Symmetrical, Dual and Linear Functions and Their Autocorrelation Coefficients

in the Proceedings of IWLS2005

J. E. Rice
Department of Math & Computer Science
University of Lethbridge
Lethbridge, Alberta, Canada
j.rice@uleth.ca

R. Jansen
Department of Computing Science
University of Alberta
Edmonton, Alberta, Canada
mjansen@ualberta.ca

***Abstract*— The ability to identify special properties such as symmetries, linearity, or duality in Boolean logic functions is very useful in many aspects of logic synthesis. Another tool whose uses have lately been introduced for logic synthesis and classification applications is the autocorrelation transform. This paper details the connections between the autocorrelation coefficients and the existence of these special properties.**

I. Introduction

Symmetry is a very useful property to identify in Boolean functions. Partial symmetries exist in most Boolean functions, particularly those used in practical applications. Both total and partial symmetry properties are commonly used in synthesis of digital circuits and in particular in the reduction of the size of Binary Decision Diagram (BDD) representations of functions [1], [2]. It is also useful to identify if a function is dual, self-dual or linear.

Another technique often used in logic synthesis is that of applying a mathematical transform to a logic function to determine a series of coefficients. Transforms such as the Hadamard and Walsh and their applications in digital logic are well researched [3]. Another transform known as the autocorrelation transform is less well-known. The autocorrelation transform has been demonstrated to be of use in areas such as variable ordering for Binary Decision Diagrams [4] and in computing the estimate $C(f)$ of a function's complexity [5], [6]. In addition, recent work [7] has used the autocorrelation coefficients in classification of Boolean functions. If one is to use the autocorrelation coefficients for one of these other uses, it seems logical to make use of them in as many ways as possible. Thus, this paper discusses how the autocorrelation coefficients are affected by symmetries and other special properties of switching functions, and how this knowledge may be utilized.

II. Background

We first present some notation and background.

A. Symmetries

There are a number of different types of symmetries. We begin with the most restrictive symmetry. A Boolean function is said to be totally symmetric if the output is unchanged by any permutation of the inputs to the function. For example, the majority function $f = x_1 + x_2 + x_3$ is totally symmetric, as is the function $f = x_1x_2 + x_2x_3 + x_1x_3$.

A slightly less restrictive form of symmetry is that of partial symmetry. A Boolean function is said to be partially symmetric, or possess a partial symmetry if the output is unchanged by any permutation of some subset of the inputs to the function.

A third type of symmetry is a symmetry of degree two. This is a partial symmetry in which two subfunctions of the original function are identical and also are independent of two of the function's variables. Symmetries of degree two are identified by finding patterns where

$$f(x_1, ..., a, ..., b, ..., x_n) = f(x_1, ..., c, ..., d, ..., x_n),$$

$a, b, c, d \in \{0, 1\}$. Equivalence (E), non-equivalence (N) and single-variable (S) symmetries as defined by Hurst *et. al.* [3] are all types of symmetries of degree two, and are defined in Table I. Without loss of generality these definitions label the two variables of interest as n and $n-1$.

Symmetry	Definition
$E\{x_{n-1}, x_n\}$	$f(x_1, ..., x_{n-2}, 0, 0) = f(x_1, ..., x_{n-2}, 1, 1)$
$N\{x_{n-1}, x_n\}$	$f(x_1, ..., x_{n-2}, 0, 1) = f(x_1, ..., x_{n-2}, 1, 0)$
$S\{x_n \vert x_{n-1}\}$	$f(x_1, ..., x_{n-2}, 1, 0) = f(x_1, ..., x_{n-2}, 1, 1)$
$S\{x_n \vert \overline{x}_{n-1}\}$	$f(x_1, ..., x_{n-2}, 0, 0) = f(x_1, ..., x_{n-2}, 0, 1)$

TABLE I
Definitions and notation for equivalence, non-equivalence, and single-variable symmetries.

A more recently introduced symmetry has been termed *antisymmetries* [8]. An antisymmetry occurs when permuting all or a subset of variables results in the exact inverse of the original function. This can also be extended to the symmetries of degree two, as given in Table II.

