathbf{a} \cdot \mathbf{x} \oplus \varepsilon$, for all $\mathbf{x} \in \mathbb{F}_2^n$, where $\mathbf{a} \in \mathbb{F}_2^n$ and $\varepsilon \in \mathbb{F}_2$. If $\varepsilon = 0$, then $l_{\mathbf{a},0}$ is a linear function.

The Hamming distance between two n-variable Boolean functions f and g, denoted by $d_H(f,g)$, is defined as $d_H(f,g) = \#\{\mathbf{x} \in \mathbb{F}_2^n : \ f(\mathbf{x}) \neq g(\mathbf{x})\} = wt(f \oplus g)$. The Walsh-Hadamard transform of $f \in \mathcal{B}_n$ at $\mathbf{a} \in \mathbb{F}_2^n$, denoted by $\mathcal{W}_f(\mathbf{a})$, is defined as

$$\mathcal{W}_f(\mathbf{a}) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{f(\mathbf{x}) \oplus \mathbf{a} \cdot \mathbf{x}}.$$

It is directly related to the so-called the Fourier transform of f, defined as:

$$\widehat{f}(\mathbf{a}) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} f(\mathbf{x})(-1)^{\mathbf{a} \cdot \mathbf{x}} = \sum_{\mathbf{x} \in supp(f)} (-1)^{\mathbf{a} \cdot \mathbf{x}}.$$

We have $\mathcal{W}_f(\mathbf{0}) = 2^n - 2\widehat{f}(\mathbf{0})$ and for every $\mathbf{a} \neq \mathbf{0}$, $\mathcal{W}_f(\mathbf{a}) = -2\widehat{f}(\mathbf{a})$. The multiset $[\mathcal{W}_f(\mathbf{a}) : \ \mathbf{a} \in \mathbb{F}_2^n]$ for a Boolean function $f \in \mathcal{B}_n$ is called the *Walsh-Hadamard spectrum* of f. The nonlinearity of $f \in \mathcal{B}_n$ is the minimum Hamming distance between f and all affine functions and it is denoted by $nl(f)$, i.e., $nl(f) = \min_{g \in \mathcal{AF}_n}\{d_H(f,g)\} = \min_{g \in \mathcal{AF}_n}\{wt(f \oplus g)\}$. The relation between the nonlinearity and the Walsh-Hadamard transform of $f \in \mathcal{B}_n$ is given by:

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{\mathbf{a} \in \mathbb{F}_2^n} |\mathcal{W}_f(\mathbf{a})|.$$

From Parseval's identity: $\sum_{\mathbf{a} \in \mathbb{F}_2^n} \mathcal{W}_f^2(\mathbf{a}) = 2^{2n}$, we deduce: $\max_{\mathbf{a} \in \mathbb{F}_2^n} |\mathcal{W}_f(\mathbf{a})| \geq 2^{\frac{n}{2}}$, for any $f \in \mathcal{B}_n$. Thus, the nonlinearity of any Boolean function f in n variables is upper bounded by $2^{n-1} - 2^{\frac{n}{2}-1}$. If a function f achieves this nonlinearity bound with equality, then f is called a *bent* function. It is also known that bent functions exist only for an even number of variables. A function $f \in \mathcal{B}_n$ is bent if and only if, for all $\mathbf{a} \in \mathbb{F}_2^n$, we have $\mathcal{W}_f(\mathbf{a}) = 2^{\frac{n}{2}}(-1)^{\tilde{f}(\mathbf{a})}$, for some function $\tilde{f}$, called the dual of f, which is also a bent function in n variables. It is clear that any bent function is unbalanced, as $\mathcal{W}_f(0) \neq 0$. The cardinality of the support of a bent function $f \in \mathcal{B}_n$ is $\#supp(f) = 2^{n-1} - 2^{\frac{n}{2}-1}(-1)^{\tilde{f}(0)}$.

A subclass of bent functions is made of hyper-bent functions, which have even stronger properties than bent functions, and are defined as follows. Here we consider the elements in $\mathbb{F}_{2^n}$ (this field being an n-dimensional vector space over $\mathbb{F}_2$, it can be identified, as a vector space, with $\mathbb{F}_2^n$).

Definition 1. *A Boolean function f in n (even) variables is said to be* hyper-bent *if the function $x \mapsto f(x^i)$ is bent for every integer i co-prime with $2^n - 1$.*

The extended Walsh-Hadamard transform of $f \in \mathcal{B}_n$ at $a \in \mathbb{F}_{2^n}$, denoted by $\mathcal{W}_f^i(a)$, is defined as

$$\mathcal{W}_f^i(a) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x) \oplus \mathrm{Tr}_1^n(ax^i)}, \tag{1}$$

where i is any integer co-prime to $2^n - 1$. A function $f \in \mathcal{B}_n$ is said to be hyper-bent if $|\mathcal{W}_f^i(a)| = 2^{\frac{n}{2}}$, for all $a \in \mathbb{F}_{2^n}$ and any integer i, co-prime to $2^n - 1$. It is clear that any hyper-bent function is a bent function, but the converse is not true in general.

In this paper, the bent functions are constructed from selecting a particular number of binary vectors from a higher dimensional vector space. Necessary and sufficient conditions are derived from the Walsh-Hadamard transform of a function, which makes it easier to check their bentness. For constructing an n-variable bent function, n being even, we need to find an n-dimensional vector subspace of $\mathbb{F}_2^{2^{n-1}-2^{\frac{n}{2}-1}}$, such that the Hamming weight of each nonzero element is either 2^{n-2} or $2^{n-2} - 2^{\frac{n}{2}-1}$. This construction avoids having to calculate the Walsh-Hadamard transform for proving bentness. We extend it into a construction of hyper-bent functions; this is a little more complex but the idea is roughly the same.

3 New characterizations and constructions of bent functions

Let $\mathbf{0}$ and $\mathbf{1}$ denote the all $0'$s and all $1'$s vectors of $\mathbb{F}_2^n$, respectively. For any $\mathbf{x} \in \mathbb{F}_2^n$, let $\bar{\mathbf{x}} = \mathbf{x} \oplus \mathbf{1}$. In the sequel, n is an even positive integer. We know that $(-1)^\varepsilon = 1 - 2\varepsilon$, where $\varepsilon \in \mathbb{F}_2$. Let us denote, for any $\mathbf{a} \in \mathbb{F}_2^n$ and $f \in \mathcal{B}_n$:

$$E_f(\mathbf{a}, 0) = \{\mathbf{x} \in supp(f) : \mathbf{a} \cdot \mathbf{x} = 0\} \text{ and } E_f(\mathbf{a}, 1) = \{\mathbf{x} \in supp(f) : \mathbf{a} \cdot \mathbf{x} = 1\}. \tag{2}$$

We have:

$$\widehat{f}(\mathbf{a}) = \#E_f(\mathbf{a}, 0) - \#E_f(\mathbf{a}, 1).$$

It is clear that $E_f(\mathbf{0}, 0) = supp(f)$, $E_f(\mathbf{0}, 1) = \emptyset$, $E_f(\mathbf{1}, 0)$ is the set of even weight elements in $supp(f)$ and $E_f(\mathbf{a}, 0) \cup E_f(\mathbf{a}, 1) = supp(f)$, for any $f \in \mathcal{B}_n$ and $\mathbf{a} \in \mathbb{F}_2^n$. If f is a bent function in n variables, then for any $\mathbf{a} \in \mathbb{F}_2^n$

$$\#E_f(\mathbf{a}, 0) + \#E_f(\mathbf{a}, 1) = \widehat{f}(\mathbf{0}) = 2^{n-1} - 2^{\frac{n}{2}-1}(-1)^{\tilde{f}(\mathbf{0})}. \tag{3}$$

Let us define $\delta_{\mathbf{0}}(\mathbf{a}) = 1$, if $\mathbf{a} = \mathbf{0}$, otherwise $\delta_{\mathbf{0}}(\mathbf{a}) = 0$, which is called the Dirac (or Kronecker) function at $\{\mathbf{0}\}$ over $\mathbb{F}_2^n$. We revisit in Proposition 2, Proposition 3 and Corollary 4, some known results on the supports of bent functions. These results are used to construct bent and hyper-bent functions.

