[2] V. D. Agrawal, S. C. Seth, and C. C. Chuang, "Probabilistically guided test generation," in *Proc. Int. Symp. Circuit Syst. (ISCAS)*, Kyoto, Japan, June 1985, pp. 687-690.

[3] S. C. Seth, L. Pan, and V. D. Agrawal, "PREDICT—Probabilistic estimation of digital circuit testability," in *Fault-Tolerant Comput. Symp. (FTCS-15) Dig. Papers*, June 1985, pp. 220-225, also *FTCS-16 Dig.*, pp. 318-323.

[4] F. Brglez, "On testability analysis of combinational networks," in *Proc. Int. Symp. Circuit Syst.*, May 1984, pp. 221-225.

[5] S. K. Jain and V. D. Agrawal, "Statistical fault analysis," *IEEE Design Test Comput.*, vol. 2, pp. 38-44, Feb. 1985.

[6] V. D. Agrawal, H. Farhat, and S. Seth, "Test generation by fault sampling," in *Proc. Int. Conf. Comput. Design (ICCD-88)*, Rye Brook, NY, Oct. 1988, pp. 58-61.

[7] S. C. Seth, V. D. Agrawal, and H. Farhat, "A theory of testability with applications to fault coverage analysis," in *Proc. 1st Euro. Test Conf.*, Paris, France, Apr. 1989, pp. 139-143.

[8] A. Papoulis, *Probability, Random Variables, and Stochastic Processes.* New York: McGraw-Hill, 1965, sect. 4.4.

[9] M. H. Schulz and E. Auth, "Advanced automatic test pattern generation and redundancy identification techniques," in *18th Int. Symp. Fault-Tolerant Comput. (FTCS-18) Dig. Papers*, Tokyo, Japan, June 1988, pp. 30-35.

Aliasing Probability for Multiple Input Signature Analyzer

DHIRAJ K. PRADHAN, SANDEEP K. GUPTA, AND MARK G. KARPOVSKY

Abstract—**Formulation of closed form expressions for computing MISR aliasing probability exactly had remained an unsolved problem. This paper presents single and multiple MISR aliasing probability expressions for arbitrary test lengths. A framework, based on algebraic codes, is developed for the analysis and synthesis of MISR-based test response compressors for BIST. This framework is used to develop closed form expressions for aliasing probability of MISR for arbitrary test length (so far only bounds have been formulated). A new error model, based on q-ary symmetric channel, is proposed using more realistic assumptions. Results are presented that provide the weight distributions for q-ary codes ($q = 2^m$, where the circuit under test has m outputs). These results are used to compute the aliasing probability for the MISR compression technique for *arbitrary* test lengths. This result is extended to compression using two different MISR's. It is shown that significant improvements can be obtained by using two signature analyzers instead of one. This paper makes a contribution to coding theory as well. It provides the weight distribution of a class of codes of arbitrary length. Also formulated is an expression bounding from above the probability of undetected error for these codes. The distance-3 Reed–Solomon codes over $GF(2^m)$ become a special case of our results.**

Index Terms—**Algebraic codes, aliasing probability, BIST, BIT, error model, MISR, Reed–Solomon codes, shift register, weight distribution.**

Manuscript received July 6, 1989; revised December 5, 1989. This work was supported by NSF Grants MIP8902014 and MIP8813748.

D. K. Pradhan and S. K. Gupta are with the Department of Electrical and Computer Engineering, University of Massachusetts, Amherst, MA 01003.

M. G. Karpovsky is with the College of Engineering, Boston University, Boston, MA 02215.

IEEE Log Number 8933881.

I. Introduction

The multiple input signature register compression (MISR) is the primary technique used in signature analysis. The outputs of the circuit under test (CUT) are connected to the inputs of the MISR while the test patterns are applied to the CUT. The final contents of the MISR are compared to that expected for a fault-free circuit to determine whether the CUT is faulty.

Deriving *closed* form expressions for computing MISR aliasing probability exactly for *arbitrary* test length had remained an unsolved problem. The chief contribution of this paper is to provide precisely such an expression. The results obtained from earlier investigations for the single input LFSR [2] are extended to multiple input MISR using the relationship between coding theory and shift-register theory. Specifically, we formulate expressions for estimating the aliasing probability for MISR using a more realistic error model by relating the analysis of an MISR to the analysis of q-ary codes where $q = 2^m$ for an m-output CUT. Also presented are aliasing probability expressions for multiple MISR's.

Also, this paper makes two new contributions to coding theory. First, a counting technique is developed for computing the weight distribution of a certain class of codes of arbitrary length which are not necessarily maximum distance separable (MDS) [8]. (Weight distributions for MDS codes are known.) Also, the probability of undetected error for this class of codes is bounded from above. (Certain known results for MDS codes [18] become special cases of our results.)

In summary, proposed here is a new approach for estimating aliasing probability for MISR compression. In the paper, we present aliasing probability expressions for m output circuits for any arbitrary test sequence of length n. We also present a multiple-MISR compression technique which reduces aliasing.

The paper is organized into three major sections. Section II presents the basic framework of the analysis of MISR techniques using coding theory. The analysis of MISR techniques is then presented in Section III. In this section, both single and multiple MISR schemes are analyzed. Finally, we conclude in Section IV.

II. Coding Theory Framework

Below we present a coding theory framework [10] for analysis and synthesis of MISR compressors. It is shown that for an m output circuit, the design and analysis of MISR-based compression techniques can be formulated using algebraic coding theory of q-ary error correcting codes ($q = 2^m$).

A. Algebraic Codes

Let c be an n-tuple $(c_{n-1}c_{n-2}\cdots c_0)$ where $c_i \in GF(q)$. Let $c(x) = c_{n-1}x^{n-1} + \cdots + c_1x + c_0$ be the polynomial representation of the n-tuple.

In the following discussion, the vector and polynomial representations shall be used interchangeably. All polynomial representations and operations will be assumed to be over $GF(q)$ where $q = 2^m$. Thus, all additions and multiplications in this section will be assumed to be over $GF(2^m)$. In this field $+\delta = -\delta$; therefore, the terms of the polynomials can be represented as only positive terms.

Definition 1: The generator polynomial $g(x)$ of a code C is that polynomial $g(x)$ which divides every codeword polynomial in C. The degree of $g(x)$ is equal to $n - k$ where n is the length of the code and k is the number of information symbols.

Two key observations should be made here. First, when $g(x)$ divides $x^n - 1$, only then does the code become a cyclic code of length n. On the other hand, when $g(x)$ does not divide $x^n - 1$, then the code is not cyclic. The results derived here are applicable to cyclic and noncyclic codes.

