Automation and Remote Control, Vol. 64, No. 12, 2003, pp. 1938–1947. Translated from Avtomatika i Telemekhanika, No. 12, 2003, pp. 122–131.

Multiplicative Properties of Spectral Walsh Coefficients of the Boolean Function[1]

C. N. Yanushkevich

Calgary University, Calgary, Canada
Received August 15, 2003

Abstract—It is shown for the first time that spectral Walsh coefficients of the Boolean function have the structure in the form of the product of Walsh derivatives of this function. A method and an algorithm are suggested for the analysis of multiplicative properties of Walsh coefficients in terms of the behavior of the Boolean function and results of the experiments on test logic circuits are given.

1. INTRODUCTION

The use of spectral methods in practice of the logic design of circuits is limited only by polynomial forms. Thus, the Reed–Muller (Zhegalkin) polynomial is the spectrum of a logic function in the Reed–Muller basis. By analogy, the representation of the logic function by an arithmetic polynomial is equivalent to the notion of a spectrum of this function in the so-called arithmetic basis. These forms (spectra) of logic functions are widely used in practice of design because each spectral coefficient has a simple interpretation in terms of a change of the function with a change of its argument (the derivative). This simplest "behavioral" information is easily "extracted" from spectral coefficients. Consequently, the most important condition of the use of spectral methods in practice of the logic design is the possibility of extracting the structural information from spectral coefficients in terms of the behavior of a logic function and a circuit. For example, the structure of the Reed–Muller spectral coefficient is defined by the product of Boolean derivatives (the behavior of the function) to which, in its turn, we place in correspondence the behavioral characteristics of a circuit, such as the circuit sensitivity, the circuit testability, the transport of errors, etc. However, in many problems, such as the problems of optimization, verification, synchronization, and recognition of the symmetry in circuits, it is expedient to extract more complex behavioral information from local sections of the circuit. Hence, another condition of the practical use of spectral methods in the logic design of circuits follows: the information content of spectral coefficients that is expressed in the behavioral characteristics of the function and the circuit. Consequently, the investigations of new, more effective, behavioral models of Boolean functions and circuits are demanded by the practice of modern logic design.

The foregoing is the motivation of the author of this work to investigate the multiplicative properties of spectral Walsh coefficients that, as is known, have a rather large information content. Traditionally, the information content of spectral coefficients in the specified basis is measured in the additive form as a sum of the weighted counts of an input signal. In this form, the interpretation of measurements of the information content in terms of the behavioral characteristics of a Boolean function and a circuit is difficult, excepting the simplest polynomial forms. To investigate

[1] This work partially received financial backing from NATO between Canada, the USA, and Poland (NATO Collaborative Linkage, project no. PST/CLG 979071) and the Natural Sciences and Engineering Research Council of Canada (NSERC), project no. 239025-02.

multiplicative properties, it is necessary to know the derivatives of the Boolean function in the appropriate basis, and the Taylor series becomes an acceptable model for the analysis. This strategy of the solution of the problem is used in this work. Thus, the problem reduces to the formal determination of the new type of derivative of the Boolean function, which is subsequently referred to as a Walsh basis of the multiplicative properties of spectral Walsh coefficients.

The investigations of the author of this work rely on the following earlier published results.

(1) Akers [1] showed that coefficients of the Reed–Muller polynomial can be described by means of Boolean derivatives. His basic approach involves the so-called logic Taylor series.

(2) The relation between Boolean derivatives of Akers and Gibbs derivatives is set up in [2]. The latter derivatives are formally found from the expansion of Boolean functions in Walsh functions on the basis of the criterion of the dyadic shift.

(3) The arithmetic derivatives of Boolean functions are studied by Toshich [3].

(4) The spectral transformations of Boolean functions are given in [4].

(5) The technique of using the multiplicative properties of spectral coefficients in the logic design of circuits is worked out in [5, 6].

2. STATEMENT OF THE PROBLEM AND THE METHOD OF ITS SOLUTION

Initial data. We prescribe an arbitrary Boolean function f of n derivatives x_i, $i = 1, 2, \ldots, n$, and its Walsh spectrum. It is necessary to investigate multiplicative properties of these coefficients and interpret them at least in behavioral terms of the initial Boolean function. The method of the solution includes the formal definition of the Walsh derivative and the representation of the Walsh spectrum of a Boolean function in the form a Taylor series. The developed algorithms for calculating the Walsh series are investigated in an experimental way.

3. WALSH DERIVATIVES IN THE MATRIX FORM

In this section, we present theorems that define the strategy of extracting the structural information on the behavior of a Boolean function from spectral Walsh coefficients.

