

Characteristic Polynomial Method for Verification and Test of Combinational Circuits

Vishwani D. Agrawal and David Lee

AT&T Bell Laboratories

Murray Hill, NJ 07974

va@research.att.com, lee@research.att.com

In a recent paper, Jain *et al* [2] probabilistically establish the equivalence of two given Boolean functions. They assign randomly selected integers to input variables and compute integer-valued transform functions. If the evaluations give the same value, the Boolean functions are shown to be identical with some probability of error. The error probability is reduced as the domain from which the integers are obtained is enlarged. Also, for a fixed domain, the probability of error can be reduced by taking multiple samples for inputs. In this paper, we assign randomly selected *real* numbers to input variables and show that when the characteristic polynomials of two Boolean functions give the same value, then the functions are identical with probability 1. It can be shown that when the inputs are sampled from the real domain [0,1], and are interpreted as probabilities of logic 1, then the corresponding value of the characteristic polynomial gives the probability of output logic 1 for the Boolean function.

CHARACTERISTIC POLYNOMIALS

Consider Boolean functions of n variables $\vec{x} = (x_1, \dots, x_n)$. Boolean functions f and g are identical ($f \equiv g$) if and only if for all $\vec{x} \in \{0, 1\}^n$ $f(\vec{x}) = g(\vec{x})$. In the *sum of products* (SOP) representation of the function, we replace each Boolean variable x_i by a real variable X_i , \bar{x}_i by $1 - X_i$, AND operation by product, and OR by summation, and thus obtain a real valued polynomial of n variables. For a Boolean function $f(\vec{x}) = f(x_1, \dots, x_n)$, the corresponding polynomial $F(\vec{X}) = F(X_1, \dots, X_n)$ is unique and we call it the *characteristic polynomial* of the Boolean function. If $g \equiv f$ then the two Boolean functions f and g have the same truth table, same SOP form, and hence the same characteristic polynomial. We denote this transformation from a Boolean function f to its characteristic polynomial F as $F = \tau(f)$.

In general, for any finite field, there is a unique embedding of Boolean functions into a polynomial ring over the field such that they have the same value when all variables take values 0 or 1. A special case follows.

Proposition 1. Two Boolean functions f and g are identical $f \equiv g$ if and only if their characteristic polynomials are identical: $\tau(f) \equiv \tau(g)$. \square

In general, evaluation of F is hard. We propose a greedy method for evaluation of the characteristic polynomials without explicitly constructing them. Given a

Boolean function f , its *Shannon expansion* is:

$$f(\vec{x}) = (x_1 \wedge f_{x_1=1}(\vec{x})) \vee (\bar{x}_1 \wedge f_{x_1=0}(\vec{x})) \quad (1)$$

where $f_{x_1=1}(\vec{x})$ is obtained from $f(\vec{x})$ by assigning $x_1 = 1$ and $f_{x_1=0}(\vec{x})$ by assigning $x_1 = 0$. The characteristic polynomial is:

$$\begin{aligned} F(\vec{X}) &= \tau(f)(\vec{X}) \\ &= X_1 \cdot F_1(X_2, \dots, X_n) + (1 - X_1) \cdot F_0(X_2, \dots, X_n) \end{aligned} \quad (2)$$

where F_1 is the characteristic polynomial of $f_{x_1=1}(\vec{x})$ and F_0 is the characteristic polynomial of $f_{x_1=0}(\vec{x})$. For a constant real vector \vec{X}^* ,

$$F(\vec{X}^*) = X_1^* \cdot F_1(X_2^*, \dots, X_n^*) + (1 - X_1^*) \cdot F_0(X_2^*, \dots, X_n^*) \quad (3)$$

Using (1), (2) and (3), the evaluation of the characteristic polynomial F of f is reduced to the evaluations of the characteristic polynomials of $f_{x_1=1}$ and $f_{x_1=0}$. We then evaluate the two polynomials of $n - 1$ variables, and continue recursively until we have one variable left. It is often necessary to deal with logic networks described as interconnection of Boolean gates. The Shannon expansion method, discussed here, can be applied to such networks also. A good heuristic is to expand with respect to the variables that fanout and then reconverge. Also, in large circuits, partitioning may be necessary. Partitioning into *supergates*, as applied to signal probability calculation, is applicable to the calculation of the characteristic polynomial [4]. Other methods, as discussed by Jain *et al* [2] and those based on binary decision diagrams [1], can also be used.

LOGIC VERIFICATION

Given two Boolean function $f(\vec{x})$ and $g(\vec{x})$, we want to verify if $f \equiv g$. From Proposition 1, this is the case if and only if their characteristic polynomials are identical: $\tau(f) \equiv \tau(g)$. For a constant real vector \vec{X}^* , if $\tau(f)(\vec{X}^*) \neq \tau(g)(\vec{X}^*)$ then definitely the two polynomials are different and consequently $f \neq g$. However, if $\tau(f)(\vec{X}^*) = \tau(g)(\vec{X}^*)$ then the two polynomials (and hence the two given Boolean functions) may or may not be identical. We will show that it is "very likely" that they are identical if we sample uniformly at random.

