設計自動化　59－1
（1991. 10. 8）

多重多入力シグネチャレジスタによるVLSI自己テストに関する一検討

森井　昌克†　　谷川　晃一†　　岩崎　一彦‡

†愛媛大学　工学部　情報工学科
‡千葉大学　工学部　情報工学科

あらまし： 最近，符号理論における重み分布と誤り見逃し確率の関係から署名解析法を見直し，エイリアス確率に関して有効な結果を得ている．特にMISR(Multiple Input Signature Register)に関してはGF(2^m)上のReed-Solomon(RS)符号との関係が指摘され，その重み分布に基づくエイリアス確率の研究が進められている．

従来，署名解析法では，αをGF(2^m)の原始元，bを非負の整数，RS符号の生成多項式を$(x-\alpha^b)(x-\alpha^{b+1})\cdots(x-\alpha^{b+d-2})$としたとき，多項式基底$(1,\alpha,\alpha^2,\cdots,\alpha^{m-1})$で展開した符号に基づく$d-1$重MISRが提案され，評価が行われてきた．しかしながら，多項式基底ではない他の基底で展開することによりエイリアス確率を低減させ得る可能性がある．本稿では特に，この展開基底とシグネチャ回路との関係，およびいくつかのシミュレーションを行い，エイリアス確率が低いという意味で優れた多重化MISRの構成を目的として考察を与える．

On VLSI built-in self-test using multiplex multiple-input signature registers

Masakatu MORII †, Kouichi TANIGAWA † *and* Kazuhiko IWASAKI ‡

† Department of Computer Science, Ehime University
Matsuyama, 790 Japan, TEL. +81-899-24-7111, ext.3704, TELEFAX +81-899-23-0682
E-mail mmorii@dpc.ehime-u.ac.jp *and* ktanigaw@dpc.ehime-u.ac.jp

‡ Department of Information and Computer Science, Chiba University
Chiba, 260 Japan, TEL. +81-472-51-1111, ext.3166, TELEFAX +81-472-51-7337
E-mail ntj3e00@cuipc.ipc.chiba-u.ac.jp

Abstract: An analysis of the aliasing probability is very important for VLSI built-in self-test(BIST). Also the search of BIST circuit(signature circuit) which have the aliasing pobability as possible as small is very interesting from both practical and theoretical points of view.

Recently the aliasing probability for MISR (Multiple Input Signature Register) based on Reed-Solomon(RS) codes over GF(2^m) are being investigated very actively. Assumming that the errors occur randomly in each bit, the aliasing probability can be analyzed using the binary weight distributions of RS codes.

This paper gives a few comments on the the aliasing probability and the binary weight distributions of RS codes. Especially we give a note on constracting MISR which have the aliasing probability as possible as small.

1 まえがき

VLSI の組み込み自己テスト法 [Fuji85][Lala88][Kino89] としての署名解析法 [Froh77][Smith80][Iwadare89] では，疑似ランダム系列の回路応答である出力系列を圧縮し，その圧縮系列と正常な回路の圧縮系列（署名）を比較することにより回路故障を検出している．したがって，実際には回路に故障があるにもかかわらず，故障を見逃す確率（エイリアス確率）が問題となる [WDGS86][WDGS88][IvaAga88][GupPra88][Iwasaki91a][DOFR89][SSMM90]．

最近，符号理論を応用してエイリアス確率の評価およびシグネチャ回路を提案することが行われている．特に効率的な誤り訂正符号としてよく知られている Hamming 符号，Reed-Solomon(RS) 符号およびそれらの短縮符号の誤り見逃し確率からシグネチャ回路のエイリアス確率を評価することが提案されている [Iwasaki89][IwaNi88][HuFeKa90][PrGu90]．

シグネチャ回路として単一入力シフトレジスタ (Single Input Signature Register, SISR)，あるいは多入力シフトレジスタ (Multiple Input Signature Register, MISR) が用いられる [WilDae89][DaWiWa90][DOFER89]．MISR を用いる場合，検査回路の出力中に生起する誤りパターンの仮定として，1 タイムスロットにおける出力 m ビットの各誤りパターンが独立かつ等確率に生起するという立場と，タイムスロットに対して無関係に各ビットが独立かつ等確率に誤りを生起するという 2 者の立場を考えることができる．前者の誤りを見逃す確率をシンボルエイリアス確率，後者をビットエイリアス確率と呼ぶことにする．これらの立場は，符号理論において符号のシンボル誤りを問題にするか，あるいはビット誤りを問題にするかの選択に対応する．

岩崎は，代表的な誤り訂正符号である RS 符号に基づいた多重化 MISR を提案し，単一 MISR に関して，ビットエイリアス確率が $GF(2^m)$ 上の RS 符号の 2 元重み分布に帰着される事を指摘した [IwaYa88][Iwasaki90]．また，更に RS 符号の 2 元重み分布を求めることにより，いくつかの多重化 MISR のビットエイリアス確率を導出している．しかしながら，RS 符号の 2 元重み分布は，特殊な場合を除いて知られていない．また理論上，求められている場合も実際に値を求めるのは容易ではない．

一般に GF(2^m) 上の RS 符号は，GF(2) 上の GF(2^m) の基底を用いて 2 元展開され，その採用する基底によって RS 符号の 2 元重み分布が異なることが示されている．また，逆に任意の RS 符号の 2 元重み分布が等しくなる基底のクラスを導出し，そのクラスの総数についての評価が与えられている [MoToKa87][MoTa90]．

