Nega–Hadamard Transform, Bent and Negabent Functions

Pantelimon Stănică[1], Sugata Gangopadhyay[2], Ankita Chaturvedi[2], Aditi Kar Gangopadhyay[2], and Subhamoy Maitra[3]

[1] Department of Applied Mathematics, Naval Postgraduate School, Monterey, CA 93943–5216, USA
pstanica@nps.edu

[2] Department of Mathematics, Indian Institute of Technology Roorkee Roorkee 247667 India
{gsugata,ankitac17,ganguli.aditi}@gmail.com

[3] Applied Statistics Unit, Indian Statistical Institute, 203 B. T. Road, Calcutta 700 108, India
subho@isical.ac.in

Abstract. In this paper we start developing a detailed theory of nega–Hadamard transforms. Consequently, we derive several results on negabentness of concatenations, and partially-symmetric functions. We also obtain a characterization of bent–negabent functions in a subclass of Maiorana–McFarland set. As a by-product of our results we obtain simple proofs of several existing facts.

Keywords: Boolean functions, nega–Hadamard transforms, bent and negabent functions.

1 Introduction

Let $\mathbb{F}_2$ be the prime field of characteristic 2 and let $\mathbb{F}_2^n$ is the n-dimensional vector space over $\mathbb{F}_2$. A function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is called a Boolean function on n variables. The reader is referred to Section 1.1 for all the basic notations and definitions related to Boolean functions.

Boolean functions received a lot of attention in the field of coding theory, sequences and cryptology. The most important method of analyzing the Boolean functions is by exploiting a certain kind of discrete Fourier transform, which is known, in Boolean function literature, as Walsh, Hadamard, or Walsh–Hadamard transform [4]. The maximum nonlinearity of a Boolean function is achieved when the maximum absolute value in the Walsh spectrum is minimized. For even n, such functions are well known as bent functions and the magnitudes of all the values in Walsh spectrum are the same. From the perspective of coding theory, these functions attain the covering radius of first order Reed–Muller code. Towards a nega–periodic analogue of the bent criteria, one can use nega–Hadamard transform and investigate Boolean functions with nega flat spectrum. This motivated several works in the area of Boolean functions [11,13,14,19] in the last few years.

C. Carlet and A. Pott (Eds.): SETA 2010, LNCS 6338, pp. 359–372, 2010.

In this paper we concentrate on the nega–Hadamard transform in more details. In particular, we have the following broad contributions.

- We present a detailed study of some of the properties of nega–Hadamard transform in Section 2. We obtain several results analogous to Hadamard transformation.
- Based on the previous analysis, we obtain several results with respect to the decomposition of negabent functions in Section 3.
- In Section 4, we study negabent functions that are symmetric with respect to two variables. Our study results simple proof of the main result in the paper [17] that all the symmetric negabent functions must be affine.
- A characterization of some bent–negabent functions in Maiorana–McFarland class is obtained in Section 5, thus complementing some results of [19].

1.1 Definitions and Notations

The set of all Boolean functions on n variables is denoted by $\mathcal{B}_n$. Any element $\mathbf{x} \in \mathbb{F}_2^n$ can be written as an n-tuple $(x_1, \ldots, x_n)$, where $x_i \in \mathbb{F}_2$ for all $i = 1, \ldots, n$. The set of integers, real numbers and complex numbers are denoted by $\mathbb{Z}$, $\mathbb{R}$ and $\mathbb{C}$ respectively. The addition over $\mathbb{Z}$, $\mathbb{R}$ and $\mathbb{C}$ is denoted by '+'. The addition over $\mathbb{F}_2^n$ for all $n \geq 1$, is denoted by $\oplus$. If $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$ are two elements of $\mathbb{F}_2^n$, we define the scalar (or inner) product, respectively, the intersection by

$$\mathbf{x} \cdot \mathbf{y} = x_1 y_1 \oplus x_2 y_2 \oplus \cdots \oplus x_n y_n, \mathbf{x} * \mathbf{y} = (x_1 y_1, x_2 y_2, \ldots, x_n y_n).$$

The cardinality of the set S is denoted by $|S|$. If $z = a + b\imath \in \mathbb{C}$, then $|z| = \sqrt{a^2 + b^2}$ denotes the absolute value of z, and $\overline{z} = a - b\imath$ denotes the complex conjugate of z, where $\imath^2 = -1$, and $a, b \in \mathbb{R}$. Any $f \in \mathcal{B}_n$ can be expressed in *algebraic normal form* (ANF) as

$$f(x_1, x_2, \ldots, x_n) = \bigoplus_{\mathbf{a}=(a_1,\ldots,a_n)\in\mathbb{F}_2^n} \mu_{\mathbf{a}} \left(\prod_{i=1}^{n} x_i^{a_i} \right), \ \mu_{\mathbf{a}} \in \mathbb{F}_2.$$

The (*Hamming*) *weight* of $\mathbf{x} \in \mathbb{F}_2^n$ is $wt(\mathbf{x}) := \sum_{i=1}^{n} x_i$. The algebraic degree of f, $\deg(f) := \max_{\mathbf{a}\in\mathbb{F}_2^n}\{wt(\mathbf{a}) : \mu_{\mathbf{a}} \neq 0\}$. Boolean functions having algebraic degree at most 1 are said to be *affine functions*. For any two functions $f, g \in \mathcal{B}_n$, we define the (*Hamming*) *distance* $d(f, g) = |\{\mathbf{x} : f(\mathbf{x}) \neq g(\mathbf{x}), \mathbf{x} \in \mathbb{F}_{2^n}\}|$.

The *Walsh–Hadamard transform* of $f \in \mathcal{B}_n$ at any point $\mathbf{u} \in \mathbb{F}_2^n$ is defined by

$$\mathcal{H}_f(\mathbf{u}) = 2^{-\frac{n}{2}} \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}}.$$

A function $f \in \mathcal{B}_n$ is a *bent function* if $|\mathcal{H}_f(\mathbf{u})| = 1$ for all $\lambda \in \mathbb{F}_2^n$. Bent functions (defined by Rothaus [15] more than thirty years ago) hold an interest among researchers in this area since they have maximum Hamming distance

from the set of all affine Boolean functions. Several classes of bent functions were constructed by Rothaus [15], Dillon [6], Dobbertin [7], and later by Carlet [1].

The sum $\mathcal{C}_{f,g}(\mathbf{z}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{f(\mathbf{x})\oplus g(\mathbf{x}\oplus\mathbf{z})}$ is the *crosscorrelation* of f and g at z. The *autocorrelation* of $f \in \mathcal{B}_n$ at $\mathbf{u} \in \mathbb{F}_2^n$ is $\mathcal{C}_{f,f}(\mathbf{u})$ above, which we denote by $\mathcal{C}_f(\mathbf{u})$. It is known [4] that a function $f \in \mathcal{B}_n$ is bent if and only if $\mathcal{C}_f(\mathbf{u}) = 0$ for all $\mathbf{u} \neq 0$.

For a detailed study of Boolean functions we refer to Carlet [2,3], and Cusick and Stănică [4].