Theorem 1. *The Walsh derivative with respect to a variable x_i of the Boolean function of n variables is defined in the form*

$$\frac{\tilde{\tilde{\tilde{\partial}}}\mathbf{X}}{\tilde{\tilde{\tilde{\partial}}}x_i} = W_{2^n}^{(p)}\mathbf{X}, \tag{1}$$

where the matrix $W_{2^n}^{(p)}$ of dimension $2^{n-i} \times 2^{n-i}$ is called the Walsh differentiation matrix and defined as a product of n matrices

$$W_{2^n}^{(p)} = \frac{1}{2^n} W_{2^n}^{(p_1)} W_{2^n}^{(p_2)} \ldots W_{2^n}^{(p_n)}, \tag{2}$$

shaped up by the rule

$$W_{2^n}^{(p_i)} = \frac{1}{2}\begin{cases} I_{2^{i-1}} \otimes \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \otimes I_{2^{n-i}}, & p_i = 0 \\[2ex] I_{2^{i-1}} \otimes \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix} \otimes I_{2^{n-i}}, & p_i = 1, \end{cases} \tag{3}$$

where $p_1 p_2 \ldots p_n$ is the binary representation of the number p.

The proof is given in the Appendix.

Example 1. The Walsh derivative with respect to the variable x_2 of the Boolean function f of three variables ($n = 3$), which is prescribed by the vector $\mathbf{X} = [11101100]^{\mathrm{T}}$ of values, is estimated in the following way:

$$\frac{\tilde{\tilde{\partial}}\mathbf{X}}{\tilde{\tilde{\partial}}x_2} = \frac{1}{2^3} W_{2^3}^{(c)}\mathbf{X} = \mathbf{W}_{2^3}^{(p_1)}\mathbf{W}_{2^3}^{(p_2)}\mathbf{W}_{2^3}^{(p_3)}\mathbf{X},$$

where $i = 2$, $p_1p_2p_3 = 010$, while the product of matrices $W_{2^3}^{(p_1)}$, $W_{2^3}^{(p_2)}$, and $W_{2^3}^{(p_3)}$ is calculated according to (3) for $p_1 = 0,\ p_2 = 1$, and $p_3 = 1$:

$$W_{2^3}^{(p_1)}W_{2^3}^{(p_2)}W_{2^3}^{(p_3)} = \begin{bmatrix} 1 & & & & 1 & & & \\ & 1 & & & & 1 & & \\ & & 1 & & & & 1 & \\ & & & 1 & & & & 1 \\ 1 & & & & 1 & & & \\ & 1 & & & & 1 & & \\ & & 1 & & & & 1 & \\ & & & 1 & & & & 1 \end{bmatrix}$$

$$\times \begin{bmatrix} 1 & & -1 & & & & & \\ & 1 & & -1 & & & & \\ -1 & & 1 & & & & & \\ & -1 & & 1 & & & & \\ & & & & 1 & & -1 & \\ & & & & & 1 & & -1 \\ & & & & -1 & & 1 & \\ & & & & & -1 & & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & & & & & & \\ 1 & 1 & & & & & & \\ & & 1 & 1 & & & & \\ & & 1 & 1 & & & & \\ & & & & 1 & 1 & & \\ & & & & 1 & 1 & & \\ & & & & & & 1 & 1 \\ & & & & & & 1 & 1 \end{bmatrix}.$$

Finally, $\dfrac{\tilde{\tilde{\partial}}\mathbf{X}}{\tilde{\tilde{\partial}}x_2} = (1/8)[3\ 3\ \ -3\ \ -3\ 3\ 3\ \ -3\ \ -3]^{\mathrm{T}}$. Let us note that the Walsh series of the zero polarity has the form $W_0 = \dfrac{1}{2^3}(5 + (-1)^{x_3} + 3(-1)^{x_2} - (-1)^{x_2+x_3} + (-1)^{x_1} + (-1)^{x_1+x_3}(-1)^{x_1+x_2} - (-1)^{x_1+x_2+x_3})$. The coefficient $w_0^{(2)}$ is equal to a value of the Walsh derivative at the zero point: $w_0^{(2)} = \dfrac{\tilde{\tilde{\partial}}f(0)}{\tilde{\tilde{\partial}}x_2} = 3$.

Consequently, to calculate the Walsh derivative with respect to a variable x_i, it is generally necessary to multiply n weakly filled matrices. The Walsh multiple derivative is defined by analogy with the Boolean multiple derivative and the arithmetic derivative [1, 3, 5].