従来，署名解析法では，α を GF(2^m) の原始元，b を非負の整数，RS 符号の生成多項式を $(x-\alpha^b)(x-\alpha^{b+1})\cdots(x-\alpha^{b+d-2})$ としたとき，多項式基底 $(1,\alpha,\alpha^2,\cdots,\alpha^{m-1})$ で展開した符号に基づく $d-1$ 重 MISR が提案され，評価が行われてきた．しかしながら，多項式基底ではない他の基底で展開することにより，RS 符号の誤り見逃し確率，すなわちエイリアス確率を低減させ得る可能性がある．本稿では，この展開基底とシグネチャ回路との関係，およびシミュレーションを行い，エイリアス確率が低いという意味で多項式基底よりも優れた基底が存在することを示し，そのシグネチャ回路を導出する．さらにシミュレーションの結果からエイリアス確率が低いという意味で優れた多重化 MISR の構成法について考察を与える．

2 MISR による署名解析法

2.1 テスト応答圧縮回路としての MISR

署名解析法では，被テスト回路 (CUT) にテスト系列としての疑似ランダム系列を入力し，その回路応答系列から故障を検出する．回路応答系列長は，CUT の入力ピン数に対して指数関数的に増加するので，LFSR 等で圧縮し，その圧縮系列と正常な回路の圧縮系列を比較することにより故障を検出している． MISR は回路応答系列を圧縮する多入力 LFSR であり，例えば図 1 のような回路で与えられる．

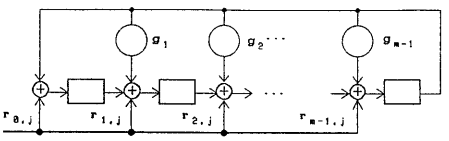

図 1. MISR(multiple-input signature register)

Fig.1 MISR(multiple-input signatre register)

図 1 の回路は第 j スロットでの入力ビット系列

$$(r_{0,j}, r_{1,j}, \cdots, r_{m-1,j})$$

を GF(2^m) 上の元

$$\beta_j = r_{0,j} + r_{1,j}\alpha + r_{2,j}\alpha^2 + \cdots + r_{m-1,j}\alpha^{m-1} \tag{1}$$

に対応させたとき，GF(2^m) 上の多項式を

$$\beta(x) = \beta_0 x^{n-1} + \beta_1 x^{n-2} + \cdots + \beta_{n-2}x + \beta_{n-1} \tag{2}$$

一次多項式

$$x - \alpha \tag{3}$$

で除した剰余を求める回路となっている． ただし，ここで n はテスト長であり，α は

$$\alpha^m = g_{m-1}\alpha^{m-1} + g_{m-2}\alpha^{m-2} + \cdots + g_1\alpha + 1 \tag{4}$$

を満たす GF(2^m) 上の元，さらに $g_i, i = 1,2,\cdots,m-1 \in$ GF(2) とする．

2.2 多重化 MISR と RS 符号の 2 元重み分布

署名解析法では，疑似ランダム系列の回路応答である出力系列を圧縮し，その圧縮系列と正常な回路の圧縮系列（署名）を比較することにより回路故障を検出している．したがって，実際には回路に故障があるにもかかわらず，故障を見逃す確率（エイリアス確率）が問題となる．このエイリアスを低減させる一つの手法として MISR を多重化する方法がある．図 2 は 2 重化 MISR の

例である．

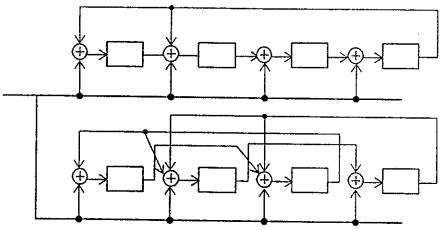

図2. 4入力2重化MISRの例

Fig.2 Example of double MISR with four input

図1の説明から容易に類推できるように，αを GF(2^4) 上の原始元で

$$\alpha^4 = \alpha + 1 \tag{5}$$

を満足するものとしたとき，上段の LFSR は式 (2) に対応する GF(2^4) 上の多項式を $(x-\alpha)$ で除した，その剰余を求める回路，下段の LFSR は同様に $(x-\alpha^2)$ の剰余を求める回路となっている．

一般には GF(2^m) 上の RS 符号を応用することにより，多重化 MISR を構成することができる． すなわち，αを GF(2^m) の原始元，b を非負の整数，生成多項式 $g(x)$ を

$$(x-\alpha^b)(x-\alpha^{b+1})\cdots(x-\alpha^{b+d-2}) \tag{6}$$

として作られるシンボル設計距離 d の RS 符号に基づく $d-1$ 重化 MISR である．この多重化 MISR の構成は，式 (6) の各一次式に対するテスト応答系列の剰余を求める回路を多重化したものとなっている．

CUT の出力で生起される誤りが出力端子（ビット出力）ごとに独立である（いわゆる2元対称通信路）と仮定した場合，式 (6) で与えられる RS 符号に基づく $d-1$ 重化 MISR のエイリアス確率（ビットエイリアス確率）は，この RS 符号を2元展開した2元線形符号の誤り見逃し確率に相当することが知られている．したがって，この RS 符号の2元重み分布を求めることにより，$d-1$ 重化 MISR のビットエイリアス確率を陽に求めることができる．

