設計自動化 72－14
（1994. 10. 28）

ビット毎に誤り率が異なるMISRのエイリアス確率と完全重み分布

岩崎 一彦† 中村重男† 嵩忠雄††

†千葉大学工学部情報工学科
〒263千葉市稲毛区弥生町1-33

††奈良先端科学技術大学院大学
〒630-01奈良県生駒市高山町8916-5

あらまし シンボル毎に誤り率が異なるようなテスト応答に対して，MISRのエイリアス確率を解析した．ガロア体上の線形符号およびその双対符号の完全重み分布を適用した．Damianiらによって別の方法で得られている結果と一致した．

和文キーワード：組込み自己テスト，MISR，エイリアス確率，完全重み分布

Aliasing Probability of MISRs with Different Error Probability for Each Input Using Complete Weight Distribution

Kazuhiko Iwasaki† Shigeo Nakamura† Tadao Kasami††

†Chiba University, Faculty of Engineering
Inage, Chiba 263, Japan

††Nara Institute of Science and Technology
Ikoma, Nara 630-01, Japan

Abstract The aliasing probability is analyzed for MISRs when the error probability of symbols in a test response is different. The complete weight distributions of linear codes over a Galois field and its dual codes are applied. The expression obtained is exactly the same to that derived by Damiani using the different technique.

英文 key words: BIST, MISR, aliasing probability, complete weight distribution

INTRODUCTION

Built-In Self-Test (BIST) is one of the key techniques to overcome VLSI test difficulties [1]. For example, BIST has been applied to commercial VLSI processors [2]-[4].

One of drawbacks of the BIST is an aliasing error. Many works have been done to analyze the aliasing probability of single-input linear feedback shift registers. In addition, the aliasing probability of multiple input signature registers (MISRs) has been analyzed for various error models such as the 2^m-ary symmetric channel [5],[6], the binary symmetric channel [7]-[9], and the time dependent error model [10],[11].

One of the works is to analyze the aliasing probability of MISRs when each error symbol has different error probability [12]-[14]. The error probability is assumed to be time independent. In this manuscript, we derive exactly the same expression in [12],[13] by applying the complete weight distributions of linear codes.

DEFINITIONS

Notations in [15] are used in this manuscript. Some notations are from [16],[17]. Let the elements of GF(q) be denoted by $\alpha_0 = 0, \alpha_1, \alpha_2, \ldots, \alpha_{q-1}$, where $q = p^m$ and p is a prime. Let t_i be the number of α_i $(0 \le i \le q - 1)$ in a vector **v** over V^n $(=GF(q)^n)$.

Consider a linear (n, n - k) code C over GF(q). Let $A(t_0, t_1, \ldots, t_{q-1})$ be the number of code words that consists of $t_0\ \alpha_0, t_1\ \alpha_1, \ldots, t_{q-1}\ \alpha_{q-1}$ $(0 \le t_i \le n)$. The complete weight enumerator, $W_C(z_0, z_1, \ldots, z_{q-1})$, is defined as follows:

$$W_C(z_0, z_1, \cdots, z_{q-1})$$
$$= \sum_{t_0=0}^{q-1} \sum_{t_1=0}^{q-1} \cdots \sum_{t_{q-1}=0}^{q-1} A(t_0, t_1, \ldots, t_{q-1}) z_0^{t_0} z_1^{t_1} \cdots z_{q-1}^{t_{q-1}}$$
$$= \sum_{v \in C} z_0^{t_0} z_1^{t_1} \cdots z_{q-1}^{t_{q-1}}.$$

Consider a complex number ξ as

$$\xi = \cos(2\pi/p) + \sqrt{-1}\sin(2\pi/p).$$

The following equation holds.

$$\xi^p = 1.$$

For $GF(2^m)$, that is $p = 2$, $\xi = -1$.