B. Self-Duality

Definition 2.1: The dual of a function $f(x_1, x_2, \ldots, x_n)$ is $\overline{f}(\overline{x}_1, \overline{x}_2, \ldots, \overline{x}_n)$ and is denoted by f^d [9].

Antisymmetry	Definition
$\overline{E}\{x_{n-1}, x_n\}$	$f(x_1, ..., x_{n-2}, 0, 0) = \overline{f(x_1, ..., x_{n-2}, 1, 1)}$
$\overline{N}\{x_{n-1}, x_n\}$	$f(x_1, ..., x_{n-2}, 0, 1) = \overline{f(x_1, ..., x_{n-2}, 1, 0)}$
$\overline{S}\{x_n \vert x_{n-1}\}$	$f(x_1, ..., x_{n-2}, 1, 0) = \overline{f(x_1, ..., x_{n-2}, 1, 1)}$
$\overline{S}\{x_n \vert \overline{x}_{n-1}\}$	$f(x_1, ..., x_{n-2}, 0, 0) = \overline{f(x_1, ..., x_{n-2}, 0, 1)}$

TABLE II

DEFINITIONS AND NOTATION FOR THE ANTISYMMETRIES OF DEGREE TWO.

f^d is obtained first by replacing each literal x_i with $\overline{x}_i$ and then by complementing the function. A self-dual function is a function such that $f = f^d$. There are $2^{2^{n-1}}$ self-dual functions of n variables.

Let f be a self-dual function of n variables, and let $|f|$ be the number of inputs a for which $f(a)$=1,then $|f|$=2^{n-1}. A function which is obtained by assigning a self-dual function to a variable of a self-dual function is also self-dual.

C. Linearity

Definition 2.2: If a logic function f is represented as

$$f = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus \cdots \oplus a_n x_n$$

where $a_i = 0$ or 1 then f is said to be a linear function [9].

It is interesting to note that a linear function is either a self-dual or self-anti-dual function. The proof is given in [9]. There are 2^{n+1} linear functions of n variables, and a linear function that is obtained by assigning a linear function to an arbitrary variable of a linear function is also a linear function.

D. Autocorrelation Coefficients

Switching functions can be translated to other domains, such as the spectral domain. In this paper we consider the calculation of a function's autocorrelation coefficients, which are one possible representation in the spectral domain. The autocorrelation function is defined as follows [6]:

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

The superscripts $f\ f$ are generally omitted.

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*; however, multiple-output functions are not yet considered in this work.

The above definition for $B(\tau)$ assumes that the outputs of the switching function f are encoded as $\{0, 1\}$. If the function is alternately encoded as $\{+1, -1\}$ then the definition of the autocorrelation function is the same, with the resulting coefficients being referred to as $C(\tau)$.

Work in [7] demonstrated that there are four invariant operations for the $\{+1, -1\}$ autocorrelation coefficients. The invariant operations are as follows:

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

These invariant operations have been used to define classes of functions, referred to as autocorrelation classes. The reader is referred to [7] for further details. Table XI lists the autocorrelation classes for $n \leq 4$.

III. TOTALLY SYMMETRIC FUNCTIONS

Before examining the relationships between totally symmetric functions and their autocorrelation coefficients, some notation is required. There are 2^n autocorrelation coefficients for a function of n inputs. In general, these coefficients are grouped according to the weight, or the number of ones in the binary expansion of the value τ used to compute each coefficient. This is written $|\tau|$. All coefficients for which $|\tau| = 1$ are referred to as first order coefficients, second order coefficients are those for which $|\tau| = 2$ and so on.

τ_i will henceforth be used to refer to a value whose binary expansion contains a 1 in the i^{th} bit, while the remaining $n-1$ bits in the binary expansion of τ are 0. Additionally, $\tau_{i\alpha}$ will be used to refer to a set of values for which the binary expansion contains a 1 in the i^{th} bit while the remaining $n-1$ bits have the value $\alpha \in \{0, ..., 2^{n-1}-1\}$. $\tau_{\overline{i}\alpha}$ refers to a set of values for which the binary expansion contains a 0 in the i^{th} bit while the remaining $n-1$ bits have the value α.