The *nega–Hadamard transform* of $f \in \mathbb{F}_2^n$ at any vector $\mathbf{u} \in \mathbb{F}_2^n$ is the complex valued function:

$$\mathcal{N}_f(\mathbf{u}) = 2^{-\frac{n}{2}} \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}}\, \imath^{wt(\mathbf{x})}.$$

A function is said to be *negabent* if the nega–Hadamard transform is flat in absolute value, namely $|\mathcal{N}_f(\mathbf{u})| = 1$ for all $\mathbf{u} \in \mathbb{F}_2^n$. The sum

$$C_{f,g}(\mathbf{z}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})\oplus g(\mathbf{x}\oplus\mathbf{z})}(-1)^{\mathbf{x}\cdot\mathbf{z}}$$

is the *nega–crosscorrelation* of f and g at z. We define the *nega–autocorrelation* of f at $\mathbf{u} \in \mathbb{F}_2^n$ by

$$C_f(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})\oplus f(\mathbf{x}\oplus\mathbf{u})}(-1)^{\mathbf{x}\cdot\mathbf{u}}.$$

The negaperiodic autocorrelation defined by Parker and Pott [11,12] is as follows

$$n_f(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})\oplus f(\mathbf{x}\oplus\mathbf{u})}(-1)^{wt(\mathbf{u})}(-1)^{\mathbf{x}\cdot\mathbf{u}}.$$

It is to be noted that the difference between the above two definitions is not critical and both the defintions can be used.

As we will be referring later, we also present the definition of a symmetric Boolean function. A Boolean function is said to be symmetric if inputs of the same weight produce the same output, that is, $f(\mathbf{x}) = f(\sigma(\mathbf{x}))$, for any permutation σ.

2 Properties of Nega–Hadamard transform

It is a well known fact that if $f \in \mathcal{B}_n$, then the Walsh–Hadamard transform $\mathcal{H}_f(\lambda)$ is invertible, and so,

$$(-1)^{f(\mathbf{x})} = 2^{-\frac{n}{2}} \sum_{\mathbf{u}\in\mathbb{F}_2^n} \mathcal{H}_f(\mathbf{u})(-1)^{\mathbf{x}\cdot\mathbf{u}}, \tag{1}$$

for all $\mathbf{x} \in \mathbb{F}_2^n$. The nega–Hadamard transform is also a unitary transformation. An immediate consequence of the definition of nega–Hadamard transformation of a function $f \in \mathcal{B}_n$ in [11,14] is the following:

Lemma 1. *Suppose $f \in \mathcal{B}_n$. Then*

$$(-1)^{f(\mathbf{y})} = 2^{-\frac{n}{2}}\, \imath^{-wt(\mathbf{y})} \sum_{u \in \mathbb{F}_2^n} \mathcal{N}_f(\mathbf{u})(-1)^{\mathbf{y}\cdot\mathbf{u}}, \tag{2}$$

for all $\mathbf{y} \in \mathbb{F}_2^n$.

Next, we prove a theorem that gives the nega–Hadamard transform of various combinations of Boolean functions. We shall use throughout the well-known identity (see [10])

$$wt(\mathbf{x} \oplus \mathbf{y}) = wt(\mathbf{x}) + wt(\mathbf{y}) - 2wt(\mathbf{x} * \mathbf{y}). \tag{3}$$

Theorem 1. *Let f, g, h be in $\mathcal{B}_n$. The following statements are true:*

(*a*) $\mathcal{N}_{\mathbf{0}}(\mathbf{u}) = -\mathcal{N}_{\mathbf{1}}(\mathbf{u}) = \omega^n\, \imath^{-wt(\mathbf{u})}$, *and* $\mathcal{N}_{h\oplus 1}(\mathbf{u}) = -\mathcal{N}_h(\mathbf{u})$, $\mathbf{u} \in \mathbb{F}_2^n$, *where* $\mathbf{0}, \mathbf{1}$ *are the constant* 0, *respectively,* 1 *functions; and,* ω *is an* 8*-th primitive root of* 1, *namely* $\omega = (1+\imath)/\sqrt{2}$. *In general, for any affine function* $\ell_{\mathbf{a},c}(\mathbf{x}) = \mathbf{a}\cdot\mathbf{x} \oplus c$, *we have* $\mathcal{N}_{\ell_{\mathbf{a},c}}(\mathbf{u}) = (-1)^c\, \omega^n\, \imath^{-wt(\mathbf{a}\oplus\mathbf{u})}$.

(*b*) *If* $h(\mathbf{x}) = f(\mathbf{x}) \oplus g(\mathbf{x})$ *on* $\mathbb{F}_2^n$, *then for* $\mathbf{u} \in \mathbb{F}_2^n$,

$$\mathcal{N}_h(\mathbf{u}) = 2^{-n/2} \sum_{\mathbf{v}\in\mathbb{F}_2^n} \mathcal{N}_f(\mathbf{v})\mathcal{H}_g(\mathbf{u}\oplus\mathbf{v}) = 2^{-n/2} \sum_{v\in\mathbb{F}_2^n} \mathcal{H}_f(\mathbf{v})\mathcal{N}_g(\mathbf{u}\oplus\mathbf{v}).$$

(*c*) *If* $\ell_{\mathbf{a},c}(\mathbf{x}) = \mathbf{a}\cdot\mathbf{x} \oplus c$ *is affine, then* $\mathcal{N}_{f\oplus\ell_{\mathbf{a},c}}(\mathbf{u}) = (-1)^c \mathcal{N}_f(\mathbf{a}\oplus\mathbf{u})$.

(*d*) *If* $h(\mathbf{x}) = f(A\mathbf{x}\oplus\mathbf{a})$, *then* $\mathcal{N}_h(\mathbf{u}) = (-1)^{\mathbf{a}\cdot(A\mathbf{u})}\, \imath^{wt(\mathbf{a})}\, \mathcal{N}_f(A\mathbf{u}\oplus\mathbf{a})$, *where* A *is an* $n\times n$ *orthogonal matrix over* $\mathbb{F}_2$ *(and so,* $A^TA = I_n$*).*

(*e*) *If* $h(\mathbf{x},\mathbf{y}) = f(\mathbf{x}) \oplus g(\mathbf{y}), \mathbf{x},\mathbf{y} \in \mathbb{F}_2^n$, *then* $\mathcal{N}_{f\oplus g}(\mathbf{u},\mathbf{v}) = \mathcal{N}_f(\mathbf{u})\mathcal{N}_g(\mathbf{v})$.

(*f*) *If* $f \in \mathcal{B}_n, g \in \mathcal{B}_k$, *and* $h(\mathbf{x},\mathbf{y}) = f(\mathbf{x})g(\mathbf{y})$, *then*

$$2^{k/2}\mathcal{N}_h(\mathbf{u},\mathbf{v}) = \mathcal{N}_f(\mathbf{u})A_{g1}(\mathbf{v}) + \omega^n\, \imath^{-wt(\mathbf{u})} A_{g0}(\mathbf{v}),$$
$$A_{g1}(\mathbf{v}) + A_{g0}(\mathbf{v}) = 2^{k/2}\omega^k \imath^{-wt(\mathbf{v})},$$

where $A_{g0}(\mathbf{v}) = \sum_{\mathbf{y},g(\mathbf{y})=0} (-1)^{\mathbf{y}\cdot\mathbf{v}}\, \imath^{wt(\mathbf{y})}$, $A_{g1}(\mathbf{v}) = \sum_{\mathbf{y},g(\mathbf{y})=1} (-1)^{\mathbf{y}\cdot\mathbf{v}}\, \imath^{wt(\mathbf{y})}$. *Moreover, if* $k = 1$,

$$2^{1/2}\mathcal{N}_{yf(\mathbf{x})}(\mathbf{u}, v) = (-1)^v\, \imath\mathcal{N}_f(\mathbf{u}) + \omega^n\, \imath^{-wt(\mathbf{u})}$$
$$2^{1/2}\mathcal{N}_{(y\oplus 1)f(\mathbf{x})}(\mathbf{u}, v) = \mathcal{N}_f(\mathbf{u}) + \omega^n(-1)^v\, \imath^{-wt(\mathbf{u})+1}.$$

