# Aliasing and Diagnosis Probability in MISR and STUMPS Using a General Error Model*

**Mark G. Karpovsky**
College of Engineering
Boston University
Boston MA 02215

**Sandeep K. Gupta**
Electrical Engineering – Systems
University of Southern California
Los Angeles CA 90089

**Dhiraj K. Pradhan**
Electrical & Computer
Engineering Department
University of Massachusetts
Amherst MA 01003

## Abstract

A number of methods have been proposed to study aliasing in MISR compression. However, most of the methods can compute aliasing probability only for specific test lengths and/or specific error models.

Recently, a GLFSR structure [15] was introduced which admits coding theory formulation. The conventional signature analyzers such as LFSR and MISR form special cases of this GLFSR structure. Using this formulation, a general result is now presented which computes the exact aliasing probability for MISRs with primitive feedback polynomials, for **any test length** and for **any error model**. The framework is then extended to study the probability of **correct diagnosis** when faulty signature is used to identify the faulty CUT in the STUMPS environment.

Specifically, the results in [7, 15, 16] are extended by proposing two new error models, a general error model which subsumes all the commonly used models, and a fixed magnitude error model which is shown to be useful for fault diagnosis. It is shown how statistical simulation can be used to determine the general error model, for a given CUT. Aliasing for some benchmark circuits, for various error models and test lengths is studied.

## 1 Introduction

Coding theory framework first proposed in [5] has formed the basis of significant research [7, 15, 16]. Unlike Markov model techniques [3, 4, 19], coding theory framework provides closed form expressions for exact aliasing probability in LFSR [5, 15] and MISR [7, 8, 15, 16]. Recently, a new structure called generalized LFSR (GLFSR) for signature analysis and random pattern generation was proposed in [15]. Specifically, it was shown that conventional LFSR, MISR and multiple MISR can be treated uniformly as special cases of GLFSR. The other significance of the GLFSR structure is that it not only admits conventional signature analyzers as special cases but also allows formulation of new structures not studied before.

In this paper, a *general* error model is developed which subsumes the commonly used symmetric [7, 16] and independent [15, 19] error models. A method for determining the parameters of the general error model for a given circuit is also presented. The applicability of our approach is illustrated by demonstrating how aliasing probabilities for different benchmark circuits under various error models can be computed.

Fault diagnosis is becoming increasingly important. Signature analysis has significant applications in diagnosis, using dictionaries of fault signatures. Proposed here is a new error model called the *fixed-magnitude* error model. This model is used to study the probability of correct diagnosis when the faulty circuit signatures, along with fault dictionaries, are used to *diagnose* the fault.

The paper is divided into four main sections. Section 2 reviews the coding theory framework developed earlier [15, 16]. Section 3 presents various error models. Then, in Section 4, the aliasing probability expressions for any test length under the general, as well as the fixed magnitude model proposed here, are presented. The results pertaining to diagnosis are then presented in Section 5.

## 2 Review of Earlier Work

The first attempts to study MISRs were based on replacing the $m$ input sequences by an equivalent sequence applied to the first input [18]; this reduces the structure to an equivalent LFSR.

In [4], the Markov model has been used to study aliasing in MISRs. Firstly, it was shown in [20] that for the independent error model, the aliasing probability asymptotically converges to $2^{-m}$ (for $m$ bit MISR). In [4], the Markov model formulation has been extended to study aliasing in MISR compression under the independent error model. An expression for aliasing probability as a function of test length has been obtained. However, this expression is not a closed form expression and therefore, is computationally complex. Consequently, only an approximate expression for the aliasing probability, as a function of test length, was presented.

Recently, coding theory formulation proposed in [5] has been used to study aliasing in MISR compression [7, 15, 16]. The advantage of the coding theory formulation is that exact closed form expressions for aliasing probability can be formulated under the symmetric error model in [7, 16] for any test length, and under the independent error model in [15] for certain test lengths. (Closed form expressions for MISR aliasing under the independent error model has been an open problem.) In the following, we briefly review prior results [15, 16] first, as they are useful later in the paper.

### 2.1 GLFSR Framework

In [15], a new framework is presented for shift-register-based test response compressors. One unique feature of this framework is that it provides a uniform technique for the analysis of LFSR, MISR, multiple LFSR, and multiple MISRs. Previous formulations had treated these compressors separately [1, 6, 18]. Such a uniform treatment is possible using a coding theory model of the underlying mathematical relationships. Importantly, this framework admits formulation of *new* structures for compression and random pattern generation.

The circuit under test (CUT) is assumed to have $m$ outputs which are inputs to the signature analyzer. In the proposed GLFSR framework, the signature analyzer is a linear shift register designed over $GF(2^m)$. All the elements in the shift register are built out of elements over $GF(2^m)$. These multipliers, adders and storage elements are designed using conventional binary elements. (As explained below, the multipliers in the circuit are simple and implemented using exor gates.) Therefore, the inputs and outputs are considered $m$ bit binary numbers which can be interpreted as elements over $GF(2^m)$.

The structure of the GLFSR is shown in Figure 1. The feedback polynomial here is given as

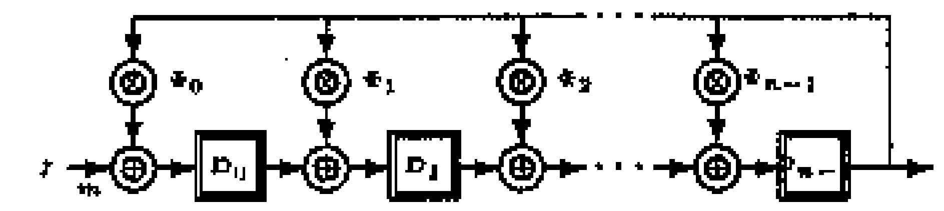

Figure 1: Generalized LFSR (GLFSR)

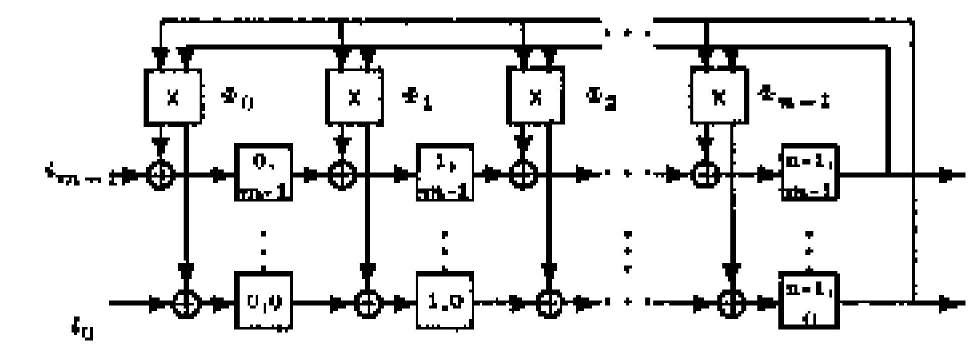

Figure 2: GLFSR$(m, n)$

$$\Phi(x) = x^n + \Phi_{n-1}x^{n-1} + \cdots + \Phi_1 x + \Phi_0$$

The coefficients of the polynomial are over $GF(2^m)$ and represent the feedback connections. The $i^{th}$ coefficient $\Phi_i$ defines the multiplier for the $i^{th}$ feedback connection, as shown in Figure 2. Actually, these are not general Galois field multipliers; instead they simply multiply the feedback input with a scalar which is a constant $\Phi_i$ over Galois field. Therefore, these are realizable using only simple ex-or gates. As shown, the GLFSR is assumed to have $m$ bit wide inputs/outputs. Also, it is assumed to have $n$ stages where each stage has $m$ storage cells. Thus, each shift shifts $m$ bits from one stage to the next. We denote this implementation of a GLFSR over GF(2) using binary logic as GLFSR$(m, n)$, where $m$ is the number of inputs and $n$ is the number of stages.

The following presents those special cases of the GLFSR that represent the conventional shift registers for signature analysis. These special cases are illustrated in Figure 3.

#### 2.1.1 $m = 1, n = 1$: Parity Compression

This corresponds to the case when a single output of the CUT is compressed to a single bit signature (which is simply the parity of the output response).

#### 2.1.2 $m = 1, n > 1$: LFSR

This GLFSR simply corresponds to a $n$-stage LFSR for compressing the response from a single output of the CUT.