3 2重化 MISR とそのエイリアス確率

3.1 RS 符号の2元重み分布による2重化 MISR の解析

RS 符号の2元重み分布を求めることにより，RS 符号に基づく多重化 MISR のビットエイリアス確率を求めることができる．しかしながら，現在までに GF(2^m) 上の RS 符号について

$$x-\alpha,\ \ (x-1)(x-\alpha),$$

$$(x-\alpha)(x-\alpha^2),\ \ (x-1)(x-\alpha)(x-\alpha^2),$$

$$(x-\alpha)(x-\alpha^2)(x-\alpha^3)$$

を生成多項式，あるいは検査多項式とする符号，およびそれらの拡大符号について2元重み分布の公式が報告されているのみであり，一般的に RS 符号の2元重み分布を求めることは非常に困難である．さらに公式が知られている場合も上記の多項式を検査多項式とする場合を除いて，実際にその重み分布を導出することは容易ではない．[1]

表 1: 例1の符号 A，B の2元重み分布

Weight	A	B
0	1	1
4	7	0
5	42	21
6	112	168
7	248	360
8	385	210
9	525	280
10	728	1008
11	728	1008
12	525	280
13	385	210
14	248	360
15	112	168
16	42	21
17	7	0
21	1	1

岩崎は，2元重み分布公式が知られている RS 符号に基づく多重化 MISR のエイリアス確率を求め，考察を与えている． 特に2重化 MISR に注目し，生成多項式として $(x-1)(x-\alpha)$ を用いた RS 符号に対応する2重化 MISR が，$(x-1)$ を生成多項式に含まない RS 符号に対応する2重化 MISR に比べてエイリアス確率が小さいことを予想している [IwaYa90]．

3.2 RS 符号の2元重み分布とその展開基底

一般に RS 符号の2元重み分布は，生成多項式が同一であっても展開する基底により異なる [MoToKa87]．

例1： αを GF(2^3) 上の原始元とする．ただし，

$$\alpha^3 + \alpha + 1 = 0 \tag{7}$$

である．RS 符号の生成多項式を

$$g(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^3) \tag{8}$$

とする．このとき $GF(2)$ 上の GF(2^3) の基底 A

$$\{1, \alpha, \alpha^2\}$$

および基底 B

$$\{1, \alpha, \alpha^5\}$$

を用いて，RS 符号を2元展開した符号 A および B の2元重み分布は表1で与えられる．表1が示すように一般に展開基底が異なれば，シンボル上で同じ符号であっても2元重み分布は異なる．

この2元重み分布から，テスト長（RS 符号のシンボル長）7，ビット幅3のテスト応答を式 (8) の各一次多項式で割った剰余をシグネチャとするような3重化 MISR のビットエイリアス確率を計算することができる．そのビットエイリアス確率を表2に与える．

[1] 双対符号の重み分布が求まれば，MacWilliams の等式を使うまでもなく，ビットエイリアス確率（誤り見逃し確率）が求め得ることに注意されたい．

表 2: 符号 A および B に基づく 3 重化 MISR のビットエイリアス確率

bit error rate	A	B
0.5	1.95×10^{-3}	1.95×10^{-3}
0.2	1.10×10^{-3}	8.21×10^{-4}
0.1	2.24×10^{-4}	8.24×10^{-5}
10^{-2}	6.27×10^{-8}	1.94×10^{-9}
10^{-3}	6.92×10^{-12}	2.08×10^{-14}
10^{-4}	6.99×10^{-16}	2.10×10^{-19}

3.3 RS 符号の 2 元重み分布と 2 元展開基底の関係

RS 符号の生成多項式が同一であってもその 2 元展開基底が異なれば，一般に 2 元重み分布は異なることを述べた．しかしながら，このことは必ずしも 2 元展開基底が異なれば 2 元重み分布も異なることを示している訳ではない．すなわち，同一 2 元重み分布を与える相違なる基底が存在する．

今村，吉田，中村は同一 2 元重み分布を与える基底に関して次の定理を導いた [ImYoNa85]．

定理 1[ImYoNa85]： GF(2^m) 上の RS 符号において基底

$$\{\beta_1, \beta_2, \cdots, \beta_m,\}$$

を用いて各シンボルを展開して得られる 2 元線形符号と基底

$$\{{\beta_1}^2, {\beta_2}^2, \cdots, {\beta_m}^2,\}$$

を用いて各シンボルを展開して得られる 2 元線形符号は同一 2 元重み分布を与える．

定理 1 はすべての GF(2^m) の基底を同一 2 元重み分布を与えるクラスで分割する 1 つの手法を与えている．さらに次の定理が証明されている．

定理 2[MoToKa87]： ξ を GF(2^m) 上の任意の非零元とする．GF(2^m) 上の RS 符号において，基底

$$\{\beta_1, \beta_2, \cdots, \beta_m,\}$$

を用いて各シンボルを展開して得られる 2 元線形符号と基底

$$\{\xi\beta_1, \xi\beta_2, \cdots, \xi\beta_m,\}$$

を用いて各シンボルを展開して得られる 2 元線形符号は同一 2 元重み分布を与える．

$\{\beta_1, \beta_2, \cdots, \beta_m,\}$ が基底であれば，$\{\xi\beta_1, \xi\beta_2, \cdots, \xi\beta_m,\}$ も基底になることは明白であり，かつ $\xi \neq 1$ であれば 2 つの基底は一致しない．したがって定理 2 を用いることにより GF(2^m) のすべての基底を同一 2 元重み分布を与える

