Journal of Engineering and Computer Sciences
Qassim University, Vol. 7, No. 2, pp. 73-112 (July 2014/Shaban 1435H)

The Walsh Spectrum and the Real Transform of a Switching Function: A Review with a Karnaugh-Map Perspective

Ali Muhammad Ali Rushdi and Fares Ahmad Muhammad Ghaleb

Department of Electrical and Computer Engineering,

King Abdulaziz University,

P.O. Box 80204, Jeddah 21589, Saudi Arabia.

arushdi@kau.edu.sa

(Received 03/02/2014; Accepted for publication 24/04/2014)

Abstract. Using a Karnaugh-map perspective, this paper investigates the definitions, exposes the properties, introduces new computational procedures, and discovers interrelationships between the Walsh spectrum and the real transform of a switching function. Appropriate Karnaugh maps explain the computation of Walsh spectrum as defined in cryptology. An alternative definition of this spectrum adopted in digital design and related areas is then presented together with procedures for its matrix computation. Then, the real transform of a switching function is defined as a real function of real arguments. This definition is clearly distinguished from similar ones such as the multi-linear form or the arithmetic transform. The real transform is visualized in terms of a particular version of the Karnaugh map called the probability map. Karnaugh maps are also used to demonstrate the computation of the spectral coefficients adopted in digital design as the weight of the switching function and weights of its subfunctions or restrictions. These maps match the earlier ones for the spectrum used in cryptology. Novel relations between the Walsh spectrum and the real transform are utilized in formulating two simplified methods for computing the spectrum via the real transform with some aid offered by Karnaugh maps. Finally, a solution is offered for the inverse problem of computing the real transform in terms of the Walsh spectrum.

Key Words. Switching functions, Walsh spectrum, Spectral coefficients, Real transform, Karnaugh maps, Probability maps.

1. Introduction

The two-valued Boolean functions (switching functions) are the simplest interesting multivariate functions [1]. They have a wide range of engineering applications, including those of coding [1-3], cryptology [1-5], digital design [6-8], system reliability [9-19], syllogistic reasoning [20-30], and operations research [31]. Switching functions have many useful representations which vary in their suitability for handling different applications and in the kind of illumination they cast on different functional properties. Notable among these presentations are:

(a) the Karnaugh map [32] which is a very powerful manual tool that provides pictorial insight about the various functional properties and procedures when the number of variables involved is small,

(b) the Walsh spectrum [33-44], which reveals information about the function that is much more global in nature, and has prominent applications in cryptology as well as digital design and related areas such as signal processing, information transmission, function classification, and circuit analysis, design, synthesis and testing, and

(c) the real or probability transform [37, 45-50], which is useful in many areas such as that of system reliability.

The aim of this paper is to investigate the definitions, expose the properties, introduce new computational procedures and discover interrelationships between the Walsh spectrum and the real transform. This aim is achieved using a Karnaugh-map perspective, which makes the exposition of the complex concepts encountered much easier to understand. We strive to settle certain sources of confusion, such as (a) a purported discrepancy between the definition of the Walsh transform used in cryptology and that used in digital design, (b) the existence of different Walsh spectra for the typical encoding {0,1} of the output of the switching function, or for its decoding to polar encoding {+1, − 1}, and (c) the nature of the domain and range of the real transform and whether this transform is $\mathrm{R}^n \rightarrow \boldsymbol{R}$, $[0.0, 1.0]^n \rightarrow [0.0, 1.0]$, or $\{0, 1\}^n \rightarrow \{0, 1\}$.

The organization of the rest of this paper is as follows. Section 2 presents some preliminary definitions needed in subsequent sections. Section 3 exposes via appropriate Karnaugh maps the computation of the Walsh spectrum as used in cryptology. Section 4 presents the definition and matrix computation of the Walsh transform as used by the digital-design community. Section 5 introduces the real transform, explains its relation with the arithmetic transform, and visualizes it in terms of a particular version of the Karnaugh map called the probability map. Section 6 computes the first spectral coefficient, i.e., the first element in the Walsh spectrum adopted in digital design, which is the weight of the switching function. Section 7 utilizes the results of Section 6 in computing the rest of the spectral coefficients as weights of subfunctions of the original function. These computations are demonstrated on Karnaugh maps and are shown to match the earlier map computations in Section 3. Sections 8 and 9 present novel relations between the Walsh spectrum and the real transform, and subsequently give two simplified methods for computing the Walsh spectrum via the real transform with some aid offered by Karnaugh maps. Section 10 discusses the inverse problem for those in Sections 8 and 9, as it computes the real transform in terms of the Walsh spectrum. Section 11 concludes the paper.

2. Preliminary Definitions

A switching function on *n* variables may be viewed as a mapping from $\{0, 1\}^n$ into $\{0, 1\}$. We interpret a switching function $f(X) = \boldsymbol{f}(X_1, X_2, \cdots, X_{n-1}, X_n)$ as the output column of its truth table $\boldsymbol{f}$, i.e., a binary vector of length 2^n

$$\boldsymbol{f} = [f(0,0,\ldots 0,0) \quad f(0,0,\ldots,0,1) \quad f(0,0,\ldots,1,0) \ \ldots \ f(1,1,\ldots,1,1)]^T \quad \textbf{(1)}$$

For switching functions $f_1(X)$, and $f_2(X)$ of the same number of variables n, and of truth table vectors f_1 and f_2, we denote by $\#(f_1 = f_2)$ (respectively, $\#(f_1 \neq f_2)$) the number of places where the vectors f_1 and f_2 are equal (respectively, unequal). The Hamming distance between the functions f_1 and $\boldsymbol{f}_2$ is denoted by $d(f_1, f_2)$, *and* given by

$$d(f_1, f_2) = \#(f_1 \neq f_2) = 2^n - . \quad \textbf{(2)}$$

We also define the *weight difference wd* between the two functions f_1 and f_2 as

$$wd(f_1, f_2) = \#(f_1 = f_2) - \#(f_1 \neq f_2), \quad \textbf{(3)}$$

$$= 2^n - 2\, d(f_1, \boldsymbol{f}_2). \quad \textbf{(4)}$$

Also, the Hamming weight or simply the weight of a switching function $f(X)$, is the number of ones in its truth-table vector f. This is denoted by $wt(f)$. An *n*-variable function *f* is said to be balanced if its output column in the truth table contains equal numbers of *0's* and *1's* (*i.e.,* $wt(\boldsymbol{f}) = 2^\wedge(\boldsymbol{n}-\mathbf{1})$). Note that the weight difference $wd(f_1, f_2)$ is not the difference between the weights of f_1 and f_2.

A switching function can also be viewed as a function on the Boolean ring [21], or as one over the simplest finite or Galois field, namely the binary field *GF(2).* The addition operator over *GF(2)* is usually denoted by +. However, in this paper, we will denote it by the symbol $\oplus$ of the *EXCLUSIVE− OR* operator in switching algebra. We will retain the symbol + for its standard meaning of real addition. In term of the $\oplus$ operator, equations (2) and (4) can be rewritten as

$$d(f_1, f_2) = wt(f_1 \oplus f_2), \quad \textbf{(2a)}$$

$$wd(f_1, f_2) = 2^n - 2\, wt(f_1 \oplus f_2). \quad \textbf{(4a)}$$

An *n*-variable switching function $f(X) = f(X_1, X_2, \cdots, X_{n-1}, X_n)$ can be considered to be a multivariate polynomial over *GF(2).* This polynomial can be expressed as a sum of k^{th}-order products $(0 \le k \le n)$ of distinct variables. More precisely, $f(X_1, X_2, \cdots, X_{n-1}, X_n)$ can be written as [51]

$$f(\boldsymbol{X}) = a_0 \bigoplus_{i=1}^{i=n} a_i X_i \bigoplus_{1 \le i < j \le n} a_{ij} X_i X_j \oplus \cdots \oplus a_{12\cdots n} X_1 X_2 \cdots X_n, \quad \textbf{(5)}$$

or in expanded form as

$$f(X) = a_0 \oplus (a_1 X_1 \oplus a_2 X_2 \ (\cdots (\ a_n X_n) \oplus (a_{12} X_1 X_2 \oplus a_{13} X_1 X_3 \quad \textbf{(6)}$$
$$(\cdots (\ a_{(n-1)n}\ X\_((n-1))\ X\_\boldsymbol{n}) \ (\cdots (\ a\_(12\cdots n)\ X_1 X_2 \cdots X_n\ ,$$

3. Walsh Spectrum for Cryptographic Studies

The Walsh spectrum of an *n*-variable switching function is based on a set of orthogonal functions defined by Walsh [52]. The spectrum is usually called the Walsh-Rademacher spectrum, because the Walsh functions are an extension of a set of functions defined by Rademacher [53]. The spectrum is also called the Walsh-Hadamard spectrum, because among several orderings of the Walsh functions, the most prominent one is the one due to Hadamard [42]. The Hadamard ordering is the one to be adopted herein. Two equivalent (albeit apparently different) mathematical descriptions of the Walsh transform appear in the literature. The description typically adopted in cryptology is considered in this section, while the one typically used in digital design and related areas is deferred to Section 4.

Let $X = (X_1, \quad X_2, \cdots, X_n)$ and $w = (w_1, \quad w_2, \cdots, w_n)$ both belong to $\{0,1\}^n$, and let $L_w(X)$ denote the linear switching function on the n variables X given by

$$L\_w\ (X) = X.w = X\_1\ \ w\_1\ \ (\ \ X\_2\ \ w\_2\ \ (\cdots (\ [\![X]\!]\_n\ \ w\_n\ . \tag{7}$$

Let *f*(X *)* be a Switching function on the *n* variables X . Then the Walsh transform of *f(X)* is a real-valued function $W_f(w)$ over $\{0, 1\}^n$ that is defined as

$$W_f(\boldsymbol{w}) = \sum_{X \in \{0,1\}^n} (-1)^{(f(X) \oplus L_w(X))} \tag{8}$$

$$= \sum_{X \in \{0,1\}^n} (1 - 2(f(\boldsymbol{X}) \oplus L_{\boldsymbol{w}}(\boldsymbol{X}))) = 2^n - 2\, wt\big(f(X) \oplus L_w(\boldsymbol{X})\big) \tag{9}$$

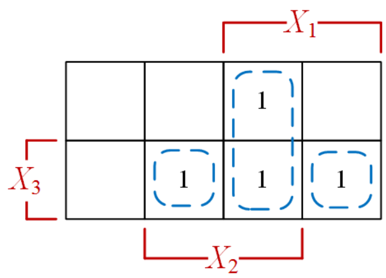
Note that *f*(X *)* $\oplus$ $L_w(X) = 0$ when *f*(X *)* $=$ $L_w(X)$ (for which $(-1)^{(f(X) \oplus L_w(X))} = 1$), while *f*($X$ *)* $\oplus$ $L_w(X) = 1$ when *f*(X *)* $\neq$ $L_w(X)$ (for which $(-1)^{(f(X) \oplus L_w(X))} = -1$). Thanks to (4a) and (9), the Walsh spectrum $W_f(w)$ can be interpreted as the weight difference between $f(X)$ and $L_w(X)$, i.e.,

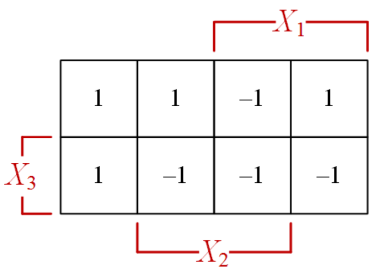
$$W_f(w) = \boldsymbol{w}\mathrm{d}\big(f(X), L_w(X)\big)\ . \tag{10}$$

Example 1:

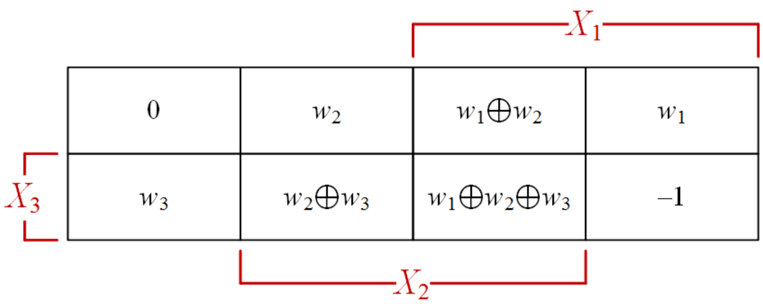
$$f(X) = f(X\_\mathbf{1}, X\_2, X\_\mathbf{3}\ ) = X\_\mathbf{1}\ X\_\mathbf{2}\ \ (\ [\![\ X]\!]\_\mathbf{2}\ X\_3\ \ (\ [\![\ X]\!]\_\mathbf{1}\ X\_3\ , \tag{11}$$

The 2-out-of-3 function is represented by the Karnaugh map in Fig. 1(a) for the usual {0, 1} encoding for its truth values. Figure 1(b) represents the same function when the truth table values {0, 1} are recoded to {+1, − 1}. Figure 1(c) shows a Karnaugh map representation for the linear function $L_w(X)$ of 3 variables.