Proposition 2. *Let $f \in \mathcal{B}_n$ be a bent function. Then for any nonzero $\mathbf{a} \in \mathbb{F}_2^n$*

$$\#E_f(\mathbf{a},0) = 2^{n-2} - 2^{\frac{n}{2}-2}\left((-1)^{\tilde{f}(\mathbf{0})} + (-1)^{\tilde{f}(\mathbf{a})}\right)$$
$$\text{and} \quad \#E_f(\mathbf{a},1) = 2^{n-2} - 2^{\frac{n}{2}-2}\left((-1)^{\tilde{f}(\mathbf{0})} - (-1)^{\tilde{f}(\mathbf{a})}\right),$$

where $E_f(\mathbf{a},0)$ and $E_f(\mathbf{a},1)$ are defined as in (2).

Proof. This is a direct consequence of (3) and of the following relation, valid for any $\mathbf{a} \in \mathbb{F}_2^n$:

$$\widehat{f}(\mathbf{a}) = \#E_f(\mathbf{a},0) - \#E_f(\mathbf{a},1) = 2^{n-1}\delta_{\mathbf{0}}(\mathbf{a}) - 2^{\frac{n}{2}-1}(-1)^{\tilde{f}(\mathbf{a})}.$$

□

From Proposition 2, it is clear that if $f \in \mathcal{B}_n$ is a bent function, then for all nonzero $\mathbf{a} \in \mathbb{F}_2^n$

$$(\#E_f(\mathbf{a},0), \#E_f(\mathbf{a},1)) \in \{(2^{n-2}, 2^{n-2} \pm 2^{\frac{n}{2}-1}), (2^{n-2} \pm 2^{\frac{n}{2}-1}, 2^{n-2})\}.$$

Without loss of generality, let $\tilde{f}(0) = 0$. Then the cardinality of the support of an n-variable bent function f is $2^{n-1} - 2^{\frac{n}{2}-1}$ and a necessary and sufficient condition for bentness is derived in the next result.

Proposition 3. *Let $f \in \mathcal{B}_n$ have Hamming weight $2^{n-1} - 2^{\frac{n}{2}-1}$. Then f is a bent function if and only if, for any nonzero $\mathbf{a} \in \mathbb{F}_2^n$, we have:*

$$(\#E_f(\mathbf{a},0), \#E_f(\mathbf{a},1)) \in \{(2^{n-2}, 2^{n-2} - 2^{\frac{n}{2}-1}), (2^{n-2} - 2^{\frac{n}{2}-1}, 2^{n-2})\},$$

where $E_f(\mathbf{a},0)$ and $E_f(\mathbf{a},1)$ are defined as in (2).

Proof. If $f \in \mathcal{B}_n$ is bent, then the condition on the weight shows that $\tilde{f}(\mathbf{0}) = 0$, and Proposition 2 shows our claim. Conversely, this same condition on the weight shows that $\mathcal{W}_f(\mathbf{0}) = 2^{\frac{n}{2}}$, and for any nonzero $\mathbf{a} \in \mathbb{F}_2^n$, we have either $(\#E_f(\mathbf{a},0), \#E_f(\mathbf{a},1)) = (2^{n-2}, 2^{n-2} - 2^{\frac{n}{2}-1})$, and then $\mathcal{W}_f(\mathbf{a}) = 2(\#E_f(\mathbf{a},1) - \#E_f(\mathbf{a},0)) = -2^{\frac{n}{2}}$, or we have $(\#E_f(\mathbf{a},0), \#E_f(\mathbf{a},1)) = (2^{n-2} - 2^{\frac{n}{2}-1}, 2^{n-2})$, and then $\mathcal{W}_f(\mathbf{a}) = 2(\#E_f(\mathbf{a},1) - \#E_f(\mathbf{a},0)) = 2^{\frac{n}{2}}$. Thus, $\mathcal{W}_f(\mathbf{a}) = \pm 2^{\frac{n}{2}}$ for all $\mathbf{a} \in \mathbb{F}_2^n$, and f is bent. □

From Proposition 3, we have the following information about the support set of a bent function.

Corollary 4. *Let $f \in \mathcal{B}_n$ be a bent function and $\tilde{f}$ be its dual with $\tilde{f}(\mathbf{0}) = 0$. Then we get the following properties.*

- *The cardinality of the set of all even weight elements in $supp(f)$ is either 2^{n-2} or $2^{n-2} - 2^{\frac{n}{2}-1}$.*
- *The total number of elements in $supp(f)$ such that, for $1 \le i \le n$, the ith coordinate is equal to 1, is either 2^{n-2} or $2^{n-2} - 2^{\frac{n}{2}-1}$.*
- *The support of $\tilde{f}$ is*

$$supp(\tilde{f}) = \{\mathbf{a} \in \mathbb{F}_2^n : \ \#E_f(\mathbf{a},0) = 2^{n-2}\}.$$

Proof. The first two claims are clear from Proposition 3 (take $\mathbf{a} = \mathbf{1}$ and $\mathbf{a}$ of Hamming weight 1). The third claim is also clear since we know from Proposition 2 that $supp(\tilde{f}) = \{\mathbf{a} \in \mathbb{F}_2^n : \ \tilde{f}(\mathbf{a}) = 1\} = \{\mathbf{a} \in \mathbb{F}_2^n : \ \#E_f(\mathbf{a}, 0) = 2^{n-2}\}$. □

We know that $\mathbf{a} \cdot \mathbf{x} = a_1x_1 \oplus a_2x_2 \oplus \cdots \oplus a_nx_n$, where $\mathbf{a}, \mathbf{x} \in \mathbb{F}_2^n$. Let $\mathbf{a} \in \mathbb{F}_2^n$ with $wt(\mathbf{a}) = r \in \{1, \ldots, n\}$, and let $i_1, i_2, \ldots, i_r$ be the r indices such that $a_{i_1} = a_{i_2} = \cdots = a_{i_r} = 1$ (the other coordinates are equal to 0). Then $\mathbf{a} \cdot \mathbf{x} = x_{i_1} \oplus x_{i_2} \oplus \cdots \oplus x_{i_r}$. We define then:

$$A_f(i_1 < i_2 < \cdots < i_r, 0) = \{\mathbf{x} \in supp(f) : \ x_{i_1} \oplus x_{i_2} \oplus \cdots \oplus x_{i_r} = 0\},$$

where $r \in \{1, 2, \ldots, n\}$. The next result is straightforward from Proposition 3; we state it because it will be convenient to refer to it in the sequel.

Corollary 5. *Let $f \in \mathcal{B}_n$ and the cardinality of $supp(f)$ be $2^{n-1} - 2^{\frac{n}{2}-1}$. Then f is a bent function if and only if, for all $r \in \{1, 2, \ldots, n\}$ and for all $1 \leq i_1 < i_2 < \cdots < i_r \leq n$, we have:*

$$\#A_f(i_1 < i_2 < \cdots < i_r, 0) \in \{2^{n-2}, 2^{n-2} - 2^{\frac{n}{2}-1}\}.$$

We will need the Pless power moment identities, which could be found in [8].

Lemma 6. *Let $\mathcal{C}$ be a binary linear code of length n and dimension k. Denote by $(A_0, A_1, \cdots, A_n)$ and $(A_0^\perp, A_1^\perp, \cdots, A_n^\perp)$ the weight distributions of $\mathcal{C}$ and its dual code $\mathcal{C}^\perp$, respectively. Then the first three Pless power moment identities are the following:*

$$\begin{aligned}
\sum_{j=0}^{n} A_j &= 2^k, \\
\sum_{j=0}^{n} jA_j &= 2^{k-1}\left(n - A_1^\perp\right), \\
\sum_{j=0}^{n} j^2A_j &= 2^{k-2}\left(n(n+1) - 2nA_1^\perp + 2A_2^\perp\right).
\end{aligned}$$

The following shall play a crucial role in the construction of bent functions from subspaces of the vector space $\mathbb{F}_2^{2^{2k-1}-2^{k-1}}$. It proves that there is no duplicate in the elements of the support of the constructed bent functions.