*Research Supported by NSF Grants MIP8902014 and MIP8813748 and IBM Fellowship


CH3032-0/91/0000-0828$01.00© 1991 IEEE

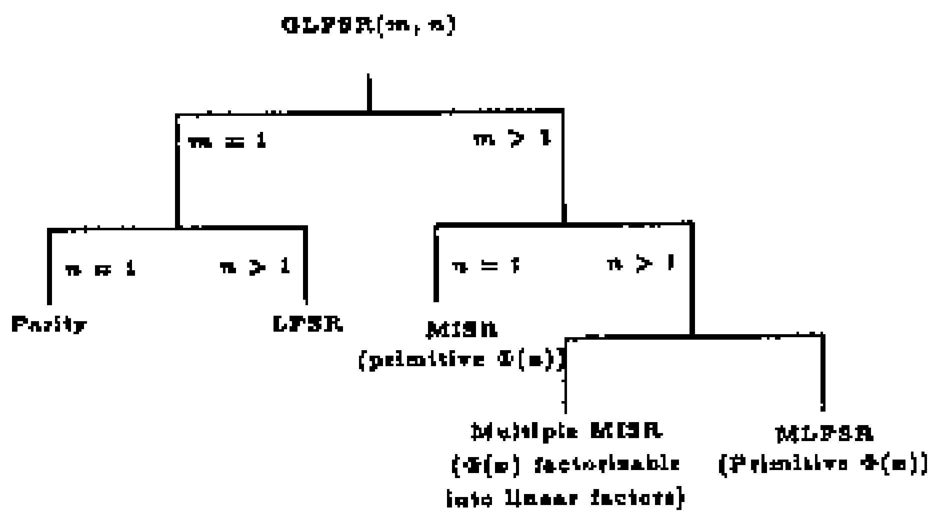


Figure 3: Special Cases of GLFSR

### 2.1.3 $m > 1$, $n = 1$: Conventional MISR

This case $m > 1$ and $n = 1$ corresponds to the conventional MISR, shown in Figure 4. The response of the CUT is commonly compressed by an $m$-stage MISR with a primitive feedback polynomial $\phi(x)$ (Figure 4). The polynomial $\phi(x)$ is usually a degree $m$ primitive polynomial over GF(2). This polynomial has an equivalent representation [15, 16] as a degree-1 feedback polynomial, $\Phi(x) = x + \alpha$, over $GF(2^m)$, as shown in Figure 5. Here, $\alpha$ is the primitive element in the $GF(2^m)$ generated by using $\phi(x)$ as the generator ($\alpha^i \neq \alpha^j$ for $i \neq j; i, j = 0, 1, \ldots, 2^m - 2$).

### 2.1.4 $m > 1$, $n > 1$: Multi-MISR & MLFSR

Two special cases of multi-stage GLFSR are of interest. One corresponds to the multiple MISR case. Multi-stage GLFSRs (MLFSR) with primitive feedback polynomial over $GF(2^m)$ are *new* structures not studied before and are presented in [15].

In the following section, the basic concepts behind signature analysis are introduced and the coding theory framework developed in [15, 16] is reviewed. With the aid of coding theory, the problem of aliasing has been shown [15, 16] to be equivalent to the problem of finding the probability of undetected error in the aliasing code (corresponding to the signature analyzer).

## 2.2 Signature Analysis

Consider a $m$-output CUT. Let $N$ be the number of tests applied to the CUT. Let

$$R(x) = r_{N-1}x^{N-1} + r_{N-2}x^{N-2} + \cdots + r_1x + r_0$$

be the polynomial representation [13] of the good circuit response where $r_i \in GF(2^m)$ $(0 \leq i < N)$ is the response of the good circuit for the $i^{th}$ [illegible]

$$R^f(x) = r^f_{N-1}x^{N-1} + r^f_{N-2}x^{N-2} + \cdots$$

be the polynomial representation of the faulty response where $r^f_i \in GF(2^m)$ for $0 \leq$ [illegible]

$$E(x) = e_{N-1}x^{N-1} + e_{N-2}x^{N-2} + \cdots$$

be the error polynomial where $e_i = r_i$ [illegible] Note that $E(x) = R(x) + R^f(x)$. (The [illegible] above relations is modulo two.)

For compression with a GLFSR with [illegible] polynomial $\Phi(x)$, the good circuit signature [illegible] given by:

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

where the degree of $S(x)$ is less than [illegible] $\Phi(x)$. Similarly, the faulty circuit signature [illegible] given by:

$$R^f(x) = h^f(x)\Phi(x) + S^f(x)$$

Aliasing occurs when the faulty response [illegible] $R(x)$ but $S(x) = S^f(x)$. Due to the linearity [illegible] compressors, the good circuit signature and [illegible] circuit signature will be identical if and only if [illegible] responding error polynomial $E(x)$ is divisible [illegible] It is known from coding theory that the [illegible] ary polynomials which are divisible by [illegible] tutes a code with generator polynomial [illegible] call this code the Aliasing Code, $AC$, of [illegible] sor [15, 16]. The following Lemma [16] [illegible] the $AC$ for MISR with a primitive feedback [illegible] mial.

**Lemma 1** [16] *If $N$ test vectors are [illegible] CUT, and the output is compressed using [illegible] feedback polynomial $\Phi(x) = x + \alpha$, where [illegible] itive element in $GF(2^m)$, then aliasing [illegible] only if the error polynomial $E(x)$ is a [illegible] $(N, N-1)$ Maximum Distance Separable [illegible] code over $GF(2^m)$ with generator $x + \alpha$* [illegible]

This is because the aliasing code [illegible] MISR is a distance 2 code over $GF(2^m)$ [illegible] gree of $\Phi(x)$ is 1, the aliasing code is MDS [illegible] tests are applied, then it is a $(N, N-1)$ [illegible] These codes correspond to the Reed-Solomon [illegible] when $N = 2^m - 1$ [13].

**Example 1** Consider a 2-output CUT [illegible] $N = 3$ tests are applied to it. Let the [illegible]



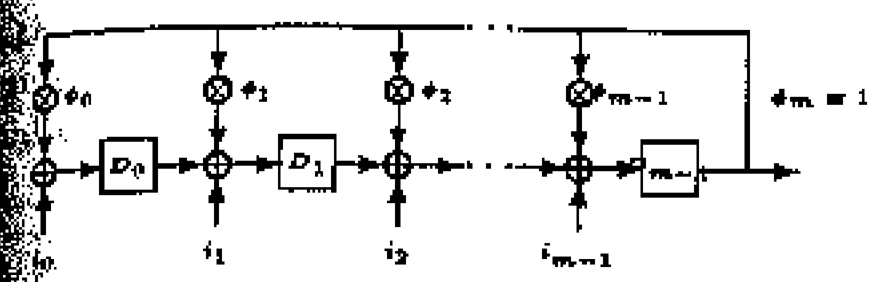

Figure 4: Conventional MISR compressor

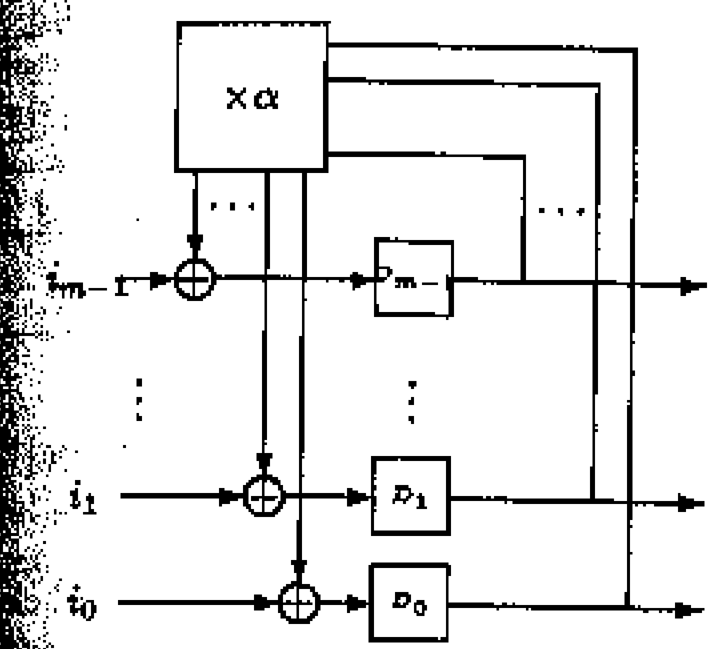

Figure 5: Single Stage $2^m$-ary LFSR

[illegible] by the MISR with a feedback polynomial [illegible] $x^2 + x + 1$ (Figure 6 (a)). (Note that this [illegible] can be represented as a single stage MISR over [illegible] with $\Phi(x) = x + \alpha$ (Figure 6 (b)), where $\alpha$ is [illegible] primitive element in $GF(2^2)$ generated by $\phi(x) =$ [illegible] i.e., $\alpha^2 + \alpha + 1 = 0$.) In this case, the field has [illegible] elements $\mathbf{0} = (0,0)$, $\mathbf{1} = (0,1)$, $\alpha = (1,0)$, and $\beta =$ [illegible] where $\beta = \alpha^2 = \alpha + 1$.