Let a base of GF(q) be denoted by $\beta_0, \beta_1, \ldots, \beta_{m-1}$. Any element $\mathbf{a} \in GF(q)$ can be expressed as a linear combination of the basis as shown below.

$$\mathbf{a} = a_0\beta_0 + a_1\beta_1 + \ldots + a_q\beta_{q-1}.$$

Define an operator $x(\mathbf{a})$, $\forall \mathbf{a} \in GF(q)$ as

$$x(\mathbf{a}) = \xi^{a_0}.$$

The following expression is said to be an Hadamard translation. For $\mathbf{u} \in V^n$,

$$\hat{F}(\mathbf{u}) = \sum_{v \in V^n} x(\mathbf{u} \cdot \mathbf{v}^T) F(\mathbf{v}).$$

MacWilliams identity for the complete weight distribution can be expressed as follows [15],[16].

$$W_C(z_0, z_1, \cdots, z_{q-1})$$
$$= q^{-k} W_{C^\perp}(z'_0, z'_1, \cdots, z'_{q-1}),$$

where

$$z'_h = \sum_{j=0}^{q-1} x(\alpha_h \alpha_j) z_j.$$

That is,

$$\sum_{v \in C} z_0^{t_0} z_1^{t_1} \cdots z_{q-1}^{t_{q-1}}$$
$$= q^{-k} \sum_{v \in C^\perp} z'^{t_0}_0 z'^{t_1}_1 \cdots z'^{t_{q-1}}_{q-1}.$$

Since $z_0 = 0$, $x(\alpha_0\alpha_j) = x(0) = 1$ $(0 \le j \le q - 1)$. Therefore,

$$z'_0 = z_0 + z_1 + \cdots + z_{q-1}.$$

Substituting $Pr(z_i)$ into z_i $(0 \le i \le q - 1)$ the following equation is obtained.

$$z'_0 = Pr(z_0) + Pr(z_1) + \cdots + Pr(z_{q-1})$$
$$= 1.$$

Consider a BIST system depicted in Fig. 1. Let p_i be the probability that the i-th input is erroneous, where $0 \le i \le m - 1$. Under this model, the probabilities for each symbol are as follows.

$$Pr(000\cdots0) = (1 - p_0)(1 - p_1)(1 - p_2)\cdots(1 - p_{m-1}),$$
$$Pr(100\cdots0) = p_0(1 - p_1)(1 - p_2)\cdots(1 - p_{m-1}),$$
$$\cdots$$
$$Pr(111\cdots1) = p_0p_1p_2\cdots p_{m-1}.$$

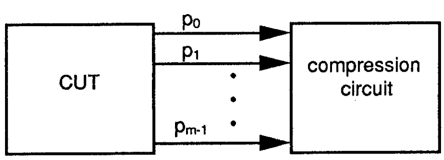


Fig. 1. A BIST system. The error probability for each input is different and time independent.

Let the binary representation for $z_0, z_1, \ldots, z_{m-1}$ be as follows.

$$z_1 = (1, 0, \cdots, 0, 0),$$
$$z_2 = (0, 1, \cdots, 0, 0),$$
$$\vdots$$
$$z_{m-1} = (0, 0, \cdots, 0, 1).$$

For $q = 2^m$ the following equation holds. This could be proved by the similar induction technique used in [12],[13].

$$z'_1 = 1 - 2Pr(z_1),$$
$$z'_2 = 1 - 2Pr(z_2),$$
$$\vdots$$
$$z'_{m-1} = 1 - 2Pr(z_{m-1}).$$

The binary symmetric channel is a special case, where $p_0 = p_1 = p_2 = \dots = p_{m-1} = p$.

SINGLE MISRS

Consider a linear compression circuit depicted in Fig. 2. The state transition matrix can be expressed by a binary m×m matrix T. Then the signature S is expressed as

$$S = a_0 + a_1 T + \cdots + a_{n-2}T^{n-2} + a_{n-1}T^{n-1},$$

where $a_0, a_1, \dots, a_{n-1}$ is a series of test response and n is the test length.