Theorem 2. *The Taylor expansion of an arbitrary Boolean function f of n variables with respect to Walsh functions is defined in the form*

$$W = \frac{1}{2^n}\sum_{j=0}^{2^n-1} w_c^{(j)}(-1)^{(x_1\oplus c_1)^{j_1}(x_2\oplus c_2)^{j_2}\ldots(x_n\oplus c_n)^{j_n}}, \tag{4}$$

where $c_1c_2\ldots c_n$ and $j_1j_2\ldots j_n$ identify the binary representation of the number c (the polarity) and j, respectively, and the jth coefficient is estimated as a Walsh derivative of the nth order of

Table 1. Multiplicative structure of Walsh coefficients of the first four polarities for the Boolean function $f = x_1\overline{x}_2 \vee \overline{x}_3$

Spectral Walsh coefficients / Walsh derivatives											
	$j_1j_2j_3$		000	001	010	011	100	101	110	111
c	$\mathbf{P}_c$	w	$\mathbf{X}$	$\frac{\tilde{\tilde{\partial}} f}{\tilde{\tilde{\partial}} x_3}$	$\frac{\tilde{\tilde{\partial}} f}{\tilde{\tilde{\partial}} x_2}$	$\frac{\tilde{\tilde{\partial}}^2 f}{\tilde{\tilde{\partial}} x_2 \tilde{\tilde{\partial}} x_3}$	$\frac{\tilde{\tilde{\partial}} f}{\tilde{\tilde{\partial}} x_1}$	$\frac{\tilde{\tilde{\partial}}^2 f}{\tilde{\tilde{\partial}} x_1 \tilde{\tilde{\partial}} x_3}$	$\frac{\tilde{\tilde{\partial}}^2 f}{\tilde{\tilde{\partial}} x_1 \tilde{\tilde{\partial}} x_2}$	$\frac{\tilde{\tilde{\partial}}^3 f}{\tilde{\tilde{\partial}} x_1 \tilde{\tilde{\partial}} x_2 \tilde{\tilde{\partial}} x_3}$
0	$\mathbf{W}_0$	5	1	3	1	−1	−1	1	−1	1
1	$\mathbf{W}_1$	5	0	−3	1	1	−1	−1	−1	−1
2	$\mathbf{W}_2$	5	1	3	−1	1	−1	1	1	−1
3	$\mathbf{W}_3$	5	0	−3	−1	−1	−1	−1	1	1

the Boolean function f prescribed at the point c $(x_1 = c_1, \ldots, x_n = c_n)$:

$$w_c^{(j)} = \frac{\tilde{\tilde{\partial}}^n f(c)}{\tilde{\tilde{\partial}} x_1^{j_1} \tilde{\tilde{\partial}} x_2^{j_2} \ldots \tilde{\tilde{\partial}} x_n^{j_n}}. \tag{5}$$

The coefficients $w_c^{(j)}$ (5) are called spectral Walsh coefficients of the Boolean function f.

The proof follows from the definition of the Taylor series and the Walsh derivative (1).

Theorem 2 asserts that n Walsh coefficients are equal to the Walsh derivative with respect to a variable. Therefore, the structure of information in these coefficients is completely defined by the properties of appropriate Walsh derivatives. The structure of information in $2^n - n$ coefficients is more complex and is generally estimated by means of the operation of the intersection of sets of properties. The solution of this problem is given in Section 5.

Example 2. Let us assume that the polarity $c = 3$ $(c_1c_2c_3 = 011)$ is preset. We denote $d = (x_1 \oplus c_1)^{j_1}(x_2 \oplus c_2)^{j_2}(x_n \oplus c_3)^{j_3} = (x_1 \oplus 0)^{j_1}(x_2 \oplus 1)^{j_2}(x_3 \oplus 1)^{j_3}$. According to Theorem 2, the Taylor series for an arbitrary Boolean function of three variables has the form

$$W_3 = \frac{1}{8}\sum_{j=0}^{7} w_3^{(j)}(-1)^d = \frac{1}{8}\Big(w(3) + \frac{\tilde{\tilde{\partial}} f(3)}{\tilde{\tilde{\partial}} x_3}(-1)^{\overline{x}_3} + \frac{\tilde{\tilde{\partial}} f(3)}{\tilde{\tilde{\partial}} x_2}(-1)^{\overline{x}_2} + \frac{\tilde{\tilde{\partial}}^2 f(3)}{\tilde{\tilde{\partial}} x_2 \tilde{\tilde{\partial}} x_3}(-1)^{\overline{x}_2\overline{x}_3}$$
$$+ \frac{\tilde{\tilde{\partial}} f(3)}{\tilde{\tilde{\partial}} x_1}(-1)^{x_1} + \frac{\tilde{\tilde{\partial}}^2 f(3)}{\tilde{\tilde{\partial}} x_1 \tilde{\tilde{\partial}} x_3}(-1)^{x_1\overline{x}_3} + \frac{\tilde{\tilde{\partial}}^2 f(3)}{\tilde{\tilde{\partial}} x_1 \tilde{\tilde{\partial}} x_2}(-1)^{x_1\overline{x}_2} + \frac{\tilde{\tilde{\partial}}^3 f(3)}{\tilde{\tilde{\partial}} x_1 \tilde{\tilde{\partial}} x_2 \tilde{\tilde{\partial}} x_3}(-1)^{x_1\overline{x}_2\overline{x}_3}\Big).$$

It will be said that for the Boolean function $f = x_1\overline{x}_2 \vee \overline{x}_3$, the spectral coefficients $f^{(111)}$, $f^{(101)}$, and $f^{(110)}$ are equal to the product of two Walsh derivatives, and the coefficient $f^{(111)}$ is equal to the product of three derivatives (Table 1).