Lemma 7. *Let $n = 2k$ be a positive integer. Let $\mathcal{C}$ be a binary linear code of length $2^{n-1}-2^{k-1}$ and dimension n, and let $G = [\mathbf{g}_1, \cdots, \mathbf{g}_{2^{n-1}-2^{k-1}}]$ (where $\mathbf{g}_1, \cdots, \mathbf{g}_{2^{n-1}-2^{k-1}}$ are column vectors) be a generator matrix of $\mathcal{C}$. Suppose that $wt(\mathbf{c})$ is equal to either 2^{n-2} or $2^{n-2} - 2^{k-1}$ for any nonzero codeword $\mathbf{c}$ in $\mathcal{C}$. Then $\mathbf{g}_i \neq \mathbf{g}_j$, for every $1 \leq i < j \leq 2^{n-1} - 2^{k-1}$.*

Proof. Let $\overline{\mathcal{C}}$ be the augmented code formed by including the all-ones vector with the codewords of $\mathcal{C}$. Note that, according to the hypothesis on the weights, the all-1 vector is linearly independent of the codewords of $\mathcal{C}$. Then $\overline{\mathcal{C}}$ is a linear code of dimension $n + 1$ and length $N = 2^{n-1} - 2^{k-1}$ with generator matrix

$$\overline{G} = \begin{bmatrix} 1, & 1, & \cdots, & 1 \\ \mathbf{g}_1, & \mathbf{g}_2, & \cdots, & \mathbf{g}_{2^{n-1}-2^{k-1}} \end{bmatrix}. \tag{4}$$

Denote $(\overline{A}_0, \overline{A}_1, \cdots, \overline{A}_N)$ and $(\overline{A}_0^\perp, \overline{A}_1^\perp, \cdots, \overline{A}_N^\perp)$ the weight distributions of $\overline{\mathcal{C}}$ and its dual code $\overline{\mathcal{C}}^\perp$, respectively. It is observed that

$$\begin{cases} \overline{A}_j = 0, \\ \overline{A}_{2^{n-1}-2^{k-1}} = 1, \quad j \notin \{0, 2^{n-2}-2^{k-1}, 2^{n-2}, 2^{n-1}-2^{k-1}\}, \\ \overline{A}_1^\perp = 0. \end{cases}$$

Using Lemma 6 yields

$$\begin{cases} \overline{A}_{i_1} + \quad \overline{A}_{i_2} = \quad 2^{n+1}-2, \\ i_1\overline{A}_{i_1} + \quad i_2\overline{A}_{i_2} = \quad 2^n\left(2^{n-1}-2^{k-1}-0\right) - 2^{n-1} - 2^{k-1}, \end{cases}$$

where $i_1 = 2^{n-2} - 2^{k-1}$ and $i_2 = 2^{n-2}$. Then, $A_{i_1} = A_{i_2} = 2^n - 1$. A standard computation shows that

$$\begin{aligned} & i_1^2 A_{i_1} + i_2^2 A_{i_2} + N^2 A_N \\ = \; & (2^n-1)\left((2^{n-2}-2^{k-1})^2 + 2^{2(n-2)}\right) + N^2 \\ = \; & (2^n-1)\left[(2^{n-2}+2^{n-2}-2^{k-1})^2 - 2^{n-1}\left(2^{n-2}-2^{k-1}\right)\right] + N^2 \\ = \; & (2^n-1)\left(N^2 - 2^{n-1}\left(2^{n-2}-2^{k-1}\right)\right) + N^2 \\ = \; & 2^n N^2 - 2^{n-1}\left(2^{n-2}-2^{k-1}\right)(2^n-1) \\ = \; & 2^n N^2 - 2^{n-1}(2^k+1)\left(2^{2k-2}-2^{k-1}\right)(2^k-1) \\ = \; & 2^n N^2 - 2^{n-1}(2^k+1)\left(2^{k-1}-1\right)\left(2^{2k-1}-2^{k-1}\right) \\ = \; & 2^n N^2 - 2^{n-1}(N-1)N \\ = \; & 2^{n-1}N(N+1). \end{aligned}$$

Thus $\sum_{i=0}^N i^2 A_i = i_1^2 A_{i_1} + i_2^2 A_{i_2} + N^2 A_N = 2^{(n+1)-2}N(N+1)$. By the third Pless power moment identity in Lemma 6, $\overline{A}_2^\perp = 0$. The desired result then follows from (4). $\square$

We introduce now our construction of bent functions:

Construction 1. Let $n = 2k$ be a positive integer. Choose n binary vectors $\mathbf{v}^1, \mathbf{v}^2, \ldots, \mathbf{v}^n$, of length $2^{n-1} - 2^{\frac{n}{2}-1}$ such that

$$wt\left(\bigoplus_{i=1}^n \varepsilon_i \mathbf{v}^i\right) \in \{2^{n-2}, 2^{n-2} - 2^{\frac{n}{2}-1}\},$$

for all $\varepsilon_i \in \mathbb{F}_2,\ 1 \le i \le n$, except all zero. We define the function $f \in \mathcal{B}_n$ such that $supp(f) = \{(v_j^1, \cdots, v_j^n) \in \mathbb{F}_2^n :\ 1 \le j \le 2^{n-1} - 2^{\frac{n}{2}-1}\}$, where v_j^i is the jth coordinate of the vector $\mathbf{v}^i$.

The functions obtained are bent, according to Corollary 5. Indeed, the condition on the weight of f in the hypothesis of the corollary is satisfied thanks to Lemma 7, and the rest of the conditions is ensured thanks to the hypothesis of the construction.

Here the dimension of the subspace of $\mathbb{F}_2^{2^{n-1}-2^{\frac{n}{2}-1}}$ generated by $\mathbf{v}^1, \mathbf{v}^2, \ldots, \mathbf{v}^n$ is n. Thus, identifying a subspace of dimension n in $\mathbb{F}_2^{2^{n-1}-2^{\frac{n}{2}-1}}$ having weight 2^{n-2} or $2^{n-2} - 2^{\frac{n}{2}-1}$ (for all nonzero elements), we can easily construct a bent function in n variables. Thus, the construction of a bent function is equivalent to the construction of a linear code of length $2^{n-1}-2^{\frac{n}{2}-1}$ and dimension n such that the weight of of any nonzero codeword is 2^{n-2} or $2^{n-2} - 2^{\frac{n}{2}-1}$. This construction also presents a characterization of

bent functions with $2k$-variables by using linear codes of length $2^{2k-1} - 2^{k-1}$. Another characterization of bent functions via linear codes of length 2^{2k} was given in [9].

Given an n-variable Boolean function, we can check its bentness using Walsh-Hadamard spectrum. But, it is difficult to construct a bent function by choice of 2^n integer values $2^{\frac{n}{2}}$ and $-2^{\frac{n}{2}}$ since we know that for any choice of 2^n integer values lies between -2^n to 2^n, the inverse Walsh-Hadamard transformation might not provide a Boolean function in n variables. We can construct an n-variable bent function using our construction method identifying n linearly independent binary vectors of length $2^{n-1} - 2^{\frac{n}{2}-1}$ one by one that are satisfied the conditions given in Construction 1. Further, our aim is to develop an algorithm for which one can check that a given Boolean function is bent or not. We know that f is bent if and only if $f \oplus 1$ is bent. To check the bentness of a given Boolean function $f \in \mathcal{B}_n$, we follow the following method.

1. If $\#supp(f) \neq 2^{n-1} \pm 2^{\frac{n}{2}-1}$, then f is not a bent function. If $\#supp(f) = 2^{n-1}+2^{\frac{n}{2}-1}$, then consider the complement function g of f, that is, $g(\mathbf{x}) = f(\mathbf{x})\oplus 1$ for all $\mathbf{x} \in \mathbb{F}_2^n$, so that, the cardinality of the support set of g is $2^{n-1} - 2^{\frac{n}{2}-1}$.

2. Construct a binary matrix M_f of order $n \times (2^{n-1} - 2^{\frac{n}{2}-1})$, whose column vectors are the elements of support set of f. Let us denote the row vectors of M_f as $\mathbf{v}^1, \mathbf{v}^2, \ldots, \mathbf{v}^n$.

3. If $wt(\varepsilon_1\mathbf{v}^1 \oplus \varepsilon_2\mathbf{v}^2 \oplus \cdots \oplus \varepsilon_n\mathbf{v}^n) \in \{2^{n-2}, 2^{n-2} - 2^{\frac{n}{2}-1}\}$, for all $\varepsilon_i \in \mathbb{F}_2,\ 1 \leq i \leq n$ (except all zero), then f is bent. Otherwise, f is not a bent function.