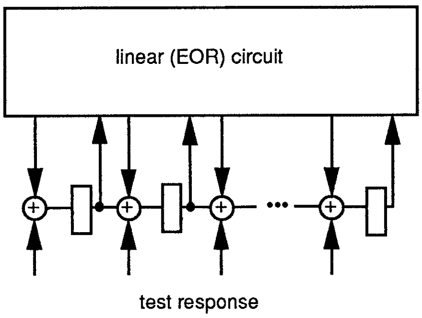


Fig. 2. A linear compression circuit.

If the matrix T is non-singular, there exists a companion matrix whose bottom row is as follows [18]:

$$1 \; g_1 \; g_2 \dots g_{m-1}$$

If the two MISR have the similar state transition matrix, that is the characteristic polynomials are exactly the same, the aliasing probability is exactly the same.

The aliasing error occurs if and only if the errors contained in the test response, $e_0, e_1, \dots, e_{n-1}$, is a code word in the (n, n - 1) linear code C whose parity check matrix is

$$H = \left[I \; T^T \left(T^2\right)^T \cdots \left(T^{n-1}\right)^T\right],$$

where n is the test length.

The aliasing probability can be expressed by using the complete weight distribution of the linear code or the dual code of the linear code. That is,

$$Pal(n) = W_C\left(Pr(z_0), Pr(z_1), \cdots, Pr(z_{2^m-1})\right) - Pr(z_0)^n$$

$$= \frac{1}{|C^\perp|} W_{C^\perp}\left(Pr(z'_0), Pr(z'_1), \cdots, Pr(z'_{2^m-1})\right) - Pr(z_0)^n$$

$$= 2^{-m} \sum_{v \in C^\perp} Pr(z'_0)^{t_0} Pr(z'_1)^{t_1} \cdots Pr(z'_{2^m-1})^{t_{2^m-1}} - Pr(z_0)^n.$$

The dual code $C^\perp$ contains one all-zero code word, that is expressed as $z'_0{}^n$. Since $z'_0 = 1$, the above expression is as follows.

$$Pal(n) = 2^{-m} + 2^{-m} \sum_{v \in C^\perp - 0} z'_0{}^{t_0} \cdots z'_{2^m-1}{}^{t_{2^m-1}} - Pr(z_0)^n.$$

Each symbol z'_i is expressed by a linear combination of the following basis

$$z'_1 = (1, 0, \cdots, 0, 0),$$
$$z'_2 = (0, 1, \cdots, 0, 0),$$
$$\vdots$$
$$z'_{m-1} = (0, 0, \cdots, 0, 1).$$

If the error probability of each input is different and time independent, $z'_1 = 1 - 2Pr(p_1)$, $z'_2 = 1 - Pr(p_2)$, ..., $z'_{m-1} = 1 - 2Pr(z_{m-1})$. Therefore, the expression in [12],[13], that is shown below, is exactly the same to that shown in the above.

$$AEP(n) = \frac{1}{2^m} + \frac{1}{2^m} \sum_{i=1}^{2^m-1} \left(\prod_{j=1}^{m} (1 - 2p_j)^{w_j(i,n)} \right) - p_0^n,$$

where $w_j(i, n)$ is the number of ones appeared at the j-th stage starting from the state i.

Single MISR characterized by primitive polynomials

Consider a single MISR shown in Fig. 3, where the MISR is characterized by a primitive polynomial g(x):

$$g(x) = 1 + g_1 x + g_2 x^2 + \cdots + g_{m-1}x^{m-1} + x^m.$$

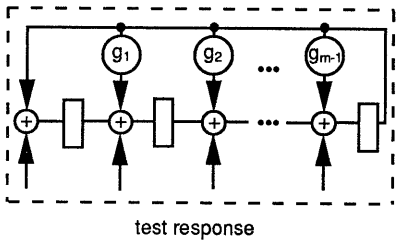


Fig. 3. A single MISR.

