Properties of Autocorrelation Coefficients

in the Proceedings of PACRIM 2003

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

J. C. Muzio
Department of Computer Science
University of Victoria
Victoria, BC, Canada
Email: jmuzio@cs.uvic.ca

***Abstract*— The use of spectral techniques in logic synthesis is well researched and well known. However, there is very little work surrounding the use of other transforms such as the autocorrelation transform. This paper introduces a variety of properties inherent to the coefficients produced by the autocorrelation transform, and discusses potential applications.**

I. Introduction

Much work has been performed in applying transforms to switching functions in order to achieve a more global view of the function. Transforms such as the Hadamard and Rademacher-Walsh and their applications in digital logic are well researched [1]. There is far less work, however, on the use of other transforms such as the autocorrelation transform.

The autocorrelation transform has been used in various areas including optimization and synthesis of combinational logic [2], variable ordering for Binary Decision Diagrams [3], and to compute the estimate $C(f)$ of a function's complexity [2], [4]. However, the use has been limited, likely due to the fact that little work has been done investigating their properties, and until recently, methods for computating the autocorrelation coefficients were exponential in the number of inputs to the function(s). Since new methods for their computation have recently been introduced by Rice *et. al.* [5], [6], we also have performed an investigation into what useful properties may be present in the autocorrelation coefficients for Boolean functions.

In this paper we present the definition and an explanation of the autocorrelation transform. We introduce several theorems relating the values of the the resulting autocorrelation coefficients to properties of the underlying switching function. A number of potential applications for these theorems are presented, and directions in which this work may progress is also discussed.

II. Background

The application of the autocorrelation transform to a switching function results in a comparison of the function to itself, shifted by a specified amount. The autocorrelation transform is a special case of the correlation transform, which is defined as [4]:

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

If f and g are the same function then this becomes the autocorrelation transform, also called the cross-correlation, or convolution function. The superscript is generally omitted when referring to the autocorrelation transform.

$B(\tau)$ is evaluated with f in the usual Boolean domain of $\{0,1\}$. If $\{+1,-1\}$ encoding is used then the resulting autocorrelation coefficients are denoted as $C(\tau)$:

$$C(\tau) = \sum_{v=0}^{2^n-1} f(v) \cdot f(v \oplus \tau). \quad (2)$$

It is possible to convert between B and C using the following equation:

$$C(\tau) = 2^n - 4k + 4B(\tau). \quad (3)$$

In this equation, $k = B(0)$, which is also the number of minterms in the function. The derivation is given in Appendix I.

III. Notation

Some additional notation is required for the latter portions of this paper:

- The variable ordering $x_n, ..., x_1$ is used through-out. Thus a coefficient $B(001)$ or $C(001)$ is the first order coefficient corresponding to x_1.
- τ and τ' indicate values ranging from 0 to $2^n - 1$. τ_a is used to indicate one such value.
- τ_i refers to a value whose binary expansion contains a 1 in the i^{th} bit, while the remaining $n-1$ bits are 0.
- $\tau_{i\alpha}$ refers 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.
- $|\tau|$ is the weight, or the number of ones in the binary expansion of τ. If $|\tau| = j$ then $B(\tau)$ and $C(\tau)$ are said to be j^{th} order coefficients.

IV. Observations on the Signs and Values of the Autocorrelation Coefficients

There are a number of restrictions on the values of both the $\{0,1\}$ and $\{+1,-1\}$ autocorrelation coefficients. Knowing

these limitations can provide a simple check as to whether the coefficients have been computed correctly. They also lead to the identification of more specific properties relating the coefficient values to the original switching function.

- $B(\tau) \in \{0, \ldots, 2^n\}\ \forall\ \tau$.
- $B(\tau)$ is even $\forall\ \tau \neq 0$.
- $B(\tau) \leq B(0)\ \forall\ \tau \neq 0$ and $B(0) = k$ where k refers to the number of minterms of the switching function.
- $C(\tau) \in \{-2^n, \ldots, 2^n\}$ and is evenly divisible by $2\ \forall\ \tau$.
- A function may have at most 2^{n-1} negative $C(\tau)$.
- $C(\tau) \leq C(0)\ \forall\ \tau \neq 0$ and $C(0) = 2^n$.

These observations are, in general, clear from the definition of the autocorrelation transform[1].