$$\mathbf{N}_{Th.2} = \frac{\mathbf{n}_B(2,m)}{2^m - 1}$$

個のクラスに分割することができる．ここで $\mathbf{n}_B(2,m)$ は GF(2^m) の基底の総数であり，

$$\mathbf{n}_B(2,m) = \frac{\{\prod_{i=0}^{m-1}(2^m - 2^i)\}}{m!}$$

で与えられる．

表 3 において $m = 3,4,5,6,7$ の場合に対して $\mathbf{n}_B(2,m)$ および $\mathbf{N}_{Th.2}$ の値を示す．なお，$\mathbf{B}_{RS}$ の値は，定理 1 および定理 2 を考慮した場合の同一 2 元重み分布を与える基底のクラスの総数である．定理 1 および定理 2 の関係は完全に独立ではないことから，$\mathbf{B}_{RS}$ の値を求めることは容易ではない．しかしながら m が素数の場合，次の定理 3 より $\mathbf{B}_{RS}$ の値を陽に与えることができる．

表 3: 同一 2 元重み分布を与える基底のクラス数の上限値

m	$\mathbf{n}_B(2,m)$	$\mathbf{N}_{Th.2}$	$\mathbf{B}_{RS}$
3	28	4	2
4	840	56	16
5	83328	2688	540
6	27998208	444416	74120
7	32509919232	255983616	36569094

表 4: 同一 2 元重み分布を与える基底

(a)	$\{1, \alpha, \alpha^2, \alpha^3\}$	(b)	$\{1, \alpha, \alpha^2, \alpha^6\}$
(c)	$\{1, \alpha, \alpha^2, \alpha^7\}$	(d)	$\{1, \alpha, \alpha^2, \alpha^9\}$
(e)	$\{1, \alpha, \alpha^2, \alpha^{11}\}$	(f)	$\{1, \alpha, \alpha^2, \alpha^{12}\}$
(g)	$\{1, \alpha, \alpha^3, \alpha^6\}$	(h)	$\{1, \alpha, \alpha^3, \alpha^{10}\}$
(i)	$\{1, \alpha, \alpha^3, \alpha^{11}\}$	(j)	$\{1, \alpha, \alpha^3, \alpha^{12}\}$
(k)	$\{1, \alpha, \alpha^3, \alpha^{13}\}$	(l)	$\{1, \alpha, \alpha^5, \alpha^6\}$
(m)	$\{1, \alpha, \alpha^6, \alpha^9\}$	(n)	$\{1, \alpha, \alpha^6, \alpha^{10}\}$
(o)	$\{1, \alpha, \alpha^9, \alpha^{13}\}$	(p)	$\{1, \alpha^3, \alpha^6, \alpha^9\}$

定理 3[MoToKa87]： m が素数の場合，同一 2 元重み分布を与える GF(2^m) 上の基底のクラスの総数に関する上限値 $\mathbf{B}_{RS}$ は次式で与えられる

$$\mathbf{B}_R S = \frac{\mathbf{N}_{Th.2} + (m-1)\mathbf{n}_{Norm.B}(2,m)}{m} \tag{9}$$

ただし，$\mathbf{n}_{Norm.B}(2,m)$ は GF(2^m) 上の異なる正規基底の総数であり

$$\mathbf{n}_{Norm.B}(2,m) = \frac{2^m \sum_{all m_i}(1 - 2^{-m_i})}{m}$$

で与えられる．

例 2： GF(2^4) の基底の総数は 840 個である．表 2 から GF(2^4) 上の RS 符号で同一 2 元重み分布を与える基底のクラスは 16 個であり，すべての基底は定理 1 および定理 2 の変換により，表 4 に与えられる 16 個の基底の何れかに変換することができる．

3.4 RS 符号の生成多項式およびその 2 元展開基底と MISR のエイリアス確率

従来，署名解析法では，α を GF(2^m) の原始元，b を非負の整数，RS 符号の生成多項式を $(x-\alpha^b)(x-\alpha^{b+1})\cdots(x-\alpha^{b+d-2})$ としたとき，多項式基底 $(1, \alpha, \alpha^2, \cdots, \alpha^{m-1})$ で展開した符号に基づく $d-1$ 重 MISR が提案され，評価が行われてきた．特に 2 元重み分布公式が知られている，RS 符号の生成多項式 $(x-1)(x-\alpha)$，および $(x-\alpha)(x-\alpha^2)$ に基づく 2 重化 MISR についてそのビットエイリアス確率が与えられている．これらの生成多項式をもつ RS 符号の 2 元重み分布は基底の選択に関して不変であることが証明されている．しかしながら，上記の多項式以外の生成多項式に基づく 2 重化 MISR に関しては，一般に展開する基底が異なれば，そのビットエイリアス確率が相異なる．したがって，上記以外の 2 重化 MISR で多項式基底を含む他の様々な基底で展開することにより，RS 符号の誤り見逃し確率，すなわちエイリアス確率を低減させ得る可能性がある．このような立場から，次節にお

いては数値実験を行う．特に GF(2^4) 上の RS 符号に基づくテスト長（シンボル長）15 の 2 重化 MISR に対しては $(x-1)(x-\alpha)$ に基づく 2 重化 MISR に比較して，ビットエイリアス確率が低いという意味で優れたシグネチャ回路を導出する．また GF(2^8) 上の RS 符号に基づくテスト長（シンボル長）200，すなわち短縮化された RS 符号に基づく 2 重化 MISR のビットエイリアス確率について数値実験を行い，優れたシグネチャ回路の構成法について考察を与える．

