Int. J. Appl. Math. Comput. Sci., 2006, Vol. 16, No. 1, 271–278

DEDICATED SPECTRAL METHOD OF BOOLEAN FUNCTION DECOMPOSITION

PIOTR PORWIK*, RADOMIR S. STANKOVIĆ**

* Institute of Informatics, University of Silesia
ul. Będzińska 39, 41–200 Sosnowiec, Poland
e-mail: porwik@us.edu.pl

** Department of Computer Science, Faculty of Electronics, University of Niš
Beogradska 14, 18 000 Niš, Serbia
e-mail: rstankovic@bankerinter.net

Spectral methods constitute a useful tool in the analysis and synthesis of Boolean functions, especially in cases when other methods reduce to brute-force search procedures. There is renewed interest in the application of spectral methods in this area, which extends also to the closely connected concept of the autocorrelation function, for which spectral methods provide fast calculation algorithms. This paper discusses the problem of spectral decomposition of Boolean functions using the Walsh transform and autocorrelation characteristics.

Keywords: Boolean function, Walsh spectrum, autocorrelation coefficients, disjoint decomposition

1. Introduction

The decomposition of Boolean functions is a basic technique which has been often used in logic design from the pioneering work by Ashenhurst (1957) and Curtis (1962), and now decomposition appears very efficient in FPGA and Look-up-table (LUT) based synthesis, see, e.g., (Lai *et al.*, 1993; Nowicka *et al.*, 1999; Sasao and Matsuura, 2004).

Because dealing with functions in large numbers of variables is nowadays a standard engineering practice, decomposition methods are important and are becoming a standard part of many CAD systems in this area. There are numerous decomposition methods based on various data structures for the representation of Boolean functions. For example, classical approaches are based on the application of decomposition charts similar to the Karnaugh map with a different ordering for the cell location (Curtis, 1962), and such methods were efficiently revised recently by (Mishchenko *et al.*, 2001; Sasao and Butler, 1997). The representations of Boolean functions in terms of Walsh coefficients were a basis for the decomposition of functions by spectral methods (Falkowski and Kannurao, 2001; Tokmen, 1980), see also (Hurst *et al.*, 1985). More recently, Decision Diagrams (DDs) have proven efficient in the derivation of decomposition methods for logic functions, see, e.g. (Lai *et al.*, 1993; Stanković and Falkowski, 2002; Stanković and Astola, 2003; Sasao and Matsuura, 2004).

Nowadays, in many investigations, decomposition based on the analysis of autocorrelation coefficients is still expanded in many areas, such as the optimization of combinational logic (Tomczuk, 1996) or the estimation of Boolean function complexity (Karpovsky, 1976; Karpovsky *et al.*, 2003).

Some Boolean functions express conveniently autocorrelation and spectral characteristics (Karpovsky, 1976). Accordingly, decomposition methods by the analysis of autocorrelation coefficients have been proposed in many papers (Karpovsky, 1976; Rice and Muzio, 2003; Tomczuk, 1996). These deterministic methods are efficiently compared with related heuristic methods (Bertacco and Damiani, 1997; Dubrova, 1999; Rice and Muzio, 2003). The efficiency of these methods depends on the computational complexity of the autocorrelation coefficients. For that reason, a new method for an efficient (in terms of space and time) calculation of autocorrelation coefficients was introduced.

A method for the reduction of the number of nodes in decision diagrams by exploiting the autocorrelation function was described in (Karpovsky *et al.*, 2003). Additionally, the same approach was used for function partitioning into linear and non-linear parts, which can be viewed as a particular case of functional decomposition (Karpovsky, 1976). In many cases, heuristic methods of partitioning input variables are used, where information measures are analyzed (Rawski *et al.*, 2001). In other words, it allows us to analyze what information between inputs and outputs of circuit is common, missing, different, etc.

In this paper, we present a method for a simple disjoint decomposition of Boolean functions by the analysis of their autocorrelation coefficients. The problem of finding a simple disjoint decomposition can be treated as splitting a given function into two parts. First, we determine whether the decomposition is possible by the analysis of autocorrelation coefficients. In the next step, we search for related subfunctions by means of a spectral method. The presented algorithm enables the user to select a subfunction in the decomposition depending on the designer's assumptions, from a class of functions whose autocorrelation characteristic is known, e.g., linear, affine, bent, majority, minority functions, etc. This property can be considered as a distinctive feature compared with the existing methods. It should be stressed that the presented method can be applied to single-output fully specified functions.

2. Preliminaries

A Boolean function is defined as a mapping $f : \{0,1\}^n \rightarrow \{0,1\}$. To each n-tuple representing an assignment of values for the variables $x = (x_0, \ldots, x_{n-1})$, $x_i \in \{0,1\}$, an integer x from the set $\{0, 1, \ldots, 2^n - 1\}$ can be assigned by the mapping $x = \sum_{i=0}^{n-1} x_i 2^{n-1-i}$. This value for x is called the decimal index for the given n-tuple.

An n-variable Boolean function f can be specified by enumerating its values at all decimal indices, which can be conveniently represented by a vector of function values $\mathbf{Y} = [y_0, y_1, \ldots, y_{2^n-1}]^T$, called the truth vector for f.

