Malaysian Journal of Mathematical Sciences 10(S) February: 409–421 (2016)
Special Issue: The 3^{rd} International Conference on Mathematical Applications in Engineering 2014 (ICMAE'14)

MALAYSIAN JOURNAL OF MATHEMATICAL SCIENCES

Journal homepage: http://einspem.upm.edu.my/journal

Haar Spectrum of Bent Boolean Functions

H.M. Rafiq[1] and M.U. Siddiqi*[1]

[1]*Department of Electrical & Computer Engineering, Faculty of Engineering, International Islamic University Malaysia (IIUM)*

E-mail: umarsiddiqi@iium.edu.my
* *Corresponding author*

ABSTRACT

Bent Boolean functions play a very significant role in the design of strong symmetric cryptosystems. In this paper, we present an analysis of Bent functions in the Haar domain. We first present a brief overview of Bent Boolean functions and then derive expressions for the Haar spectrum of Bent functions. The Haar spectral coefficients of Bent functions are given in two ways namely; in terms of sub-intervals over the entire spectrum, as well as, individual spectral coefficients. Finally, we conclude the paper with a summary of findings and suggestions for further work for utilizing the results for design of secure cryptosystems.

Keywords: Cryptographic Boolean functions, Bent functions, Haar–transform, Walsh transform, Rademacher functions, Walsh orderings, Spectral Coefficients.

1. Introduction

Boolean functions have been of great interest in many fields of engineering and science, especially in cryptography (Thomas and Pantelimon, 2009, Carlet, 2010). They play a significant role in the security of conventional cryptographic systems for both block ciphers as well as stream ciphers. They can be viewed

as component parts of S-box (Thomas and Pantelimon, 2009, Neiderreiter, 2002) in a block cipher and are used in pseudo-random generators of stream ciphers as combining or filtering functions (Carlet, 2010, Read, 2007, Kui and Kwangjo, 2005, Courtois and Meier, 2003). Bent functions specifically, serve as a benchmark for high nonlinearity which is one of the most desirable properties for secure cryptographic functions. They can as well be synthesized to produce highly nonlinear functions. They have been defined, generalized, and presented in terms of the Walsh transform (Thomas and Pantelimon, 2009, Carlet, 2010, Zhang and Zheng, 1995).

In this paper we focus on the spectral transforms as methods of representation for the cryptographic Boolean functions. We look into the analogy between the Walsh and the Haar transforms which are known as fast Fourier-like transforms (Karpovsky and Astola, 2008, Thornton and Drechsler, 2001). With the advancement in technology over the years and compact methods of implementations, the Haar transform has progressively penetrated different fields of engineering and science, proving to be of significant use, and brought about attraction for further explorations on its applications (Khuri, 1997, Stanković and Falkowski, 2003, Rafiq and Siddiqi, 2009). The aim of this paper is to explore the Bent functions from the Haar domain perspective. In the process, we derive the general Haar spectral coefficients′ representation in terms of both: coefficients′ sub-intervals within the Haar spectrum, as well as, the individual spectral coefficients. Throughout the paper, we consider the Haar connection to Walsh functions in different orderings that include Strict-Sequency, Paley, and Hadamard orderings derived through Rademacher functions.

The paper is organized as follows. Section 2 presents an overview of Boolean functions including the spectral transform methods. The section also covers some of the known results to be employed in the later sections in addition to the Walsh definition of Bent functions. In section 3, we derive the Haar representation of Bent functions with two approaches based on representation of spectral coefficients′ sub-intervals as well as individual coefficients. Finally, in section 4, we present the conclusion of the paper and discussion on future work.

2. Overview

2.1 Boolean Functions

Boolean functions maps n binary inputs to a single binary output. More formally, this can be presented as follows (Thomas and Pantelimon, 2009,

Carlet, 2010):

$$f : \mathbb{F}_2^n \to \mathbb{F}_2 \quad \text{Maps} \quad (x_1, \ldots, x_n) \in \mathbb{F}_2^n \mapsto f(x) \in \mathbb{F}_2.$$

Such a function f is called a Boolean function of n variables. A Boolean function takes an n–dimensional vector$(x = (x_1, \ldots, x_n), x_i \in \mathbb{F}_2)$ over a two–element field as its domain, and outputs a single element from the same field as its range$(f(x))$. The set of all Boolean functions is denoted by B_n. Any $f \in B_n$ has a unique representation in each of the following forms (Carlet, 2010):

