# *Determine Spectral Coefficients of Boolean Functions by Using Walsh-Rademacher Transform*

*By*

***Ass.teacher***
***Hameed Kadhim dawood***
***Department of Mathematics \ College of Basic Education***
***University of Diyala \Iraq***

*Abstract:*

*In this paper, we will define Walsh- Rademacher ,and using it to find the Spectral coefficients of n variables Boolean functions. Also, this paper presents the method, which allows us to investigate the linearity of Boolean functions directly on their spectrum.*
*This method can easily be used in investigations of large Boolean functions ( of many variables), which seem very powerful for modern digital technologies compared with Walsh –Hadamard transform.*

*Keywords:*

*Walsh coefficients, coefficients distribution, Boolean functions, affine functions, linearity measure of a Boolean function.*

## *1- Introduction :*

*Walsh transform belongs to a class of orthogonal transforms, which used in many problems, like spectral methods. One of these problems is to check the linearity of Boolean functions by means of Walsh spectral technique. Walsh transform can be represented by many ways like,walsh-Hadamard transform (W-H.T) and Walsh-Rademacher transform (W-R.T). Porwik,[4] used Walsh-Hadamard transform to determine the Spectral coefficient of Boolean functions, and used it to investigate the linearity of Boolean functions directly on the basis of Walsh coefficients.*

*Linearity and non-linearity play important roles in cryptography, transmission, correction errors, etc.*

*2- preliminaries :*

*The vector spaces used in this paper composed of length n of numbers in* $F_2 = \{0,1\}$ *,and we can denote it as* $F_2^n$ *. If f is a Boolean function from* $F_2^n$ *,then it can be expressed as unique polynomial in n co-ordinates* $x_1,x_2,\ldots,x_n$ *.For this reason f will be identified as a unique multi-variable polynomial* $f(\underline{X})$ *, where* $\underline{X} = (x_1,x_2,\ldots,x_n)$

*For two vectors* $u = (u_1, u_2, \ldots, u_n)$ *and* $v = (v_1, v_2, \ldots, v_n)$

*addition is defined by:*

$$u \oplus v = (u_1 \oplus v_1, u_2 \oplus v_2, \ldots, u_n \oplus v_n)$$

*where, each* $u_i$ *or* $v_i$ *is either 1 or 0 , i = 1,2,...,n , and*

$$1 \oplus 1 = 0 \quad ,0 \oplus 1 = 1 \quad ,1 \oplus 0 = 1 \quad ,0 \oplus 0 = 0$$

*Multiplication is defined by the formula,*

$$u * v = (u_1 * v_1, u_2 * v_2, \ldots, u_n * v_n)$$

*Where, each* $u_i$ *and* $v_i$ *is either 1 or 0 , i = 1,2,...,n , and*

$$1 * 1 = 1 \quad ,0 * 1 = 0 \quad ,1 * 0 = 0 \quad ,0 * 0 = 0$$

*The vector* $\overline{u} \in F_2^n$ *can be defined by the following formula:*

$$\overline{u} = u \oplus \underline{1} = (\overline{u}_1, \overline{u}_2, \ldots, \overline{u}_n) = (1 \oplus u_1, 1 \oplus u_2, \ldots, 1 \oplus u_n)$$

*Definition (1):[4]*

*An n-variable Boolean function is a function* $f : F_2^n \rightarrow F_2$ .

*Example (1) :*

*Table (2-1) shows the truth vector of 2-variable Boolean function* $f(x_1, x_2) = \overline{x}_1 \overline{x}_2 + \overline{x}_1 x_2 + x_1 \overline{x}_2$

| $\underline{x}$ | $(x_1,x_2)$ | $f(x_1,x_2)$ |
|---|---|---|
| *0* | *(0,0)* | *1* |
| *1* | *(0,1)* | *1* |
| *2* | *(1,0)* | *1* |
| *3* | *(1,1)* | *0* |

*Table (2.1) : The trut function of Boolean function*

$$f(x_1, x_2) = \overline{x}_1 \overline{x}_2 + \overline{x}_1 x_2 + x_1 \overline{x}_2$$