[illegible] can be shown that only those $R^f(x)$ can cause [illegible] for which the error $E$ belongs to the following [illegible] code ($AC$).

$$AC = \left\{ \begin{array}{llll} 000 & 1\alpha0 & \beta0\alpha & \beta\alpha1 \\ 01\alpha & \alpha\beta0 & 10\beta & 111 \\ 0\alpha\beta & \beta10 & 1\beta\alpha & \alpha\alpha\alpha \\ 0\beta1 & \alpha01 & \alpha1\beta & \beta\beta\beta \end{array} \right\}$$

In this case, out of $4^3 - 1 = 63$ possible nonzero [illegible] vectors, there are 15 nonzero errors $E$ such that [illegible] and these errors will result in aliasing in the [illegible] of Figure 6.

## 3 Error Models

[illegible] selection of the correct error model for the CUT is [illegible] accurate computation of aliasing probability. In the following, we present a very general error model. It is shown that the commonly used independent and symmetric error models can be interpreted as special cases of this model.

There are two important components of any error model, *temporal* and *spatial*. The first aspect, *temporal*, models the correlation between the errors caused by different test vectors. For combinational circuits, and combinational faults, errors can be assumed to be *independent in time*. That is, if $E(x) = e_{N-1}x^{N-1} + \cdots + e_1x + e_0$, then $e_i$ and $e_j$ are statistically independent of each other. This is a reasonable assumption because in BIST, pseudo-random vectors are applied to the CUT. Since the test vectors for any fault are randomly distributed in the input sequence, there is no correlation between errors due to any two test vectors. The following discusses various *spatial* models.

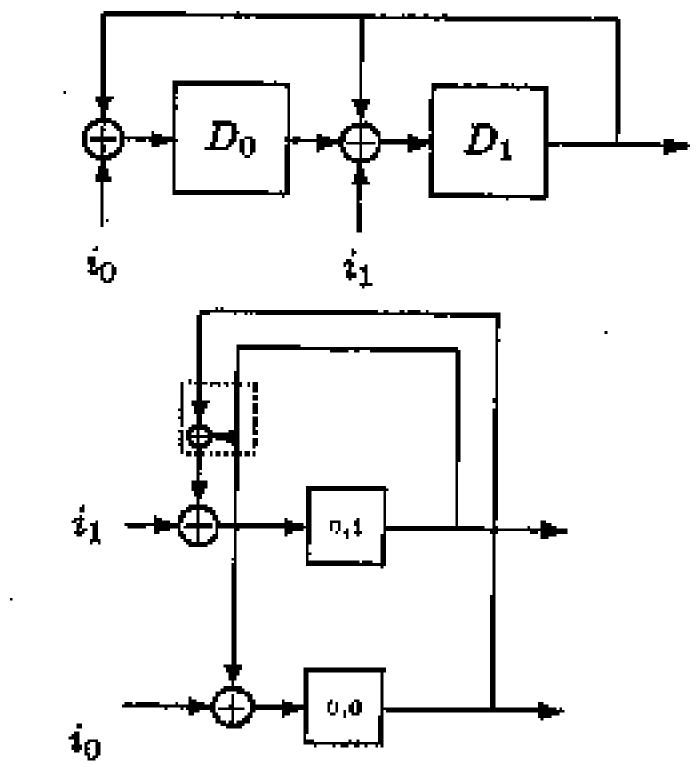


Figure 6: MISR with (a) $\phi(x) = x^2 + x + 1$ over GF(2); (b) $\Phi(x) = x + \alpha$ over $GF(2^2)$

## 3.1 Spatial Models

The other aspect of the error model in multi-output CUTs is the manner in which the errors manifest themselves at the various outputs of the CUT at any given moment, for randomly chosen test vectors. Let the error value for the test-$i$ be $e_i$. For an $m$-output circuit, $e_i \in GF(2^m)$; hence, it can take $2^m$ values and $e_i = \mathbf{0} = (\overbrace{0\ldots0}^{m})$ indicates that the test-$i$ did not detect any fault. On the other hand, a non-zero value of $e_i$ indicates that the test detected a fault and the effect was observed at one or more outputs of the CUT. The spatial model for the circuit is closely related to the topology of the circuit.

#### 3.1.1 General Error Model

Independent and symmetric error models have been used in the literature. These models can be used efficiently for some circuits. However, in general, it is difficult to determine which error model is appropriate for a given circuit. Hence, in the following, a general model is proposed. All 'independent in time' error models are subsumed by this model. This model assumes that the error $e_i$ can take any of its $2^m$ values, $\{0, 1, \alpha, \alpha^2, \ldots, \alpha^{2^m-2}\}$, with probabilities $p_0, p_1, \ldots, p_{2^m-1}$, respectively.

#### 3.1.2 $2^m$-ary Symmetric Error Model

This model assumes that the error, for any test vector, $e_i$, can take a value 0 with a probability $1-p$ and can take any of the $2^m - 1$ non-0 (faulty) values with a probability $p/(2^m-1)$ [15, 16]. This model is useful if the outputs of the circuit share logic and the effect of faults can get propagated to any of the outputs. Note that this can be obtained as a special case of the general error model by substituting $p_0 = 1-p$ and $p_i = p/(2^m-1), 1 \le i \le 2^m - 1$.

#### 3.1.3 Independent Error Model

This model assumes that a test can propagate the effect of a fault to any output of the CUT, *independently* of its propagation to any other output. That is, each output bit of the CUT can be in error with a probability $p$ independent of the other outputs. Hence, if $e_i$ is seen as a binary $m$-tuple ($e_i = \alpha^j \in GF(2^m)$), then the probability that $e_i$ has a weight $w$ (i.e., $w$ is the number of 1's in $e_i$) is $\binom{m}{w} p^w (1-p)^{m-w}$. The results for this case can be found in [4, 15]. In this case, the general error model parameter $p_0 = (1-p)^m$ and $p_j = \binom{m}{w} p^w (1-p)^{m-w}$, where $w$ is as defined above.

#### 3.1.4 Errors of a Given Magnitude

This error model assumes that if a test vector detects a fault, then the error $e_i$ is always equal to some fixed value $a \in GF(2^m)$. That is, the probability that $e_i = a$ is $p$ and the probability that $e_i = 0$ is $1-p$. This model is appropriate for circuits where every fault affects only a fixed set of outputs for all tests. Also, this model is useful for approaches such as STUMPS [1] (Figure 7) where a fault within a *single* chip can affect only a *single* input of MISR.

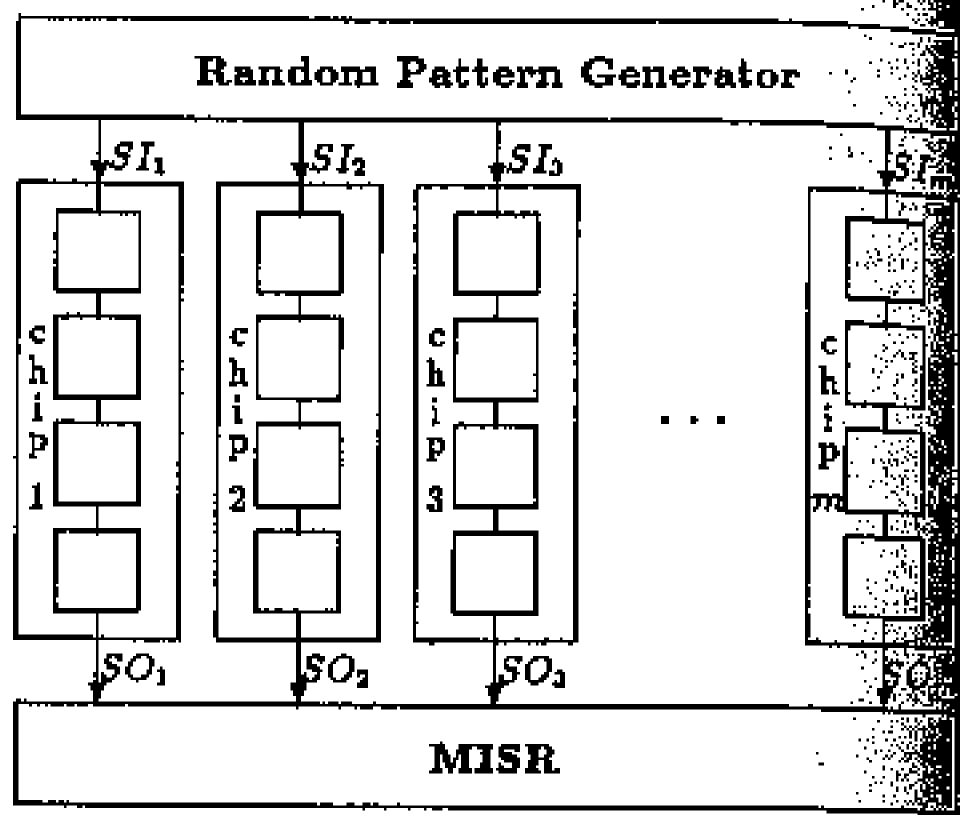


Figure 7: Global Test using STUMPS [1]

