A note on generalized bent criteria for Boolean functions

Sugata Gangopadhyay, Enes Pasalic, Pantelimon Stănică

***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 obtain a relationship between bent, semi–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]. As a corollary to this result 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-TIT 52:9 (2006), 4142–4159].**

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 $\mathbf{x} = (x_n,\dots,x_1)$ 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 $\mathbf{x} = (x_n,\dots,x_1)$ and $\mathbf{y} = (y_n,\dots,y_1)$ are in $\mathbb{Z}_2^n$, we define the scalar (or inner) product by $\mathbf{x}\cdot\mathbf{y} = x_n y_n \oplus \cdots \oplus x_2 y_2 \oplus x_1 y_1$. In $\mathbb{Z}_2^n$, let $\mathbf{0}$ and $\mathbf{1}$ denote the zero vector, respectively, the all 1 vector. 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 $a,b \in \mathbb{R}$.

Sugata Gangopadhyay is with the Department of Mathematics, Indian Institute of Technology Roorkee, Roorkee 247667 INDIA. Email: gsugata@gmail.com

Enes Pasalic is with the Faculty of Mathematics, Natural Sciences and Information Technologies (FAMNIT), University of Primorska, Koper, SLOVENIA. Email: enes.pasalic6@gmail.com

Pantelimon Stănică is with the Department of Applied Mathematics, Naval Postgraduate School, Monterey, CA 93943–5216, USA. Email: pstanica@nps.edu

We call any function from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2$ a *Boolean function* in 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* in n variables [5], whose set is 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

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

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

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

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

The inverse of the Walsh–Hadamard transform is given by

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

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 (n even) is $\frac{n}{2}$ and for a semi–bent function on n variables (n odd) is $\frac{n+1}{2}$ (cf. [1, Proposition 8.15], [2]).

Let $f \in \mathcal{B}_n$ and V be 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 well known (cf. [1]) result is stated without proof.

Proposition 1: Let $n = 2k$, $f \in \mathcal{B}_n$ be 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 $\mathbf{u}\in\mathbb{Z}_2^n$.

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

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

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

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

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

The Hadamard kernel, the nega–Hadamard kernel and the identity transform on $\mathbb{C}^2$, 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

$$U=\prod_{j\in\mathbf{R}_H}H_j\prod_{j\in\mathbf{R}_N}N_j \quad (6)$$

where

$$H_j=I\otimes I\otimes\ldots\otimes I\otimes H\otimes I\otimes\ldots\otimes I$$

with H in the jth position, similarly for N_j, 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

$$i_{\mathbf{x}}=x_n2^{n-1}+x_{n-1}2^{n-2}+\cdots+x_22+x_1$$

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 obtain a relationship between bent, semi–bent and bent$_4$ functions, which is a generalization of the relationship between bent and negabent Boolean functions proved by Parker and Pott [3]. This leads us to 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].

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

$$s_r(\mathbf{x})=\bigoplus_{1\le i_1<\ldots<i_r\le n}x_{i_1}\ldots x_{i_r}. \quad (7)$$

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 the vector

$$\mathbf{c}*\mathbf{x}=(c_nx_n,\ldots,c_1x_1).$$

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

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

We also define the function $g\in\mathcal{GB}_n^4$ by $g(\mathbf{x})=wt(\mathbf{x})\mod 4$, for all $\mathbf{x}\in\mathbb{Z}_2^n$, and we set $s_2^{\mathbf{c}}(\mathbf{x})=s_2(\mathbf{c}*\mathbf{x})$, for easy writing. In the following proposition we obtain a connection between g and $s_2^{\mathbf{c}}$ which plays a crucial role in developing connections between different bent criteria. We note that the result of Proposition 3, for $\mathbf{c}=\mathbf{1}$ is mentioned earlier by Su, Pott and Tang in the proof of [9, Lemma 1]. In the same paper they provide a construction of bent–negabent functions of all algebraic degrees ranging from 2 to $\frac{n}{2}$ (n even).

Proposition 3: Let $\mathbf{x},\mathbf{c}\in\mathbb{Z}_2^n$. Then, for all $\mathbf{x}\in\mathbb{Z}_2^n$,

$$\mathbf{c}\cdot\mathbf{x}+2s_2^{\mathbf{c}}(\mathbf{x})=wt(\mathbf{c}*\mathbf{x})\mod 4. \quad (9)$$

Proof: Using the identity $x_0+x_1\mod 4=(x_0\oplus x_1)+2x_0x_1\mod 4$, by induction on n, we get $\mathbf{1}\cdot\mathbf{x}\mod 4=wt(\mathbf{x})+2\sum_{i<j}x_ix_j\mod 4$. Replacing $\mathbf{x}$ by $\mathbf{c}*\mathbf{x}$, we obtain our result. ∎