Theorem 3.1: If a function f is totally symmetric or totally antisymmetric then all $\{+1, -1\}$ autocorrelation coefficients for any given order will be equal within the order. This may be written as $C(\tau) = C(\tau')\ \forall\ \tau, \tau'$ such that $|\tau| = |\tau'|$.

Work in [7] showed that permuting any two variables j and k results in exchanging the values of the coefficients $C(\tau_{j\alpha})$ and $C(\tau_{k\alpha})$. Since a function symmetric in two variables j and k by definition will not change if j and k are permuted then the autocorrelation coefficients will also not change – the function remains the same. Thus for $C(\tau_{j\alpha})$ and $C(\tau_{k\alpha})$ to be exchanged and yet no change to occur, we must have $C(\tau_{j\alpha}) = C(\tau_{k\alpha})$. A function that is totally symmetric will not change for any permutation of its variables, so $C(\tau_{1\alpha}) = C(\tau_{2\alpha}) = ... = C(\tau_{n\alpha})$, assuming the variables are numbered from 1 to n. We can express this as $C(\tau) = C(\tau')$ where $|\tau| = |\tau'|$ since α can take on any value and the property still holds.

We note that this implies that there are non-totally- symmetric functions with coefficients of this pattern. An example of this is given below in Section IV. However, such a function must be in the same autocorrelation class as some totally symmetric function. We expand upon this in Section IX.

We note also that the above theorem includes totally anti-symmetric functions. Since the negation of a function does not affect the $\{+1, -1\}$ autocorrelation coefficients it is relatively easy to include anti-symmetries in any discussion of symmetry, as an anti-symmetry involves only negation of the function or subfunction in question.

x_1x_2 \ x_3x_4	00	01	11	10
00	a	b	c	b
01	b	c	d	c
11	c	d	e	d
10	b	c	d	c

Fig. 1. The Karnaugh map for a completely symmetric 4-variable Boolean function .

In terms of the autocorrelation classes, totally symmetric functions can appear in a number of the classes. Examination of the 32 possible totally symmetric functions for $n = 4$ shows that 8 of the 18 autocorrelation classes for $n = 4$ (as shown in the Appendix) contain totally symmetric functions. This is contrary to what we had expected; preliminary thinking on this subject had considered the possibility that all totally symmetric functions would fall into the same autocorrelation class. However, upon examination (and by brute force) this is clearly not the case. Consider the a Karnaugh-map for a four-variable function f, as shown in Figure 1. Possible assignments for the letters include $a, b, c, d, e = 0$, $a = 1, b, c, d, e = 0$, $a, b = 1, c, d, e = 0$ and so on. Clearly the first assignment and second assignment must be in different autocorrelation classes, as a totally symmetric function with the first assignment is the trivial function $f(X) = 0$ while the function with the second assignment is a function with 1 true minterm, $f(X) = \overline{x}_1\overline{x}_2\overline{x}_3\overline{x}_4$. No application of any of the invariant operations can generate a function with 1 true minterm from a function that has no true minterms. In fact, this can be somewhat generalized; the only invariant operation that can generate a differing number of true minterms in a function belonging to the same autocorrelation class is that of negating the function. In this case the resulting function will have $2^n - k$ true minterms, k being the number of original true minterms. Thus many of the possible totally symmetric functions must belong to different autocorrelation classes, simply because they have different values for k.

Examination of the $n \leq 4$ autocorrelation classes, however, shows that in some cases there are several classes whose member functions have the same numbers of true minterms. For instance, there are 4 distinct classes whose functions each have 8 true minterms. In this case all totally symmetric functions with 8 true minterms fall into the same autocorrelation class. The only situation for which this does not occur is the situation in which there are 6 true minterms. Totally symmetric functions with 6 true minterms may be generated in three ways (for $n \leq 4$): either $c = 1$ and $a, b, d, e = 0$, or $a, b, e = 1$ and $c, d = 0$, or $a, d, e = 1$ and $b, c = 0$. In one case we have only a single letter being assigned a 1 while in the other two cases we have three letters being assigned 1's. We hypothesize that the structures thus illustrated are different enough that no combination of the invariant operations can result in a transformation from one structure to the other, and thus we have two unique classes, each whose functions have 6 true minterms, and each containing one or more totally symmetric functions. We are continuing to investigate this concept of a function's structure, and how it relates to classes and the autocorrelation coefficients.

