Use of the Autocorrelation Function in the Classification of Switching Functions

J. E. Rice and J. C. Muzio
VLSI Design and Test Group, Dept. of Computer Science
University of Victoria, BC, Canada
[jrice jmuzio]@cs.uvic.ca

Abstract

Four operations on switching functions are used to define a classification technique based on the autocorrelation function. The relationship between these classes and the well-known spectral classes is investigated, and a canonical representative for each class is proposed. It is thought that these classes will be of use in logic synthesis employing decision diagram representations for intermediate steps.

1. Introduction

Boolean functions are functions for which the inputs and the output(s) are restricted to the Boolean domain. If a transformation matrix $\mathbf{T}^n$ is premultiplied by the output vector of the function, the result is a representation of the function in the spectral domain, usually referred to as the *spectral coefficients* of a function. An alternative view of the function is the *autocorrelation coefficients* of the function.

A function's spectral coefficients give a measure of similarity of the function to one of its inputs, or, to linear combinations of the inputs. The spectral coefficients of a function have been used in many areas of design, optimisation, and testing of digital circuits [4, 8, 9] and for solving problems such as classification of functions [8] and Boolean matching [3]. The autocorrelation coefficients provide a measure of the function's similarity to itself, shifted by a given amount. This is also called the cross-correlation, or convolution function. The autocorrelation coefficients have been used in optimisation and synthesis of combinational logic [13], in variable ordering for ROBDDs [12], and to compute the estimate $C(f)$ of a function's complexity [13, 9]; however, their use has been limited, likely due to the fact that the commonly used methods of computation are exponential in the number of inputs to the function(s).

The information inherent in the autocorrelation coefficients also has the potential to be of use in many other areas, such as in identifying other types of complexity measures [14], symmetry identification, and most recently in the optimisation of decision diagrams [10]. In this paper we apply the autocorrelation coefficients to the problem of function classification.

Because there are 2^{2^n} possible Boolean functions of n variables, there is a strong need to be able to group these functions in some logical manner. One objective of classifying switching functions into such groupings is to list more compactly all 2^{2^n} possible functions. Another, more practical goal is to be able to state that certain information is true about all functions in a particular group, or, that all switching functions in a particular class have certain similarities. From this a standard or canonical function for each class may be designated, thus leading to increased understanding about functions in that class, better fault diagnosis and testing procedures for that class of functions, and more efficient implementations [7].

2. Notation

The following notation is used throughout the paper:

$f(X)$ and $g(X)$ are each switching functions in which $X = \{x_1 ... x_{n-1} x_n\}$.

$$\tau = \sum_{i=1}^{n} \tau_i \cdot 2^{i-1}.$$

$$v = \sum_{i=1}^{n} v_i \cdot 2^{i-1}.$$

n is the number of inputs to the switching function $f(X)$.

The symbol $\oplus$ represents the bitwise exclusive-or function.

The symbol $\cdot$ represents arithmetic multiplication while $+$ represents arithmetic addition.

The symbol $\vee$ represents the logical or function while $\wedge$ represents the logical and function. This notation is used to avoid confusion between the more common usage of $+$

and $\cdot$ meaning addition/or multiplication/and respectively, depending on the context.

The outputs of a switching function are either true or false. This is generally encoded as $\{0, 1\}$. However, an alternative encoding of $\{+1, -1\}$ may also be used. When referring to a vector of a switching function's outputs, if $\{0, 1\}$ encoding is used then the vector is referred to as Z. If $\{+1, -1\}$ encoding is used then the vector is referred to as Y.

Both $B(\tau)$ and $b_{x_i x_j ...}$ may be used to refer to the individual autocorrelation coefficients of a function. In the second case, $x_i x_j ...$ indicate that τ contains a 1 exactly in those positions. The same applies to $C(\tau)$ and $c_{x_i x_j ...}$.

3. Background

Some definitions and background in the areas of classification and autocorrelation functions are given in the following Subsections.

3.1. Autocorrelation Coefficients

Boolean functions can be translated to other domains, such as the *spectral domain*. In this paper we consider the calculation of the function's *autocorrelation coefficients*.

