A note on generalized bent criteria for Boolean functions

Sugata Gangopadhyay[1], Enes Pasalic[2], Pantelimon Stănică[3]
[1] Computer Science Unit
Indian Statistical Institute, Chennai Centre
Chennai - 600113, INDIA
sugo@isichennai.res.in
[2]University of Primorska, FAMNIT
Koper, SLOVENIA
enes.pasalic6@gmail.com
[3]Department of Applied Mathematics
Naval Postgraduate School
Monterey, CA 93943–5216, USA
pstanica@nps.edu

***Abstract*—In this paper, we consider the spectra of Boolean functions with respect to the action of unitary transforms obtained by taking tensor products of the Hadamard kernel, denoted by H, and the nega–Hadamard kernel, denoted by N. The set of all such transforms is denoted by $\{H, N\}^n$. A Boolean function is said to be bent$_4$ if its spectrum with respect to at least one unitary transform in $\{H, N\}^n$ is flat. We prove that the maximum possible algebraic degree of a bent$_4$ function on n variables is $\lceil \frac{n}{2} \rceil$, and hence solve an open problem posed by Riera and Parker [cf. IEEE-IT: 52:9 (2006), 4142–4159]. We obtain a relationship between bent and bent$_4$ functions which is a generalization of the relationship between bent and negabent Boolean functions proved by Parker and Pott [cf. LNCS: 4893 (2007), 9–23].**

Keywords: Walsh–Hadamard transform, nega–Hadamard transform, bent function, bent$_4$ function, algebraic degree.

I. INTRODUCTION

Let us denote the set of integers, real numbers and complex numbers by $\mathbb{Z}$, $\mathbb{R}$ and $\mathbb{C}$, respectively and let the ring of integers modulo r be denoted by $\mathbb{Z}_r$. The vector space $\mathbb{Z}_2^n$ is the space of all n-tuples $\mathbf{x} = (x_n, \ldots, x_1)$ of elements from $\mathbb{Z}_2$ with the standard operations. By '$+$' we denote the addition over $\mathbb{Z}$, $\mathbb{R}$ and $\mathbb{C}$, whereas '$\oplus$' denotes the addition over $\mathbb{Z}_2^n$ for all $n \geq 1$. Addition modulo q is denoted by '$+$' and it is understood from the context. If $\mathbf{x} = (x_n, \ldots, x_1)$ and $\mathbf{y} = (y_n, \ldots, y_1)$ are in $\mathbb{Z}_2^n$, we define the scalar (or inner) product by $\mathbf{x}\cdot\mathbf{y} = x_n y_n \oplus \cdots \oplus x_2 y_2 \oplus x_1 y_1$. 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 $a, b \in \mathbb{R}$.

We call any function from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2$ a *Boolean function* on n variables and denote the set of all Boolean functions by $\mathcal{B}_n$. In general any function from $\mathbb{Z}_2^n$ to $\mathbb{Z}_q$ ($q \geq 2$ a positive integer) is said to be a *generalized Boolean function* on n variables [5], the set of all such functions being denoted by $\mathcal{GB}_n^q$. Clearly $\mathcal{GB}_n^2 = \mathcal{B}_n$. For any $f \in \mathcal{B}_n$, the algebraic normal form (ANF) is

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

where $\mu_{\mathbf{a}} \in \mathbb{Z}_2$, for all $\mathbf{a} \in \mathbb{Z}_2^n$. For any $\mathbf{a} \in \mathbb{Z}_2^n$, $wt(\mathbf{a}) := \sum_{i=1}^n a_i$ is the Hamming weight. The algebraic degree of f, $\deg(f) := \max\{wt(\mathbf{a}) : \mathbf{a} \in \mathbb{Z}_2^n, \mu_{\mathbf{a}} \neq 0\}$.

Now, let $q \geq 2$ be an integer, and let $\zeta = e^{2\pi\imath/q}$ be the complex q-primitive root of unity. The *Walsh–Hadamard transform* of $f \in \mathcal{GB}_n^q$ at any point $\mathbf{u} \in \mathbb{Z}_2^n$ is the complex valued function

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

The inverse of the Walsh–Hadamard transform is given by

$$\zeta^{f(\mathbf{y})} = 2^{-\frac{n}{2}} \sum_{\mathbf{u}\in\mathbb{Z}_2^n} \mathcal{H}_f(\mathbf{u})(-1)^{\mathbf{u}\cdot\mathbf{y}}. \quad (3)$$

A function $f \in \mathcal{GB}_n^q$ is a *generalized bent* function if and only if $|\mathcal{H}_f(\mathbf{u})| = 1$ for all $\mathbf{u} \in \mathbb{Z}_2^n$. If $q = 2$ and n is even, then a generalized bent function is called a bent function. A function $f \in \mathcal{B}_n$, where n is odd, is said to be *semi–bent* if and only if $|\mathcal{H}_f(\mathbf{u})| \in \{0, \sqrt{2}\}$, for all $\mathbf{u} \in \mathbb{Z}_2^n$. The maximum possible algebraic degree of a bent function on n variables (when n even) is $\frac{n}{2}$ and for a semi–bent function on n variables (when n odd) is $\frac{n+1}{2}$ (cf. [1], [2]).