(a) $f(X)$ with values $\in \{0, 1\}$ and disjoint coverage. Typically, 0 entries are left blank. **(b) $f(X)$ with values recoded to {+1, − 1}.**



(C) $L_w(X)$

Fig. (1). Karnaugh-map representations for the 2-out-of-3 function with different encodings, and the 3-variable linear function $L_w(X)$

Figures 2 is a Karnaugh map that represents $(1 - \mathbf{2}(\boldsymbol{f}(\boldsymbol{X}) \oplus L\_w\,(\boldsymbol{X}))$ as a function of ***X***. Entries of this map add to give the Walsh transform, namely

$$W_f(w) = 1 + (1 - 2\,w_1) + (1 - 2\,w_2) + (1 - 2\,w_3) + (1 - \mathbf{2}\,(1 \oplus w_1 \oplus w_2)) + (1 - 2\,(1 \oplus w_1 \oplus w_3)) + (1 - \mathbf{2}\,(1 \oplus w_2 \oplus w_3)) + (1 - 2\,(1 \oplus w_1 \oplus w_2 \oplus w_3)). \quad \textbf{(12)}$$

			X_1	X_1
	1	$1-2w_2$	$1-2(1\oplus w_1\oplus w_2)$	$1-2w_1$
X_3	$1-2w_3$	$1-2(1\oplus w_2\oplus w_3)$	$1-2(1\oplus w_1\oplus w_2\oplus w_3)$	$1-2(1\oplus w_1\oplus w_3)$
		X_2	X_2	

Fig. (2). Particular values of $\left(1-2\left(f(X)\oplus L_w(X)\right)\right)$ for specific values of X

Finally, Fig. 3 obtains the Walsh transform of the function $f(X)$ in the form of a Karnaugh map of map variables $w_1, w_2,$ and w_3. A temporary entry of each cell of this map is a specific instant of the map in Fig. 2 with entries computed for pertinent values of $w_1, w_2,$ and w_3. Each of these entries is either +1 or $-$ 1. Initially, the temporary entry in the all-0 cell $((w_1, w_2, w_3) = (0, 0, \mathbf{0}))$ is the $f(X)$ map in Fig. 1(b). The temporary entries in other cells are derived from this initial entry by switching each 1 to -1 and each -1 to 1 for values within the loops shown. Note that this switching action is cumulative for overlapping loops. Now, the actual intended entries of the large map in Fig. 3 result by adding the entries within the smaller maps in each cell. Figure 3 therefore represents $W_f(w)$ as a pseudo-Boolean function of w [31, 32]. This figure can now be read to give the following expression for the Walsh transform

$$W_f(w) = W_f(w_1, w_2, w_3) = \tag{14a}$$

$$S.w = 4\,\overline{w}_1\overline{w}_2 w_3 + 4\overline{w}_1 w_2 \overline{w}_3 + 4 w_1 \overline{w}_2 \overline{w}_3 - 4 w_1 w_2 w_3,$$ where

$$w = [\overline{w}_1\overline{w}_2\overline{w}_3 \;\; \overline{w}_1\overline{w}_2 w_3 \;\; \overline{w}_1 w_2\overline{w}_3 \;\; \overline{w}_1 w_2 w_3 \;\; w_1\overline{w}_2\overline{w}_3 \;\; w_1\overline{w}_2 w_3 \;\; w_1 w_2\overline{w}_3 \;\; w_1 w_2 w_3]^T. \tag{13}$$

$$S = [0 \quad 4 \quad 4 \quad 0 \quad 4 \quad 0 \quad 0 \quad -4]^T, \tag{14b}$$

$$= [s_0 \quad s_3 \quad s_2 \quad s_{23} \quad s_1 \quad s_{13} \quad s_{12} \quad s_{123}]^T.$$

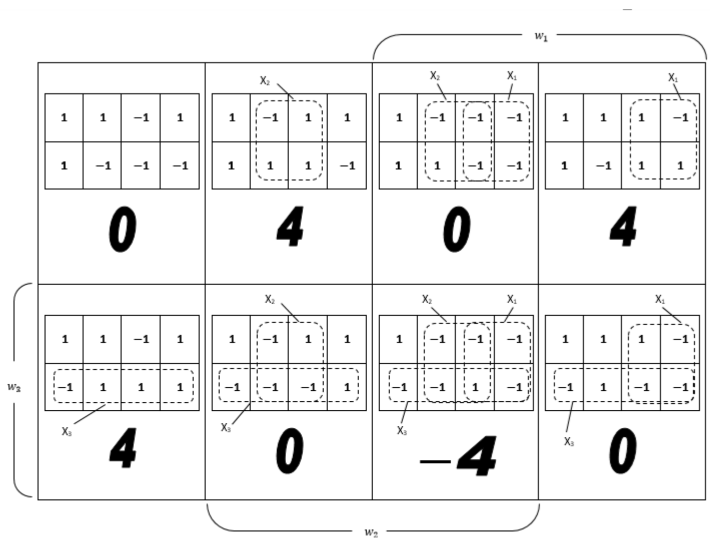


Fig. (3). A Karnaugh-map evaluation of the Walsh transform of $f(X)$ in Fig. 1(b)

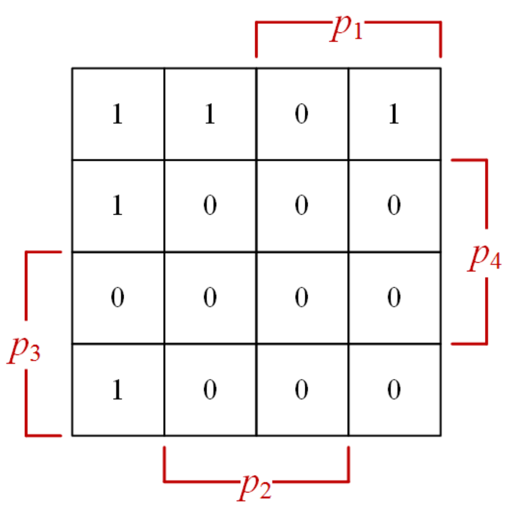


Fig. (4). The truth table of $R(p)$ in (49), cast in the form of a probability map

4. Walsh Spectrum for Digital Logic

The Hadamard ordering of the Walsh spectrum has a simple recursive structure of a $2^n \times 2^n$ transform matrix, T_n, which is called a Hadamard matrix. This matrix relates the Walsh spectrum vector R (which is a vector of 2^n spectral coefficients) to the truth-table vector f of $f(X)$, which is a vector of 2^n elements belonging to $\{0, 1\}$ that express the functional values of the minterms or discriminators of $f(X)$ as in (1). This is called the R-encoding in [42]. In an alternative formulation, the Walsh spectrum is given by a vector S which is T_n multiplied by the polar truth-table vector F of $f(X)$, namely

$$F = 1 - 2f \,, \tag{14}$$

Where **1** is a vector of 2^n elements, each of value 1. Note that in F, logic 0 is coded as $+1$ and logic 1 is coded as -1, an encoding called the *S*-encoding in [42]. Figures 1(a) and 1(b) are examples of R-encoding and S-encoding for the 2-out-of-3 function. In summary, we have:

$$R = T_n f \,, \tag{15}$$

$$S = T_n F \,. \tag{16}$$

The Hadamard matrix T_n in (15) and (16) is a $2^n \times 2^n$ matrix with entries belonging to $\{+1, -1\}$ and a recursive structure given by

$$T_0 = [1] \,, \tag{17}$$

$$T_n = \begin{bmatrix} T_{n-1} & T_{n-1} \\ T_{n-1} & -T_{n-1} \end{bmatrix}. \tag{18}$$

The rows of T_n are the set of 2^n *n*-variable Walsh functions [42]. The matrix T_n is symmetric $([T\_n]^T = T\_n)$, orthogonal $(T_n T_n^T = I)$ and idempotent $(T_n^2 = I)$. The matrix T_n is also quasi-involutary (quasi self-inverse). It is equal to its own inverse to within a multiplicative constant $(T_n^{-1} = 2^{-n} T_n)$.

The matrix T_n can be equivalently defined via Kronecker products [42, 51, 54-57] as follows

$$T_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad (19)$$

$$\boldsymbol{T}_n = \boldsymbol{T}_1 \otimes \boldsymbol{T}_{n-1} = \boldsymbol{T}_{n-1} \otimes \boldsymbol{T}_1 \quad , \quad (20)$$

where (20) could be rewritten as

$$\boldsymbol{T}_n = \otimes_{k=1}^{n} \ \boldsymbol{T}_1. \quad (21)$$

In the following, we will stress the S-encoding and use S as our Walsh spectrum, unless otherwise stated. This choice agrees with the definition used in cryptography studies. The Walsh spectrum R for the *R-encoding* is related to S. Thanks to (14) and its inverse relation

$$f = \frac{1}{2}(1 - F), \quad (22)$$

we have the following interrelationships between the elements of R and those of S

$$\boldsymbol{r}_0 = \frac{1}{2(2^n - \boldsymbol{s}_0)}, \quad (23)$$

$$r_i = -\frac{1}{2} s_i, \qquad \boldsymbol{i} \neq \boldsymbol{0}, \quad (24)$$

$$\boldsymbol{s}_0 = 2^n - 2\boldsymbol{r}_0 \quad (25)$$

$$s_i = -2r_i \, , \qquad \boldsymbol{i} \neq \boldsymbol{0} \, . \quad (26)$$

In passing, we note that the truth-table vector f represents the function $f(X)$ via a basis vector X_n, i.e.,

$$f(X) = f.X_n, \quad \textbf{(27)}$$

where X_n is expressed recursively as

$$X_0 = [1], \quad \textbf{(28a)}$$

$$\boldsymbol{X}_n = \boldsymbol{X}_{n-1} \otimes \begin{bmatrix} \overline{X}_n \\ X_n \end{bmatrix}. \quad \textbf{(28b)}$$

5. The Real Transform of a Switching Function

Various forms of the real transform (also called the probability or arithmetic transform) are discussed in [37, 45-50]. The following definition is taken from [37], and the following exposition relies on results obtained in [18, 36, 37, 47, 48].