4. WALSH DERIVATIVES IN THE SYMBOLIC FORM

Definition 1. The differential operator $\frac{\mathcal{L}^p}{\mathcal{L}x_i}$ (in the concise form, the $\mathcal{L}$-operator) of the Boolean function with respect to a variable x_i with the parameter $p = p_1p_2\ldots p_n$ is given in the form

$$\frac{\mathcal{L}^{p_i} f}{\mathcal{L}x_i} = f(x_1 \ldots x_i \ldots x_n) + (-1)^{p_i} f(x_1 \ldots \overline{x}_i \ldots x_n). \tag{6}$$

Table 2. Correspondence of the properties of Walsh derivatives with switching characteristics of the Boolean function

Change of the function f	$\frac{\tilde{\tilde{\partial}} f(0)}{\tilde{\tilde{\partial}} x_i} = \frac{\mathcal{L}^0 f}{\mathcal{L} x_i}$	$\frac{\tilde{\tilde{\partial}} f(1)}{\tilde{\tilde{\partial}} x_i} = \frac{\mathcal{L}^1 f}{\mathcal{L} x_i}$	Cube form
if $f_{x_i=0} = 0$ and $f_{x_i=1} = 0$, then	0	0	$\frac{\tilde{\tilde{\partial}}}{\tilde{\tilde{\partial}} x_i}[C] = \emptyset$
if $f_{x_i=0} = 0$ and $f_{x_i=1} = 1$, then	1	1	$\frac{\tilde{\tilde{\partial}} f}{\tilde{\tilde{\partial}} x_i}[C] = [C]_{x_i=b}$ or $[C]_{x_i=a}$
if $f_{x_i=0} = 1$ and $f_{x_i=1} = 0$, then	1	-1	$\frac{\tilde{\tilde{\partial}} f}{\tilde{\tilde{\partial}} x_i}[C] = [C]_{x_i=b}$
if $f_{x_i=0} = 1$ and $f_{x_i=1} = 1$, then	2	0	$\frac{\tilde{\tilde{\partial}} f}{\tilde{\tilde{\partial}} x_i}[C] = 2[C]$ or $\emptyset$

It follows from this definition that

$$\frac{\mathcal{L}^{p_i} f}{\mathcal{L} x_i} = \begin{cases} f(x_1 \ldots 1 \ldots x_n) + f(x_1 \ldots 0 \ldots x_n), \ p_i = 0 \\ f(x_1 \ldots 1 \ldots x_n) - f(x_1 \ldots 0 \ldots x_n), \ p_i = 1. \end{cases}$$

Thus, the $\mathcal{L}$-operator recognizes the behavior of the Boolean function as a value of the prescribed variable changes; namely, $\frac{\mathcal{L}^1 f}{\mathcal{L} x_i} = -\frac{\tilde{\tilde{\partial}} f}{\tilde{\tilde{\partial}} x_i}$ generates all signs of a change in the function, while $\frac{\mathcal{L}^0 f}{\mathcal{L} x_i}$ recognizes the signs when the function does not change its value with a change in the variable (Table 2).

Lemma. *The Walsh derivative with respect to a variable x_i of the Boolean function f of n variables, which is preset by the vector $\mathbf{X}$ of values, is a differential operator of order n:*

$$\frac{\tilde{\tilde{\partial}} f}{\tilde{\tilde{\partial}} x_i} = \frac{\mathcal{L}^{p_1}}{\mathcal{L} x_1}\left(\ldots\left(\frac{\mathcal{L}^{p_n} f}{\mathcal{L} x_n}\right)\right), \tag{7}$$

where $p_i = 1$ and $p_j = 0$ for $j \neq i$.

Proof. Relation (7) directly follows from the n-iterative transformation (1).

The Walsh derivative with respect to a variable x_i corresponds to the standard configuration "butterfly" of the operational graph because the matrix $\widetilde{D}_{2^{n-i}}$ is the matrix of the ith iteration of the Walsh transform. Consequently, the algorithm for calculating the Walsh derivative reduces to the classical algorithm of the fast Walsh transform. The difference lies only in the interpretation: the iteration corresponds to the Walsh derivative with respect to the variable, while the prescribed sequence of iterations corresponds to the multiple Walsh derivative. The limitations of the algorithm are obvious: it is difficult to calculate the Walsh spectrum of the Boolean function of more than 20 variables.