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

$$\mathcal{N}_f(\mathbf{u}) = 2^{-\frac{n}{2}} \sum_{\mathbf{x}\in\mathbb{Z}_2^n} (-1)^{f(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}}\, \imath^{wt(\mathbf{x})}. \tag{4}$$

A function $f \in \mathcal{B}_n$ is said to be *negabent* if and only if $|\mathcal{N}_f(\mathbf{u})| = 1$ for all $\mathbf{u} \in \mathbb{Z}_2^n$. If $f \in \mathcal{B}_n$, then the inverse of the nega–Hadamard transform $\mathcal{N}_f$ is

$$(-1)^{f(\mathbf{y})} = 2^{-\frac{n}{2}}\, \imath^{-wt(\mathbf{y})} \sum_{\mathbf{u}\in\mathbb{Z}_2^n} \mathcal{N}_f(\mathbf{u})(-1)^{\mathbf{y}\cdot\mathbf{u}}, \tag{5}$$

for all $\mathbf{y} \in \mathbb{Z}_2^n$. We recall the following result.

Proposition 1: [6, Lemma 1] For any $\mathbf{u} \in \mathbb{Z}_2^n$ we have

$$\sum_{\mathbf{x}\in\mathbb{Z}_2^n} (-1)^{\mathbf{u}\cdot\mathbf{x}}\imath^{wt(\mathbf{x})} = 2^{\frac{n}{2}}\omega^n \imath^{-wt(\mathbf{u})}, \tag{6}$$

where $\omega = (1+\imath)/\sqrt{2}$ is a primitive 8th root of unity.

The Hadamard kernel, the nega–Hadamard kernel and the identity transform on $\mathbb{Z}_2^2$, denoted by H, N and I, respectively, are

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, N = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & \imath \\ 1 & -\imath \end{pmatrix}$$

and

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

The set of 2^n different unitary transforms that are obtained by performing tensor products H and N, n times in any possible sequence is denoted by $\{H, N\}^n$. If $\mathbf{R}_H$ and $\mathbf{R}_N$ partition $\{1, \ldots, n\}$, then the unitary transform, U of dimension $2^n \times 2^n$, corresponding to this partition is

$$U = \prod_{j\in\mathbf{R}_H} H_j \prod_{j\in\mathbf{R}_N} N_j \tag{7}$$

where

$$K_j = I \otimes I \otimes \ldots \otimes I \otimes K \otimes I \otimes \ldots \otimes I$$

with K in the jth position, $K \in \{H, N\}$ and "$\otimes$" indicating the tensor product of matrices. Let $i_\mathbf{x} \in \{0, 1, \ldots, 2^n - 1\}$ denote a row or column number of the unitary matrix U. We write

$$i_\mathbf{x} = x_n 2^{n-1} + x_{n-1}2^{n-2} + \cdots + x_2 2 + x_1$$

where $\mathbf{x} = (x_n, \ldots, x_1) \in \mathbb{Z}_2^n$. For any Boolean function $f \in \mathcal{B}_n$, let $(-1)^\mathbf{f}$ denote a $2^n \times 1$ column vector whose $i_\mathbf{u}$ row entry is $(-1)^{f(\mathbf{u})}$, for all $\mathbf{u} \in \mathbb{Z}_2^n$. The spectrum of f with respect to $U \in \{H, N\}^n$ is the vector $U(-1)^\mathbf{f}$. If $\mathbf{R}_H = \{1, \ldots, n\}$, then the entry in the $i_\mathbf{u}$th row of $U(-1)^\mathbf{f}$ is $\mathcal{H}_f(\mathbf{u})$ and, if $\mathbf{R}_N = \{1, \ldots, n\}$, then the entry in the $i_\mathbf{u}$th row of $U(-1)^\mathbf{f}$ is $\mathcal{N}_f(\mathbf{u})$, for all $\mathbf{u} \in \mathbb{Z}_2^n$. In the former case, $U(-1)^\mathbf{f}$ is said to be the Walsh–Hadamard spectrum of f, while in the latter case it is the nega–Hadamard spectrum of f. The spectrum of a function f with respect to a unitary transform U is said to be flat if and only if the absolute value of each entry of $U(-1)^\mathbf{f}$ is 1.

Definition 2: A function $f \in \mathcal{B}_n$ is said to be bent$_4$ if there exists at least one $U \in \{H, N\}^n$ such that $U(-1)^\mathbf{f}$ is flat.

The bent and the negabent functions belong to the class of bent$_4$ functions as extreme cases. For results on negabent and bent–negabent functions we refer to [3], [6], [7], [9].

In this paper, we consider the spectra of Boolean functions with respect to the action of unitary transforms in $\{H, N\}^n$. We prove that the maximum possible algebraic degree of a bent$_4$ function on n variables is $\lceil \frac{n}{2} \rceil$, and hence solve an open problem posed by Riera and Parker [4]. Further, we obtain a relationship between bent and bent$_4$ functions which is a generalization of the relationship between bent and negabent Boolean functions proved by Parker and Pott [3, Theorem 12].

II. Bent properties with respect to $\{H, N\}^n$

Let $s_r(\mathbf{x})$ be the homogeneous symmetric Boolean function of algebraic degree r whose ANF is

$$s_r(\mathbf{x}) = \bigoplus_{1\le i_1<\ldots<i_r\le n} x_{i_1}\ldots x_{i_r}. \tag{8}$$

The intersection of two vectors $\mathbf{c} = (c_n, \ldots, c_1), \mathbf{x} = (x_n, \ldots, x_1) \in \mathbb{Z}_2^n$ is defined as

$$\mathbf{c} * \mathbf{x} = (c_n x_n, \ldots, c_1 x_1).$$

We define the function $s_r(\mathbf{c} * \mathbf{x})$ as

$$s_r(\mathbf{c} * \mathbf{x}) = \bigoplus_{1\le i_1<\ldots<i_r\le n} (c_{i_1}x_{i_1})\ldots(c_{i_r}x_{i_r}). \tag{9}$$

Suppose, the function $g \in \mathcal{GB}_n^4$ defined as $g(\mathbf{x}) = wt(\mathbf{x}) \mod 4$, for all $\mathbf{x} \in \mathbb{Z}_2^n$. In the following proposition and its corollary we obtain a connection between g and s_2 which plays a crucial role in developing connections between different bent criteria. It is to be noted that the result of Proposition 3 is mentioned earlier by Su, Pott and Tang in the proof of [9, Lemma 1]. We provide an alternative proof.