In the following, the Galois field elements $\mathbf{0} = (0, 0)$ and $\mathbf{1} = (0, 1)$ are denoted by boldface to distinguish from the binary 0, 1.

Example 1: Consider a cyclic (3, 2) Reed–Solomon code over

0018-9340/90/0400-0586$01.00 © 1990 IEEE

$GF(2^2)$. The following is a list of codewords in the code C.

$$C = \begin{Bmatrix} 000 & 1\alpha 0 & \beta 0 \alpha & \beta \alpha 1 \\ 01\alpha & \alpha\beta 0 & 10\beta & 111 \\ 0\alpha\beta & \beta 10 & 1\beta\alpha & \alpha\alpha\alpha \\ 0\beta 1 & \alpha 01 & \alpha 1 \beta & \beta\beta\beta \end{Bmatrix}$$

Here $\mathbf{0}$, $\mathbf{1}$, α, and β are elements of $GF(2^2)$ where $\mathbf{0} = (0, 0)$, $\mathbf{1} = (0, 1)$, $\alpha = (1, 0)$, and $\beta = (1, 1)$. Here α is the primitive element [8] and $\beta = \alpha^2$. It can be seen that the generator polynomial for this code is $x+\alpha$ which divides all the 16 codeword polynomials. For example, the codeword $\mathbf{1}\beta\alpha = \mathbf{1}x^2+\beta x+\alpha$ is divisible by $(x+\alpha)$ as $\mathbf{1}x^2+\beta x+\alpha = (x+\alpha)(x+\mathbf{1})$. The above codewords can also be expressed in binary form as

$$\begin{Bmatrix} (0,0)(0,0)(0,0) & (0,1)(1,0)(0,0) & (1,1)(0,0)(1,0) & (1,1)(1,0)(0,1) \\ (0,0)(0,1)(1,0) & (1,0)(1,1)(0,0) & (0,1)(0,0)(1,1) & (0,1)(0,1)(0,1) \\ (0,0)(1,0)(1,1) & (1,1)(0,1)(0,0) & (0,1)(1,1)(1,0) & (1,0)(1,0)(1,0) \\ (0,0)(1,1)(0,1) & (1,0)(0,0)(0,1) & (1,0)(0,1)(1,1) & (1,1)(1,1)(1,1) \end{Bmatrix}.$$

All the codewords in the code C are multiples of its generator polynomial $g(x)$. This fact is used in detecting errors in the codewords.

Definition 2: The remainder $s(x)$ obtained by dividing a word $r(x)$ by the generator polynomial $g(x)$ is referred to as the *syndrome*, corresponding to $r(x)$ in the code generated by $g(x)$.

That is, syndrome $s(x)$ of $r(x)$ is given by

$$r(x) = a(x)g(x) + s(x) \tag{1}$$

where $s(x)$ is the remainder of the polynomial division and has a degree of $n-k-1$ or less.

In the following, we illustrate the use of MISR in computing $s(x)$. First, it may be noted that an MISR can be viewed as a divider. Given a sequence of parallel input to the MISR, the final state of the MISR given the initial state $\mathbf{0}$ is the remainder obtained by dividing the input sequence, interpreted as a polynomial, with $(x+\alpha)$, where α is an element in $GF(2^m)$ and m is the number of inputs to MISR. The element α is determined from the feedback polynomial defining the MISR. In particular, if the feedback polynomial is a primitive polynomial over $GF(2)$ then α is the primitive element over the field $GF(2^m)$ which is defined by the given primitive feedback polynomial. (Every $GF(2^m)$ field is defined by a primitive polynomial of degree m, over $GF(2)$.) In the following, the feedback polynomial representations over $GF(2)$ and $GF(2^m)$ shall be used interchangeably.

Example 2: Consider the MISR shown in Fig. 1. The feedback polynomial here is given as x^2+x+1. If α is a primitive element over $GF(2^2)$ defined by (x^2+x+1), one can see that the final state of the MISR corresponds to the remainder resulting from dividing the input sequence by $(x+\alpha)$. Consider the input sequence $(\alpha\mathbf{1}\beta)$. This in polynomial form is $(\alpha x^2+x+\beta)$. This is a codeword in the RS code in Example 1. Therefore, $\alpha x^2+x+\beta$ must be divisible by $(x+\alpha)$. The following shows that the remainder, as expected, will be equal to $\mathbf{0} = (0, 0)$.

Input		State of MISR	
4-ary	Binary	4-ary	Binary
—	—	$\mathbf{0}$	(0, 0)
α	(1, 0)	α	(1, 0)
$\mathbf{1}$	(0, 1)	α	(1, 0)
β	(1, 1)	$\mathbf{0}$	(0, 0).

On the other hand, let the input sequence be $(\alpha\alpha\beta)$ which is not a codeword in the code in Example 1. Therefore, the final state of the MISR for this input sequence is not equal to $\mathbf{0}$ and is instead equal to the remainder $\mathbf{1} = (0, 1)$ in the binary. This is the result of dividing $\alpha x^2+\alpha x+\beta$ by $x+\alpha$.

Input		State of MISR	
4-ary	Binary	4-ary	Binary
—	—	$\mathbf{0}$	(0, 0)
α	(1, 0)	α	(1, 0)
α	(1, 0)	$\mathbf{1}$	(0, 1)
β	(1, 1)	$\mathbf{1}$	(0, 1).

It may also be noted that the sequence of states of MISR forms the quotients. For example, in dividing $\alpha x^2+\alpha x+\beta$ by $x+\alpha$, one has $\alpha x+\mathbf{1}$ as the quotient and a remainder of $\mathbf{1}$. This is given by α followed by $\mathbf{1}$'s, as shown above.

Lemma 1: Let $R(x)$ and $R^*(x)$ be polynomial representations of two different vectors R and R^* of length n. Then both $R(x)$ and $R^*(x)$ will produce the same syndrome with respect to $g(x)$ if and only if $R(x)+R^*(x)$ is a codeword polynomial in the code C generated by $g(x)$.

Example 3: Given code C shown above generated by $g(x) = x+\alpha$. Consider $R(x) = \beta x^2+\mathbf{1}x+\mathbf{1}$ and $R^*(x) = \mathbf{1}x^2+\mathbf{1}x+\alpha$. Now $R(x)$ and $R^*(x)$ will not produce the same syndrome as $R(x)+R^*(x) = \alpha x^2+\beta \notin C$. On the other hand, $R^{**}(x) = \alpha x^2$ will yield the same syndrome as $R(x)$, as shown in Table I, since the sum $R^{**}(x)+R(x) = \mathbf{1}x^2+\mathbf{1}x+\mathbf{1}$ is a codeword in C.