5. EXTRACTION OF STRUCTURAL PROPERTIES OF INFORMATION

In this section, we will solve three problems. The first problem is stated as the extraction of the structural information from spectral Walsh coefficients prescribed in the multiplicative form (by the product of derivatives). The second problem consists in developing the effective algorithm of the calculation of Walsh derivatives and, on this basis, developing the algorithm of the calculation of the Walsh spectrum (the Walsh form of a Boolean function) by means of a Taylor series. The third problem lies in the acceptable union of the methods of solving the two preceding problems.

5.1. Representation of the Boolean Function by Cubes

We denote by $x_i^{c_i}$ a literal of the Boolean function x_i, i.e., $x_i^{c_i} = \overline{x}_i$ if $c_i = 0$ and $x_i^{c_i} = x_i$ if $c_i = 1$. The product of the literals $x_1^{c_1} x_2^{c_2} \dots x_1^{c_n}$ is a term. The variable x_i, which is unavailable in the singular cube, will be designated as $c_i = \mathbf{x}$, i.e., $x_i^{\mathbf{x}} = 1$. The vector $[c_1 c_2 \dots c_n]$ with elements $c_i \in \{0,\ 1,\ \mathbf{x}\}$ is a cube describing the term $x_1^{c_1} x_2^{c_2} \dots x_1^{c_n}$. For example, the function $f = x_1 x_2 \vee \overline{x}_3$ is described by the set of cubes [1 1 x] and [x x 0]. The set of cubes corresponds to unit values of the Boolean function and represents the sum of literals or the sum-of-products (SOP) form.

5.2. Operations on Cubes

New cubes can be set up by means of the simplest OR, AND, and EXOR logic operations on two cubes by the rules

AND

C_i / C_j	0	1	**x**
0	0	∅	0
1	∅	1	1
x	0	1	**x**

OR

C_i / C_j	0	1	**x**
0	0	**x**	**x**
1	**x**	1	1
x	**x**	1	**x**

EXOR

C_i / C_j	0	1	**x**
0	0	**x**	1
1	**x**	1	0
x	1	0	**x**

For example, for the cubes [11**x**] and [10**x**], we obtain $[11\mathbf{x}] \wedge [10\mathbf{x}] = [1\emptyset\mathbf{x}] = \emptyset$, $[11\mathbf{x}] \vee [10\mathbf{x}] = [1\mathbf{xx}]$, and $[11\mathbf{x}] \oplus [10\mathbf{x}] = [1\mathbf{xx}]$.

5.3. Cubes of Reed–Muller Polynomials

Let the SOP form of the function f be preset by cubes. To represent this function in the Reed–Muller form, we use the relation $x \vee y = x \oplus y \oplus xy$. Consequently, the cube of the Reed–Muller polynomial is made up according to the relation

$$[C_1] \vee [C_2] = [C_1] \oplus [C_2] \oplus [C_1][C_2]. \tag{8}$$

The cubes in the right side of relation (8) represent the terms entering into the Reed–Muller spectrum. For example, $x_1 x_2 \oplus x_1$ is represented by the cubes [1 1] and [1 **x**].

5.4. Cubes of Arithmetic Polynomials

To represent functions in the arithmetic form, use is made of the relation $x \vee y = x + y - xy$. Therefore, the cube of the arithmetic polynomial is set up by the relation

$$[C_1] \vee [C_2] = [C_1] + [C_2] - [C_1][C_2]. \tag{9}$$

For example, in accordance with (9), for the cube $[C_1] = [\mathbf{x}\ 1\ 0\ \mathbf{x}\ 0\ 1\ 1\ \mathbf{x}\ \mathbf{x}]$ and the cube $[C_2] = [\mathbf{x}\ 1\ 0\ 1\ \mathbf{x}\ \mathbf{x}\ 1\ \mathbf{x}\ 1]$, three cubes are shaped up: $[C_1]$, $[C_2]$, and a new cube $-[C_1][C_2] = -[\mathbf{x}\ 1\ 0\ 1\ 0\ 1\ 1\ \mathbf{x}\ 1]$. The result $[C_1] + [C_2] - [C_1][C_2]$ corresponds to the arithmetic polynomial $\overline{x}_2 x_3 \overline{x}_5 x_6 x_7 + x_2 \overline{x}_3 x_4 x_7 x_8 - x_1 \overline{x}_2 x_3 \overline{x}_4 x_5 x_6 x_8$.

Table 3. Operations on cubes of the Walsh form

Cube	$\dfrac{\mathcal{L}^1}{\mathcal{L}x_i}$	$\dfrac{\mathcal{L}^0}{\mathcal{L}x_i}$
$[C]_{x_i=0}$	$[C]_{x_i=\mathbf{x}}$	$[C]_{x_i=b}$
$[C]_{x_i=1}$	$[C]_{x_i=\mathbf{x}}$	$[C]_{x_i=a}$
$[C]_{x_i=\mathbf{x}}$	$2[C]_{x_i=\mathbf{x}}$	$\emptyset$

Table 3 lists operations on cubes with the aid of the $\mathcal{L}$-operator (the plus sign and the value equal to unity are not noted). Here $[C]_{x_i=a}$ denotes a cube. For example, the cube obtained a result of the operation $-\overline{x}_1x_2+x_1x_2=(-\overline{x}_1+x_1)x_2=(-1)^{\overline{x}_1}x_2$ is denoted by $[C]_{x_i=a}$. Correspondingly, $-x_1x_2+\overline{x}_1x_2=(-x_1+\overline{x}_1)x_2=(-1)^{x_1}x_2$ is denoted by $[C]_{x_i=b}$.