Proposition 3: If $g \in \mathcal{GB}_n^4$ is defined by $g(\mathbf{x}) = wt(\mathbf{x}) \mod 4$ for all $\mathbf{x} \in \mathbb{Z}_2^n$, then

$$g(\mathbf{x}) = \mathbf{1}\cdot\mathbf{x} + 2s_2(\mathbf{x}) = wt(\mathbf{x}) \mod 4, \tag{10}$$

for all $\mathbf{x} \in \mathbb{Z}_2^n$.

Proof: By Proposition 1, we have

$$2^{-\frac{n}{2}} \sum_{\mathbf{x}\in\mathbb{Z}_2^n} (-1)^{\mathbf{u}\cdot\mathbf{x}} \imath^{wt(\mathbf{x})} = \omega^n \imath^{-wt(\mathbf{u})}. \tag{11}$$

Therefore, $g(\mathbf{x}) = wt(\mathbf{x}) \mod 4$ is a generalized bent on $\mathbb{Z}_4$, which we refer to as $\mathbb{Z}_4$-bent. According to [8, Corollary 15] and [5], there exist $a, b \in \mathcal{B}_n$ such that b and $a+b$ are bent functions and $g(\mathbf{x}) = a(\mathbf{x}) + 2b(\mathbf{x}) = wt(\mathbf{x}) \mod 4$, for all $\mathbf{x} \in \mathbb{Z}_2^n$. From this we have

$$2b(\mathbf{x}) \equiv wt(\mathbf{x}) - a(\mathbf{x}) \pmod 4,$$

i.e.,

$$2 \mid (wt(\mathbf{x}) - a(\mathbf{x})),$$

i.e.,

$$a(\mathbf{x}) = \mathbf{1}\cdot\mathbf{x}$$

where $\mathbf{1} = (1,1,\ldots,1) \in \mathbb{Z}_2^n$, for all $\mathbf{x} \in \mathbb{Z}_2^n$. Therefore,

$$g(\mathbf{x}) = \mathbf{1}\cdot\mathbf{x} + 2b(\mathbf{x}) = wt(\mathbf{x}) \mod 4, \text{ for all } \mathbf{x} \in \mathbb{Z}_2^n,$$

i.e.,

$$b(\mathbf{x}) = \frac{-\mathbf{1}\cdot\mathbf{x} + wt(\mathbf{x})}{2} \mod 2, \text{ for all } \mathbf{x} \in \mathbb{Z}_2^n.$$

Since $b \in \mathcal{B}_n$ is a symmetric bent function and $b(\mathbf{0}) = 0$ we have $b(\mathbf{x}) = s_2(\mathbf{x})$ or $s_2(\mathbf{x}) \oplus s_1(\mathbf{x})$. Since $b(0\ldots01) = 0$, we have $b(\mathbf{x}) = s_2(\mathbf{x})$. Therefore

$$g(\mathbf{x}) = \mathbf{1}\cdot\mathbf{x} + 2s_2(\mathbf{x}) = wt(\mathbf{x}) \mod 4, \text{for all } \mathbf{x} \in \mathbb{Z}_2^n.$$

■

The following corollary generalizes (10) which is useful in finding a general expression of entries of any matrix $U \in \{H, N\}^n$.

Corollary 4: Let $\mathbf{x}, \mathbf{c} \in \mathbb{Z}_2^n$. Then

$$\mathbf{c}\cdot\mathbf{x} + 2s_2(\mathbf{c} * \mathbf{x}) = wt(\mathbf{c} * \mathbf{x}) \mod 4, \tag{12}$$

for all $\mathbf{x} \in \mathbb{Z}_2^n$.

Proof: In Proposition 3 it is proved that

$$\mathbf{1}\cdot\mathbf{x} + 2s_2(\mathbf{x}) = wt(\mathbf{x}) \mod 4, \text{ for all } \mathbf{x} \in \mathbb{Z}_2^n,$$

i.e.,

$$\begin{aligned}&(1,\ldots,1)\cdot(x_n,\ldots,x_1) + 2s_2(x_n,\ldots,x_1)\\ &= wt(x_n,\ldots,x_1) \mod 4, \text{ for all } \mathbf{x} \in \mathbb{Z}_2^n.\end{aligned}$$

Replacing x_i by $c_i x_i$ we get

$$\begin{aligned}&(1,\ldots,1)\cdot(c_n x_n,\ldots,c_1 x_1) + 2s_2(c_n x_n,\ldots,c_1 x_1)\\ &\quad = wt(c_n x_n,\ldots,c_1 x_1) \mod 4, \text{ for all } \mathbf{x} \in \mathbb{Z}_2^n,\end{aligned}$$

i.e.,

$$\begin{aligned}&(c_n x_n \oplus \ldots \oplus c_1 x_1) + 2s_2(c_n x_n,\ldots,c_1 x_1)\\ &= wt(c_n x_n,\ldots,c_1 x_1) \mod 4, \text{ for all } \mathbf{x} \in \mathbb{Z}_2^n.\end{aligned}$$

Therefore,

$$\mathbf{c}\cdot\mathbf{x} + 2s_2(\mathbf{c}*\mathbf{x}) = wt(\mathbf{c}*\mathbf{x}) \mod 4, \text{ for all } \mathbf{x} \in \mathbb{Z}_2^n.$$

■

Riera and Parker [4, Lemma 7] have obtained a general expression for the entries of any matrix $U \in \{H, N\}^n$. We obtain an alternative description below which we use to connect the spectrum $U(-1)^{\mathbf{f}}$ of any $f \in \mathcal{B}_n$ to the Walsh–Hadamard spectra of some associated functions.