It is significant to note that as seen below, [illegible] coding theory framework can be used to compute [illegible] probability of aliasing in MISR compression for [illegible] one of the proposed error models including the [illegible] eral error model. To use the general error model [illegible] a given CUT, one has to determine the values of [illegible] parameters $p_i, i = 0, 1, \ldots, 2^m - 1$. In the following, a statistical method to determine precisely these [illegible] rameters is presented.

### 3.2 Statistical Determination of the Gen[illegible] Error Model

One approach to compute the parameters $p_i$ would [illegible] to perform a fault simulation on the circuit with [illegible] of random test vectors. Then, the resulting error [illegible] tors at the output of the CUT for the various [illegible] can be studied to compute $p_i$s. Basically, $p_i$ can [illegible] estimated to be equal to the number of times a [illegible] ticular $e_i$ occurs, in the output, divided by the [illegible] number of errors at the output. This procedure [illegible] computationally complex. Specifically, the comp[illegible] of this procedure increases linearly with the number [illegible] gates in the circuit, linearly with the number of [illegible] vergent fan-out lines, and linearly with the num[illegible] vectors applied.

The space complexity of storing the count [illegible] the possible error patterns $e_0, e_1, \ldots, e_{2^m-1}$ dep[illegible] on the number of outputs. However, for any given [illegible] cuit, a large number of these error patterns can [illegible] occur. We present below an upper bound on a [illegible] mal number of nonzero error patterns.



Consider a circuit with $n$ inputs $x_1, x_2, \ldots, x_n$ such that $k_i$ outputs are dependent on input $x_i$. Then, the number of error patterns, $N_p$ due to single stuck-at-faults, is bounded from above by:

$$N_p \le \sum_{i=1}^{n} 2^{k_i}.$$

For example, if the CUT has 32 inputs and 32 outputs and if $\max_i k_i = 10$, then $N_p \le 32 \times 2^{10} (\ll 2^{32})$.

This bound can be improved by a more detailed topological analysis of the CUT. Let $Y_i$ be the set of outputs that depend on the input $x_i$, $0 \le i < n$. Let $|Y_i| = k_i$, $|Y_i \cap Y_j| = k_{ij}$, $|Y_i \cap Y_j \cap Y_r| = K_{ijr}, \ldots$. Then, by the principle of inclusion and exclusion,

$$N_p \le \sum_i 2^{k_i} - \sum_{ij} 2^{k_{ij}} + \sum_{ijr} 2^{k_{ijr}} - \ldots.$$

The following shows how the parameters of the general error model can be directly used in computing aliasing probability.

## 4 Computation of Aliasing Probability by Weight Distribution of Aliasing Codes

Consider an $m$-output circuit. For each test vector that is applied to the CUT, a $m$ bit output is produced. Let $N$ be the number of tests applied to the CUT and let the response be compressed using a MISR with a degree $m$ primitive feedback polynomial, as shown in Figure 4. This is analogous to compression using a single stage GLFSR [15], as shown in Figure 5. As noted before, the feedback polynomial of this is $\Phi(x) = x + \alpha$ where $\alpha$ is a primitive element in the field $GF(2^m)$, generated using $\phi(x)$, the feedback polynomial of the MISR. This equivalence holds when $\phi(x)$ is primitive. The aliasing code $AC$ is the code over $GF(2^m)$, generated by $\Phi(x) = x + \alpha$ as the generator polynomial.

Key to developing expressions for aliasing probability is the formulation of expressions for appropriate weight enumerators for the aliasing code [15]. There are different weight enumerators. The type of weight enumerator to be used depends on the particular error model. Specifically, the Hamming weight enumerator was shown to be useful in computing MISR aliasing probability for any test length [16] under the symmetric error model. In [15] the binary weight enumerator was developed to compute the MISR aliasing probability for certain test lengths [15] under the independent error model. (The formulation of a closed form expression for MISR aliasing probability under independent error model had been an open problem.) In the following, the complete weight enumerator is presented, used to compute the aliasing probability for the general error model.

### 4.1 Complete Weight Enumerator

The composition of a codeword over $GF(2^m)$ is a $2^m$-tuple whose entries represent the number of times each $GF(2^m)$ symbol appears in the codeword. The complete weight enumerator of a code contains information about the number of codewords which have any given composition. It is represented as $W_C(z_0, z_1, \ldots, z_{2^m-1})$, where $z_i$ are the parameters corresponding to the symbols $\{0, 1, \alpha, \ldots, \alpha^{2^m-2}\}$. The following example illustrates the concept.

**Example 2** Consider a degree-2 primitive polynomial $\phi(x) = x^2 + x + 1$. This polynomial generates the field $GF(4)$ with elements $\{0, 1, \alpha, \alpha^2\}$ denoted as $\{\omega_0, \omega_1, \omega_2, \omega_3\}$.

Consider code $C$ over $GF(2^2)$ with the generator polynomial

$$g(x) = (x + \alpha^2)(x + \alpha^3) = x^2 + \alpha x + \alpha^2,$$

where $\alpha$ is the primitive element of $GF(2^2)$. The codewords of this code are

$$\{(0,0,0), (1, \alpha, \alpha^2), (\alpha, \alpha^2, 1), (\alpha^2, 1, \alpha)\}$$

(This is the distance three Reed-Solomon code, RS(3, 1) [13].) The CWE of this code is given by

$$W_{RS(3,1)}(z_0, z_1, z_2, z_3) = z_0^3 + 3 z_1 z_2 z_3.$$

The CWE of a code can be obtained from the CWE of its dual using the MacWilliam's identity for CWE. A detailed discussion on CWE can be found in [2, 13].

Let $w = (w^{(0)}, w^{(1)}, \ldots, w^{(m-1)})$, $s = (s^{(0)}, s^{(1)}, \ldots, s^{(m-1)}) \in GF(2^m)$ ($w^{(i)}, s^{(j)} \in \{0, 1\}$), and let $\hat{z}_w$ be the Walsh Transform [10, 11] of $z$, where

$$\hat{z}_w = \sum_{s=0}^{2^m-1} (-1)^{<w,s>} z_s \qquad (1)$$

and,

$$<w, s> = \sum_{i=0}^{m-1} w^{(i)} s^{(i)}.$$

Then, by the MacWilliam's identity for CWE [13] we have

$$W_C(z_0, \ldots, z_{2^m-1}) = \frac{1}{|C^{\perp}|} W_{C^{\perp}}(\hat{z}_0, \ldots, \hat{z}_{2^m-1}). \tag{2}$$

Computation of the Walsh transform $z_s \rightarrow \hat{z}_v$ can be implemented by the Fast Walsh Transform algorithm [10] which requires $m2^m$ additions and subtractions only.

**Example 3** Let us compute the CWE for the RS(3, 2) code with generator $g(x) = x + \alpha$, using the weight distribution derived in Example 2 for RS(3, 1) = $RS^{\perp}(3, 2)$ code, and the above identity. Note that in this case $\hat{z}_0 = z_0 + z_1 + z_2 + z_3$, $\hat{z}_1 = z_0 - z_1 + z_2 - z_3$, $\hat{z}_2 = z_0 + z_1 - z_2 - z_3$, and $\hat{z}_3 = z_0 - z_1 - z_2 + z_3$. Hence, we have

$$\begin{aligned} W_{RS(3,2)} &= \frac{1}{4}[(z_0 + z_1 + z_2 + z_3)^3 \\ &\quad +3(z_0 - z_1 + z_2 - z_3)(z_0 + z_1 \\ &\quad -z_2 - z_3)(z_0 - z_1 - z_2 + z_3)] \\ &= z_0^3 + 3z_0z_1z_2 + 3z_0z_2z_3 + 3z_0z_1z_3 \\ &\quad +3z_1z_2z_3 + z_1^3 + z_2^3 + z_3^3. \end{aligned}$$

The proposed approach for computing the MISR aliasing probability under a given error model for the CUT consists of the following three steps. (i) First, compute the appropriate weight enumerator, corresponding to the chosen error model, for the code which is dual of the MISR aliasing code. (ii) Next, use MacWilliam's identity (Eq. 2) to determine the weight enumerator of the aliasing code itself. (iii) Finally, use the weight enumerator of the aliasing code to compute the aliasing probability as shown next.