The general cross-correlation (convolution) function between two given functions f and g at a distance τ is defined as

$$B^{\,f\,g}(\tau) = \sum_{v=0}^{2^n-1} f(v) \cdot g(v \oplus \tau) \tag{1}$$

When $f(X) = g(X)$, the resulting equation gives the cross-correlation of a function with itself, translated by τ. The resulting coefficients are referred to as the autocorrelation coefficients of the function.

The autocorrelation function is defined as follows [9]:

$$B^{\,f\,f}(\tau) = \sum_{v=0}^{2^n-1} f(v) \cdot f(v \oplus \tau) \tag{2}$$

If the superscripts $f\ f$ are omitted then it assumed that an autocorrelation function is being computed, rather than a cross-correlation function.

For multiple output functions a second step must be performed to combine the autocorrelation function for each of the individual functions into the *total autocorrelation function*. The total autocorrelation function is defined as

$$\sum_{i=0}^{m-1} B_i(\tau) = \sum_{i=0}^{m-1} \sum_{v=0}^{2^n-1} f_i(v) \cdot f_i(v \oplus \tau) \tag{3}$$

where m is the number of outputs and the multiple-output function F consists of $f_0 f_1 ... f_{m-1}$. This definition is included in the interest of completeness; only single-output functions are considered in this paper.

In the above definitions it assumed that the function $f(X)$ is encoded using the standard 1 for true minterms and 0 for false minterms. However, both Definitions 2 and 3 also apply if $\{+1, -1\}$ encoding of the function outputs is used. In this case the resulting autocorrelation coefficients are referred to as $C^{\,f\,f}(\tau)$, or $C(\tau)$.

The autocorrelation coefficients may also be computed from the spectral coefficients of the function, as demonstrated in Section 10.2.

3.2. Classification of Switching Functions

There are several methods of classification for switching functions. The primary algebraic classification method involves the application of a number of operations. The operations are as follows [8]:

(a) negation (N) of one or more of the input variables of the function;

(b) permutation (P) of input variables x_i and x_j, $i, j \in 1..n$, $i \neq j$; and

(c) negation (N) of the output of the function.

Functions that are equivalent under these operations, either applied individually or collectively, are said to be NPN-equivalent functions. Alternatively, they are said to belong to the same NPN-equivalence class. These operations are then invariance operations for the NPN-equivalence classes.

Another classification method is a technique using a function's spectral coefficients. The spectral coefficients of a function are obtained by premultiplying a transform matrix T^n such as the Hadamard matrix by the vector of outputs Y as shown in Equation 4 [8].

$$S = T^n \cdot Y \tag{4}$$

The resulting vector S consists of the coefficients of the transform, and are referred to as the spectral coefficients of the function. Using these spectral coefficients as an alternative representation of a switching function, it has been found that there are identical sets of spectral coefficient values for various different switching functions (disregarding sign and position changes of the coefficients) [6]. These classes of functions with the same set of spectral coefficients are defined by a set of invariance functions. The spectral invariance functions are listed below.

(i) Permutation of any input variables x_i and x_j, $i, j \in 1..n$, $i \neq j$.

(ii) Negation of any input variable x_i, $i \in 1..n$.

(iii) Negation of the output of the switching function.

(iv) Replacement of any input variable x_i with $x_i \oplus x_j$, $i, j \in 1..n, i \neq j$.

(v) Modifying the output of the switching function from $f(X)$ to $f(X) \oplus x_i$, $i \in 1..n$.

Note that the first three spectral invariance operations are the NPN operations; thus the spectral classes encompass more functions than do than the NPN classes. For this reason the spectral classes are said to be stronger than the NPN classes.

4. Defining the Autocorrelation Classes

The autocorrelation classes are defined by four invariance operations:

(i) Permutation of any input variables x_i and x_j, $i, j \in 1..n, i \neq j$.

(ii) Negation of any input variable x_i, $i \in 1..n$.

(iii) Negation of the output of the switching function.

(iv) Replacement of any input variable x_i with $x_i \oplus x_j$, $i, j \in 1..n, i \neq j$.