Theorem 5: If $U = \prod_{j\in\mathbf{R}_H} H_j \prod_{j\in\mathbf{R}_N} N_j$, is a unitary matrix constructed as in (7), corresponding to the partition $\mathbf{R}_H, \mathbf{R}_N$ of $\{1,\ldots,n\}$ where $n \geq 2$, then for any $\mathbf{u}, \mathbf{x} \in \mathbb{Z}_2^n$ the entry in the $i_{\mathbf{u}}$th row and $i_{\mathbf{x}}$th column of $2^{\frac{n}{2}} U$ is

$$(-1)^{\mathbf{u}\cdot\mathbf{x} \oplus s_2(\mathbf{c}*\mathbf{x})} \imath^{\mathbf{c}\cdot\mathbf{x}},$$

where $\mathbf{c} = (c_n,\ldots,c_1) \in \mathbb{Z}_2^n$ is such that $c_i = 0$ if $i \in \mathbf{R}_H$ and $c_i = 1$ if $i \in \mathbf{R}_N$.

Proof: We prove this by induction. Let $n = 2$. If $\mathbf{c} = (0,0)$ then clearly $U = H \otimes H$, and if $\mathbf{c} = (1,1)$ then $U = N \otimes N$. We explicitly compute U when $\mathbf{c} = (0,1)$ and $\mathbf{c} = (1,0)$ and find that U is equal to

$$H \otimes N = \frac{1}{2}\begin{pmatrix} 1 & \imath & 1 & \imath \\ 1 & -\imath & 1 & -\imath \\ 1 & \imath & -1 & -\imath \\ 1 & -\imath & -1 & \imath \end{pmatrix},$$

and

$$N \otimes H = \frac{1}{2}\begin{pmatrix} 1 & 1 & \imath & \imath \\ 1 & -1 & \imath & -\imath \\ 1 & 1 & -\imath & -\imath \\ 1 & -1 & -\imath & \imath \end{pmatrix},$$

respectively. By Corollary 4

$$(-1)^{\mathbf{u}\cdot\mathbf{x}\oplus s_2(\mathbf{c}*\mathbf{x})} \imath^{\mathbf{c}\cdot\mathbf{x}} = (-1)^{\mathbf{u}\cdot\mathbf{x}} \imath^{wt(\mathbf{c}*\mathbf{x})}.$$

Suppose the result is true for n. Let $\mathbf{u}, \mathbf{x}, \mathbf{c} \in \mathbb{Z}_2^n$, and $\mathbf{u}' = (u_{n+1}, \mathbf{u}), \mathbf{x}' = (x_{n+1}, \mathbf{x}), \mathbf{c}' = (c_{n+1}, \mathbf{c}) \in \mathbb{Z}_2^{n+1}$. Let $U \in \{H, N\}^n$ be the unitary transform induced by the partition corresponding to $\mathbf{c} \in \mathbb{Z}_2^n$. The transform corresponding to the partition induced by

$\mathbf{c}' = (0, \mathbf{c}) \in \mathbb{Z}_2^{n+1}$ is $H \otimes U$. By taking the tensor product of H and U we obtain

$$2^{\frac{n+1}{2}}(H \otimes U) = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix}$$

where

$$\begin{aligned} A_{11} &= \left((-1)^{\mathbf{u}\cdot\mathbf{x}} \imath^{wt(\mathbf{c}*\mathbf{x})}\right)_{2^n \times 2^n} \\ &= \left((-1)^{(0,\mathbf{u})\cdot(0,\mathbf{x})} \imath^{wt((0,\mathbf{c})*(0,\mathbf{x}))}\right)_{2^n \times 2^n}, \end{aligned}$$

$$\begin{aligned} A_{12} &= \left((-1)^{\mathbf{u}\cdot\mathbf{x}} \imath^{wt(\mathbf{c}*\mathbf{x})}\right)_{2^n \times 2^n} \\ &= \left((-1)^{(0,\mathbf{u})\cdot(1,\mathbf{x})} \imath^{wt((0,\mathbf{c})*(1,\mathbf{x}))}\right)_{2^n \times 2^n}, \end{aligned}$$

$$\begin{aligned} A_{21} &= \left((-1)^{\mathbf{u}\cdot\mathbf{x}} \imath^{wt(\mathbf{c}*\mathbf{x})}\right)_{2^n \times 2^n} \\ &= \left((-1)^{(1,\mathbf{u})\cdot(0,\mathbf{x})} \imath^{wt((0,\mathbf{c})*(0,\mathbf{x}))}\right)_{2^n \times 2^n} \end{aligned}$$

and

$$\begin{aligned} A_{22} &= \left((-1)(-1)^{\mathbf{u}\cdot\mathbf{x}} \imath^{wt(\mathbf{c}*\mathbf{x})}\right)_{2^n \times 2^n} \\ &= \left((-1)^{(1,\mathbf{u})\cdot(1,\mathbf{x})} \imath^{wt((0,\mathbf{c})*(1,\mathbf{x}))}\right)_{2^n \times 2^n}. \end{aligned}$$