Further observations may be made about the sum of autocorrelation coefficients:

Theorem 4.1:

$$\sum_{\tau=0}^{2^n-1} B(\tau) = k^2. \tag{4}$$

Lemma 4.1:

$$\sum_{\tau=1}^{2^n-1} B(\tau) = 2\binom{k}{2}. \tag{5}$$

$\binom{k}{2}$ is the number of pairings of the minterms as computed in the summation of the autocorrelation coefficients. This is then multiplied by 2 to produce all possible pairings in the form i, j and j, i. *Proof:* Using Lemma 4.1 the sum of all of the $\{0, 1\}$ autocorrelation coefficients is as follows:

$$\begin{aligned}\sum_{\tau=0}^{2^n-1} B(\tau) &= B(0) + 2\binom{k}{2} \\ &= k + 2\tfrac{k(k-1)}{2} \\ &= k^2.\end{aligned}$$

■

By applying Equation 3 to the above Theorem, we find that

$$\sum_{\tau=0}^{2^n-1} C(\tau) = (2^n - 2k)^2. \tag{6}$$

V. General Properties

This section introduces three theorems that relate particular patterns in the autocorrelation coefficients to underlying properties of the switching function. If a designer is given a function to work with for which no information is available, these theorems may be applied to provide the designer with some information about the type of function with which he/she is working.

A. Trivial Functions

Theorem 5.1: $C(\tau) = C(\tau')\ \forall\ \tau$ *and* $\tau' \in \{0, \ldots, 2^n - 1\}$ *if and only if* $f(X) = 1$ *or* $f(X) = 0$.

Proof: If all the coefficients are equal, they must all have the value 2^n as the coefficient $C(0)$ always has this value. Based on this, if all of the coefficients have equal value, then this implies that the function matches itself at every value of τ. This can only occur if the function consists entirely of true minterms, or entirely of false minterms. ■

The corollary for $\{0, 1\}$ coefficients is found by applying Equation 3 to Theorem 5.1.

B. Degenerate Functions

The following two theorems may be applied to identify degenerate functions. The simplest situation occurs when the function is dependent on only one input variable. This is described in Theorem 5.2. A more general case occurs when the function is dependent on only j ($j < n$) of its input variables, which is detailed in Theorem 5.3.

Theorem 5.2: A function $f(X)$ has 2^{n-1} autocorrelation coefficients $C(\tau) = 2^n$ (including $C(0)$) and the remaining 2^{n-1} coefficients $C(\tau') = -2^n$ if and only if the function has exactly 2^{n-1} true minterms.

Proof: A function that is dependent on only one input variable must have half of the minterms true and half of them false. Without loss of generality let us define $f(X) = x_1$ where x_1 is the lowest order bit of the input X. Then if τ is an odd number the binary expansion of τ contains a 1 in the lowest order bit, and then by definition $f(v) = \overline{f(v \oplus \tau)}$. Then

$$\begin{aligned}C(\tau) &= \sum_{v=0}^{2^n-1} 1 \times -1 \\ &= -2^n.\end{aligned}$$

Similarly if τ' is an even number, then the binary expansion contains a 0 in the lowest order bit and by definition $f(v) = f(v \oplus \tau')$. Then

$$\begin{aligned}C(\tau') &= \sum_{v=0}^{2^n-1} (-)1 \times (-)1 \\ &= 2^n.\end{aligned}$$

Given autocorrelation coefficients of the pattern described above the function must be dependent on only one of the input variables (or related to such a function). Without loss of generality we assume that $C(\tau') = 2^n$ where τ' is even and $C(\tau) = -2^n$ where τ is odd. $C(\tau') = 2^n$ where τ' is even indicates that the function matches up two false or two true minterms for every product in the summation. Additionally every product being computed is comparing two inputs for which x_1 remains unchanged. Moreover, $C(\tau) = -2^n$ where τ is odd indicates that the function matches a false minterm with a true minterm for every product in the summation, and that every product is matching a pair of inputs for which x_1 varies. Based on this we can determine that the function must be dependent only on x_1, and so there must be 2^{n-1} true minterms in the function. ■

The corollary for $\{0, 1\}$ encoding can be found by applying Equation 3 to Theorem 5.2.

Theorem 5.3: A function $f(X)$ is independent of j of its input variables if and only if $C(\tau_i) = 2^n\ \forall\ i\ \in 1..n$ such that the function does not depend on variable x_i.

[1]Some proofs were omitted from this work due to size constraints. Complete proofs are provided in [6].