As will be discussed below, output negation has very different results depending on whether the $\{+1, -1\}$ or $\{0, 1\}$ representation is used. For the purpose of classification we use only the $\{+1, -1\}$ representation for the autocorrelation coefficients.

Each class defined by these operations may be related to one or more other classes through the application of the type (v) spectral invariance operation. Identification of these related classes is relatively straightforward, since the only difference in autocorrelation values between the classes is the sign of the values.

5. Invariance Operations

The operations described in Section 3.2 define the NPN-equivalence and spectral classes, respectively. Similarly, the operations described in this and the previous Sections define the autocorrelation classes. This section goes on to prove their effects on the autocorrelation coefficients for a function.

5.1. Permutation

The first invariance operation for the autocorrelation classes is permutation of the input variables. Since the autocorrelation coefficients are directly related to the structure of the function, any relabeling of the variables is directly reflected in the labeling of the coefficients. Permutation can be described as simply relabeling the inputs. The explanation given by Hurst [7] for the spectral coefficients can be easily extended to the autocorrelation coefficients.

5.2. Input Negation

The second invariance operation for the autocorrelation classes is negation of any inputs. Negation of an input has no effect on the autocorrelation coefficients of a function.

This is shown as follows: given a function $f(x_1, ..., x_n)$, without loss of generality let us define another function $f^*(x_1, ..., x_n^*)$ where

$$f^*(x_1, ..., x_n^*) \triangleq f(x_1, ..., \overline{x}_n)$$

The question of how the autocorrelation coefficients for $f^*(X)$ relate to the coefficients for $f(X)$ is answered by the following.

By definition

$$\sum_{v=0}^{2^{n-1}-1} f^*(v) \triangleq \sum_{v=2^{n-1}}^{2^n-1} f(v)$$

and

$$\sum_{v=2^{n-1}}^{2^n-1} f^*(v) \triangleq \sum_{v=0}^{2^{n-1}-1} f(v)$$

Then

$$\begin{aligned}
B^{f^* f^*}(\tau) &= \sum_{v=1}^{2^n-1} f^*(v) \cdot f^*(v \oplus \tau) \\
&= \sum_{v=0}^{2^{n-1}-1} f^*(v) \cdot f^*(v \oplus \tau) + \\
&\qquad \sum_{v=2^{n-1}}^{2^n-1} f^*(v) \cdot f^*(v \oplus \tau) \\
&= \sum_{v=2^{n-1}}^{2^n-1} f(v) \cdot f(v \oplus \tau) + \\
&\qquad \sum_{v=0}^{2^{n-1}-1} f(v) \cdot f(v \oplus \tau) \\
&= B^{f f}(\tau)
\end{aligned}$$

Thus input negation is an invariance operation for the autocorrelation classes.

5.3. Output Negation

Output negation is also an invariance operation for the autocorrelation classes, but only if $\{+1, -1\}$ encoding is used.

Let us define two functions $g(x_1, ..., x_n)$ and $g^*(x_1, ..., x_n)$ such that

$$g^*(x_1, ..., x_n) \triangleq \overline{g(x_1, ..., x_n)}$$

The question of how the autocorrelation coefficients for $g^*(X)$ relate to the coefficients for $g(X)$ is answered by the following.

In $\{+1, -1\}$ encoding the arithmetic equivalent of $g^*(X) = \overline{g(X)}$ is $g^*(X) = -g(X)$.

Therefore

$$\begin{aligned} C^{\,g^*\,g^*}(\tau) &= \sum_{v=0}^{2^n-1} g^*(v) \cdot g^*(v \oplus \tau) \\ &= \sum_{v=0}^{2^n-1} -g(v) \cdot -g(v \oplus \tau) \\ &= \sum_{v=0}^{2^n-1} g(v) \cdot g(v \oplus \tau) \\ &= C^{\,g\,g}(\tau) \end{aligned}$$

In $\{0, 1\}$ notation let us similarly define $f^*(X) \triangleq \overline{f(X)}$. Then the arithmetic equivalent is $f^*(X) = 1 - f(X)$.