Therefore,

$$2^{\frac{n+1}{2}}(H \otimes U) = \left((-1)^{\mathbf{u}'\cdot\mathbf{x}'} \imath^{wt(\mathbf{c}'*\mathbf{x}')}\right)_{2^{n+1} \times 2^{n+1}}.$$

The transform corresponding to the partition induced by $\mathbf{c}' = (1, \mathbf{c}) \in \mathbb{Z}_2^{n+1}$ is $N \otimes U$. By taking the tensor product of H and U we obtain

$$2^{\frac{n+1}{2}}(N \otimes U) = \begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix}$$

where

$$\begin{aligned} B_{11} &= \left((-1)^{\mathbf{u}\cdot\mathbf{x}} \imath^{wt(\mathbf{c}*\mathbf{x})}\right)_{2^n \times 2^n} \\ &= \left((-1)^{(0,\mathbf{u})\cdot(0,\mathbf{x})} \imath^{wt((1,\mathbf{c})*(0,\mathbf{x}))}\right)_{2^n \times 2^n}, \end{aligned}$$

$$\begin{aligned} B_{12} &= \left(\imath(-1)^{\mathbf{u}\cdot\mathbf{x}} \imath^{wt(\mathbf{c}*\mathbf{x})}\right)_{2^n \times 2^n} \\ &= \left((-1)^{(0,\mathbf{u})\cdot(1,\mathbf{x})} \imath^{wt((1,\mathbf{c})*(1,\mathbf{x}))}\right)_{2^n \times 2^n}, \end{aligned}$$

$$\begin{aligned} B_{21} &= \left((-1)^{\mathbf{u}\cdot\mathbf{x}} \imath^{wt(\mathbf{c}*\mathbf{x})}\right)_{2^n \times 2^n} \\ &= \left((-1)^{(1,\mathbf{u})\cdot(0,\mathbf{x})} \imath^{wt((1,\mathbf{c})*(0,\mathbf{x}))}\right)_{2^n \times 2^n} \end{aligned}$$

and

$$\begin{aligned} B_{22} &= \left((-\imath)(-1)^{\mathbf{u}\cdot\mathbf{x}} \imath^{wt(\mathbf{c}*\mathbf{x})}\right)_{2^n \times 2^n} \\ &= \left((-1)^{(1,\mathbf{u})\cdot(1,\mathbf{x})} \imath^{wt((1,\mathbf{c})*(1,\mathbf{x}))}\right)_{2^n \times 2^n}. \end{aligned}$$

Therefore,

$$2^{\frac{n+1}{2}}(N \otimes U) = \left((-1)^{\mathbf{u}'\cdot\mathbf{x}'} \imath^{wt(\mathbf{c}'*\mathbf{x}')}\right)_{2^{n+1} \times 2^{n+1}}.$$

This proves the result. ■

Using Theorem 5 we can state that given any $U \in \{H, N\}^n$ there exists $\mathbf{c} \in \mathbb{Z}_2^n$ such that for any $f \in \mathcal{B}_n$ the $i_{\mathbf{u}}$th row of the column vector $U(-1)^{\mathbf{f}}$ is

$$\begin{aligned} \mathcal{U}_f^{\mathbf{c}}(\mathbf{u}) &= 2^{-\frac{n}{2}} \sum_{\mathbf{x} \in \mathbb{Z}_2^n} (-1)^{f(\mathbf{x}) \oplus s_2(\mathbf{c}*\mathbf{x})} \imath^{\mathbf{c}\cdot\mathbf{x}} (-1)^{\mathbf{u}\cdot\mathbf{x}} \\ &= 2^{-\frac{n}{2}} \sum_{\mathbf{x} \in \mathbf{c}^\perp} (-1)^{f(\mathbf{x}) \oplus s_2(\mathbf{c}*\mathbf{x})} (-1)^{\mathbf{u}\cdot\mathbf{x}} \\ &\quad + \imath 2^{-\frac{n}{2}} \sum_{\mathbf{x} \notin \mathbf{c}^\perp} (-1)^{f(\mathbf{x}) \oplus s_2(\mathbf{c}*\mathbf{x})} (-1)^{\mathbf{u}\cdot\mathbf{x}}. \end{aligned} \tag{13}$$

Therefore, $\mathcal{U}_f^{\mathbf{c}}(\mathbf{u})$ is related to the Walsh–Hadamard transform of restrictions $f(\mathbf{x}) \oplus s_2(\mathbf{c} * \mathbf{x})$ to the subspace $\mathbf{c}^\perp$ and its coset. From another perspective this transform provides a measure of the distance of the function f to the functions of the form $s_2(\mathbf{c}*\mathbf{x}) \oplus \mathbf{u}\cdot\mathbf{x}$. Thus, if $|\mathcal{U}_f^{\mathbf{c}}(\mathbf{u})|$ has high value for a choice of $\mathbf{u}, \mathbf{c} \in \mathbb{Z}_2^n$ then f has low Hamming distance from the function of the form $s_2(\mathbf{c} * \mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x}$. This means that the function may be approximated efficiently by the function $s_2(\mathbf{c} * \mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x}$. This may have some cryptographic significance for the spectra of f with respect to the transform $U \in \{H, N\}^n$.

Riera and Parker [4, p. 4125] posed the following open problem:

What is the maximum algebraic degree of a bent$_4$ Boolean function of n variables?

Su, Pott and Tang [9] have recently proved that the maximum algebraic degree of a bent–negabent function is $\frac{n}{2}$ (note that n is even, since bent functions exist only on even variables). Further, they have provided a method to construct bent–negabent functions of algebraic degree ranging from 2 to $\frac{n}{2}$. In the next theorem we solve the problem proposed by Riera and Parker and thus generalize the result related to the upper bound of algebraic degree proved in [9].