*Definition (2):[3]*
*The linear combination of two Boolean functions*
$f, g : F_2^n \rightarrow F_2$ *is defined as :*
$(f \oplus g)(\underline{x}) = f(\underline{x}) \oplus g(\underline{x})$
*where* $\oplus$ *denotes addition modulo 2.*

*Definition (3) :[1]*
*The Hamming weight* $\omega(u)$ *.of a vector u is equal to the number of non-zero components in the vector u.*

*Definition (4) :[1]*
*The Hamming distance d(u,v) between two binary sequences u and v of length n is the number of the places in which they differ.*

## *3. Walsh-Rademacher Transform( W-R.T )*

*The American mathematician Palely,[1] defined a new method to generate Walsh functions. His definition was based on finite products of Rademacher functions.*
*Rademcher functions were described by the German mathematician H.Rademacher(in1922),[2],where he defined a system of orthogonal functions (called Rademacher functions) that is incomplete over the normalized interval [0,1), each function assumes only the values +1 or –1 ,except at jumps , where they assume the value 0. Fig.(3.1) shows some Rademacher functions.*

*Walsh functions can be defined by using play representation as follows:*

$$\omega_0(t) \equiv R_0(t) \equiv 1 \quad \forall\, t \in [0,1] \qquad \text{.....( 3.1)}$$