Therefore

$$\begin{aligned} B^{\,f^*\,f^*}(\tau) &= \sum_{v=0}^{2^n-1} f^*(v) \cdot f^*(v \oplus \tau) \\ &= \sum_{v=0}^{2^n-1} (1 - f(v)) \cdot (1 - g(v \oplus \tau)) \\ &= \sum_{v=0}^{2^n-1} [f(v) \cdot f(v \oplus \tau) - \\ &\qquad f(v) - f(v \oplus \tau) + 1] \\ &= B^{\,f\,f}(\tau) - \sum_{v=0}^{2^n-1} f(v) - \\ &\qquad \sum_{v=0}^{2^n-1} f(v \oplus \tau) + \sum_{v=0}^{2^n-1} 1 \\ &= B^{\,f\,f}(\tau) - 2\sum_{v=0}^{2^n-1} f(v) + 2^n \\ &= B^{\,f\,f}(\tau) - 2B^{\,f\,f}(0) + 2^n \end{aligned}$$

5.4. Type (iv) Invariance Operation

This operation is called the type (iv) operation as it is referring to the fact that it is the fourth type of invariance operation for the spectral classes. It is also the fourth type of invariance operation for the autocorrelation classes.

If we label the variable being replaced as x_i and the replacement operation as $x_i \oplus x_j$ then the autocorrelation coefficients associated with x_i are not affected, while coefficients associated with x_j are exchanged with those associated with both x_i and x_j. A proof of this result is given in the Appendix in Section 10.1.

6. Connections between the Spectral and Autocorrelation Classes

There is a clear relationship between the autocorrelation classes and the spectral classes, in that the invariance operations defining each classification method are very similar. Since the autocorrelation classes are defined using a subset of the spectral invariance operations, clearly these classes contain fewer functions than do the spectral classes. Moreover, one can state that if $f(X)$ and $g(X)$ both belong to autocorrelation class A, then both must belong to the same spectral class B.

If $f(X)$ and $g(X)$ both belong to spectral class A, then they will not necessarily both belong to the same autocorrelation class B. However, if $f(X)$ belongs to autocorrelation class B, then $g(X)$ will belong either to autocorrelation class B or to a related autocorrelation class C. C and B in this case are classes for which it is possible to generate any function in C given any function in B through the application individually or collectively of the four autocorrelation invariance operations, plus the type (v) spectral invariance operation.

7. Canonical Autocorrelation Spectra

The canonical spectrum for the spectral classes consists of a list of the 2^n coefficient values in the identification order $s_0, s_1, s_2, ..., s_n, s_{12}, ..., s_{12...n}$ but with the zero- and first-order coefficients all positive integer values and arranged in decreasing magnitude. Since the sum of the spectral coefficients must always total $\pm 2^n$ this implies a relationship amongst all the coefficients; thus modifying the spectra to match the given arrangement for the lower order coefficients will clearly affect the higher order coefficients [8]. The choice of this canonical representation was in order to ensure that the canonic function for each spectral class had the large magnitude coefficients in the first order positions, and thus would have an optimum synthesis in terms of threshold logic [6].

For the autocorrelation coefficients it would seem logical to select a canonic representation with the same underlying reasoning. High values in the first-order spectral coefficients corresponds to high values in the first-order autocorrelation coefficients; however in the autocorrelation coefficients the values should be decreasing over the $\{+1, -1\}$ first-order coefficients $c_{x_n}, c_{x_{n-1}}, ..., c_{x_1}$. The reason for this is demonstrated in the Appendix in Section 10.2.

Table 1 in the Appendix lists the canonical autocorrelation class representatives for $n \leq 4$.

8. Significance and Applications of the Autocorrelation Classes

8.1 Logic Synthesis

The spectral classes were, when introduced, of particular value in logic synthesis. They allowed functions in the same spectral class to be synthesized from the class' canonical function by adding logic to complement and/or permute the variables, and/or by appending suitable exclusive-or logic. The same can be applied using the autocorrelation classes. For example, the function $f(X) = x_1x_2 + x_1x_3 + x_2x_3$ is a very desirable function, as it is totally symmetric. Given the autocorrelation coefficients for f and f^*, some function in the same autocorrelation class as f, appropriate logic may be added to convert this desirable function – which is likely to have an efficient implementation due to the symmetry property it possesses – into f^*, which may or may not possess the same property.