## 4.2 Computation of Aliasing Probability for Various Error Models

We will present in this section a general solution for the aliasing problem for arbitrary test length $N$ for the proposed general error model. We show how the expression for the general error model can be used for other error models as well. First, the complete weight enumerators of $2^m$-ary codes generated using the generator $\Phi(x) = x + \alpha$, are presented. (Note that for any arbitrary block length $N$, these codes are not cyclic. However, these are MDS codes for all values of $N$ and their Hamming weight enumerator is known [13] for all block lengths.) The following theorem gives the CWE for these codes for arbitrary block length $N$.

**Theorem 1** *[15] Let $C = C(N, N-1)$ … code generated by $\Phi(x) = x + \alpha$. Then … matrix of the code $C$ is given by*

$$H = \left[\alpha^{2^m-2}\alpha^{2^m-3} \ldots \alpha^{2^m-N-1}\right]$$

*(where, $\alpha^{-1} = \alpha^{2^m-2}, \alpha^{-2} = \alpha^{2^m-3}$ … CWE of the dual code $C^{\perp}(N, 1)$ is given by*

$$W_{C^{\perp}}(z_0, z_1, \ldots, z_{2^m-1}) = z_0^N + \sum^{2^m-1} \prod \ldots$$

*where, $z_{2^m} = z_1, z_{2^m+1} = z_2, \ldots$.*

**Example 4** Consider the field GF(4) gen… $\phi(x) = x^2 + x + 1$. The elements of the … $\{0, 1, \alpha, \alpha^2\}$. Consider $\Phi(x) = x + \alpha$. For the … responding code $C = C(4, 3)$, the generator … given by

$$G = \begin{bmatrix} 1 & \alpha & 0 & 0 \\ 0 & 1 & \alpha & 0 \\ 0 & 0 & 1 & \alpha \end{bmatrix}$$

It can be seen that the parity check matrix … code can be written as

$$H = \left[\begin{array}{cccc} \alpha^2 & \alpha & 1 & \alpha^2 \end{array}\right]$$

Hence, the CWE of the dual code $C^{\perp}(4, 1)$ is

$$W_{C^{\perp}} = z_0^4 + z_1^2 z_2 z_3 + z_1 z_2^2 z_3 + \ldots$$

Theorem 1 shall now be used to … in MISR for various error models.

**General Error Model:** The weight enume… rived above can be used to compute the alias… ability for any **test length** $N$, for any erro… as given by the following theorem.

**Theorem 2** *Let $N$ be the number of tests … an $m$-output circuit whose response is compr… ing a primitive feedback polynomial; then the … probability assuming general error model is …*

$$\begin{aligned} P_{al} &= W_C(p_0, p_1, \ldots, p_{2^m-1}) - \ldots \\ &= \frac{1}{2^m}\left(\hat{p}_0^N + \sum_{i=1}^{2^m-1} \prod_{j=0}^{N-1} \hat{p}_{i+} \ldots \right. \end{aligned}$$

*where, $W_C(z_0, z_1, \ldots, z_{2^m-1})$ is the CWE … $C(N, N-1)$ code over $GF(2^m)$ with $x + \alpha$ … ator polynomial, $p_0, p_1, \ldots, p_{2^m-1}$ are the … of errors in the general error model, … Walsh transform of $p_s$.*

…orem 2 which follows from Theorem 1 and Eq. (2) … a closed form expression. However, for symmet… …d independent error models, closed form expres… have already been derived and are given below. …lly, a closed form expression for fixed magnitude … model is now derived and presented here for the … time. The proofs of all the theorems can be found … [12].

It may also be noted that the computation of …ing using Theorem 2 is not computationally inten… …s seen in Section 4.3.

**…ary Symmetric Error Model.** The Hamming …ht enumerator for the distance-2 RS code [13] can … used to compute the aliasing probability for this … model. This is given by the following theorem … **any test length.**

**…eorem 3** [7, 16] *If $N$ tests are applied to an $m$-… CUT whose response is compressed using a … with a primitive feedback polynomial, then the … …ing probability assuming $2^m$-ary symmetric error … is given by:*

$$\begin{aligned} P_{al} &= \frac{1}{2^m}\left[1 - 2^m(1-p)^N \right. \\ &\quad \left. +(2^m - 1)\left(1 - \frac{2^m p}{2^m - 1}\right)^N\right]. \end{aligned} \tag{6}$$

**…ependent Error Model:** This is the most com… …y used error model. The aliasing probability for … case can be computed using the weight enumer… … of the binary image of the aliasing code $AC$. … is what was called the binary weight enumera… … $BW_{AC}(x, y)$ of the $AC(r(2^m - 1), r(2^m - 1) - 1)$ … and is derived in [15]. $BW_{AC}(x, y)$ can be used … compute the aliasing probability for MISR compres… … under the independent error model, as given by … following theorem.

**…eorem 4** [15] *If $N = r(2^m - 1)$ tests are applied … m-output CUT whose response is compressed us… … MISR with primitive feedback polynomial, then … aliasing probability, assuming independent error … is given by:*

$$\ldots \frac{1}{2^m}\left[1 + (2^m - 1)(1 - 2p)^{\frac{rm2^m}{2}}\right] - (1-p)^{rm(2^m-1)}. \tag{7}$$

**Errors of a Given Magnitude.** The weight enumerator of binary Hamming code [7] can be used to compute the aliasing probability for this error model.

**Theorem 5** *Let $N = 2^m - 1$ tests be applied to an $m$-output CUT whose response is compressed using a MISR with primitive feedback polynomial. The aliasing probability, assuming that the errors have a fixed magnitude, is given by:*

$$P_{al} = \frac{1}{2^m}\left[1 + (2^m - 1)(1 - 2p)^{2^{m-1}}\right] - (1 - p)^{2^m - 1}. \tag{8}$$

## 4.3 Experimental Results Comparing Aliasing Probabilities for Various Error Models

In this section, aliasing probabilities will be compared for certain benchmark circuits, for the error models discussed here. First, the general error model is obtained by statistical simulation of these circuits. Then, the parameters for the other error models are computed by approximating the parameters of the general error model. Using these parameters, aliasing probabilities are computed under various error models. The following example illustrates the process.

**Example 5** Consider the ALU 181. This circuit has 14 inputs, $m = 8$ outputs and 197 lines. Let the outputs be connected to a 8-bit MISR with primitive feedback polynomial. The circuit was simulated using 2,000 pseudo-random vectors; the parameters $p_0, p_1, \ldots, p_{255}$ for the general error model were determined statistically. The probability $p_0$ that a randomly selected test vector would not detect any fault was found to be 0.74865. Similarly, $p_1, p_2, \ldots, p_{255}$ were determined. The aliasing probability of the 8-bit MISR with a primitive feedback polynomial for the general error model is shown in Figure 8 for various test lengths using Theorem 2.

Also shown in this figure is the aliasing for ALU 181 under other error models. As discussed above, the parameters for these other error models were derived by approximating the general error model parameters, as discussed below.

**$2^m$-ary Symmetric Model:** The parameter $p$ for this case was found by equating $p_0$ in the general error model, to the zero error probability in the $2^8$-ary symmetric model. Thus, $p_0 = 1 - p$ and one has $p = 0.25135$. This value of $p$ was substituted directly in Theorem 3, as it is valid for any test length.