Suppose $f \in \mathcal{B}_{2k}$ is a bent function and $\#supp(f) = 2^{2k-1} + 2^{k-1}$. Then we can similarly prove that for any nonzero $\mathbf{a} \in \mathbb{F}_2^{2k}$

$$(\#E_f(\mathbf{a}, 0), \#E_f(\mathbf{a}, 1)) \in \{(2^{2k-2}, 2^{2k-2} + 2^{k-1}), (2^{2k-2} + 2^{k-1}, 2^{2k-2})\}.$$

We know that two functions $f, g \in \mathcal{B}_n$ are affine equivalent if and only if there exist an element A in $GL(n, \mathbb{F}_2)$, the set of all nonsingular binary matrices of order n, and $\mathbf{b} \in \mathbb{F}_2^n$ such that $g(\mathbf{x}) = f(\mathbf{x}A \oplus \mathbf{b})$, for all $\mathbf{x} \in \mathbb{F}_2^n$. It is also clear that if two functions are affine equivalent, then their support sets have equal cardinality. Suppose $\mathbf{y} = \mathbf{x}A \oplus \mathbf{b}$, for all $\mathbf{x} \in \mathbb{F}_2^n$, where $A = (a_{ij})_{n\times n} \in GL(n, \mathbb{F}_2)$ and $\mathbf{b} \in \mathbb{F}_2^n$. Then $y_k = \bigoplus_{l=1}^n x_l a_{lk} \oplus b_k$, for all $1 \leq k \leq n$. Define binary matrices M_f and M_g of order $n \times \#supp(f)$ corresponding to two n-variable Boolean functions f and g, whose column vectors are the elements of supports of f and g, respectively. Thus, the ith row vector, $1 \leq i \leq n$, of M_f is related to the ith coordinate of the elements of support set of f. Then we get the following remark.

Remark 8. *Let f and g be two affine equivalent Boolean functions in n variables, i.e., $g(\mathbf{x}) = f(\mathbf{x}A \oplus \mathbf{b})$, for all $\mathbf{x} \in \mathbb{F}_2^n$, where $A \in GL(n, \mathbb{F}_2)$ and $\mathbf{b} \in \mathbb{F}_2^n$. Let M_f and M_g be the two matrices defined as above for f and g, respectively.*

- *Let $\mathbf{b} = \mathbf{0}$. Then all the row vectors of M_f can be expressed (maybe after swapping some fixed, for all row vectors of M_f, positions) as nonzero linear combinations of the row vectors of M_g.*

- *Let $\mathbf{b} \neq \mathbf{0}$ and $\mathbf{b} = \mathbf{b}'A$, where $\mathbf{b}' \in \mathbb{F}_2^n \setminus \{\mathbf{0}\}$. Without loss of generality, we assume that $wt(\mathbf{b}') = r,\ 1 \leq r \leq n$. There are exactly r indices i_j such that*

$b'_{i_j} = 1,\ 1 \le j \le r$. *Let the row vectors of* M_g *be* $\mathbf{v}^1, \mathbf{v}^2, \ldots,$ *and* $\mathbf{v}^n$. *Define a matrix* M'_g *such that if* $b'_i = 1$, *then* $\bar{\mathbf{v}}^i$ *is the* i*th row vector of* M'_g, *otherwise* $\mathbf{v}^i$ *is the* i*th row vector* M'_g. *Then all the row vectors of* M_f *can be expressed (maybe after swapping some fixed, for all row vectors of* M_f, *positions) as nonzero linear combinations of the row vectors of* M'_g.

Proof. Let $\mathbf{y} = \mathbf{x}A \oplus \mathbf{b} = (\mathbf{x} \oplus \mathbf{b}')A$, for all $\mathbf{x} \in \mathbb{F}_2^n$, where $A = (a_{ij})_{n\times n} \in GL(n, \mathbb{F}_2)$ and $\mathbf{b} = \mathbf{b}'A,\ \mathbf{b}' \in \mathbb{F}_2^n$. Then $y_k = \bigoplus_{l=1}^{n}(x_l \oplus b'_l)a_{lk}$, for all $1 \le k \le n$. Here $(a_{1k}, \ldots, a_{nk})$ is a nonzero element of $\mathbb{F}_2^n$, for all $1 \le k \le n$, since $A \in GL(n, \mathbb{F}_2)$. Suppose $\mathbf{b} = \mathbf{0}$. Then $\mathbf{b}' = \mathbf{0}$, and we get the first claim. Let $\mathbf{b} \neq \mathbf{0}$. Then $\mathbf{b}' \neq \mathbf{0}$, and define a matrix M'_g from M_g such that if $b'_i = 1$, then $\bar{\mathbf{v}}^i$ is the ith row vector of M'_g, otherwise $\mathbf{v}^i$ is the ith row vector M'_g. Then we get our second claim. □

Now we extend the previous result and derive a necessary and sufficient condition for the affine equivalence of two Boolean functions $f, g \in \mathcal{B}_n$. Define a binary matrix M'_g from M_g such that the ith row, $1 \le i \le n$, of M'_g is equal to the ith row of M_g or its complement.

Theorem 9. *Two Boolean functions* f *and* g *in* n *variables are affine equivalent if and only if there exist two nonsingular matrices* P *and* Q *of orders* $n \times n$ *and* $\#supp(g) \times \#supp(g)$, *respectively, such that* $M_f = PM'_gQ$, *where* M'_g *is defined as above.*

Proof. Let us denote the row vectors of M_g are $\mathbf{v}^1,\ \mathbf{v}^2,\ \ldots,\ \mathbf{v}^n$. Suppose $f, g \in \mathcal{B}_n$ are affine equivalent, i.e., $g(\mathbf{x}) = f(\mathbf{x}A \oplus \mathbf{b})$, for all $\mathbf{x} \in \mathbb{F}_2^n$, where $A \in GL(n, \mathbb{F}_2)$ and $\mathbf{b} \in \mathbb{F}_2^n$. There exists an unique $\mathbf{b}' \in \mathbb{F}_2^n$ such that $\mathbf{b} = \mathbf{b}'A$, and so, $g(\mathbf{x}) = f((\mathbf{x} \oplus \mathbf{b}')A)$. Define a matrix M'_g from M_g as if $b'_i = 1,\ 1 \le i \le n$, then $\bar{\mathbf{v}}^i$ is the ith row of M'_g, otherwise $\mathbf{v}^i$ is the ith row of M'_g. We consider $P = A^T$, transpose matrix of A, and a nonsigular matrix Q of order $\#supp(g) \times \#supp(g)$, which swap only column vectors, if necessary. Then we get $M_f = PM'_gQ$. To prove the converse part, it is sufficient to find a $A \in GL(n, \mathbb{F}_2)$ and $\mathbf{b}' \in \mathbb{F}_2^n$ such that $g(\mathbf{x}) = f((\mathbf{x} \oplus \mathbf{b}')A)$, for all $\mathbf{x} \in \mathbb{F}_2^n$. Let $b'_i = 1$ if the ith rows of M_g and M'_g are complement to each other, otherwise $b'_i = 0,\ 1 \le i \le n$. The ith row of A is same as the ith column of $P,\ 1 \le i \le n$. Then A is nonsingular and $g(\mathbf{x}) = f((\mathbf{x} \oplus \mathbf{b}')A)$, for all $\mathbf{x} \in \mathbb{F}_2^n$. □

Let $n = 2k$. Suppose P_i, $1 \le i \le 2^k - 1$, is a binary matrix of order $k \times 2^{k-1}$ and row vectors of P_i are $\mathbf{a}^{i1}, \mathbf{a}^{i2}, \ldots, \mathbf{a}^{ik}$ such that for any $1 \le i \le 2^k - 1$, $wt(\oplus_{t=1}^{k}\varepsilon_{it}\mathbf{a}^{it}) = k$, where $(\varepsilon_{i1}, \varepsilon_{i2}, \ldots, \varepsilon_{ik}) \in \mathbb{F}_2^k$, and $(\varepsilon_{i1}, \varepsilon_{i2}, \ldots, \varepsilon_{ik}) \neq (\varepsilon_{j1}, \varepsilon_{j2}, \ldots, \varepsilon_{jk})$ for all $1 \le i \neq j \le 2^k - 1$. Let us define $2^k - 1$ binary matrix Q_i, $1 \le i \le 2^k - 1$, of order $k \times 2^{k-1}$ such that all column vectors are same, and column vectors of Q_i and Q_j are distinct for all $1 \le i \neq j \le 2^k - 1$. Define a matrix M of order $2k \times (2^{2k-1} - 2^{k-1})$:

$$M = \begin{pmatrix} P_1 & P_2 & \cdots & P_{2^k-1} \\ Q_1 & Q_2 & \cdots & Q_{2^k-1} \end{pmatrix}.$$

For any fixed choice of P_i's and Q_i's, the row vectors of M provide a linear code of length $2^{2k-1} - 2^{k-1}$ and dimension $2k$ such that the weight of of any nonzero codeword is 2^{2k-2} or $2^{2k-2} - 2^{k-1}$ since M is a support matrix corresponding to a bent function in Maiorana-McFarland class of the form $\mathbf{x} \cdot \pi(\mathbf{y})$. Here P_i and Q_i are related to the variables $\mathbf{x}$ and $\mathbf{y}$, respectively.