If the g(x) is primitive, the aliasing error occurs if and only if the error in the test response is a code word in the (n, n - 1) Reed-Solomon (RS) code generated by (x - α), where α is a primitive element of $GF(2^m)$. The parity check matrix of the code is expressed as follows.

$$H = \left[1 \; \alpha \; \alpha^2 \cdots \alpha^{n-1}\right].$$

The dual code is generated by the above matrix. Therefore, code words of the dual code can be listed as following.

$$\begin{gathered} 0\,0\,0 \cdots 0, \\ 1\ \alpha\ \alpha^2 \cdots \alpha^{n-1}, \\ \alpha\ \alpha^2\ \alpha^3 \cdots \alpha^n, \\ \cdots \\ \alpha^{-1}\ 1\ \alpha \cdots \alpha^{n-2}. \end{gathered}$$

The binary representation for each code word can be obtained by substituting the binary representation into each symbol. For $n = 2^m - 1$, that is the code is not shortened, the weight distribution of the dual code can be expressed as follows.

$$W_{C^\perp}(z'_0, z'_1, \cdots, z'_{2^m-1}) = {z'_0}^n + (2^m - 1) z'_0 z'_1 \cdots z'_{2^m-1}.$$

The aliasing probability for the MISR characterized by $(x - \alpha)$ can be expressed as follows for the test length $n = 2^m - 1$.

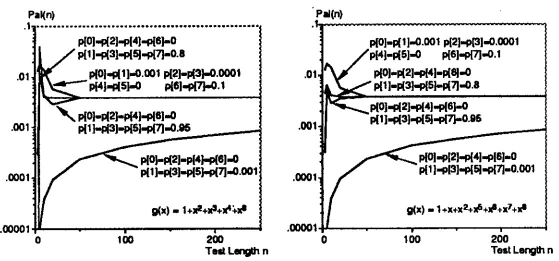
$$\begin{aligned} Pal(n) &= 2^{-m} W_{C^\perp}\big(Pr(z'_0), Pr(z'_1), \cdots, Pr(z'_{2^m-1})\big) - Pr(z_0)^n \\ &= 2^{-m} + 2^{-m}(2^m - 1)\big((1 - 2p_1)(1 - 2p_2) \cdots (1 - 2p_{m-1})\big)^{2^{m-1}} \\ &\quad - \big((1 - p_1)(1 - p_2) \cdots (1 - p_{m-1})\big)^n. \end{aligned}$$

For the bianry represntation of the code words in the dual code the number of ones is $2^m - 1$ for each bit position.

Example 1

Fig. 4 shows the aliasing probabilities for MISRs characterized by the following primitive polynomials.

$$g_1(x) = 1 + x^2 + x^3 + x^4 + x^8,$$
$$g_2(x) = 1 + x + x^2 + x^5 + x^6 + x^7 + x^8.$$



(a) (b)

Fig. 3. The aliasing probability of MISRs.
(a) characterized by $g_1(x) = 1 + x^2 + x^3 + x^4 + x^8$,
(b) characterized by $g_2(x) = 1 + x + x^2 + x^5 + x^6 + x^7 + x^8$.

Single MISRs characterized by non-primitive polynomials

IF g(x) is a non-primitive polynomial, the aliasing error occurs if and only if the error in the test response is a code word in the linear (n, n - 1) code whose parity check matrix is follows.

$$H = \left[I\ T^T\ (T^2)^T \cdots (T^{n-1})^T\right].$$

The complete weight distribution can be calculated as following. For each element in $GF(2^m)$, multiply the binary representation of the element with the above parity check matrix. Collecting the multiplications for 2^m elements, the complete weight distribution can be obtained.

Example 2

Consider single MISRs characterized by the following primitive polynomial

$$g_3(x) = 1 + x + x^3,$$

and the following non-primitive polynomials.

$$g_4(x) = 1 + x + x^2 + x^3,$$
$$g_5(x) = 1 + x^3.$$

The state transition matrix for $g_3(x)$, $g_4(x)$ and $g_5(x)$ is as follows.

$$T_3 = \begin{pmatrix} 0&1&0 \\ 0&0&1 \\ 1&1&0 \end{pmatrix},\ T_4 = \begin{pmatrix} 0&1&0 \\ 0&0&1 \\ 1&0&0 \end{pmatrix},\ T_5 = \begin{pmatrix} 0&1&0 \\ 0&0&1 \\ 1&1&1 \end{pmatrix}.$$