3.5 シミュレーション結果およびその考察

3.5.1 シミュレーション [I]

GF(2^4) 上の RS 符号に基づくテスト長（シンボル長）15 の 2 重化 MISR のビットエイリアス確率についてシミュレーションを行う．すなわち，生成多項式

$$(x-\alpha^b)(x-\alpha^{b+1}), \quad b=0,1,2,\cdots,14.$$

をもつ RS 符号に対して，すべての基底に関して 2 元展開した RS 符号の 2 元重み分布を求め，その重み分布から 2 重化 MISR のビットエイリアス確率を導出した．図 3 は以下に示す 2 重化 MISR のビットエイリアス確率を与えるのものである．なお，図 4 は図 3 に関してビット誤り確率が比較的大きい場合のエイリアス確率を抽出拡大したものである．

- ビットエイリアス確率が最も低い RS 符号に基づく 2 重化 MISR
- ビットエイリアス確率が最も高い RS 符号に基づく 2 重化 MISR
- ビットエイリアス確率が最も低い，多項式基底で 2 元展開された RS 符号に基づく 2 重化 MISR
- ビットエイリアス確率が最も高い，多項式基底で 2 元展開された RS 符号に基づく 2 重化 MISR

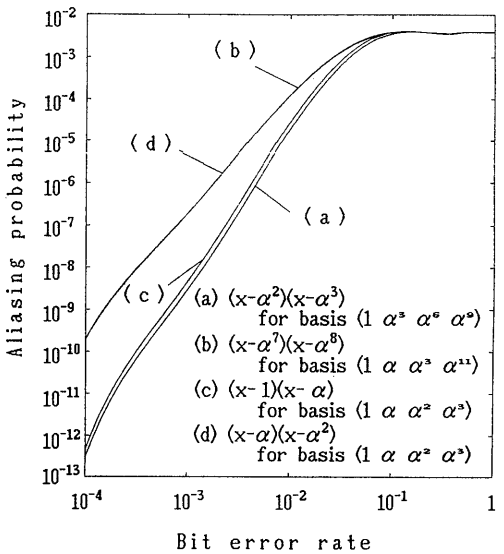

図 3. 4 入力 2 重化 MISR のビットエイリアス確率

Fig.3 Aliasing probabilities of double MISR with four input

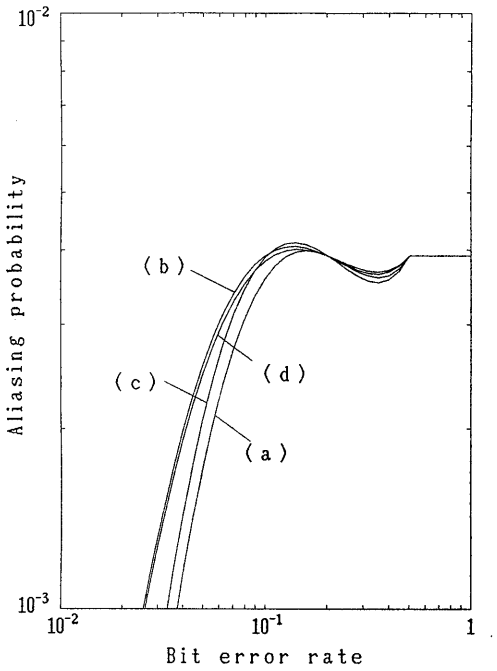

図 4. 4 入力 2 重化 MISR のビットエイリアス確率（図 3 の部分拡大）

Fig.4 Aliasing probabilities for high bit-error-rate of double MISR with four input

図 5 は図 3 で与えたビットエイリアス確率が最も低い 2 重化 MISR の回路構成を示したものである．

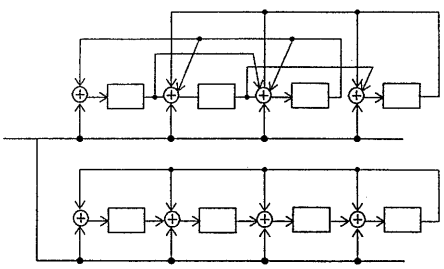

図 5. 4 入力 2 重化 MISR の回路構成（ビットエイリアス確率が最も低い RS 符号に基づく 2 重化 MISR）

Fig.5 Circuit of double MISR with four input for polynomial $(x-\alpha^2)(x-\alpha^3)$ and for basis $(1, \alpha^3, \alpha^6, \alpha^9)$.

図 3 で与えられたシミュレーション結果に関して次の点が非常に興味深い．

1. ビットエイリアス確率が最も低い 2 重化 MISR と逆に最も高い 2 重化 MISR では，ビット誤り確率が 10^{-4} でほぼ 1000 倍の差が存在する．

2. 多項式基底で2元展開されたRS符号に基づく2重化MISRの中で，最悪な2重化MISRのビットエイリアス確率にほぼ等しいものが存在する．

3. $(x-1)(x-\alpha)$ に基づく2重化MISRに比較して，ビットエイリアス確率が低いという意味で優れた2重化MISRが存在する．

3.5.2 シミュレーション[II]

