Investigations on Bent and Negabent Functions via the Nega-Hadamard Transform

Pantelimon Stănică, Sugata Gangopadhyay, Ankita Chaturvedi, Aditi Kar Gangopadhyay, and Subhamoy Maitra

***Abstract*—Parker *et al.* considered a new type of discrete Fourier transform, called nega-Hadamard transform. We prove several results regarding its behavior on combinations of Boolean functions and use this theory to derive several results on negabentness (that is, flat nega-spectrum) of concatenations, and partially symmetric functions. We derive the upper bound $\lceil \frac{n}{2} \rceil$ for the algebraic degree of a negabent function on n variables. Further, a characterization of bent–negabent functions is obtained within a subclass of the Maiorana–McFarland set. We develop a technique to construct bent–negabent Boolean functions by using complete mapping polynomials. Using this technique, we demonstrate that for each $\ell \geq 2$, there exist bent–negabent functions on $n = 12\ell$ variables with algebraic degree $\frac{n}{4} + 1 = 3\ell + 1$. It is also demonstrated that there exist bent–negabent functions on eight variables with algebraic degrees 2, 3, and 4. Simple proofs of several previously known facts are obtained as immediate consequences of our work.**

***Index Terms*—Bent and negabent functions, Hadamard and nega-Hadamard transforms.**

I. Introduction

Let $\mathbb{F}_2^n$ be the n-dimensional vector space over the two-element field $\mathbb{F}_2$. 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 I-A for all the basic notations and definitions related to Boolean functions.

The Walsh–Hadamard transform (a particular case of a discrete Fourier transform) has been exploited extensively for the analysis of Boolean functions and used in coding theory and cryptology [3], [4], [6]. For even dimension n, the functions that attain the largest distance from the set of affine functions (this maximum distance is the nonlinearity) are called bent functions. From the perspective of coding theory, these functions attain the covering radius of the first-order Reed–Muller code. Further, a Boolean function on an even number of variables is bent if and only if the magnitude of all the values in its Walsh–Hadamard spectrum are the same (flat Walsh–Hadamard spectrum). The Walsh–Hadamard transform is an example of a unitary transformation on the space of all Boolean functions. Riera and Parker [18] considered some generalized bent criteria for Boolean functions by analyzing Boolean functions that have flat spectrum with respect to one or more transforms chosen from a set of unitary transforms. The transforms chosen by Riera and Parker [18] are n-fold tensor products of the identity mapping $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, the Walsh–Hadamard transformation $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, and the nega-Hadamard transformation $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & \imath \\ 1 & -\imath \end{pmatrix}$, where $\imath^2 = -1$. Riera and Parker [18] mention that this choice is motivated by local unitary transforms that play an important role in the structural analysis of pure n-qubit stabilizer quantum states. As in the case of the classical discrete Fourier transform, a Boolean function whose nega-Hadamard magnitude spectrum is flat is said to be a *negabent* function.

The research initiated in [18] leads to the natural question of constructing Boolean functions which are both bent and negabent (these are referred to as bent–negabent functions [16], [23], [24]).

First, we concentrate on the nega-Hadamard transform in more detail. We prove various results in Section II on the behavior of the nega-Hadamard transform on affine functions, and also on sums and products of functions. Then, we use this analysis to obtain insights related to the decomposition of negabent functions in Section III. Further, in Section IV, negabent functions, symmetric with respect to two variables, are studied. Our technique renders a simple proof of the main result of [21], namely that all symmetric negabent functions must be affine. Moreover, a characterization of some bent–negabent functions in the Maiorana–McFarland (MM) class is obtained in Section V, thus complementing some results of [23]. In Theorem 17, we present another method of constructing bent–negabent functions on $2n$ variables for each algebraic degree from 2 to $\frac{n}{2}$, where $n \equiv 0 \pmod 2$.

In [23, Th. 10], it is proved that if f is an MM-type bent function on n variables (n even) which is also negabent then the algebraic degree of f is at most $\frac{n}{2} - 1$. Example 6 in [23] describes a technique to construct bent–negabent functions on n variables of algebraic degree ranging from 2 to $\frac{n}{4}$. Moreover, there is no known general construction of bent–negabent functions of algebraic degree greater than $\frac{n}{4}$, for all $n \equiv 0 \pmod 4$.

In Section VI, we describe a technique of constructing bent–negabent functions by using complete mapping polynomials on finite fields that constitute a special class of permutation polynomials [11], [14]. First, we demonstrate

Manuscript received March 09, 2011; accepted December 20, 2011. Date of publication February 03, 2012; date of current version May 15, 2012. This is a substantially revised and extended version of the conference paper that appears in [24]. We obtained additional results over the conference version; in particular, Section VI is completely new.

P. Stănică is with the Department of Applied Mathematics, Naval Postgraduate School, Monterey, CA 93943–5216 USA (e-mail: pstanica@nps.edu).

S. Gangopadhyay, A. Chaturvedi, and A. K. Gangopadhyay are with the Department of Mathematics, Indian Institute of Technology Roorkee, Roorkee 247667, India (e-mail: gsugata@gmail.com; ankitac17@gmail.com; ganguli.aditi@gmail.com).

S. Maitra is with the Applied Statistics Unit, Indian Statistical Institute, Kolkata 700108, India (e-mail: subho@isical.ac.in).

