Journal of The Institution of Engineers, Singapore
Vol.35, No.1 February 1995

ON THE BINARY SEQUENCES WITH INDISTINGUISHABLE SIGNATURE FOR A GIVEN ERROR MULTIPLICITY IN ELECTRONIC TESTING

S. Demidenko[1], A. Ivanyukovich[2], L. Makhist[3] and V. Piuri[4]

ABSTRACT

Distinct binary sequences ($2^m - 1$ bits long) may be compressed by an m-bit signature register into the same signature value, when a given error multiplicity is considered. Analytical expressions to compute the number of distinct sequences collapsed into the same signature are presented, by exploiting the properties of the binary Hamming code theory and of the binomial coefficients.

INTRODUCTION

With the recent progress of VLSI technology, it is possible to fabricate thousands of gates and interconnections into a single chip. The advantages of VLSI are reduced system cost, higher performance and greater reliability. However, these advantages would be lost unless VLSI chips can be tested effectively and economically. For this reason testing is playing at present extremely important role in VLSI design and manufacturing processes. Over a couple of decades many test approaches have been proposed. Signature analysis is one of the most well-known and effective among them.

Signature analysis since its introduction in 1977 by Hewlett-Packard (Frohwerk,1977) is widely used both in external tester environment and in the Built-In-Self-Test environment reducing the volume (compressing) of the diagnostic data (Bardell et al., 1987). The compression is achieved by means of an m-bit linear feedback shift register (signature register), whose structure is determined by the adopted primitive irreducible polynomial of degree m ($m=1,2,3,...$) (Williams, 1986; Bardell et al., 1987).

The polynomial division algorithm over $GF(2)$ is the basic mathematic tool to describe the signature compression. For an n-bits dividend (where the length n of the sequence being compressed is usually greater than m), an $(n-m)$-bits quotient and an m-bits reminder (i.e., the signature) are obtained. The actual n-bit input sequence of the signature register and the reference one (related to the fault-free operation of the circuit under test) are indirectly compared by observing the possible matching between their signatures: the actual and the reference input sequences are assumed equal if their signature are identical.

It is worth to note that the same signature will be generated for 2^{n-m} distinct quotients; the reference sequence is thus associated to several (namely, $2^{n-m} - 1$) n-bit binary sequences. These $2^{n-m} - 1$ binary sequences – related to erroneous behaviors of the circuit under test in the presence of faults - are undetectable since they cannot be distinguished from the reference sequence.

Let us consider the error sequence defined as the *modulo-2* bit-wise addition of the actual binary sequence (in the presence of errors) and the reference one (Bardell et al., 1987). The weight of an error sequence may then be defined as the Hamming weight of the binary sequence itself (i.e., the number of non-zero components (Blahut, 1983)).

It is well-known that signature compression has the ability to detect all single-bit errors for any n value, and all double-bit errors for $n \leq 2^m - 1$ (Bardell et al., 1987; Smith, 1980; Yarmolik et al., 1989). Therefore the $2^{n-m} - 1$ signature indistinguishable error sequences associated with the given reference one have weight greater than *2*.

A detailed knowledge of the relationship between the error multiplicity (i.e., the weight of the error sequence) and the number of undetectable erroneous binary sequences collapsed onto the reference one is important:

- to analyze the signature compression effectiveness (Bardell et al., 1987; Yarmolik, 1990),
- to locate the erroneous bits within the circuit under test by using information derived from the error signature (Chan et al., 1990; Demidenko et al., 1993),
- to develop and investigate effective methods for data compression (Robinson et al., 1988), and for other applications.

Some partial results concerning these tasks (e.g., recurrent-type expressions, formulae for low-

[1] Lecturer, Singapore Polytechnic, Electronics and Communication Engineering Department, 500 Dover Road, Singapore 0513.
[2] Researcher, Academy of Sciences of Belarus, Institute of Engineering Cybernetics, Brest Branch, 34 Kuybishev Street, Brest 224000, Belarus, CIS.
[3] Researcher, Academy of Sciences of Belarus, Institute of Engineering Cybernetics, Brest Branch, 34 Kuybishev Street, Brest 224000, Belarus, CIS.
[4] Professor, Politecnico di Milano, Department of Electronics and Information, Piazza Leonardo da Vinci 32, 20133 Milano, Italy.

multiplicity error cases, approximate solutions, and so on) were obtained (Bardell et al.; Yarmolik,1990; Chan et al.,1990; Demidenko et al.,1993; Robinson et al., 1988). In this paper, we present the analytical method to derive the general solution for the case $n = 2^m - 1$.