Figure 2 illustrates such a situation, given the functions f and f^* as defined in Figure 1.

$x_1x_2x_3$	$f(X)$	B	C	$f^*(X)$	B	C
000	0	4	8	1	4	8
001	0	2	0	1	2	0
010	0	2	0	0	2	0
011	1	2	0	1	2	0
100	0	2	0	1	2	0
101	1	2	0	0	2	0
110	1	2	0	0	0	-8
111	1	0	-8	0	2	0

Figure 1. The truth table and autocorrelation vectors for two functions in the same autocorrelation class.

The problem with this application is that one of the autocorrelation invariance operations, input negation, has no effect on the autocorrelation coefficients. With the other invariance operations, examination of the changes in the coefficients should lead to a determination of which operations

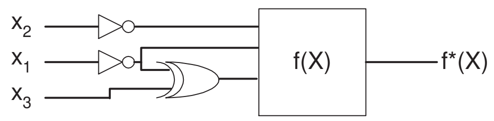

Figure 2. The additional logic required to convert f into f^*.

have been applied to the initial function. This is not so with input negation. Work developing an algorithm for this process must take this factor into account, either disregarding whether positive or negative literals are used in the functions, or by performing some sort of verification at each stage of the algorithm to determine if the correct function has been synthesized.

8.2 Decision Diagrams

The use of the autocorrelation classes can also be demonstrated in relation to logic synthesis involving the recently popular decision diagram representations [2]. Briefly, Binary Decision Diagrams (BDDs) were first introduced by Lee [11] and later by Akers [1], and were more recently popularized by Bryant [2]. A BDD is defined by Bryant as a directed acyclic graph in which each vertex is labeled by a Boolean variable and has outgoing arcs labeled 0 and 1. Each arc leads either to another vertex or to a terminal label F (0) or T (1). The value of the function for a given assignment to the inputs is determined by traversing from the root down to a terminal label, each time following the arc corresponding to the value assigned to the variable specified by the vertex label.

Various rules are applied to BDDs in order to produce a canonical form, generally referred to as a Reduced Ordered Binary Decision Diagram (ROBDD). These rules include sharing of isomorphic subgraphs within the BDD, and removal of redundant nodes. Details are given in [2]. Various extensions of decision diagrams exist and are described in [5]; however, the addition of inverters is of relevance to this work. Inverters, or complemented edges are used to indicate that the function represented by the graph below the complemented edge is inverted. Additional rules to ensure the canonicity of the decision diagram under this addition are detailed in [5].

Given two functions $f(X)$ and $g(X)$ in the same autocorrelation class, a straightforward technique for transforming a BDD representation for f to g (or vice versa) can be determined. Initial investigation in this area indicates that the application of any of the first three autocorrelation invariant operations to the BDD representation of a function is trivial: permutation of two variables is easily performed simply by relabeling the nodes in the graph, and negation of either the output or inputs of a function can be performed through the use of inverters. The final invariant operation requires a more complex solution, and has the potential to cause changes in the size of the BDD (unlike the previous operations). In practice, replacement of an input variable x_i with $x_i \oplus x_j$ requires only the addition of two internal inverters. These inverters are used to invert the nodes on the branches where x_j has the assignment 1 (assuming x_i follows x_j in the current variable ordering). This is not a difficult operation to perform, but may cause the BDD to grow as previously isomorphic (and thus shared) sub-graphs may no longer be isomorphic. However, it appears that additional inverters will solve this problem.

Further work is continuing in this area. Assuming that a "good" decision diagram representation is one that has a size (*i.e.* the number of nodes) that is not exponential in the number of inputs, then the goal is to construct a fast algorithm for generating a good decision diagram for f given a good decision diagram for g, and assuming that f and g are both in the same autocorrelation class.