Suppose P_0 and Q_0 are two binary matrices of order $k \times 2^k$ such that P_0 is a zero matrix and the column vectors of Q_0 are all binary vectors of length k. Define a matrix M' of order $2k \times (2^{2k-1} + 2^{k-1})$:

$$M' = \begin{pmatrix} P_0 & P_1 & P_2 & \cdots & P_{2^k-1} \\ Q_0 & Q_1 & Q_2 & \cdots & Q_{2^k-1} \end{pmatrix}.$$

It is clear that $\mathbf{0}$ is not a column vector of P_i, $1 \leq i \leq 2^k - 1$, otherwise $wt(\oplus_{t=1}^{k} \varepsilon_{it}\mathbf{a}^{it}) \neq k$. Thus, all the column vectors of M' are distinct. For any fixed choice of P_i's and Q_i's, the row vectors of M' provide a linear code of length $2^{2k-1} + 2^{k-1}$ and dimension $2k$ such that the weight of of any nonzero codeword is 2^{2k-2} or $2^{2k-2} + 2^{k-1}$ since M' is a support matrix corresponding to a bent function in $\mathcal{D}_0$ class [1] of the form $\mathbf{x} \cdot \pi(\mathbf{y}) \oplus \prod_{i=1}^{k}(x_i \oplus 1)$.

In Theorem 9, we can consider that Q is an orthogonal matrix of order $\#supp(g) \times \#supp(g)$ such that each row and column have exactly one 1. So, Q is weight invariant, i.e., $wt(\mathbf{x}) = wt(\mathbf{x}Q)$, for all $\mathbf{x} \in \mathbb{F}_2^{\#supp(g)}$. Knowing a bent function, we can construct another bent function. Let us define $RC(2^{n-1} - 2^{\frac{n}{2}-1}, \mathbb{F}_2) \subset GL(2^{n-1} - 2^{\frac{n}{2}-1}, \mathbb{F}_2)$ such that if $wt(\mathbf{x}) \in \{2^{n-2}, 2^{n-2} - 2^{\frac{n}{2}-1}\}$, then $wt(\mathbf{x}A) \in \{2^{n-2}, 2^{n-2} - 2^{\frac{n}{2}-1}\}$. It is clear that the matrix $Q \in RC(2^{n-1} - 2^{\frac{n}{2}-1}, \mathbb{F}_2)$. From Construction 1 we get the next result.

Corollary 10. *Let $f \in \mathcal{B}_n$ be a bent function with $\#supp(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$ and M_f be the matrix corresponding to f. Suppose $T \in RC(2^{n-1} - 2^{\frac{n}{2}-1}, \mathbb{F}_2)$. Then the Boolean function corresponding to M_fT is bent.*

Proof. Let $f \in \mathcal{B}_n$ be a bent function and $\mathbf{u}^1, \mathbf{u}^2, \ldots, \mathbf{u}^n$ be the row vectors of M_f. From Corollary 5 we have $wt(\oplus_{i=1}^{n} \varepsilon_i \mathbf{u}^i) \in \{2^{n-2}, 2^{n-2} - 2^{\frac{n}{2}-1}\}$, where $\varepsilon_i \in \mathbb{F}_2,\ 1 \leq i \leq n$, except all zero. Suppose the row vectors of M_fT are $\mathbf{v}^1, \mathbf{v}^2, \ldots, \mathbf{v}^n$, i.e., $\mathbf{v}^i = \mathbf{u}^iT,\ 1 \leq i \leq n$. The weight of any nonzero linear combination of $\mathbf{v}^i,\ 1 \leq i \leq n$, is $wt(\oplus_{i=1}^{n} \varepsilon_i \mathbf{v}^i) = wt(\oplus_{i=1}^{n} (\varepsilon_i \mathbf{u}^i)T) = wt((\oplus_{i=1}^{n} \varepsilon_i \mathbf{u}^i)T) \in \{2^{n-2}, 2^{n-2} - 2^{\frac{n}{2}-1}\}$. The proof is completed. □

If $f \in \mathcal{B}_n$ is a bent function with $\#supp(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$, then we can rewrite the necessary and sufficient condition given in Theorem 9 in more simple way. The rank of the corresponding matrix M_f is n, so the n row vectors generate $2^n - 1$ nonzero vectors having Hamming weight either 2^{n-2} or $2^{n-2} - 2^{\frac{n}{2}-1}$. Let $g \in \mathcal{B}_n$ be a bent function with $\#supp(g) = 2^{n-1} - 2^{\frac{n}{2}-1}$. To check the affine equivalence between f and g, we follow the steps given below.

- We first define a binary matrix M'_g using M_g as the ith row of M'_g is either $\mathbf{v}^i$ or $\bar{\mathbf{v}}^i$, where $\mathbf{v}^i$ is the ith row of $M_g,\ 1 \leq i \leq n$.
- There exists a M'_g such that each row vector (maybe after swapping some fixed, for all row vectors of M_f, positions) of M_f can be express as a nonzero linear combinations of row vectors of M'_g.

If above condition is satisfied then f and g are affine equivalent, i.e., $g(\mathbf{x}) = f(\mathbf{x}A \oplus \mathbf{b})$, for all $\mathbf{x} \in \mathbb{F}_2^n$, where $A \in GL(n, \mathbb{F}_2)$ and $\mathbf{b} \in \mathbb{F}_2^n$ depends on the choice of $\mathbf{v}^i$ and $\bar{\mathbf{v}}^i$. Let $\mathbf{b} = \mathbf{0}$ and the ith row vector $\mathbf{u}^i$ of M_f be equal to $\mathbf{u}^i = \bigoplus_{j=1}^{n} \varepsilon_j \mathbf{v}^j$, where $\varepsilon_j \in \mathbb{F}_2,\ 1 \leq i, j \leq n$. Then the ith column of A is equal to $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n)$.

Now we identify all bent functions which are affine equivalent to a know bent function. Suppose $f \in \mathcal{B}_n$ be a bent function with $\#supp(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$ and the row vectors of M_f are $\mathbf{v}^1,\ \mathbf{v}^2,\ \ldots,\ \mathbf{v}^n$. Now, we derive all the bent functions which are affine equivalent to f as following way.

- First we construct the sets $A(\delta_1, \delta_2, \ldots, \delta_n)$ as

$$A(\delta_1, \delta_2, \ldots, \delta_n) = \{\mathbf{u}^i \in \mathbb{F}_2^{2^{n-1}-2^{\frac{n}{2}-1}} :\ \mathbf{u}^i = \delta_i \mathbf{v}^i \oplus \bar{\delta}_i \bar{\mathbf{v}}^i,\ \delta_i \in \mathbb{F}_2,\ 1 \le i \le n\}.$$

- For each choice of $\delta_i \in \mathbb{F}_2,\ 1 \le i \le n$, we choose any n linearly independent elements from linear span of $A(\delta_1, \delta_2, \ldots, \delta_n)$, and from each choice we can construct a bent function which is affine equivalent to f.