- The ordered tuple $T_f = \left(f(x^{(0)}), f(x^{(1)}), \ldots, f(x^{(2^n-1)})\right)$ is called the binary truth table of f(f taking values from the two–element set $\{0, 1\}$). The truth table gives the function's outputs for all the possible 2^n input combinations, where $x^{(0)} = (0, \ldots, 0)$ (the all–zeroes vector), $x^{(2^n-1)} = (1, \ldots, 1)$(the all–ones vector), and generally $x^{(k)}$ as the binary vector representation of the integer k, for $0 \leq k \leq 2^n - 1$. The relationship between x and k is simply given by $k = \sum_{i=1}^{n} 2^{n-i} x_i$.
- Sometimes instead of T_f, it may be more convenient to use the real valued function of f, which is called the sign function ξ or the polarity truth table (ξ takes values from the set $\{1, -1\}$). It is defined as $\xi(x) = (-1)^{f(x)} \equiv 1 - 2f(x)$, $\forall x \in \mathbb{F}_2^n$. The truth table of the sign function is called the sequence of f.
- The polynomial representation (ANF); the algebraic normal formal can be written uniquely as a sum (XOR) of products (AND):

  $$f(x) = a_0 \oplus a_1 x_1 \oplus \cdots \oplus a_1 x_1 \oplus a_{12} x_1 x_2 \oplus \cdots \oplus a_{12\cdots n} x_1 x_2 \cdots x_n$$

  where $a_i, x_i \in \mathbb{F}_2$.

The highest number of variables in the product terms of ANF gives the degree of f and is denoted by $\deg(f)$. For other representation such as NNF can be found in (Thomas and Pantelimon, 2009, Carlet, 2010).

The weight of a function is defined as the number of nonzero entries in T_f and is denoted by $\mathrm{w}(f)$. If the weight of a function is 2^{n-1}, that is the numbers of $0's$ and $1's$ are equal, then the function is called balanced.

Let $f, g \in B_n$. Then the distance between f and g is the distance between T_f and T_g on $\mathbb{F}_2^{2^n}$, which is denoted by $\mathrm{d}(f, g)$ and given by $\mathrm{d}(f, g) = \mathrm{w}(f \oplus g)$.

Linear and Affine Boolean Functions: A *linear* Boolean function, selected by $\omega \in \mathbb{F}_2^n$ is denoted by L_ω with the general expression $L_\omega = \omega_1 x_1 \oplus \omega_2 x_2 \oplus \cdots \oplus \omega_n x_n$.

Any function of the form $f = c \oplus L_\omega$ where $c \in \mathbb{F}_2$ is called *Affine* function. The set of affine functions contain all the linear functions.

2.2 Spectral Transforms

In this section we look at the main spectral transforms considered suitable for representation of Boolean functions. The two spectral transforms under context are the Walsh and Haar transforms. We also present some of the existing results that will be employed in the subsequent sections of the paper.

Throughout this paper, the following notations and abbreviations will be employed:

- M_Y: The Y spectral transform of M (Y is either Walsh(W) or Haar(H)).
- (*WH, WS, WP*): Walsh-Hadamard, Walsh-Sequency, Walsh-Paley orderings respectively.
- $\vec{y}_j$: The j-th row (Y function) in the respective transform matrix.
- $Y_j \cdot f$: The inner dot product between the elements of Y and f.

***Walsh-Hadamard Transform*:** The Walsh-Hadamard transform (ξ_{WH}) of a function ξ on $\mathbb{F}_2^n$ is given by (Thomas and Pantelimon, 2009, Carlet, 2010)

$$\xi_{WH}(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus x \cdot u} \equiv WH_u(x) \cdot \xi(x). \tag{1}$$

An equivalent representation of the transform in matrix form is (Thornton and Drechsler, 2001):

$$\xi_W = [W_n] \cdot [\xi]^t \tag{2}$$

where $[W_n] = [\vec{w}_j]$ is a $2^n \times 2^n$ Walsh transform matrix whose rows ($j \in [0, 2^n)$) consists of the Walsh functions ($\vec{w}_j$), and $[\xi]^t$ is a column vector of ξ.