Alternatively, a Boolean function can be represented as a Sum-of-Products expression defined as follows:

Definition 1. An *n-variable Boolean function* $f(x_0, x_1, \ldots, x_{n-1})$ can be represented as $\sum_{j=0}^{2^n-1} y_j x_0^{c_0} x_1^{c_1} \cdots x_{n-1}^{c_{n-1}}$, where y_j is the value of f for the decimal index j, and $c_0, c_1, \ldots, c_{n-1} \in \{0,1\}$ are coordinates in the binary representation for j and $x_i^{c_i=0} = \overline{x}_i$, $x_i^{c_i=1} = x_i$ for $i = 0, 1, \ldots, n-1$.

Example 1. The truth vector of the three-variable Boolean function $f(x_0, x_1, x_2) = \overline{x}_0\overline{x}_1\overline{x}_2 + \overline{x}_0\overline{x}_1 x_2 + \overline{x}_0 x_1 x_2 + x_0\overline{x}_1 x_2 + x_0 x_1 x_2$ is $\mathbf{Y} = [1,1,0,1,0,1,0,1]$. ♦

Definition 2. The *Hamming weight* $w(\mathbf{Y})$ of a Boolean vector $\mathbf{Y}$ is equal to the number of nonzero elements in $\mathbf{Y}$.

3. Spectral Description of Boolean Functions

Spectral data are used in many applications in digital logic design. A Boolean function $f(x_0, x_1, \ldots, x_{n-1})$ given by the truth vector $\mathbf{Y} = [y_0, y_1, \ldots, y_{2^n-1}]^T$ can be transformed from the Boolean domain $\{0,1\}$ into the spectral domain by a linear transformation $\mathbf{H} \cdot \mathbf{Y} = \mathbf{S}$, where $\mathbf{H}$ is a $2^n \times 2^n$ transform matrix, and $\mathbf{S} = [s_0, s_1, \ldots, s_{2^n-1}]^T$ is the vector of spectral coefficients called the spectrum for f (Ahmed, 1975; Falkowski and Porwik, 1999; Karpovsky, 1976; Porwik, 2004b; Yanushkevich, 1998).

In particular, we get the Walsh transform when $\mathbf{H}$ is the Walsh matrix defined as

$$\mathbf{W}(n) = \bigotimes_{i=1}^{n} \mathbf{W}(1), \tag{1}$$

where

$$\mathbf{W}(1) = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

is the basic Walsh matrix and '$\otimes$' denotes the Kronecker product.

In a Walsh matrix, the Walsh functions $wal(i,x)$, which are the rows of the Walsh matrix, are in the so-called Hadamard order. Thus, the spectrum calculated by the application of this transform matrix is a Walsh-Hadamard spectrum. In a study of the decomposability of Boolean functions it may be convenient to use also the Walsh transform defined in terms of Walsh functions in the Paley ordering. In this case, we talk about the Walsh-Paley spectrum. Recall that between these orderings there is the relation $wal_H(i,x) = wal_P(b(i),x)$, where $b(i)$ is obtained by the bit-reversal of i, and H and P denote the Hadamard and Paley orderings, respectively. The spectral coefficients $s_i \in \mathbf{S}$ in the Paley ordering will be used, because the matrix equations described in the next parts of the paper have a convenient structure for such an ordering.

In this paper, we exploit also another important concept, namely, that of the autocorrelation function for functions on $\{0,1\}^n$.

Definition 3. The *autocorrelation function* of a given function $f(x)$ is defined as follows (Stanković and Astola, 2003):

$$b_\tau = \sum_{x=0}^{2^n-1} f(x) f(x \oplus \tau) = \sum_{x=0}^{2^n-1} (-1)^{f(x) \oplus f(x \oplus \tau)}, \tag{2}$$

where $\tau \in \{0, 1, \ldots, 2^n - 1\}$, $\tau = \sum_{k=0}^{n-1} \tau_k 2^{n-1-k}$, $\tau_k \in \{0,1\}$. The autocorrelation coefficients are conveniently represented as a vector $\mathbf{B} = [b_0, b_1, \ldots, b_{2^n-1}]$.

It can be shown that due to the Wiener-Khinchin theorem, the autocorrelation function can be calculated as (Karpovsky *et al.*, 2003):

$$b_\tau = 2^{-n} \sum_{x=0}^{2^n-1} (s_x)^2 (-1)^{\langle x, \tau \rangle}, \tag{3}$$

where $\langle x, \tau \rangle$ is the scalar product of the vectors $x = [x_0, x_1, \ldots, x_{n-1}]$ and $\tau = [\tau_0, \tau_1, \ldots, \tau_{n-1}]$

through their binary representations, i.e., $\langle x, \tau \rangle = [x_0, x_1, \ldots, x_{n-1}] \cdot [\tau_0, \tau_1, \ldots, \tau_{n-1}]^T = x_0\tau_0 \oplus x_1\tau_1 \oplus \cdots \oplus x_{n-1}\tau_{n-1}$.