Proof. Claim (*a*) follows from Lemma 1 of [19], since $\mathcal{N}_{\mathbf{0}}(\mathbf{u}) = -\mathcal{N}_{\mathbf{1}}(\mathbf{u}) = 2^{-n/2}\sum_{\mathbf{y}}(-1)^{\mathbf{u}\cdot\mathbf{y}}\, \imath^{wt(\mathbf{y})} = \omega^n\, \imath^{-wt(\mathbf{u})}$. We now show the first identity of (*b*) (the second is absolutely similar). Since

$$\mathcal{N}_f(\mathbf{v}) = 2^{-n/2} \sum_{\mathbf{y}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{y})\oplus\mathbf{y}\cdot\mathbf{v}}\, \imath^{wt(\mathbf{y})}$$
$$\mathcal{H}_g(\mathbf{u}\oplus\mathbf{v}) = 2^{-n/2} \sum_{\mathbf{z}\in\mathbb{F}_2^n} (-1)^{g(\mathbf{z})\oplus\mathbf{z}\cdot(\mathbf{u}\oplus\mathbf{v})}$$

and (see [4, p. 8])

$$\sum_{\mathbf{x}}(-1)^{\mathbf{v}\cdot\mathbf{x}} = \begin{cases} 2^n & \text{if } \mathbf{v}=\mathbf{0} \\ 0 & \text{if } \mathbf{v}\neq\mathbf{0}, \end{cases}$$

we obtain (all sums are over $\mathbb{F}_2^n$)

$$\begin{aligned}\sum_{\mathbf{v}\in\mathbb{F}_2^n}\mathcal{N}_f(\mathbf{v})\mathcal{H}_g(\mathbf{u}\oplus\mathbf{v}) &= 2^{-n}\sum_{\mathbf{v},\mathbf{y},\mathbf{z}}(-1)^{f(\mathbf{y})\oplus g(\mathbf{z})+\mathbf{v}\cdot(\mathbf{y}\oplus\mathbf{z})\oplus\mathbf{u}\cdot\mathbf{z}}\imath^{wt(\mathbf{y})} \\ &= 2^{-n}\sum_{\mathbf{y},\mathbf{z}}(-1)^{f(\mathbf{y})\oplus g(\mathbf{z})\oplus\mathbf{u}\cdot\mathbf{z}}\imath^{wt(\mathbf{y})}\sum_{\mathbf{v}}(-1)^{\mathbf{v}\cdot(\mathbf{y}\oplus\mathbf{z})} \\ &= \sum_{\mathbf{y}}(-1)^{f(\mathbf{y})\oplus g(\mathbf{y})\oplus\mathbf{u}\cdot\mathbf{y}}\imath^{wt(\mathbf{y})} = 2^{n/2}\mathcal{N}_{f\oplus g}(\mathbf{u}).\end{aligned}$$

Further, (c) follows from (b), since

$$\begin{aligned}\mathcal{H}_{\ell_{\mathbf{a},c}}(\mathbf{w}) &= 2^{-n/2}\sum_{\mathbf{y}}(-1)^{\mathbf{a}\cdot\mathbf{y}\oplus\mathbf{w}\cdot\mathbf{y}\oplus c} \\ &= 2^{-n/2}(-1)^c\sum_{\mathbf{y}}(-1)^{(\mathbf{a}\oplus\mathbf{w})\cdot\mathbf{y}} \\ &= \begin{cases}(-1)^c 2^{n/2} & \text{if } \mathbf{a}=\mathbf{w} \\ 0 & \text{if } \mathbf{a}\neq\mathbf{w}.\end{cases}\end{aligned}$$

The property (d) can be derived from [11, Lemma 2] and [19, Theorem 2]. It is to be noted that [19, Theorem 2] further proves that the action of orthogonal group preserves bent–negabentness property of a Boolean function. Item (e) is straightforward. To show item (f), we write

$$\begin{aligned}2^{(n+k)/2}\mathcal{N}_h(\mathbf{u},\mathbf{v}) &= \sum_{(\mathbf{x},\mathbf{y})\in\mathbb{F}_2^{n+k}}(-1)^{f(\mathbf{x})g(\mathbf{y})\oplus\mathbf{x}\cdot\mathbf{u}\oplus\mathbf{y}\cdot\mathbf{v}}\imath^{wt(\mathbf{x})+wt(\mathbf{y})} \\ &= \sum_{\mathbf{y},g(\mathbf{y})=1}(-1)^{\mathbf{y}\cdot\mathbf{v}}\imath^{wt(\mathbf{y})}\sum_{\mathbf{x}}(-1)^{f(\mathbf{x})\oplus\mathbf{x}\cdot\mathbf{u}}\imath^{wt(\mathbf{x})} \\ &\quad+\sum_{\mathbf{y},g(\mathbf{y})=0}(-1)^{\mathbf{y}\cdot\mathbf{v}}\imath^{wt(\mathbf{y})}\sum_{\mathbf{x}}(-1)^{\mathbf{x}\cdot u}\imath^{wt(\mathbf{x})} \\ &= 2^{n/2}\mathcal{N}_f(\mathbf{u})\sum_{\mathbf{y},g(\mathbf{y})=1}(-1)^{\mathbf{y}\cdot\mathbf{v}}\imath^{wt(\mathbf{y})} \\ &\quad+2^{n/2}\omega^n\imath^{-wt(\mathbf{u})}\sum_{\mathbf{y},g(\mathbf{y})=0}(-1)^{\mathbf{y}\cdot\mathbf{v}}\imath^{wt(\mathbf{y})},\end{aligned}$$

from which we obtain the desired identity. Moreover, if $k=1$, and $g(y)=y$, then $A_{g0}(v)=1, A_{g1}(v)=(-1)^v\imath$, and if $g(y)=y\oplus 1$, then $A_{g1}(v)=1, A_{g0}(v)=(-1)^v\imath$, and so

$$\begin{aligned}2^{1/2}\mathcal{N}_{yf(\mathbf{x})}(\mathbf{u},v) &= (-1)^v\imath\mathcal{N}_f(\mathbf{u})+\omega^n\imath^{-wt(\mathbf{u})} \\ 2^{1/2}\mathcal{N}_{(y\oplus 1)f(\mathbf{x})}(\mathbf{u},v) &= \mathcal{N}_f(\mathbf{u})+\omega^n(-1)^v\imath^{-wt(\mathbf{u})+1}.\end{aligned}$$

The proof of the theorem is done. □

The next result is analogous to the result on the crosscorrelation of two Boolean functions [16]. In the nega–Hadamard transform context, the basic idea of this result is explained in [5] and equation (15) of [13]. In Lemma 2 we are able to use Hadamard transform because unlike the definition in [5,13] our nega–crosscorrelation does not include the factor $(-1)^{wt(\mathbf{u})}$.