***Haar Functions*:** The set of Haar functions ${H_l}^q$(simply H_j), forms a complete set of orthogonal rectangular basis functions (Karpovsky and Astola, 2008, Khuri, 1997). They are defined on the interval $[0, 2^n)$ as un–normalized

taking the values of 0 and ±1 as follows:

$$H_0{}^0(x) = H_0(x) = 1, \quad \forall x \in [0, 2^n)$$
$$H_j(x) = \begin{cases} 1, & (2q) \cdot 2^{n-l-1} \le x < (2q+1) \cdot 2^{n-l-1} \\ -1, & (2q+1) \cdot 2^{n-l-1} \le x < (2q+2) \cdot 2^{n-l-1} \\ 0, & \text{otherwise} \end{cases}, \tag{3}$$

where: l and q are degree and order of the Haar functions respectively, with $j = 2^l + q$ (for $j \ge 1$) and for each value of $l = 0, 1, \ldots, n-1$, we have $q = 0, 1, \ldots, 2^l - 1$.

***Haar Transform*:** The Haar transform (ξ_H) of ξ is defined by (Karpovsky and Astola, 2008, Khuri, 1997):

$$\xi_H(j) = \sum_{x=0}^{2^n-1} H_l{}^q(x) \cdot \xi(x) \equiv \sum_x H_j(x) \cdot \xi(x). \tag{4}$$

Equivalently in matrix form as (Thornton and Drechsler, 2001, Rafiq and Siddiqi, 2009):

$$\xi_H = [H_n] \cdot [\xi]^t \tag{5}$$

where: $[H_n] = \left[\vec{H}_j\right]$ is a $2^n \times 2^n$ Haar transform matrix whose rows consist of Haar functions (H_j's).

2.3 Known Results

Definition 2.1. *(Thomas and Pantelimon, 2009, Carlet, 2010)**Bent function:** An n–variable Boolean function ξ (resp. f) is said to be a Bent Boolean function if its Walsh spectrum satisfies the following condition:*

$$\xi_W(u) = W_u(x) \cdot \xi(x) = \pm 2^{\frac{n}{2}} \quad (\textit{resp. } f_W(u) = W_u(x) \cdot f(x) = \pm 2^{\frac{n}{2}-1}).$$

The Bent functions exist only for even number of variables and they are the furthest from the affine functions.

The following three lemmas (Lemma 2.1, 2.2, and 2.3) were presented by (Karpovsky and Astola, 2008).

Lemma 2.1. *Rademacher functions R_s, as subset of Walsh-Paley functions $WP_{\underbrace{\omega}}$ (with index's (ω) weight equals 1):*

$$R_s(x) = WP_{2^{s-1}}(x) = (-1)^{x_{s-1}} \qquad (s = 1, ..., n)$$

where: x_s, ω_s are determined by the binary expansions of $\overleftarrow{x}$ and $\overleftarrow{\omega}$ (Paley in bit-reverse)

$$\overleftarrow{x} = \sum_{s=0}^{n-1} x_s 2^{n-1-s};\ \overleftarrow{\omega} = \sum_{s=0}^{n-1} \omega_s 2^{n-1-s};\ WP_{\overleftarrow{\omega}}(x) = (-1)^{\sum_{s=0}^{n-1} \omega_{n-1-s} x_s}$$

with binary code arguments as: $x = (x_0, \ldots, x_{n-1})$ and $\omega = (\omega_0, \ldots, \omega_{n-1})$.

Lemma 2.2. *Relationship between the Haar functions $H_l^q(x)$ and the Rademacher functions $R_s(x)$ through Walsh-Paley functions:*

$$H_l^q(x) = \begin{cases} R_{l+1}, & x \in \left[q \cdot 2^{n-l}, (q+1) \cdot 2^{n-l}\right) \\ 0, & \textit{otherwise} \end{cases},\ l \in [0, n);\ q \in \left[0, 2^l\right).$$

Lemma 2.3. *Rademacher functions $R_s(x)$, as subset of Walsh-Hadamard functions WH_ω in connection to Paley-ordering:*

$$R_s(x) = WH_{2^{n-s}}(x) = (-1)^{x_{s-1}} \qquad (s = 1, \ldots, n)$$

where: x_s, ω_s are determined by the binary expansions of x and ω

$$x = \sum_{s=0}^{n-1} x_s 2^s;\ \omega = \sum_{s=0}^{n-1} \omega_s 2^s;\ WH_\omega(x) = (-1)^{\sum_{s=0}^{n-1} \omega_s x_s}$$

with binary code arguments as: $x = (x_0, \ldots, x_{n-1})$ and $\omega = (\omega_0, \ldots, \omega_{n-1})$.