It is easy to see that the complexity of computations of autocorrelation coefficients is $O(n2^n)$ (Karpovsky, 1976; Tomczuk, 1996). In this paper, the autocorrelation coefficients will be calculated by (3).

4. Spectral Linearization of a Boolean Function

A useful property of Walsh functions is that they take only two values ± 1, and in that respect they are compatible with two-valued switching functions. If the values of the truth vector of a Boolean function f will be encoded according to the formula $\{0,1\} \to \{1,-1\}$, then such a vector will be denoted as $\mathbf{Y}_f$. For a given vector $\mathbf{Y}_f = [y_0, y_1, \ldots, y_{2^n-1}]$, the scalar product $s_i = \langle \mathbf{Y}_f, wal(i,t) \rangle = \sum_t y_t wal(i,t)$ determines the correlation between the Boolean function f and the appropriate i-th Walsh function. In this paper, the set of spectral coefficients $\{s_0, s_1, \ldots, s_{2^n-1}\} \in \mathbf{S}$ is determined on the basis of the encoding of elements of the vector $\mathbf{Y}_f$ according to the formula $y_i \to 1 - 2y_i$.

Definition 4. A Boolean function $f(x_0, x_1, \ldots, x_{n-1})$ of n-variables is called *affine* if it can be represented as $f(x) = a_0x_0 \oplus a_1x_1 \cdots \oplus a_{n-1}x_{n-1} \oplus c$, where $a_j, c \in \{0,1\}$ and $k = c + \sum_{i=0}^{n-1} a_i 2^i$. In particular, if $c = 0$, then f is called a *linear function*.

Theorem 1. (Porwik, 2004a) *Any affine Boolean function f, encoded according to $\{0,1\} \to \{1,-1\}$, is characterized by the following unique Walsh-Hadamard spectrum distribution:*

$$s_x = \begin{cases} (-1)^c \times 2^n & \text{for } x = \dfrac{1}{2}(k-c), \\ 0 & \text{otherwise}, \end{cases} \tag{4}$$

where k and c have the same meaning as in Definition 4, and $x = 0, 1, \ldots, 2^n - 1$.

Thus, in order to decide whether a Boolean function is affine, it is sufficient to calculate its spectrum. The spectrum contains only one nonzero value: $s_x = +2^n$, if f is a linear, or $s_x = -2^n$, if f has complement form.

It can be noticed that the spectrum can also be performed by means of the so-called $\mathbf{R}$-type coefficients, where the values of a Boolean function are not encoded (Hurst *et al.*, 1985). Between the coefficients of different types, a simple correlation can be observed: $r_0 = (2^n - s_0)/2$ and $r_i = -s_i/2$ (Hurst *et al.*, 1985). Taking into account the above discussion, Theorem 1 can be formulated in another form.

Theorem 2. *Any affine Boolean function f, encoded according to the formula $\{0,1\} \to \{0,1\}$, is characterized by the following unique Walsh-Hadamard spectrum distribution:*

$$r_x = \begin{cases} +2^{n-1} & \text{for } x = 0, \\ (-1)^{1-c} \times 2^{n-1} & \text{for } x = \dfrac{1}{2}(k-c), \\ 0 & \text{otherwise}. \end{cases} \tag{5}$$

Spectral coefficients of the $\mathbf{S}$-type are more practical. For example, an affine function can be described by one spectral coefficient $s_i \neq 0$, whereas the description by means of the $\mathbf{R}$-type spectrum requires two coefficients $r_0 \neq 0$ and $r_i \neq 0$. For this reason, only the $\mathbf{S}$-type spectrum will be used.

In many practical problems, Boolean functions are given in an incomplete form. In such cases, the vector $\mathbf{Y}$ includes values $\{0, 1, -\}$, where the symbol '$-$' denotes 'do not care' minterms. In this case, the values $\{0, 1, -\}$ of the vector $\mathbf{Y}$ are replaced by $\{1, -1, 0\}$, respectively. If it is possible, incompletely defined Boolean functions can be satisfactorily completed to affine forms (Porwik, 2003), but functions with 'do not care' elements will not be considered in this paper.

It is obvious that many functions cannot be realized as affine functions. In such cases, the linearization of a given function can be carried out, i.e., a given function can be split into a linear and a nonlinear part while attempting to minimize the nonlinear part (Karpovsky, 1976; Karpovsky *et al.*, 2003).

Remark 1. Consider an n-variable Boolean function f with the autocorrelation coefficients b_x, $x = 0, 1, \ldots, 2^n - 1$. The set of all x, such that $b_x = b_0$, is an Abelian group $G(f) \mod 2$. Additionally, from (2) it can be stated that for a given function $f(x)$,

$$b_0 = \sum_{x=0}^{2^n-1} (f(x))^2.$$

If the function f is a Boolean function, then $f(x) \in \{0,1\}$, so the autocorrelation coefficient b_0 can be easily computed from the formula $b_0 = \sum_{x=0}^{2^n-1} f(x)$.

This remark follows from the property that the set of all binary sequences of the length n with the operation of componentwise addition $\mod 2$ is an Abelian group.