This is illustrated in Table I. The final register entries marked with *. These represent the remainder after division by $(x+\alpha)$. The final register entries in Table I(a) and I(c) are the same and the entry in Table I(b) is different. In the following, we relate the above observations to MISR and identify the conditions that result in aliasing.

B. MISR Compression

Let N be the circuit under test (CUT) with m outputs. Thus, any output of N can be interpreted as a symbol in $GF(q)$, $q = 2^m$.

Let n be the number of tests applied.

$F = \{f_1, f_2, \cdots, f_h\}$, set of faults considered for the CUT

$T = \{t_{n-1}, t_{n-2}, \cdots, t_1, t_0\}$, set of input vectors applied

$R = \{r_{n-1}, r_{n-2}, \cdots, r_1, r_0\}$ the good circuit response corresponding to the input sequence T, $r_i \in GF(2^m)$

$R^* = \{r^*_{n-1}, r^*_{n-2}, \cdots, r^*_1, r^*_0\}$ the faulty circuit response corresponding to the input sequence T for a fault $f \in F$, $r^*_i \in GF(2^m)$ and where r_i is the response to t_i.

If $t_k \in T$ is a test pattern for a fault $f \in F$, then the response $r^*_k \neq r_k$ when CUT is faulty with fault f.

The symbol by symbol addition of R and R^* over $GF(2^m)$ will be denoted as E, and is referred to as the error vector due to a fault.

Let $R(x)$ and $R^*(x)$ be the polynomial representations of the test responses R and R^*, respectively.

Let $E(x) = R(x)+R^*(x)$ be the polynomial representation of the error vector E. If t_k is test for a fault $f \in F$, then the term $e_k x^k$ must appear in $E(x)$, where $e_k = r_k + r^*_k$.

Let the output response be compressed by using an MISR, with a feedback polynomial $\phi(x)$. First it may be noted that any binary polynomial of degree m can be presented as $x+\alpha$ over $GF(2^m)$.

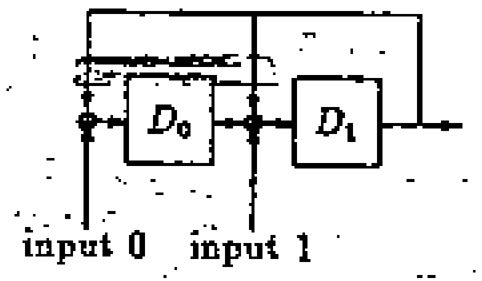

Fig. 1. MISR as the generator of RS code.

TABLE I
THE CONTENTS OF THE SHIFT REGISTER DURING SIGNATURE ANALYSIS
(a) GOOD CIRCUIT RESPONSE. (b) FAULTY CIRCUIT RESPONSE-1.
(c) FAULTY CIRCUIT RESPONSE-2.

Test	$R(x)$	Register Values
		(0, 0)
t_2	β	(1, 1)
t_1	1	(0, 0)
t_0	1	(0, 1)*

(a)

Test	$R^*(x)$	Register Values
		(0, 0)
t_2	1	(0, 1)
t_1	1	(1, 1)
t_0	α	(1, 1)*

(b)

Test	$R^{**}(x)$	Register Values
		(0, 0)
t_2	α	(1, 0)
t_1	0	(1, 1)
t_0	0	(0, 1)*

(c)

BIST	Coding Theory
Output response	Received message
MISR	Syndrome Generator
Signature	Syndrome
Aliasing	Undetected Error
Aliasing Probability	Probability of undetected error

Fig. 2. BIST and coding theory equivalence.

Therefore, the MISR feedback polynomial which is of degree m can be represented as $\phi(x) = x + \alpha$ for some $\alpha \in GF(2^m)$. Thus, the compressed signature $S(x)$ of the response $R(x)$ is given by

$$R(x) = h(x)\phi(x) + S(x)$$

where the polynomials $R(x)$, $h(x)$, and $S(x)$ are also polynomials over $GF(2^m)$. The degree of $S(x)$ is less than the degree of $\phi(x) = x + \alpha$ which is of degree 1. This implies $S(x)$ has to be of degree 0. Thus, $S(x) = \beta$, where $\beta \in GF(2^m)$.

Similarly, the signature of the faulty circuit response is given by

$$R^*(x) = h^*(x)\phi(x) + S^*(x).$$

Aliasing occurs when the faulty response $R^*(x)$ is not equal to good circuit response $R(x)$ but faulty circuit signature $S^*(x)$ is equal to the good circuit signature $S(x)$.

This happens if and only if $E(x) = R(x) + R^*(x)$ is divisible by $\phi(x)$. Consequently $E(x)$ has to be a codeword in the code generated by $g(x) = x + \alpha$. This establishes the relationship between coding theory and MISR signature analysis [2], [4], [10] as illustrated in Figs. 2 and 3.

The following result is a direct consequence of the above relationships.

Theorem 1: An error polynomial $E(x)$ causes aliasing iff $E(x)$ belongs to the code C, generated by the polynomial $\phi(x) = x + \alpha$ where α is the primitive root of the corresponding feedback polynomial over $GF(2)$.

Corollary 1: If the feedback polynomial is $\phi(x) = x + \alpha$ then any error polynomial $E(x)$ that causes aliasing must have α as a root, i.e., $E(\alpha) = 0$.