Lemma 2.4. *The relationship between the Haar and Walsh sub-matrices is defined by (Falkowski and Rahardja, 1996, Fino, 1972):*

$$\left[SH_{2^n}^l\right] = 2^{-(l-1)} \cdot [WS_{2^{l-1}}] \cdot [P_{2^{l-1}}] \cdot \left[SWS_{2^n}^l\right] \quad (l = 1, \ldots, n)$$

where:

$\left[SWS_{2^n}^l\right]$ is a $2^{l-1} \times 2^n$ Walsh sub-matrix,
$\left[SH_{2^n}^l\right]$: The Haar sub-matrix $(2^{l-1} \times 2^n)$,
$[WS_{2^{l-1}}]$: Walsh matrix in sequency order $(2^{l-1} \times 2^{l-1})$, the transform matrix between the two spectral domains for the respective sub-intervals,
$[P_{2^{l-1}}]$: the permutation matrix $(2^{l-1} \times 2^{l-1})$ in the following form

$$\begin{bmatrix} 0 & \cdots & 1 \\ \vdots & \ddots & \vdots \\ 1 & \cdots & 0 \end{bmatrix} \text{ with } l = 1, 2, \ldots, n.$$

Lemma 2.5. *The relationship between the Walsh functions in different orderings ($WP, WS,$ and WH) is given through Rademacher functions by (Karpovsky and Astola, 2008, Falkowski and Sasao, 2005):*

$$WP_{2^l} \equiv WH_{2^{n-(l+1)}} \equiv WS_{2^{l+1}-1}$$

3. Haar Transform of Bent Functions

This section presents mathematical derivation of Haar transform of Bent functions. The first sub-section looks into the sub-intervals of Haar spectral coefficients while the second sub-section covers the individual spectral coefficients.

3.1 Spectral Coefficients within the Sub-Intervals

The sub-intervals under context are defined based on the respective degrees (l) of the Haar functions as $\left[2^l, 2^{l+1}-1\right]$. The following proposition is the extension and generalization of lemmas 2.2, 2.3 and 2.5 over the whole spectral interval domain ($[0, 2^n)$).

Proposition 3.1. *The sum of Haar functions for a given degree (l) over the respective orders (q) results into a Walsh function:*

$$\sum_q H_{2^l+q} = \begin{cases} WP_{2^l}, & \textit{Walsh in Paley Ordering} \\ WH_{2^{n-(l+1)}}, & \textit{Walsh in Hadamard Ordering} \\ WS_{2^{l+1}-1}, & \textit{Walsh in Sequency Ordering} \end{cases}$$

Proof.

$$\begin{aligned}
\sum_q H_{2^l+q} = \sum_{q=0}^{2^l-1} H_{2^l+q}(x) &= H_{2^l}(x) + H_{2^l+1}(x) + \cdots + H_{2^{l+1}-1}(x) \\
&\equiv \left[R_{l+1}(0), R_{l+1}(1), \ldots, R_{l+1}(2^{n-l}-1), 0, \ldots, 0\right] + \\
&\quad \left[0, \ldots, 0, R_{l+1}(2^{n-l}), , \ldots, R_{l+1}(2^{n-l+1}-1), 0, \ldots, 0\right] + \cdots \\
&\quad + \left[0, \ldots, 0, R_{l+1}(2^n - 2^{n-l}), , \ldots, R_{l+1}(2^n-1)\right] \quad \text{(Lemma 2.2)} \\
&\equiv \left[R_{l+1}(0), R_{l+1}(1), \ldots, R_{l+1}(2^n-1)\right] \\
&\equiv R_{l+1}(x) \\
&\equiv \begin{cases} WP_{2^l} \\ WH_{2^{n-(l+1)}} \\ WS_{2^{l+1}-1} \end{cases} \quad \text{(Lemma 2.1 2.3 and 2.5)}
\end{aligned}$$

□

Note: for the Walsh-Sequency function, the function's row $(2^{l+1}-1)$ represents the number of sign changes between positive-ones and negative-ones, which is given by the relation $(2 \cdot \frac{2^n}{2^{n-l}} - 1)$.