Lemma 2. *If $f, g \in \mathcal{B}_n$, then the nega–crosscorrelation*

$$C_{f,g}(\mathbf{z}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})\oplus g(\mathbf{x}\oplus\mathbf{z})}(-1)^{\mathbf{x}\cdot\mathbf{z}} = \imath^{wt(\mathbf{z})} \sum_{\mathbf{u}\in\mathbb{F}_2^n} \mathcal{N}_f(\mathbf{u})\overline{\mathcal{N}_g(\mathbf{u})}(-1)^{\mathbf{u}\cdot\mathbf{z}}.$$

Proof. The sum

$$\begin{aligned}\imath^{wt(\mathbf{z})} \sum_{\mathbf{u}\in\mathbb{F}_2^n} \mathcal{N}_f(\mathbf{u})\overline{\mathcal{N}_g(\mathbf{u})}(-1)^{\mathbf{u}\cdot\mathbf{z}} &= 2^{-n} \sum_{\mathbf{x}\in\mathbb{F}_2^n}\sum_{\mathbf{y}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})\oplus g(\mathbf{y})}\, \imath^{wt(\mathbf{x})-wt(\mathbf{y})+wt(\mathbf{z})} \\ &\quad \times \sum_{\mathbf{u}\in\mathbb{F}_2^n} (-1)^{\mathbf{u}\cdot(\mathbf{x}\oplus\mathbf{y}\oplus\mathbf{z})} \\ &= \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})\oplus g(\mathbf{x}\oplus\mathbf{z})}(-1)^{\mathbf{x}\cdot\mathbf{z}}.\end{aligned}$$

□

If we consider the case $f = g$ in the previous lemma, then we obtain

$$\begin{aligned}\sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})\oplus f(\mathbf{x}\oplus\mathbf{z})}(-1)^{\mathbf{x}\cdot\mathbf{z}} &= \imath^{wt(\mathbf{z})} \sum_{\mathbf{u}\in\mathbb{F}_2^n} \mathcal{N}_f(\mathbf{u})\overline{\mathcal{N}_f(\mathbf{u})}(-1)^{\mathbf{u}\cdot\mathbf{z}} \\ &= \imath^{wt(\mathbf{z})} \sum_{\mathbf{u}\in\mathbb{F}_2^n} |\mathcal{N}_f(\mathbf{u})|^2(-1)^{\mathbf{u}\cdot\mathbf{z}}.\end{aligned} \tag{4}$$

This is an analogue of autocorrelation of Boolean functions. It is to be noted that since both Hadamard and nega–Hadamard transforms are unitary they are energy preserving and hence, Parseval's theorem holds for both the transformations. The classical Parseval's identity takes the form

$$\sum_{\mathbf{u}\in\mathbb{F}_2^n} (\mathcal{H}_f(\mathbf{u}))^2 = 2^n$$

for Walsh–Hadamard transform. Substituting $\mathbf{z} = \mathbf{0}$ in the equation (4), we obtain a proof of this fact for the particular case of nega–Hadamard transforms.

Corollary 1 (*nega–Parseval's identity).* *We have*

$$\sum_{\mathbf{u}\in\mathbb{F}_2^n} |\mathcal{N}_f(\mathbf{u})|^2 = 2^n. \tag{5}$$

Lemma 3. *A Boolean function $f \in \mathcal{B}_n$ is negabent if and only if, $C_f(\mathbf{z}) = 0$ for all $\mathbf{z} \in \mathbb{F}_2^n \setminus \{0\}$.*

Proof. If f is a negabent function then $|\mathcal{N}_f(\mathbf{u})| = 1$ for all $\mathbf{u} \in \mathbb{F}_2^n$. For all $\mathbf{z} \neq \mathbf{0}$, then by (4) we obtain $C_f(\mathbf{z}) = 0$. The converse also follows from the equation (4). □

An equivalent result is proved after equation (15) in [13], and in [11, Theorem 2] for the negaperiodic autocorrelation.

Remark 1. Lemma 3 provides an alternative characterization of negabent functions.

If f is an affine function, then for all $\mathbf{z} \in \mathbb{F}_2^n \setminus \{\mathbf{0}\}$ the nega–autocorrelation $C_f(\mathbf{z}) = 0$. This implies that any affine function is negabent. For alternative proofs we refer to [19, Lemma 1] and [11, Proposition 1].

3 Decomposition of Negabent Functions with Respect to Co-dimension One Subspaces

Suppose $1 \leq r \leq n$. Then any function $f \in \mathcal{B}_n$ can be thought of as a function from $\mathbb{F}_2^r \times \mathbb{F}_2^{n-r}$ into $\mathbb{F}_2$. For any fixed $\mathbf{v} \in \mathbb{F}_2^r$, the function $f_\mathbf{v} \in \mathcal{B}_{n-r}$ is defined as $f_\mathbf{v}(\mathbf{x}) = f(\mathbf{v}, \mathbf{x})$ for all $\mathbf{x} \in \mathbb{F}_2^{n-r}$.

Theorem 2. *Let $f \in \mathcal{B}_n$ expressed as $f : \mathbb{F}_2^r \times \mathbb{F}_2^{n-r} \to \mathbb{F}_2$. Then*

$$C_f(\mathbf{u}, \mathbf{w}) = \sum_{\mathbf{v} \in \mathbb{F}_2^r} C_{f_\mathbf{v}, f_{\mathbf{v}\oplus\mathbf{u}}}(\mathbf{w})(-1)^{\mathbf{v}\cdot\mathbf{u}}.$$

Proof. By definition

$$\begin{aligned} C_f(\mathbf{u}, \mathbf{w}) &= \sum_{\mathbf{v} \in \mathbb{F}_2^r} \sum_{\mathbf{z} \in \mathbb{F}_2^{n-r}} (-1)^{f(\mathbf{v},\mathbf{z}) \oplus f(\mathbf{v}\oplus\mathbf{u}, \mathbf{z}\oplus\mathbf{w})} (-1)^{\mathbf{v}\cdot\mathbf{u} \oplus \mathbf{z}\cdot\mathbf{w}} \\ &= \sum_{\mathbf{v} \in \mathbb{F}_2^r} (-1)^{\mathbf{v}\cdot\mathbf{u}} \sum_{\mathbf{z} \in \mathbb{F}_2^{n-r}} (-1)^{f_\mathbf{v}(\mathbf{z}) \oplus f_{\mathbf{v}\oplus\mathbf{u}}(\mathbf{z}\oplus\mathbf{w})} (-1)^{\mathbf{z}\cdot\mathbf{w}} \qquad (6) \\ &= \sum_{\mathbf{v} \in \mathbb{F}_2^r} C_{f_\mathbf{v}, f_{\mathbf{v}\oplus\mathbf{u}}}(\mathbf{w})(-1)^{\mathbf{v}\cdot\mathbf{u}}. \end{aligned}$$

□

Corollary 2. *Suppose $f \in \mathcal{B}_n$ is expressed as*

$$f(\mathbf{x}, y) = f_0(\mathbf{x})(1 \oplus y) \oplus f_1(\mathbf{x})y, \text{ for all } (\mathbf{x}, y) \in \mathbb{F}_2^{n-1} \times \mathbb{F}_2,$$

where $f_0, f_1 \in \mathcal{B}_{n-1}$. Then

$$\begin{aligned} C_f(\mathbf{w}, 0) &= C_{f_0}(\mathbf{w}) + C_{f_1}(\mathbf{w}) \\ C_f(\mathbf{w}, 1) &= C_{f_0,f_1}(\mathbf{w}) - (-1)^{wt(\mathbf{w})} C_{f_0,f_1}(\mathbf{w}). \end{aligned}$$

The functions f and g are said to have *complementary nega–autocorrelation* if for all nonzero $\mathbf{u} \in \mathbb{F}_2^n$

$$C_f(\mathbf{u}) + C_g(\mathbf{u}) = 0.$$

The following lemma establishes a connection between the nega–autocorrelations of f, g and their nega–Hadamard transformations.