Theorem 3. (Karpovsky, 1976) *An n-variable Boolean function f can be decomposed as follows:*

$$f(x_0, x_1, \ldots, x_{n-1}) = \varphi(\lambda(x_0, \ldots, x_{n-1-b}), x_{n-b}, \ldots, x_{n-1}) \tag{6}$$

if and only if $b = a_f + 1$, where $a_f = \log_2 |G(f)|$, $|G(f)|$ is the order of the group $G(f)$, and λ is a linear function.

The linearization of Boolean functions on the basis of Theorem 3 was discussed in (Karpovsky, 1976; Karpovsky *et al.*, 2003; Stanković and Astola, 2003).

5. Spectral Decomposition of Boolean Functions

From Theorem 3 it follows that a given Boolean function f can be described by linear and nonlinear parts, $\lambda(x_0,\ldots,x_{n-1-b})$ and $f_{nl}(x_{n-b},\ldots,x_{n-1})$, respectively. Generally, this idea can be expanded (subfunctions do not have any restrictions) and used for a simple disjoint decomposition of Boolean functions by autocorrelation functions.

In many cases, the spectral and autocorrelation characteristics of Boolean functions are known in an analytical form (for instance, linear, affine, bent, majority, minority functions) (Karpovsky, 1976; MacWilliams and Sloane, 1977). Therefore, the method proposed below can be changed and the function f can be decomposed by selecting a subfunction φ or λ from the set of functions with known autocorrelations according to the designer's assumptions. This can be considered as a unique feature of the method when compared with other related methods where the subfunctions are determined automatically by a decomposition procedure or are restricted to a set of elementary logic functions, such as AND, OR and XOR.

Theorem 3 can be expanded and stated in another form. Let the set $X = \{x_0, x_1, \ldots, x_{n-1}\}$ of the arguments of a Boolean function $f(x_0, x_1, \ldots, x_{n-1})$ be partitioned into two disjoint subsets X_1 and X_2, i.e., $X_1 \cap X_2 = \varnothing$ and $X_1 \cup X_2 = X$. With these assumptions, the function $f(x) : \{0,1\}^{|X_1|+|X_2|} \to \{1,-1\}$ can be described (decomposed) in terms of subfunctions $\lambda : \{0,1\}^{|X_1|} \to \{1,-1\}$ and $\varphi : \{0,1\}^{|X_2|+1} \to \{1,-1\}$ such that $f(x) = \varphi(\lambda(X_1), X_2)$.

If an appropriate partition of the set of arguments can be found, then the decomposition (6) will be more flexible, because the partition of the set of input variables can be different and as the subfunctions φ and λ, many another functions can be used.

Theorem 4. *A simple disjoint decomposition of a given Boolean function f can be found if, on the basis of its autocorrelation characteristic, the arguments of the function f can be partitioned into two disjoint sets in the following way: Let $x = \sum_{i=0}^{n-1} x_i 2^{n-1-i}$. If the autocorrelation coefficients of f fulfil the condition*

$$\underset{x\neq 0}{\exists}\, x : b_x = 0 \quad \wedge \quad w(x_0,\ldots,x_{n-1}) = 1, \tag{7}$$

then the arguments $x_0, x_1, \ldots, x_{n-1}$ for which $w(x) = 1$ are connected with the function φ and form the set X_2. In other words, x refers to a value whose binary expansion contains a logic 1 in the i-th bit, while the remaining $n-1$ bits are 0.

If the autocorrelation coefficients of f fulfil the condition

$$\underset{x\neq 0}{\exists}\, x : b_x = \max b_x \quad \wedge \quad w(x_0,\ldots,x_{n-1}) > 1, \tag{8}$$

then the arguments $x_0, x_1, \ldots, x_{n-1}$ for which $w(x) > 1$ are connected with the function λ and form the set X_1. In other words, the index x refers to a value whose binary expansion contains a logic 1 in the $k \in \{2,\ldots,n\}$ bits, while the remaining $n-k$ bits are equal to 0.

The conditions (7) and (8) are sufficient to determine the partition of the arguments of f.

Proof. Note that for any Boolean function the condition $b_x \le b_0$ follows from Definition 3 and Theorem 3, especially for the balanced Boolean functions $b_0 = 2^{n-1}$. The criterion (8) determines the elements β of the group $G(f)$ and hence, if $\beta \in G(f)$, then $f(x) = f(x \oplus \beta)$ (Karpovsky *et al.*, 2003). It is equivalent to the partition of arguments of f. If the criterion (8) is not fulfilled, then it is necessary to find other, independent variables. Such conditions fulfil the criterion (7). ■

Theorem 4 can be used as a simple test to determine whether a given Boolean function f has a simple disjoint decomposition. To find such a decomposition, we have to check all $\binom{n_1+n_2}{n_1}$ partitions of $n = n_1 + n_2$, where n_i is the number of variables in the subsets X_i $(i = 1, 2)$. The criterion presented above permits us to check immediately whether such a decomposition is possible.

If the conditions of Theorem 3 are not satisfied, then f has bidecomposition topologies (Nowicka *et al.*, 1999; Sasao and Butler, 1997).

As the first step, the criterion (7) is used. If no partition of arguments can be found, then the criterion (8) is applied.