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 4: 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 (6), 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 the result by induction. The case of $n = 2$ can be checked directly. By Proposition 3

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

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 $\mathbf{c}' = (c_{n+1}, \mathbf{c})$ is $T_{c_{n+1}} \otimes U$ where $T_{c_{n+1}} = H$ if $c_{n+1} = 0$ and $T_{c_{n+1}} = N$ if $c_{n+1} = 1$. By taking the tensor product of $T_{c_{n+1}}$ and U we obtain

$$2^{\frac{n+1}{2}}(T_{c_{n+1}} \otimes U) = \begin{pmatrix} A_{00}^{c_{n+1}} & A_{01}^{c_{n+1}} \\ A_{10}^{c_{n+1}} & A_{11}^{c_{n+1}} \end{pmatrix}$$

where

$$A_{ij}^{c_{n+1}} = \left((-1)^{(i,\mathbf{u})\cdot(j,\mathbf{x})}\imath^{wt((c_{n+1},\mathbf{c})*(j,\mathbf{x}))}\right)_{2^n\times 2^n}.$$

Therefore,

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

This proves the result. ■

In the following two theorems we establish a connection between bent, semi–bent and bent$_4$ functions, which is a generalization of the relationship between bent and negabent Boolean functions proved by Parker and Pott [3]. The unitary transform in $\{H, N\}^n$ induced by the partition corresponding to $\mathbf{c} \in \mathbb{Z}_2^n$ is denoted by $U_{\mathbf{c}}$ while the entry in the $i_{\mathbf{u}}$th row of the spectrum $U_{\mathbf{c}}(-1)^{\mathbf{f}}$ is $\mathcal{U}_f^{\mathbf{c}}(\mathbf{u})$.

Theorem 5: Let $f \in \mathcal{B}_n$, where n is even. Then, f is bent$_4$ if and only if there exists $\mathbf{c} \in \mathbb{Z}_2^n$ such that $f \oplus s_2^{\mathbf{c}}$ is bent.

Proof: If f is bent$_4$, then there exists $\mathbf{c} \in \mathbb{Z}_2^n$ such that $|\mathcal{U}_f^{\mathbf{c}}(\mathbf{u})| = 1$ for all $\mathbf{u} \in \mathbb{Z}_2^n$. By Theorem 4 we obtain

$$\begin{aligned}\mathcal{U}_f^{\mathbf{c}}(\mathbf{u}) &= 2^{-\frac{n}{2}}\sum_{\mathbf{x}\in\mathbb{Z}_2^n}(-1)^{f(\mathbf{x})\oplus s_2^{\mathbf{c}}(\mathbf{x})}\imath^{\mathbf{c}\cdot\mathbf{x}}(-1)^{\mathbf{u}\cdot\mathbf{x}} \\ &= 2^{-\frac{n}{2}}\sum_{\mathbf{x}\in\mathbf{c}^\perp}(-1)^{f(\mathbf{x})\oplus s_2^{\mathbf{c}}(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}} \\ &\quad + \imath 2^{-\frac{n}{2}}\sum_{\mathbf{x}\notin\mathbf{c}^\perp}(-1)^{f(\mathbf{x})\oplus s_2^{\mathbf{c}}(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}}.\end{aligned} \tag{10}$$

Therefore

$$2^n = \left(\sum_{\mathbf{x}\in\mathbf{c}^\perp}(-1)^{f(\mathbf{x})\oplus s_2^{\mathbf{c}}(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}}\right)^2 + \left(\sum_{\mathbf{x}\notin\mathbf{c}^\perp}(-1)^{f(\mathbf{x})\oplus s_2^{\mathbf{c}}(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}}\right)^2. \tag{11}$$

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. Then for n even,

$$\begin{aligned}|\mathcal{H}_{f\oplus s_2^{\mathbf{c}}}(\mathbf{u})| &= |2^{-\frac{n}{2}}\sum_{\mathbf{x}\in\mathbb{Z}_2^n}(-1)^{f(\mathbf{x})\oplus s_2^{\mathbf{c}}(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}}| \\ &= |2^{-\frac{n}{2}}\sum_{\mathbf{x}\in\mathbf{c}^\perp}(-1)^{f(\mathbf{x})\oplus s_2^{\mathbf{c}}(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}} \\ &\quad + 2^{-\frac{n}{2}}\sum_{\mathbf{x}\notin\mathbf{c}^\perp}(-1)^{f(\mathbf{x})\oplus s_2^{\mathbf{c}}(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}}| \\ &= 1,\ \forall\mathbf{u}\in\mathbb{Z}_2^n.\end{aligned} \tag{12}$$

Thus, $f \oplus s_2^{\mathbf{c}}$ is a bent function.