The real transform $R(p) = \boldsymbol{R}(p_1, p_2, \cdots, p_n)$ of a switching function f (X), denoted by $R\ell(f),$ is defined to possess the following two properties:

a) *R(**p**)* is a multi-affine continuous real function of continuous real variables $p = [p_1 \; p_2 \cdots p_n]^T,$ i.e., *R* is a first-degree polynomial in each of its arguments p_i .

b. *R(**p**)* has the same "truth table" as f (X), i.e.

$$R(p = t_j) = \boldsymbol{f}(X = t_j), \qquad \text{for } j = 0, 1, \ldots, (2^n - 1), \quad \textbf{(29)}$$

where $\mathbf{t}_j$ is the jth input line of the truth table ; $\mathbf{t}_j$ is an *n*-vector of binary components such that

$$\sum_{i=1}^{n} 2^{n-i} t_{ji} = j, \qquad \text{for } j = 0, 1, \ldots, (2^n - 1). \quad \textbf{(30)}$$

We stress that property (b) above does not suffice to produce a unique $R(p)$ and it must be supplemented by the requirement that $R(p)$ be multiaffine to define $R(p)$ uniquely [47]. We also note that if the real transform R and its arguments p are restricted to discrete binary values (i.e., if $R\colon \{0, \quad 1\}^n \to \{0, \quad 1\}$) then R becomes the multilinear form of a switching function [58, 59], typically referred to as the structure function [60, 61] in system reliability.

The definition above for $R(p)$ implies that it is a function from the n-dimensional real space to the real line $(R(p): R^n \to R)$. Though both R and $\boldsymbol{p}$ could be free real values, they have a very interesting interpretations as probabilities, i.e., when restricted to the [0.0, 1.0] and $[0.0, 1.0]^n$ real intervals. An important property of the real transform $R(\boldsymbol{p})$ is that if its vector argument or input $\boldsymbol{p}$ is restricted to the domain within the n-dimensional interval $[\,0.0, 1.0\,]^n$, i.e. if $0.0 \le p_i \le 1.0$ for $1 \le i \le n$, then the image of $R(\boldsymbol{p})$ will be restricted to the unit real interval [0.0, 1.0].

The probability transform is a bijective (one-to-one and onto) mapping from the set of switching functions to the subset of multi-affine functions such that if the function's domain is the power binary set $\{0, 1\}^n$ then its image belongs to the binary set {0, 1}. Evidently, an $R(\boldsymbol{p})$ restricted to binary values whenever its arguments are restricted to binary values can produce the "truth table" that completely specifies its inverse image $f(X)$ via (29). On the other hand, a multi-affine function of n variables is completely specified by 2^n independent conditions [47], e.g., the ones in (29). In fact, such a function can be expressed by the finite multivariable Taylor's expansion [48]

$$R(\mathbf{p}) = R(\boldsymbol{\alpha}) + \sum_{i=1}^{n} (\partial R/\partial p_i)_{\mathbf{p}=\boldsymbol{\alpha}} (p_i - \alpha_i) + \sum\sum_{1\le i<j\le n} (\partial^2 R/\partial p_i \partial p_j)_{\mathbf{p}=\boldsymbol{\alpha}} (p_i - \alpha_i)(p_j - \alpha_j) +$$

$$\sum\sum\sum_{1\le i<j<k\le n} (\partial^3 R/\partial p_i \partial p_j \partial p_k)_{\mathbf{p}=\boldsymbol{\alpha}} (p_i - \alpha_i)(p_j - \alpha_j)(p_k - \alpha_k) + \ldots\ldots\ldots.$$

$$+ (\partial^n R/\partial p_1 \partial p_2 \ldots \partial p_n)_{\mathbf{p}=\boldsymbol{\alpha}} (p_1 - \alpha_1)(p_2 - \alpha_2)\ldots\ldots(p_n - \alpha_n). \quad \mathbf{(31)}$$

The expansion (31) has $\sum_{m=0}^{n} \binom{n}{m} = 2^n$ coefficients which are functions of the expansion point $\boldsymbol{p} = \boldsymbol{\alpha}$. These coefficients can be viewed to form a spectrum for the switching function $f(X) = R\ell^{-1}(R(p))$. Note that the partial derivative of R in (31) w.r.t certain variables p_i is independent of such variables, and therefore this derivative is not affected by the assignments $p_i = \alpha_i$ which are part of the restriction $p = \alpha$. In particular, the nth-order derivative $(\partial^n R/\partial p_1\ p_2 \cdots \partial p_n)$ is a constant, and its restriction via $p = \alpha$ might be omitted.

The real transform as defined above is related to the vector A of the arithmetic transform in [49] as follows. The vector A is simply a representation of $R(p)$ on a basis P_n, namely

$$R(p) = A \,.\, P_n, \quad \mathbf{(32)}$$

where P_n is defined recursively as

$$P_0 = [1], \quad \textbf{(33)}$$

$$P_n = P_{n-1} \otimes \begin{bmatrix} 1 \\ p_n \end{bmatrix}. \quad \textbf{(34)}$$

For example,

$$P_1 = [1 \quad p_1]^T ,$$
$$P_2 = [1 \quad p_2 \quad p_1 \quad p_1p_2]^T ,$$
$$P_3 = [1 \quad p_3 \quad p_2 \quad p_2p_3 \quad p_1 \quad p_1p_3 \quad p_1p_2 \quad p_1p_2p_3]^T$$

In [49], the vector A is obtained from the truth-table vector f via

$$A = V_n \boldsymbol{f} , \quad \textbf{(35)}$$

where V_n is defined recursively as

$$V_0 = [1], \quad \textbf{(36)}$$

$$V_n = \begin{bmatrix} V_{n-1} & 0 \\ -V_{n-1} & V_{n-1} \end{bmatrix}. \quad \textbf{(37)}$$

Alternatively V_n can be defined as a Kronecker product via:

$$V_1 = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}, \quad \textbf{(38)}$$

$$V_n = V_1 \otimes V_{n-1} . \quad \textbf{(39)}$$

The inverse of V_n is Q_n defined by

$$Q_0 = [1] \text{ ,}\mathbf{(40)}$$

$$Q_n = \begin{bmatrix} Q_{n-1} & 0 \\ Q_{n-1} & Q_{n-1} \end{bmatrix} \text{.}\mathbf{(41)}$$

or equivalently by

$$Q_1 = \begin{bmatrix} \mathbf{1} & \mathbf{0} \\ \mathbf{1} & \mathbf{1} \end{bmatrix} \text{,}\mathbf{(42)}$$

$$Q_n = Q_1 \otimes Q_{n-1} \text{ .}\mathbf{(43)}$$

In the following, we show that the real transform of a switching function is readily obtained via a disjoint sum-of-products expression of it. This observation in very useful since there are literally hundreds of algorithms for producing such an expression (see, e.g., [9-19]).

Theorem 1:

Let the switching function $f(X)$ be expressed by the disjoint sum-of-products (s-o-p) form

$$f\,(\boldsymbol{X}) = \vee_{k=1}^{m} D_k, \qquad \mathbf{(44)}$$

Where

$$D_i \wedge D_j = 0 \qquad \forall \text{ i, j ,} \qquad \mathbf{(44a)}$$

$$D_k = \left(\wedge_{i\in I_{k_1}} X_i\right) \left(\wedge_{i\in I_{k_2}} \overline{X}_i\right), \qquad \forall \text{ k,} \qquad \mathbf{(44b)}$$

and none of the products D_k has any redundant literal (redundant literals can be eliminated via idempotency of the AND operator $(X\_i \; (X\_i \;\; = X\_i \;)$. Here, I_{k_1} and I_{k_2} are the sets of indices for uncomplemented literals and complemented literals in the product D_k . Now, we let the expression

$$\mathrm{T}(\mathrm{f}) = \sum_{k=1}^{m} \mathrm{T}(\mathrm{D}_k), \tag{45}$$

Where

$$T(D_k) = \left(\prod_{i \in I_{k_1}} p_i\right) \left(\prod_{i \in I k_2} (1 - p_i)\right) \qquad \forall k, \tag{46}$$

be obtained from (44) by replacing the AND operator by the multiplication operator, the *OR* operator by the addition operator, each un-complemented variable X_i by p_i, and each complemented variable $\overline{X}_i$ by $(1- p_i)$. Then $\mathrm{T}(\mathrm{f}) = \mathrm{R}\ell(\mathrm{f})$.

Proof: For j = 1, 2,.. ., n, the degree of p_j in $T(D_k)$ for k = 1, 2, ..., m is at most 1. Hence, its degree in T(f) is also at most 1, i.e. T(f) is a first-degree polynomial in p_j. This means that T(f) is a multi-affine function of $\boldsymbol{p}$. Furthermore, for each line of the “truth table” $\boldsymbol{X} = \boldsymbol{p} = \boldsymbol{t}_j$, $T(D_k)$ has the same value (0 or 1) as D_k. If $f(\boldsymbol{t}_j) = 0$, then all products D_k are 0, all $T(D_k)$ are 0, and $T(f)$ is 0. If $f(\boldsymbol{t}_j) = 1$, then exactly one product D_k is 1 since the products are disjoint. Only the transformed product $T(D_k)$ originating from this particular D_k is 1, while all other transformed products are 0. Hence, $T(f)$ is 1. Thus, f and $T(f)$ have the same truth table. Since $T(f)$ is a multi-affine function with the same truth table as f, it is equal to $\mathrm{R}\ell(\mathrm{f})$.

Example 2:

Let us consider a switching function

$$\mathrm{f}(\mathrm{X}) = \overline{X}_1\overline{X}_2\overline{X}_3 \vee \overline{X}_1\overline{X}_2\overline{X}_4 \vee \overline{X}_1\overline{X}_3\overline{X}_4 \vee \overline{X}_2\overline{X}_3\overline{X}_4 \,. \tag{47}$$

which represents the failure of a 3-out-of-4:F (2-out-of-4:G) system [62, 63]. This function in a disjoint s-o-p form is [62]:

$$\mathrm{f}(\mathrm{X}) = \overline{X}_1\overline{X}_2\overline{X}_3 \vee \overline{X}_1\overline{X}_2 X_3\overline{X}_4 \vee \overline{X}_1 X_2\overline{X}_3\overline{X}_4 \vee X_1\overline{X}_2\overline{X}_3\overline{X}_4 \tag{48}$$

The real transform of $f(\boldsymbol{X})$ is obtained by replacing the AND operations and the OR operations in (48) by their algebraic counterparts of addition and multiplications, and replacing variables X_i and $\overline{X}_i$ by their expectations p_i and $(1- p_i)$, via:

$$R(\mathbf{p}) = (1 - p_1)(1 - p_2)(1 - p_3) + (1 - p_1)(1 - p_2)p_3(1 - p_4)$$
$$+ (1 - p_1)p_2(1 - p_3)(1 - p_4) + p_1(1 - p_2)(1 - p_3)(1 - p_4)$$
$$= 1 - (p_1p_2 + p_1p_3 + p_1p_4 + p_2p_3 + p_2p_4 + p_3p_4) + 2(p_1p_2p_3 + p_1p_2p_4 + p_1p_3p_4 + p_2p_3p_4) - 3p_1p_2p_3p_4 \quad \textbf{(49)}$$

The "truth values" in the "truth table" of $R(\mathbf{p})$ are necessary and sufficient for determining $R(\mathbf{p})$. The "truth table" of $R(\mathbf{p})$ is similar to that of $f(\mathbf{X})$ and is given by the following special version of a Karnaugh map called probability map [11], shown in Fig. 4

6. Computation of The Weight of a Switching Function

Theorem 2:

The weight of the switching function $f(X)$ is given in terms of its real transform as

$$\mathrm{wt}(f) = 2^{n} * R(2^{-1}) = 2^{n} * \boldsymbol{R}(2^{-1}, 2^{-1}, \cdots, 2^{-1}), \quad \textbf{(50)}$$

where $R(\mathbf{p})$ denotes the real transform of $f(\mathbf{X})$, and 2^{-1} means a vector of n elements each of which is $2^{-1} = \mathbf{0.5}$

Theorem 3:

Let the switching function $f(\mathbf{X})$ be expressed by the disjoint sum-of-products (s-o-p) form (44), then the weight of $f(\mathbf{X})$ is given by

$$\mathrm{wt}(f) = \sum_{k=1}^{m} 2^{(n - \ell(D_k))}, \quad \textbf{(51)}$$

where $\ell(D_k)$ is the number of irredundant literals in the product D_k, e. g. $\ell(1) = \mathbf{0}$, $\ell(X_i) = \ell(\overline{X}_i) = \mathbf{1}$, $\ell(X_iX_j) = \ell(X_i\overline{X}_j) = \mathbf{2}$. The logical value 0 is not considered a product D_k. But anyhow we assume that $\ell(0) = \infty$, so were we to have $D_k = 0$, it would contribute nothing to $\mathrm{wt}(f)$. The minterm expansion of $f(\mathbf{X})$ is a special case of (44). for which $\ell(D_k) = n$, ∀k, and (51) produces the correct result $\mathrm{wt}(f) = \boldsymbol{m}$ for this special case.