Communicated by M. G. Parker, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2012.2186785

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2012		**00-00-2012 to 00-00-2012**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Investigations on Bent and Negabent Functions via the Nega-Hadamard Transform	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval Postgraduate School (NPS),Department of Applied Mathematics,Monterey,CA,93943**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Parker et al. considered a new type of discrete Fourier transform, called nega-Hadamard transform.We prove several results regarding its behavior on combinations of Boolean functions and use this theory to derive several results on negabentness (that is, flat nega-spectrum) of concatenations, and partially symmetric functions. We derive the upper bound for the algebraic degree of a negabent function on variables. Further, a characterization of bent?negabent functions is obtained within a subclass of theMaiorana?McFarland set.We develop a technique to construct bent?negabent Boolean functions by using completemapping polynomials. Using this technique, we demonstrate that for each there exist bent?negabent functions on variables with algebraic degree . It is also demonstrated that there exist bent?negabent functions on eight variables with algebraic degrees 2, 3, and 4. Simple proofs of several previously known facts are obtained as immediate consequences of our work.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**9**	

the connection between existence of complete mapping polynomials over a finite field and the existence of a class of bent–negabent functions. Then, we demonstrate that for each $\ell \geq 2$, there exist bent–negabent functions on $n = 12\ell$ variables with algebraic degree $\frac{n}{4} + 1 = 3\ell + 1$.

A. Definitions and Notations

The set of integers, real numbers, and complex numbers are denoted by $\mathbb{Z}$, $\mathbb{R}$, and $\mathbb{C}$, respectively. The set of all Boolean functions on n variables is denoted by $\mathcal{B}_n$. Addition over $\mathbb{Z}$, $\mathbb{R}$, and $\mathbb{C}$ is denoted by "+," while 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 $\mathbf{x} \cdot \mathbf{y}$ and, the intersection $\mathbf{x} * \mathbf{y}$ 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 a 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

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

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 degrees 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

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

Similarly, the *Fourier transform* of $f \in \mathcal{B}_n$ at any point $\mathbf{u} \in \mathbb{F}_2^n$ is defined by

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

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 [19] more than 30 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 Dillon [8], Dobbertin [9], Rothaus [19], and later by Carlet [2].

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. Taking $f = g$ above, we get the *autocorrelation* $\mathcal{C}_f(\mathbf{u})$ of $f \in \mathcal{B}_n$ at $\mathbf{u} \in \mathbb{F}_2^n$. It is known [6] that a function $f \in \mathcal{B}_n$ is bent if and only if $\mathcal{C}_f(\mathbf{u}) = 0$ for all $\mathbf{u} \neq \mathbf{0}$.

For a detailed study of Boolean functions, we refer to [3], [4], and [6].

The *nega-Hadamard transform* of $f \in \mathcal{B}_n$ 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 f on $\mathbb{F}_2^n$ 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 $\mathbf{z}$. 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 [16] is

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

However, the difference between the aforementioned two definitions is not critical and both definitions can be used.

A Boolean function is said to be symmetric if inputs of the same weight produce the same output, i.e., $f(\mathbf{x}) = f(\sigma(\mathbf{x}))$, for any permutation σ.

The group of all invertible $n \times n$ matrices over $\mathbb{F}_2$ is denoted by $GL(n, \mathbb{F}_2)$. Two Boolean functions $f, g \in \mathcal{B}_n$ are said to be equivalent if there exist $A \in GL(n, \mathbb{F}_2)$, $\mathbf{b}, \mathbf{u} \in \mathbb{F}_2^n$ and $\epsilon \in \mathbb{F}_2$ such that $g(\mathbf{x}) = f(\mathbf{x}A \oplus \mathbf{b}) \oplus \mathbf{u}\cdot\mathbf{x} \oplus \epsilon$ for all $\mathbf{x} \in \mathbb{F}_2^n$. If $\mathbf{u} = \mathbf{0}$ and $\epsilon = 0$, then f and g are said to be affine equivalent.

B. Quadratic Boolean Functions

The properties of quadratic Boolean functions, that is Boolean functions having algebraic degree 2, can be found in [15, ch. 15]. If f is a quadratic Boolean function on n variables, the associated symplectic form of f is a map $\Psi : \mathbb{F}_2^n \times \mathbb{F}_2^n \to \mathbb{F}_2$ defined by

$$\Psi(\mathbf{u}, \mathbf{v}) = f(\mathbf{0}) \oplus f(\mathbf{u}) \oplus f(\mathbf{v}) \oplus f(\mathbf{u} \oplus \mathbf{v}).$$

The kernel $\mathcal{E}_f$ of Ψ is defined as

$$\mathcal{E}_f = \{\mathbf{u} \in \mathbb{F}_2^n : \text{ for all } \mathbf{v} \in \mathbb{F}_2^n \text{ such that } \Psi(\mathbf{u}, \mathbf{v}) = 0\}.$$

The set $\mathcal{E}_f$ is a subspace of $\mathbb{F}_2^n$ with dimension $n - 2h$ where $2h$ is the rank of Ψ. It is known that two quadratic functions f and g are equivalent if and only if $dim(\mathcal{E}_f) = dim(\mathcal{E}_g)$[15, ch. 15, Th. 4]. We recall the following result [1, Prop. A1].

Proposition 1: An element $\mathbf{a} \in \mathcal{E}_f$ if and only if the function $D_{\mathbf{a}}f$, defined as $D_{\mathbf{a}}f(\mathbf{x}) = f(\mathbf{x}) \oplus f(\mathbf{x} \oplus \mathbf{a})$ for all $\mathbf{x} \in \mathbb{F}_2^n$, is constant. The subspace $\mathcal{E}_f$ is said to be the linear kernel of f.

Since the autocorrelation spectrum of any bent function is zero at all points except at $\mathbf{u} = 0$, the linear kernel of any quadratic bent function is of dimension 0. Therefore, by [15,

ch. 15, Th. 4] and Proposition 1, all quadratic bent function are equivalent to each other.