Lemma 4. *Two functions $f, g \in \mathcal{B}_n$ have complementary nega–autocorrelations if and only if*

$$|\mathcal{N}_f(\mathbf{u})|^2 + |\mathcal{N}_g(\mathbf{u})|^2 = 2 \text{ for all } \mathbf{u} \in \mathbb{F}_2^n.$$

Proof. Let f, g be two functions with complementary nega–autocorrelations. Then

$$\begin{aligned} |\mathcal{N}_f(\mathbf{u})|^2 + |\mathcal{N}_g(\mathbf{u})|^2 &= 2^{-n} \sum_{\mathbf{z} \in \mathbb{F}_2^n} \imath^{-wt(\mathbf{z})} (C_f(\mathbf{z}) + C_g(\mathbf{z}))(-1)^{\mathbf{z}\cdot\mathbf{u}} \\ &= 2^{-n} 2^{n+1} = 2. \end{aligned}$$

Conversely, suppose $|\mathcal{N}_f(\mathbf{u})|^2 + |\mathcal{N}_g(\mathbf{u})|^2 = 2$ for all $\mathbf{u} \in \mathbb{F}_2^n$. Then

$$\begin{aligned} C_f(\mathbf{z}) + C_g(\mathbf{z}) &= \imath^{wt(\mathbf{z})} \sum_{\mathbf{u} \in \mathbb{F}_2^n} (|\mathcal{N}_f(\mathbf{u})|^2 + |\mathcal{N}_g(\mathbf{u})|^2)(-1)^{\mathbf{u}\cdot\mathbf{z}} \\ &= 2\imath^{wt(\mathbf{z})} \sum_{\mathbf{u} \in \mathbb{F}_2^n} (-1)^{\mathbf{u}\cdot\mathbf{z}} \\ &= 2^{n+1} \imath^{wt(\mathbf{z})} \delta_0(\mathbf{z}), \end{aligned}$$

where

$$\delta_0(\mathbf{z}) = \begin{cases} 0 & \text{if } \mathbf{z} \neq \mathbf{0}; \\ 1 & \text{if } \mathbf{z} = \mathbf{0}. \end{cases} \tag{7}$$

Thus the functions f and g have complementary nega–autocorrelations. □

Theorem 3. *Suppose $h \in \mathcal{B}_{n+1}$ is expressed as*

$$h(\mathbf{x}, y) = f(\mathbf{x})(1 \oplus y) \oplus g(\mathbf{x})y, \text{ for all } (\mathbf{x}, y) \in \mathbb{F}_2^n \times \mathbb{F}_2,$$

where $f, g \in \mathcal{B}_n$. Then the following statements are equivalent:

(1) *h is negabent.*
(2) *f and g have complementary nega–autocorrelations and $C_{f_0,f_1}(\mathbf{u}) = 0$ for all $\mathbf{u} \in \mathbb{F}_2^n$ with $wt(\mathbf{u}) \equiv 1 \pmod 2$.*
(3) *$|\mathcal{N}_f(\mathbf{u})|^2 + |\mathcal{N}_g(\mathbf{u})|^2 = 2$ for all $\mathbf{u} \in \mathbb{F}_2^n$ and $\frac{\mathcal{N}_f(\mathbf{u})}{\mathcal{N}_g(\mathbf{u})}$ is a real number whenever $|\mathcal{N}_f(\mathbf{u})||\mathcal{N}_g(\mathbf{u})| \neq 0$.*

Proof. We show first (1) $\iff$ (2). Suppose h is a negabent function. Then $C_h(\mathbf{u}, a) = 0$ for all nonzero $(\mathbf{u}, a) \in \mathbb{F}_2^n \times \mathbb{F}_2$. From Corollary 2 we obtain

$$C_h(\mathbf{u}, 0) = C_f(\mathbf{u}) + C_g(\mathbf{u}) = 0,$$

for all $\mathbf{u} \in \mathbb{F}_2^n \setminus \{0\}$ and

$$C_h(\mathbf{u}, 1) = C_{f,g}(\mathbf{u})(1 - (-1)^{wt(\mathbf{u})}) = 0,$$

which implies $C_{f,g}(\mathbf{u}) = 0$ for all $\mathbf{u} \in \mathbb{F}_2^n$ with $wt(\mathbf{u}) \equiv 1 \pmod 2$.

Conversely, let us assume that the functions f and g have complementary nega–autocorrelations and $C_{f,g}(\mathbf{u}) = 0$ for all $\mathbf{u} \in \mathbb{F}_2^n$ with $wt(\mathbf{u}) \equiv 1 \pmod 2$. Then by Corollary 2, $C_h(\mathbf{u}, a) = 0$ for all nonzero $(\mathbf{u}, a) \in \mathbb{F}_2^n \times \mathbb{F}_2$. This implies that h is a negabent function.

We now show (1) $\iff$ (3). The nega–Hadamard transform of h at $(\mathbf{u}, a) \in \mathbb{F}_2^n \times \mathbb{F}_2$ is

$$\begin{aligned}\mathcal{N}_h(\mathbf{u}, a) &= 2^{-\frac{n+1}{2}} \sum_{(\mathbf{x},y)\in\mathbb{F}_2^n\times\mathbb{F}_2} (-1)^{h(\mathbf{x},y)\oplus\mathbf{u}\cdot\mathbf{x}\oplus ay}\, \imath^{wt(\mathbf{x},y)} \\ &= 2^{-\frac{n+1}{2}} \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{f(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}}\, \imath^{wt(\mathbf{x})} + 2^{-\frac{n+1}{2}} \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{g(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}\oplus a}\, \imath^{wt(\mathbf{x})+1} \\ &= \frac{1}{\sqrt{2}}\mathcal{N}_f(\mathbf{u}) + \imath\,(-1)^a \frac{1}{\sqrt{2}}\mathcal{N}_g(\mathbf{u}).\end{aligned}$$

Thus,

$$\mathcal{N}_h(\mathbf{u}, a) = \begin{cases} \frac{1}{\sqrt{2}}\mathcal{N}_f(\mathbf{u}) + \frac{\imath}{\sqrt{2}}\mathcal{N}_g(\mathbf{u}) & \text{if } a = 0; \\ \frac{1}{\sqrt{2}}\mathcal{N}_f(\mathbf{u}) - \frac{\imath}{\sqrt{2}}\mathcal{N}_g(\mathbf{u}) & \text{if } a = 1. \end{cases} \tag{8}$$

Since h is negabent $|\mathcal{N}_h(\mathbf{u}, a)| = 1$ for all $(\mathbf{u}, a) \in \mathbb{F}_2^n \times \mathbb{F}_2$ we obtain

$$\begin{aligned} \left|\frac{1}{\sqrt{2}}\mathcal{N}_f(\mathbf{u}) + \frac{\imath}{\sqrt{2}}\mathcal{N}_g(\mathbf{u})\right| &= 1, \\ \left|\frac{1}{\sqrt{2}}\mathcal{N}_f(\mathbf{u}) - \frac{\imath}{\sqrt{2}}\mathcal{N}_g(\mathbf{u})\right| &= 1. \end{aligned} \tag{9}$$