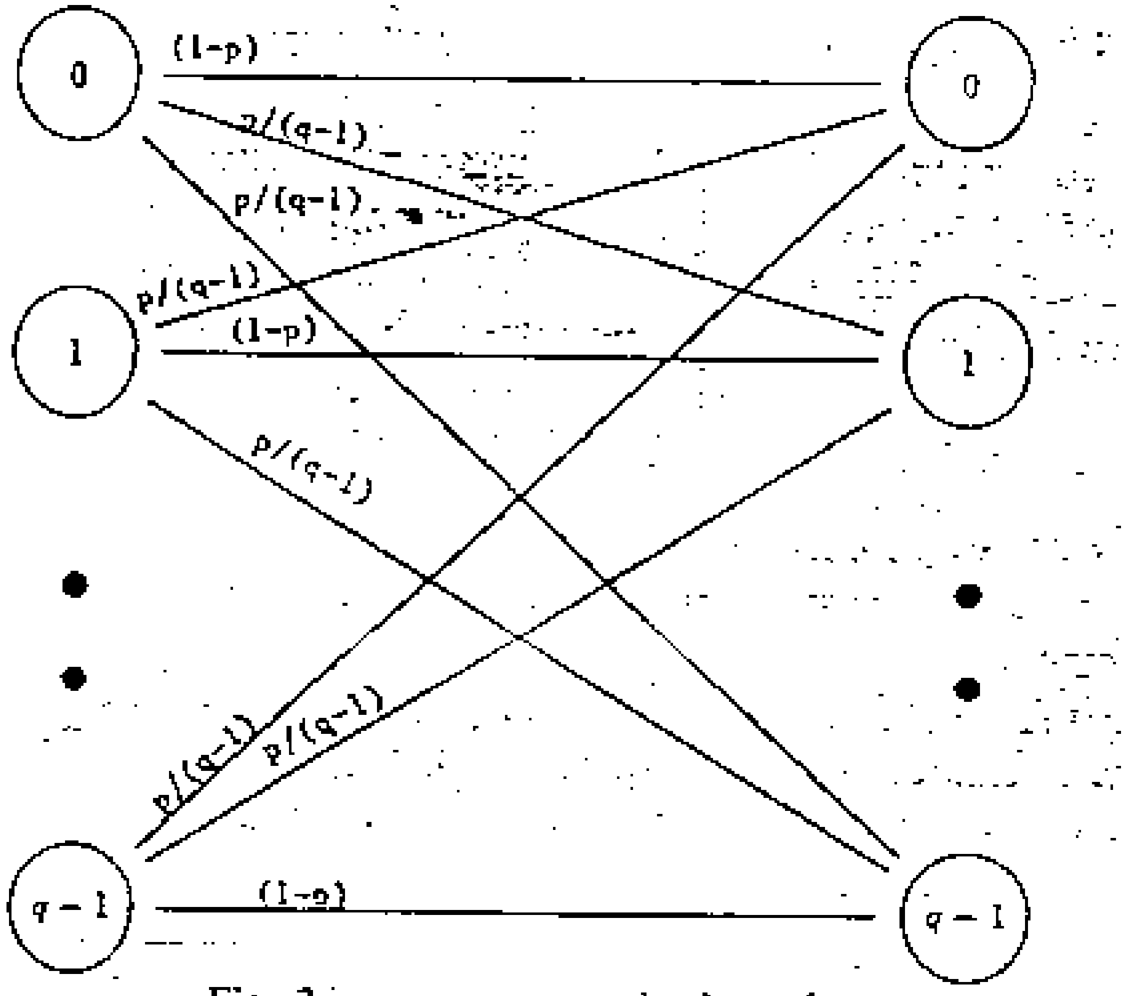

Fig. 3. q-ary symmetric channel.

The following example illustrates the result in Theorem 1.

Example 4: Let us consider a two-output CUT. Let the good circuit response be $r(x) = \beta x^2 + 1x + 1$. The MISR compression for the good circuit will yield a signature $S(x) = (0, 1)$. Now if the output of the CUT is $R^*(x) = 1x^2 + 1x + \alpha$. For the code constructed in Example 1, with $g(x) = \phi(x) = x + \alpha$, as $E(x) = R(x) + R^*(x) \notin C$, the syndrome is $S^*(x) = (1, 1)$. The contents of the MISR for these two sequences are shown in Table I.

III. ALIASING PROBABILITY

Techniques for analysis of aliasing probabilities for single input linear feedback shift registers have been discussed in [2]–[4], [10]–[12]. No exact expression for aliasing probability for MISR's is available that admits arbitrary length test response. In the following, we present the expressions for aliasing probability of an MISR for *any* test length. We also present bounds on aliasing probabilities when using two MISR's for any arbitrary test length $n \leq 2^m - 1$. For the particular case where the MISR's are designed using the generator polynomials of Reed–Solomon codes, then the aliasing probability expressions are presented for $n = 2^m - 1$, for any number of MISR's.

Aliasing probability depends on error distributions. In the following, we propose a new error model for multiple output circuits that is more realistic than the traditional model used previously [13].

A. Error Model for Multiple Output Circuits

The error model used in previous work in aliasing [13] assumes the errors at each output are independent. This model therefore makes the implicit assumption that there is no sharing of logic between the outputs. However, most real world VLSI circuits have considerable sharing of logic between outputs. Therefore, any fault is likely to cause multiple correlated errors. This is precisely the reason we propose to use the q-ary ($q = 2^m$) symmetric channel shown in Fig. 3. Here p corresponds to the probability that for any given test the output is in error. Note that p depends on the test vectors that are being applied to the CUT, e.g., if the tests applied are efficient then p will be high. Here it is assumed that all $(2^m - 1)$ error patterns possible at the m-output circuit are equally likely. However, the errors are considered independent over time sequence (as in the previous models). In other words, errors caused by two consecutive tests are not correlated. But for a particular test the errors at different outputs may be correlated. Hence, the errors in the CUT are modeled as shown in Fig. 3. With this model one can interpret the faulty circuit response as the received sequence corresponding to transmitting good circuit response R over a noisy channel as shown in Fig. 4. Thus, the good circuit response is modified by the errors due to fault in the CUT. The vector R^* corresponds to the faulty circuit response which is compressed by the MISR. The problem of estimating aliasing probability is therefore equivalent to determining the probability of undetected error at the receiver with the following interpretation: an error in the received sequence is detected iff the error vector corresponds to a noncodeword in the code generated by $(x - \alpha)$ where α is the root of the MISR feedback polynomial

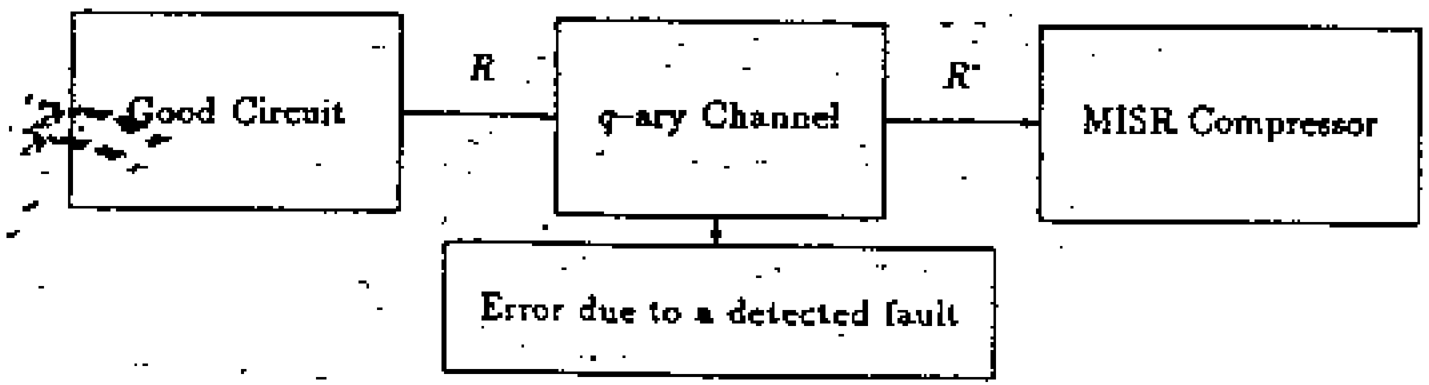

Fig. 4. Errors in CUT modeled as errors in a channel.