Suppose $n = 2p$, $\pi : \mathbb{F}_2^p \to \mathbb{F}_2^p$ is a permutation and $g : \mathbb{F}_2^p \to \mathbb{F}_2$ is any Boolean function. Rothaus proved that a Boolean function $f : \mathbb{F}_2^p \times \mathbb{F}_2^p \to \mathbb{F}_2$ defined by

$$f(\mathbf{x}, \mathbf{y}) = \pi(\mathbf{x}) \cdot \mathbf{y} \oplus g(\mathbf{x}) \quad \text{for all } (\mathbf{x}, \mathbf{y}) \in \mathbb{F}_2^p \times \mathbb{F}_2^p$$

is a bent function. The collection of bent functions of this type is called the MM class. If π is the identity permutation and $g(\mathbf{x}) = 0$ for all $\mathbf{x} \in \mathbb{F}_2^p$, then the function $h(\mathbf{x}, \mathbf{y}) = \mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^{p} x_i y_i$ for all $(\mathbf{x}, \mathbf{y}) \in \mathbb{F}_2^p \times \mathbb{F}_2^p$ is a quadratic bent function. Thus, any quadratic bent function of n variables is equivalent to h, which can be written as $h(\mathbf{x}) = \sum_{i=1}^{p} x_i x_{p+i}$ (by labeling $x_{p+i} = y_i$). From the previous discussions, it is clear that if $f \in \mathcal{B}_n$ is a quadratic bent function, then there exist $A \in GL(n, \mathbb{F}_2)$, $\mathbf{b}, \mathbf{u} \in \mathbb{F}_2^n$, and $\epsilon \in \mathbb{F}_2$ such that $h(\mathbf{x}) = f(\mathbf{x}A \oplus \mathbf{b}) \oplus \mathbf{u} \cdot \mathbf{x} \oplus \epsilon$.

II. Properties of the Nega-Hadamard Transform

It is well known that the inverse of the Walsh–Hadamard transform $\mathcal{H}_f(\lambda)$ of $f \in \mathcal{B}_n$ is given by

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

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 the nega-Hadamard transformation of a function $f \in \mathcal{B}_n$ in [16] and [18] is the following.

Lemma 2: 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 [15])

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

Theorem 3: Let f, g, h be in $\mathcal{B}_n$. The following statements are true.

(a) For any affine function $\ell_{\mathbf{a},c}(\mathbf{x}) = \mathbf{a} \cdot \mathbf{x} \oplus c$ and $f \in \mathcal{B}_n$, $\mathcal{N}_{f \oplus \ell_{\mathbf{a},c}}(\mathbf{u}) = (-1)^c \mathcal{N}_f(\mathbf{a} \oplus \mathbf{u})$.
Further, $\mathcal{N}_{\ell_{\mathbf{a},c}}(\mathbf{u}) = (-1)^c \omega^n \imath^{-wt(\mathbf{a} \oplus \mathbf{u})}$. In particular, $\mathcal{N}_{\mathbf{0}}(\mathbf{u}) = -\mathcal{N}_{\mathbf{1}}(\mathbf{u}) = \omega^n \imath^{-wt(\mathbf{u})}$, 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 $\omega = \frac{1+\imath}{\sqrt{2}}$ is an eighth primitive root of 1.

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

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

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

(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, $A^T A = I_n$).

(e) If $f \in \mathcal{B}_n, g \in \mathcal{B}_k$, and $h(\mathbf{x}, \mathbf{y}) = f(\mathbf{x}) g(\mathbf{y})$, then $2^{\frac{k}{2}} \mathcal{N}_h(\mathbf{u}, \mathbf{v}) = \mathcal{N}_f(\mathbf{u}) A_{g1}(\mathbf{v}) + \omega^n \imath^{-wt(\mathbf{u})} A_{g0}(\mathbf{v})$, $A_{g1}(\mathbf{v}) + A_{g0}(\mathbf{v}) = 2^{\frac{k}{2}} \omega^k \imath^{-wt(\mathbf{v})}$, 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 $k = 1$, $2^{\frac{1}{2}} \mathcal{N}_{yf(\mathbf{x})}(\mathbf{u}, v) = (-1)^v \imath \mathcal{N}_f(\mathbf{u}) + \omega^n \imath^{-wt(\mathbf{u})}$, $2^{\frac{1}{2}} \mathcal{N}_{(y \oplus 1) f(\mathbf{x})}(\mathbf{u}, v) = \mathcal{N}_f(\mathbf{u}) + \omega^n (-1)^v \imath^{-wt(\mathbf{u})+1}$.

Proof: The first part of (a) is direct from the definition of the nega-Hadamard transform. The second part of the claim (a) can be derived from [23, Lemma 1], since $\mathcal{N}_{\mathbf{0}}(\mathbf{u}) = -\mathcal{N}_{\mathbf{1}}(\mathbf{u}) = 2^{-\frac{n}{2}} \sum_{\mathbf{y}} (-1)^{\mathbf{u} \cdot \mathbf{y}} \imath^{wt(\mathbf{y})} = \omega^n \imath^{-wt(\mathbf{u})}$.

We show the first identity of (b) (the second follows by symmetry). Since

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

and (see [6, 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 (sums are over $\mathbb{F}_2^n$)

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

Item (c) is straightforward. The property (d) can be derived from [16, Lemma 2] and [23, Th. 2]. It is to be noted that [23, Th. 2] further proves that the action of the orthogonal group preserves the bent–negabentness property of a Boolean function.

To show item (e), we write, $2^{\frac{n+k}{2}} \mathcal{N}_h(\mathbf{u}, \mathbf{v})$

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

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

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

■

The next result is analogous to the result on the crosscorrelation of two Boolean functions [20]. In the nega-Hadamard transform context, the basic idea of this result is explained in [7] and [17, eq. (15)].

Lemma 4: If $f,g\in\mathcal{B}_n$, then the nega-crosscorrelation equals

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

Proof: We start with the sum at the right hand side.

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

■

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

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

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

Corollary 5 (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 6: 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 (4). ■

An equivalent result is proved after [17, eq. (15)] and in [16, Th. 2] for the negaperiodic autocorrelation.

Remark 7: Lemma 6 provides an alternate 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 other proofs, we refer to [23, Lemma 1] and [16, Prop. 1]. A bound on the algebraic degrees of negabent functions is an important question. In the following, we provide such a bound.