If h is negabent, then by Lemma 4 and the equivalence of the first two statements proved above we obtain:

$$|\mathcal{N}_f(\mathbf{u})|^2 + |\mathcal{N}_g(\mathbf{u})|^2 = 2 \text{ for all } \ \mathbf{u} \in \mathbb{F}_2^n.$$

Suppose for $\mathbf{u} \in \mathbb{F}_2^n$, $|\mathcal{N}_f(\mathbf{u})||\mathcal{N}_g(\mathbf{u})| \neq 0$. Let $z_1 = \frac{1}{\sqrt{2}}\mathcal{N}_f(\mathbf{u})$ and $z_2 = \frac{\imath}{\sqrt{2}}\mathcal{N}_g(\mathbf{u})$. Then by equation (9) we obtain

$$\begin{gathered} |z_1 + z_2|^2 = |z_1 - z_2|^2, \text{ that is} \\ z_1\overline{z_2} = -z_2\overline{z_1} \end{gathered}$$

Therefore we have $\mathcal{N}_f(\mathbf{u})\overline{\mathcal{N}_g(\mathbf{u})} = \mathcal{N}_g(\mathbf{u})\overline{\mathcal{N}_f(\mathbf{u})}$, i.e., $\frac{\mathcal{N}_f(\mathbf{u})}{\mathcal{N}_g(\mathbf{u})} = \frac{\overline{\mathcal{N}_f(\mathbf{u})}}{\overline{\mathcal{N}_g(\mathbf{u})}} = \overline{\left(\frac{\mathcal{N}_f(\mathbf{u})}{\mathcal{N}_g(\mathbf{u})}\right)}$. This proves that $\frac{\mathcal{N}_f(\mathbf{u})}{\mathcal{N}_g(\mathbf{u})}$ is a real number.

Conversely, suppose $|\mathcal{N}_f(\mathbf{u})|^2 + |\mathcal{N}_g(\mathbf{u})|^2 = 2$ for all $\mathbf{u} \in \mathbb{F}_2^n$ and $\frac{\mathcal{N}_f(\mathbf{u})}{\mathcal{N}_g(\mathbf{u})}$ is a real number whenever $|\mathcal{N}_f(\mathbf{u})||\mathcal{N}_g(\mathbf{u})| \neq 0$.

Without loss of generality, we may first assume $\mathcal{N}_f(\mathbf{u}) = 0$, for some $\mathbf{u} \in \mathbb{F}_2^n$. Then by the above condition $|\mathcal{N}_g(\mathbf{u})| = \sqrt{2}$. By equation (8), $|\mathcal{N}_h(\mathbf{u}, a)| = 1$ for

all $a \in \mathbb{F}_2$. Next we consider the case when $|\mathcal{N}_f(\mathbf{u})||\mathcal{N}_g(\mathbf{u})| \neq 0$. Let $\phi(\mathbf{u}) = \frac{\mathcal{N}_g(\mathbf{u})}{\mathcal{N}_f(\mathbf{u})}$. Then

$$\begin{aligned}
|\mathcal{N}_h(\mathbf{u},a)|^2 &= |\frac{1}{\sqrt{2}}\mathcal{N}_f(\mathbf{u}) + \imath(-1)^a\frac{1}{\sqrt{2}}\phi(\mathbf{u})\mathcal{N}_f(\mathbf{u})|^2 \\
&= \frac{1}{2}|\mathcal{N}_f(\mathbf{u})|^2|1+\imath(-1)^a\phi(\mathbf{u})|^2 \\
&= \frac{1}{2}|\mathcal{N}_f(\mathbf{u})|^2(1+|\phi(\mathbf{u})|^2) \qquad (10)\\
&= \frac{1}{2}|\mathcal{N}_f(\mathbf{u})|^2\left(1+\frac{|\mathcal{N}_g(\mathbf{u})|^2}{|\mathcal{N}_f(\mathbf{u})|^2}\right) \\
&= \frac{1}{2}(|\mathcal{N}_f(\mathbf{u})|^2+|\mathcal{N}_g(\mathbf{u})|^2) = 1.
\end{aligned}$$

Thus h is negabent. □

4 Negabent Functions Symmetric about Two Variables

Suppose $h \in \mathcal{B}_n$ is a Boolean function which is symmetric with respect to two variables, y and z say. Then there exist functions $f, g, s \in \mathcal{B}_{n-2}$ such that

$$h(\mathbf{x},y,z) = f(\mathbf{x}) \oplus (f(\mathbf{x}) \oplus g(\mathbf{x}))(y \oplus z) \oplus s(\mathbf{x})yz \qquad (11)$$

for all $(\mathbf{x},y,z) \in \mathbb{F}_2^{n-2} \times \mathbb{F}_2 \times \mathbb{F}_2$. The Boolean function h is bent if and only if, f and g are bent and $s(\mathbf{x}) = 1$ for all $\mathbf{x} \in \mathbb{F}_2^{n-2}$ (see [2,3,4,20]). For negabent functions we prove the following similar result.

Theorem 4. *Suppose $h \in \mathcal{B}_n$ is expressed as $h(\mathbf{x},y,z) = f(\mathbf{x}) \oplus (f(\mathbf{x}) \oplus g(\mathbf{x}))(y \oplus z) \oplus s(\mathbf{x})yz$ for all $(\mathbf{x},y,z) \in \mathbb{F}_2^{n-2} \times \mathbb{F}_2 \times \mathbb{F}_2$. The Boolean function h is negabent if and only if f and g are negabent and $s(\mathbf{x}) = 0$ for all $\mathbf{x} \in \mathbb{F}_2^n$.*

Proof. The nega–autocorrelation of h at $(0,1,1)$ is

$$\begin{aligned}
C_h(\mathbf{0},1,1) &= \sum_{\mathbf{x}\in\mathbb{F}_2^{n-2}}\sum_{y\in\mathbb{F}_2}\sum_{z\in\mathbb{F}_2}(-1)^{s(\mathbf{x})(1\oplus y\oplus z)}(-1)^{y\oplus z} \\
&= \sum_{\mathbf{x}\in\mathbb{F}_2^{n-2}}(-1)^{s(\mathbf{x})}\sum_{y\in\mathbb{F}_2}(-1)^{s(\mathbf{x})y\oplus y}\sum_{z\in\mathbb{F}_2}(-1)^{s(\mathbf{x})z\oplus z} \\
&= \sum_{\mathbf{x}\in\mathbb{F}_2^{n-2}}(-1)^{s(\mathbf{x})}\sum_{y\in\mathbb{F}_2}(-1)^{s(\mathbf{x})y\oplus y}(1+(-1)^{s(\mathbf{x})\oplus 1}) \\
&= 2\sum_{\mathbf{x}\in\mathbb{F}_2^{n-2},s(\mathbf{x})=1}(-1)\sum_{y\in\mathbb{F}_2}(-1)^{2y} = 4\sum_{\mathbf{x}\in\mathbb{F}_2^{n-2},s(\mathbf{x})=1}(-1) \\
&= -4|\{\mathbf{x}\in\mathbb{F}_2^{n-2} : s(\mathbf{x}) = 1\}|.
\end{aligned}$$