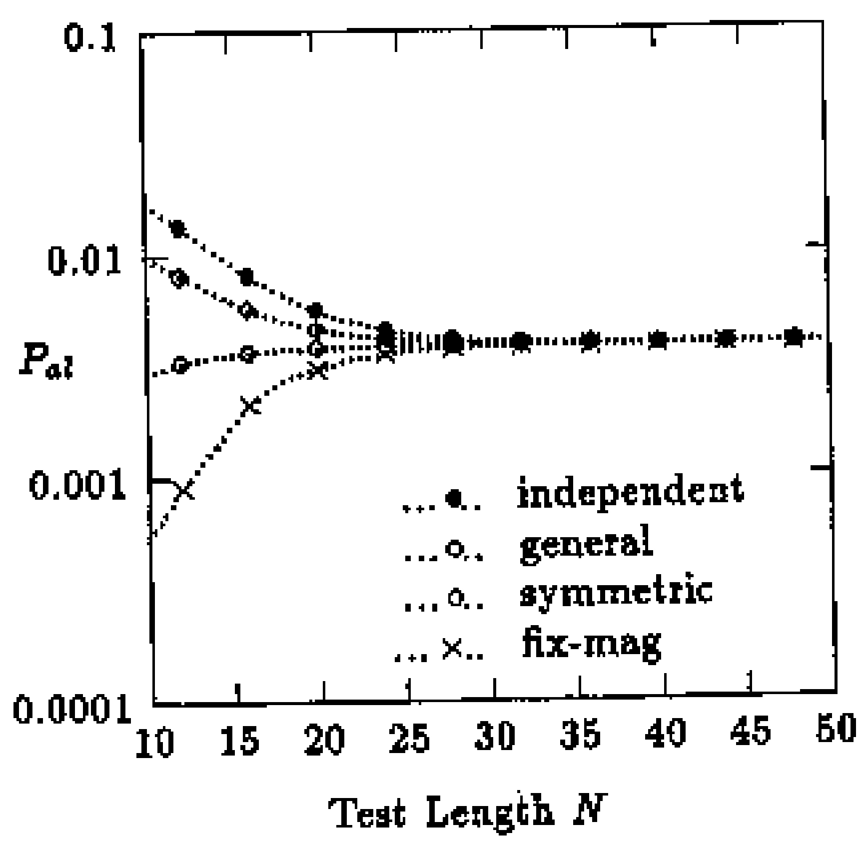


Figure 8: Aliasing probability for ALU 181

**Independent Error Model:** For this error model, $p_0$ for the general model was equated to the probability that the test does not detect any faults. Thus, the bit-error rate, $p$, was obtained by equating $(1-p)^m$ to $p_0$, where $m = 8$. Hence, $p = 0.035539$. This value of $p$ was used in Theorem 2 as described earlier.

**Errors of a Fixed Magnitude:** In this case, there are only two possible error values, 0 (error free) and some fixed error value $\alpha^j$. These occur with probabilities $1-p$ and $p$, respectively. $p$ was computed by equating $p_0 = 1 - p$. Hence, $p$ was determined to be the same as in the $2^m$-ary symmetric error model. This was used in Theorem 2 as described earlier.

Similarly, the benchmark circuit C432 ($m = 7$) was analyzed; aliasing probabilities for various error models are shown in Figure 9. Additionally, some benchmark PLAs (Table 1) were resynthesized as multi-level circuits. These resynthesized circuits were also analyzed, as above. Figures 10-13 present these results.

It is interesting to note that for large test lengths $N$, all the error models converge to the same aliasing probability. However, for small $N$, the independent error model predicts maximum aliasing, whereas the symmetric error model predicts minimum aliasing. We conjecture that the symmetric error model predicts aliasing more accurately than the other error models. If our conjecture is true, then the prediction of aliasing becomes trivial because closed form

| Circuit | Lines | #PI | #PO | Vectors Simulated |
|---|---|---|---|---|
| C181 | 197 | 14 | 8 | [illegible] |
| C432 | 432 | 36 | 7 | [illegible] |
| 5xp1 | 212 | 7 | 10 | [illegible] |
| alu4 | 673 | 14 | 8 | [illegible] |
| clip | 308 | 9 | 5 | [illegible] |
| vg2 | 173 | 25 | 8 | 65536 |

Table 1: Benchmark Circuits used to study [illegible]

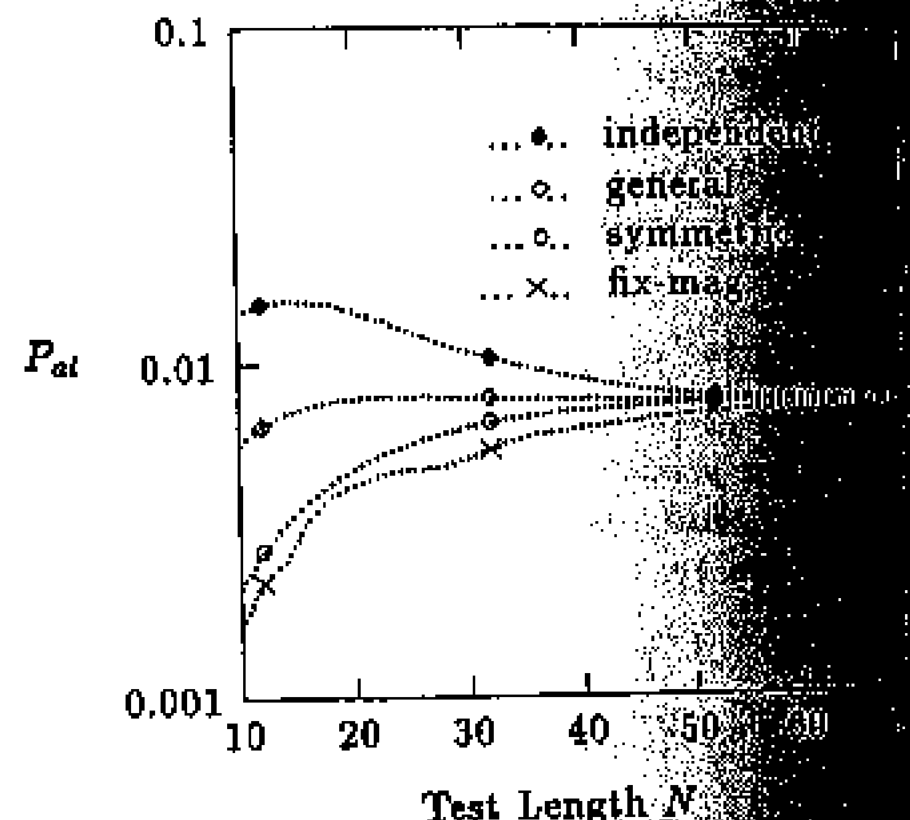


Figure 9: Aliasing probability for [illegible]

expressions for any test length exist [illegible] metric error model. It may also be [illegible] circuit has only a few outputs, as the [illegible] ure 12), then all the error models give [illegible]

## 5 Diagnosis by Signature [illegible]

Signature analyzers have been traditionally [illegible] both testing and diagnosis. In performing [illegible] faulty signature is used to locate the [illegible] ticularly useful when a signature analyzer [illegible] natures from a number of modules like [illegible] approach. The final signature is then [illegible] the faulty module for repair. The [illegible] ally done off-line with the help of a [illegible] which provides mapping between the [illegible] and the most likely fault. Misdiagnosis [illegible] unnecessarily replacing a good part [illegible]



