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 has 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. New formulas are derived that provide the weight distributions for q-ary codes (q = 2m, 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 MISRs. 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 distributions 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(2m) become a special case of our results.

Index Terms—Algebraic codes, aliasing probability, BIST, BIT, error models, MISR, Reed-Solomon codes, shift register, weight distribution.

Manuscript received July 6, 1989, revised December 29, 1989. This work was supported by NSF Grant MIP8900104 and MIP8313748.

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.
GFC(2). The following is a list of codewords in the code C:

\[
\begin{align*}
00 & 
\rightarrow 0 \beta 
\rightarrow \alpha \rightarrow 0 \beta \\
01 & 
\rightarrow 0 \beta 
\rightarrow \alpha \\
10 & 
\rightarrow 0 \beta 
\rightarrow \alpha \\
11 & 
\rightarrow 0 \beta 
\rightarrow \alpha
\end{align*}
\]

Here 0, 1, and 2 are elements of GF(2^2) where 0 = (0, 0), 1 = (0, 1), and 2 = (1, 1). Here \( \alpha \) and \( \beta \) are the primitive elements in GF(2^2) and \( \beta = \alpha^2 \). It can be seen that the generator polynomial for this code is \( x^2 + x + 1 \) which divides all the 16 codewords. For example, the codeword 12a = \( x^2 + x + 1 \) divided by \( (x + a) \) equals \( x + a(x + 1) \). The above codewords can also be expressed in binary form as:

\[
\begin{align*}
0 & \rightarrow 0000 \\
1 & \rightarrow 0100 \\
2 & \rightarrow 0110 \\
3 & \rightarrow 0111 \\
4 & \rightarrow 0000 \\
5 & \rightarrow 0100 \\
6 & \rightarrow 0110 \\
7 & \rightarrow 0111
\end{align*}
\]

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

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

This is, syndrome \( r(x) \) of \( r(x) \) is given by:

\[
r(x) = x(x)g(x) + r(x)
\]

where \( x(x) \) 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 \( r(x) \).

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 \( 0 \), is the remainder obtained by dividing the input sequence, interpreted as a polynomial, with \( x^2 + x + 1 \), where \( \alpha \) is an element in \( GF(2^2) \) and \( m \) is the number of inputs to the MISR.

The element \( \alpha \) is determined from the feedback polynomial defining the MISR. In particular, if the feedback polynomial is a primitive polynomial over \( GF(2^2) \), then \( \alpha \) is the primitive element over the field \( GF(2^2) \) which is defined by the given primitive feedback polynomial. (Every \( GF(2^2) \) field is defined by a primitive polynomial of degree \( m \) over \( GF(2) \)). In the following, the feedback polynomial representations over \( GF(2) \) and \( GF(2^2) \) 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 \( \alpha \) 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 \( x^2 + x + 1 \). Consider the input sequence \( (0,1,2,0) \). This is a codeword in the RS code in Example 1. Therefore, \( \alpha^2 + x + 1 \) is a codeword in the RS code in Example 1. Therefore, \( \alpha^2 + x + 1 \) is divisible by \( \alpha \). The following shows that the remainder, as expected, will be equal to \( 0 \) on \( 0 \).

<table>
<thead>
<tr>
<th>Input</th>
<th>State of MISR</th>
</tr>
</thead>
<tbody>
<tr>
<td>4-ary</td>
<td>Binary</td>
</tr>
<tr>
<td>( \alpha )</td>
<td>( (1,0) )</td>
</tr>
<tr>
<td>( \beta )</td>
<td>( (1,1) )</td>
</tr>
</tbody>
</table>

It may also be noted that the syndrome of states of MISR forms the quotient. For example, in dividing \( \alpha x^2 + \alpha x + \beta \) by \( x + \alpha \), one has \( \alpha x + 1 \) as the quotient and a remainder of 1. This is given by \( \alpha \) followed by 1, as shown above.

**Lemma 2:** Let \( R(x) \) and \( R'(x) \) be polynomial representations of two different vectors \( R \) and \( R' \) of length \( n \). Then both \( R(x) \) and \( R'(x) \) produce the same syndrome with respect to \( g(x) \) if and only if \( R(x) + R'(x) \) is a word polynomial in the code \( C \) generated by \( g(x) \).

**Example 3:** Given code \( C \) shown above generated by \( g(x) = x + \alpha \). Consider \( R(x) = \beta \alpha x^2 + \alpha x + 1 \) and \( R'(x) = \alpha x^2 + \alpha x + 1 \). Now \( R(x) \) and \( R'(x) \) will not produce the same syndrome as \( R(x) \) and \( R'(x) \) will produce the same syndrome as \( R(x) + R'(x) \), which is \( x^2 + x + 1 \). It is equal to a codeword in \( C \).