Theorem 6: The maximum algebraic degree of a bent$_4$ Boolean function on n variables is $\lceil \frac{n}{2} \rceil$.

Proof: Using Theorem 5 we can state that given any $U \in \{H, N\}^n$ there exists $\mathbf{c} \in \mathbb{Z}_2^n$ such that for any $f \in \mathcal{B}_n$ the $i_{\mathbf{u}}$th row entry of the column vector

$U(-1)^{\mathbf{f}}$ is

$$
\begin{aligned}
2^{\frac{n}{2}}\mathcal{U}_f^{\mathbf{c}}(\mathbf{u}) &= \sum_{\mathbf{x}\in\mathbb{Z}_2^n}(-1)^{f(\mathbf{x})\oplus s_2(\mathbf{c}*\mathbf{x})}\imath^{\mathbf{c}\cdot\mathbf{x}}(-1)^{\mathbf{u}\cdot\mathbf{x}} \\
&= \sum_{\mathbf{x}\in\mathbf{c}^{\perp}}(-1)^{f(\mathbf{x})\oplus s_2(\mathbf{c}*\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}} \\
&\quad + \imath\sum_{\mathbf{x}\notin\mathbf{c}^{\perp}}(-1)^{f(\mathbf{x})\oplus s_2(\mathbf{c}*\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}}.
\end{aligned} \tag{14}
$$

Let us suppose that f is bent$_4$ with respect to the chosen transform U. Therefore, we have $|\mathcal{U}_f^{\mathbf{c}}(\mathbf{u})| = 1$, for all $\mathbf{u}\in\mathbb{Z}_2^n$. By (14)

$$
\begin{aligned}
2^n &= \left(\sum_{\mathbf{x}\in\mathbf{c}^{\perp}}(-1)^{f(\mathbf{x})\oplus s_2(\mathbf{c}*\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}}\right)^2 \\
&\quad + \left(\sum_{\mathbf{x}\notin\mathbf{c}^{\perp}}(-1)^{f(\mathbf{x})\oplus s_2(\mathbf{c}*\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}}\right)^2.
\end{aligned} \tag{15}
$$

By Jacobi's two-square theorem we know that 2^n has a unique representation (disregarding the sign and order) as a sum of two squares, namely $2^n = (2^{\frac{n}{2}})^2 + 0$, if n is even, and $2^n = (2^{\frac{n-1}{2}})^2 + (2^{\frac{n-1}{2}})^2$, if n is odd. Let $g_{\mathbf{c}}(\mathbf{x}) = s_2(\mathbf{c}*\mathbf{x})$, for all $\mathbf{x}\in\mathbb{Z}_2^n$.

$$
\begin{aligned}
|\mathcal{H}_{f\oplus g_{\mathbf{c}}}(\mathbf{u})| &= |2^{-\frac{n}{2}}\sum_{\mathbf{x}\in\mathbb{Z}_2^n}(-1)^{f(\mathbf{x})\oplus s_2(\mathbf{c}*\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}}| \\
&= |2^{-\frac{n}{2}}\sum_{\mathbf{x}\in\mathbf{c}^{\perp}}(-1)^{f(\mathbf{x})\oplus s_2(\mathbf{c}*\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}} \\
&\quad + 2^{-\frac{n}{2}}\sum_{\mathbf{x}\notin\mathbf{c}^{\perp}}(-1)^{f(\mathbf{x})\oplus s_2(\mathbf{c}*\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}}| \\
&= 1,
\end{aligned} \tag{16}
$$

for all $\mathbf{u}\in\mathbb{Z}_2^n$. Therefore, $f\oplus g_{\mathbf{c}}$ is a bent function and its algebraic degree is bounded above by $\frac{n}{2}$. The algebraic degree of $g_{\mathbf{c}}$ is upper-bounded by 2, so the upper bound of the algebraic degree of a bent$_4$ Boolean function f is $\frac{n}{2}$, when n is even.

In case n is odd by a similar argument we get $|\mathcal{H}_{f\oplus g_{\mathbf{c}}}(\mathbf{u})| \in \{0,\sqrt{2}\}$, that is $f\oplus g_{\mathbf{c}}$ is semi–bent, and therefore the algebraic degree of f is bounded above by $\frac{n+1}{2}$. ∎

III. Connecting bent and bent$_4$ functions

Let $f\in\mathcal{B}_n$ and V is a subspace of $\mathbb{Z}_2^n$. For any $\mathbf{a}\in\mathbb{Z}_2^n$ the restriction of f to the coset $\mathbf{a}+V$ is defined as $f|_{\mathbf{a}+V}(\mathbf{x}) = f(\mathbf{a}+\mathbf{x})$, for all $\mathbf{x}\in V$. It is to be noted that the restriction of a function f to a coset $\mathbf{a}+V$ is unique up to a translation. The following lemma is well known (cf. [1]), nevertheless we provide a complete proof for clarity.

Lemma 7: Let $n=2k$, $f\in\mathcal{B}_n$ a bent function, V be an $(n-1)$-dimensional subspace of $\mathbb{Z}_2^n$, $\mathbf{a}\in\mathbb{Z}_2^n\setminus V$ such that $\mathbb{Z}_2^n = V\cup(\mathbf{a}\oplus V)$. Then the restrictions of f to V and $\mathbf{a}\oplus V$, denoted $f|_V$ and $f|_{\mathbf{a}\oplus V}$ respectively, are semi–bent functions and $\mathcal{H}_{f|_V}(\mathbf{u})\mathcal{H}_{f|_{\mathbf{a}\oplus V}}(\mathbf{u}) = 0$ for all $\mathbf{u}\in\mathbb{F}_2^n$.