EVALUATION OF THE NUMBER OF INDISTINGUISHABLE SEQUENCES

Signature compression is often described by using terms and methodology of the well-established theory of binary cyclic codes (Bardell et al., 1987; Blahut, 1983; Rao et al., 1989). Let us consider the binary cyclic code of length $n = 2^m - 1$, for which the characteristic polynomial is the minimal polynomial over *GF(2)* for some primitive element *GF*(2^m). It has been proved that such a code is equivalent to the binary Hamming code of length *n* (Blahut, 1983; Lidl et al., 1983).

Therefore, in the presence of errors having multiplicity i ($i = 0, 1, 2, \ldots, 2^m - 1$), the number of undetectable errors in a ($2^m - 1$)-bit binary sequence (i.e., the number of error sequences having weight i) is equal to the number of code words with weight i in the binary Hamming code of length $2^m - 1$. This number is given by the following theorem.

Theorem 1.

The number V_i of code words with weight i in the binary Hamming code of length $2^m - 1$ is:

$$V_i = 2^{-m}\left[\binom{2^m-1}{i} + (-1)^{\left\lceil \frac{i}{2} \right\rceil}\binom{2^{m-1}-1}{\left\lfloor \frac{i}{2} \right\rfloor}\left(2^m-1\right)\right],$$

$$m = 1, 2\ 3, \ldots,\ i = 0, 1, 2, \ldots, 2^m{-}1 \qquad (1)$$

where $\lfloor t \rfloor$ and $\lceil t \rceil$ are the floor and the ceiling functions, respectively.

Proof.

It has been shown (Lidl et al., 1983) that the weight enumerator for the binary Hamming code, having length $n = 2^m - 1$ and dimension *(n-m)* over *GF(2)*, is given by:

$$V(z) = 2^{-m}\left[(1+z)^{2^m-1} + \left(2^m-1\right)\right.$$

$$\left.(1-z)^{2^{m-1}}(1+z)^{2^{m-1}-1}\right]$$

By rearranging the components of this expression, we obtain:

$$V(z) = 2^{-m}\left[(1+z)^{2^m-1} + \left(2^m-1\right)\left(1-z^2\right)^{2^{m-1}-1}(1-z)\right]$$

By applying the binomial decomposition (Gellert et al., 1989) to $(1+z)^{2^{m-1}-1}$ and to $(1-z^2)^{2^{m-1}-1}$ it is:

$$V(z) = 2^{-m}\left\{\sum_{i=1}^{2^m-1}\binom{2^m-1}{i}z^i + \left(2^m-1\right)\left[\sum_{j=1}^{2^{m-1}-1}(-1)^j\right.\right.$$

$$\left.\left.\binom{2^{m-1}-1}{j}z^{2j} + \sum_{k=1}^{2^{m-1}-1}(-1)^{k+1}\binom{2^{m-1}-1}{k}z^{2k+1}\right]\right\}$$

By grouping the homogeneous components, it is:

$$V(z) = 2^{-m}\left[\sum_{i=1}^{2^m-1}\binom{2^m-1}{i} + (-1)^{\left\lceil \frac{i}{2} \right\rceil}\binom{2^{m-1}-1}{\left\lfloor \frac{i}{2} \right\rfloor}\left(2^m-1\right)\right]$$

Since $V(z) = \sum_{i=1}^{2^m-1} V_i z_i$, where V_i is the number of code words with weight i in the binary Hamming code (Blahut, 1983), we finally obtain by comparing the above two expressions:

$$V_i = 2^{-m}\left[\binom{2^m-1}{i} + (-1)^{\left\lceil \frac{i}{2} \right\rceil}\binom{2^{m-1}-1}{\left\lfloor \frac{i}{2} \right\rfloor}\left(2^m-1\right)\right]$$

■

Remark 1.