Theorem 3.1. *Let f be a Bent Boolean function (ξ, its corresponding sign function), then the sum of its Haar spectral coefficients f_H (ξ_H, corresponding polarity form) over the interval $2^l \leq j < 2^{l+1}$ is given by:*

$$\sum_j f_H(j) = \pm 2^{\frac{n}{2}-1} \quad \text{or} \quad \sum_j \xi_H = \pm 2^{\frac{n}{2}}$$

Proof.

$$\begin{aligned}
\sum_j f_H(j) &= f_H(2^l) + \cdots + f_H(2^{l+1}-1) \\
&= \sum_x H_{2^l}(x) \cdot f(x) + \cdots + \sum_x H_{2^{l+1}-1}(x) \cdot f(x) \\
&\equiv \left(\sum_{j=2^l}^{2^{l+1}-1} H_j \right) \cdot f \\
&\equiv \left(\sum_q H_{2^l+q} \right) \cdot f \\
&= \begin{cases} WP_{2^l}(x) \cdot f(x) \\ WH_{2^{n-(l+1)}} \cdot f(x) \\ WS_{2^{l+1}-1} \cdot f(x) \end{cases} \qquad \text{(Proposition 3.1)} \\
&= \begin{cases} f_{WP}(2^l) \\ f_{WH}(2^{n-(l+1)}) \\ f_{WS}(2^{l+1}-1) \end{cases} \qquad \text{(Walsh transform of } f\text{)} \\
&= \pm 2^{\frac{n}{2}-1} \quad \text{(Definition 2.1)}
\end{aligned}$$

□

For the case of the sign function (ξ), the arguments are straight forward as one employs it in place of f.

Example 3.1. *Consider the Bent function ξ with polarity truth table,* $[1, -1, -1, 1, 1, 1, -1, -1, 1, -1, 1, -1, 1, 1, 1, 1]$*, then its Haar and Walsh spectral transforms are given in the table below (see Table 1), where the distribution and relations between the spectral coefficients are obvious:*

Note that, the columns from left to right in Table 1 represents: the input variable, the sign function, the Walsh spectrum in order (Hadamard, Paley, and Sequency), and the Haar spectrum respectively.

Table 1: Haar and Walsh Spectrums

x	$\xi(x)$	$\xi_{WH}(x)$	$\xi_{WP}(x)$	$\xi_{WS}(x)$	$\xi_H(x)$
0	1	4	4	4	4
1	-1	4	-4	-4	-4
2	-1	4	-4	4	0
3	1	4	4	-4	-4
4	1	-4	4	-4	0
5	1	4	4	-4	4
6	-1	-4	-4	4	0
7	-1	4	-4	4	0
8	1	-4	4	4	2
9	-1	-4	-4	4	-2
10	1	4	4	4	0
11	-1	4	-4	4	0
12	1	4	4	4	2
13	1	-4	4	-4	2
14	1	-4	4	-4	0
15	1	4	4	4	0

3.2 Individual Spectral Coefficients

We approach the individual spectral coefficients through the relationship between the Haar and Walsh sub-matrices using Lemma 2.4. The derivation gives the relationship between each Haar spectral coefficient of Bent function and its Walsh counterpart (in Sequency ordering).

Proposition 3.2. *Multiplying a sub-matrix of a transform matrix by a function gives spectral coefficients corresponding to the rows of the sub-matrix:*

$$\textit{Haar: } \left[SH_{2^n}^l\right] \cdot [\xi]^t = [\xi_H(x)]^t \quad \textit{or} \quad \textit{Walsh: } \left[SWS_{2^n}^l\right] \cdot [\xi]^t = [\xi_{WS}(x)]^t$$

$$\textit{where: } x \in \left[2^{l-1}, 2^l\right).$$

Proof. The proof of the proposition is obvious as, each sub-matrix corresponds to the rows ($2^{l-1} \leq j \leq 2^l - 1$) of the respective main transform matrix, and in turn these rows represent the corresponding Haar/Walsh function to be multiplied by the given Boolean function, as well as, each row from a transform matrix produces a corresponding row in a column vector representing the spectrum. □