9. Summary and Conclusions

We present in this paper a classification technique for switching functions based on the autocorrelation coefficients of a function. The autocorrelation classes are related to the spectral classes, but do not encompass the type (v) spectral invariance operation. The hypothetical advantage of this is in the synthesis from these classes of decision diagram representatives for the classes; the omission of the type (v) spectral invariance operation implies that fewer functions requiring exclusive-or logic in their synthesis from the representative are contained in each autocorrelation class. We also propose a canonical ordering of the autocorrelation representatives for each class. The proposed ordering is similar to that proposed by Edwards [6] for the spectral classes. The Appendix (Table 1) lists the canonical representatives for $n \leq 4$. Further work in this area is currently underway, including extensions to partially specified functions and to multi-output functions.

10. Appendix

10.1. Proof of the Effect of Type (iv) Operations on the Autocorrelation Coefficients

The following proves that when replacing an input variable x_i with $x_i \oplus x_j$ the effect on the autocorrelation coefficients is to exchange all coefficients associated with x_j with coefficients associated with both x_i and x_j; *i.e.*

$$b_{x_j} \Leftrightarrow b_{x_i x_j}$$

The same holds true for the $\{+1, -1\}$ autocorrelation coefficients $C(\tau)$ (or c_α).

Without loss of generality, let us define two functions $f(x_1, ..., x_{n-1}, x_n)$ and $f^*(x_1, ..., x^*_{n-1}, x_n)$ such that

$$\begin{array}{ll} f^*(x_1, ..., x^*_{n-1}, x_n) \triangleq f(x_1, ..., x_{n-1}, x_n) & \\ \text{and} \qquad x^*_{n-1} \triangleq x_{n-1} \oplus x_n. & \end{array}$$

Then

$$\begin{array}{lll} \text{(A)} & 0 \leq v \leq 2^{n-1} - 1 \Rightarrow f^*(v) = f(v) & \text{and} \\ \text{(B)} & 2^{n-1} \leq v \leq 2^n - 1 \Rightarrow f^*(v) = f(v \oplus \rho_{x_{n-1}}) & \end{array}$$

where $\rho_{x_{n-1}}$ contains only one 1 in the x_{n-1} position.

We then consider two cases,

$$\begin{array}{lll} \text{(i)} & 0 \leq \tau \leq 2^{n-1} - 1 & \text{and} \\ \text{(ii)} & 2^{n-1} \leq \tau \leq 2^n - 1. & \end{array}$$

Case (i) If $0 \leq \tau \leq 2^{n-1} - 1$ then both the x_n and x_{n-1} bits in τ are 0, and we know that

- $0 \leq v \leq 2^{n-1} - 1 \Rightarrow 0 \leq v \oplus \tau \leq 2^{n-1}$ and so (A) applies
- $2^{n-1} \leq v \leq 2^n - 1 \Rightarrow 2^{n-1} \leq v \oplus \tau \leq 2^n - 1$ and so (B) applies.

Therefore

$$\begin{aligned} B^{\,f^*\,f^*}(\tau) &= \sum_{v=0}^{2^n-1} f^*(v) \cdot f^*(v \oplus \tau) \\ &= \sum_{v=0}^{2^{n-1}-1} f^*(v) \cdot f^*(v \oplus \tau) \\ &\qquad + \sum_{v=2^{n-1}}^{2^n-1} f^*(v) \cdot f^*(v \oplus \tau) \\ &= \sum_{v=0}^{2^{n-1}-1} f(v) \cdot f(v \oplus \tau) \\ &+ \sum_{v=2^{n-1}}^{2^n-1} f(v \oplus \rho_{x_{n-1}}) \cdot f(v \oplus \tau \oplus \rho_{x_{n-1}}) \\ &= B^{\,f\,f}(\tau) \end{aligned}$$

Hence $B^{\,f*\,f*}(\tau) = B^{\,f\,f}(\tau)$ where $0 \leq \tau \leq 2^{n-1} - 1$, or $b^*_\alpha = b_\alpha$ where $x_n \notin \alpha$, and similarly for $C(\tau)$.