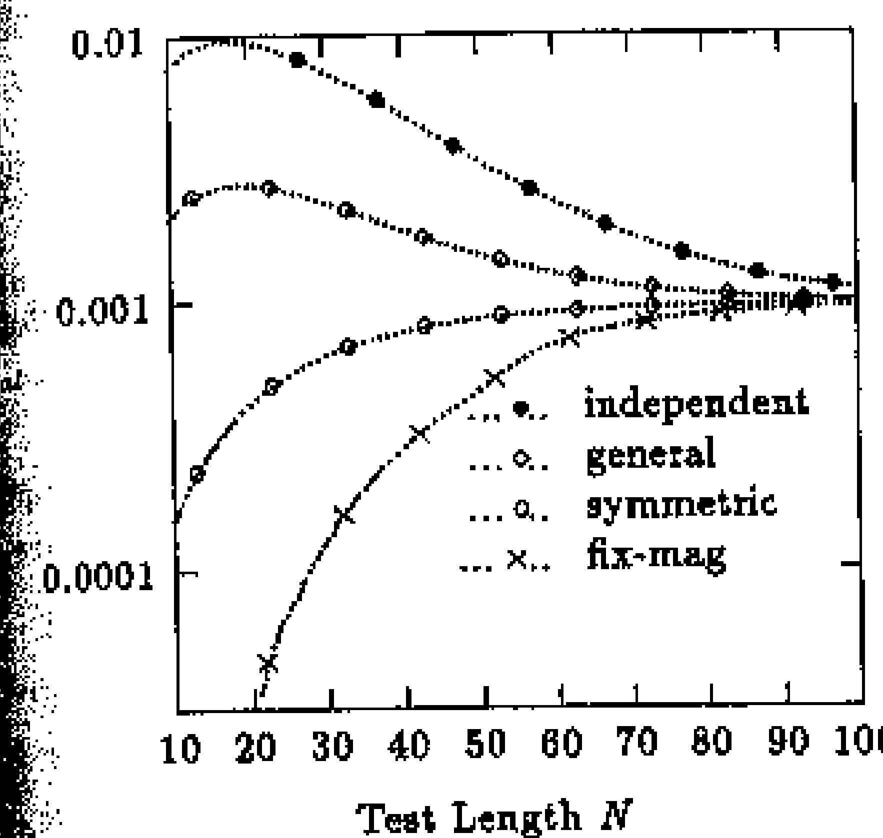


Figure 10: Aliasing probability for 5xp1

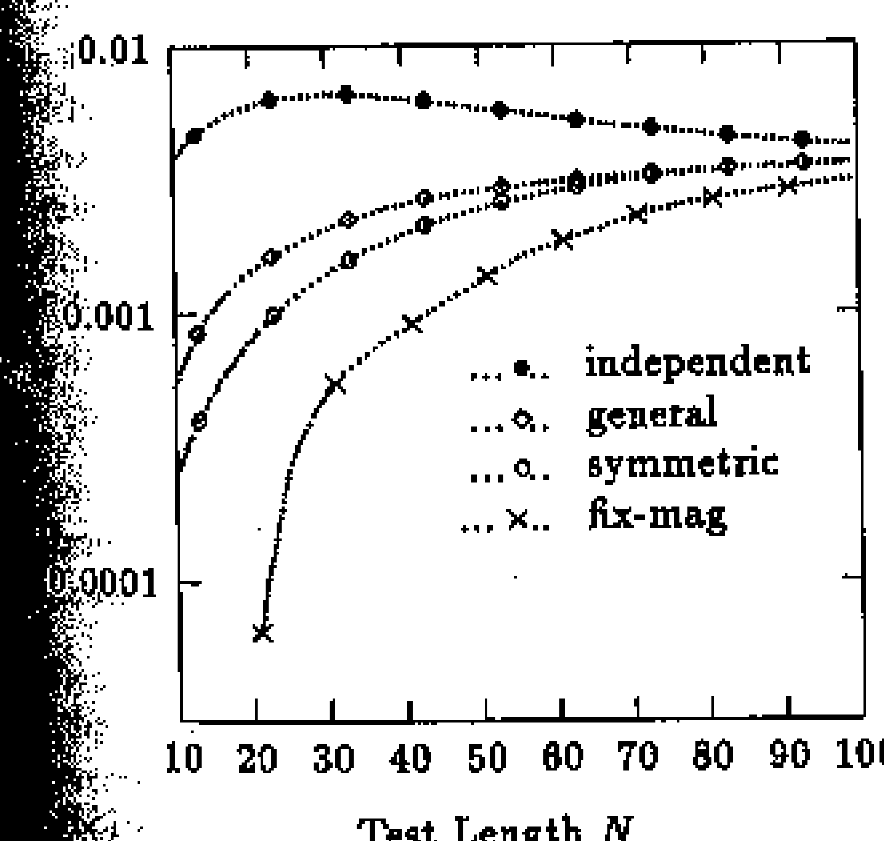


Figure 11: Aliasing probability for alu4

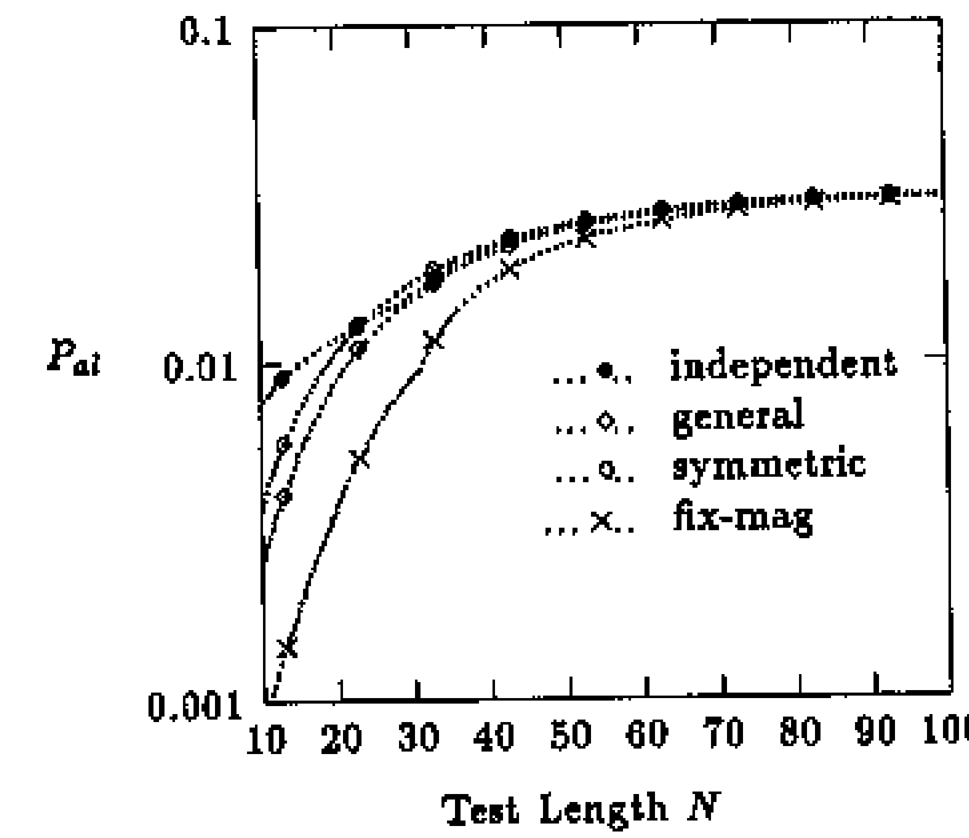


Figure 12: Aliasing probability for clip

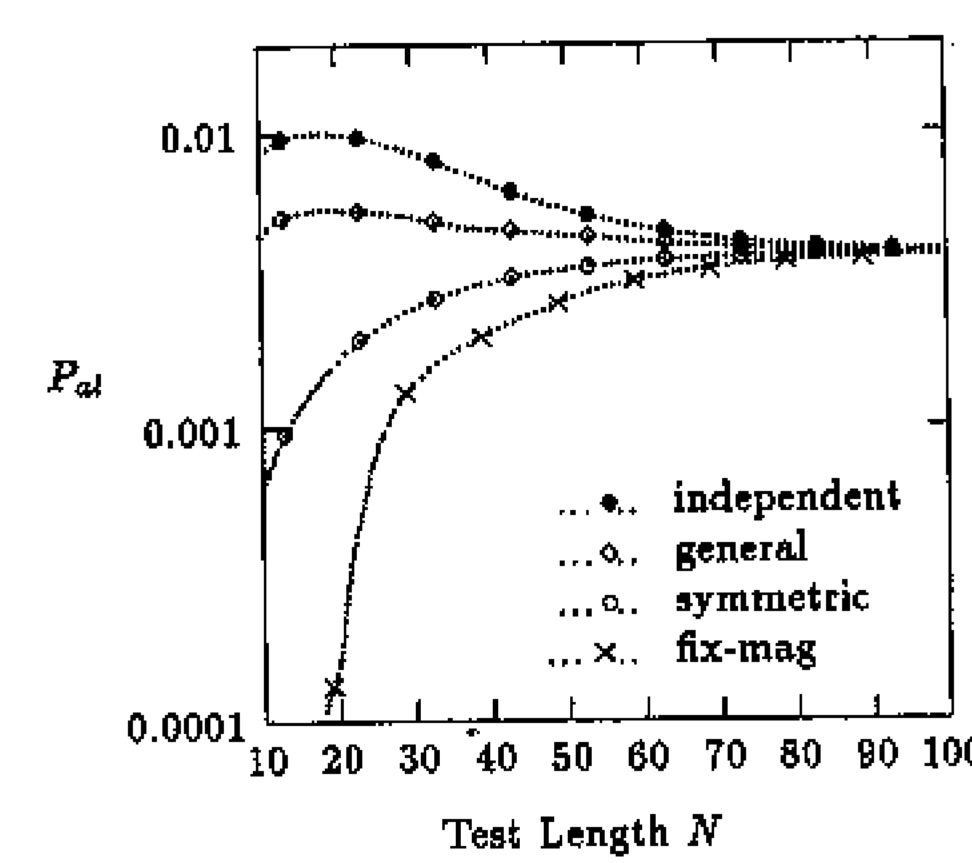


Figure 13: Aliasing probability for vg2

Therefore, it is crucial to minimize the probability of misdiagnosis like the probability of aliasing.