The properties listed below of differential operators follow from Table 3:

$$\begin{aligned}
\frac{\mathcal{L}^0}{\mathcal{L}x_i}[C]_{x_i=1} &= [C]_{x_i=a},\\
\frac{\mathcal{L}^0 f}{\mathcal{L}x_i}[C]_{x_i=0} &= [C]_{x_i=b},\\
\frac{\mathcal{L}^0 f}{\mathcal{L}x_i}[C]_{x_i=\mathbf{x}} &= \emptyset,\\
\frac{\mathcal{L}^1 f}{\mathcal{L}x_i}[C]_{x_i=0} &= \frac{\mathcal{L}^1 f}{\mathcal{L}x_i}[C]_{x_i=1} = [C]_{x_i=\mathbf{x}},\\
\frac{\mathcal{L}^1 f}{\mathcal{L}x_i}[C]_{x_i=1} &= 2[C]_{x_i=\mathbf{x}}.
\end{aligned}$$

5.5. Arithmetic Cubes of the Walsh Form

To calculate Walsh coefficients, we use the cubes of arithmetic polynomials.

Theorem 3. *The Walsh derivative with respect to a variable x_i of the Boolean function of n variables is equal to the sum of Walsh derivatives of cubes $[C_i]$ in the Walsh form*

$$\frac{\tilde{\tilde{\partial}} f}{\tilde{\tilde{\partial}} x_i}=\sum_{i=1}^{t}\frac{\tilde{\tilde{\partial}}}{\tilde{\tilde{\partial}} x_i}[C_i]. \tag{10}$$

Proof. A cube of the Walsh form is made up according to relation (7) in n iterations by way of the use of the operator $\mathcal{L}^{p_i}$ n times. This cube is an additive component of the Walsh derivative (10).

Example 3. There is a need to calculate the Walsh coefficient $w^{(9)}$ of the Boolean function f of five variables for $p=0$ prescribed by cubes of the arithmetic form. To solve this problem, we will use the $\mathcal{L}^0$-operator. As a result, we obtain

$$\frac{\mathcal{L}^0 f}{\mathcal{L}x_4}=\frac{\mathcal{L}^0}{\mathcal{L}x_4}\begin{matrix}+\\+\\+\\+\\-\end{matrix}\begin{bmatrix}0&\mathbf{x}&0&1&\mathbf{x}\\1&\mathbf{x}&\mathbf{x}&1&1\\0&1&\mathbf{x}&\mathbf{x}&1\\1&1&\mathbf{x}&\mathbf{x}&0\\\mathbf{x}&0&\mathbf{x}&0&0\end{bmatrix}=\begin{matrix}+\\+\\+\\+\\-\end{matrix}\begin{bmatrix}0&\mathbf{x}&0&\mathbf{x}&\mathbf{x}\\1&\mathbf{x}&\mathbf{x}&\mathbf{x}&1\\0&1&\mathbf{x}&\mathbf{x}&1\\1&1&\mathbf{x}&\mathbf{x}&0\\\mathbf{x}&0&\mathbf{x}&\mathbf{x}&0\end{bmatrix}\begin{matrix}1\\1\\2\\2\\1\end{matrix}.$$

We will write the matrix expression in the symbolic form

$$\frac{\mathcal{L}^0 f}{\mathcal{L}x_4} = \frac{\mathcal{L}^0}{\mathcal{L}x_4}[0\mathbf{x}01\mathbf{x}] + \frac{\mathcal{L}^0}{\mathcal{L}x_4}[1\mathbf{xx}11] + \frac{\mathcal{L}^0}{\mathcal{L}x_4}[01\mathbf{xx}1] + \frac{\mathcal{L}^0}{\mathcal{L}x_4}[11\mathbf{xx}0] - \frac{\mathcal{L}^0}{\mathcal{L}x_4}[\mathbf{x}0\mathbf{x}00]$$
$$= \overline{x}_1\overline{x}_3 + x_1x_5 + 2\overline{x}_1x_2x_5 + 2x_1x_2\overline{x}_2\overline{x}_5 - \overline{x}_2\overline{x}_5.$$

Consequently, $w^{(2)} = \left.\frac{\mathcal{L}^0 f}{\mathcal{L}x_4}\right|_{p=00010} = 1 + 0 + 0 + 0 - 1 = 0.$

We will clarify by way of the following example the calculation of spectral Walsh coefficients corresponding to Walsh derivatives of the order higher than the 1st order.