If h is a negabent function then $C_h(\mathbf{0}, 1, 1) = 0$. Therefore $|\{\mathbf{x} \in \mathbb{F}_2^{n-2} : s(\mathbf{x}) = 1\}| = 0$, which implies that $s(\mathbf{x}) = 0$ for all $\mathbf{x} \in \mathbb{F}_2^{n-2}$. Thus, if h is a negabent function and symmetric with respect to the variables y and z, then it can be expressed as

$h(\mathbf{x}, y, z) = f(\mathbf{x}) \oplus (f(\mathbf{x}) \oplus g(\mathbf{x}))(y \oplus z)$, for all $(\mathbf{x}, y, z) \in \mathbb{F}_2^{n-2} \times \mathbb{F}_2 \times \mathbb{F}_2$. The nega–Hadamard transform $\mathcal{N}_h(\mathbf{u}, a, b)$ of h at $(\mathbf{u}, a, b) \in \mathbb{F}_2^{n-2} \times \mathbb{F}_2 \times \mathbb{F}_2$ is

$$2^{-\frac{n}{2}} \sum_{\mathbf{x} \in \mathbb{F}_2^{n-2}} \sum_{y \in \mathbb{F}_2} \sum_{z \in \mathbb{F}_2} (-1)^{f(\mathbf{x}) \oplus (f(\mathbf{x}) \oplus g(\mathbf{x}))(y \oplus z) + \mathbf{u} \cdot \mathbf{x} \oplus ay \oplus bz} \imath^{wt(\mathbf{x}, y, z)}.$$

Expanding the above sum by substituting all possible values of $(y, z) \in \mathbb{F}_2 \times \mathbb{F}_2$ we obtain

$$\mathcal{N}_h(\mathbf{u}, a, b) = \tfrac{1-(-1)^{a \oplus b}}{2} \mathcal{N}_f(\mathbf{u}) + \imath \tfrac{(-1)^a + (-1)^b}{2} \mathcal{N}_g(\mathbf{u}). \tag{12}$$

Therefore $\mathcal{N}_h(\mathbf{u}, a, b) \in \{\mathcal{N}_f(\mathbf{u}), \pm \imath \mathcal{N}_g(\mathbf{u})\}$ for all $(\mathbf{u}, a, b) \in \mathbb{F}_2^{n-2} \times \mathbb{F}_2 \times \mathbb{F}_2$. This proves that both f and g are negabent. On the other hand if f and g are negabent functions then h is also negabent. This shows the converse. □

Corollary 3. *A symmetric negabent function is affine.*

Proof. Let $h \in \mathcal{B}_n$ be a symmetric negabent function. Let us suppose that h has algebraic degree greater than or equal to 2. Since h is symmetric, it is symmetric with respect to any two variables. Therefore, it is possible to express h, for at least one pair y, z of variables, as follows

$$h(\mathbf{x}, y, z) = f(\mathbf{x}) \oplus (f(\mathbf{x}) \oplus g(\mathbf{x}))(y \oplus z) \oplus s(\mathbf{x})yz,$$

where $s(\mathbf{x}) \neq 0$ for at least one $\mathbf{x} \in \mathbb{F}_2^{n-2}$. But this contradicts the fact that h is negabent. Hence all symmetric negabent functions are affine. □

The result of Corollary 3 gives an alternate proof of the fact proved in [17]. In fact, the case for even n can be immediately obtained following the result of Parker and Pott [11], which gives a connection between bent and negabent functions.

Theorem 5 ([11, Thm. 12]). *A function $f : \mathbb{F}_2^{2m} \to \mathbb{F}_2$ is negabent if and only if $f \oplus s_2$ is bent, where $s_2(x_1, x_2, \ldots, x_{2m}) = \sum_{i<j} x_i x_j$ is the elementary symmetric function of degree 2.*

We note that s_2 is actually a homogeneous (that is, all terms of its ANF are of the same degree), symmetric and quadratic bent function.

Let $s_1(x_1, x_2, \ldots, x_{2m}) = \sum_i x_i$, the (only) symmetric linear function involving all the variables. In [18] it is shown that the only symmetric bent functions are s_2, $s_2 \oplus s_1$, $1 \oplus s_2$, $1 \oplus s_2 \oplus s_1$.

In [17], it is proved (by a long argument) that all the symmetric negabent functions are affine. Following [18,11], the result of [17] can be achieved in a few lines for even n.

Theorem 6. *Let n be even. A symmetric function $f \in \mathcal{B}_n$ is negabent if and only if it is affine.*

Proof. Suppose $f \in \mathcal{B}_n$ is a symmetric negabent function. Then $f \oplus s_2$ is a bent function. Since the direct sum of two symmetric functions is symmetric, then $f \oplus s_2$ is a symmetric bent function. The only symmetric bent functions are s_2, $s_2 \oplus s_1$, $1 \oplus s_2$, $1 \oplus s_2 \oplus s_1$ (see [18]). Therefore f can be 0, 1, s_1, $1 \oplus s_1$ and nothing else. This proves that if f is a symmetric negabent function on even number of variables then it is affine.

Conversely, it is known that all affine functions are negabent [19]. Therefore, symmetric functions on even number of variables, if affine, are negabent. □

Bent functions do not exist for odd number of input variables. Thus there is no equivalent characterization of Theorem 5 for odd dimension, and the result of [17] cannot be proved trivially as before. However, the odd (as well as the even) case has already been taken care of by Corollary 3.

5 Bent–Negabent Functions in Maiorana–McFarland Class

In this section we shall investigate bent functions which are also negabent in the Maiorana-McFarland (MM) class of bent functions, namely

$$f(\mathbf{x}, \mathbf{y}) = \pi(\mathbf{x}) \cdot \mathbf{y} \oplus g(\mathbf{x}), \ \mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n \tag{13}$$

where π is a permutation satisfying $wt(\mathbf{x} \oplus \mathbf{y}) = wt(\pi(\mathbf{x}) \oplus \pi(\mathbf{y}))$ (we call π a *weight-sum invariant* permutation), for all $\mathbf{x}, \mathbf{y}$, and g is an arbitrary Boolean function, both on $\mathbb{F}_2^n$. We remark that if π is orthogonal, that is, $\pi(\mathbf{x}) = A \cdot \mathbf{x}$ with A orthogonal ($A^T A = I_n$), then it satisfies the imposed condition (since $wt(\pi(\mathbf{x}) \oplus \pi(\mathbf{y})) = wt(A(\mathbf{x} \oplus \mathbf{y}))$, it suffices to show that $wt(A\mathbf{z}) = wt(\mathbf{z})$; for that, consider $wt(A\mathbf{z}) = (A\mathbf{z})^T \cdot (A\mathbf{z}) = \mathbf{z}^T (A^T A)\mathbf{z} = wt(\mathbf{z})$). It could be interesting to see if there are such weight-sum invariant permutations outside of the linear orthogonal group generated ones.