$$\equiv \underline{0} \quad \textit{( in the sequence order )}$$

*where* $\underline{0}$ *is the zero vector.*

*For j>0 , we write the dyadic expansion of j :*

$$j = \sum_{k=0}^{k(j)} B_k 2^k \qquad \text{..... .(3.2)}$$

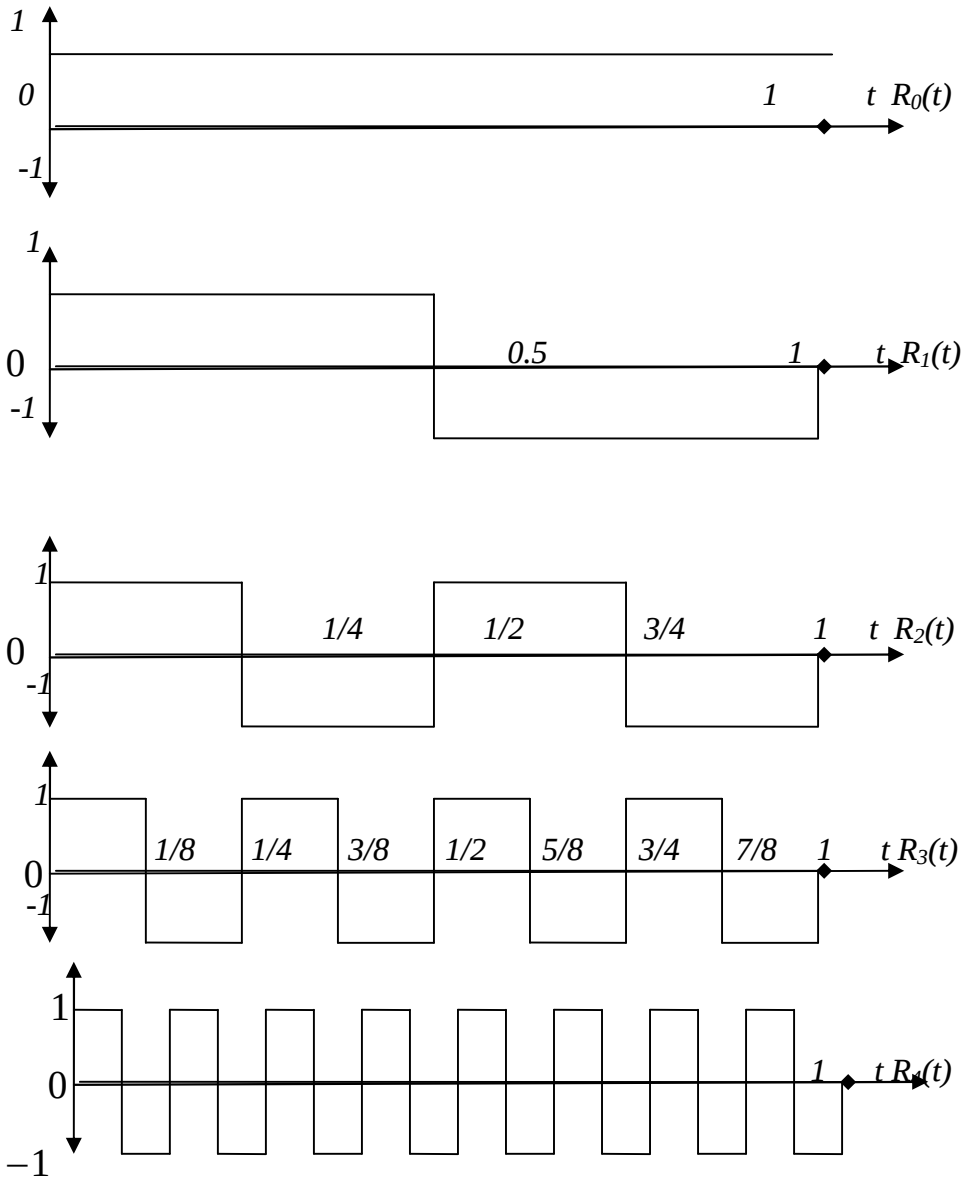
*where*

$$k(j) = [\log_2 \; j] \quad \& \quad B_k \in F_2 \;, \forall\, k = 0,1,..., k(j)$$

*and define:*

$$\omega_j(t) \equiv R_{k(j)+1}(t) \prod_{k=0}^{k(j)-1} (R_{k+1}(t))^{B_k} \qquad \text{.....(3.3)}$$

$$\equiv R_{k(j)+1} \oplus \sum_{k=0}^{k(j)-1} {}_{\oplus} (R_{k+1}(t))^{B_k} \quad \textit{( in the sequence order )}$$




$R_0 \equiv$ ( 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)

$R_1 \equiv$ (0,0,0,0,0,0,0,0,1,1,1,1,1,1,1,1)

$R_2 \equiv$ (0,0,0,0,1,1,1,1,0,0,0,0,1,1,1,1)

$R_3 \equiv$ (0,0,1,1,0,0,1,1,0,0,1,1,0,0,1,1)