A Boolean function $f\in\mathcal{B}_n$ is said to be *near-bent* [12] if its Fourier transform values belong to $\{0,\pm 2^{\frac{n+1}{2}}\}$. It is rather immediate that near-bent functions exist only for odd values of n. It is known [3] that if f is an n variable Boolean function ($n\geq 2$) and $1\leq k\leq n$ such that the Fourier transform values of f are divisible by 2^k, then f has algebraic degree at most $n-k+1$. In case f is near-bent, $k=\frac{n+1}{2}$ which implies that the algebraic degree of f is at most $\frac{n+1}{2}$.

The following theorem (which will be also used later) proved by Parker and Pott establishes a connection between bent and negabent functions.

Theorem 8 (see [16, Th. 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 $s_2(x_1,x_2,\ldots,x_{2m})=\sum_{i<j}x_ix_j$ is the elementary symmetric function of degree 2.

Theorem 9: The algebraic degree of a negabent function $f\in\mathcal{B}_n$ is at most $\lceil\frac{n}{2}\rceil$, for any integer n.

Proof: Suppose n is even and f is negabent. Then $f\oplus s_2$ is bent, and so, its algebraic degree is bounded above by $\frac{n}{2}$, therefore the algebraic degree of f is at most $\frac{n}{2}$.

Suppose n is odd and $f\in\mathcal{B}_n$ is a negabent function. Then, by [16, Remark 1], the Walsh–Hadamard transform values of $f\oplus s_2$ belong to $\{0,\pm 2^{\frac{n+1}{2}}\}$, in other words $f\oplus s_2$ is a near-bent function. Therefore, the algebraic degree of f is at most $\frac{n+1}{2}$. ■

III. Decomposition of Negabent Functions With Respect to Codimension One Subspaces

Suppose $1\leq r\leq n$. Then, any function $f\in\mathcal{B}_n$ can be thought of as a function from $\mathbb{F}_2^r\times\mathbb{F}_2^{n-r}$ to $\mathbb{F}_2$. 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 10: Let $f\in\mathcal{B}_n$ be 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, $C_f(\mathbf{u},\mathbf{w})$

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

■

Corollary 11: 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

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

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 12: Two functions $f, g \in \mathcal{B}_n$ have complementary nega-autocorrelations if and only if

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

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

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

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, $C_f(\mathbf{z}) + C_g(\mathbf{z})$

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

where

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

Thus, the functions f and g have complementary nega-autocorrelations. ∎

Theorem 13: Suppose $h \in \mathcal{B}_{n+1}$ is expressed as

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

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 $C_{f,g}(\mathbf{u}) = 0$ 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 11, 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, 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 11, $C_h(\mathbf{u}, a) = 0$ 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

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

Thus

$$\mathcal{N}_h(\mathbf{u}, a) = \begin{cases} \frac{1}{\sqrt{2}} \mathcal{N}_f(\mathbf{u}) + \frac{\imath}{\sqrt{2}} \mathcal{N}_g(\mathbf{u}), & \text{if } a = 0 \\ \frac{1}{\sqrt{2}} \mathcal{N}_f(\mathbf{u}) - \frac{\imath}{\sqrt{2}} \mathcal{N}_g(\mathbf{u}), & \text{if } a = 1. \end{cases} \tag{7}$$

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

$$\left| \frac{1}{\sqrt{2}} \mathcal{N}_f(\mathbf{u}) + \frac{\imath}{\sqrt{2}} \mathcal{N}_g(\mathbf{u}) \right| = 1$$
$$\left| \frac{1}{\sqrt{2}} \mathcal{N}_f(\mathbf{u}) - \frac{\imath}{\sqrt{2}} \mathcal{N}_g(\mathbf{u}) \right| = 1. \tag{8}$$

If h is negabent, then by Lemma 12 and the equivalence of the first two statements proved above, we obtain

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

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 (8), we obtain

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

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., $\frac{\mathcal{N}_f(\mathbf{u})}{\mathcal{N}_g(\mathbf{u})} = \overline{\frac{\mathcal{N}_f(\mathbf{u})}{\mathcal{N}_g(\mathbf{u})}} = \left(\frac{\mathcal{N}_f(\mathbf{u})}{\mathcal{N}_g(\mathbf{u})}\right)$. 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 aforementioned condition, $|\mathcal{N}_g(\mathbf{u})| = \sqrt{2}$. By (7), $|\mathcal{N}_h(\mathbf{u}, a)| = 1$ 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

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

Thus, h is negabent. ■

IV. 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

$$h(\mathbf{x}, y, z) = f(\mathbf{x}) \oplus (f(\mathbf{x}) \oplus g(\mathbf{x}))(y \oplus z) \oplus s(\mathbf{x})yz \tag{10}$$

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 [3], [4], [6], and [26]). For negabent functions we prove the following similar result.

Theorem 14: 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

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

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 is of the form $h(\mathbf{x}, y, z) = f(\mathbf{x}) \oplus (f(\mathbf{x}) \oplus g(\mathbf{x}))(y \oplus z)$, 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

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

where $(\mathbf{x}, y, z)$ varies over $\mathbb{F}_2^{n-2} \times \mathbb{F}_2 \times \mathbb{F}_2$. Expanding the above sum by substituting all possible values of $(y, z) \in \mathbb{F}_2 \times \mathbb{F}_2$, we obtain

$$\mathcal{N}_h(\mathbf{u}, a, b) = \frac{1 - (-1)^{a\oplus b}}{2}\mathcal{N}_f(\mathbf{u}) + \imath\frac{(-1)^a + (-1)^b}{2}\mathcal{N}_g(\mathbf{u}). \tag{11}$$

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, and $s(\mathbf{x}) = 0$ for all $\mathbf{x} \in \mathbb{F}_2^{n-2}$, then h is also negabent. This shows the converse. ■

Corollary 15: 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 15 gives an alternate proof of the fact proved in [21]. In fact, the case for even n can be immediately obtained from Theorem 8.