Now, multiplying each side of the equation in Lemma 2.4 by a Bent sequence $[\xi]^t$ and using Proposition 3.2 gives:

$$\begin{aligned}
&\left[SH^l_{2^n}\right]\cdot[\xi]^t = 2^{-(l-1)}\cdot[WS_{2^{l-1}}]\cdot[P_{2^{l-1}}]\cdot\left[SWS^l_{2^n}\right]\cdot[\xi]^t \quad (l=1,\ldots,n)\\
&[\xi_H(x)]^t = 2^{-(l-1)}\cdot[WS_{2^{l-1}}]\cdot[P_{2^{l-1}}]\cdot\left(\left[SWS^l_{2^n}\right]\cdot[\xi]^t\right) \ (x\in\left[2^{l-1},2^l\right)\\
&[\xi_H(x)]^t = 2^{-(l-1)}\cdot[WS_{2^{l-1}}]\cdot[P_{2^{l-1}}]\cdot\left([\xi_{WS}(x)]^t\right) \qquad (6)
\end{aligned}$$

Hence, Eqn. 6 gives the direct relation between each of the Haar spectral coefficients of n-variable Bent functions in terms of the Walsh coefficients.

Example 3.2. *Considering the same function given in the previous example then:*

$$\begin{aligned}
l=1 \Rightarrow \left[\xi_H(2^{1-1})\right] &= 2^{1-1}\cdot[WS_{2^{1-1}}]\cdot[P_{2^{1-1}}]\cdot\left[\xi_{WS}(2^{1-1})\right]\\
&= [WS_{2^0}]\cdot[P_{2^0}]\cdot[\xi_{WS}(1)] = [1]\cdot[1]\cdot[\xi_{WS}(1)]\\
&= -4\\
l=2 \Rightarrow \begin{bmatrix}\xi_H(2)\\ \xi_H(3)\end{bmatrix} &= 2^{-1}\cdot[WS_{2^1}]\cdot[P_{2^1}]\cdot\begin{bmatrix}\xi_{WS}(2)\\ \xi_{WS}(3)\end{bmatrix}\\
&= 2^{-1}\cdot\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\cdot\begin{bmatrix}\xi_{WS}(3)\\ \xi_{WS}(2)\end{bmatrix}\\
&= 2^{-1}\cdot\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\cdot\begin{bmatrix}-4\\ 4\end{bmatrix} = \begin{bmatrix}0\\ -4\end{bmatrix}\\
l=3 \Rightarrow \begin{bmatrix}\xi_H(4)\\ \xi_H(5)\\ \xi_H(6)\\ \xi_H(7)\end{bmatrix} &= 2^{-2}\cdot[WS_{2^2}]\cdot[P_{2^2}]\cdot\begin{bmatrix}\xi_{WS}(4)\\ \xi_{WS}(5)\\ \xi_{WS}(6)\\ \xi_{WS}(7)\end{bmatrix}\\
&= 2^{-2}\cdot\begin{bmatrix}1 & 1 & 1 & 1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\\ 1 & -1 & 1 & -1\end{bmatrix}\cdot\begin{bmatrix}\xi_{WS}(7)\\ \xi_{WS}(6)\\ \xi_{WS}(5)\\ \xi_{WS}(4)\end{bmatrix}\\
&= 2^{-2}\cdot\begin{bmatrix}0\\ 16\\ 0\\ 0\end{bmatrix} = \begin{bmatrix}0\\ 4\\ 0\\ 0\end{bmatrix}
\end{aligned}$$

$$
\begin{aligned}
l=4 \Rightarrow \begin{bmatrix} \xi_H(8) \\ \vdots \\ \vdots \\ \xi_H(15) \end{bmatrix} &= 2^{-3} \cdot [WS_{2^3}] \cdot [P_{2^3}] \cdot \begin{bmatrix} \xi_{WS}(8) \\ \vdots \\ \vdots \\ \xi_{WS}(15) \end{bmatrix} \\
&= 2^{-3} \cdot [WS_{2^3}] \cdot \begin{bmatrix} \xi_{WS}(15) \\ \vdots \\ \vdots \\ \xi_{WS}(8) \end{bmatrix} \\
&= 2^{-3} \cdot \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 4 \\ -4 \\ -4 \\ 4 \\ 4 \\ 4 \\ 4 \\ 4 \end{bmatrix} = \begin{bmatrix} 2 \\ -2 \\ 0 \\ 0 \\ 2 \\ 2 \\ 0 \\ 0 \end{bmatrix}
\end{aligned}
$$

The following section presents the conclusion of the paper.