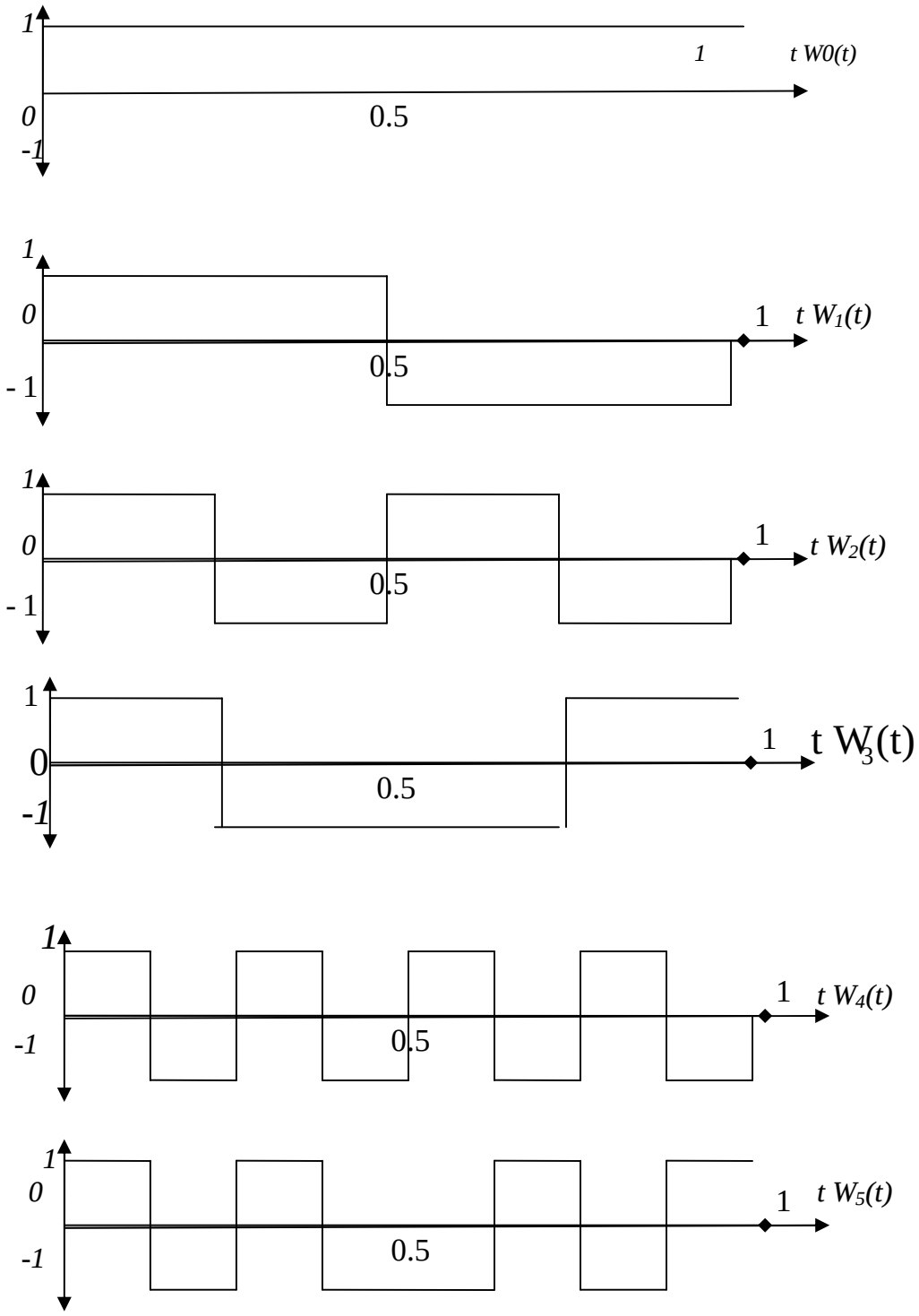
$R_4 \equiv$ (0,1,0,1,0,1,0,1,0,1,0,1,0,1,0,1)

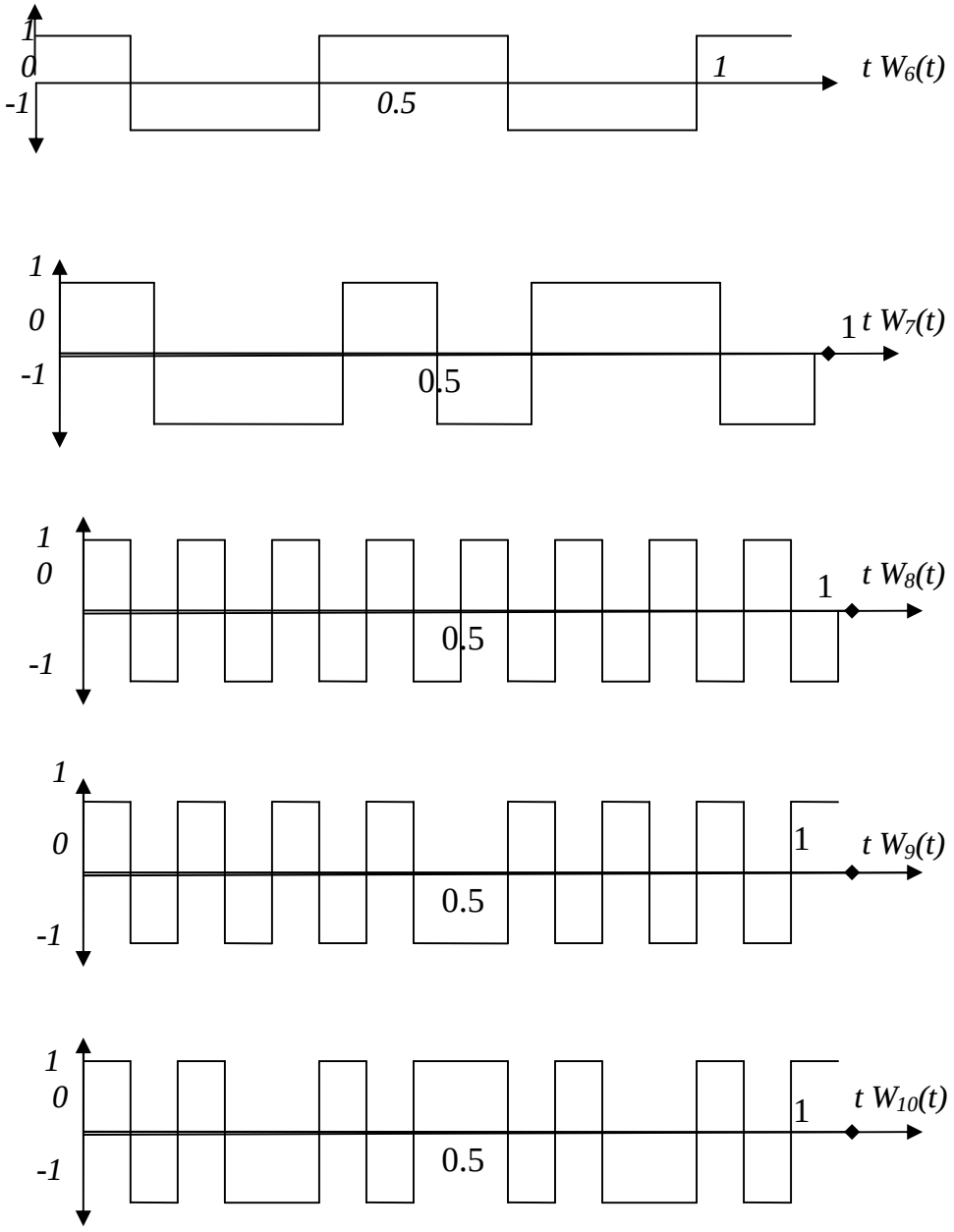
*Fig.(3.1): Graphs of $R_0, R_1, \ldots, R_4$ Rademacher functions (Rademacher sequences) .*