This is illustrated in Table 1. The final register entries marked with * represent the remainder after division by \( x + \alpha \). The final register entries in Table 1(a) and 1(b) are the same and the entry in Table 1(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. \( F = \{f_1, f_2, \ldots, f_n\} \) be the set of faults considered for the CUT. \( T = \{t_1, t_2, \ldots, t_n\} \) be the set of inputs vectors applied. \( R = \{r_1, r_2, \ldots, r_n\} \) be the good circuit responses corresponding to the input sequence \( T \). \( r_t \in GF(2^m) \) be the faulty circuit response corresponding to the input sequence \( T \) for a fault \( f \in F \). \( r_t' \in GF(2^m) \) and \( r_t' = r_t + r_f \). Let \( V \) be a test pattern for a fault \( f \in F \), then the response \( r_t' \neq r_t \) when CUT is fault with \( f \).

The symbols of the output responses \( R \) and \( R' \) over \( GF(2^m) \) will be denoted as \( E \), and is referred to as the error vector due to a fault, if \( r_t' \neq r_t \).

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 \( t_x \) is test for a fault \( f \in F \), then the term \( e_x^t \) must appear in \( E(x) \), where \( e_x^t \) is x \( t_x \).

The output response is compressed by using an MISR, with a feedback polynomial of degree \( m \) can be presented as \( x + \alpha \) in \( GF(2^m) \).
Fig. 1. MISR as the generator of RS code.

Table I

<table>
<thead>
<tr>
<th>Test</th>
<th>R(x)</th>
<th>Register Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>T0</td>
<td>R0</td>
<td>(0, 0)</td>
</tr>
<tr>
<td>T1</td>
<td>R1</td>
<td>(0, 1)</td>
</tr>
<tr>
<td>T2</td>
<td>R2</td>
<td>(0, 1)</td>
</tr>
<tr>
<td>T3</td>
<td>R3</td>
<td>(0, 1)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Test</th>
<th>IF(x)</th>
<th>Register Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>T0</td>
<td>F0</td>
<td>(0, 0)</td>
</tr>
<tr>
<td>T1</td>
<td>F1</td>
<td>(0, 1)</td>
</tr>
<tr>
<td>T2</td>
<td>F2</td>
<td>(0, 1)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Test</th>
<th>a(n)</th>
<th>Register Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>T0</td>
<td>A0</td>
<td>(0, 0)</td>
</tr>
<tr>
<td>T1</td>
<td>A1</td>
<td>(0, 1)</td>
</tr>
</tbody>
</table>

The following example illustrates the result in Theorem 1.

Example 4: Let us consider a two-output CUT. Let the good circuit response be \( r(x) = R(x) = x^2 + 1 \). The MISR compression for the good circuit will yield a signature \( S(x) = (0, 1, 1) \). Now if the output of the CUT is \( R'(x) = x^2 + x + 1 \). For the code constructed in Example 1, with \( S(x) = (x^2 + x + 1) \), the syndrome is \( S'(x) = (1, 0, 1) \). The outputs 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 is available that applies 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 a 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 circuits 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 fault 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 in the received sequence corresponding to transmitting good circuit response as 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 the problem of estimating effect of correlated error in the received sequence detected at the MISR.

Theorem 1: An error polynomial \( E(x) \) causes aliasing iff \( E(x) \) belongs to the code \( C \) generated by the polynomial \( f(x) = x^m + \alpha \), where \( \alpha \) is the primitive root of the corresponding feedback polynomial over \( GF(2^m) \), \( n \leq 2^m - 1 \), and \( \alpha \) is a root of the MISR feedback polynomial.
(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 $0(x) = 3$. 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

$$P_A = \sum_{l=1}^{n} E(l) \left( \frac{p}{q-1} \right) \left( 1 - p \right)^{l-1}$$

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 $E(l) = \lambda \lambda d(l)$ where $d(l)$ is the number of codewords of weight $l$ in the code generated by $g(x) = d(x)$. Thus,

$$P_A = \sum_{l=1}^{n} d(l) \left( \frac{p}{q-1} \right) \left( 1 - p \right)^{l-1}$$

Consequently, the aliasing probability in an MISR technique is the same as the probability of undetected error in the corresponding $q$-ary code generator 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 $d(x) = x + \alpha$ where $\alpha$ is the primitive element over $GF(2^m)$. First it may be noted that when $d(x) = x + \alpha$ this corresponds to the distance $2m$ maximum distance separable (MDS) code whose weight distribution is known [8] and is given as

$$d(l) = \binom{n}{l} \sum_{i=0}^{\lfloor l/2 \rfloor} (-1)^i \binom{n-1}{i} \left( \frac{p}{q-1} \right)^i \left( 1 - p \right)^{l-i-i}. \tag{4}$$