Since the periods of $g_3(x)$, $g_4(x)$, and $g_5(x)$ are 7, 4, and 3, the test lengths n_3, n_4, and n_5 are assumed to be the multiple of the periods, respectively. Let the code generated by $g_3(x)$, $g_4(x)$ and $g_5(x)$ be C_3, C_4, and C_5, respectively. The parity check matrixes for C_3, C_4, and C_5 are as follows for $n_3 = 7$, $n_4 = 4$, and $n_5 = 3$, respectively.

$$H_3 = \begin{bmatrix} 100 & 010 & 001 & 110 & 011 & 111 & 101 \\ 010 & 001 & 101 & 011 & 111 & 101 & 100 \\ 001 & 110 & 100 & 111 & 101 & 100 & 010 \end{bmatrix},$$

$$H_4 = \begin{bmatrix} 100 & 001 & 011 & 110 \\ 010 & 101 & 010 & 101 \\ 001 & 011 & 110 & 100 \end{bmatrix},$$

$$H_5 = \begin{bmatrix} 100 & 001 & 010 \\ 010 & 100 & 001 \\ 001 & 010 & 100 \end{bmatrix}.$$

Let the binary representation of $z_0, z_1, \ldots, z_7$ $(z'_0, z'_1, \ldots, z'_7)$ be as follows. They are characterized by $g_3(x)$.

$$\begin{aligned} z_0 &= 0 = (0, 0, 0), \\ z_1 &= 1 = (1, 0, 0), \\ z_2 &= \alpha = (0, 1, 0), \\ z_3 &= \alpha^2 = (0, 0, 1), \\ z_4 &= \alpha^3 = (1, 1, 0), \\ z_5 &= \alpha^4 = (0, 1, 1), \\ z_6 &= \alpha^5 = (1, 1, 1), \\ z_7 &= \alpha^6 = (1, 0, 1). \end{aligned}$$

The symbols in the MacWilliams identity $z'_0, z'_1, \ldots, z'_7$ can be expressed using $z_0, z_1, \ldots, z_7$ as shown in the previous section. The expression "$\alpha_h \alpha_j$" is considered as the inner product of the binary representation of α_h and α_j. This is because the parity check matrix for the MISR characterized by a non-primitive polynomial is expressed by a binary matrix instead of a matrix over $GF(2^m)$. As a binary code, the inner product shows the duality.

$$\begin{aligned}
z'_0 &= z_0 + z_1 + z_2 + z_3 + z_4 + z_5 + z_6 + z_7,\\
z'_1 &= z_0 - z_1 + z_2 + z_3 - z_4 + z_5 - z_6 - z_7,\\
z'_2 &= z_0 + z_1 - z_2 + z_3 - z_4 - z_5 - z_6 + z_7,\\
z'_3 &= z_0 + z_1 + z_2 - z_3 + z_4 - z_5 - z_6 - z_7,\\
z'_4 &= z_0 - z_1 - z_2 + z_3 + z_4 - z_5 + z_6 - z_7,\\
z'_5 &= z_0 + z_1 - z_2 - z_3 - z_4 + z_5 + z_6 - z_7,\\
z'_6 &= z_0 - z_1 - z_2 - z_3 + z_4 + z_5 - z_6 + z_7,\\
z'_7 &= z_0 - z_1 + z_2 - z_3 - z_4 - z_5 + z_6 + z_7.
\end{aligned}$$

The complete weight distributions of the codes generated by H_3, H_4, and H_5 are as follows.

$$W_{C_3^\perp} = z'^{7n_3}_0 + 7(z'_1z'_2z'_3z'_4z'_5z'_6z'_7)^{n_3},$$

$$W_{C_4^\perp} = z'^{4n_4}_0 + 4(z'_1z'_3z'_4z'_5)^{n_4} + 2(z'^2_2z'^2_7)^{n_4} + z'^{4n_4}_6,$$

$$W_{C_5^\perp} = z'^{3n_5}_0 + 3(z'_1z'_2z'_3)^{n_5} + 3(z'_4z'_5z'_7)^{n_5} + z'^{4n_5}_6.$$