Example 2. Table 1 shows a Boolean function f, its Walsh-Hadamard spectrum and autocorrelation coefficients. From an analysis of the autocorrelation coefficients, the arguments of the function f can be partitioned into two subsets. Table 1 presents spectral coefficients in the Walsh-Hadamard ordering because the spectrum has been determined using (1). The spectral coefficients of the function f can be easily ordered in the Walsh-Paley ordering, which will be used in further deliberations.[1]

From the criterion (7), for the coefficient $b_1 = 0$ the Hamming weight of the input vector is equal to $w(x = 1) = 1$ and hence, for this case, $x = [0,0,0,1]$. For the

[1] In this paper, for the simplicity of programming implementations, the Walsh-Hadamard spectrum is calculated, and then converted into the Walsh-Paley spectrum for subsequent applications. Notice that there are FFT-like algorithms for a direct calculation of the Walsh-Paley spectrum, see, e.g., (Yaroslavsky, 2003).

Table 1. Boolean function and its spectral and autocorrelation coefficients.

x_0, x_1, x_2, x_3	$x = \sum_{i=0}^{n-1} x_i 2^{n-1-i}$	$f(x)$	s_x	b_x
0000	0	0	0	8
0001	1	1	0	0
0010	2	0	0	4
0011	3	1	8	4
0100	4	0	0	4
0101	5	1	8	4
0110	6	1	0	4
0111	7	0	0	4
1000	8	0	0	4
1001	9	1	8	4
1010	10	1	0	4
1011	11	0	0	4
1100	12	1	0	4
1101	13	0	0	4
1110	14	1	0	0
1111	15	0	−8	8

coefficient b_{14}, the criterion (7) is not satisfied because $w(x = 14) \neq 1$, and $x = [1, 1, 1, 0]$. Hence the set of the arguments of the subfunction φ contains only the variable x_3. The other variables x_0, x_1, x_2 are arguments of the subfunction λ. ♦

Example 3. Reasoning similar to that followed in the previous example can be applied to a five-variable Boolean function f which has the autocorrelation characteristic

$$\mathbf{B}_f = [16, 8, 8, 8, 8, 8, 8, 8, 0, 8, 8, 8, 8, 0, 16, 8, 8, 8, 8, 8, 8, 8, 0, 16, 8, 8, 8, 16, 8, 8, 8, 8, 8, 8, 8, 0]^T.$$

For this function, the condition (7) is not satisfied because for any x such that $w(x) = 1$ we have $b_x \neq 0$. Therefore, we have to use the criterion (8), from which we observe that $b_x = b_0 = b_{12} = b_{20} = b_{24}$. According to the assumption of Theorem 4, the coefficient b_0 is not analyzed. In this case, the sets of arguments for the subfunctions λ and φ consist of the variables x_0, x_1, x_2 and x_3, x_4, respectively. ♦

If, given a function f, a partition of the set of variables can be found, then the Walsh-Paley spectra of the corresponding subfunctions φ and λ satisfy the matrix equation.

Suppose that decomposition has the form

$$f(x_0, x_1, \ldots, x_{n-1}) = \varphi(\lambda(x_0, \ldots, x_k), x_{k+1}, \ldots, x_{n-1}), \quad k > 0.$$

Then

$$\frac{1}{2}\begin{bmatrix} [\mathbf{S}^\lambda] & & 0 \\ & \ddots & \\ 0 & & [\mathbf{S}^\lambda] \end{bmatrix} \times \begin{bmatrix} \mathbf{S}^\varphi \end{bmatrix}_{2^{n-k}\times 1} = \begin{bmatrix} \mathbf{S}^f \end{bmatrix}_{2^n \times 1}, \tag{9}$$

where

$$[\mathbf{S}^\lambda] = \begin{bmatrix} 2^{k+1} & \\ 0 & \\ 0 & \mathbf{S}^\lambda \\ \vdots & \end{bmatrix}_{2^{k+1}\times 2}, \tag{10}$$

$\mathbf{S}^f$, $\mathbf{S}^\varphi$, and $\mathbf{S}^\lambda$ are Walsh-Paley spectra of the functions f, φ and λ, respectively.

A method for the decomposition of Boolean functions by using a matrix in the Walsh-Hadamard spectral domain was proposed in (Hurst *et al.*, 1985), see also (Tokmen, 1980). Notice that if there exists a disjoint decomposition of f, then there exists a valid relationship between the spectra of the Boolean functions f, λ and φ. However, a drawback of this spectral characterization of the decomposability is that if the decomposition of a given Boolean function f is possible, it may not be immediately apparent how the set of input variables x_i, $(i = 0, \ldots, n-1)$ should be partitioned to achieve such a decomposition. In (Hurst *et al.*, 1985), the subfunction λ is selected randomly. The partition of disjoint subsets is also selected arbitrarily. Furthermore, for some choices, Eqn. (9) has no solutions. If the subfunction λ was selected correctly, then it is necessary to find the unknown partition of variables into two subsets. For n-input variables, we have $n!$ of its permutations and only one of them is correct. The correctness of the solution can be checked using (9). If a solution exists, then the decomposition is possible. Therefore, given $\mathbf{S}_f$ and $\lambda(\varphi)$, $n!$ examinations are needed to ensure whether the disjoint decomposition exists. Each permutation of input variables can be treated as a reordering of the spectrum of $\mathbf{S}_f$.