先のシミュレーションと同様，$GF(2^8)$ 上のRS符号に基づくテスト長（シンボル長）200，すなわち短縮化されたRS符号に基づく2重化MISRのビットエイリアス確率についてシミュレーションを行う．生成多項式として

$$(x-1)(x-\alpha),\quad (x-\alpha)(x-\alpha^2),$$

$$(x-\alpha^2)(x-\alpha^3),\quad (x-\alpha^6)(x-\alpha^7),$$

$$(x-\alpha^{73})(x-\alpha^{74})$$

をもつRS符号に対して，いくつかの基底に関して2元展開したRS符号の2元重み分布を求め，その重み分布から2重化MISRのビットエイリアス確率を導出した．ただし，

$$\alpha^8+\alpha^4+\alpha^3+\alpha^2+1=0$$

である．

図6はそれぞれ

(a) 生成多項式 $(x-\alpha^6)(x-\alpha^7)$ をもつ $GF(2^8)$ 上の符号シンボル長200のRS符号で，基底 $(\alpha^2,\alpha^3,\alpha^{46},\alpha^{49},\alpha^{196},\alpha^{252},\alpha^{253},\alpha^{254})$ で2元展開された符号に基づく2重化MISRのビットエイリアス確率．

(b) 生成多項式 $(x-\alpha^6)(x-\alpha^7)$ をもつ $GF(2^8)$ 上の符号シンボル長200のRS符号で，基底 $(\alpha^{22},\alpha^{23},\alpha^{24},\alpha^{46},\alpha^{98},\alpha^{136},\alpha^{236},\alpha^{253})$ で2元展開された符号に基づく2重化MISRのビットエイリアス確率．

(c) 生成多項式 $(x-\alpha^6)(x-\alpha^7)$ をもつ $GF(2^8)$ 上の符号シンボル長200のRS符号で，多項式基底 $(1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7)$ で2元展開された符号に基づく2重化MISRのビットエイリアス確率．

(d) 生成多項式 $(x-1)(x-\alpha)$ をもつ $GF(2^8)$ 上の符号シンボル長200のRS符号で，多項式基底 $(1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7)$ で2元展開された符号に基づく2重化MISRのビットエイリアス確率．

を与えている．

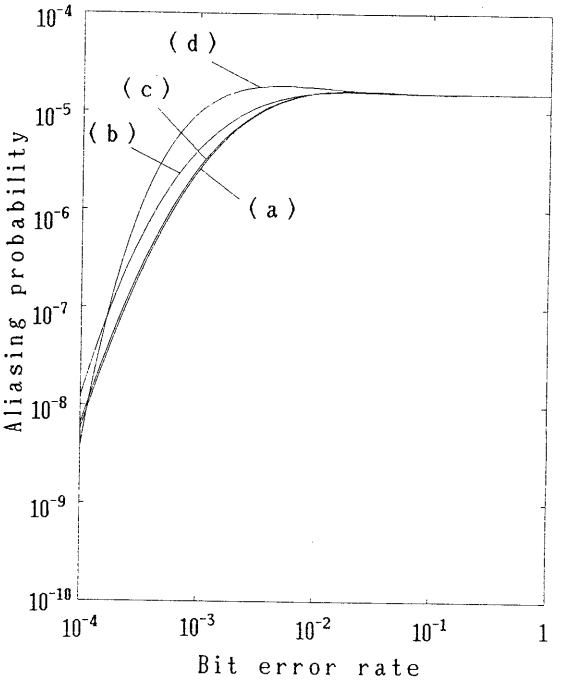

図6. 8入力2重化MISRのビットエイリアス確率（その1）

Fig.6 Aliasing probabilities of double MISR with eight input (No.1)

生成多項式 $(x-\alpha^6)(x-\alpha^7)$ による2重化MISRにおいて，多項式基底で展開されたRS符号に基づく2重化MISR**(c)** よりも，ビットエイリアス確率が低いという意味で改善された2重化MISR**(a)** が存在する．また，逆に多項式基底に基づく2重化MISR**(c)** よりもビットエイリアス確率がかなり高くなる2重化MISR**(b)** も存在する．　多項式基底で展開された生成多項式 $(x-1)(x-\alpha)$ をもつRS符号に基づく2重化MISR**(d)** に比べて，**(a)** はビット誤り率εが比較的大きい範囲$(0.5>\varepsilon>10^{-4})$では十分優れている．**(d)** よりも$\varepsilon$のすべての範囲で優れた2重化MISRが存在するか否かは未解決である．なお生成多項式 $(x-1)(x-\alpha)$ をもつRS符号に基づく2重化MISRは展開基底を変化させても，そのビットエイリアス確率にさほどの変化は見られなかった．

図7ではそれぞれ

(a) 生成多項式 $(x-\alpha)(x-\alpha^2)$ をもつ $GF(2^8)$ 上の符号シンボル長200のRS符号で，基底 $(\alpha^{24},\alpha^{46},\alpha^{98},\alpha^{136},\alpha^{236},\alpha^{252},\alpha^{253},\alpha^{254})$ で2元展開された符号に基づく2重化MISRのビットエイリアス確率．

(b) 生成多項式 $(x-\alpha)(x-\alpha^2)$ をもつ $GF(2^8)$ 上の符号シンボル長200のRS符号で，基底 $(1,\alpha^{23},\alpha^{45},\alpha^{98},\alpha^{221},\alpha^{251},\alpha^{252},\alpha^{253})$ で2元展開された符号に基づく2重化MISRのビットエイリアス確率．

(c) 生成多項式 $(x-1)(x-\alpha)$ をもつ $GF(2^8)$ 上の符号シンボル長200のRS符号で，多項式基底 $(1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7)$ で2元展開された符号に基づく2重化MISRのビットエイリアス確率．