IV. Partially Symmetric Functions

Theorem 4.1: If a function f is partially symmetric in a subset of its input variables $x_i, \ldots, x_{i_m}$ then the autocorrelation coefficients $C(\tau_{j\ \alpha})$ will have equal values for all $j \in \{i, \ldots, i + m\}$.

The same reasoning as used above for Theorem 3.1 can be used here. Permuting any m variables i through $i + m$ results in exchanging the values of the coefficients $C(\tau_{i\alpha})$ through $C(\tau_{(i+m)\alpha})$. However, the function does not change, by definition, and so coefficients $C(\tau i\alpha)$ through $C(\tau_{(i+m)\alpha})$ must be equal.

For example, the function $f(X) = \overline{x}_1\overline{x}_2\overline{x}_3 + \overline{x}_3x_4 + \overline{x}_1x_4 + x_2x_3 + x_1x_2 + x_1x_3$ is partially symmetric in x_1, x_2, x_3. It appears that the product $\overline{x}_2x_4$ is missing, when actually it is unnecessary as it is covered by the other products. The autocorrelation coefficients for this function are given in Table III. Of note are the second order coefficients, which illustrate the Theorem above.

τ	$C(\tau)$	τ	$C(\tau)$	τ	$C(\tau)$	τ	$C(\tau)$
0000	16	0100	4	1000	4	1100	12
0001	4	0101	4	1001	4	1101	4
0010	4	0110	12	1010	12	1110	4
0011	4	0111	4	1011	4	1111	4

TABLE III

THE $\{+1, -1\}$ AUTOCORRELATION COEFFICIENTS FOR THE PARTIALLY SYMMETRIC FUNCTION

$f(X) = \overline{x}_1\overline{x}_2\overline{x}_3 + \overline{x}_3x_4 + \overline{x}_1x_4 + x_2x_3 + x_1x_2 + x_1x_3.$

We have also investigated how partially symmetric functions fall into the autocorrelation classes. However, there are clearly far more possibilities and a brute force examination is not possible, even for $n \leq 4$. One interesting observation was made; it appears that all of the $n \leq 4$ autocorrelation classes contain functions with partial symmetries on three variables except class number 15.

V. Functions with Symmetries of Degree Two

Theorem 5.1: A function $f(X)$ with some type of symmetry of degree two will have autocorrelation coefficient values as follows:

$E\{x_i, x_j\}$ or $N\{x_i, x_j\} \rightarrow C(\tau_{i\alpha}) = C(\tau_{j\alpha})$

$S\{x_j|x_i\}$ or $S\{x_j|\overline{x}_i\} \rightarrow C(\tau_{i\alpha}) = C(\tau_{ij\alpha})$

$S\{x_i|x_j\}$ or $S\{x_i|\overline{x}_j\} \rightarrow C(\tau_{j\alpha}) = C(\tau_{ij\alpha})$

Proofs for these are given in [7]. Again, as for partial symmetries, it appears that all autocorrelation classes contain functions with symmetries of degree two.

VI. Is it Possible to Determine Symmetries from the Autocorrelation Coefficients?

Hurst *et. al.* [3] provide tests based on a function's spectral coefficients that will ascertain whether or not the function possesses a particular symmetry. However, as indicated by the example in Table III, the autocorrelation coefficients cannot be

used in the same way. This can be explained by examining the spectral symmetry tests, as described in Table IV. The notation used in this table is as follows:

S^0 includes all spectral coefficients that involve neither of x_i or x_j,
S^1 includes all spectral coefficients that involve x_i but not x_j,
S^2 includes all spectral coefficients that involve x_j but not x_i, and
S^3 includes all spectral coefficients that involve both x_i and x_j.