Case (ii) If $2^{n-1} \leq \tau \leq 2^n - 1$ then the x_n bit in τ is 1, and we know that

- $0 \leq v \leq 2^{n-1} - 1 \Rightarrow 2^{n-1} \leq v \oplus \tau \leq 2^n - 1$ and so (B) applies

- $2^{n-1} \leq v \leq 2^n - 1 \Rightarrow 0 \leq v \oplus \tau \leq 2^{n-1} - 1$ and so (A) applies.

Therefore

$$
\begin{aligned}
B^{f^* f^*}(\tau) &= \sum_{v=0}^{2^n-1} f^*(v) \cdot f^*(v \oplus \tau) \\
&= \sum_{v=0}^{2^{n-1}-1} f^*(v) \cdot f^*(v \oplus \tau) \\
&\quad + \sum_{v=2^{n-1}}^{2^n-1} f^*(v) \cdot f^*(v \oplus \tau) \\
&= \sum_{v=0}^{2^{n-1}-1} f(v) \cdot f(v \oplus \tau \oplus \rho_{x_{n-1}}) \\
+ \sum_{v=2^{n-1}}^{2^n-1} & f(v \oplus \rho_{x_{n-1}}) \cdot f(v \oplus \rho_{x_{n-1}} \oplus \tau \oplus \rho_{x_{n-1}}) \\
&= B^{f\,f}(\tau \oplus \rho_{x_{n-1}})
\end{aligned}
$$

Hence $B^{f* f*}(\tau) = B^{f\,f}(\tau\rho_{x_{n-1}})$ where $2^{n-1} \leq \tau \leq 2^n - 1$, or $b^*_{x_n\alpha} = b_{x_n x_{n-1}\alpha}$ where $x_n, x_{n-1} \notin \alpha$, and similarly for the $\{+1, -1\}$ coefficients.

10.2. Derivation of Canonical Autocorrelation Representation

The canonical ordering for the representatives of the autocorrelation classes is derived from that used for the spectral classes. Equation 5 defines how the spectral coefficients may be used to compute the autocorrelation coefficient. Figure 3 demonstrates how each spectral coefficient contributes to each autocorrelation coefficient in an example for three variables.

$$C = \frac{1}{2^n} \cdot T^n \cdot S^2 \tag{5}$$

where S^2 is the $\{+1, -1\}$ spectral coefficient vector with each entry squared.

Given that the canonical ordering for the spectral class representatives requires all first-order coefficients be positive and of large (comparative) magnitude in decreasing order for $s_0, s_1, ..., s_n$, one can see that the autocorrelation coefficients with the most contribution from the largest of these spectral coefficients is c_0, followed by c_{x_3} which has positive contributions from s_0, s_1 and s_2, followed by c_{x_2} which has positive contributions from s_0, s_1 and s_3, and so on. Due to the recursive nature of the chosen transform matrix (the Hadamard matrix), this observation can be extended to any number of variables.

10.3. Canonical Autocorrelation Class Representatives, $n \leq 4$

Table 1 lists the 18 canonical class representatives for the autocorrelation classes for $n \leq 4$. It should be noted that there are 8 spectral classes for $n \leq 4$.

References

[1] S. Akers. Binary Decision Diagrams. *IEEE Trans. on Comp.*, C-27(6):509–516, June 1978.

[2] R. Bryant. Graph-Based Algorithms for Boolean Function Manipulation. *IEEE Trans. on Comp.*, C-35(8):677–691, Aug. 1986.

[3] E. M. Clarke, K. L. McMillan, X. Zhao, M. Fujita, and J. Yang. Spectral Transforms for Large Boolean Functions with Application to Technology Mapping. In *Proceedings of the 30th ACM/IEEE Design Automation Conference*, 1993.

[4] S. Devadas, D. Varma, and E. A. Trachtenberg. Design Automation Tools for Efficient Implementation of Logic Functions by Decomposition. *IEEE Trans. on Computer Aided Design*, 8(8), Aug. 1989.

[5] R. Drechsler and B. Becker. Overview of Decision Diagrams. *Computers and Digital Techniques, IEE Proceedings-*, 144:187–193, May 1997.

[6] C. Edwards. The Application of the Rademacher-Walsh Transform to Boolean Function Classification and Threshold Logic Synthesis. *IEEE Trans. on Comp.*, pages 48–62, Jan. 1975.