を与えている．

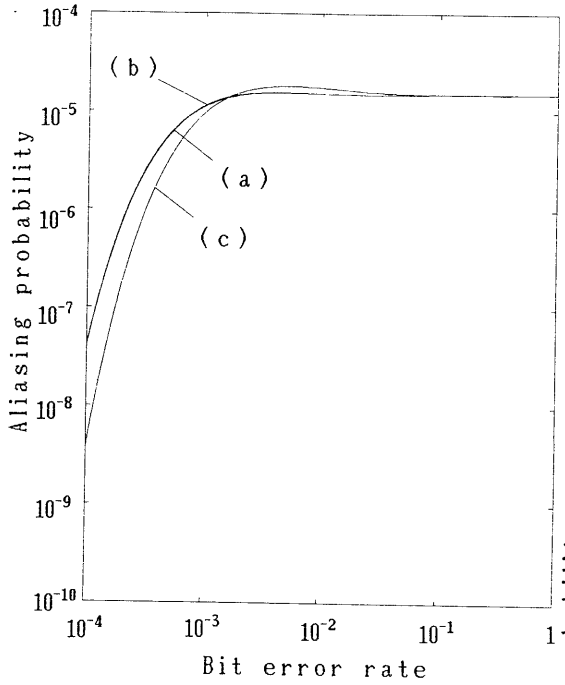

図7. 8入力2重化MISRのビットエイリアス確率(その2)

Fig.7 Aliasing probabilities of double MISR with eight input (No.2)

図7では，ビットエイリアス確率が低いという意味で最適な2重化MISRと予想されている，$(x-1)(x-\alpha)$を生成多項式とする2重化MISR**(c)**と逆にビットエイリアス確率が高くなると考えられている$(x-\alpha)(x-\alpha^2)$を生成多項式とする2重化MISR**(a), (b)**を比較している．**(c)**に比べて**(a), (b)**はビットエイリアス確率が高くなっている．なお，$(x-\alpha)(x-\alpha^2)$を生成多項式とする2重化MISRでは，展開基底を変化させてもそのビットエイリアス確率にはさほどの変化は見られなかった．

3.5.3 シミュレーション結果に対する考察

GF(2^4)上では$(x-1)(x-\alpha)$を生成多項式とする2重化MISRよりも，展開基底を変化させることによってビットエイリアス確率が低いという意味で優れた2重化MISRを導出することができた．GF(2^8)上ではそのような例を見つけることができなかったが，これは展開基底の数が非常に多く，すべての展開基底に対して検査できなかったためとも考えられる．

一般に$(x-1)(x-\alpha)$を生成多項式とする2重化MISRはビット誤り率εが小さい範囲($\varepsilon < 10^{-4}$)では十分優れているが，その他の範囲では図6にみられるように他に比べてかなり劣化する場合が存在する．したがって回路故障によって生起するビット誤りが比較的大きい値(シミュレーション[II]の例では$\varepsilon \approx 10^{-3}$)が支配的である場合，MISRの選択に関して注意する必要がある．

図7でも示されたように$(x-1)(x-\alpha)$を生成多項式とする2重化MISRの比べて$(x-\alpha)(x-\alpha^2)$を生成多項式とする2重化MISRはその展開基底を変化させても一般にビットエイリアス確率が高くなる．しかしながらビットエイリアス確率が高くなる理由は生成多項式を$(x-\alpha)(x-\alpha^2)$としていることが本質的ではなく，その2根が互いに共役根の関係にあることが原因と考えられる．GF(2^8)において，連続する2根ではαとα^2の他にα^{73}とα^{74}がある．

図8ではそれぞれ

(a) 生成多項式$(x-1)(x-\alpha)$をもつGF(2^8)上の符号シンボル長200のRS符号で，多項式基底$(1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7)$で2元展開された符号に基づく2重化MISRのビットエイリアス確率．

(b) 生成多項式$(x-\alpha^{73})(x-\alpha^{74})$をもつGF($2^8$)上の符号シンボル長200のRS符号で，多項式基底$(1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7)$で2元展開された符号に基づく2重化MISRのビットエイリアス確率．

を与えている．

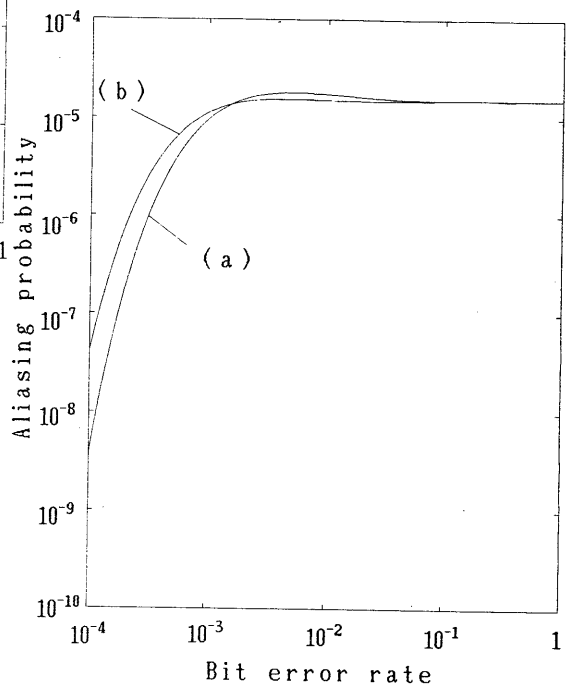

図8. 8入力2重化MISRのビットエイリアス確率(その3)