The expression (1) can be rewritten in a simpler form, for odd and even values of variable i.

$$V_{2k} = 2^{-m}\left[\binom{2^m-1}{2k} + (-1)^k\binom{2^{m-1}-1}{k}\left(2^m-1\right)\right],$$

$$i = 2k,\ k = 0, 1, 2, \ldots, 2^{m-1}{-}1\,, \qquad (2)$$

$$V_{2k+1} = 2^{-m}\left[\binom{2^m-1}{2k+1} + (-1)^{k+1}\binom{2^{m-1}-1}{k}\left(2^m-1\right)\right],$$

$$i = 2k{+}1,\ k = 0, 1, 2, \ldots, 2^{m-1}{-}1\,, \qquad (3)$$

Some characteristics of V_i are defined by the following corollaries: they are useful to simplify the computation of V_i for all possible values of i.

Corollary 1.

$$V_{2k+1} = 2^{-m}\binom{2^m}{2k+1} - V_{2k},$$

$$k = 0, 1, 2, \ldots, 2^{m-1}{-}1,\ V_0 = 1 \qquad (4)$$

Proof.

Let us consider the expressions given in Remark 1 for V_{2k} and V_{2k+1}. Pascal's triangular equation for the binomial coefficients (Gellert et al., 1989) states that $\binom{a}{b} + \binom{a}{b+1} = \binom{a+1}{b+1}$.

By summing V_{2k} and V_{2k+1} and by applying the Pascal's triangular equation:

$$V_{2k} + V_{2k+1} = 2^{-m}\left[\binom{2^m - 1}{2k} + (-1)^k \binom{2^{m-1} - 1}{k}(2^m - 1)\right.$$

$$\left. + \binom{2^m - 1}{2k+1} + (-1)^{k+1}\binom{2^{m-1} - 1}{k}(2^m - 1)\right]$$

$$= 2^{-m}\left[\binom{2^m - 1}{2k} + \binom{2^m - 1}{2k+1}\right] = 2^{-m}\binom{2^m}{2k+1}$$

■

Corollary 2.

$$V_{2k} = \frac{2^{m-1} - k}{k} V_{2k-1}, \quad k = 1, 2, 3, \ldots, 2^{m-1}-1 \qquad (5)$$

Proof.

By applying the binomial coefficient property $\binom{y}{x} = \binom{y}{x-1}\frac{y-x+1}{x}$ to V_{2k}:

$$V_{2k} = 2^{-m}\left[\binom{2^m - 1}{2k-1}\frac{2^m - 2k}{2k} + (-1)^{(k-1)+1}\binom{2^{m-1} - 1}{k-1}\right.$$

$$\left.\frac{2^{m-1} - k}{k}(2^m - 1)\right]$$

$$= \frac{2^m - 2k}{2k}\left\{2^{-m}\left[\binom{2^m - 1}{2(k-1)+1} + (-1)^{(k-1)+1}\right.\right.$$

$$\left.\left.\binom{2^{m-1} - 1}{k-1}(2^m - 1)\right]\right\}$$

$$= \frac{2^m - 2k}{2^k} V_{2k-1}$$

■

Corollary 3 – Symmetry property.

$$V_i = V_{2^m - i - 1}, \quad i = 0, 1, 2, \ldots, 2^m-1 \qquad (6)$$

Proof.

By applying the binomial coefficient property $\binom{y}{x} = \binom{y}{y-x}$ to expression Eqn. (1) and by taking into account that $(-1)^{\left|\frac{i}{2}\right|} = (-1)^{2^{m-1}\left|\frac{i}{2}\right|}$, we obtain:

$$V_i = 2^{-m}\left[\binom{2^m - 1}{2^m - i - 1} + (-1)^{\left\lceil\frac{i}{2}\right\rceil}\binom{2^{m-1} - 1}{2^{m-1} - 1 - \left\lfloor\frac{i}{2}\right\rfloor}(2^m - 1)\right]$$

$$2^{-m}\left[\binom{2^m - 1}{2^m - i - 1} + (-1)^{2^{m-1} - \left\lceil\frac{i}{2}\right\rceil}\binom{2^{m-1} - 1}{2^{m-1} - 1 - \left\lfloor\frac{i}{2}\right\rfloor}(2^m - 1)\right]$$