Example 4. It is necessary to estimate the Walsh derivative $\frac{\tilde{\tilde{\partial}}^2 f}{\tilde{\tilde{\partial}} x_1 \tilde{\tilde{\partial}} x_3}$ for the Boolean function prescribed in the arithmetic form $f = [10\mathbf{x}] + [\mathbf{xx}0] - [100]$. To solve this problem, we will use the $\mathcal{L}^0$-operator with respect to the variable x_2 and the $\mathcal{L}^1$-operator with respect to the variables x_1, and x_3:

$$\frac{\tilde{\tilde{\partial}}^2 f}{\tilde{\tilde{\partial}} x_1 \tilde{\tilde{\partial}} x_3} = \frac{\mathcal{L}^1}{\mathcal{L}x_1}\left(\frac{\mathcal{L}^0}{\mathcal{L}x_2}\left(\frac{\mathcal{L}^1 f}{\mathcal{L}x_3}\right)\right) = \frac{\mathcal{L}^1}{\mathcal{L}x_1}\left(\frac{\mathcal{L}^0}{\mathcal{L}x_2}([\mathbf{xx}b] - [10b])\right)$$
$$= \frac{\mathcal{L}^1}{\mathcal{L}x_1}(2[\mathbf{xx}b] - [1\mathbf{x}b]) = -[a\mathbf{x}b] = -(-1)^{\overline{x}_1 + x_3}.$$

6. RESULTS OF THE EXPERIMENTS AND DISCUSSION

The experiments were performed on a Pentium III-type computer of 450 MHz, 128 Mb RAM. The program for calculations of the Walsh derivatives and the Walsh spectrum is written in the language C++.[2] We used in the experiments more than thirty test circuits from the LGSynth 93 base.[3] The program of the experiments included the following: the calculation of individual spectral components and groups of spectral components, the analysis of distributions of changes

Table 4. Results of experimental investigations of the algorithm for calculating the Walsh spectrum on the basis of the Taylor series

Test			Walsh spectrum [time(s)]/cubes, $p = 0$			Walsh spectrum [7]	
name	I/O	cubes	256	1024	4096	256	1024
apex4	9/19	1372	0.500 (1726)	–	–	0.02	–
ex1010	10/10	1471	0.561 (1181)	2.251 (1471)	–	0.02	0.06
alu4	14/8	1028	0.232 (2567)	2.040 (5444)	11.592 (9270)	0.01	0.04
misex3	14/14	1848	0.182 (1071)	2.430 (3732)	16.752 (8200)	0.01	0.07
add6	13/7	607	0.082 (133)	0.180 (607)	2.970 (2537)	0.01	0.02
duke2	22/29	242	0.135 (148)	0.120 (189)	0.160 (218)	0.01	0.02
vg2	25/8	110	0.000 (104)	0.000 (163)	0.110 (261)	0.01	0.02
misex2	25/18	29	0.000 (26)	0.000 (26)	0.000 (26)	<0.01	0.02
e64	65/65	65	0.001 (65)	0.160 (65)	0.280 (65)	0.02	0.06
Sum		6772	1.783 (7021)	7.181 (11697)	31.864 (20577)	<0.130	0.310

[2] The program is accessible by the address http://www.ucalgary.ca/People/yanush/research/spectra.html.
[3] http://www.cbl.ncsu.edu/CBL_Docs/lgs93.html.

of functions (Walsh derivatives) in separate sections of the spectrum, and the investigation of statistical distributions of changes, which is necessary in the analysis, for example, the capacity of the scattering of circuits, the recognition of symmetries, and the solution of verification problems.

A fragment of the results of an experiment is shown in Table 4, in which **Name** is the designation of the test circuit and **I/O** is the number of inputs/outputs in the circuit. In the experiments, we used circuits of up to 100 inputs and outputs (the circuit `e64` in Table 4 has the dimension of 64 inputs and 64 outputs). The number of singular cubes of the circuit is shown in the column **Cubes**. The following four columns present the time of calculations of the first 256, 1024, and 4096 Walsh coefficients of the zero polarity ($p = 0$); the optimized number of cubes of the Walsh form is given in brackets. From the results listed in Table 4, we define the following:

(1) To extract the behavioral characteristics of the Boolean function from the multiplicative structure of Walsh coefficients, it is necessary to have quite an acceptable number of cubes of the Walsh form. Consequently, the choice of the method of cubes is experimentally valid;

(2) The time it takes to calculate Walsh derivatives (the main component of the time taken for the estimation of the Walsh spectrum) is quite acceptable. To confirm this conclusion, Table 4 provides the comparison of the results with the best known package [7] (the last two rows) that implements the method of solving diagrams. Let us note that the advantage of this package in regard to time is of no importance in problems of the logic design, in which it is necessary to calculate only individual components.