The polarized weight of a switching function (*wp (f)*) is the sum of its truth table entries when its truth table is recoded from {0, 1} to {+1, − 1}, The value of *wp(f)* is given by

wp (f) = (No. of Off values of *f*) * (− 1)^0 + (No. of On values of *f*) * (− 1)^1

$$= [2^n - wt(f)] * (1) + [wt(f)] * (-1) = 2^n - 2wt(f)$$

$$= 2^n - 2\sum_{k=1}^{m} 2^{(n-\ell(D_k))}. \quad (52)$$

In particular, the polarized weight is given in terms of the real transform as

$$wp(f) = 2^n - 2^{n+1} * R(2^{-1}, 2^{-1}, \cdots, 2^{-1}), \quad (53)$$

Example 3:

The 2-out-of-3 function discussed earlier in Example 1, is shown with a disjoint coverage of non-overlapping loops in Fig. 1(a), and hence is expressed by the disjoint s-o-p expression

$$f(X_1, X_2, X_3) = X_1X_2 \vee \bar{X}_1X_2X_3 \vee X_1\bar{X}_2X_3. \quad (11a)$$

Therefore, its weight and polarized weight are obtained via (51) and (52) as

$$wt(f) = 2^{3-2} + 2^{3-3} + 2^{3-3} = 2 + 1 + 1 = 4,$$

$$w_p(f) = 2^3 - 2(4) = 0,$$

in agreement with what can be deduced from Figs. 1(a) and 1(b).

7. The Walsh Spectrum in Terms of Subfunction Weights

Each row of T_n can be viewed as an encoding {1→ 0, − 1→1} of a particular odd parity function $f_o(X_{i_1}, X_{i_2}, \cdots, X_{i_m}) = X_{i_1} \oplus X_{i_2} \oplus \cdots \oplus X_{i_m}$, which involves the (possibly empty) subset $\{X_{i_1}, X_{i_2}, \cdots, X_{i_m}\}$ of the set of *n* elements of ***X***. For a given row, the variables involved are those corresponding to l's in the binary expansion of the row index, with X_1 corresponding to the most significant bit [37]. The spectral coefficients are distinguished using subscripts identifying the variables involved in the corresponding row. Such a subscript identification is useful, since $r_{i_1 i_2 \cdots i_m}$ measures the 'correlation' between $f(X)$ and the odd parity function $f_o(X_{i_1}, X_{i_2}, \cdots, X_{i_m})$. In fact, $r_{i_1 i_2 \cdots i_m}$ equals the number of input vectors for which

$$\left(f(X) \wedge \bar{f}_o\left(X_{i_1}, \boldsymbol{X}_{i_2}, \cdots, X_{i_m}\right)\right) = 1, \quad \textbf{(54a)}$$

minus the number of input vectors for which

$$\left(f(X) \wedge f_o\left(X_{i_1}, \boldsymbol{X}_{i_2}, \cdots, X_{i_m}\right)\right) = 1. \quad \textbf{(54b)}$$

The first spectral coefficient is denoted by r_0 and measures the 'correlation' of *f(**X**)* to $f_o(\emptyset) = 0$, and hence equals the number of input vectors for which *f(**X**)* = 1, i.e. equals the weight *wt(f(**X**))*, namely:

$$r_0 = wt\big(f(X)\big), \quad \textbf{(55)}$$

There is a set of a 'first-order' spectral coefficients r_i, i =1, 2,..., n, each of which measures the correlation of *f(**X**)* to $f_o(X_i) = X_i$, and hence equals

$$r_i = wt(f(\boldsymbol{X} \mid f_o(X_i) = 0) - wt(f(\boldsymbol{X} \mid f_o(X_i) = 1)). \quad \textbf{(56)}$$

Here, the notation $f(X|f_o(X_i) = j) = \boldsymbol{f}(X|X_i = \boldsymbol{j})$ denotes the subfunction or restriction of $f(X)$ when $X_i = \boldsymbol{j},$ where $j = 0 \text{ or } 1.$ This result is generalized into the following theorem.

Theorem 4:

The spectral coefficients of a switching function are given by:

$$r_{i_1 i_2 \cdots i_m} = wt(f(\boldsymbol{X} \mid f\_o\ (X\_(i\_1), X\_(i\_2), \cdots, X\_(i\_m)) = 0)) - wt(f(\boldsymbol{X} \mid f\_o\ (X\_(i\_1), X\_(i\_2), \cdots, X\_(i\_m)) = 1)). \quad \textbf{(57)}$$

Equations (55)-(57) are for the R-encoding. Note that for m = 0, we need $f_o(\emptyset)$, i.e., the odd-parity function of 0 variables, which is 0, and (57) reduces to (55) if we understand that $wt(f(X)|0 = 1) = 0$. The counterparts of (55)-(57) for the S-encoding use polarized weights and {+1, $-$ 1} encoding for the odd-parity functions. They are given by

$$s_0 = wp(f(X)), \tag{55a}$$

$$s\_i = wp(f(X \mid f\_o (X\_i) = +1) - wp(f(X \mid f\_o (X\_i) = -1), \tag{56a}$$

$$s\_(i\_1\ i\_2\ \cdots\ i\_m) = wp(f(X \mid f\_o (X\_(i\_1), X\_(i\_2), \cdots, X\_(i\_m)) = +1) \tag{57a}$$

$$-wp(f(X \mid f\_o (X\_(i\_1), X\_(i\_2), \cdots, X\_(i\_m)) = -1).$$

Example 4:

Figure 5 demonstrates the matrix computation of the ***S*** spectrum as the matrix product $T_3\, F$, where for convenience the column vector ***F*** is not placed to the right of T_3, but instead the transpose of ***F*** (a row vector) is placed above T_3 . This is a well-known trick used frequently [64] to enhance the readability of matrix multiplication. Figure 6 illustrates Karnaugh maps for ***F*** with superimposed loops representing pertinent odd parity functions. Each of these maps is a demonstration of equations (55a)-(57a), since it gives the pertinent spectral coefficient as a sum of un-circled entries (for which the pertinent $f_o = +1$) minus the sum of encircled entries (for which the pertinent $f_o = -1$). For convenience, we indicate below each map the odd-party function f_o used, and the value of the corresponding spectral coefficient. Figures 6 and 3 are in total agreement. In Fig. 6, all the maps have identical entries and we take the difference of the sum of un-circled entries and that of encircled ones, and in Fig. 3, each map has its own entries that we simply add. In other words, we observe that we could redraw the Karnaugh maps in Fig. 6 without loops by simply negating all the entries encircled by the loops therein, and then calculating the spectral coefficients simply as the sums of each map entries. This observation brings us exactly to the situation depicted in Fig. 3. In passing, we note that since the 2-out-of-3 function is a totally symmetric function, its spectral coefficients of equal numbers of subscripts are the same, i.e.,

$$s_1 = s_2 = s_3, \qquad \textbf{(58a)}$$

$$s_{12} = s_{13} = s_{23}. \qquad \textbf{(58b)}$$

Row index	X_1	X_2	X_3	Row encodes	1	1	1	−1	1	−1	−1	−1			
0	0	0	0	0	1	1	1	1	1	1	1	1		0	s_0
1	0	0	1	X_3	1	−1	1	−1	1	−1	1	−1		4	s_3
2	0	1	0	X_2	1	1	−1	−1	1	1	−1	−1		4	s_2
3	0	1	1	$X_2 \oplus X_3$	1	−1	−1	1	1	−1	−1	1		0	s_{23}
4	1	0	0	X1	1	1	1	1	−1	−1	−1	−1	=	4	s_1
5	1	0	1	$X_1 \oplus X_3$	1	−1	1	−1	−1	1	−1	1		0	s_{13}
6	1	1	0	$X_1 \oplus X_2$	1	1	−1	−1	−1	−1	1	1		0	s_{12}
7	1	1	1	$X_1 \oplus X_2 \oplus X_3$	1	−1	−1	1	−1	1	1	−1		−4	s_{123}

Fig. (5). Matrix computation of the spectrum *S* for the 2-out-of-3 function

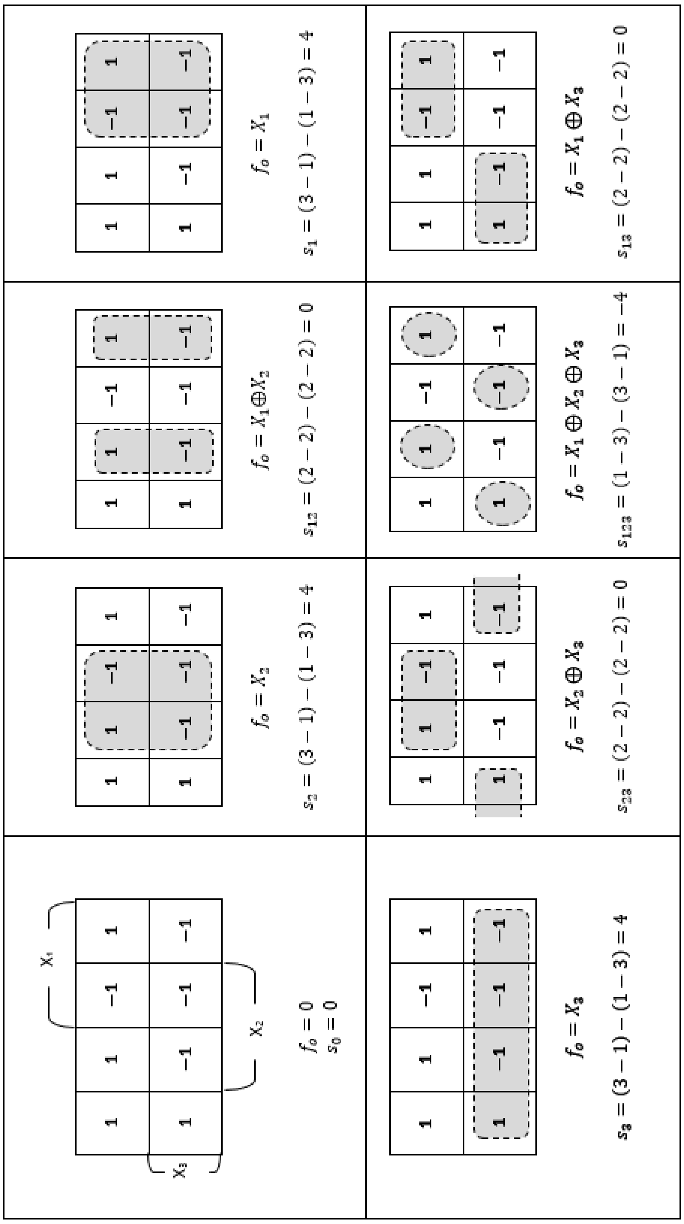


Fig. (6). Computation of the Walsh Spectrum (S-encoding) for the 2-out-of-3 function