Since $2^{m-1} - 1 - \left\lfloor\frac{i}{2}\right\rfloor = \left\lfloor\frac{2^m - i - 1}{2}\right\rfloor$ and $2^{m-1} - \left\lceil\frac{i}{2}\right\rceil = \left\lfloor\frac{2^m - i - 1}{2}\right\rfloor$, the last expression for V_i can be rewritten in the following form:

$$V_i = 2^{-m}\left[\binom{2^m - 1}{2^m - i - 1} + (-1)^{\left\lceil\frac{2^m - 1 - i}{2}\right\rceil}\right.$$

$$\left.\binom{2^{m-1} - 1}{\left\lfloor\frac{2^m - i - 1}{2}\right\rfloor}(2^2 - 1)\right]$$

that is equal to $V_{2^{m-i-1}}$.

■

CONCLUSION

Analytical expressions Eqns. (1–3) have been derived to compute, for a given error multiplicity, the number of erroneous binary sequences (having length n = 2^m–1) which are undetectable by the *m*-bit signature register compression. The corollary expressions Eqns. (4–6) show some properties of V_i that can be used to simplify such computation. Our results complete and generalize the expressions presented in several earlier papers on the subject (e.g., (Bardell et al., 1987; Yarmolik et al., 1989; Yarmolik, 1990; Chan et al., 1990; Demidenko et al., 1993; Robinson et al., 1988)).

These results can be applied for error localization by using information derived from error sequence signature, in the area of data compression techniques, and for testable design. For example, in the case of multiple-bit error localization in the sequence being compressed by using the superposition approach defined in (Chan et al., 1990; Demidenko et al., 1993), the above expressions give the number of sets of partial signatures (corresponding to single-bit error occurrences) into which the actual signature must be partitioned.

REFERENCES

Bardell, P.H, McAnney, W.H. and Savir:, J. (1987). Built-In Test for VLSI: Pseudorandom Techniques, John Wiley & Sons, New York.

Blahut, R. (1983). Theory and Practice of Error Control Codes, Addison-Wesley, Reading, MA.

Chan, J.C. and Womak, B.F. (1990). A Study of Faulty Signature for Diagnostics, IEEE International Symposium on Circuits and Systems, New Orleans, 2701-2704.

Demidenko, S., Piuri, V. and Ivanyukovich, A. (1993). Error Localization in Test Outputs: a Generalized Analysis of Signature Compression, IEEE Second Asian Test Symposium, Beijing, P.R. of China, 317-322.

Frohwerk, R.A. (1977). Signature Analysis: A New Digital Field Services Method, Hewlett-Packard Journal, May, 2-8.

Gellert, W., Gottwald, S., Hellwich, M., Kastner, H. and Kustner, H. (Editors) (1989). The VNR Concise Encyclopedia of Mathematics, Van Nostrand, New York.

Lidl, R. and Niederreiter, H. (1983). Finite Fields, Addison Wesley, Reading, MA

Rao, T.R.N. and Fujiwara, E. (1989). Error-Control Coding for Computer Systems, Prentice Hall, Englewood Cliffs.

Robinson, J.P. and Saxena:, N.R. (1988). Simultaneous Signature and Syndrome Compression, IEEE Transactions on CAD, 7:7, 584-589.

Smith, I.F. (1980). Measures of Effectiveness of Fault Signature Analysis, IEEE Transaction on Computers, C-29:6, 510-514.

Williams, T.W. (1986). VLSI-Testing, North-Holland, Amsterdam.

Yarmolik, V.N. and Demidenko, S.N. (1989). Generation and Application of Pseudorandom Sequences for Random Testing, John Wiley & Sons, Chichester.

Yarmolik, V.N. (1990). Fault Diagnosis of Digital Circuits, John Wiley & Sons, Chichester.