Suppose $f \oplus s_2^{\mathbf{c}}$ is a bent function. If $\mathbf{c} = \mathbf{0}$ there is nothing to prove. If $\mathbf{c} \neq \mathbf{0}$, then

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

Since $f \oplus s_2^{\mathbf{c}}$ is a bent function and $\mathbf{c}^\perp$ is a subspace of codimension 1, by Proposition 1 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 that f is a bent$_4$ function. ■

Theorem 6: Let $f \in \mathcal{B}_n$ where n is odd. If f is bent$_4$, then there exists $\mathbf{c} \in \mathbb{Z}_2^n$ such that $f \oplus s_2^{\mathbf{c}}$ is semi–bent.

Proof: As in the previous theorem, the function f is bent$_4$ implies that there exists $\mathbf{c} \in \mathbb{Z}_2^n$ such that $|\mathcal{U}_f^{\mathbf{c}}(\mathbf{u})| = 1$ for all $\mathbf{u} \in \mathbb{Z}_2^n$. Since n is an odd integer by (11) we have $\sum_{\mathbf{x}\in\mathbf{c}^\perp}(-1)^{f(\mathbf{x})\oplus s_2^{\mathbf{c}}(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}}$, $\sum_{\mathbf{x}\notin\mathbf{c}^\perp}(-1)^{f(\mathbf{x})\oplus s_2^{\mathbf{c}}(\mathbf{x})}(-1)^{\mathbf{u}\cdot\mathbf{x}} \in \{-2^{\frac{n-1}{2}}, 2^{\frac{n-1}{2}}\}$. Therefore, by similar argument as in (12) we obtain $|\mathcal{H}_{f\oplus s_2^{\mathbf{c}}}(\mathbf{u})| \in \{0, \sqrt{2}\}$, which implies that $f \oplus s_2^{\mathbf{c}}$ is semi–bent. ■

The converse of Theorem 6 is not true in general, since the argument used in Theorem 5 to prove the converse is not applicable when n is an odd integer. This is illustrated by the following example.

Example 7: Suppose $n = 3$. The function $s_2^{\mathbf{1}}(\mathbf{x}) = x_1x_2 + x_1x_3 + x_2x_3$. Let $f(\mathbf{x}) = x_1x_2$. It can be directly checked that $f + s_2^{\mathbf{1}}$ is semi–bent but $|\mathcal{U}_f^{\mathbf{1}}(0)| = \sqrt{2}$. Therefore, the spectrum of f is not flat with respect to the transform $U_{\mathbf{1}}$.

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?

The solution of this problem can be obtained as a corollary to Theorems 5 and 6.

Corollary 8: The maximum algebraic degree of a bent$_4$ Boolean function on n variables is $\lceil \frac{n}{2} \rceil$.

Proof: Suppose $f \in \mathcal{B}_n$ is a bent$_4$ function. Then by Theorems 5 and 6 the function $f \oplus s_2^{\mathbf{c}}$ is bent or semi–bent depending upon n being an even or an odd integer, respectively. It is known that the maximum algebraic degree of a bent or semi–bent function is $\lceil \frac{n}{2} \rceil$ whereas $s_2^{\mathbf{c}}$ is an at most quadratic function. This proves that the algebraic degree of f is upper bounded by $\lceil \frac{n}{2} \rceil$. ■

Remark 9: Equation (10) connects $U \in \{H, N\}^n$ to the approximation of a Boolean function by the functions of the form $s_2^{\mathbf{c}}(\mathbf{x}) \oplus \mathbf{u} \cdot \mathbf{x}$. This may endow some cryptographic significance to the spectra of f with respect to the transforms in $\{H, N\}^n$.

Acknowledgement: The authors would like to thank the anonymous referees for the detailed comments that significantly improved the technical, as well as the editorial quality of the paper.

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, LNCS 4893, pp. 9–23.

[4] C. Riera, M. G. Parker, "Generalized bent criteria for Boolean functions," *IEEE Trans. Inf. Theory* 52:9 (2006), 4142–4159.

[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, 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* 58:6 (2012), 4064–4072.

[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.

PLACE PHOTO HERE

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 Associate Professor at the Indian Institute of Technology Roorkee. His research interests are in Cryptology and Discrete Mathematics.

PLACE PHOTO HERE

Enes Pasalic received the Ph.D. degree in cryptology from Lund University, Lund, Sweden, in 2003. His main research interest is in cryptology and in particular design and analysis of symmetric encryption schemes. Since May 2003, he has been doing a postdoctoral research at INRIA (Versaille, France) crypto group, and later in 2005 at the Technical University of Denmark, Lyngby. He is currently with University of Primorska, FAMNIT and IAM, Koper, Slovenia. His main research interest is cryptography with emphasis on symmetric-key cryptography.

PLACE PHOTO HERE

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.