8. The Walsh Spectrum in Terms of The Real Transform

Equation (57a) can be rewritten for $m \geq 1$ in the form

$$s_{i_1 i_2 \cdots i_m} = \sum_{Y \in E_m} wp\left(f\left(X/Y\right)\right) - \sum_{Y \in O_m} wp\left(f\left(X/Y\right)\right), \quad (59)$$

where $f\left(X/Y\right)$ is an $(n - m)$ variable function obtained as a subfunction or a restriction of *f(X)* through one particular assignment of the m variables $Y = \left(X_{i_1}, X_{i_2}, \cdots, X_{i_m}\right)$ which constitute a subset of ***X***. Since the vectors ***X, Y*** and $\left(X/Y\right)$ are of dimensions n, m, and $(n - m)$, respectively, there are $2^n, 2^m,$ and $2^{(n-m)}$ such vectors, respectively. The set of Y vectors for which the number of l's in the components of the m-tuple Y is even (odd) is denoted by E_m (O_m). The cardinality (number of elements) of each of the sets E_m and O_m (for $m \geq 1$) is 2^{m-1}. Due to (53), equation (59) can be reduced to

$$s_{i_1 i_2 \cdots i_m} = -2^{n-m+1}\left[\sum_{Y \in E_m} R\left(P/Y\right)_{P/_{Y=2^{-1}}} - \sum_{Y \in O_m} R\left(P/Y\right)_{P/_{Y=2^{-1}}}\right], \quad (60)$$

where *R* is the real transform of *f(X)*. Since *R* is a multi-affine function, mathematical induction can be used to reduce the expression for $s_{i_1 i_2 \cdots i_m}$ further into

$$s_{i_1 i_2 \cdots i_m} = (-1)^{m+1}\, 2^{(n-m+1)} \left(\frac{\partial^m R}{\partial p_{i_1} \partial p_{i_2} \cdots \partial p_{i_m}}\right)_{P/Y=2^{-1}}. \quad (61)$$

Equation (61) means that an m^{th}-order spectral coefficient is proportional to the m^{th} derivative of the real transform of the switching function with respect to the pertinent variables. That derivative is independent of these variables; an immediate consequence of the multi-affine nature of *R*. As a corollary of (61), if the switching function is vacuous in any input variable X_{i_j}, i.e., $R(p)$ is independent of p_{i_j}, then the 2^{n-1} spectral coefficients that contain i_j in their subscript identification will be zero valued. Also if $f(X)$ is partially symmetric in X_{i_j} and X_{i_ℓ}, (and hence, p_{i_j} and

p_{i_ℓ} are interchangeable in $R(p))$, then $s_{i_j} = s_{i_\ell}$, and moreover any two spectral coefficients that share the same subscripts and differ only in the replacement of i_j by i_ℓ are also equal. We stress that (59)-(61) are used for $m \geq 1$. The first spectral coefficient s_0 is given by (55a), possibly combined with (53).

Example 5:

The real transform of the 2-out-of-3 function in Examples 1 and 3 can be obtained from its disjoint s-o-p expression (54) as

$$R(p_1, p_2, p_3) = p_1 p_2 + (1- p_1) p_2 p_3 + p_1(1- p_2) p_3 = p_1 p_2 + p_2 p_3 + p_1 p_3 - 2 p_1 p_2 p_3 \quad \textbf{(62)}$$

The first spectral coefficient s_0 is obtained as

$$s_0 = 2^3 - 2^4 * R(2^{-1}, 2^{-1}, 2^{-1}) = 0,$$

while the spectral coefficients s_1 , s_{12} , and s_{123} can be obtained via (60) as

$$s_1 = -2^{(3-1+1)} [R(0, 2^{-1}, 2^{-1}) - R(1, 2^{-1}, 2^{-1})] = -8\left[\frac{1}{4} - \frac{3}{4}\right] = 4 ,$$

$$s_{12} = -2^{(3-2+1)} [R(0, 0, 2^{-1}) + R(1, 1, 2^{-1}) - R(0, 1, 2^{-1}) - R(1, 0, 2^{-1})]$$
$$= -4\left[0 + 1 - \frac{1}{2} - \frac{1}{2}\right] = 0 ,$$

$$s_{123} = -2^{(3-3+1)} [R(0, 0, 0) + R(1, 1, 0) + R(1, 0, 1) + R(0, 1, 1)$$
$$- R(1, 0, 0) - R(0, 1, 0) - R(0, 0, 1) - R(1, 1, 1)]$$
$$= -2[0 + 1 + 1 + 1 - 0 - 0 - 0 - 1] = -4 .$$

Alternatively, these spectral coefficients can be found via (61) as

$$s_1 = 2^3 \left(\frac{\partial R}{\partial p_1}\right)_{p_2=p_3=2^{-1}} = 2^3 (p_2 + p_3 - 2p_2p_3)_{p_2=p_3=2^{-1}} = 4,$$

$$s_{12} = -2^2 \left(\frac{\partial^2 R}{\partial p_1 \partial p_2}\right)_{p_3=2^{-1}} = -2^2 (1 - 2p_3)_{p_3=2^{-1}} = 0,$$

$$s_{123} = 2\left(\frac{\partial^3 R}{\partial p_1 \partial p_2 \partial p_3}\right) = 2(-2) = -4.$$

Example 6:

With a little abuse of notation, we use $\overline{R}(p), \overline{r},$ and $\overline{s}$ to denote the real transform and the two types of the spectral coefficients of the complement $\bar{f}(\mathbf{X})$ of $f(\boldsymbol{X})$. The real transform $\overline{R}(p)$ is given by

$$\overline{R}(\boldsymbol{p}) = 1 - R(\boldsymbol{p}). \qquad \textbf{(63)}$$

Equations (55)-(57) and (55a)–(57a) can be used to express the spectrum of $\bar{f}(\mathbf{X})$ as

$$\overline{r}_0 = 2^n - r_0, \qquad \textbf{(64a)}$$

$$\overline{r}_{i_1 i_2 \cdots i_m} = -r_{i_1 i_2 \cdots i_m}, \quad \text{for } m \geq 1 \qquad \textbf{(64b)}$$

$$\overline{s}_0 = s_0, \qquad \textbf{(65a)}$$

$$\overline{s}_{i_1 i_2 \cdots i_m} = -s_{i_1 i_2 \cdots i_m}, \quad \text{for } m \geq 1 \qquad \textbf{(65b)}$$

It is interesting to note that the Dotson and Gobien algorithm [10] for producing a disjoint s-o-p expression of f, also yields a disjoint s-o-p expression for $\bar{f}$ as an offshoot output. The more compact expression among the disjoint ones for f and $\bar{f}$ is to be chosen, and the corresponding spectrum is to be obtained. If the spectrum of f is obtained, the conversion to that of $\bar{f}$ is straight via (64), or (65), and vice versa.

Example 7:

The basic spectrum for an n-variable function $f(\boldsymbol{X})$ that expresses a single literal X_i is obtained as follows:

$$f(\boldsymbol{X}) = X_i \ , \qquad R(\boldsymbol{p}) = p_i$$

$$s_0 = 2^n - 2^{n+1} R(\mathbf{2^{-1}}) = 0,$$

$$s_i = 2^n (\partial R / \partial p_i) = 2^n,$$

while all the remaining spectral coefficients are 0's.

Example 8:

The first spectral coefficient of a single product D_k is obtained from (52) and (55a) as follows:

$$s_0 \ (D_k) = 2^n - 2^{(n+1-\ell(D_k))} . \qquad \textbf{(66)}$$

The real transform of D_k is obtained from (46) as

$$R\ell(D_k) = \left(\prod_{i\in I_{k_1}} p_i\right) \left(\prod_{i\in I_{k_2}} (1-p_i)\right). \qquad \textbf{(46a)}$$

Thanks to (61), the higher-order spectral coefficient $s_{i_1 i_2 \cdots i_m}$ of D_k is proportional to the m[th]-order derivative of $R\ell(D_k)$ w.r.t. $p_{i_1}, p_{i_2}, \cdots, and\ p_{i_m}$. Now, we consider three cases:

Case a: $M = \{1, 2, \cdots, m\}$ is not a subset of $(I_{k_1} \cup I_{k_2})$, i.e., if one or more of the variables X_{i_j} $(j = 1, 2, \cdots m)$ does not appear in D_k , and hence p_{i_j} does not appear in $R\ell(D_k)$, then according to (61)

$$s_{i_1 i_2 \cdots i_m}(\boldsymbol{D}_k) = \mathbf{0}, \qquad \textbf{(67a)}$$

Case b: If $M = \{1, 2, \cdots, m\}$ is equal to $(I_{k_1} \cup I_{k_2})$ then according to (61):

$$s_{i_1 i_2 \cdots i_m}(\boldsymbol{D}_k) = (-1)^{m+1+|I_{k_2} \cap M|} \ 2^{(n-m+1)}, \qquad \textbf{(67b)}$$

where $|I_{k_2} \cap M|$ is the cardinality of the set $(I_{k_2} \cap M)$ or simply the number of complemented literals in the product D_k whose literal subscripts are considered in $s_{i_1 i_2 \cdots i_m}(\boldsymbol{D}_k)$.

Case c: If $M = \{1, 2, \cdots, m\}$ is a proper subset of $(I_{k_1} \cup I_{k_2})$,

$$s_{i_1 i_2 \cdots i_m}(\boldsymbol{D}_k) = (-1)^{m+1+|I_{k_2} \cap M|} \; 2^{\left(n-m+1-\left|(I_{k_1} \cup I_{k_2})-M\right|\right)}, \quad \textbf{(67c)}$$

Note that (67c) includes (67b) when the cardinality $\left|(I_{k_1} \cup I_{k_2}) - \boldsymbol{M}\right| = \mathbf{0}$.