Recall that $s_2(x_1, x_2, \ldots, x_{2m}) = \sum_{i<j} x_ix_j$ is the homogeneous (i.e., 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. In [22], 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 [21], it is proved (by a long argument) that all the symmetric negabent functions are affine. Following [16] and [22], the result in [21] can be achieved in a few lines for even n.

Theorem 16: 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 [22]). 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 [23]. Therefore, symmetric functions on even number of variables, if affine, are negabent. ■

Bent functions do not exist for an odd number of input variables. Thus, there is no equivalent characterization of Theorem 8 for odd dimension, and the result in [21] cannot be proved trivially as before. However, the odd (as well as the even) case has already been taken care of by Corollary 15.

V. Bent–Negabent Functions in MM Class

In this section we shall investigate bent functions which are also negabent in the MM class of bent functions, namely

$$f(\mathbf{x},\mathbf{y}) = \pi(\mathbf{x})\cdot\mathbf{y} \oplus g(\mathbf{x}), \quad \mathbf{x},\mathbf{y}\in\mathbb{F}_2^n \tag{12}$$

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 ($A^TA = I_n$), 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 $wt(A\mathbf{z}) = (A\mathbf{z})^T\cdot(A\mathbf{z}) = \mathbf{z}^T(A^TA)\mathbf{z} = wt(\mathbf{z})$). It could be interesting to see if there are such weight-sum invariant permutations outside of the ones generated by the linear orthogonal group.

Theorem 17: A function in (12) on $\mathbb{F}_2^{2n}$ is bent–negabent if and only if g is bent.

Proof: We evaluate $\mathcal{N}_f(\mathbf{u},\mathbf{v})$

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

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

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

which implies that $\mathcal{N}_f(\mathbf{u},\mathbf{v})$

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

Consequently

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

that proves 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 [23, Th. 10] gives an upper bound of $n-1$ on the degree of an MM-type bent–negabent function on $2n$ variables, but not an existence result.

Corollary 18: If f as in (12) is bent–negabent with π weight-sum invariant, then the degree of f is bounded by $\frac{n}{2}$. Moreover, there exist bent–negabent functions in the MM class of any degree between 2 and $\frac{n}{2}$ (n is even).

VI. Construction of a New Class of Bent–Negabent Boolean Functions

It is well known that the maximum degree of a bent function on n variables is $\frac{n}{2}$ and the maximum degree of a negabent function is $\lceil\frac{n}{2}\rceil$ (Theorem 9), which is $\frac{n}{2}$ for even n. Thus, it may be an interesting problem to find out a nontrivial upper bound on the algebraic degrees of the bent–negabent functions. However, no upper bound strictly less than $\frac{n}{2}$ is known to this date. Parker and Pott also raised this question in [16, Problem 3, p. 19].

So far all the known general constructions of bent–negabent functions on n variables produce functions with algebraic degrees less than or equal to $\frac{n}{4}$, where n is any positive integer divisible by 4. In this section, we construct bent–negabent functions on $n = 12\ell$ variables with algebraic degree equal to $\frac{n}{4}+1$, where ℓ is any positive integer greater than or equal to 2.

Throughout this section, $n = 2p$ and h is a quadratic bent function defined as $h(\mathbf{x}) = \sum_{i=1}^{p} x_ix_{p+i}$ for all $\mathbf{x} = (x_1,\ldots,x_n)\in\mathbb{F}_2^n$. It is known that the quadratic symmetric Boolean function of the form $s_2(\mathbf{x}) = \sum_{i<j} x_ix_j$, for all $\mathbf{x} = (x_1,\ldots,x_n)\in\mathbb{F}_2^n$ is bent. Therefore, by the results of Section I-B, the function s_2 is equivalent to the quadratic bent function h defined previously. Using Theorem 8, proved by Parker and Pott, we obtain the following.

Lemma 19: A Boolean function $f\in\mathcal{B}_n$ ($n = 2p$) is bent–negabent if and only if both f and $f\oplus s_2$ are bent functions.

Proof: Assume that $f\in\mathcal{B}_{2p}$ is a bent–negabent function. Since f is a negabent function, $f\oplus s_2$ is a bent function. Thus, f and $f\oplus s_2$ both are bent functions.

Conversely let us suppose that f and $f\oplus s_2$ both are bent functions. Since $f\oplus s_2$ is a bent function $f\oplus s_2\oplus s_2 = f$ is a negabent function. Therefore, f is a bent–negabent function. ■

The following theorem provides a strategy to construct bent–negabent functions.

Theorem 20: Let $s_2(\mathbf{x}) = h(\mathbf{x}A\oplus\mathbf{b})\oplus\mathbf{u}\cdot\mathbf{x}\oplus\epsilon$ for all $\mathbf{x}\in\mathbb{F}_2^n$, where $A\in GL(n,\mathbb{F}_2)$, $\mathbf{b},\mathbf{u}\in\mathbb{F}_2^n$ and $\epsilon\in\mathbb{F}_2$. Suppose $f\in\mathcal{B}_n$ is a bent function such that $f\oplus h$ is also a bent function. Then, $g\in\mathcal{B}_n$ defined by

$$g(\mathbf{x}) = f(\mathbf{x}A\oplus\mathbf{b})\oplus h(\mathbf{x}A\oplus\mathbf{b})\oplus\mathbf{u}\cdot\mathbf{x}\oplus\epsilon = f(\mathbf{x}A\oplus\mathbf{b})\oplus s_2(\mathbf{x})$$

for all $x\in\mathbb{F}_2^n$ is a bent–negabent function.