7. CONCLUSIONS

Using the Walsh spectrum of Boolean functions as an example, the suggestion is made to refine the statement of the problem for the more effective use of spectral methods in the systems of the logic design of circuits. It is shown that the multiplicative structure of the information in terms of spectral coefficients is an acceptable base for the interpretation of behavioral characteristics of a logic function (Table 2). The obtained results are reassuring, and it is advisable to elaborate them for establishing the correspondence between the informational structure of spectral coefficients and the behavioral characteristics of a circuit.

APPENDIX

Proof of Theorem 1. From the definition of the Hadamard matrix $H_{2^n} = \bigotimes^n \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, where $H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, it follows that we define the expression $H_{2^n}^{(c)} = \frac{1}{2^n} H_2^{(c_1)} \otimes \ldots \otimes H_2^{(c_n)}$ for the Walsh transform of the polarity c, where $H_2^{(0)} = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ and $H_2^{(1)} = \begin{bmatrix} -1 & 1 \\ 1 & 1 \end{bmatrix}$. The factorized Walsh transform has the form $H_{2^n}^{(c)} = \frac{1}{2^n} H_{2^n}^{(c_1)} H_{2^n}^{(c_2)} \ldots H_{2^n}^{(c_n)}$, where the matrix $H_{2^n}^{(c_i)}$ is shaped up by the rule

$$H_{2^n}^{(c_i)} = \frac{1}{2} \begin{cases} I_{2^{i-1}} \otimes \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes I_{2^{n-i}}, & c_i = 0 \\ \\ I_{2^{i-1}} \otimes \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \otimes I_{2^{n-i}}, & c_i = 1. \end{cases}$$

Here, $c_1c_2\ldots c_n$ is the binary representation of the polarity c. Therefore, the Walsh transformation matrix corresponds to each of the 2^n polarities. The matrix structures of factorized spectral transformations in various basic systems of functions are identical [8]. Consequently, it is admissible to generalize the structure of the Boolean and the arithmetic derivative [6] for the Walsh differentiation matrix. The elementary Walsh differentiation matrices of the zero and the first polarity are equal to $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}$, respectively. According to (6), from the rows of these matrices, we form the rows of the matrices $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ and $\begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$ of the zero and the unit polarity. Applying the same rules to the Walsh transformation matrices of dimension $2^n \times 2^n$, we obtain Walsh differentiation matrices with respect to variables $x_1^{p_1}, \ldots, x_n^{p_n}$, where $x_i^0 = 1$ and $x_i^1 = x_i$. For example, using the differentiation matrix $W_{2^3}^{(101)}$, we calculate Walsh derivatives of the second order with respect to variables x_1 and x_3. The relation used for calculating the Walsh differentiation matrix has the form $W_{2^n}^{p} = \dfrac{1}{2^n} W_2^{p_1} \otimes \ldots \otimes W_2^{p_n}$, where $W_2^0 = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$ and $W_2^1 = \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}$. Expression (1) is the factorized form of this expression.

REFERENCES

1. Akers, S.B., On a Theory of Boolean Functions, *SIAM J.*, 1959, vol. 7, no. 4, pp. 487–498.
2. Edwards, C.R., The Gibbs Dyadic Differentiator and Its Relationship to the Boolean Difference, *Comput. Electron. Eng.*, 1978, vol. 5, no. 4, pp. 335–344.
3. Toshich, Zh., *Arifmeticheskie predstavleniya logicheskikh funktsii. Diskretnye avtomaty i seti svyazi* (Arithmetic Representations of Logic Functions. Discrete Automata and Communication Networks), Moscow: Nauka, 1970.
4. Shmerko, V.P., Synthesis of the Arithmetic Forms of Boolean Functions by Means of the Fourier Transform, *Avtom. Telemekh.*, 1989, no. 5, pp. 134–142.
5. Yanushkevich, S.N., Development of Methods of the Boolean Differential Calculus for the Arithmetic Logic, *Avtom. Telemekh.*, 1994, no. 5, pp. 121–137.
6. Yanushkevich, S.N., Systolic Algorithms of Synthesis of Arithmetic Polynomial Forms of the k-Valued Functions of the Boolean Algebra, *Avtom. Telemekh.*, 1994, no. 12, pp. 128–142.
7. Jankovic, D., Stankovic, R., and Drechsler, R., Decision Diagram Method for Calculation of Pruned Walsh Transform, *IEEE Trans. Comput.*, 2001, vol. 50, no. 2, pp. 147–157.
8. Sadykhov, P.Kh., Chegolin, P.M., and Shmerko, V.P., *Obrabotka signalov v diskretenykh bazisakh* (Processing of Signals in Discrete Bases), Minsk: Nauka i Tekhnika, 1986.

This paper was recommended for publication by P.P. Parkhomenko, a member of the Editorial Board