For example consider the product $\overline{X}_3 X_4$ when viewed as a function of the four variables X_1, X_2, X_3, X_4. According to (66), and (67) all its spectral coefficients are 0's, except

$$s_0(\overline{X}_3 X_4) = \mathbf{2^4} - 2^{(4+1-2)} = 16 - \mathbf{8} = \mathbf{8},$$
$$s_3(\overline{X}_3 X_4) = (-1)^{1+1+1} \; 2^{(4-1+1-1)} = -8,$$
$$s_4(\overline{X}_3 X_4) = (-1)^{1+1+0} \; 2^{(4-1+1-1)} = 8,$$
$$s_{34}(\overline{X}_3 X_4) = (-1)^{2+1+1} \; 2^{(4-2+1)} = 8.$$

9. Walsh Spectrum Computation Revisited

If the switching function *f (**X**)* is given by the disjoint s-o-p expression (44), then its real transform is given by

$$R\ell(f) = \sum_{k=1}^{m} R\ell(D_k). \quad \textbf{(68)}$$

The first spectral coefficient is obtained from (52), (55a), and (66) as

$$s_o(f) = \sum_{k=1}^{m} s_o(D_k) - (m-1)2^n. \quad \textbf{(69)}$$

Thanks to (61), (68), and the fact that the two linear operators of differentiation and finite summation are interchangeable, the higher-order spectral coefficients are obtained as

$$s_{i_1 i_2 \cdots i_m}(f) = \sum_{k=1}^{m} s_{i_1 i_2 \cdots i_m}(D_k), \quad \textbf{(70)}$$

In (68) and (69), the coefficient $s_0(D_k)$ and $s_{i_1 i_2 \cdots i_m}(D_k)$ represent the spectrum of single product D_k, and can be obtained via equations (66) and (67). The set of equations (66), (67), (69), and (70) constitute a procedure for spectrum computation. This procedure can be viewed as a formal development of the method outlined in [6, pp. 35-40] and [34].

As a special case, *f(X)* can be expressed by its minterm expansion

$$f(X) = \vee_{k \in K} m_k, \quad \textbf{(71)}$$

where ***K*** is the set of indices for the true minterms of *f*. In this case, the spectrum of f is given by

$$s_{i_1 i_2 \cdots i_m} = \sum_{k \in K} s_{i_1 i_2 \cdots i_m}(m_k), \quad \textbf{(72)}$$

Here, $s_{i_1 i_2 \cdots i_m}$ can be obtained from (67c), or via (25), (26) and the fact that $r_{i_1 i_2 \cdots i_m}(m_k) = +1$ (-1) if the number of uncomplemented variables among $X_{i_1}, X_{i_2}, \ldots, X_{i_m}$ in the minterm m_k is even (odd). This observation can be used to explain the technique of [65], and is equivalent to the basic definition of the spectrum (equation (16)).

Example 9:

Consider the 4-variable function

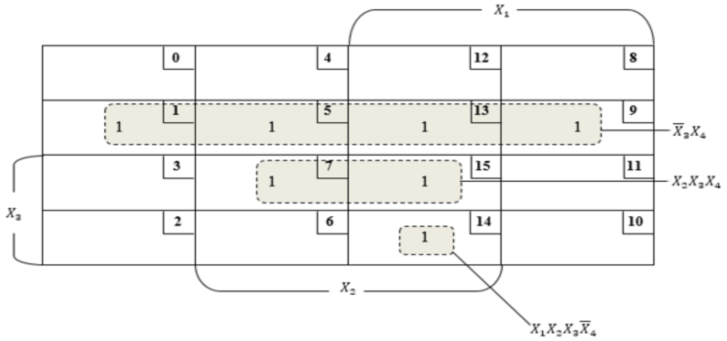
$$f(X_1, X_2, X_3, X_4) = \sum(1, 5, 7, 9, 13, \mathbf{14}, \mathbf{15}). \quad \textbf{(73)}$$

The disjoint s-o-p representations of *f* and $\bar{f}$ are obtained in Fig. 7(a) and (b) as

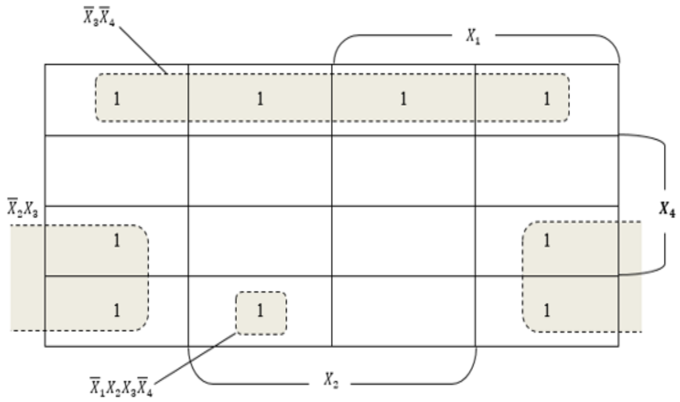
$$f = \overline{X}_3X_4 \vee X_2X_3X_4 \vee X_1X_2X_3\overline{X}_4\,, \qquad \textbf{(73a)}$$

$$\bar{f} = \overline{X}_3\overline{X}_4 \vee \overline{X}_2X_3 \vee \overline{X}_1X_2X_3\overline{X}_4\,. \qquad \textbf{(73b)}$$

Computation of the spectra of f and $\bar{f}$ via (66), (67), (69), and (70) are illustrated on the spectral - coefficients maps of Figs. 7(c) and 7(d). The spectra obtained satisfy (16) and (65).



$(a)f$



$(b)\overline{f}$

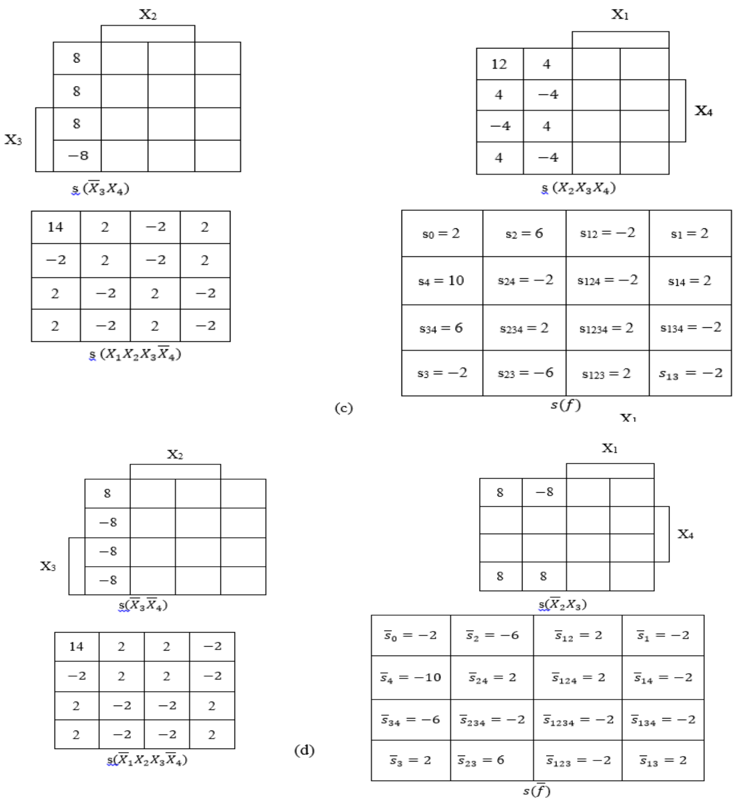


Fig. (7). Disjoint representation of (a) f and (b) $\bar{f}$ and spectral-coefficient maps for computing the spectra of (c) f and (d) $\bar{f}$

10. The Real Transform in Terms of The Spectrum

The real transform *R(p)* can be expanded about an arbitrary point ***p*** = ***t*** via a finite multivariable Taylor's expansion of 2^n coefficients [36, equation (8)]. If ***t*** is chosen as 2^{-1}, and the conditions of equation (61) are invoked, then R(**p**) is given by

$$R(p) = \left(2^{-1} - 2^{-(n+1)} s_0\right) + 2^{-n} \sum_{i=1}^{n} s_i\ (p_i - 2^{-1}) - 2^{-(n-1)} \sum_{1 \le i} \sum_{< j \le n} s_{ij}\ (p_i - 2^{-1})(p_j - 2^{-1}) + 2^{-(n-2)} \sum_{1 \le i} \sum_{< j} \sum_{< k \le n} s_{ijk}\ (p_i - 2^{-1})\ (p_j - 2^{-1})\ (p_k - 2^{-1}) + \cdots + 2^{-1}(-1)^{n+1} s_{123\cdots n}\ (p_1 - 2^{-1})(p_2 - 2^{-1}) \cdots (p_n - 2^{-1}). \quad (74)$$

Equation (74) expresses the real transform in terms of the spectral coefficients. Since a switching function is uniquely defined by its real transform, eq. (74) can be viewed as a computational method for the inverse spectrum, i.e. for determining the switching function in terms of its spectral coefficients.

Example 10:

We know that the spectral coefficients of the 2-out-of-3 function are $s_0 = 0,\quad s_1 = s_2 = s_3 = 4,\quad s_{12} = s_{13} = s_{23} = 0,$ and $s_{123} = -4$. Hence, its real transform is

$$R(p_1, p_2, p_3) = [2^{-1} - 2^{-4}\ (0)] + 2^{-3}\ (4\ (p_1 - 2^{-1}) + 4\ (p_2 - 2^{-1})) + 4\ (p_3 - 2^{-1}) - 0 + (2^{-1})(-4)\ (p_1 - 2^{-1})\ (p_2 - 2^{-1})\ (p_3 - 2^{-1}) = p_1p_2 + p_2p_3 + p_3p_1 - 2p_1p_2p_3. \quad \mathbf{(75)}$$

Since f and R share the same truth table, the 2-out-of-3 function is easily retrieved from (75).

Example 11:

Figure 8 summarizes some of the properties discussed herein for the sixteen binary switching functions of the form

$$f(X_1, X_2) = a_0\bar{X}_1\bar{X}_2 \vee a_1\bar{X}_1X_2 \vee a_2X_1\bar{X}_2 \vee a_3X_1X_2 . \quad \mathbf{(76)}$$

The functions are displayed within the cells of a Karnaugh map of arguments $a_0, a_1, a_2, and\ a_3$. Each map cell represents the name of the pertinent function, its Boolean expression $f(X_1, X_2),$ its real transform $R(p_1, p_2)$, its truth-table encodings f and F and its corresponding Walsh spectra R and S , where

$$R(p_1, p_2) = a_0 + (-a_0 + a_1)p_2 + (-a_0 + a_2)p_1 + (a_0 - a_1 - a_2 + a_3)p_1p_2 \quad \mathbf{(77)}$$

$$f = [a_0 \quad a_1 \quad a_2 \quad a_3]^T, \tag{78}$$

$$F = [1 - 2a_0 \quad 1 - 2a_1 \quad 1 - 2a_2 \quad 1 - 2a_3]^T, \tag{79}$$

$$R = \left[\left(a_0 + a_1 + a_2 + a_3 \& \left(a_0 - a_1 + a_2 - a_3 \right) \& \left(a_0 + a_1 - a_2 - a_3 \right) \& \left(a_0 - a_1 - a_2 + a_3 \right) \right) \right]^T, \tag{80}$$

$$S = \begin{bmatrix} 4 - 2(a_0 + a_1 + a_2 + a_3) \\ -2(a_0 - a_1 + a_2 - a_3) \\ -2(a_0 + a_1 - a_2 - a_3) \\ -2(a_0 - a_1 - a_2 + a_3) \end{bmatrix} \tag{81}$$

In passing, we note that Fig. 8 has a wealth of useful information that facilitates easy reference, and which is even richer then the contents of a full paper [66] that rediscovers the arithmetic transform as an arithmetic version of Boolean algebra. The arrangement of the 16 binary switching functions on the Karnaugh map of Fig. 8 is equivalent to their arrangement on a Hasse diagram (see, e.g., [67, 68]). With such an arrangement, Fig. 8 can be used to reproduce Figs. 1 and 2 of [69] in which the real transform is rediscovered under the disguised name of the Generalized Boolean polynomial (GBP). Another reference which rediscovers the real transform is [70] which labels it as a measure on a finite free Boolean algebra, and uses it in the evaluation of sizes of queries applied to binary tables in relational databases and to the identification of frequent sets of items and to association rules in data mining.