Proof: The function g is equivalent to $f\oplus h$. Therefore, g is bent. The function $g\oplus s_2$ is affine equivalent to f. Since f is a bent function, $g\oplus s_2$ is also a bent function. Therefore, by Lemma 19, g is a bent–negabent function. ■

Remark 21: Since all quadratic bent functions are equivalent (see Section I-B), if h_1 is any quadratic bent function on n variables, then there exist $A\in GL(n,\mathbb{F}_2)$, $\mathbf{b},\mathbf{u}\in\mathbb{F}_2^n$ and $\epsilon\in\mathbb{F}_2$, such that $s_2(\mathbf{x}) = h_1(\mathbf{x}A\oplus\mathbf{b})\oplus\mathbf{u}\cdot\mathbf{x}\oplus\epsilon$ for all $\mathbf{x}\in\mathbb{F}_2^n$.

Therefore, if $f \in \mathcal{B}_n$ is a bent function and $h_1 \in \mathcal{B}_n$ is any quadratic bent function such that $f + h_1$ is also a bent function, then by using the strategy described in Theorem 20 we obtain a bent–negabent function.

Theorem 20 reduces the problem of constructing bent–negabent functions to characterizing bent functions f such that $f + h$ is also a bent function. We demonstrate below that such functions can be constructed by using complete mapping polynomials.

A. Complete Mapping Polynomials

Let $\mathbb{F}_{2^p}$ be the field extension of $\mathbb{F}_2$ of degree p. The finite field $\mathbb{F}_{2^p}$ is isomorphic to $\mathbb{F}_2^p$ as a vector space over $\mathbb{F}_2$. Any permutation of $\mathbb{F}_{2^p}$ can be identified with a permutation on $\mathbb{F}_2^p$. Any permutation on $\mathbb{F}_{2^p}$ can be represented by a polynomial in $\mathbb{F}_{2^p}[X]$ of degree at most $2^p - 2$. A polynomial $F(X) \in \mathbb{F}_{2^p}[X]$ is said to be a complete mapping polynomial if $F(X)$ and $F(X) + X$ both correspond to permutations on $\mathbb{F}_{2^p}$. For details on complete mapping polynomials, we refer to [11] and [14]. The following provides us a strategy to construct bent–negabent functions by using complete mapping polynomials.

Theorem 22: Let $n = 2p$. Suppose π_F denotes the permutation on $\mathbb{F}_2^p$ induced by a complete mapping polynomial $F(X) \in \mathbb{F}_{2^p}[X]$. Let $f_F \in \mathcal{B}_n$ be defined by $f_F(\mathbf{x}) = \pi_F(x_1, \ldots, x_p) \cdot (x_{p+1}, \ldots, x_n)$ for all $\mathbf{x} \in \mathbb{F}_2^n$, and h is a quadratic bent function defined as $h(\mathbf{x}) = \sum_{i=1}^{p} x_i x_{p+i}$ for all $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$, such that $s_2(\mathbf{x}) = h(\mathbf{x}A \oplus \mathbf{b}) \oplus \mathbf{u} \cdot \mathbf{x} \oplus \epsilon$ for all $\mathbf{x} \in \mathbb{F}_2^n$, where $A \in GL(n, \mathbb{F}_2)$, $\mathbf{b}, \mathbf{u} \in \mathbb{F}_2^n$ and $\epsilon \in \mathbb{F}_2$. Then, the Boolean function $f_F \oplus h$ is an MM-type bent function and

$$\begin{aligned} g(\mathbf{x}) &= f_F(\mathbf{x}A \oplus \mathbf{b}) \oplus h(\mathbf{x}A \oplus \mathbf{b}) \oplus \mathbf{u} \cdot \mathbf{x} \oplus \epsilon \\ &= f_F(\mathbf{x}A \oplus \mathbf{b}) \oplus s_2(\mathbf{x}) \quad \text{for all } \mathbf{x} \in \mathbb{F}_2^n \end{aligned}$$

is a bent–negabent function. The algebraic degrees of g and f_F are equal.

Proof: Since π_F is a permutation on $\mathbb{F}_2^p$, the function f_F is a bent function on $n = 2p$ variables belonging to the MM class. The function

$$\begin{aligned} (f_F \oplus h)(\mathbf{x}) &= f_F(\mathbf{x}) \oplus h(\mathbf{x}) \\ &= \pi_F(x_1, \ldots, x_p) \cdot (x_{p+1}, \ldots, x_n) \\ &\quad \oplus (x_1, \ldots, x_p) \cdot (x_{p+1}, \ldots, x_n) \\ &= (\pi_F(x_1, \ldots, x_p) \\ &\quad \oplus (x_1, \ldots, x_p)) \cdot (x_{p+1}, \ldots, x_n) \end{aligned}$$

is also a bent function in the MM class since π_F is induced from a complete mapping polynomial. Thus, using Theorem 20, we infer that g is a bent–negabent function. ■

B. Bent–Negabent Functions on n Variables With Algebraic Degree Greater Than $\frac{n}{4}$

We consider a particular complete mapping polynomial constructed by Laigle-Chapuy [11].

Theorem 23 ([11, Th. 4.3]): Let p be a prime and $(m, \ell) \in \mathbb{N}^2$. Let k be the order of p in $\mathbb{Z}/m\mathbb{Z}$. Take $q = p^{k\ell m}$ and r a positive integer coprime to $q - 1$. Assume $a \in \mathbb{F}_{p^{k\ell}}$ is such that $(-a)^m \neq 1$. Then, the polynomials

$$P(X) = X(X^{\frac{q-1}{m}} + a) \text{ and } Q(X) = aX^{\frac{q-1}{m}+1}$$

are complete mapping polynomials.

First, we construct a bent–negabent function on 24 variables having algebraic degree 7.