Proof: Without loss of generality let us define a function $f(X)$ that is independent of x_n. By definition, $f(0, x_{n-1}, \ldots, x_1) = f(1, x_{n-1}, \ldots, x_1)$. Then

$$\begin{aligned} C(\tau_n) &= \sum_{v=0}^{2^n-1} f(v) \times f(v \oplus \tau_n) \\ &= \sum_{v=0}^{2^{n-1}-1} f(v) \times f(v \oplus \tau_n) \\ &\quad + \sum_{v=2^{n-1}}^{2^n-1} f(v) \times f(v \oplus \tau_n). \end{aligned}$$

Let us define the range 0 *to* $2^{n-1}-1$ as A and 2^{n-1} *to* 2^n-1 as B. Then $v \in A \Rightarrow v \oplus \tau_n \in B$ and $v \in B \Rightarrow v \oplus \tau_n \in A$. Since the function is defined to have $f(A) = f(B)$ then

$$\begin{aligned} C(\tau_n) &= \sum_{v=0}^{2^{n-1}-1} f(v) \times f(v \oplus \tau_n) \\ &\quad + \sum_{v=2^{n-1}}^{2^n-1} f(v) \times f(v \oplus \tau_n) \\ &= \sum_{v=0}^{2^{n-1}-1} 1 + \sum_{v=2^{n-1}}^{2^n-1} 1 \\ &= 2^n. \end{aligned}$$

To prove the second part of the theorem we define (without loss of generality) a function $f(X)$ for which $C(\tau_n) = 2^n$. This is only possible if $f(v) = f(v \oplus \tau_n)\ \forall\ v$. This implies that $f(1, x_{n-1}, \ldots, x_1) = f(0, x_{n-1}, \ldots, x_1)$, indicating that $f(X)$ is not dependent on x_n. ■

The corollary of this for the $\{0, 1\}$ encoding may be found by applying Equation 3 to Theorem 5.3.

C. Dissimilar Minterms

The following are three theorems that allow a designer to identify a sparse (or the inverse) function from the values of the function's autocorrelation coefficients. The first two theorems detail two specific cases: functions that possess one and only one true minterm (or the inverse) and functions that possess only two true minterms (or the inverse).

Theorem 5.4: A function f(X) has exactly one dissimilar minterm if and only if $C(\tau) = 2^n - 4\ \forall\ \tau \neq 0$.

Proof: Without loss of generality let us define a function f such that

$$\begin{aligned} f(v) &= 1,\ v \in\ 0, \ldots, 2^n - 2 \\ f(v) &= -1,\ v = 2^n - 1. \end{aligned}$$

Then

$$\begin{aligned} C(\tau) &= \sum_{v=0}^{2^n-1} f(v) \times f(v \oplus \tau) \\ &= (\sum_{v=0}^{2^n-2} f(v) \times f(v \oplus \tau)) + f(2^n - 1) \times f(2^n - 1 \oplus \tau) \\ &= (\sum_{v=0}^{2^n-2} 1 \times f(v \oplus \tau)) + -1 \times 1 \\ &= (2^n - 2 - 1) - 1 \\ &= 2^n - 4\ \forall\ \tau \neq 0. \end{aligned}$$

Thus if $f(X)$ has exactly one true minterm then all of the coefficients $C(\tau) = 2^n - 4$, $\tau \neq 0$.

For the second part of this proof, if all that is known of the function is the coefficients of this pattern, then it can be shown as follows that the function must have either exactly one true or exactly one false minterm.

For a coefficient $C(\tau)$ let us define q as the number of positive pairs in the summation, and r as the number of negative pairs in the summation. A pair in this case is a combination of two minterms i, j, and a positive pair results when both minterms are true or when both are false. It should be noted that in the summation for the autocorrelation equation each pair is encountered twice. Then

$$2q - 2r = 2^n - 4 \text{ and } 2q + 2r = 2^n.$$

These equations can be solved to show that $r = 1$. If there is only one negative pair in the summation then there is only one pair combining a true and a false minterm; all other pairs must combine either two true minterms or two false minterms. If there is only one coefficient $C(\tau)$ for which this holds, then there can be any number of combinations of true and false minterms to meet these requirements. However, there are $2^n - 1$ coefficients that have only one negative pair; therefore there can be only one dissimilar minterm in the function. ■

The corollary for the $\{0, 1\}$ encoding can be shown by applying Equation 3 to the Theorem above. The general result is as follows:

Corollary 5.1: A function $f(X)$ has exactly one dissimilar minterm if and only if $B(\tau) = k - 1$.

It should be pointed out that this general result is somewhat misleading; in practice the values for $B(\tau)$ are quite limited. This is because for a function to have exactly one dissimilar minterm then either $k = 2^n - 1$, in which case $B(\tau) = 2^n - 2\ \forall\ \tau \neq 0$, or $k = 1$, which results in $B(\tau) = 0\ \forall\ \tau \neq 0$.