the spectral coefficients are computed using

$$T^n \cdot Y = S. \tag{2}$$

For example, for a $n = 3$ Boolean function,

$$T^n = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix},$$

Y is the output vector of the function, for example

$$Y = \begin{bmatrix} 1 \\ -1 \\ -1 \\ 1 \\ 1 \\ 1 \\ 1 \\ -1 \end{bmatrix} \begin{matrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7, \end{matrix}$$

and S is the resulting spectral coefficients. Using the sample function from above, the coefficients would be

$$S = \begin{bmatrix} 2 \\ 2 \\ 2 \\ 2 \\ -2 \\ -2 \\ -2 \\ 6 \end{bmatrix} \begin{matrix} s_0 \\ s_1 \\ s_2 \\ s_{12} \\ s_3 \\ s_{13} \\ s_{23} \\ s_{123}. \end{matrix}$$

Examination of the spectral symmetry tests for three variables

Symmetry	Test
$S\{x_{n-1}\|\overline{x}_n\}$	$S^1 + S^3 = 0$
$S\{x_n\|\overline{x}_{n-1}\}$	$S^2 + S^3 = 0$
$E\{x_n, x_{n-1}\}$	$S^1 + S^2 = 0$
$N\{x_n, x_{n-1}\}$	$S^1 - S^2 = 0$
$S\{x_n\|x_{n-1}\}$	$S^2 - S^3 = 0$
$S\{x_{n-1}\|x_n\}$	$S^1 - S^3 = 0$

TABLE IV

SPECTRAL SYMMETRY TESTS FOR SYMMETRIES IN $\{x_{n-1}, x_n\}$

illustrates that if

$$\begin{bmatrix} s_2 \\ s_{12} \end{bmatrix} = \begin{bmatrix} s_3 \\ s_{13} \end{bmatrix}$$

then the function must possess $N\{x_2, x_3\}$. Similarly, if

$$\begin{bmatrix} s_2 \\ s_{12} \end{bmatrix} = \begin{bmatrix} -s_3 \\ -s_{13} \end{bmatrix}$$

then the function must possess $E\{x_2, x_3\}$. The notation used here for labeling of coefficients is as illustrated in the example above.

In the autocorrelation coefficients, this distinction is lost. This brings to question the following situation. If

$$\begin{bmatrix} s_2 \\ s_{12} \end{bmatrix} = \begin{bmatrix} -s_3 \\ s_{13} \end{bmatrix}$$

then the autocorrelation coefficients will still be equal; however, the symmetries do not exist. The same holds true if $s_2 = s_3$ and $s_{12} = -s_{13}$. Therefore it is not possible to determine if a function has a particular equivalence, nonequivalence or single variable symmetry solely by examining the autocorrelation coefficients. The same holds true for totally and partially symmetric functions.

VII. SELF-DUAL FUNCTIONS

Theorem 7.1: A function will have $C(2^n - 1) = -2^n$ if and only if it is a self-dual function. Similarly, a function will have $C(2^n - 1) = 2^n$ if and only if it is a self-dual function.

If a function is self-dual, then by definition

$$f(X) = \overline{f}(\overline{X}),$$

which can be rewritten as

$$f(X) = \overline{f}(X \oplus 2^n - 1).$$

Using $\{+1, -1\}$ notation $f(X) \cdot \overline{f}(X) = -1$. Thus

$$\begin{aligned} C(2^n - 1) &= \sum_{v=0}^{2^n-1} f(v) \cdot f(v \oplus 2^n - 1) \text{ by defn} \\ &= \sum_{v=0}^{2^n-1} f(v) \cdot \overline{f}(v) \\ &= -2^n. \end{aligned}$$

Similarly, for self-anti-dual functions, by definition

$$f(X) = f(\overline{X}),$$

which can be rewritten

$$f(X) = f(X \oplus 2^n - 1)$$

and so

$$\begin{aligned} C(2^n - 1) &= \sum_{v=0}^{2^n-1} f(v) \cdot f(v \oplus 2^n - 1) \text{ by defn} \\ &= \sum_{v=0}^{2^n-1} f(v) \cdot f(v) \\ &= 2^n. \end{aligned}$$

If $C(2^n - 1) = -2^n$ then every pair of minterms $f(v)$ and $f(v \oplus 2^n - 1)$ in the summation $\sum_{v=0}^{2^n-1} f(v) \cdot f(v \oplus 2^n - 1)$ must result in a -1 when multiplied and thus must have inverse values of each other. So

$$f(v) = \overline{f}(v \oplus 2^n - 1),$$

or,

$$f(v) = \overline{f}(\overline{v}),$$

which is the definition of a self-dual function.