Example 24: Following the notations of Theorem 23, let $p = 2$, $\ell = 2$, and $m = 3$. The order of p in $\mathbb{Z}/3\mathbb{Z}$ is 2, that is $k = 2$. Thus, $k\ell m = (2)(2)(3) = 12$ and $q = p^{k\ell m} = 2^{12}$. Consider the polynomial $P(X) = X(X^{\frac{q-1}{m}} + a) = X(X^{1365} + a)$, where $a \in \mathbb{F}_{2^4} \setminus \mathbb{F}_{2^2}$. The last condition guarantees $(-a)^m = (-a)^3 \neq 1$. By using $P(X)$ in Theorem 22, we obtain a bent–negabent function on 24 variables and algebraic degree 7. The algebraic degrees of the bent–negabent functions constructed in [23] are bounded above by $\frac{n}{4}$. Thus, the bent–negabent function constructed above does not belong to these classes.

Certainly, the order of $p = 2$ in $\mathbb{Z}/3\mathbb{Z}$ is $k = 2$, so in general we have the following result.

Lemma 25: For any $\ell \geq 2$, the polynomials

$$P(X) = X(X^{\frac{2^{6\ell}-1}{3}} + a) \text{ and } Q(X) = aX^{\frac{2^{6\ell}-1}{3}+1}$$

have algebraic degree 3ℓ.

Proof: Let $t = \frac{2^{6\ell}-1}{3} + 1$. Then

$$\begin{aligned} t &= \frac{2^{6\ell} - 1}{3} + 1 \\ &= \frac{(2^2 - 1)((2^2)^{3\ell-1} + (2^2)^{3\ell-2} + \cdots + (2^2) + 1)}{(2^2 - 1)} + 1 \\ &= \underbrace{2^{6\ell-2} + 2^{6\ell-4} + 2^{6\ell-6} + \cdots + 2^4 + 2^2 + 2}_{3\ell \text{ terms}}. \end{aligned}$$

This proves that both $P(X)$ and $Q(X)$ have degree 3ℓ. ■

Theorem 26: For each $\ell \geq 2$, there exist bent–negabent functions on $n = 12\ell$ variables with algebraic degree $\frac{n}{4} + 1 = 3\ell + 1$.

Proof: For each $\ell \geq 2$, it is possible to construct $P(X)$ and $Q(X)$ as in Lemma 25 with $p = 2$ and $m = 3$. It is proved in Lemma 25 that $P(X)$ and $Q(X)$ both have algebraic degree 3ℓ. It is also to be noted that if $\ell \geq 2$, we can choose $a \in \mathbb{F}_{2^{2\ell}} \setminus \mathbb{F}_2$ so that $(-a)^m \neq 1$. Therefore, $P(X)$ and $Q(X)$ constructed in this way are complete mapping polynomials. If we use Theorem 22 by inducing the permutation π_F where $F(X) \in \{P(X), Q(X)\}$, then we obtain bent–negabent functions on $n = (2)(6\ell) = 12\ell$ variables with algebraic degree $3\ell + 1$. It is also to be noted that these functions may not be of MM type but belong to the complete class of MM-type functions. ■

Complete mapping polynomials over $\mathbb{F}_{2^4}$ of algebraic degrees 1, 2, and 3, listed in Table I, are obtained by Yuan *et al.* [25]. In Table I, α denotes a primitive element of $\mathbb{F}_{2^4}$. Using these polynomials and Theorem 22 we can construct bent–negabent functions on eight variables having algebraic degrees 2, 3, and 4. Thus, we note that there exist bent–negabent functions on eight variables with maximum possible algebraic degree that

TABLE I
COMPLETE MAPPING POLYNOMIALS OVER $\mathbb{F}_{2^4}$

Algebraic degree	Complete mapping polynomial
1	$a(x^4+bx)$ where $ab \neq 0$, and $b, b+a^{-1} \neq \alpha^3, \alpha^6, \alpha^9, \alpha^{12}$
2	$\alpha^4 x^{10} + \alpha^{13} x^9 + \alpha^2 x^8 + \alpha^7 x^3 + \alpha^4 x$
3	$\alpha^{14} x^{13} + \alpha^8 x^{10} + \alpha^7 x^7 + \alpha^8 x$

is 4. It is not known whether such is the case for $n > 4$. This leads us to state the following as an open problem.

Open Problem: For any $n \equiv 0 \pmod 4$, give a general construction of bent-negabent Boolean functions on n variables with algebraic degree strictly greater than $\frac{n}{4}+1$.

VII. CONCLUSION

In this paper, we have investigated the nega-Hadamard transform of Boolean functions in detail. First, we study the properties of nega-Hadamard transform. Next, we concentrate on decompositions of negabent functions with respect to codimension one subspaces, and negabent functions that are symmetric about two variables. A characterization of some bent–negabent functions in the MM class allows us to construct bent–negabent Boolean functions on $\mathbb{F}_2^{2n}$ of all degrees up to $\lfloor \frac{n}{2} \rfloor$. Use of complete mapping polynomials allows us to further construct new classes of bent–negabent functions on $2n$ variables of degree greater than $\frac{n}{2}$.

ACKNOWLEDGMENT

The authors gratefully thank the anonymous reviewers and the associate editor for the detailed and excellent comments, that significantly improved the editorial as well as technical quality of the paper.