4 New characterizations and constructions of hyper-bent functions

In this section, we derive a necessary and sufficient condition for hyper-bent functions. The hyper-bent functions are usually defined over $\mathbb{F}_{2^n}$. Here we identify any element $a \in \mathbb{F}_{2^n}$ as a binary vector $\mathbf{a} \in \mathbb{F}_2^n$. Let us denote, for any $a \in \mathbb{F}_{2^n}$ and $f \in \mathcal{B}_n$:

$$\begin{aligned} E_f(i,a,0) &= \{x \in supp(f) : \mathrm{Tr}_1^n(ax^i) = 0\} \\ \text{and}\quad E_f(i,a,1) &= \{x \in supp(f) : \mathrm{Tr}_1^n(ax^i) = 1\}, \end{aligned} \tag{5}$$

where i is an integer co-prime to $2^n - 1$. It is clear that $E_f(i,0,0) = supp(f)$ and $E_f(i,a,0) \cup E_f(i,a,1) = supp(f)$, for all $f \in \mathcal{B}_n$, $a \in \mathbb{F}_{2^n}$ and i, defined as in above. If f is a hyper-bent function in n variables, then f is also bent, and so, for any $a \in \mathbb{F}_{2^n}$

$$\#supp(f) = \#E_f(i,a,0) + \#E_f(i,a,1) = 2^{n-1} \pm 2^{\frac{n}{2}-1}. \tag{6}$$

It is clear that $\mathcal{W}^i_{f\oplus 1}(a) = -\mathcal{W}^i_f(a)$, for all $a \in \mathbb{F}_{2^n}$ and i, co-prime to $2^n - 1$. Thus, if f is hyper-bent, then $f \oplus 1$ is also, and the converse is also true. Without loss of generality, let $\#supp(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$, in the rest of the paper. It is also known that if $i = 1$, then f is bent, and so the results described in Sections 3 and 4 are same when $i = 1$. Let $f, g \in \mathcal{B}_n$ be affine equivalent, i.e., $g(x) = f(L(x) \oplus b)$, for all $x \in \mathbb{F}_{2^n}$, where L is a linear permutation over $\mathbb{F}_{2^n}$ and $b \in \mathbb{F}_{2^n}$. Then for any $a \in \mathbb{F}_{2^n}$

$$\begin{aligned} \mathcal{W}^i_g(a) &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{g(x)\oplus \mathrm{Tr}_1^n(ax^i)} = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{f(L(x)\oplus b)\oplus \mathrm{Tr}_1^n(ax^i)} \\ &= \sum_{y\in\mathbb{F}_{2^n}} (-1)^{f(y)\oplus \mathrm{Tr}_1^n(a(L^{-1}(y\oplus b))^i)} \neq \pm 2^{\frac{n}{2}},\ \text{in general.} \end{aligned}$$

Thus, if f is hyper-bent then g may be not a hyper-bent function.

Proposition 11. *Let $f \in \mathcal{B}_n$ be a hyper-bent function and $\#supp(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$. Then for any nonzero $a \in \mathbb{F}_{2^n}$ and i, co-prime to $2^n - 1$,*

$$(\#E_f(i,a,0), \#E_f(i,a,1)) \in \{(2^{n-2}, 2^{n-2} - 2^{\frac{n}{2}-1}), (2^{n-2} - 2^{\frac{n}{2}-1}, 2^{n-2})\},$$

where $E_f(i,a,0)$ and $E_f(i,a,0)$ are defined as in (5).

Proof. For any hyper-bent function $f \in \mathcal{B}_n$ we know that $\mathcal{W}_f^i(a) = \pm 2^{\frac{n}{2}}$ for all $a \in \mathbb{F}_{2^n}$ and i, co-prime to $2^n - 1$. So, for any nonzero $a \in \mathbb{F}_{2^n}$, we have

$$\begin{aligned}\pm 2^{\frac{n}{2}} &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x) \oplus \mathrm{Tr}_1^n(ax^i)} = \sum_{x \in \mathbb{F}_{2^n}} (1 - 2f(x))(-1)^{\mathrm{Tr}_1^n(ax^i)} \\ &= 2^n \delta_0(a) - 2 \sum_{x \in supp(f)} (-1)^{\mathrm{Tr}_1^n(ax^i)} = -2 \sum_{x \in supp(f)} (-1)^{\mathrm{Tr}_1^n(ax^i)}.\end{aligned}$$

Thus, $\#E_f(i,a,0) - \#E_f(i,a,1) = \pm 2^{\frac{n}{2}-1}$. From (6), we have $\#E_f(i,a,0) + \#E_f(i,a,1) = 2^{n-1} - 2^{\frac{n}{2}-1}$, and so, combing these two equations we get the results. □

Proposition 12. *Let $f \in \mathcal{B}_n$ and the cardinality of $supp(f)$ be $2^{n-1} - 2^{\frac{n}{2}-1}$. Then f is a hyper-bent function if and only if for any nonzero $a \in \mathbb{F}_{2^n}$*

$$(\#E_f(i,a,0), \#E_f(i,a,1)) \in \{(2^{n-2}, 2^{n-2} - 2^{\frac{n}{2}-1}), (2^{n-2} - 2^{\frac{n}{2}-1}, 2^{n-2})\},$$

where $E_f(i,a,0)$ and $E_f(i,a,1)$ are defined as in (5), for all i, co-prime to $2^n - 1$.

Proof. Let $f \in \mathcal{B}_n$ and $\#supp(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$. Suppose f is a hyper-bent function. Then from Proposition 11, we get the necessary claim. To prove the converse part, it is sufficient to prove that $\mathcal{W}_f^i(a) = \pm 2^{\frac{n}{2}}$, for all $a \in \mathbb{F}_{2^n}$ and i, co-prime to $2^n - 1$. For any i, co-prime to $2^n - 1$, $\mathcal{W}_f^i(0) = 2^n - 2\#supp(f) = 2^{\frac{n}{2}}$. For any nonzero $a \in \mathbb{F}_{2^n}$ and i, co-prime to $2^n - 1$, we have either $(\#E_f(i,a,0), \#E_f(i,a,1)) = (2^{n-2}, 2^{n-2} - 2^{\frac{n}{2}-1})$, and then $\mathcal{W}_f^i(a) = 2(\#E_f(i,a,0) - \#E_f(i,a,1)) = 2^{\frac{n}{2}}$, or we have $(\#E_f(i,a,0), \#E_f(i,a,1)) = (2^{n-2} - 2^{\frac{n}{2}-1}, 2^{n-2})$, and then $\mathcal{W}_f^i(a) = -2^{\frac{n}{2}}$. Thus, $\mathcal{W}_f^i(a) = \pm 2^{\frac{n}{2}}$ for all $a \in \mathbb{F}_{2^n}$ and i, co-prime to $2^n - 1$. Hence, we get the result. □

From Proposition 12, we also get some information about the support set of hyper-bent functions which are similar as in Corollary 4.

Let α be a primitive element of $\mathbb{F}_{2^n}$ and $\mathbb{F}_{2^n} = \{0\} \cup \{\alpha^k : \ 0 \le k \le 2^n - 2\}$. Suppose $f \in \mathcal{B}_n$ such that $f(0) = 0$ and $S = \{k : \ f(\alpha^k) = 1, \ 0 \le k \le 2^n - 2\}$ with $\#S = 2^{n-1} - 2^{\frac{n}{2}-1}$. From Proposition 12, we have the following remark.

Remark 13. *Let $f \in \mathcal{B}_n$, n even, such that $f(0) = 0$ and S be defined as above. Then f is hyper-bent if and only if $\sum_{k \in S} \mathrm{Tr}_1^n(\alpha^{ik+t}) \in \{2^{n-2}, 2^{n-2} - 2^{\frac{n}{2}-1}\}$, for all $0 \le t \le 2^n - 2$, where $\gcd(i, 2^n - 1) = 1$.*

Proof. Suppose α is a primitive element of $\mathbb{F}_{2^n}$ and $a = \alpha^t \in \mathbb{F}_{2^n}$. Let $f \in \mathcal{B}_n$ such that $f(0) = 0$ and $S = \{k : \ f(\alpha^k) = 1, \ 0 \le k \le 2^n - 2\}$ with $\#S = 2^{n-1} - 2^{\frac{n}{2}-1}$. Then for any $0 \le t \le 2^n - 2$ and i, co-prime to $2^n - 1$, we have

$$\begin{aligned}\sum_{k \in S} \mathrm{Tr}_1^n(\alpha^{ik+t}) &= \#\{k \in S : \mathrm{Tr}_1^n(\alpha^{ik+t}) = 1\} = \#\{x \in supp(f) : \mathrm{Tr}_1^n(ax^i) = 1\} \\ &= \#E_f(i,a,1),\end{aligned}$$

and so, from Proposition 12 we get the result. □

Youssef et al. [21, Theorem 1] constructed a class of hyper-bent functions by considering a particular form of S so that the conditions are satisfied. Identify a hyper-bent

function other than the ones obtained by Youssef et al. [21, Theorem 1] is till an open problem.