Algorithm Verification. *Inputs:* two Boolean functions f and g of n variables; *Output:* whether they are identical.
begin

find a compact subset $D \subseteq R^n$;
 sample uniformly at random from D *and obtain*
 $\vec{X}^* \in D$;
 if ($eval(f, \vec{X}^*) \neq eval(g, \vec{X}^*)$)
 then return ‘ $f \neq g$ ’;
 else return ‘ $f \equiv g$ ’;
end

Fig. 1. Verification algorithm using characteristic polynomials.

Schwartz [3] first studied probabilistic algorithms for verification of polynomial identities with applications to elimination theory and elementary plane geometry.

Proposition 2. Suppose that D is a compact set in R^n with a Lebesgue measure μ and $\mu(D) = 1$. Given a polynomial $F(\vec{X})$ of n variables that are not identically zero, the algebraic variety of F is $V = \{\vec{X} : F(\vec{X}) = 0\}$. Then $\mu(V) = 0$. \square

Corollary. Suppose that D is a compact set in R^n with a Lebesgue measure μ and $\mu(D) = 1$. Given two polynomials $F(\vec{X})$ and $G(\vec{X})$ of n variables, if $F \neq G$ then they have the same value on a subset of D of measure zero. \square

This Corollary has an interesting implication. We want to determine whether two Boolean functions f and g are identical. Suppose that we can sample uniformly at random (according to the Lebesgue measure) in D and obtain $\vec{X}^* \in D$. We compute $\tau(f)(\vec{X}^*)$ and $\tau(g)(\vec{X}^*)$. If they are different then definitely $f \neq g$. Otherwise, we claim that they are identical. The only case our claim is incorrect is that when $f \neq g$ and the sample \vec{X}^* is in the algebraic variety of $\tau(f) - \tau(g)$, which is of measure zero. Therefore, the probability that we make an incorrect claim is zero. Figure 1 gives a verification algorithm.

Proposition 3. The probability that the algorithm of Fig. 1 returns an incorrect answer is zero. \square

For an easy implementation, we can take an n -cylinder for D : $-\infty < a_i < b_i < +\infty, i = 1, \dots, n$, or a unit n -cube where $a_i = 0$ and $b_i = 1$. To sample uniformly at random from an n -cylinder, we can just sample uniformly at random from each interval $[a_i, b_i]$ independently for $X_i, i = 1, \dots, n$, and obtain a sample \vec{X}^* .

Example. Consider the functions f and g shown in Figure 2. The function f is a logic AND function of variables a, b and c . Its characteristic polynomial is $F(A, B, C) = ABC$. The function g is a multiplexer function with characteristic polynomial, $G(A, B, C) = AB + (1-B)C$. In the latter case, the polynomial is obtained by Shannon expansion as explained in the previous section. It is advantageous to expand about the fanout variables (input variable b in these example circuits.)

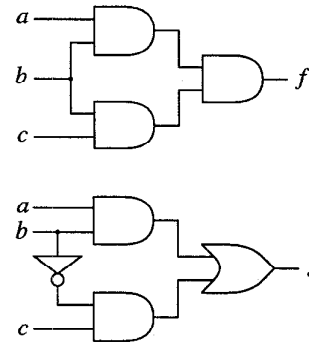


Fig. 2. Circuits used in Example.

Consider a random sample of real numbers from $[-1, 1]$: $A^* = 0.75, B^* = 0.30$ and $C^* = -0.65$. We get, $F(A^*, B^*, C^*) = -0.4625$ and $G(A^*, B^*, C^*) = -0.23$. Although we have not checked all cases, it is unlikely that any two or more of the 2^8 Boolean functions of three variables will have the same value for the characteristic polynomial at this point. For inputs from the integer set $[0, 1]$, the functions f and g will appear identical with probability $5/8 = 0.625$. For the increased range $[-1, 0, 1]$, the error probability becomes $10/27 = 0.370$.

CONCLUSION

The strength of the present proposal stems from the fact that in the real number domain, we take just one sample to gain high confidence. This is because, any finite domain contains infinitely many real numbers. This is not true with the integer domain where a finite domain will only have a countably finite number of integers. On the negative side, the evaluation of a real-valued function is sensitive to round-off errors. Such considerations, though not included here, are to be addressed in the future research. Other aspects of the characteristic polynomial, not discussed here, are its probability interpretation and application to logic testing.

REFERENCES

- [1] R.E. Bryant, "Graph-Based Algorithms for Boolean Function Manipulation," *IEEE Trans. Comput.*, Vol. C-35, pp. 677-691, August 1986.
- [2] J. Jain, J. Bitner, D.S. Fussell, and J.A. Abraham, "Probabilistic Verification of Boolean Functions," *Formal Methods in System Design*, Vol. 1, pp. 63-117, 1992.
- [3] J.T. Schwartz, "Fast Probabilistic Algorithms for Verification of Polynomial Identities," *Jour. ACM*, Vol. 27(4), pp. 701-717, October 1980.
- [4] S.C. Seth and V.D. Agrawal, "A New Model for Computation of Probabilistic Testability in Combinational Circuits," *Integration, the VLSI Journal*, Vol. 7, pp. 49-75, 1989.