(Corollary 1). Thus, the problem of computing aliasing probability is exactly equivalent to the problem of computing probability of errors as described below.

The *weight* of a vector refers to the number of nonzero terms in it. Thus, the weight of $(0\alpha01\beta)$ is 3.

Let $E(l)$ be the number of error patterns of weight l that causes aliasing in a sequence of n tests. Using the above model one has aliasing probability

$$P_{al} = \sum_{l=1}^{n} E(l) \left(\frac{p}{q-1}\right)^{l} (1-p)^{n-l} \qquad (2)$$

where p is the probability that the output vector will be in error when one test pattern is applied to the CUT.

From Theorem 1, one has $E(l) = A(l)$ where $A(l)$ is the number of codewords of weight l in the code generated by $g(x) = \phi(x)$. Thus,

$$P_{al} = \sum_{l=1}^{n} A(l) \left(\frac{p}{q-1}\right)^{l} (1-p)^{n-l}. \qquad (3)$$

Consequently, the aliasing probability in an MISR technique is the same as the probability of undetected error in the corresponding q-ary code generated by $g(x) = x + \alpha$. We now derive aliasing probability expressions for MISR's using the above q-ary symmetric channel error model. (However, if an independent error model is to be used, then one could also use the same framework and use the binary weight distributions instead [5].)

B. Aliasing Probability—Single MISR

In this subsection, we present aliasing probability expression for single MISR. We assume $\phi(x) = x + \alpha$ where α is the primitive element over $GF(2^m)$. First it may be noted that when $\phi(x) = x + \alpha$ this corresponds to the distance 2 maximum distance separable (MDS) code whose weight distribution is known [8] and is given as

$$A(l) = \binom{q-1}{l} \sum_{i=0}^{l-2} (-1)^i \binom{l}{i} (q^{l-1-i} - 1). \qquad (4)$$

(These codes correspond to MDS because for any block length they have a minimum distance of 2 with one check symbol.) Using (4) in (3) one has the aliasing probability P_{al} for a m-bit MISR for any test length n as

$$P_{al} = \sum_{l=1}^{n} \left[\binom{q-1}{l} \sum_{i=0}^{l-2} (-1)^i \binom{l}{i} \cdot (q^{l-1-i} - 1) \right] \left(\frac{p}{q-1}\right)^{l} (1-p)^{n-l}. \qquad (5)$$

In the following, we derive the expressions for aliasing probability for any test sequence length using an alternate formulation. As shall be seen later, the expression obtained is simpler than the one obtained above.

Let $N_1(m, l)$ be the number of error vectors that can cause aliasing given any fixed l positions in which errors occur in a test response of length n. Thus, $N_1(m, l)$ represents error vectors of weight l and length n where the errors are confined to some fixed l positions only. Thus, $E(l) = \binom{n}{l} N_1(m, l)$ represents total number of error vectors of length n and weight l that can cause aliasing.

Lemma 2: $N_1(m, l) = 2^{-m}((2^m - 1)^l + (-1)^l(2^m - 1))$.

Proof: Let $i_1, i_2, \cdots, i_l$ be some l positions in which errors can occur. By definition of $N_1(m, l)$ and Corollary 1 one can see that $N_1(m, l)$ is the number of solutions $(e_1, e_2, \cdots, e_l)$, $(e_i \neq 0)$, for the following linear equation over $GF(2^m)$

$$e_1\alpha^{i_1} + e_2\alpha^{i_2} + \cdots + e_l\alpha^{i_l} = 0, \qquad (i_1 < i_2 < \cdots i_l) \qquad (6)$$

where $\alpha \in GF(2^m)$ is the primitive root of the feedback polynomial.

Now consider (6) rewritten as follows

$$e_1\alpha^{i_1} + e_2\alpha^{i_2} + \cdots + e_{l-1}\alpha^{i_{l-1}} = e_l\alpha^{i_l}. \qquad (7)$$

From (6) and (7) we have the following recursive formula for $N_1(m, l)$

$$N_1(m, l) = (2^m - 1)^{l-1} - N_1(m, l-1). \qquad (8)$$

This is obtained from the following observations. The number of nonzero e_i combinations that satisfy (7) is equal to the number of combinations of e_i's with all nonzero e_i's that result in left-hand side of (7) being nonzero. There are $(2^m - 1)^{l-1}$ possible combinations of nonzero e_i's for the left-hand side of (7). Of these combinations, by definition there are precisely $N_1(m, l-1)$ combinations which make the left-hand side of (7) zero. Thus, there are precisely $(2^m - 1)^{l-1} - N_1(m, l-1)$ combinations of $e_1, e_2, \cdots, e_l$ for which the left-hand side is nonzero and hence e_l must also be nonzero. Solving (8) with the initial condition $N_1(m, 1) = 0$ we have

$$N_1(m, l) = 2^{-m}((2^m - 1)^l + (-1)^l(2^m - 1)). \qquad (9)$$

Lemma 2 is a generalization of the result presented in (4). To show this, we note that for the $[n, n-1, 2]$ Reed–Solomon code with $n = 2^m - 1$ [8]. The weight distribution of this code is given in (4). This can be seen to be a special case of (9) as shown below. From (4), one has

$$\begin{aligned} A(l) &= \binom{n}{l} \sum_{j=0}^{l-2} (-1)^j \binom{l}{j} (2^{m(l-1-j)} - 1) \\ &= \binom{n}{l} (2^m - 1) \sum_{j=0}^{l-2} (-1)^j \binom{l-1}{j} 2^{m(l-2-j)} \\ &= \binom{n}{l} (2^m - 1) 2^{-m}((2^m - 1)^{l-1} - (-1)^{l-1}) \\ &= \binom{n}{l} 2^{-m}((2^m - 1)^l + (-1)^l(2^m - 1)) \\ &= \binom{n}{l} N_1(m, l). \end{aligned} \qquad (10)$$