(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 $P_A$ for a $m$-bit MISR for any test length $n$ as

$$P_A = \sum_{l=1}^{n} \binom{n}{l} \sum_{i=0}^{\lfloor l/2 \rfloor} (-1)^i \binom{n-1}{i} \left( \frac{p}{q-1} \right)^i \left( 1 - p \right)^{l-i-i} \cdot \left( q^{l-i-i} - 1 \right) \left( \frac{p}{q-1} \right)^i \left( 1 - p \right)^{l-i-i}. \tag{5}$$

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 $N_i(m, l)$ 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, $N_i(m, l)$ represents error vectors of weight $l$ and length $n$ where the errors are confined to some fixed $l$ positions only. Thus, $E(l) = \binom{n}{l} N_i(m, l)$ represents total number of error vectors of length $n$ and weight $l$ that can cause aliasing.

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

**Proof:** Let $i_1, i_2, \ldots, i_l$ be some $l$ positions in which errors can occur. By definition of $N_i(m, l)$ and Corollary 1 one can see that $N_i(m, l)$ is the number of solutions $(e_{i_1}, e_{i_2}, \ldots, e_{i_l}, e_{j_1}, \ldots, e_{j_{m-l}})$, $(e_{j_1}, \ldots, e_{j_{m-l}} \neq 0)$, for the following linear equation over $GF(2^m)$

$$e_{i_1} + e_{i_2} + \cdots + e_{i_l} + \alpha e_{j_1} + \cdots + \alpha e_{j_{m-l}} = 0, \quad (i_1 < i_2 < \cdots < i_l) \quad (6)$$

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

Now consider (6) rewritten as follows

$$e_{i_1} + e_{i_2} + \cdots + e_{i_l} = e_{j_1} e_{j_2} \cdots e_{j_{m-l}}. \tag{7}$$

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

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

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 $(2^m - 1)^l$ possible combinations of nonzero $e_i$'s for the left-hand side of (7). Of these combinations, by definition there are precisely $N_i(m, l - 1)$ combinations which make the left-hand side of (7) zero. Thus, there are precisely $(2^m - 1)^l = N_i(m, l - 1)$ combinations of $e_i$'s, $e_{j_2} \ldots, e_{j_{m-l}}$ for which the left-hand side is nonzero and hence $e_i$ must also be nonzero. Solving (8) with the initial condition $N_i(m, 1) = 0$ we have

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

**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

$$A(l) = \binom{n}{l} \sum_{j=0}^{\lfloor l/2 \rfloor} (-1)^j \binom{n-1}{j} \left( \frac{2^m - 1}{2^m} \right)^j \left( \frac{1}{2^m} \right)^{l-j}. \tag{10}$$

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

$$P_A = 2^{-m} \left[ 1 - 2^{m-1}(1-\rho)^n + (2^m - 1) \left( 1 - 2^m \frac{p}{2^m - 1} \right)^n \right]. \tag{11}$$

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

$$P_A = \sum_{l=1}^{n} \binom{n}{l} \left( \frac{p}{q-1} \right)^l \left( 1 - p \right)^{l-1} \left( 2^m - 1 \right)^l \left( 1 - \left( \frac{2^m - 1}{2^m} \right)^l \right), \quad (q = 2^m)$$

$$= 2^{-n} \left[ 1 - 2^m(1-\rho)^n + (2^m - 1) \left( 1 - \left( \frac{2^m - 1}{2^m} \right)^n \right) \right]. \quad \text{Q.E.D.}$$
linear equations over $GF(2^m)$

$$
\begin{align*}
\varepsilon_0a^i + \varepsilon_1a^{i+1} + \cdots + \varepsilon_{m-1}a^{i+m-1} &= 0 \\
\varepsilon_0\beta^j + \varepsilon_1\beta^{j+1} + \cdots + \varepsilon_{m-1}\beta^{j+m-1} &= 0
\end{align*}
$$

where $(1 \leq i < \cdots < i_j)$ and $\alpha$ and $\beta$ are primitive roots for the feedback polynomials of the MISR's $(\alpha' \neq \alpha; \beta' \neq \beta'(\alpha \neq \beta); i, j \in {0, 1, \ldots, 2^m - 2})$

Lemma 3:

$$
N_2(m, I) = (2m - 1)^2 - (2m - 1)^2 + \Delta)
$$

where

$$
\Delta = \begin{cases} 
-1 & \text{if } I \text{ odd} \\
-2 & \text{if } I \text{ even}
\end{cases}
$$