a_0

a_3

Zero (0)	0	1	0	4	X_2 *INHIBIT* X_1	0	1	1	2	*NOT* X_1	1	−1	2	0	X_1 *NOR* X_2	1	−1	1	2
0	0	1	0	0	$\overline{X}_1 X_2$	1	−1	−1	2	$\overline{X}_1$	1	−1	0	0	$\overline{X}_1 \overline{X}_2$	0	1	1	−2
	0	1	0	0		0	1	1	−2	$1 - p_1$	0	1	2	−4		0	1	1	−2
0	0	1	0	0	$p_2 - p_1 p_2$	0	1	−1	2		0	1	0	0	$1 - p_2 - p_1 + p_1 p_2$	0	1	1	−2
X_1 *AND* X_2	0	1	1	2	X_2	0	1	2	0	X_1 *IMPLY* X_2	1	−1	3	−2	X_1 *XNOR* X_2	1	−1	2	0
$X_1 \wedge X_2$	0	1	−1	2	X_2	1	−1	−2	4	$\overline{X}_1 \vee X_2$	1	−1	−1	2	$\overline{X}_1 \overline{X}_2 \vee X_1 X_2$	0	1	0	0
	0	1	−1	2		0	1	0	0		0	1	1	−2		0	1	0	0
$p_1 p_2$	1	−1	1	−2	p_2	1	−1	0	0	$1 - p + p_1 p_2$	1	−1	1	−2	$1 - p_2 - p_1 + 2p_1 p_2$	1	−1	2	−4
X_1	0	1	2	0	X_1 *OR* X_2	0	1	3	−2	One (1)	1	−1	4	−4	X_2 *IMPLY* X_1	1	−1	3	−2
X_1	0	1	0	0	$X_1 \vee X_2$	1	−1	−1	2	1	1	−1	0	0	$X_1 \vee \overline{X}_2$	0	1	1	−2
p_1	1	−1	−2	4	$p_2 + p_1 - p_1 p_2$	1	−1	−1	2	1	1	−1	0	0	$1 - p_2 + p_1 p_2$	1	−1	−1	2
	1	−1	0	0		1	−1	−1	2		1	−1	0	0		1	−1	1	−2
X_1 *INHIBIT* X_2	0	1	1	2	X_1 *XOR* X_2	0	1	2	0	X_1 *NAND* X_2	1	−1	3	−2	*NOT* X_2	1	−1	2	0
$X_1 \overline{X}_2$	0	1	1	−2	$\overline{X}_1 X_2 \vee X_1 \overline{X}_2$	1	−1	0	0	$\overline{X}_1 \vee \overline{X}_2$	1	−1	1	−2	$\overline{X}_2$	0	1	2	−4
$p_1 - p_1 p_2$	1	−1	−1	2	$p_2 + p_1 - 2p_1 p_2$	1	−1	0	0	$1 - p_1 p_2$	1	−1	1	−2	$1 - p_2$	1	−1	0	0
	0	1	−1	2		0	1	−2	4		0	1	−1	2		0	1	0	0

a_2

a_1

Fig. (8). The sixteen binary switching functions.

11. Conclusions

The pictorial insight provided by the Karnaugh map makes the discussion of many topics in combinatorics from a Karnaugh-map perspective a lucid and appealing task. An earlier example supporting this point is the comparative study of methods of system reliability analysis in a Karnaugh-map perspective [71].

The current paper is a clear demonstration of the utility of the Karnaugh map as a pedagogical tool not only for its conventional usage in solving various coverage problems for switching functions, but also for novel non-conventional uses in explaining a variety of complex concepts. The task addressed herein is the exposition of two famous representations for switching functions, namely, the Walsh spectrum and the real transform. The literature on these two representations is both complex and confusing due to the existence of different definitions used by different communities of researchers. This paper is a serious attempt for a unified and simplified treatment of the subject fully addressing sources of ambiguity or discrepancy. The interrelationship between the Walsh spectrum and real transform is thoroughly and explicitly expressed and utilized as a basis for computational procedures of one representation in terms of the other.

Acknowledgement

The authors are deeply indebted and sincerely grateful to Dr. Ahmad Ali Rushdi of ALFARABI Consulting Group, California, USA for the help he offered in the preparation of this manuscript.

12. References

[1] **Crama, Y., and P. L. Hammer,** *Boolean Functions*: *Theory, Algorithms, And Applications*, Cambridge, United Kingdom, Cambridge University Press, (2011).

[2] **Elhosary, A. M., N. Hamdy, I. A. Farag, and A. Rohiem,** "State Of The Art In Boolean Functions Cryptographic Assessment," *International Journal Of Computer Networks And Communications Security*, Vol. **1**, No. 3, (2013), pp. 88-94.

[3] **Carlet C.,** "Boolean Functions For Cryptography And Error Correcting Codes," *In Boolean Models And Methods In Mathematics, Computer Science, And Engineering*, Cambridge University Press, (2010), pp. 257-397.

[4] **Xiao, G-Z., and J. L. Massey,** "A Spectral Characterization Of Correlation-Immune Combining Functions," *IEEE Transactions on Information Theory*, Vol. **IT-34**, No. 3, (1988), pp. 569-571.

[5] **Maity, S., C. Arackaparambil, and K. Meyase,** "A New Construction Of Resilient Boolean Functions With High Nonlinearity," *Ars Comb*, Vol. **109**, (2013), pp. 171-192.

[6] **Hurst, S. L., D. M. Miller, and J. C. Muzio,** *Spectral Techniques in Digital Logic*, Academic press, London, (1985).

[7] **Karpovsky, M. G., R. S. Stankovic, and J. T.,** Astola, *Spectral Logic and Its Applications for the Design of Digital Devices*, Wiley, New York, NY, USA, (2008).

[8] **Thornton, M. A., R. Drechsler, and D. M Miller,** *Spectral Techniques in VLSI CAD*, Springer, Berlin, Germany, (2001).

[9] **Abraham, J. A.,** "An Improved Algorithm For Network Reliability," *IEEE Transactions on Reliability*, Vol. **R-28**, No.1, (1979), pp. 58-61.

[10] **Dotson, W., and J. Gobien,** "A New Analysis Technique For Probabilistic Graphs," *IEEE Transactions on Circuits and Systems,* Vol. **CAS-26**, No. 10, (1979), pp. 855-865.

[11] **Rushdi, A. M.,** "Symbolic Reliability Analysis With The Aid Of Variable-Entered Karnaugh Maps," *IEEE Transactions on Reliability,* Vol. **R-32**, No. 2, (1983), pp. 134-139.

[12] **Rushdi, A. M.,** "On Reliability Evaluation By Network Decomposition," *IEEE Transactions on Reliability,* Vol. **R-33**, No.5, (1984), pp. 379-384, Corrections: *ibid,* Vol. **R-34**, No. 4, (1985), p. 319.

[13] **Rushdi, A. M., and A. S. Goda,** "Symbolic Reliability Analysis Via Shannon's Expansion And Statistical Independence," *Microelectronics and Reliability,* Vol. **25**, No. 6, (1985), pp. 1041-1053.

[14] **Rushdi, A., M.,** "Utilization Of Symmetric Switching Functions In The Computation Of K-Out-Of-N System Reliability," *Microelectronics and Reliability,* Vol. **26**, No. 5, (1986), pp. 973-987.

[15] **Locks, M. O.,** "A Minimizing Algorithm For Sum Of Disjoint Products," *IEEE Transactions on Reliability*, Vol. **R-36**, No. 4, (1987), pp. 445-453.

[16] **Wilson, J. M.,** "An Improved Minimizing Algorithm For Sum Of Disjoint Products," *IEEE Transactions on Reliability,* Vol. **R-39**, No.1, (1990), pp. 42-45.

[17] **Rushdi, A. M., and A. A. Abdulghani,** "A Comparison Between Reliability Analyses Based Primarily On Disjointness Or Statistical Independence: The Case Of The Generalized Indra Network," *Microelectronics and Reliability*, Vol. **33**, No. 7, (1993), pp. 965-978.

[18] **Rushdi, A. M., and O. M. Ba-Rukab,** "Fault-Tree Modelling Of Computer System Security," *International Journal of Computer Mathematics*, Vol. **82**, No. 7, (2005), pp. 805-819.

[19] **Falkowski, B. J., C. C. Lozano, and T. Łuba,** "Arithmetic And Boolean Techniques For Derivation Of System Reliability Expressions, " *Electronics and Telecommunications Quarterly*, Vol. **54**, (2008), pp. 167-177.

[20] **Blake, A.,** *Canonical Expressions in Boolean Algebra*, Ph. D dissertation, Department of Mathematics, University of Chicago, (1937).

[21] **Rudeanu, S.,** *Boolean Functions and Equations*, North-Holland Publishing Company & American Elsevier, Amsterdam, the Netherlands, (1974).

[22] **Brown, F. M.,** *Boolean Reasoning: The Logic of Boolean Equations*, Kluwer Academic Publishers, Boston, MA, USA (1990).

[23] **Gregg, J. R.,** *Ones and Zeros: Understanding Boolean Algebra, Digital Circuits, and the Logic of Sets*, IEEE Press, New York, NY, USA (1998).

[24] **Rudeanu, S.,** *Lattice Functions and Equations*, Springer, London, UK, (2001).

[25] **Rushdi, A. M., and H. A. Al-Yahya,** "Derivation Of The Complete Sum Of A Switching Function With The Aid Of The Variable-Entered Karnaugh Map," *Journal of King Saud University*, Vol. **13**, No. 2, (2001), pp. 239-269.

[26] **Rushdi, A. M., and Al-Shehri, A. S.,** Logical Reasoning And Its Supporting Role In The Service Of Security And Justice, *Journal of Security Studies*, Vol. **11**, No**.** 22, (2002), pp. 115-153, (In Arabic with an English abstract).

[27] **Rushdi, A. M., and Ba-Rukab, O. M.,** "Some Engineering Applications Of The Modern Syllogistic Method," SEC7 Paper 226, *Proceedings of the 7th Saudi Engineering Conference (SEC7*), Riyadh, Saudi Arabia, Vol. 4, (2007), pp. 389-401, (Also p.201 in Abstracts Volume).

[28] **Rushdi, A. M., and Ba-Rukab, O. M.,** "Powerful Features Of The Modern Syllogistic Method Of Propositional Logic," *Journal of Mathematics and Statistics*, Vol. **4**, No. 3, (2008), pp. 186-193.

[29] **Rushdi, A. M., and O. M. Ba-Rukab,** "The Modern Syllogistic Method As A Tool For Engineering Problem Solving," *Journal of Qassim University : Engineering and Computer Sciences*, Vol. **1**, No. 1, (2008), pp. 57-70.

[30] **Rushdi, A. M., and Ba-Rukab, O. M.,** "An Exposition Of The Modern Syllogistic Method Of Propositional Logic," *Umm Al-Qura University Journal: Engineering and Architecture*, Vol. **1**, No. 1, (2009), pp. 17-49.

[31] **Hammer, P. L., and S., Rudeanu,** *Boolean Methods in Operations Research and Related Areas*, Springer, Berlin, Germany, (1968).

[32] **Rushdi A. M.,** "Karnaugh Map," *Encyclopedia of Mathematics,* Supplement Volume I: pp. 327-328, M. Hazewinkel, (Ed.) Kluwer Academic publishers, Boston, USA, (1996). Available at: http://www.encyclopediaofmath.org/index.php/Karnaugh_map.

[33] **Edwards, C. R.,** "The Application Of The Rademacher–Walsh Transform To Boolean Function Classification And Threshold Logic Synthesis," *IEEE Transactions on Computers*, Vol. **C-24**, No.1, (1975), pp. 48-62.