Theorem 2: For any m-bit MISR with a primitive feedback polynomial and any test length n, $(q = 2^m)$

$$P_{al} = 2^{-m} \left[1 - 2^m(1-p)^n + (2^m - 1)\left(1 - \frac{2^m p}{2^m - 1}\right)^n \right]. \qquad (11)$$

Proof: From (10) we see that $A(l) = \binom{n}{l} N_1(m, l)$ for all n. Using this in (3) one has

$$\begin{aligned} P_{al} &= \sum_{l=1}^{n} \binom{n}{l} \left(\frac{p}{q-1}\right)^l \cdot (1-p)^{n-l} 2^{-m}((2^m - 1)^l + (-1)^l(2^m - 1)), \qquad q = 2^m \\ &= 2^{-m} \left[1 - 2^m(1-p)^n + (2^m - 1)\left(1 - \frac{2^m p}{2^m - 1}\right)^n \right]. \end{aligned}$$

Q.E.D.

TABLE II
ALIASING PROBABILITY FOR SINGLE MISR

p	P_{al}		
	32 Tests	15 Tests	8 Tests
0.01	2.694×10^{-3}	6.401×10^{-4}	1.791×10^{-4}
0.05	3.107×10^{-2}	1.124×10^{-2}	3.791×10^{-3}
0.10	5.353×10^{-2}	2.926×10^{-2}	1.229×10^{-2}
0.20	6.214×10^{-2}	5.295×10^{-2}	3.223×10^{-2}

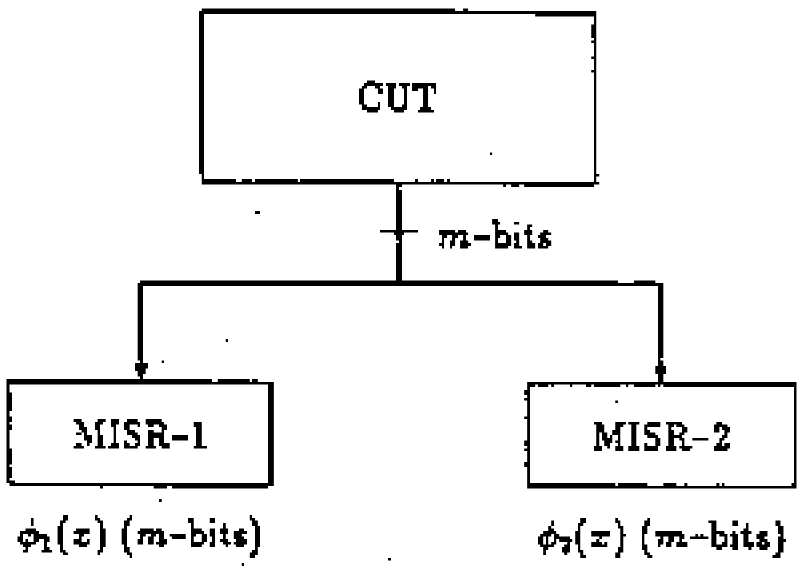

Fig. 5. Using two MISR's for signature analysis.

Corollary 2: $\lim_{m\to\infty, n\to\infty}(P_{al} - 2^{-m}) = 0.$ (12)

Table II shows the aliasing probability for a 4-output ($m = 4$) circuit. It may be observed that finding an optimal number of tests is a two-dimensional optimization problem. For a given fault coverage, an efficient set of tests will attempt to maximize p. However, in general smaller values of p lead to lower aliasing as well as fewer tests lead to lower aliasing. Therefore, one needs to find the combination of p and number of tests that leads to the lowest possible aliasing probability P_{al}. For example, for a given CUT if

Test Set	Test Set Size	p
T_1	32	0.01
T_2	16	0.05
T_3	8	0.20

one may select the test set with 16 tests because it produces the lowest aliasing.

C. Multiple Signatures

Consider the use of two MISR's to obtain two independent signatures concurrently. Below we present the aliasing probabilities for the case of two m-bit MISR's with feedback polynomials $\phi_1(x)$ and $\phi_2(x)(\phi_1(x) \neq \phi_2(x))$ of degree m (Fig. 5). Let $\phi_1(x)$ and $\phi_2(x)$ both be primitive polynomials with roots α and β, respectively. In the following we shall assume the $\beta = \alpha^s$ where $s - 1$ and $2^m - 1$ are mutually prime.

First, it may be noted that for $n = 2^m - 1$, $(x + \alpha)(x + \beta)$ divides $x^n - 1$. However, this is not necessarily true for any $n < 2^m - 1$. Hence, for any α, β, and n the corresponding codes are neither cyclic, nor Reed–Solomon. Also, since α and β are as defined above, the codes are not necessarily MDS. The weight distribution for these codes cannot be obtained as a direct consequence of well-known results about MDS [8]. Consequently the aliasing probability P_{al} in this case is not implicit in the known coding theory work. Coding theory results can be used only when $n = 2^m - 1$ and specific α and β so that one has a MDS code to derive an exact expression for P_{al}. What we formulate below is an upperbound on P_{al} for any $n \leq 2^m - 1$.

Let $N_2(m, l)$ be an upper bound on the number of error vectors with errors in some fixed l positions that can cause aliasing and let $n_2(m, l)$ be the exact number of error vectors that can cause aliasing with errors in some fixed l positions. Thus, $n_2(m, l) \leq N_2(m, l)$. $N_2(m, l)$ is an upper bound on the number of solutions $(e_1, e_2, \cdots, e_l)$, $e_i \neq 0$ for the following system of two linear equations over $GF(2^m)$

$$\begin{aligned} e_1\alpha^{i_1} + e_2\alpha^{i_2} + \cdots + e_l\alpha^{i_l} &= 0 \\ e_1\beta^{i_1} + e_2\beta^{i_2} + \cdots + e_l\beta^{i_l} &= 0 \end{aligned} \tag{13}$$

where $(i_1 < i_2 < \cdots < i_l)$ and α and β are primitive roots for the feedback polynomials of the MISR's ($\alpha^i \neq \alpha^j$; $\beta^i \neq \beta^j (\alpha \neq \beta)$; $i, j \in \{0, 1, \cdots, 2^m - 2\}$).