Proof: Since the dimension of V is $n-1$, the dimension of the orthogonal subspace $V^{\perp}$ is 1. Let $V^{\perp} = \{\mathbf{0},\mathbf{b}\}$. Since $\mathbf{a}\notin V$, $\mathbf{a}\cdot\mathbf{b} = 1$. For all $\mathbf{u}\in\mathbb{Z}_2^n$ we have the following

$$
\begin{aligned}
2^{\frac{n}{2}}\mathcal{H}_f(\mathbf{u}) &= \sum_{\mathbf{x}\in V}(-1)^{f(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}} \\
&\quad + (-1)^{\mathbf{u}\cdot\mathbf{a}}\sum_{\mathbf{x}\in V}(-1)^{f(\mathbf{x}+\mathbf{a})\oplus\mathbf{u}\cdot\mathbf{x}} \\
&\in \{-2^{\frac{n}{2}}, 2^{\frac{n}{2}}\}
\end{aligned} \tag{17}
$$

$$
\begin{aligned}
2^{\frac{n}{2}}\mathcal{H}_f(\mathbf{u}\oplus\mathbf{b}) &= \sum_{\mathbf{x}\in V}(-1)^{f(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}} \\
&\quad - (-1)^{\mathbf{u}\cdot\mathbf{a}}\sum_{\mathbf{x}\in V}(-1)^{f(\mathbf{x}+\mathbf{a})\oplus\mathbf{u}\cdot\mathbf{x}} \\
&\in \{-2^{\frac{n}{2}}, 2^{\frac{n}{2}}\}.
\end{aligned} \tag{18}
$$

By adding (17) and (18) we obtain $\sum_{\mathbf{x}\in V}(-1)^{f(\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}} \in \{-2^{\frac{n}{2}},0,2^{\frac{n}{2}}\}$, and by subtracting (18) from (17) we obtain $\sum_{\mathbf{x}\in V}(-1)^{f(\mathbf{a}\oplus\mathbf{x})\oplus\mathbf{u}\cdot\mathbf{x}} \in \{-2^{\frac{n}{2}},0,2^{\frac{n}{2}}\}$. This proves that both $f|_V$ and $f|_{\mathbf{a}\oplus V}$ are semi–bent functions. Further, since the sums in (17) and (18) are both in $\{-2^{\frac{n}{2}},2^{\frac{n}{2}}\}$, for all $\mathbf{u}\in\mathbb{Z}_2^n$, we have $\mathcal{H}_{f|_V}(\mathbf{u})\mathcal{H}_{f|_{\mathbf{a}\oplus V}}(\mathbf{u}) = 0$, for all $\mathbf{u}\in\mathbb{Z}_2^n$. ∎

This leads us to a generalization of [3, Theorem 12] due to Parker and Pott. Recall that for any $\mathbf{c}\in\mathbb{Z}_2^n$ we have defined $g_{\mathbf{c}}(\mathbf{x}) = s_2(\mathbf{c}*\mathbf{x})$, for all $\mathbf{x}\in\mathbb{Z}_2^n$.

Theorem 8: Let $f\in\mathcal{B}_n$ where n is even. Then the following two statements are true.

1) If f is bent, then $f\oplus g_{\mathbf{c}}$ is bent$_4$ and $|\mathcal{U}_{f\oplus g_{\mathbf{c}}}^{\mathbf{c}}(\mathbf{u})| = 1$, for all $\mathbf{u}\in\mathbb{Z}_2^n$
2) If f is bent$_4$, i.e., there exists $\mathbf{c}\in\mathbb{Z}_2^n$ such that $|\mathcal{U}_f^{\mathbf{c}}(\mathbf{u})| = 1$, for all $\mathbf{u}\in\mathbb{Z}_2^n$, then $f\oplus g_{\mathbf{c}}$ is bent.

Proof: Suppose f is a bent function. If $\mathbf{c} = \mathbf{0}$ there is nothing to prove. If $\mathbf{c} \neq \mathbf{0}$, then

$$\begin{aligned}2^{\frac{n}{2}}\mathcal{U}^{\mathbf{c}}_{f\oplus g_{\mathbf{c}}}(\mathbf{u}) &= \sum_{\mathbf{x}\in\mathbb{Z}_2^n}(-1)^{f(\mathbf{x})\oplus s_2(\mathbf{c}*\mathbf{x})}\imath^{wt(\mathbf{c}*\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}}\\ &= \sum_{\mathbf{x}\in\mathbb{Z}_2^n}(-1)^{f(\mathbf{x})\oplus s_2(\mathbf{c}*\mathbf{x})\oplus s_2(\mathbf{c}*\mathbf{x})\oplus \mathbf{u}\cdot\mathbf{x}}\imath^{\mathbf{c}\cdot\mathbf{x}}\\ &= \sum_{\mathbf{x}\in\mathbb{Z}_2^n}(-1)^{f(\mathbf{x})\oplus \mathbf{u}\cdot\mathbf{x}}\imath^{\mathbf{c}\cdot\mathbf{x}}\\ &= \sum_{\mathbf{x}\in\mathbf{c}^{\perp}}(-1)^{f(\mathbf{x})\oplus \mathbf{u}\cdot\mathbf{x}}\\ &\quad + \imath\sum_{\mathbf{x}\notin\mathbf{c}^{\perp}}(-1)^{f(\mathbf{x})\oplus \mathbf{u}\cdot\mathbf{x}}.\end{aligned} \tag{19}$$

Since f is a bent function and $\mathbf{c}^{\perp}$ is a subspace of codimension 1, by Lemma 7 the restrictions of f on $\mathbf{c}^{\perp}$ and its remaining coset are semi–bent and their Walsh-Hadamard spectra are disjoint. Therefore, the right hand side of the above equation belongs to the set $\{\pm 2^{\frac{n}{2}}, \pm 2^{\frac{n}{2}}\imath\}$ for all $\mathbf{u} \in \mathbb{Z}_2^n$. This proves the first statement.