Following presents results for estimating the probability of misdiagnosis. Probability of misdiagnosis is defined as the probability that two faults produce the same faulty signature. This is therefore analogous to the aliasing concept.

In the following, we assume the STUMPS organization, shown in Figure 7. Further, we assume only one channel (Field Replaceable Unit (FRU)) is faulty. Therefore, the question arises that given that errors are confined to a single input of MISR, what is the probability of correctly locating this fault?

Let the aliasing code for a signature analyzer be $AC = C(N, N-1)$, and the good circuit signature be $S$. The probability of misdiagnosis $P_{md}$ is the probability that two faults produce the same erroneous signature $S^f$. Let $W_C^{S^f}(z_0, z_1, \ldots, z_{2^m-1})$ be the weight enumerators of the coset $C(N, N-1) + S^f + S$ of the code $C(N, N-1)$. The following theorem gives the probability of misdiagnosis. Note that for the special case when $S^f = S$, this reduces to aliasing probability $P_{al}$.

**Theorem 6** *Let $N$ be the number of tests applied to an $m$-output circuit, and let the good circuit signature be $S$. The probability of misdiagnosis when the faulty circuit signature is $S^f$, $P_{md}$, is given by*

$$P_{md} = W_C^{S^f}(p_0, p_1, \ldots, p_{2^m-1}) \qquad (9)$$

*where, $W_C^{S^f}(z_0, z_1, \ldots, z_{2^m-1})$ is the complete weight enumerator of the coset $C(N, N-1) + S^f + S$ of the aliasing code $C(N, N-1)$.*

In the following, we will present an example of application of Theorem 5 to obtain a closed form expression for $P_{md}$ given $S^f \neq S$. We assume that the number of tests applied $N = 2^m - 1$. The error model used here is appropriately the fixed magnitude error model. In a multi-chip environment, the global test is usually conducted using STUMPS [1] (Figure 7). In that case, this error model is accurate as a faulty chip can produce erroneous results only at a single input to the MISR. Diagnosis can then be performed to identify the faulty chip.

In Theorem 5, the weight enumerator of the $(2^m - 1, 2^m - m - 1)$ binary Hamming code was used to compute the aliasing probability $P_{al}$ for the fixed error magnitude. Similarly, the weight enumerator of the coset of the Hamming code can be used to compute the probability of misdiagnosis.

The weight distribution of the coset $S^* \neq 0$ of the $(2^m - 1, 2^m - m - 1)$ binary Hamming code is given by [13]:

$$A_i^{S^*} = \frac{1}{2^m - 1}\left(\binom{2^m - 1}{i} - A_i\right)$$

for any $S^* = S^f + S$ and $A_i$ is the weight distribution of the binary Hamming code.

**Theorem 7** *For $N = 2^m - 1$, we have for the probability of misdiagnosis for any $S^f \neq 0$, for errors of a given magnitude,*

$$P_{md} = \frac{1}{2^m - 1}\left(1 - 2^{-m}(1 + (2^m - 1)(1 - 2p)^{2^{m-1}})\right) \qquad (10)$$

Note that for MISRs of size $m \geq 6$, this value is of the order of $2^{-m}$. Hence, this theorem shows that if a STUMPS approach is used, the probability that two faults will lead to the same faulty signature is quite low. This indicates that fault dictionaries can be quite effective as there is little chance of locating the fault to the wrong FRU.

## 6 Conclusions

In the paper, a framework is developed which can be used to analyze aliasing in the compression of test responses, using MISRs with primitive feedback polynomials. The two limitations that the earlier techniques suffered from were their lack of generality with respect to the test length, and error models. This paper presents a method which can compute the aliasing probability for any test length for any error model.

A number of commonly used error models are studied. A very general error model is presented which subsumes all these models.

Closed form solutions have been derived for different error models and test lengths. These indicate that the aliasing probability for a $m$ bit MISR is the *same* no matter *which* primitive feedback polynomial is used. Aliasing probability is computed for various error models for some benchmark circuits. For many benchmark circuits, the *independent* error model provides *maximum* estimation of aliasing, and the $2^m$-ary *symmetric* model provides *minimum* estimations.



The coding theory framework is then extended to study the probability of misdiagnosis, when the faulty signatures are used to locate the faulty FRU in a STUMPS environment. It is shown that the probability of *misdiagnosis* in a STUMPS environment can be quite *low*.

## Acknowledgement

The authors would like to thank Dr. L.B. Levitin of Boston University, Boston MA, for many helpful discussions.

## References

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

[2] Blake, I.F. and Kith, K., "On the complete weight enumerator of Reed-Solomon codes," Proceedings of the Conference on Information Sciences and Systems, Princeton, NJ, 1990.

[3] Damiani, M. et al., "An Analytical Model for the Aliasing probability in Signature Analysis Testing," IEEE Trans. CAD, vol. 8, no. 11, November 1989, pp. 1133–1144.

[4] Damiani, M. et al., "Aliasing in Signature Analysis Testing with Multiple Input Shift Registers," IEEE Transactions on CAD, Vol. 9, No. 12, pp. 1344-1353, December 1990.

[5] Gupta, S.K. and Pradhan, D.K., "A New Framework for Designing & Analyzing BIST Techniques: Computation of Aliasing Probability," Proceedings of International Test Conference, pp. 329-341, 1988.

[6] Ivanov, I. and Agrawal, V.K., "An Iterative Technique for Calculating Aliasing Probability of Linear Feedback Shift Registers," Proc. of the 18th International Symposium on Fault Tolerant Computing, Tokyo, Japan, 1988.

[7] Iwasaki, K. and Arakawa, F., "An Analysis of the Aliasing Probability of Multiple Input Signature Registers in the Case of a $2^m$-ary Symmetric Channel," IEEE Trans. on CAD, Vol. 9, No. 4, pp. 427-438, April 1990.

[8] Iwasaki, K. and Yamaguchi, N., "Design of Signature Circuits Based on Weight Distributions of Error-Correcting Codes," Proc. Int. Test Conf. 1990.

[9] Kasami, T. and Lin, S., "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 $(x-\alpha)(x-\alpha^2)(x-\alpha^3)$," Journal of Linear Algebra and Its Applications, vol. 98, 1988, pp. 291-307.

[10] Karpovsky, M.G., Finite Orthogonal Series in the Design of Digital Devices, Academic Press, 1976.

[11] Karpovsky, M.G. (Ed.), Spectral Techniques and Fault Detection, Academic Press, 1985.

[12] Karpovsky, M.G., Gupta, S.K. and Pradhan, D.K., "Aliasing and Diagnosis Probability in MISR and STUMPS Using a General Error Model," Technical Report TR-91-CSE-42, Elec. and Comp. Engg Dept., University of Massachusetts, Amherst, Jul. 1991.

[13] MacWilliams, F.J. and Sloane, N.J.A., Theory of Error-Correcting Codes, North-Holland Publishing, 1978.

[14] Pradhan, D.K. (ed.), Fault Tolerant Computing: Theory and Techniques, Prentice Hall, NJ, 1986.

[15] Pradhan, D.K. and Gupta, S.K., "A Framework for Designing and Analyzing New BIST Techniques and Zero Aliasing Compression," IEEE Trans. on Computers, Vol. 40, no. 6, pp. 743-763, June 1991.

[16] Pradhan, D.K., Gupta, S.K. and Karpovsky, M.G., "Aliasing Probability for Multiple Input Signature Analyzer," IEEE Trans. on Computers, April 1990, vol. 39, no. 4, pp. 586–591.

[17] Robinson, J.P. and Saxena, N.R, "A Unified View of Test Compression Methods," IEEE Trans. on Computers, Vol. C-36, No. 1, pp. 94–99, Jan 1987.

[18] Sridhar, T. et al., "Analysis and Simulation of Parallel Signature Analyzers," Proceedings of International Test Conference, pp. 656-661, 1982.

[19] Williams, T.W., Daehn, A., Gruetzner, M. and Starke, C.W., "Aliasing Errors in Signature Analysis Registers," IEEE Design & Test of Computers, Vol. C-36, No. 4, pp. 39-45, Apr 1987.

[20] Williams, T.W. and Daehn, W., "Aliasing Errors in Multiple Input Signature Analysis Registers," Proceeding of the European Test Conference, pp. 338-345, 1988.