In our method, Theorem 4 permits us to immediately partition the set of input variables by the analysis of the autcorrelation coefficients. Therefore, we propose the following, two-stage decomposition method:

1. From the analysis of the autocorrelation coefficients, deduce whether a given function f is decomposable and determine the corresponding partition of the set of input variables.

2. From the matrix relations in the Walsh-Paley spectral domain, determine the corresponding subfunctions φ and λ.

Taking into account the above discussion, the method of decomposing Boolean functions proceeds as follows:

1. Compute the autocorrelation vector $\mathbf{B}_f = [b_0, b_1, \ldots, b_{2^n-1}]$ of a given Boolean function f from the spectral coefficients $\mathbf{S}_f = [s_0, s_1, \ldots, s_{2^n-1}]$ and check whether decomposition exists. In this case, determine the corresponding partition of the set of input variables X into subsets X_1 and X_2.
2. Reorder the Walsh-Hadamard spectrum $\mathbf{S}_f$ into the Walsh-Paley spectrum $\mathbf{S}^f$ of f.
3. Select arbitrarily a Boolean function λ depending on variables in X_1 and construct the truth vector $\mathbf{Y}_f^{\lambda}$.
4. Compute the Walsh-Paley spectrum $\mathbf{S}^{\lambda}$ for $\mathbf{Y}_f^{\lambda}$.
5. Try to solve the matrix relation (9) in $\mathbf{S}^{\varphi}$ and determine the Walsh-Paley spectrum for φ.
6. If for selected λ, $\mathbf{S}^{\varphi}$cannot be determined from (9), then select another function λ and repeat Steps 3 to 5.

Notice that the application of Theorem 4 in Step 3 of the above algorithm is simplified if λ is selected from the class of functions whose autocorrelation functions are known (Karpovsky, 1976).

Example 4. In Example 2, from Theorem 4 we determined a partition of the set of variables for the function f given in Table 1. All coefficients in (11) are ordered in the Walsh-Paley order, but Table 1 includes the spectrum in the Wash-Hadamard order obtained directly from (1). We select the majority function as a possible function λ and determine its Walsh-Paley spectrum. For this reason we prepare the truth vector $\mathbf{Y}_f^{\lambda} = [1,1,1,-1,1,-1,-1,-1]$ encoded according to the rule $\{0,1\} \to \{1,-1\}$, and from the Walsh-Hadamard transform we obtain the appropriate $\mathbf{S}$-type spectrum $\mathbf{S}^{\lambda} = [0,4,4,0,4,0,0,-4]$ of the function λ. In the next stage we solve the matrix equation (11).

$$\frac{1}{2}\begin{bmatrix} \begin{bmatrix} 8 & 0 \\ 0 & 4 \\ 0 & 4 \\ 0 & 0 \\ 0 & 4 \\ 0 & 0 \\ 0 & 0 \\ 0 & -4 \end{bmatrix} & \mathbf{0} \\ \mathbf{0} & \begin{bmatrix} 8 & 0 \\ 0 & 4 \\ 0 & 4 \\ 0 & 0 \\ 0 & 4 \\ 0 & 0 \\ 0 & 0 \\ 0 & -4 \end{bmatrix} \end{bmatrix} \times \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 8 \\ 8 \\ 0 \\ 8 \\ 0 \\ 0 \\ 0 \\ -8 \end{bmatrix}. \quad (11)$$

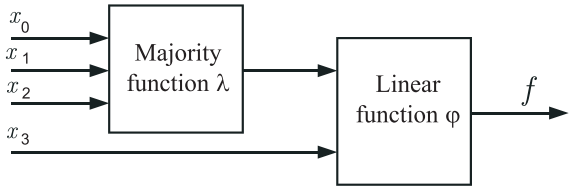

Fig. 1. Decomposition of the Boolean function f from Example 4.

After calculations, we obtain the spectral coefficients $s_0 = 0, s_1 = 0, s_2 = 0, s_3 = 4$. Hence the function φ is a linear one. Finally, after decomposition procedures we obtain two boolean functions: $\lambda(x_0, x_1, x_2) = x_1x_2 + x_0x_2 + x_0x_1$, and $\varphi(\lambda, x_3) = \lambda(x_0, x_1, x_2) \oplus x_3$. The functions λ and φ form the function f. Figure 1 shows the corresponding realization of the decomposition of the function f. ♦

Example 5. Consider a Boolean function f given by the truth vector $\mathbf{Y} = [0,1,0,1,0,0,0,1,0,0,0,1,0,0,0,0]^T$. For this function, the autocorrelation coefficients are

$$\mathbf{B}_f = [4,0,2,0,2,0,2,0,2,0,2,0,2,0,0,0]^T.$$

From Theorem 4, we obtain the following partition of arguments:

$$f(x_0, x_1, x_2, x_3) = \varphi(\lambda(x_0, x_1, x_2), x_3).$$

Suppose that φ is a bent function. A Boolean function φ is called bent if φ has the maximum possible value of nonlinearity equal to $(2^n \pm 2^{n/2})/2$, where n is even. Hence all spectral coefficients of a bent function have the values $s_i = \pm 2^{n/2}$, $i = 0, 1, \ldots, 2^n - 1$. The spectrum of a bent function φ is $\mathbf{S}^{\varphi} = [2,2,2,-2]$.