*The representation has the advantage that, since Rademacher functions are regular and periodic they are easy to remember and their products are easy form.Table (3.1) shows the paley representation of Walsh functions from Rademacher functions ,and drawing them in figure (3.2).*

| *Integer (j)* | *Natural binary number* $(j)_b=(B_{k(j)},\ldots,B_0)$ | $K(j)=[\log_2 j]$ | *Walsh function* $w_j$ | *Walsh functions In sequencey order* |
|---|---|---|---|---|
| *1* | *(0,01)* | *K(1)=0* | $\omega_1(t)=R_1(t)$ | $\omega_1=(0,0,0,0,1,1,1,1)$ |
| *2* | *(0,1,0)* | *K(2)=1* | $\omega_2(t)=R_2(t)$ | $\omega_2=(0,0,1,1,0,0,1,1)$ |
| *3* | *(0,1,1)* | *K(3)=1* | $\omega_3(t)=R_2(t)R_1(t)$ | $\omega_3=(0,1,0,1,0,1,0,1)$ |
| *4* | *(1,0,0)* | *K(4)=2* | $\omega_4(t)=R_3(t)$ | $\omega_4=(0,0,1,1,1,1,0,0)$ |
| *5* | *(1,0,1)* | *K(5)=2* | $\omega_5(t)=R_3(t)R_1(t)$ | $\omega_5=(0,1,0,1,1,0,1,0)$ |
| *6* | *(1,1,0)* | *K(6)=2* | $\omega_6(t)=R_3(t)R_2(t)$ | $\omega_6=(0,1,1,0,0,1,1,0)$ |
| *7* | *(1,1,1)* | *K(7)=2* | $\omega_7(t)=R_3(t)R_2(t)R_1(t)$ | $\omega_7=(0,1,1,0,1,0,0,1)$ |

*Table (3.1) the first seven Walsh functions by means of paley represntation*


1
0
-1
0.5
1
t W0(t)
1
0
- 1
0.5
1
t W1(t)
1
0
- 1
0.5
1
t W2(t)
1
0
-1
0.5
1
t W3(t)
1
0
-1
0.5
1
t W4(t)
1
0
-1
0.5
1
t W5(t)