For example, assume that only the error pattern $z_7 = (1, 0, 1)$ occurs. That is

$$\begin{gathered}
Pr(z_0) = 1 - Pr(z_7),\\
Pr(z_1) = Pr(z_2) = Pr(z_3) = Pr(z_4) = Pr(z_5) = Pr(z_6) = 0,\\
Pr(z_7) \neq 0.
\end{gathered}$$

By substituting each probability into a previous equation,

$$\begin{aligned}
z'_0 &= 1,\\
z'_1 &= 1 - 2Pr(z_7),\\
z'_2 &= 1,\\
z'_3 &= 1 - 2Pr(z_7),\\
z'_4 &= 1 - 2Pr(z_7),\\
z'_5 &= 1 - 2Pr(z_7),\\
z'_6 &= 1,\\
z'_7 &= 1.
\end{aligned}$$

By substituting the above equations into the complete weight enumerators of the dual codes, the following expressions can be obtained.

$$W_{C_3^\perp} = 1 + 7(1 - 2Pr(z_7))^{4n_3},$$

$$W_{C_4^\perp} = 1 + 4(1 - 2Pr(z_7))^{4n_4} + 2 + 1,$$

$$W_{C_5^\perp} = 1 + 3(1 - 2Pr(z_7))^{2n_5} + 3(1 - 2Pr(z_7))^{2n_5} + 1.$$

The aliasing probability for the condition is expressed as follows.

$$Pal(n)_{g_3} = 1/8(1 + 7(1 - 2Pr(z_7))^{4n_3}),$$

$$Pal(n)_{g_4} = 1/8(4 + 4(1 - 2Pr(z_7))^{4n_4}),$$

$$Pal(n)_{g_5} = 1/8(2 + 6(1 - 2Pr(z_7))^{2n_5}).$$

Since $-1 < (1 - 2Pr(z_7)) < 0$, $(1 - 2Pr(z_7))^n$ converges to zero for a large n. From the above equations, the aliasing probability of the MISRs characterized by g_3, g_4 and g_5 converges to 1/8, 1/2, and 1/4 for a long test length, respectively. This can be confirmed by a state transition diagram. The state transition diagrams are shown in Fig. 5 for each MISR.

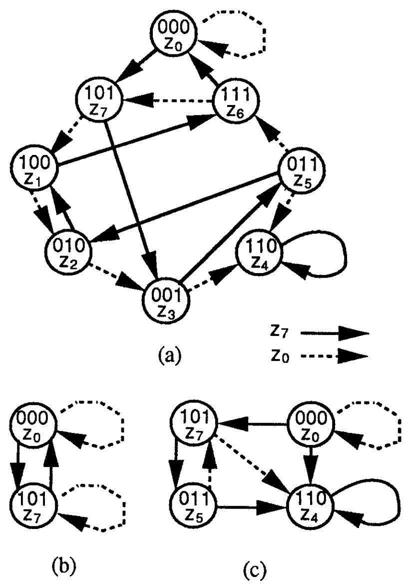


Fig. 5. The state transition diagrams for MISRs when only the error $z_7 = (1, 0, 1)$ occurs. (a) characterized by $1 + x + x^3$. (b) characterized by $1 + x + x^2 + x^3$. (c) characterized by $1 + x^3$.

MULTIPLE MISRS

Consider a multiple MISR depicted in Fig. 6, where the signature circuit consists of d MISRs. The aliasing error occurs if and only if the error in the test response is a code word in the RS code generated by $(x - \alpha^b)(x - \alpha^{b+1}) \cdots (x - \alpha^{b+d+1})$.