The function λ can be determined from the matrix equation

$$\frac{1}{2}\begin{bmatrix} \begin{bmatrix} 8 & s_0 \\ 0 & s_1 \\ 0 & s_2 \\ 0 & s_3 \\ 0 & s_4 \\ 0 & s_5 \\ 0 & s_6 \\ 0 & s_7 \end{bmatrix} & \mathbf{0} \\ \mathbf{0} & \begin{bmatrix} 8 & s_0 \\ 0 & s_1 \\ 0 & s_2 \\ 0 & s_3 \\ 0 & s_4 \\ 0 & s_5 \\ 0 & s_6 \\ 0 & s_7 \end{bmatrix} \end{bmatrix} \times \begin{bmatrix} 2 \\ 2 \\ 2 \\ -2 \end{bmatrix} = \begin{bmatrix} 8 \\ -4 \\ -4 \\ 0 \\ 4 \\ 0 \\ 0 \\ -4 \\ 8 \\ 4 \\ 4 \\ 0 \\ -4 \\ 0 \\ 0 \\ 4 \end{bmatrix}. \quad (12)$$

In consequence, we obtain the Walsh-Paley spectrum of the unknown function λ: $s_0 = 0$, $s_1 = -4$, $s_2 = -4$, $s_3 = 0$, $s_4 = 4$, $s_5 = 0$, $s_6 = 0$, $s_7 = -4$, and determine its truth vector as $\mathbf{Y}_f = [-1, -1, 1, -1, 1, -1, 1, 1]$. Hence, $\lambda(x_0, x_1, x_2) = \overline{x}_0\overline{x}_2 + x_1\overline{x}_0 + x_1x_2$, $\varphi(\lambda, x_3) = \lambda(x_0, x_1, x_2)x_3$. ♦

6. Experimental Results

We performed a series of experiments over a set of standard benchmark functions to estimate the features of the proposed method for a simple disjoint decomposition of Boolean functions. Table 2 shows a sample of these results. The symbol 'x' means that the obtained subfunctions have spectral characteristics different from those mentioned in this table, i.e., different from linear, bent, majority and self-dual functions. The correctness of the presented results was verified by a comparison with the results produced by the DEMAIN algorithm (Nowicka *et al.*, 1999). DEMAIN implements a balanced serial and parallel functional decomposition and, in many cases, it decomposes a larger number of benchmarks than other methods do (Nowicka *et al.*, 1999). The set of benchmarks is restricted to functions in up to 12 variables due to the restrictions of DEMAIN programming realization. The circuits from Table 2 were compared with both methods presented in this paper, and DEMAIN/serial/disjoint decomposition. Both methods give the same decomposition results and, therefore, in Table 2 only possibilities of functions decomposition are shown.

Table 2. Results of decomposition for benchmark functions.

Benchmark	In.	Sub-function λ	Sub-function φ	Serial decomp.
sqr6_1	6	x	self-dual	yes
a2_3	4	x	linear	yes
xor5	5	linear	linear	yes
check0	4	linear	x	yes
max1024_6	10			no
apex4 (2^{nd})	9			no
sao2 (1^{st})	10	x	x	yes
z5xp1_3	7			no
Example 4	4	majority	linear	yes
Example 5	4	self-dual	bent	yes

We also applied the algorithm proposed in this paper to 80 benchmark functions in various numbers of variables. In the case of multi-output functions, each output was considered as a separate function. Additionally, experiments were carried out where functions up to 20 input variables were tested.

For approximately 60% of the examined functions, the simple disjoint decomposition was possible with one of the subfunctions selected as an affine, self-dual, majority, minority or bent function. The proposed synthesis method can be used for Boolean functions which have $n \leq 30$ variables because for larger functions memory complexity is disadvantageous. It should be noticed, however, that similar problems can be observed even if the fast Fourier transform family is used (Stanković and Astola, 2003; Yanushkevich, 1998).

7. Conclusions

We presented an algorithm for a simple disjoint decomposition of logic functions starting from an autocorrelation characteristic of a function and its spectral description. The analysis of the autocorrelation coefficients allow us to partition the set of input variables into appropriate disjoint subsets. Given a Boolean function, if a partition of the set of variables can be found, then Walsh-Paley spectra of the corresponding subfunctions can be derived. Experimental results show that even if the decomposition form is restricted, many practical functions can be effectively by decomposed. The described method is especially efficient when one of subfunctions has well-known spectral characteristics.

Acknowledgments

The authors thank the anonymous reviewers for their constructive comments. Additionally, we would like to thank Professor Arkadij Zakrevskij for his detailed remarks, which allowed us to improve the paper.

References

Ahmed N. and Rao K.R. (1975): *Orthogonal Transforms for Digital Signal Processing*. — Berlin: Springer.