Similarly, if $C(2^n - 1) = 2^n$ then every pair of minterms $f(v)$ and $f(v \oplus 2^n - 1)$ in the summation $\sum_{v=0}^{2^n-1} f(v) \cdot f(v \oplus 2^n - 1)$ must result in a 1 when multiplied and thus must have identical values. So

$$f(v) = f(v \oplus 2^n - 1),$$

or,

$$f(v) = f(\overline{v}),$$

which is the definition of a self-anti-dual function.

VIII. Linear Functions

Theorem 8.1: A function is linear if and only if all of its coefficients $C(\tau) = -2^n$, such that the weight of τ $|\tau| = 1$.

This theorem comes from work in [7] in which the following theorem is proven:

Theorem 8.2: $C(\tau_i) = -2^n$ if and only if $f(X)$ has a decomposition

$$f(X) = f^*(X) \oplus x_i$$

such that $f^*(X)$ is independent of x_i and τ_i has the binary expansion consisting of a 1 in position i and zeroes in all other positions.

We extend this theorem further to specify that if ALL values of τ with a single one in the binary expansion result in $C(\tau) = -2^n$ then the function must be decomposable for all variables in the fashion described above.

IX. Discussion and Future Work

As noted in Sections III and IV, identifying where a function has equal coefficients within a given order, or in a subset of that order, is not sufficient to identify a symmetric function. However, a function that does not have a symmetry but whose autocorrelation coefficients reflect this property must be in the same class as some totally/partially symmetric function. Thus it may be possible to identify the necessary operations to apply in order to transform the subject function into a some type of symmetric function, thus making it possible to leverage the advantages inherent in symmetries during the optimization or other processing of the subject function. Future work will address tools to make this determination.

Additionally, Section III also discusses the possiblity that two functions which are each totally symmetric may be grouped into two different autocorrelation classes. This implies a significant difference in their underlying structures. Without applying all possible combinations of the invariant operations it can be impossible to determine whether or not two functions will be grouped into the same class. Thus we are investigating this analysis of the structure of a function, to attempt to find a fast determination of whether two functions are in the same autocorrelation class. This could then be extended to other classification schemes.

A comment on the suitability of the autocorrelation transform as an analysis tool is appropriate; the authors have found that properties defined on the outputs of a function are better suited to analysis with autocorrelation coefficients than are properties defined based on the structure of a function. For instance, the properties of self-duality and self-anti-duality lend themselves very nicely to identification through autocorrelation coefficients, while on the other hand monotone functions are much more difficult to identify.

X. Conclusion

There are many existing techniques for the identification of properties such as symmetries, including [10], [11] and [2]. Rather than competing with these, this paper concentrates instead on the theoretical aspects of the autocorrelation transform as an analysis tool. We can conclude from this work that the autocorrelation transform can identify if a function does *not* possess a symmetry, but that the autocorrelation coefficients resulting from the transform do not provide a sufficient condition for the existence of symmetries. Ongoing work in this area includes implementation of our technique in order that we may compare it with existing techniques as mentioned above, as well as the various directions described in Section IX. An extension of the analysis led to necessary and sufficient conditions for the identification of self-dual/self-anti-dual and linear functions. Future work will include implementations for these properties as well.

References

[1] L. Heinrich-Litan and P. Molitor, "Least Upper Bounds for the Size of OBDDs Using Symmetry Properties," *IEEE Trans. on Comp.*, pp. 360–368, Apr. 2000.

[2] S. Panda, F. Somenzi, and B. Plessier, "Symmetry Detection and Dynamic Variable Ordering of Decision Diagrams," in *Proceedings of the International Conference on Computer-Aided Design (ICCAD)*, 1994.

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

[4] 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.