1
0
-1
0.5
1
t W6(t)
1
0
-1
0.5
1
t W7(t)
1
0
-1
0.5
1
t W8(t)
1
0
-1
0.5
1
t W9(t)
1
0
-1
0.5
1
t W10(t)

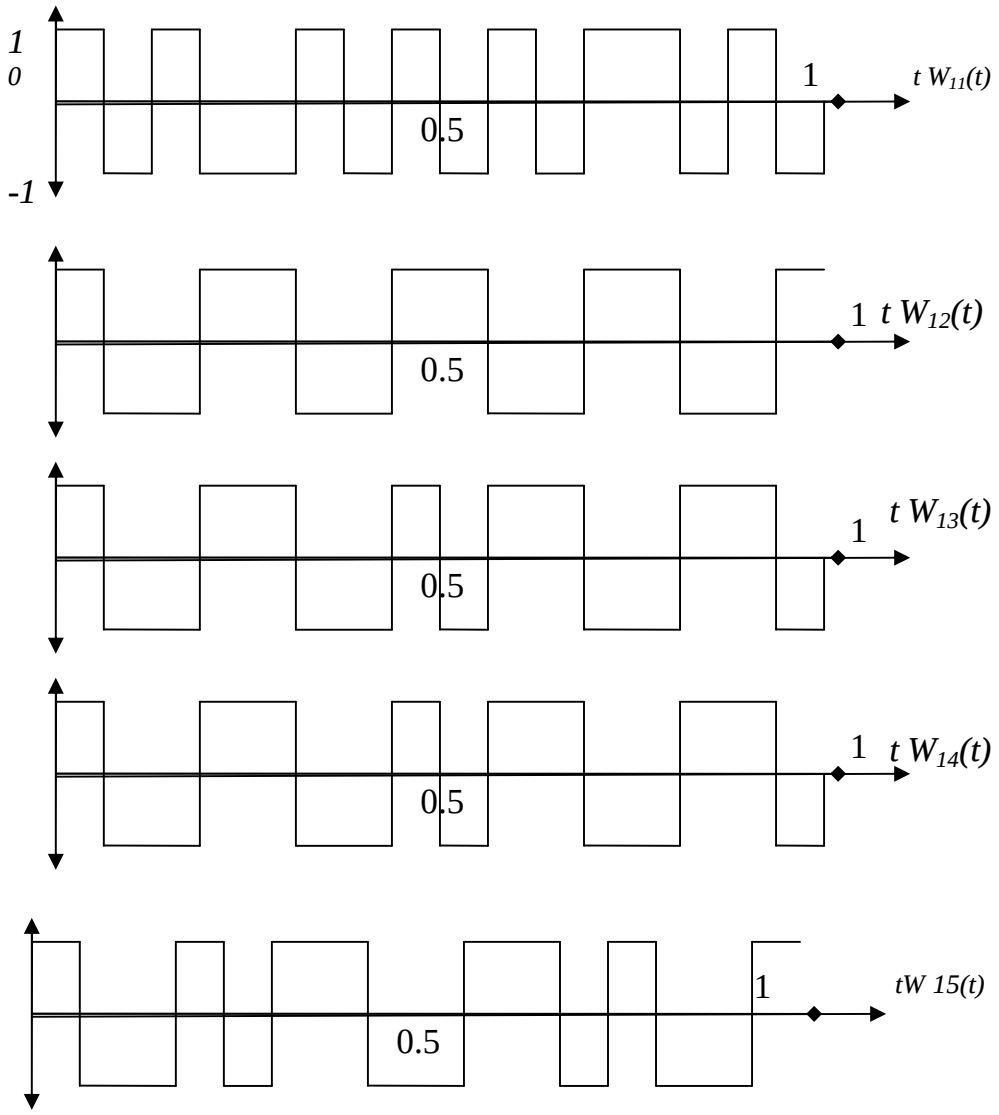



*Fig.(3.2) The first sixteen of the Walsh functions.*

## *4. The Main Result :(Spectral Coefficients of Boolean functions :*

*The spectral coefficients of Boolean functions is fownd by means of Walsh-Rademacher transform (W-R.T) and we also consider the linearity of Boolean functions from their spectrum. This shown as follows:*