Ashenhurst R. (1957): *The decomposition of switching functions*. — Proc. Int. Symp. *Theory of Switching*, Annual Computation Laboratory, Harvard University, Vol. 29, pp. 74–116.

Dubrova E. (1999): *AOXMIN-MV: A heuristic algorithm for AND-OR-XOR minimization*. — Proc. Int. Workshop *Applications of Reed-Muller Expansion in Circuit Design, RM'99*, Victoria, Canada, pp. 37–53.

Curtis H.A. (1962): *A New Approach to the Design of Switching Circuits*. — Princeton: Van Nostrand.

Bertacco V. and Damiani M. (1997): *The disjunctive decomposition of logic functions*. — Proc. *Computer-Aided Design, ICCAD'97*, San Jose, CA, pp. 78–82.

Falkowski B.J. and Kannurao S. (2001): *Analysis of disjunctive decomposition of balanced Boolean functions through Walsh spectrum*. — IEE Proc. Comput. Digit. Techn., Vol. 148, No. 2, pp. 71–78.

Falkowski B.J. and Porwik P. (1999): *Evaluation of nonlinearity in Boolean functions by extended Walsh-Hadamard transform*. — Proc. 2nd Int. Conf. *Information Communications and Signal Processing, ICISC'99*, Singapore, paper 2B2.2, pp. 1–4.

Hurst S.L., Miller D.M. and Muzio J.C. (1985): *Spectral Techniques in Digital Logic*. — London: Academic Press.

Karpovsky M.G. (1976): *Finite Orthogonal Series in the Design of Design of Digital Devices*. — New York: Wiley.

Karpovsky M.G., Stanković R.S. and Astola J.T. (2003): *Reduction of size decision diagrams by autocorrelation functions*. — IEEE Trans. Comput., Vol. 52, No. 5, pp. 592–606.

Lai Y., Pedram M. and Vrudhula S. (1993): *BDD based decomposition of logic function with application to FPGA synthesis*. — Proc. 30-th Conf. *Design Automation, DAC'93*, Dallas, Texas, pp. 642–647.

MacWilliams F.J. and Sloane N.J. (1977): *The Theory of Error-Correctiong Codes*. — Amsterdam: Nord-Holland Publishing Company.

Mishchenko A., Steinbach B. and Perkowski M. (2001): *An algorithm for bi-decomposition of logic functions*. — Proc. 38-th Conf. *Design Automation, DAC'01*, Las Vegas, NV, pp. 103–108.

Nowicka M., Rawski M. and Łuba T. (1999): *DEMAIN – An interactive tool for FPGA-based logic decomposition*. — Proc. 6-th Int. Conf. *Mixed Design of Integrated Circuits and Systems*, Cracow, Poland, pp. 115–120.

Porwik P. (2003): *The spectral test of the Boolean function linearity*. — Int. J. Appl. Math. Comput. Sci., Vol. 13, No. 4, pp. 567–575.

Porwik P. (2004a): *Efficient spectral method of identification of linear Boolean function*. — Int. J. Contr. Cybern., Vol. 33, No. 4, pp. 663–678.

Porwik P. (2004b): *Walsh coefficients distribution for some types of Boolean function*. — Arch. Theoret. Appl. Informat., Vol. 16, No. 2, pp. 109–120.

Rawski M., Jóźwiak L. and Łuba T. (2001): *Functional decomposition with an efficient input support selection for sub-functions based on information relationship measures*. — J. Syst. Archit., Vol. 47, Elsevier Science, pp. 137–155.

Rice J. and Muzio J.C. (2003): *On the use of autocorrelation coefficients in the identification of three-level decompositions*. — Proc. Int. Workshop *Logic Synthesis, IWLS'03*, Laguna Beach, CA, pp. 187–191.

Stanković R.S. and Astola J.T., (2003): *Spectral Interpretation of Decision Diagram*. — New York: Springer.

Stanković R.S. and Falkowski B. (2002): *Spectral transforms calculation trough decision diagrams*. — VLSI Design., Vol. 14, No. 1, pp. 5–12.

Sasao T. and Butler J.T. (1997): *On bi-decomposition of logic functions*. — Proc. Int. Workshop *Logic Synthesis*, Lake Tahoe, CA, Vol. 2, pp. 1–6.

Sasao T. and Matsuura M. (2004): *A method to decompose multiple-output logic functions*. — Proc. 41-th Conf. *Design Automation, DAC'04*, San Diego, CA, pp. 428–433.

Tokmen V.H. (1980): *Disjoint decomposability of multi-valued functions by spectral means*. — Proc. IEEE 10-th Int. Symp. *Multiple-Valued Logic*, New York, USA, pp. 88–93.

Tomczuk R. (1996): *Autocorrelation and decomposition methods in combinational logic design*. — Ph.D. thesis, University of Victoria, Victoria, Cadada.

Yanushkevich S. (1998): *Logic Differential Calculus in Multi-Valued Logic Design*. — Szczecin: Techn. University of Szczecin Academic Publishers, Poland.

Yaroslavsky L. (2003): *Digital Image Processing*. — Boston, MA: Kluwer Academic Publisher.

Received: 28 June 2005
Revised: 10 October 2005