[34] **Muzio, J. C., and S. L. Hurst,** "The Computation Of Complete And Reduced Sets Of Orthogonal Spectral Coefficients For Logic Design And Pattern Recognition Purposes," *Computers and Electrical Engineering*, Vol. **5**, No. 3, (1978), pp. 231-249.

[35] **Debnath, R. C., and A. K. Karmakar,** "Method For Finding Rademacher-Walsh Spectral Coefficients Of Boolean Functions," *International Journal of Electronics: Theoretical and Experimental*, Vol. **60**, No. 2, (1986), pp. 245-250.

[36] **Rushdi, A. M.,** "On Computing The Syndrome Of A Switching Function," *Microelectronics and Reliability,* Vol. **27**, No. 4, (1987), pp. 703-716.

[37] **Rushdi, A. M.,** "On Computing The Spectral Coefficients Of A Switching Function," *Microelectronics and Reliability*, Vol. **27**, No. 6, (1987), pp. 965-979.

[38] **Falkowski, B. J., and M. A. Perkowski,** "One More Way To Calculate The Hadamard-Walsh Spectrum For Completely And Incompletely Specified Boolean Functions," *International Journal of Electronics: Theoretical and Experimental*, Vol. 69, No. **5**, (1990), pp. 595-602.

[39] **Falkowski, B. J.,** "Calculation Of Rademacher-Walsh Spectral Coefficients For Systems Of Completely And Incompletely Specified Boolean Functions," *IEEE International Symposium on Circuits and Systems, ISCAS'93*, IEEE, (1993).

[40] **Thornton, M. A., and V. S. S. Nair,** "Efficient Spectral Coefficient Calculation Using Circuit Output Probabilities," *Digital Signal Processing,* Vol. **4**, No. 4, (1994), pp. 245-254.

[41] **Thornton, M. A., and V. S. S. Nair,** "Efficient Calculation Of Spectral Coefficients And Their Applications," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, Vol. **CAD-14**, No. 11, (1995), pp. 1328-1341.

[42] **Thornton, M. A., D. M. Miller, and R. Drechsler,** "Transformations Amongst The Walsh, Haar, Arithmetic And Reed-Muller Spectral Domains," *International Workshop on Applications of the Reed-Muller Expansion in Circuit Design (RMW), (2001).*

[43] **Miller, D. M., and G. W. Dueck,** "Spectral Techniques For Reversible Logic Synthesis," *6th International Symposium on Representations and Methodology of Future Computing Technologies,* (2003).

[44] **Stankovic, R., J., A., and B. Steinbach,** "Former And Recent Work In Classification Of Switching Functions," *Boolean Problems, Proceedings of the 8th International Workshops on Boolean Problems.* Vol. **18**, (2008).

[45] **Papaioannou, S., G., and W. A. Barrett,** "The Real Transform Of A Boolean Function And Its Applications," *Computers and Electrical Engineering*, Vol. **2**, No. 2, (1975), pp. 215-224.

[46] **Kumar, S. K., and M. A. Breuer,** "Probabilistic Aspects Of Boolean Switching Functions Via A New Transform," *Journal of the ACM (JACM)*, Vol. **28**, No. 3, (1981), pp. 502-520.

[47] **Rushdi, A. M.,** "How To Hand-Check A Symbolic Reliability Expression," *IEEE Transactions on Reliability,* Vol. **R-32**, No.5, (1983), pp. 402-408.

[48] **Rushdi, A. M.,** "Uncertainty Analysis Of Fault-Tree Outputs," *IEEE Transactions on Reliability,* Vol. **R-34**, No. 5, (1985), pp. 458-462.

[49] **Heidtmann, K. D.,** "Arithmetic Spectrum Applied To Fault Detection For Combinational Networks," *IEEE Transactions on Computers,* Vol. **C-40**, No. 3, (1991), pp. 320-324.

[50] **Jain, J.,** "Arithmetic Transform Of Boolean Functions," in *Representations of Discrete Functions,* in Sasao, T., and M. Fujita (Editors), Kluwer Academic Publishers, *Dordrecht*, the Netherlands, (1996), pp. 133-161.

[51] **Rushdi, A. M., and F. A. M. Ghaleb,** "On Self-Inverse Binary Matrices Over The Binary Galois Field," *Journal of Mathematics and Statistics*, Vol. **9**, No. 3, (2013), pp. 238-248.

[52] **Walsh, J. L.,** "A Closed Set Of Normal Orthogonal Functions," *American Journal of Mathematics,* Vol. **55**, (1923), pp. 5-24.

[53] **Rademacher, H.,** "Einige Sätze Über Reihen Von Allgemeinen Orthogonalen Funktionen, (Some Propositions About Series Of General Orthogonal Functions)" (in German), *Annals of Mathematics*, Vol. **87**, (1922), pp. 112-138.

[54] **Brewer, J.,** "Kronecker Products And Matrix Calculus In System Theory," *IEEE Transactions on Circuits and Systems,* Vol. **CAS-25**, No. 9, pp. 772-781, (1978), corrections: *ibid.*, Vol. **CAS-26**, No. 5, (1979), p. 360.

[55] **Graham, A.,** *Kronecker Products and Matrix Calculus: with Applications*, Ellis Horwood Limited and John Wiley & Sons, New York, (1981).

[56] **Singh, J., and Shikha G.,** "Eigen Decomposition Of Reed-Muller Transform Using Kronecker Method," *International Journal of Computer Applications*, Vol. **1**, NO. 10, (2010), pp. 1-7.

[57] **Rushdi, A. M. A., and F. A. M. Ghaleb,** "A Tutorial Exposition Of Semi-Tensor Products Of Matrices With A Stress On Their Representation Of Boolean Functions," *Journal of King Abdulaziz University: FCIT*, Vol. **1,** No. 2, (2013), pp.1-39.

[58] **Schneeweiss, W. G.,** "Calculating The Probability Of A Boolean Expression Being 1," *IEEE Transactions on Reliability*, Vol. **R-26**, No. 1 (1977), pp. 16-22.

[59] **Schneeweiss, W. G.,** *Boolean Functions with Engineering Applications and Computer Programs*, Springer-Verlag, New York, NY, USA, (1989).

[60] **Barlow, R. E., and F. Prochan,** *Mathematical Theory of Reliability*, Wiley, New York, NY, USA, (1996).

[61] **Aven, T. and U. Jensen,** *Stochastic Models in Reliability*, Springer-Verlag, New York, NY, USA, Vol. **41**, (1999).

[62] **Rushdi, A. M.,** *Reliability of k-out-of-n Systems*, Chapter 5 in Misra, K. B. (Editor), *New Trends in System Reliability Evaluation,* Vol. **16**, *Fundamental Studies in Engineering,* Elsevier Science Publishers, Amsterdam, The Netherlands, (1993), pp. 185-227.

[63] **Rushdi, A. M.,** "Partially-Redundant Systems: Examples, Reliability, And Life Expectancy," *International Magazine on Advances in Computer Science and Telecommunications,* Vol. **1**, No. 1, (2010), pp. 1-13.

[64] **Rushdi, A. M.,** "Development Of Modified Nodal Analysis Into A Pedagogical Tool," *IEEE Transactions on Education*, Vol. **E-28**, No. 1, (1985), pp. 17-25.

[65] **Debnath , R. C., and A. K. Karmakar,** " Methods For Finding Rademacher-Walsh Spectral Coefficients Of Boolean Functions," *International Journals of Electronics,* Vol. **60**, (1986), pp.245-250.

[66] **Azram, M., J. I. Daoud, and F. A. M. Elfaki,** "Arithmetic Version Of Boolean Algebra," *International Islamic University,* Malaysia, (2009), pp. 79-80.

[67] **Rushdi, A. M., and O. M. Ba-Rukab,** "A Map Procedure For Two-Level Multiple-Output Logic Minimization," *Proceedings of the Seventeenth National Computer Conference,* Al-Madinah Al-Munw'warah, Saudi Arabia, (2004), pp. 517-528.

[68] **Rushdi, A. M., and O. M. Ba-Rukab,** "A Purely-Map Procedure For Two-Level Multiple-Output Logic Minimization," *International Journal of Computer Mathematics,* Vol. **84**, No. 1, (2007), pp. 1-10.

[69] **Radojevic, D.** "There Is Enough Room For Zadeh's Ideas, Besides Aristotle's In A Boolean Frame," *Proceedings of the Second IEEE Conference on Soft Computing Applications (SOFA2007), Gyula, Hungary-Oradea, Romania*, (2007), pp. 79-82.

[70] **Rosenberg, I., D. A. Simovici, and S. Jaroszewicz,** "On Functions Defined On Free Boolean Algebras," *Proceedings of the 32nd IEEE international Symposium on Multiple-Valued Logic (ISMVL' 02),* (2002), pp. 192-199.

[71] **Rushdi, A. M., and D. L. Al-Khateeb,** "A Review Of Methods For System Reliability Analysis: A Karnaugh-Map Perspective," *Proceedings of the First Saudi Engineering Conference*, Jeddah, Saudi Arabia, Vol. 1, pp. 57-95, (May 1983) (In Arabic, with an English abstract).

طيف والش والتحويل الحقيقي لدالة تبديلية: مراجعة من منظور خريطة كارنوه

علي محمد علي رشدي و فارس أحمد محمد غالب

قسم الهندسة الكهربائية وهندسة الحاسبات، كلية الهندسة،

ص. ب. ٨٠٢٠٤، جامعة الملك عبد العزيز، جدة، ٢١٥٨٩، المملكة العربية السعودية

arushdi@kau.edu.sa

(قدم للنشر بتاريخ ٢٠١٤/٢/٣م ؛ قبل للنشر بتاريخ ٢٠١٤/٤/٢٤م)

ملخص البحث. تستخدم ورقة البحث هذه منظور خريطة كارنوه في استقصاء التعريفات وشرح الخصائص واستحداث إجراءات حسابية جديدة واكتشاف التزاوجات بين طيف والش والتحويل الحقيقي لدالة تبديلية. يتم استخدام خرائط كارنوه مناسبة في شرح كيفية حساب طيف والش كما يُعرَف في علم التعمية. يلي ذلك تقديم تعريف بديل لهذا الطيف مستخدم في التصميم الرقمي والمجالات اللصيقة به، ويُردَف ذلك بالإجراءات المصفوفية اللازمة لحسابه. ثم يتم تعريف التحويل الحقيقي لدالة تبديلية كدالة حقيقية في متغيرات حقيقية، ويجري التمييز بوضوح بين هذا التعريف وتعريفات شبيهة به مثل الصيغة عديدة الخطية أو التحويل الحسابي. كما يتم شرح التحويل الحقيقي تصويريا من خلال صيغة خاصة لخريطة كارنوه تدعى خريطة الاحتمالات. تُستعمَل خرائط كارنوه أيضاً لبيان كيفية حساب المعاملات الطيفية المستخدمة في التصميم الرقمي كوزن للدالة التبديلية وكأوزان للدوال الفرعية الناشئة من تقييد هذه الدالة. تتواءم هذه الخرائط مع الخرائط السابقة للطيف المستعمل في علم التعمية. يُستفاد من التزاوجات المستحدثة بين طيف والش والتحويل الحقيقي في صياغة طريقتين مبسطتين لحساب الطيف بدلالة التحويل الحقيقي من خلال بعض المعاونة من خرائط كارنوه. تُختَتم الورقة بحل المسألة العكسية المعنية بحساب التحويل الحقيقي بدلالة طيف والش.