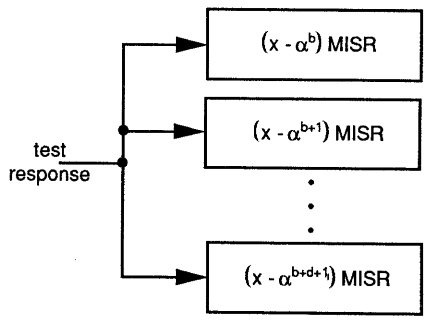


Fig. 6. Multiple MISR.

The parity check matrix for the RS code is as follows.

$$H = \begin{bmatrix} I & \alpha^b & \alpha^{2b} & \cdots & \alpha^{(n-1)b} \\ I & \alpha^{b+1} & \alpha^{2(b+1)} & \cdots & \alpha^{(n-1)(b+1)} \\ & & & \cdots & \\ I & \alpha^{b+d+1} & \alpha^{2(b+d+1)} & \cdots & \alpha^{(n-1)(b+d+1)} \end{bmatrix}.$$

Aliasing probability for this multiple MISR can be expressed by using the similar technique for the single MISR. That is as follows.

$$\begin{aligned} Pal(n) &= W_C(Pr(z_0), Pr(z_1), \cdots, Pr(z_{2^m-1})) - Pr(z_0)^n \\ &= 2^{-dm} W_{C^\perp}(Pr(z'_0), Pr(z'_1), \cdots, Pr(z'_{2^m-1})) - Pr(z_0)^n \\ &= 2^{-dm} + 2^{-dm} \sum_{v \in C^\perp - 0} Pr(z'_0)^{t_0} \cdots Pr(z'_{2^m-1})^{t_{2^m-1}} - Pr(z_0)^n. \end{aligned}$$

The complete weight distribution can be calculated as following. For each vector in $GF(2^m)^d$, multiply the vector with the parity check matrix H, resulting in the code word in the dual code, $C^\perp$, of the RS code generated by $(x - \alpha^b)(x - \alpha^{b+1}) \cdots (x - \alpha^{b+d+1})$.

Fig. 7 shows examples of the aliasing probability for double MISRs

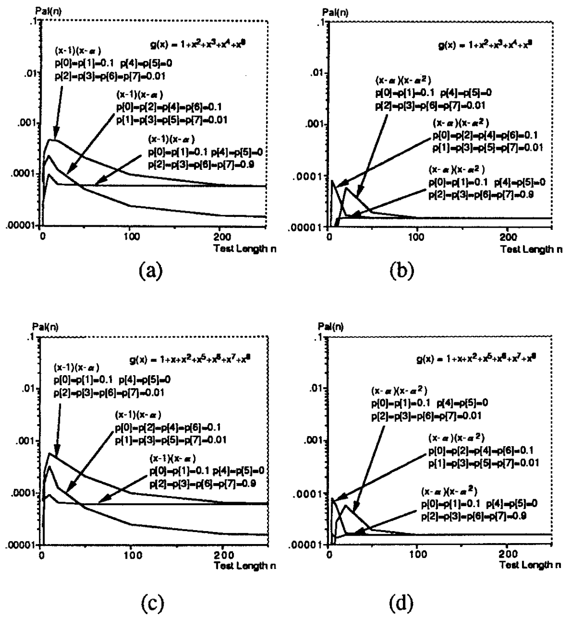


Fig. 7. The aliasing probability of double MISRs. (a) $(x - 1)(x - \alpha)$, $g(x) = 1 + x^3 + x^4 + x^5 + x^8$, (b) $(x - \alpha)(x - \alpha^2)$, $g(x) = 1 + x^3 + x^4 + x^5 + x^8$, (c) $(x - 1)(x - \alpha)$, $g(x) = 1 + x + x^2 + x^5 + x^6 + x^7 + x^8$, (d) $(x - \alpha)(x - \alpha^2)$, $g(x) = 1 + x + x^2 + x^5 + x^6 + x^7 + x^8$.

The binary weight enumerator is shown for RS code for d = 1, 2, 3, and 4 [19]. And the complete weight enumerator is shown for RS code for d = 1, 2, 3, and 4 [20].