Theorem 7. *A function as in* (13) *on $\mathbb{F}_2^{2n}$ is bent–negabent if and only if g is bent.*

Proof. We evaluate

$$\begin{aligned}
\mathcal{N}_f(\mathbf{u}, \mathbf{v}) &= 2^{-n} \sum_{(\mathbf{x},\mathbf{y}) \in \mathbb{F}_2^{2n}} (-1)^{\pi(\mathbf{x}) \cdot \mathbf{y} \oplus g(\mathbf{x}) \oplus \mathbf{x} \cdot \mathbf{u} \oplus \mathbf{y} \cdot \mathbf{v}} \imath^{wt(\mathbf{x}) + wt(\mathbf{y})} \\
&= 2^{-n} \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{g(\mathbf{x}) \oplus \mathbf{x} \cdot \mathbf{u}} \imath^{wt(\mathbf{x})} \sum_{\mathbf{y} \in \mathbb{F}_2^n} (-1)^{\pi(\mathbf{x}) \cdot \mathbf{y} \oplus \mathbf{y} \cdot \mathbf{v}} \imath^{wt(\mathbf{y})} \\
&= 2^{-n} \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{g(\mathbf{x}) \oplus \mathbf{x} \cdot \mathbf{u}} \imath^{wt(\mathbf{x})} 2^{n/2} \omega^n \imath^{-wt(\pi(\mathbf{x}) \oplus \mathbf{v})} \\
&= 2^{-n/2} \omega^n \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{g(\mathbf{x}) \oplus \mathbf{x} \cdot \mathbf{u}} \imath^{wt(\mathbf{x}) - wt(\pi(\mathbf{x}) \oplus \mathbf{v})}.
\end{aligned}$$

Now, using the fact that π is a weight-sum invariant permutation, and by (3), we obtain

$$\begin{aligned}
&wt(\pi(\mathbf{x}) \oplus \mathbf{v}) = wt(\mathbf{x} \oplus \pi^{-1}(\mathbf{v})),\\
&wt(\mathbf{x}) - wt(\pi(\mathbf{x}) \oplus \mathbf{v}) = -wt(\pi^{-1}(\mathbf{v})) + 2wt(\mathbf{x} * \pi^{-1}(\mathbf{v})), \text{ and}\\
&\imath^{2wt(\mathbf{x}*\pi^{-1}(\mathbf{v}))} = (-1)^{\mathbf{x}\cdot\pi^{-1}(\mathbf{v})},
\end{aligned}$$

which implies that

$$\begin{aligned}
\mathcal{N}_f(\mathbf{u},\mathbf{v}) &= 2^{-n/2}\omega^n\, \imath^{-wt(\pi^{-1}(\mathbf{v}))} \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{g(\mathbf{x})\oplus\mathbf{x}\cdot(\mathbf{u}\oplus\pi^{-1}(\mathbf{v}))}\\
&= \omega^n\, \imath^{-wt(\pi^{-1}(\mathbf{v}))}\mathcal{H}_g(\mathbf{u}\oplus\pi^{-1}(\mathbf{v})).
\end{aligned}$$

Consequently,

$$|\mathcal{N}_f(\mathbf{u},\mathbf{v})| = |\mathcal{H}_g(\mathbf{u}\oplus\pi^{-1}(\mathbf{v}))|,$$

which implies our claim. □

The following corollary follows easily from our theorem, since bent functions exist for any degree up to half of the (even) dimension. We remark that Theorem 10 of [11] gives an upper bound of $n-1$ on the degree of a bent–negabent function, but not an existence result.

Corollary 4. *If f as in* (13) *is bent–negabent with π weight-sum invariant, then the degree of f is bounded by $n/2$. Moreover, there exist bent–negabent functions in the MM class of any degree between* 2 *and* $n/2$.

Acknowledgements. The authors are thankful to the anonymous reviewers whose comments have improved the technical as well as the editorial quality of the paper. Ankita Chaturvedi thanks the University Grants Commission of India for supporting her research.

References

1. Carlet, C.: Two new classes of bent functions. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 77–101. Springer, Heidelberg (1994)
2. Carlet, C.: Boolean functions for cryptography and error correcting codes. In: Crama, Y., Hammer, P. (eds.) Boolean Methods and Models. Cambridge Univ. Press, Cambridge, `http://www-roc.inria.fr/secret/Claude.Carlet/pubs.html`
3. Carlet, C.: Vectorial Boolean functions for cryptography. In: Crama, Y., Hammer, P. (eds.) Boolean Methods and Models. Cambridge Univ. Press, Cambridge, `http://www-roc.inria.fr/secret/Claude.Carlet/pubs.html`
4. Cusick, T.W., Stănică, P.: Cryptographic Boolean functions and Applications. Elsevier/Academic Press (2009)
5. Danielsen, L.E., Gulliver, T.A., Parker, M.G.: Aperiodic Propagation Criteria for Boolean Functions. Inform. Comput. 204(5), 741–770 (2006)

6. Dillon, J.F.: Elementary Hadamard difference sets. In: Proceedings of Sixth S. E. Conference of Combinatorics, Graph Theory, and Computing, Utility Mathematics, Winnipeg, pp. 237–249 (1975)
7. Dobbertin, H.: Construction of bent functions and balanced Boolean functions with high nonlinearity. In: Preneel, B. (ed.) FSE 1994. LNCS, vol. 1008, pp. 61–74. Springer, Heidelberg (1995)
8. Dobbertin, H., Leander, G.: Bent functions embedded into the recursive framework of $\mathbb{Z}$-bent functions. Des. Codes Cryptography 49, 3–22 (2008)
9. Lidl, R., Niederreiter, H.: Introduction to finite fields and their applications. Cambridge University Press, Cambridge (1983)
10. MacWilliams, F.J., Sloane, N.J.A.: The theory of error–correcting codes. North-Holland, Amsterdam (1977)
11. Parker, M.G., Pott, A.: On Boolean functions which are bent and negabent. In: Golomb, S.W., Gong, G., Helleseth, T., Song, H.-Y. (eds.) SSC 2007. LNCS, vol. 4893, pp. 9–23. Springer, Heidelberg (2007)
12. Parker, M.G., Pott, A.: Personal Communications
13. Riera, C., Parker, M.G.: One and two-variable interlace polynomials: A spectral interpretation. In: Ytrehus, Ø. (ed.) WCC 2005. LNCS, vol. 3969, pp. 397–411. Springer, Heidelberg (2006)
14. Riera, C., Parker, M.G.: Generalized bent criteria for Boolean functions. IEEE Trans. Inform. Theory 52(9), 4142–4159 (2006)
15. Rothaus, O.S.: On bent functions. Journal of Combinatorial Theory Series A 20, 300–305 (1976)
16. Sarkar, P., Maitra, S.: Cross–Correlation Analysis of Cryptographically Useful Boolean Functions and S-Boxes. Theory Comput. Systems 35, 39–57 (2002)
17. Sarkar, S.: On the symmetric negabent Boolean functions. In: Roy, B., Sendrier, N. (eds.) INDOCRYPT 2009. LNCS, vol. 5922, pp. 136–143. Springer, Heidelberg (2009)
18. Savicky, P.: On the bent Boolean functions that are symmetric. European J. Comb. 15, 407–410 (1994)
19. Schmidt, K.U., Parker, M.G., Pott, A.: Negabent functions in the Maiorana–McFarland class. In: Golomb, S.W., Parker, M.G., Pott, A., Winterhof, A. (eds.) SETA 2008. LNCS, vol. 5203, pp. 390–402. Springer, Heidelberg (2008)
20. Zhao, Y., Li, H.: On bent functions with some symmetric properties. Discrete Appl. Math. 154, 2537–2543 (2006)