Lemma 3:

$$N_2(m, l) = ((2^m - 1)^2 + 1)^{-1}((2^m - 1)^l + \Delta) \tag{14}$$

where

$$\Delta = \begin{cases} (-1)^{((l+1)/2)}(2^m - 1), & l \text{ odd;} \\ (-1)^{l/2}(2^m - 1)^2, & l \text{ even.} \end{cases} \tag{15}$$

Proof: One can select $l - 2$ of the coefficients $e_1, e_2, \cdots, e_{l-2}$ arbitrarily. One can rewrite (13) as follows:

$$\begin{aligned} e_1\alpha^{i_1} + e_2\alpha^{i_2} + \cdots + e_{l-2}\alpha^{i_{l-2}} &= e_{l-1}\alpha^{i_{l-1}} + e_l\alpha^{i_l} \\ e_1\beta^{i_1} + e_2\beta^{i_2} + \cdots + e_{l-2}\beta^{i_{l-2}} &= e_{l-1}\beta^{i_{l-1}} + e_l\beta^{i_l}. \end{aligned} \tag{16}$$

This can be done in $(2^m - 1)^{l-2}$ ways. Then e_{l-1} and e_l need to be selected such that they satisfy (16). As we have assumed that $\beta = \alpha^s$ where $s - 1$ and $2^m - 1$ are mutually prime, e_{l-1} and e_l have unique values. This follows from the fact that the matrix $\begin{bmatrix} \alpha^{i_{l-1}} & \alpha^{i_l} \\ \beta^{i_{l-1}} & \beta^{i_l} \end{bmatrix}$ is nonsingular when the above condition is satisfied. By definition one has $n_2(m, l - 2)$ solutions to (13) were $e_{l-1} = e_l = 0$. Let $\delta(l)$ be the number of solutions where either $e_{l-1} = 0$ or $e_l = 0$ but not both. Hence, we have

$$n_2(m, l) = (2^m - 1)^{l-2} - n_2(m, l - 2) - \delta(l).$$

This follows from the observation that $n_2(m, l)$ represents the number of solutions in which all e_i, $1 \leq i \leq l$, are nonzero in (13) and $\delta(l) \geq 0$. Substituting for $n_2(m, l - 2)$ one has

$$n_2(m, l) = (2^m - 1)^{l-2} - (2^m - 1)^{l-4} - (\delta(l) - \delta(l - 2)).$$

Now, $\delta(l - 2) \leq \delta(l)$. Hence, $\delta(l) - \delta(l - 2) \geq 0$. Therefore, one can drop the term $\delta(l)$ from the recurrence to get the upper bound

$$N_2(m, l) = (2^m - 1)^{l-2} - N_2(m, l - 2). \tag{17}$$

Note that the above recurrence holds due to the special structure of $\delta(l)$. Since $N_2(m, 1) = N_2(m, 2) = 0$, solving (17) we have (14) where Δ is as given by (15).

Theorem 3: Let the CUT have m output lines and the compression of test responses is implemented by two primitive m-bit MISR's. Then for any test of length $n \leq 2^m - 1$ we have for the aliasing probability

$$P_{al} \leq \sum_{l=1}^{n} \binom{n}{l} \left(\frac{p}{q-1}\right)^l (1 - p)^{n-l} \cdot ((2^m - 1)^2 + 1)^{-1}((2^m - 1)^l + \Delta) \tag{18}$$

where Δ is as defined by (15).

Proof: First it may be seen that given some fixed l positions $i_1, i_2, \cdots, i_l$ in which errors can occur we know that the aliasing probability is given by

$$P_{al} \leq \sum_{l=1}^{n} \binom{n}{l} N_2(m, l) \left(\frac{p}{q-1}\right)^l (1 - p)^{n-l} \tag{19}$$

P_{al} can be obtained by using (14) in (19). Q.E.D.

Table III shows the bounds on the aliasing probabilities for data compression obtained using two 4-bit MISR's to compress the re-

TABLE III
ALIASING PROBABILITY FOR TWO MISR's

p	P_{al}	
	15 Tests	8 Tests
0.01	1.848×10^{-6}	2.397×10^{-7}
0.05	1.608×10^{-4}	2.572×10^{-5}
0.10	8.177×10^{-4}	1.693×10^{-4}
0.20	2.672×10^{-3}	9.024×10^{-4}