4. Conclusion

In this paper we have presented a general Haar representation of Bent functions. In the process, we have derived the representation of Haar spectral coefficients both in terms of the individual coefficients, as well as in terms of coefficients′ sub-intervals. The individual coefficients were derived and represented in terms of Walsh coefficients in Strict-sequency ordering for the Walsh functions, while for the sub-interval representation, a general Haar spectral transform representation was derived based on the Walsh orderings of both Strict-sequency, Paley, and Hadamard. The Haar spectral characteristics are reflected upon its local behavior in relation to the transformed function. One important observation is that, the Walsh spectrum of Bent functions is flat in terms of absolute magnitude for each spectral coefficient. On the other hand, that same property is portrayed locally within the Haar spectral coefficients′ sub-intervals when such coefficients are considered together. This Haar spectral characterization is intended for further explorations in determining the nonlinearity measure of a given Boolean function which in turn is part of an ongoing work.

Acknowledgments

The work reported here has been partially funded by a grant from IIUM Endowment Fund.

References

Thomas, C. W. & Pantelimon, S. *Cryptographic Boolean Functions and Applications*. Academic Press, Elsevier Inc., 2009.

Carlet, C. Boolean functions for cryptography and error correcting codes. In Crama, Y. & Hammer, P. L., editors, *Boolean Models and Methods in Mathematics, Computer Science and Engineering*, pages 257–397. Cambridge University Press, 2010.

Neiderreiter, H., editor. *Coding Theory and Cryptology*. World Scientific Publishing Co. Inc., University Press Singapore, 2002.

Read, M. Explicable boolean functions. Dissertation submitted in part fulfillment for the degree of MEng. In Computer Systems and Software Engineering, Department of Computer Science, The University of York, 2007.

Kui, P., R. Jaemin & Kwangjo, K. On the Construction of Cryptographically Strong Boolean Functions with Desirable Trade-Off. *Journal of Zhejiang University Science*, 6A(5):358–364, 2005.

Courtois, N. T. & Meier, W. Algebraic attacks on stream ciphers with linear feedback. *Eurocrypt 2003, Springer*, LNCS 2656:345–359, 2003.

Zhang, X. M. & Zheng, Y. Gac–the criterion for global avalanche characteristics of cryptographic functions. *Journal of Universal Computer Science*, 1(5): 320–337, 1995.

Karpovsky, R. S., M. G. Stanković & Astola, J. T. *Spectral Logic and Its Applications for the Design of Digital Devices*. Oohn Wiley & Sons, Inc., 2008.

Thornton, D., M.A. Miller & Drechsler, R. Transformations amongst the walsh, haar, arithmetic and reed-muller spectral domains. *Proc 4th Intl. Workshop on Applications of Reed-Muller Expansion in Circuit Design*, pages 215–225, 2001.

Khuri, S. Computing with haar functions. *Proceedings of the 1997 ACM Symposium on Applied Computing*, pages 223–227, 1997.

Stanković, R. & Falkowski, B. The haar wavelet transform: Its status and achievement. *Computers and Electrical Engineering, An International Journal*, 29:25–44, 2003.

Rafiq, H. M. & Siddiqi, M. U. Haar transformation of linear boolean function. *Proceeding of IEEE International Conference on Signal Processing Systems*, pages 802–805, 2009.

Falkowski, B. J. & Rahardja, S. Walsh-like functions and their relations. *IEEE Proceedings on Vision, Image and Signal Processing*, 143(5):279–284, 1996.

Fino, B. Relations between haar and walsh/hadamard transforms. *Proc. IEEE*, 60:647–648, 1972.

Falkowski, B. & Sasao, T. Unified algorithm to generate walsh functions in four different orderings and its programmable hardware implementations. *IEE Proc., Vis. Image Signal Process.*, 152(6):819–826, 2005.