In the second part, we assume f to be a bent$_4$ function such that there exists $\mathbf{c} \in \mathbb{Z}_2^n$ for which $|\mathcal{U}_f^{\mathbf{c}}(\mathbf{u})| = 1$, for all $\mathbf{u} \in \mathbb{Z}_2^n$. We have

$$\begin{aligned}\mathcal{U}_f^{\mathbf{c}}(\mathbf{u}) &= 2^{-\frac{n}{2}}\sum_{\mathbf{x}\in\mathbb{Z}_2^n}(-1)^{f(\mathbf{x})}\imath^{wt(\mathbf{c}*\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}}\\ &= 2^{-\frac{n}{2}}\sum_{\mathbf{x}\in\mathbb{Z}_2^n}\imath^{wt(\mathbf{c}*\mathbf{x})+2f(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}}.\end{aligned} \tag{20}$$

Thus, the function $h(\mathbf{x}) = wt(\mathbf{c}*\mathbf{x}) + 2f(\mathbf{x}) \mod 4$, for all $\mathbf{x} \in \mathbb{Z}_2^n$, is a $\mathbb{Z}_4$-bent function which implies the existence of Boolean functions $a, b \in \mathcal{B}_n$ such that b, $a+b$ are bents [8, Corollary 15], with

$$\begin{aligned}h(\mathbf{x}) &= a(\mathbf{x}) + 2b(\mathbf{x})\\ &= wt(\mathbf{c}*\mathbf{x}) + 2f(\mathbf{x}) \mod 4,\end{aligned} \tag{21}$$

for all $\mathbf{x} \in \mathbb{Z}_2^n$. Therefore, $2 \mid (a(\mathbf{x}) - wt(\mathbf{c}*\mathbf{x}))$, which implies $a(\mathbf{x}) = \mathbf{c}\cdot\mathbf{x}$, for all $\mathbf{x} \in \mathbb{Z}_2^n$. By Corollary 4 and (20) we have

$$b(\mathbf{x}) = f(\mathbf{x}) \oplus s_2(\mathbf{c}*\mathbf{x}),$$

for all $\mathbf{x} \in \mathbb{Z}_2^n$. Since $b \in \mathcal{B}_n$ is a bent function, $f \oplus g_{\mathbf{c}}$ is a bent function. Thus, we have proved that if f is bent$_4$ function, with respect to the unitary transform corresponding to $\mathbf{c} \in \mathbb{Z}_2^n$, then $f \oplus g_{\mathbf{c}}$ is a bent function. ∎

IV. Conclusion

In this paper we have developed an approach to study the action of the transforms in $\{H, N\}^n$ on Boolean functions on n variables. By using our approach we have proved that the maximum possible algebraic degree of a bent$_4$ function on n variables is $\lceil \frac{n}{2} \rceil$ and hence solve an open problem proposed by Riera and Parker [4]. We have also obtained a connection between bent and bent$_4$ functions, which is a generalization of the connection between bent and negabent function proved by Parker and Pott [3]. It is observed that if the absolute value of an entry in the spectrum of a function with respect to a transform $U \in \{H, N\}^n$ is large, then the function has low Hamming distance from a particular quadratic function determined by U. Thus, we have established a connection between the generalized bent criteria and approximation of a Boolean function of arbitrary algebraic degree by quadratic Boolean functions.

References

[1] 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.

[2] T. W. Cusick, P. Stănică, *Cryptographic Boolean functions and applications*. New York: Academic, 2009.

[3] M. G. Parker, A. Pott, "On Boolean functions which are bent and negabent," in *Proc. Int. Conf. Sequences, Subsequences, Consequences*, 2007, vol. LNCS–4893, pp. 9–23.

[4] C. Riera, M. G. Parker, "Generalized bent criteria for Boolean functions," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 4142–4159, Sep. 2006.

[5] P. Solé, N. Tokareva, "Connections between Quaternary and Binary Bent Functions," *Prikl. Diskr. Mat.*, vol 1, pp. 16–18, 2009, (http://eprint.iacr.org/2009/544.pdf).

[6] K. U. Schmidt, M. G. Parker, A. Pott, "Negabent functions in the Maiorana–McFarland class," in Proc. Int. Conf. Sequences Appl., 2008, vol. LNCS–5203, pp. 390–402.

[7] P. Stănică, S. Gangopadhyay, A. Chaturvedi, A. K. Gangopadhyay, S. Maitra, "Investigations on bent and negabent functions via the nega–Hadamard transform," *IEEE Trans. Inf. Theory*, vol. 58, no. 6, pp. 4064–4072, June 2012.

[8] P. Stănică, T. Martinsen, S. Gangopadhyay, B. K. Singh, "Bent and generalized bent Boolean functions," *Des. Codes Cryptogr.*, DOI 10.1007/s10623-012-9622-5.

[9] W. Su, A. Pott, X. Tang, "Characterization of negabent functions and construction of bent–negabent functions with maximum algebraic degree," *arXiv*: 1205.6568v1 [cs.IT], 30 May 2012.