REFERENCES

[1] A. Canteaut, C. Carlet, P. Charpin, and C. Fontaine, "On cryptographic properties of the cosets of $R(1, m)$," *IEEE Trans. Inf. Theory*, vol. 47, no. 4, pp. 1494–1513, May 2001.
[2] C. Carlet, "Two new classes of bent functions," in *Proc. Workshop theory Appl. cryptographic Tech. Adv. Cryptology*, 1994, vol. LNCS-765, pp. 77–101.
[3] C. Carlet, "Boolean functions for cryptography and error correcting codes," in *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, Y. Crama and P. L. Hammer, Eds. Cambridge, U.K.: Cambridge Univ. Press, 2010, pp. 257–397.
[4] C. Carlet, "Vectorial Boolean functions for cryptography," in *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, Y. Crama and P. L. Hammer, Eds. Cambridge, U.K.: Cambridge Univ. Press, 2010, pp. 398–469.
[5] C. Carlet, P. Charpin, and V. Zinoviev, "Codes, bent functions and permutations suitable for DES-like cryptosystems," *Designs, Codes Cryptography*, vol. 15, pp. 125–156, 1998.
[6] T. W. Cusick and P. Stănică, *Cryptographic Boolean functions and Applications*. New York: Academic, 2009.
[7] L. E. Danielsen, T. A. Gulliver, and M. G. Parker, "Aperiodic propagation criteria for Boolean functions," *Inf. Comput.*, vol. 204, no. 5, pp. 741–770, 2006.
[8] J. F. Dillon, "Elementary Hadamard difference sets," in *Proc. 6th S. E. Conf. Combinator., Graph Theory, Comput., Util. Math.*, Winnipeg, MB, Canada, 1975, pp. 237–249.
[9] H. Dobbertin, "Construction of bent functions and balanced Boolean functions with high nonlinearity," in *Fast Software Encryption (Workshop on Cryptographic Algorithms)*. New York: Springer-Verlag, 1995, vol. LNCS-1008, pp. 61–74.
[10] H. Dobbertin and G. Leander, "Bent functions embedded into the recursive framework of $\mathbb{Z}$-bent functions," *Designs, Codes Cryptography*, vol. 49, pp. 3–22, 2008.
[11] Y. Laigle–Chapuy, "Permutation polynomials and applications to coding theory," *Finite Fields Appl.*, vol. 13, pp. 58–70, 2007.
[12] G. Leander and G. McGuire, "Construction of bent functions from near-bent functions," *J. Combinat. Theory, Series A*, vol. 116, pp. 960–970, 2009.
[13] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*. Cambridge, U.K.: Cambridge Univ. Press, 1983.
[14] H. Niederreiter and K. H. Robinson, "Complete mappings of finite fields," *J. Austral. Math. Soc. (Series A)*, vol. 33, pp. 197–212, 1982.
[15] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error–Correcting Codes*. Amsterdam, The Netherlands: North Holland, 1977.
[16] M. G. Parker and A. Pott, "On Boolean functions which are bent and negabent," in *Proc. Int. Conf. Sequences, Subsequences, Consequences*, 2007, vol. LNCS-4893, pp. 9–23.
[17] C. Riera and M. G. Parker, "One and two-variable interlace polynomials: A spectral interpretation," in *Proc. Int. Conf. Coding Cryptography*, 2006, vol. LNCS-3969, pp. 397–411.
[18] C. Riera and M. G. Parker, "Generalized bent criteria for Boolean functions," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 4142–4159, Sep. 2006.
[19] O. S. Rothaus, "On bent functions," *J. Combin. Theory Ser. A*, vol. 20, pp. 300–305, 1976.
[20] P. Sarkar and S. Maitra, "Cross–correlation analysis of cryptographically useful Boolean functions and S-Boxes," *Theory Comput. Syst.*, vol. 35, pp. 39–57, 2002.
[21] S. Sarkar, "On the symmetric negabent Boolean functions," in *Progress in Cryptology—INDOCRYPT 2009*. New York: Springer, 2009, vol. LNCS-5922, pp. 136–143.
[22] P. Savicky, "On the bent Boolean functions that are symmetric," *Eur. J. Combin.*, vol. 15, pp. 407–410, 1994.
[23] K. U. Schmidt, M. G. Parker, and A. Pott, "Negabent functions in the Maiorana–McFarland class," in *Proc. Int. Conf. Sequences Appl.*, 2008, vol. LNCS-5203, pp. 390–402.
[24] P. Stanica, S. Gangopadhyay, A. Chaturvedi, A. Kar Gangopadhyay, and S. Maitra, "Nega-Hadamard transform, bent and negabent functions," in *Proc. Int. Conf. Sequences Appl.*, 2010, vol. LNCS-6338, pp. 359–372.
[25] Y. Yuan, Y. Tong, and H. Zhan, "Complete mapping polynomials over finite field $\mathbb{F}_{16}$," in *Proc. Int. Workshop Arithmetic Finite Fields*, 2007, vol. LNCS-4547, pp. 147–158.
[26] Y. Zhao and H. Li, "On bent functions with some symmetric properties," *Discrete Appl. Math.*, vol. 154, pp. 2537–2543, 2006.

Pantelimon Stănică received his Master of Science in Mathematics degree in 1992 from University of Bucharest, Romania. He completed his Ph.D. in Mathematics at State University of New York at Buffalo in 1998. Currently, he is a Professor at the Naval Postgraduate School, in Monterey, California. His research interests are in Cryptology, Number Theory and Discrete Mathematics.

Sugata Gangopadhyay received his Master of Science in Mathematics degree in the year 1993 from the Indian Institute of Technology Kharagpur. He completed Ph.D. from the Indian Institute of Technology Kharagpur in 1998. Currently he is an Assistant Professor at Indian Institute of Technology Roorkee. His research interests are in Cryptology and Discrete Mathematics.

Ankita Chaturvedi received her Master of Science in Mathematics degree in the year 2006 from CSJM University Kanpur. Currently she is a Ph.D. student in the Indian Institute of Technology Roorkee. Her research interest is in Discrete Mathematics and Cryptology.

Aditi Kar Gangopadhyay received her Master of Science in Mathematics degree in the year 1995 from the Indian Institute of Technology Kharagpur. She completed Ph.D. from the Indian Institute of Technology Kharagpur in 2000. Currently she is an Assistant Professor at Indian Institute of Technology Roorkee. Her research interests are in Statistical Inference and Discrete Mathematics.

Subhamoy Maitra received his Bachelor of Electronics and Telecommunication Engineering degree in the year 1992 from Jadavpur University, Calcutta and Master of Technology in Computer Science in the year 1996 from Indian Statistical Institute, Calcutta. He has completed Ph.D from Indian Statistical Institute in 2001. Currently he is a Professor at Indian Statistical Institute. His research interests are in Cryptology and Security.