*A Boolean function $f(\underline{x}) = f(x_1,x_2,\ldots,x_n)$ can be transformed from the domain $F_2 =\{0,1\}$ into the spectral domain by the linear transformation:*

$$A.B = S \quad \ldots\ldots (4.1)$$

*Where A is any $2^n \times 2^n$ orthogonal matrix ,$B=[b_0,b_1,\ldots, b_{2^n-1}]^T$ is the vector of spectral cofficients.Spectral cofficients can be calculated by using walsh functions, as follows,[3]"*

*If $i =0$ ,then $S_0$ is the number of cases when $f(\underline{x}) = 1$.*

*If $i \neq 0$ then*

$$S_j = 2^{n-1} - d(f, w_{j,i}) \quad \ldots.(4.2)$$

$$= 2^{n-1} - \omega(f, w_{j,i})$$

*where , $j= 1,2,\ldots,2^{n-1}$ , $i= 1,2,\ldots,2^{n-1}$ ,and*

*$\omega_{j,i}$ is the value of the jth Walsh function. in the ith subinterval.*

*To illustrate how this method work, consider the following example:*

*Example (1):*

*Table (4.1) shows the two valued truth vector of a Boolean functions $f^1(\underline{x})$ and $f^2(\underline{x})$ $(f^2(\underline{x}) = \underline{1} \oplus f_1(\underline{x}))$, with their spectrum by means of Walsh-Rademacher representation.*

| *Integer (j)* | $j = \sum_{k=0}^{k(j)} B_k 2^k$ | $f_1(\underline{x})$ | $S_1$ | $f_2(\underline{x})$ | $S_2$ |
|---|---|---|---|---|---|
| *0* | *(0,0,0)* | *1* | *4* | *0* | *4* |
| *1* | *(0,0,1)* | *0* | *0* | *1* | *0* |
| *2* | *(0,1,0)* | *0* | *0* | *1* | *0* |
| *3* | *(0,1,1)* | *1* | *0* | *0* | *0* |
| *4* | *(1,0,0)* | *0* | *0* | *1* | *0* |
| *5* | *(1,0,1)* | *1* | *0* | *0* | *0* |
| *6* | *(1,1,0)* | *1* | *0* | *0* | *0* |
| *7* | *(1,1,1)* | *0* | *4* | *1* | *-4* |

*Table (4.1) The spectral coefficients by using Walsh-Rademacher representation*

*In order to decide whether or not a Boolean function is linear ,we present the following definition :*

*Definition (5) :*

*A Boolean function of n-variables is affIfine if and only if* $S_0=2^{n-1}$ *and the value of the n-th order spectral coefficient is* $\pm 2^{n-1}$ *,[4].*

*Note: If the spectrum contains only two non-zero value, ,and the Boolean function is affine, then the Boolean function is linear.*

*From the example (1) , we note that, both Boolean functions* $f_1(\underline{x})$ *and* $f_2(\underline{x})$ *are linear .*

## *5- Conclusions*

*1- Generating or representing Walsh functions by means of Rademacher functions (sequences) is easy to find, than Hadamard matrices, which have many operations.*

*2- This method enable us to find the spectrum coefficients of n-variable Boolean functions, as well as to find the linearity from their spectrum.*

*3- Since Rademacher functions are regular and periodic they are easy to remember and their products are easy forms which meaus that it is more efficient than Hadamard method.*

## *6- References*

*[*] Falkowski,B.J. and Sasao T., "Unified algorithm to generate Walsh functions in four different orderings and its programmable hardware implementations", IEE proc. Vis. Image process. ,December 2005, V.152,No.6.*

*[*] Kashin,B.S.,and Saak yan A.A.,"Orthogonal Series ",Trans.of Monographs. ,1989,VoL.75.*

*[*] Porwik .P:"Towards calulation of Boolean functions nonlinearity using Walsh transform –Arch'.Theoret. Appl. Comp, Sci.Polish Acad.Sci.,Fase.No.1,2000,Vol.1.12,pp.51-64.*

*[*] Porwik .P "The spectral test of the Boolean function linearity" .Int . J.AppL.Math.Comput.Sci., 2003,Vol.13, No.4, 567-575.*