For any $a, x \in \mathbb{F}_{2^n}$, $\mathrm{Tr}_1^n(ax)$ can be identified as $\mathbf{a} \cdot \mathbf{x} = a_1x_1 \oplus a_2x_2 \oplus \cdots \oplus a_nx_n$, where $\mathbf{a}$ and $\mathbf{x}$ are the n-bit binary strings corresponding to a and x, respectively. Let π_i be a permutation over $\mathbb{F}_{2^n}$ defined by $\pi_i(x) = x^i$, for all $x \in \mathbb{F}_{2^n}$ and i, co-prime to $2^n - 1$. An equivalent permutation over vector space is denoted by $\pi_i(\mathbf{x}) = \mathbf{x}^i$, $\mathbf{x} \in \mathbb{F}_2^n$.

Let $\mathbf{a} \in \mathbb{F}_2^n$ with $wt(\mathbf{a}) = r$, $1 \leq r \leq n$, that is, there exist r indexes $i_1, i_2, \ldots, i_r$ such that $a_{i_1} = a_{i_2} = \cdots = a_{i_r} = 1$ and other coordinates are equal to 0. Then $\mathbf{a} \cdot \mathbf{x} = x_{i_1} \oplus x_{i_2} \oplus \cdots \oplus x_{i_r}$. For all $1 \leq i_1 < i_2 < \cdots < i_r \leq n$ and i, co-prime to $2^n - 1$, let

$$A_f(i,\ i_1 < i_2 < \cdots < i_r, 0) = \{\mathbf{x}^i :\ \mathbf{x} \in supp(f) \text{ and } x_{i_1}^i \oplus x_{i_2}^i \oplus \cdots \oplus x_{i_r}^i = 0\},$$

where $r \in \{1, 2, \ldots, n\}$. We get the next result directly from Proposition 12.

Corollary 14. *Let $f \in \mathcal{B}_n$ and the cardinality of $supp(f)$ be $2^{n-1} - 2^{\frac{n}{2}-1}$. Then f is a hyper-bent function if and only if for all $r \in \{1, 2, \ldots, n\}$ and for all $1 \leq i_1 < i_2 < \cdots < i_r \leq n$ and i, co-prime to $2^n - 1$,*

$$\#A_f(i,\ i_1 < i_2 < \cdots < i_r, 0) \in \{2^{n-2}, 2^{n-2} - 2^{\frac{n}{2}-1}\}.$$

It is clear that if $\#A_f(1,\ i_1 < i_2 < \cdots < i_r, 0) \in \{2^{n-2}, 2^{n-2} - 2^{\frac{n}{2}-1}\}$, then $\#A_f(2^j,\ i_1 < i_2 < \cdots < i_r, 0) \in \{2^{n-2}, 2^{n-2} - 2^{\frac{n}{2}-1}\}$, for any non-negative integer j. From Lemma 7 and Corollary 14, we can construct an n-variable hyper-bent function, where n is even, in the following way.

Construction 2. Let n be an even positive integer and $S = \{i :\ \gcd(i, 2^n - 1) = 1 \text{ and } 1 \leq i \leq 2^n - 1\}$. Choose $\#S$ subsets $A_i,\ i \in S$, of $\mathbb{F}_2^{2^{n-1}-2^{\frac{n}{2}-1}}$, where the cardinality of each subset A_i is n. For any $i \in S$, let $A_i = \{\mathbf{v}^{i1}, \mathbf{v}^{i2}, \ldots, \mathbf{v}^{in}\}$. Define subsets B_i of $\mathbb{F}_2^n$ using A_i, and B_i' of $\mathbb{F}_2^n$ using $B_1,\ i \in S$ (here $B_1 = B_1'$) as

$$B_i = \{\mathbf{x} \in \mathbb{F}_2^n :\ x_j = v_k^{ij},\ 1 \leq j \leq n \text{ and for a fixed } 1 \leq k \leq 2^{n-1} - 2^{\frac{n}{2}-1}\}$$
$$B_i' = \{\mathbf{y} \in \mathbb{F}_2^n :\ \mathbf{y} = \mathbf{x}^i,\ \mathbf{x} \in B_1\}\ \ (\mathbf{x}^i \text{ is the binary representation of } x^i,\ x \in \mathbb{F}_{2^n})$$

such that the following conditions are satisfied.

- For any $i \in S$,
$$wt\left(\bigoplus_{j=1}^{n} \varepsilon_{ij}\mathbf{v}^{ij}\right) \in \{2^{n-2}, 2^{n-2} - 2^{\frac{n}{2}-1}\},$$
where $\varepsilon_{ij} \in \mathbb{F}_2,\ 1 \leq j \leq n$, except all zero.
- For any $i \in S$ with $i \neq 1$, $B_i = B_i'$.

Define a function $f \in \mathcal{B}_n$ such that $supp(f) = B_1$. Then f is hyper-bent, according to Lemma 7 and Corollary 14.

Let $n = 2m$ and $f \in \mathcal{B}_n$ of the form $f(x) = \mathrm{Tr}_1^n(ax^{2^m-1})$, for all $x \in \mathbb{F}_{2^n}$, where $a \in \mathbb{F}_{2^m}$. Then f is a bent function [10, 11] if and only if the Kloosterman sum $K_m(a)$ is equal to 0, where $K_m(a) = 1 + \sum_{x \in \mathbb{F}_{2^m}^*} (-1)^{\mathrm{Tr}_1^m(ax + \frac{1}{x})}$. From [7, Lemma 1] we know

that if $\mathrm{Tr}_1^m(a) = 1$, then $K_m(a) \neq 0$, and so f is not a bent function. Then f is not hyper-bent.

Now we identify a hyper-bent function in 4 variables of the form $g(x) = \mathrm{Tr}_1^4(\alpha x^3)$, for all $x \in \mathbb{F}_{2^4}$, where α is a root of the primitive polynomial $x^4 \oplus x^3 \oplus 1$ over $\mathbb{F}_2$. It is clear that $\alpha \notin \mathbb{F}_{2^2}$ as $\alpha^3 \neq 1$. We consider the normal basis $\{\alpha, \alpha^2, \alpha^4, \alpha^8\}$ and move from $\mathbb{F}_{2^4}$ to $\mathbb{F}_2^4$ and converse. The support of g is $supp(g) = \{1, \alpha, \alpha^5, \alpha^6, \alpha^{10}, \alpha^{11}\}$, the corresponding vector representation is

$$supp(g) = \{1111, 1000, 1010, 1110, 0101, 0110\}.$$

Now we prove that the support set of g satisfy the conditions given in Corollary 14. The matrix representation of the support set of g is

$$M_g = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

The subspace generated by the row vectors of M_g is

$$Rot(100010) \cup Rot(110110) \cup Rot(111100) \cup Rot(000000),$$

where $Rot(\mathbf{x})$ is the set of all elements under the action of permutation group which contains the rotations of 6 symbols. Thus, the weight of any nonzero elements are 2 or 4, and so, g is bent.

Denote $S = \{i : \ \gcd(i, 15) = 1 \text{ and } 1 \leq i \leq 15\} = \{1, 2, 4, 7, 8, 11, 13, 14\}$. If g is hyper-bent if and only if the above conditions are true after ith power of all elements of $supp(g)$, where $i \in S$. When $i = 2, 4$ and 8, the binary representation of $x^i, \ x \in \mathbb{F}_{2^4}$, is shifted by $1, 2$ and 3, respectively. So the corresponding matrix is just the row interchange(s) of M_g, and so, the weight of any nonzero elements generated from row vectors are 2 or 4. Let us denote the set of ith power of all elements of $supp(g)$ be $\{supp(g)\}^i$ and corresponding matrix $M_g^i, \ i \in S$.
For $i = 7$: $\{supp(g)\}^7 = \{1, \alpha^7, \alpha^5, \alpha^{12}, \alpha^{10}, \alpha^2\} = \{1111, 0011, 1010, 0111, 0101, 0100\}$, so

$$M_g^7 = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}.$$

Thus, the subspaces generated by the row vectors of M_g and M_g^7 are same.
For $i = 11$: $\{supp(g)\}^{11} = \{1, \alpha^{11}, \alpha^{10}, \alpha^6, \alpha^5, \alpha\} = \{1111, 0110, 0101, 1110, 1010, 1000\}$, so

$$M_g^{11} = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

Thus, the subspaces generated by the row vectors of M_g and M_g^{11} are same.