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

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

[7] J. E. Rice, *Autocorrelation Coefficients in the Representation and Classification of Switching Functions*, Ph.D. thesis, University of Victoria, 2003.

[8] J. E. Rice and J. C. Muzio, "Antisymmetries in the Realization of Boolean Functions," in *Proceedings of the International Symposium on Circuits and Systems (ISCAS)*, 2002, CD ROM paper number 2666.

[9] T. Sasao, *Switching Theory for Logic Synthesis*, Kluwer Academic Publishers, 1999.

[10] D. Möller, J. Mohnke, and M. Weber, "Detection of Symmetry of Boolean Functions Represented by ROBDDs," in *Proceedings of the International Conference on Computer-Aided Design (ICCAD)*, 1993, pp. 680–684.

[11] S. Kannurao and B. J. Falkowski, "Identification of Complement Single Variable Symmetry in Boolean Functions Through Walsh Transform," in *Proceedings of the International Symposium on Circuits and Systems (ISCAS)*, 2002.

XI. Appendix

class no.																
1	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16
	$f(X) = 0$															
2	16	16	16	16	-16	16	16	-16	16	-16	-16	-16	-16	-16	16	-16
	$f(X) = x_4$															
3	16	16	16	0	0	16	0	0	0	0	0	0	0	0	0	0
	$f(X) = x_3x_4$															
4	16	16	0	0	0	0	0	0	0	0	0	-16	0	0	0	-16
	$f(X) = x_1x_2 + x_2x_4 + x_2x_3$															
5	16	16	8	8	8	8	8	8	8	8	8	8	8	8	8	8
	$f(X) = x_2x_3x_4$															
6	16	16	8	8	-8	8	8	-8	8	-8	-8	-8	-8	-8	8	-8
	$f(X) = x_3x_4 + x_2x_4$															
7	16	12	12	12	-12	12	12	-12	12	-12	-12	-12	-12	-12	12	-12
	$f(X) = x_1x_2 + x_1x_3 + x_1x_4$															
8	16	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12
	$f(X) = x_1x_2x_3x_4$															
9	16	12	12	4	4	12	4	4	4	4	4	4	4	4	4	4
	$f(X) = x_2x_3x_4 + x_1x_3x_4$															
10	16	12	12	4	-4	12	4	-4	4	-4	-4	-4	-4	-4	4	-4
	$f(X) = x_1x_2x_4 + x_3x_4$															
11	16	12	4	4	-4	4	4	-4	4	-4	-4	-12	-4	-4	4	-12
	$f(X) = x_1x_2x_3 + x_3x_4 + x_2x_4$															
12	16	8	8	8	0	0	8	0	8	0	0	0	0	0	8	0
	$f(X) = x_2x_3x_4 + x_1x_3x_4 + x_1x_2x_4$															
13	16	8	8	8	-8	8	8	-8	8	-8	-8	-8	-8	-8	8	-16
	$f(X) = x_1x_2x_3 + x_3x_4 + x_2x_4 + x_1x_4$															
14	16	8	8	0	0	8	0	0	0	0	0	-8	-8	0	0	-8
	$f(X) = x_3x_4 + x_1x_2x_4 + x_1x_2x_3$															
15	16	8	8	0	0	0	0	0	0	0	-8	-8	-8	0	0	-8
	$f(X) = x_2x_3 + x_1x_4 + x_3x_4$															
16	16	4	4	4	4	4	4	-4	-4	4	-4	-4	-4	4	4	4
	$f(X) = x_2x_3x_4 + x_1x_3x_4 + x_1x_2x_4 + x_1x_2x_3$															
17	16	4	4	4	4	4	-4	-4	-4	-4	4	-4	-4	-4	-4	-4
	$f(X) = x_2x_3 + x_1x_4$															
18	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	$f(X) = \overline{x}_1x_2x_3 + x_1\overline{x}_2x_4 + x_1\overline{x}_3x_4 + x_2x_3\overline{x}_4$															
	0000	1000	0100	0010	0001	1100	1010	1001	0110	0101	0011	0111	1011	1101	1110	1111	τ

TABLE V

The $n \leq 4$ autocorrelation classes and their underlying functions.