[7] S. Hurst. *The Logical Processing of Digital Signals*. Crane Russak, 1978.

[8] S. L. Hurst, D. M. Miller, and J. C. Muzio. *Spectral Techniques in Digital Logic*. Academic Press, Inc., Orlando, Florida, 1985.

[9] M. Karpovsky. *Finite Orthogonal Series in the Design of Digital Devices*. John Wiley & Sons, 1976.

[10] M. G. Karpovsky, R. S. Stanković, and J. T. Astola. Reduction of Size of Decision Diagrams by Autocorrelation Functions. *submitted to IEEE Trans. on Comp.*, 2001.

[11] C. Y. Lee. Representation of Switching Circuits by Binary Decision Diagrams. *Bell System Technical Journal*, pages 958–999, 1959.

[12] J. E. Rice, J. C. Muzio, and M. Serra. The Use of Autocorrelation Coefficients for Variable Ordering for ROBDDs. In *Proceedings of the 4th International Workshop on Applications of the Reed-Müller Expansion in Circuit Design*, 1999.

[13] R. Tomczuk. *Autocorrelation and Decomposition Methods in Combinational Logic Design*. PhD thesis, University of Victoria, 1996.

[14] D. Varma and E. A. Trachtenberg. Efficient Spectral Techniques for Logic Synthesis. In *Logic Synthesis and Optimization, edited by T. Sasao*, 1993. Chapter 10.

$$
\begin{bmatrix} c_0 \\ c_{x_1} \\ c_{x_2} \\ c_{x_1x_2} \\ c_{x_3} \\ c_{x_1x_3} \\ c_{x_2x_3} \\ c_{x_1x_2x_3} \end{bmatrix}
= \frac{1}{2^n} \cdot
\begin{bmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\
1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\
1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\
1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\
1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\
1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\
1 & -1 & -1 & 1 & -1 & 1 & 1 & -1
\end{bmatrix}
\cdot
\begin{bmatrix} s_0^2 \\ s_1^2 \\ s_2^2 \\ s_{12}^2 \\ s_3^2 \\ s_{13}^2 \\ s_{23}^2 \\ s_{123}^2 \end{bmatrix}
$$

Figure 3. A three variable example of computing the autocorrelation coefficients from the spectral coefficients using the Hadamard transform matrix.

function no.																	
1	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	
2	16	16	16	16	-16	16	16	-16	16	-16	-16	-16	-16	-16	16	-16	
3	16	16	16	0	0	16	0	0	0	0	0	0	0	0	0	0	
4	16	16	0	0	0	0	0	0	0	0	0	-16	0	0	0	-16	
5	16	16	8	8	8	8	8	8	8	8	8	8	8	8	8	8	
6	16	16	8	8	-8	8	8	-8	8	-8	-8	-8	-8	-8	8	-8	
7	16	12	12	12	-12	12	12	-12	12	-12	-12	-12	-12	-12	12	-12	
8	16	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	
9	16	12	12	4	4	12	4	4	4	4	4	4	4	4	4	4	
10	16	12	12	4	-4	12	4	-4	4	-4	-4	-4	-4	-4	4	-4	
11	16	12	4	4	-4	4	4	-4	4	-4	-4	-12	-4	-4	4	-12	
12	16	8	8	8	0	0	8	0	8	0	0	0	0	0	8	0	
13	16	8	8	8	-8	8	8	-8	8	-8	-8	-8	-8	-8	8	-16	
14	16	8	8	0	0	8	0	0	0	0	0	-8	-8	0	0	-8	
15	16	8	8	0	0	0	0	0	0	0	-8	-8	-8	0	0	-8	
16	16	4	4	4	4	4	4	-4	-4	4	-4	-4	-4	4	4	4	
17	16	4	4	4	4	4	-4	-4	-4	-4	4	-4	-4	-4	-4	-4	
18	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
	0000	1000	0100	0010	0001	1100	1010	1001	0110	0101	0011	0111	1011	1101	1110	1111	τ

Table 1. The canonical representatives for the $n \leq 4$ autocorrelation classes in $\{+1, -1\}$ notation.