Proof: One can select $I - 2$ of the coefficients $e_1, e_2, \ldots, e_{I-1}$ arbitrarily. One can rewrite (13) as follows:

$$
e^{1+e_1} + e^{2+e_2} + \cdots + e^{I-1+e_{I-1}} = e^{0+0} + e^{0+0} + \cdots + e^{0+0}$$

$$e^{\beta^j} + e^{\beta^{j+1}} + \cdots + e^{\beta^{j+I-1}} = \varepsilon_{m-1}\beta^{I+1} + \varepsilon_{m-1}\beta^{I+2} + \cdots
$$

This can be done in $(2m - 1)^2 - 1$ ways. Then $\varepsilon_{m-1}$ and $\varepsilon_{I}$ need to be selected such that they satisfy (16). As we have assumed that $\beta = \beta'$ where $s - 1$ and $2m - 1$ are mutually prime, $\varepsilon_{m-1}$ and $\varepsilon_{I}$ have unique values. This follows from the fact that the matrix $\begin{pmatrix} \beta & \beta^j \\
\beta^0 & \beta^j
\end{pmatrix}$ is nonsingular when the above condition is satisfied. By definition one has $N_2(m, I - 2)$ solutions to (12) were $e_{m-1} + e_I = 0$. Let $\delta(I)$ be the number of solutions where either $e_{m-1} = 0$ or $e_I = 0$ but not both. Hence, we have

$$
n_2(m, I) = (2m - 1)^2 - n_2(m, I - 2) - \delta(I)
$$

This follows from the observation that $N_2(m, I)$ represents the number of solutions in which all $e_i, 1 \leq i \leq I$, are nonzero in (13) and $\delta(I) \geq 0$. Substituting for $N_2(m, I - 2)$ one has

$$
n_2(m, I) = (2m - 1)^2 - (2m - 1)^2 + \delta(I) - \delta(I - 2)
$$

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

$$
N_2(m, I) = (2m - 1)^2 - N_2(m, I - 1)
$$

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

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

$$
P_A \leq \sum_{i=1}^{n} \binom{n}{i} (1 - \rho)^{i-1} (1 - \rho)^{n-i}$$

$$
(2m - 1)^2 + 11(2m - 1)^2 - \Delta)
$$

where $\Delta$ is as defined by (15).

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

$$
P_A \leq \sum_{i=1}^{n} \binom{n}{i} N_2(m, I) (1 - \rho)^{I-1} (1 - \rho)^{n-i}
$$

Table III shows the bounds on the aliasing probabilities for this compression obtained using two 4-bit MISR's to compress the
Fig. 6. Comparison of aliasing probability for one and two MISRs.

The aliasing probabilities for two MISRs 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. For the case where 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 with the single MISR scheme of which the size the following may be noted. First, the single MISR producing 2m-bit signatures 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, \( N_2(m, 2) \neq 0 \) 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 a single MISR scheme.

The open set of MISR’s and Reed-Solomon Codes. We note that for the special case where in (19) both \( a \) and \( b \) are primitive elements, and \( \sum_{i} N_2(m, 1) \) is the weight distribution of the Reed-Solomon code over \( GF(2^m) \) with distance 3. The codes generated for \( n = 2^n - 1 \) is the maximum distance separable and its aliasing probability is given by

\[
P_a = \sum_{i} \left( \begin{array}{c} q-1 \\ 2^{i} \\ 2^{i-1} \\ q-1 \\ 1 - p \end{array} \right) \left( \begin{array}{c} 1 \\ q-1 \\ p \end{array} \right)^{1-p} \left( \begin{array}{c} 1 \end{array} \right)^{2^{i-1}} \left( \begin{array}{c} 1 \end{array} \right)^{2^{i-1}}
\]

This result can be extended to multiple MISR’s designed corresponding to Reed-Solomon codes. The aliasing probability in this case for \( n = 2^n - 1 \) can be computed exactly for any number of MISR’s. It may be thus noted that (20) is upper bounded by our (20).

IV. CONCLUSION

Closed form expressions for MISR aliasing probability for arbitrary test lengths and 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 test compression schemes 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 arbitrary symmetric channel, is proposed using more realistic assumptions. Results are presented that provide the weight distributions for \( q \)-ary codes \( (q = 2^p \) where the circuit under test has \( n \) 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 \( GF(q^m) \) became a special case of our results. Further results and a general model for LFSR and MISR compression will appear in (10).

REFERENCES

[5] T. Kasami and S. Lin, "The binary weight distribution of the extended (2^n - 1, 2^n - 1) code of the Reed-Solomon code over GF(2^m) with generator polynomial \( (x^{2^n} + 1) \), Linear Alph. Appl., vol. 96, pp. 199-210.