For $i = 13$*:* $\{supp(g)\}^{13} = \{1, \alpha^{13}, \alpha^5, \alpha^3, \alpha^{10}, \alpha^8\} = \{1111, 1100, 1010, 1101, 0101, 0001\}$, so

$$M_g^{13} = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Thus, the subspaces generated by the row vectors of M_g and M_g^{13} are same.
For $i = 14$*:* $\{supp(g)\}^{14} = \{1, \alpha^{14}, \alpha^{10}, \alpha^9, \alpha^5, \alpha^4\} = \{1111, 1001, 0101, 1011, 1010, 0010\}$, so

$$M_g^{14} = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

Thus, the subspaces generated by the row vectors of M_g and M_g^{14} are same. Hence, g is hyper-bent.

Now we consider a Maiorana–McFarland bent function h in 4 variables of the form $h(x_1, x_2, x_3, x_4) = x_1x_2 \oplus x_3x_4$, for all $\mathbf{x} \in \mathbb{F}_2^4$. Then the support set of h is $supp(h) = \{0011, 0111, 1011, 1100, 1101, 1110\} = \{\alpha^7, \alpha^{12}, \alpha^9, \alpha^{13}, \alpha^3, \alpha^6\}$ (corresponding elements over $\mathbb{F}_{2^4}$). Then

$$M_h = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 \end{pmatrix},$$

and subspace generated by the row vectors of M_h is

$$\{000000, 100010, 010100, 000011, 001100, 011000, 100001, 111001, 111100,$$
$$011011, 101101, 110110, 111010, 101110, 110101\}.$$

So, the conditions described in Corollary 5 are satisfied. It seems that all elements of the subspace generated by the row vectors of M_h belong to $Rot(100010)$, $Rot(000011)$, $Rot(111001)$, $Rot(011011)$, $Rot(111010)$ and $Rot(000000)$. Thus, there is a difference between the subspaces generated by the row vectors of M_g and M_h. Now we are going to check the other conditions for hyper-bentness.
For $i = 7$*:* $\{supp(h)\}^7 = \{\alpha^4, \alpha^9, \alpha^3, \alpha, \alpha^6, \alpha^{12}\} = \{0010, 1011, 1101, 1000, 1110, 0111\}$, so

$$M_h^7 = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

The conditions given in Corollary 14 are not satisfied, so h is not hyper-bent.

5 Conclusions

Bent and hyper-bent functions are not classified. A complete classification of these functions is elusive and looks hopeless. So, it is important to design constructions

in order to know as many of (hyper)-bent functions as possible. In this paper, we exhibit new characterizations and original construction methods for designing bent and hyper-bent Boolean functions by analyzing their supports. Arguments from coding theory have been used to derive such constructions. The given construction method is promising especially for the case of hyper-bent functions for which no method has been given since their introduction 20 years ago.

Acknowledgment. The authors are very grateful to the reviewers and the Associate Editor for their helpful comments and suggestions which have highly improved the manuscript. They thank INRIA, France for supporting this research. The research of C. Tang was supported by National Natural Science Foundation of China (Grant No. 11871058).

References

[1] C. Carlet, *Two New Classes of Bent Functions*, Eurocrypt '93, LNCS, vol. 765 , pp. 77–101, 1994.

[2] C. Carlet, P. Guillot, *A characterization of binary bent functions*, Journal of Combinatorial Theory, Series A, vol. 76, pp. 328–335, 1996.

[3] C. Carlet, *Boolean Functions for Cryptography and Error Correcting Codes*, Chapter of the monograph: Boolean Models and Methods in Mathematics, Computer Science, and Engineering, Cambridge University Press, Yves Crama and Peter L. Hammer (eds.), pp. 257–397, 2010. Available: `http://www-roc.inria.fr/secret/Claude.Carlet/pubs.html`.

[4] C. Carlet and S. Mesnager, *Four decades of research on bent functions* Designs, Codes and Cryptography, vol. 78 (1), pp. 5–50, 2016.

[5] A. Canteaut and P. Charpin, *Decomposing Bent Functions*, IEEE Transactions on Information Theory, vol. 49 (8), pp. 2004–2019, 2003.

[6] T. W. Cusick, P. Stănică, *Cryptographic Boolean functions and applications*, Elsevier–Academic Press, 2009.

[7] P. Charpin, G. Gong, *Hyper-bent functions, Kloosterman sums and Dickson polynomials*, IEEE International Symposium on Information Theory, Toronto, ON, Canada, 2008.

[8] C. Ding, *Designs from Linear Codes*. World Scientific, Singapore, 2018.

[9] C. Ding, A. Munemasa, V. Tonchev, *Bent vectorial functions, codes and designs*, IEEE Trans. Inf. Theory, vol. 65, no. 11, pp. 7533–7541, 2019.

[10] J. F. Dillon, *Elementary Hadamard Difference sets*, PhD Thesis, University of Maryland, 1974.

[11] J. F. Dillon, *Elementary Hadamard Difference Sets*, Proceedings of 6th S. E. Conference of Combinatorics, Graph Theory, and Computing, Utility Mathematics, Winnipeg, pp. 237–249, 1975.

[12] H. Dobbertin, *Construction of bent functions and balanced Boolean functions with high nonlinearity*, Fast Software Encryption, Leuven 1994, LNCS 1008, Springer-Verlag, pp. 61–74, 1995.

[13] S. W. Golomb and G. Gong, *Transform domain analysis of DES*, IEEE Transactions on Information Theory, vol. 45 (6), pp. 2065–2073, 1999.

[14] M. Hell, T. Johansson, W. Meier, *A stream cipher proposal: Grain-128,* eSTREAM ECRYPT Stream Cipher Project; 2006. URL: http://www.ecrypt.eu.org/stream/grainpf.html.

[15] R. L. McFarland, *A family of noncyclic difference sets*, Journal of Combinatorial Theory, Series A, vol. 15, pp. 1–10, 1973.

[16] S. Mesnager, *Bent Functions–Fundamentals and Results* Springer, Switzerland ISBN 978-3-319-32593-4, pp. 1–544, 2016.

[17] O. S. Rothaus, *On Bent Functions*, Journal of Combinatorial Theory, Series A, vol. 20, pp. 300–305, 1976.

[18] D. Tang, B. Mandal and S. Maitra, *Vectorial Boolean functions with very low differential-linear uniformity using Maiorana–McFarland type construction,* Indocrypt 2019, LNCS, vol. 11898. pp. 341–360, 2019.

[19] D. Tang, S. Kavut, B. Mandal and S. Maitra, *Modifying Maiorana–McFarland type bent functions for good cryptographic properties and efficient implementation* SIAM Journal on Discrete Mathematics, vol. 33 (1), pp. 238–256, 2019.

[20] D. Tang and S. Maitra, *Constructions of n-variable* ($n \equiv 2 \mod 4$) *balanced Boolean functions with maximum absolute value in autocorrelation spectra* $< 2^{\frac{n}{2}}$, IEEE Transactions on Information Theory, vol. 64 (1), pp. 393–402, 2018.

[21] A. M. Youssef and G. Gong, *Hyper–Bent Functions*, Advances in Cryptology – EUROCRYP'01, Lecture Notes in Computer Science, vol. 2045, pp. 406–419, 2001.

[22] Y. Zheng, J Pieprzyk, J Seberry, *Haval–a one-way hashing algorithm with variable length of output (extended abstract)'* ASIACRYPT 1992, LNCS, vol. 718, pp. 83–104, 1993.

[23] — *CAST-128. Rfc 2144–the cast-128 encryption algorithm;* 1997. URL: http://www. faqs.org/rfcs/rfc2144.html.