Theorem 5.5: A function has exactly two dissimilar minterms if and only if

$$\begin{aligned} &C(0) = 2^n, \\ &C(\tau_a) = 2^n, \text{ and} \\ &C(\tau) = 2n - 8\ \forall\ \tau, \tau_a \neq 0 \text{ and } \tau \neq \tau_a. \end{aligned}$$

The proof is similar to that given for Theorem 5.4.

Corollary 5.2: A function has exactly two dissimilar minterms if and only if

$$\begin{aligned} &B(0) = B(\tau_a) = k \text{ and} \\ &B(\tau) = k - 2\ \forall\ \tau\ and\ \tau_a \neq 0 \text{ and } \tau \neq \tau_a. \end{aligned}$$

The above is determined by substituting the results of Theorem 5.5 into the conversion equation $C(\tau) = 2^n - 4k + 4B(\tau)$. Again, although Corollary 5.2 states a general result, in practice the values are limited to the following:

(i) $B(0) = B(\tau_a) = 2$ and $B(\tau) = 0$, or
(ii) $B(0) = B(\tau_a) = 2^n - 2$ and $B(\tau) = 2^n - 4$.

It should also be noted that this pattern of coefficients indicates that the function is either itself degenerate or is related through the application of the autocorrelation invariance operators [6] to a degenerate function. The third theorem generalizes the above results to d dissimilar minterms:

Theorem 5.6: A function has d dissimilar minterms if and only if the autocorrelation coefficients have the following properties:

- $C(0) = 2^n$,
- for $\binom{d}{p}$ $p \in 2, 4, 6, ..., d$, (or $2, 4, 6, ..., d-1$ if d is odd)
  $C(\tau) = 2^n - 4d + 4p$, and
- for the remaining coefficients, $C(\tau) = 2^n - 4d$.

Again, the proof is similar to that for Theorem 5.4.

VI. Conclusion

This work has presented a number of observations regarding the values of the autocorrelation coefficients for switching functions, as well as six theorems relating the values of particular coefficients to underlying properties of the originating switching function. This information can be used in a situation where a designer is given a switching function to optimize and/or synthesize, but no information about the function's use or structure is provided.

We envision making use of the autocorrelation coefficients and the research presented in this paper to develop a preprocessing tool that will inform the user about the function with which they are working. Information such as whether the function is degenerate, sparse, or has a particular structure can then be used to decide on the optimization or synthesis tools to be used. Other work in the area of autocorrelation coefficients has made use of them in the determination of three-level decompositions [7], and this would also be incorporated into such a tool.

Future work includes extending this research to the incompletely specified and multiple-output cases, and further investigation into other properties that may be identifiable through the use of the autocorrelation coefficients.

Appendix I
Derivation of Equation 3

Assuming that input variables encoded as $\{0, 1\}$ are referred to as z_i and input variables encoded as $\{+1, -1\}$ are encoded as y_i, then it is known that

$$y_i = -2z_i + 1. \tag{7}$$

Based on Equation 7 and the equation for computing the spectral coefficients ($R = T^n \times Z$ or $S = T^n \times Y$ [1]), one can also derive the following conversion between spectral coefficients computed using $\{+1, -1\}$ encoding (s_i) and the $\{0, 1\}$ spectral coefficients (r_i):

$$\begin{aligned} s_i &= -2r_i \text{ and} \\ s_0 &= -2r_0 + 2^n. \end{aligned} \tag{8}$$

Karpovksy demonstrated in [4] that the autocorrelation coefficients may be computed from the spectral coefficients using the following equation:

$$B = \frac{1}{2^n} \times T^n \times R^2 \tag{9}$$

where R^2 is the vector of $\{0, 1\}$ spectral coefficients with each element squared. Based on the relationships defined in these equations, we can determine that

$$C(\tau) = 2^n - 4k + 4B(\tau)$$

where $k = B(0)$.

References

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

[2] R. Tomczuk, "Autocorrelation and Decomposition Methods in Combinational Logic Design," Ph.D. dissertation, University of Victoria, 1996.

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

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

[5] J. E. Rice and J. C. Muzio, "Methods for Calculating Autocorrelation Coefficients," in *Proceedings of the 4th International Workshop on Boolean Problems, (IWSBP)*, 2000, pp. 69–76.

[6] J. E. Rice, "Autocorrelation Coefficients in the Representation and Classification of Switching Functions," Ph.D. dissertation, University of Victoria, 2003.

[7] J. E. Rice and J. C. Muzio, "On the Use of Autocorrelation Coefficients in the Identification of Three-Level Decompositions," in *Proceedings of the International Workshop on Logic Synthesis (IWLS)*, 2003, to appear.