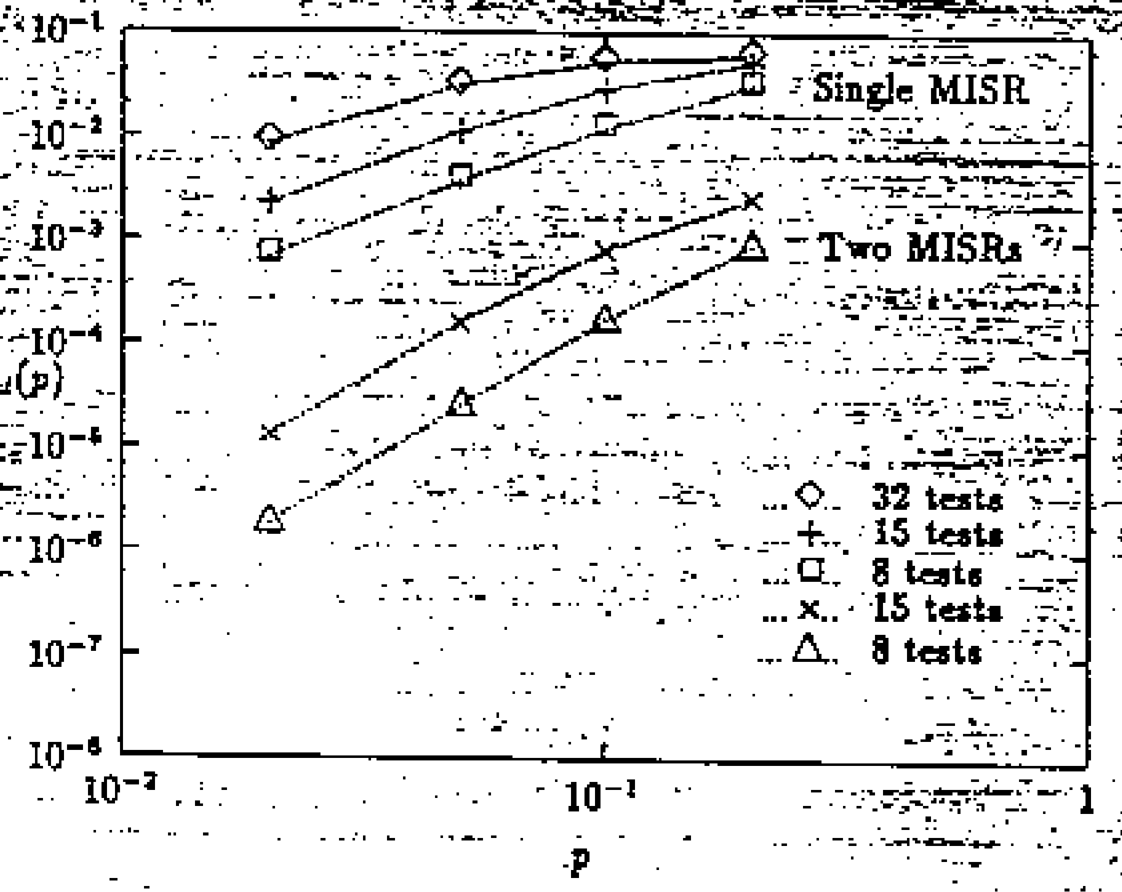

Fig. 6. Comparison of aliasing probability for one and two MISR's.

sponse of a 4-output circuit. The aliasing probabilities are given for two different test lengths. It may be noted that the aliasing probabilities are lower than in Table II when only one 4-bit MISR was used (see Fig. 6). Note that the aliasing probability for two MISR's is greater than the square of that for the single MISR case. This is due to the fact that the second MISR produces nonzero signature for a number of error vectors which are already detected with the first MISR alone.

Now comparing the two separate MISR schemes to a single MISR scheme of twice the size the following may be noted. First, the single MISR producing $2m$-bit signature will require longer feedback paths than required in two separate m-bit long MISR's. Second, errors of small multiplicity may cause aliasing in the single MISR scheme but not in the two separate MISR schemes. For example, $N_1(m, 2) \neq 0$ whereas $N_2(m, 2) = 0$. Thus, all errors of multiplicity two will not cause aliasing in two MISR schemes whereas some may alias in any single MISR scheme.

1) Multiple MISR's and Reed–Solomon Codes: We note that for the special case where in (19) both α and β are primitive elements, and $\binom{n}{l} N_2(m, l)$ is the weight distribution of the Reed–Solomon code over $GF(2^m)$ with distance 3. The code generated for $n = 2^m - 1$ is the maximum distance separable and its aliasing probability is given by

$$P_{al} = \sum_{l=1}^{n}\left[\binom{q-1}{l}\sum_{i=0}^{l-3}(-1)^i\binom{l}{i}\right.$$
$$\left.(q^{l-2-i}-1)\right]\left(\frac{p}{q-1}\right)^l (1-p)^{n-l} \qquad (20)$$

This result can be extended to multiple MISR's designed corresponding to Reed–Solomon codes. The aliasing probability in this case for $n = 2^m - 1$ can be computed exactly for any number of MISR's. It may be thus noted that (20) is upper bounded by our Theorem 3. Thus, Theorem 3 also provides a contribution to coding theory.

IV. CONCLUSION

Closed form expressions for MISR aliasing probability for arbitrary test lengths had not been available. This paper presents single and multiple MISR aliasing probability expressions for arbitrary test lengths. A framework, based on algebraic codes, is developed for the analysis and synthesis of MISR-based test response compressors for BIST. This framework is used to develop closed form expressions for aliasing probability of MISR for arbitrary test length (so far only bounds have been formulated). A new error model, based on q-ary symmetric channel, is proposed using more realistic assumptions. Results are presented that provide the weight distributions for q-ary codes ($q = 2^m$, where the circuit under test has m outputs). These results are used to compute the aliasing probability for the MISR compression technique for *arbitrary* test lengths. This result is extended to compression using two different MISR. It is shown that significant improvements can be obtained by using two signature analyzers instead of one. This paper makes a contribution to coding theory as well. It provides techniques for finding the weight distribution of a class of codes of arbitrary length. Also formulated is an expression bounding from above the probability of undetected error for these codes. The known results for the distance-3 Reed–Solomon codes over $GF(2^m)$ become a special case of our results. Further results and a general model for LFSR and MISR compression will appear in [10].

REFERENCES

[1] P. H. Bardell, W. H. McAnney, and J. Savir, *Built-In Test for VLSI: Pseudorandom Techniques.* New York: Wiley, 1987.

[2] S. K. Gupta and D. K. Pradhan, "Combining data compression techniques," in *Proc. BIST Workshop*, Charleston, SC, 1987.

[3] A. Ivanov and V. K. Agarwal, "Analysis of the probabilistic behavior of linear feedback signature registers," *IEEE Trans. Comput.-Aided Design*, vol. 8, pp. 1074–1088, Oct. 1988.

[4] K. Iwasaki, "Analysis and proposal of signature circuits for LSI testing," *IEEE Trans. Comput.-Aided Design*, vol. 7, pp. 84–90, Jan. 1988.

[5] T. Kasami and S. Lin, "The binary weight distribution of the extended $(2^m, 2^m - 4)$ code of the Reed–Solomon code over $GF(2^m)$ with generator polynomial $(x - \alpha)(x - \alpha^2)(x - \alpha^3)$," *Linear Alg. Appl.*, vol. 98, pp. 291–307.

[6] M. G. Karpovsky and P. Nagvajara, "Optimal time and space compression of test responses for VLSI devices," in *Proc. Int. Test Conf.*, 1987, pp. 523–528.

[7] ——, "Optimal robust compression of test responses," *IEEE Trans. Comput.*, vol. 37, Nov. 1988.

[8] F. J. MacWilliams and N. J. A. Sloane, *Theory of Error-Correcting Codes.* New York: North-Holland, 1978.

[9] P. C. Maxwell, "Comparative analysis of different implementations of multiple-input signature analyzers," *IEEE Trans. Comput.*, vol. 37, pp. 1411–1414, Nov. 1988.

[10] D. K. Pradhan and S. Gupta, "A new framework for designing and analyzing BIST techniques: Computation of exact aliasing probability," *IEEE Trans. Comput.*, submitted for publication.

[11] J. E. Smith, "Measures of the effectiveness of fault signature analysis," *IEEE Trans. Comput.*, vol. C-29, pp. 510–514, June 1980.

[12] T. W. Williams *et al.*, "Bounds and analysis of aliasing errors in linear feedback shift registers," *IEEE Trans. Comput.-Aided Design*, vol. 7, pp. 75–83, Jan. 1988.

[13] T. W. Williams and A. Daehn, "Aliasing errors in multiple input signature analysis registers," in *Proc. BIST Workshop*, Charleston, SC, 1989.