CONCLUSIONS

The aliasing probability was analyzed for MISRs when the error probability for each symbol is different. The complete weight distributions of linear codes over a Galois field and its dual codes were applied. The expression obtained is exactly the same to that derived by Damiani using the different technique.

Acknowledgments The authors would like to thank Mr. Hiroyuki Goto for his programming efforts.

References

[1] P. Bardell, W. McAnney and J. Savir, *Built-In Self-Test for VLSI*, John Wiley, 1987.

[2] R. Patel and K. Yarlagadda, "Testability features of the SuperSPARC microprocessor," *ITC'93*, pp. 773-781, 1993.

[3] J. Broseghini and D. H. Lenhert, "An ALU based programmable MISR/pseudorandom generator for a MC68HC11 family self-test," *ITC'93*, pp. 349-358, 1993.

[4] V. D. Agrawal, C. R. Kime, and K. K. Saluja, "A tutorial on Built-In Self-Test, Part 2: Applications," *IEEE Design & Test of Comput.*, 10, 2, pp. 69-77, June 1993.

[5] K. Iwasaki and F. Arakawa, "An analysis of aliasing probability of multiple input signature registers in the case of 2^m-ary symmetric channel," *IEEE Trans. CAD/ICAS*, 9, 4, pp. 427-438, Apr. 1990.

[6] D. K. Pradhan, S. K. Gupta and M. G. Karpovsky, "Aliasing probability for multiple-input signature analyzer and a new compression technique," *IEEE Trans. Comput.*, 39, 4, pp. 586-591, Apr. 1990.

[7] K. Iwasaki and N. Yamaguchi, "Design of signature circuits based on weight distribution of error-correcting codes," *ITC'90*, pp. 779-785, Sept. 1990.

[8] K. Iwasaki, S. Feng, T. Fujiwara and T. Kasami, "Comparison of aliasing probability for multiple MISRs and M-stage MISRs with m inputs," *IEICE Trans. Info. and Systems*, E75-D, 6, pp. 835-841, Nov. 1992.

[9] D. K. Pradhan and S. K. Gupta, "A new framework for designing and analyzing BIST techniques and zero aliasing compression," *IEEE Trans. Comput.*, 40, 6, pp. 743-763, June 1991.

[10] T. Kameda, S. Pilarski and A. Ivanov, "Notes on multiple input signature analysis," *IEEE Trans. Comput.*, 42, 2, pp. 228-234, Feb. 1993.

[11] G. Edirisooriya and J. P. Robinson, "Time and space correlated errors in signature analysis," *VLSI Test Symposium*, pp. 275-281, Apr. 1993.

[12] M. Damiani, O. Olivo, M. Favalli, S. Ercolani, and B. Ricco, "Aliasing in signature analysis testing with multiple input shift registers," *IEEE Trans. CAD/ICAS*, 9, 2, pp. 1344-1353, Dec. 1990.

[13] M. Damiani, O. Olivo, and B. Ricco, "Analysis and design of linear finite state machine for signature analysis testing," *IEEE Trans. Comput.*, 40, 9, pp. 1034-1045, Sept. 1991.

[14] W. Daehn, T. W. Williams, K. D. Wagner, "Aliasing errors in linear automata used as multiple-input signature analyzers," *IBM J. R&D*, 34, 2/3, pp. 363-380, Mar./May 1990.

[15] T. Kasami, *Introduction to Information and Coding Theory*, Shokodo, 1989. (in Japanese)

[16] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, 1977.

[17] S. Lin and D. J. Costello, Jr., *Error Control Coding*, Prentice-Hall, 1983.

[18] M. Serra, T. Slater, J. C. Muzio, and D. M. Miller, "The analysis of one-dimensional linear cellular automata and their aliasing properties," *IEEE Trans. CAD/ICAS*, 9, 7, pp. 768-778, July 1990.

[19] 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 Algebra and Its Appl.*, 98, pp. 291-307, 1988.

[20] I. F. Blake and K. Kith, "On the complete weight enumerator of Reed-Solomon codes," *SIAM J. Disc. Math.*, 4, 2, pp. 164-171, May 1991.