Fig.8 Aliasing probabilities of double MISR with eight input (No.3)

4 むすび

本稿では回路の出力で生起される誤りが出力端子(ビット出力)ごとに独立であると仮定し，シグネチャ回路としてMISRを2重以上用いた多重MISRのビットエイリアス確率について考察を与えた．すなわちテスト応答で得られる同一タイムスロット内のmビット出力をGF(2^m)上の元に対応させる基底が異なれば，一般にビットエイリアス確率が異なることを指摘し，そのシミュレーションを行った．その結果としてビットエイリアス確率が低いという意味で多項式基底よりも優れた基底が存在することを示し，そのシグネチャ回路を導出した．特にGF(2^4)上のRS符号に基づく2重化MISRに関して生成多項式として$(x-1)(x-\alpha)$を用いたRS符号に対応する2重化MISRよりもビットエイリア

ス確率が低いという意味で優れた2重化MISRを導出できたことは非常に興味深い．またGF(2^8)上のRS符号に基づく2重化MISRに関して，展開基底を変化させることによりエイリアス確率が変化する場合があることを示した．さらにエイリアス確率が高い2重化MISRの一つの条件を与えた．

今後は生成多項式の根の間の関係が顕著となる3重以上のMISRのビットエイリアス確率に関しても考察を行う予定である．

謝辞

森井および谷川は日頃より回路故障検査全般について愛媛大学工学部情報工学科高松雄三教授にご指導頂いている．ここに感謝の意を表する．

参考文献

[Fuji85] H.Fujiwara: "Logic testing and design for testability", MIT Press (1985)

[Lala88] P.K.Lala 著，当麻善弘監訳，" フォールト *cdot* トレランス入門"，オーム社 (1988)

[Kino89] 樹下行三，" VLSIテスト容易化設計技術の研究動向"，情報処理学会誌, Vol.30, No.12, pp.1451-1460 (1989-12)

[Froh77] R.A.Frohwerk: "Signature analysis: a new digital field service method", Hewlett-Packard Journal, pp.2-8 (May 1977)

[Smith80] J.E.Smith: "Measures of effectiveness of fault signature analysis", IEEE Trans. Comput., Vol.c-29, pp.510-514 (June 1980)

[Iwadare89] 岩垂好裕: 情報システムの信頼性，電子情報通信学会 (1989-02)

[WDGS86] T.W.Williams, W.Dahen, M.Gruetzner and C.W.Starke: "Comparison of aliasing errors for primitive and non-primitive polynomials", Int'l Test Conf., pp.282-288 (Sept. 1986)

[WDGS88] T.W.Williams, W.Dahen, M.Gruetzner and C.W.Starke: "Bound and analysis of aliasing errors in linear feedback shift registers", IEEE Trans. CAD/ICAS, Vol.7, pp.75-83 (Jan. 1988)

[IvaAga88] A.Ivanov and V.K.Agarwal: "An iterative technique for calculating aliasing probability of linear feedback shift register", Fault-Tolerant Computing Symp., pp.70-75 (1988)

[GupPra88] S.K.Gupta and D.K.Pradhan: "A new framework for designing & analyzing BIST techniques", Int'l Test Conf., pp.329-342 (Sept. 1988)

[DOFR89] M.Damiani, P.Olivo, M.Favalli and B.Ricco: "An analytical model for the aliasing probability in signature analysis testing", IEEE Trans. CAD/ICAS, Vol.8, pp.1133-1144 (Nov. 1989)

[SSMM90] M.Serra, T.Slater, J.C.Muzio and D.M.Miller: "The analysis of one-demensional linear celluar automata and their aliasing probabilities", IEEE Trans. CAD/ICAS, Vol.9, No.7, pp.767-778 (July 1990)

[Iwasaki91a] 岩崎一彦：" 誤り訂正符号のVLSI自己テストへの応用"，ワークショップ「符号理論とその応用」，松山，(1991-05)

[Iwasaki89] K.Iwasaki:"Analysis and proposal of signature circuits for LSI testing", IEEE Trans. CAD, **7**, 1, pp.84-99 (Jan. 1988)

[IwaNi88] 岩崎，西向井：" シグネチャ検査法のエイリアス確率と符号の重み分布"，信学論 (D)，**J71-D**, 9, pp.1797-1803 (1988-09)

[HuFeKa90] 藤原融，馮首平，嵩忠雄：" シグネチャ検査法における故障見逃し確率の近似"，信学論 (A)，**J73-A**, no.10, pp.1669-1677 (1990-10)

[PrGu90] D.K.Pradhan, S.K.Gupta and M.G.Karpovsky, "Aliasing probability for multiple input signature analyzer", IEEE Trans. on Computer, **39**, 4, pp.586-591 (Apr. 1990)

[WilDae89] T.W.Williams and W.Daehn: "Aliasing errors in multiple input signature analysis registers", European Test Conf. in Paris, pp.338-345 (Apr. 1989)

[DaWiWa90] W.Daehn, T.W.Williams and K.D.Wagner: "Aliasing errors in linear automata used as multiple-input signature analyzer", IBM J.R&D, Vol.34, No.2/3, pp.363-380 (Mar. and May 1990)

[DOFER89] M.Damiani, P.Olivo, M.Favalli, S.Ereolani and B.Ricco: "Aliasing in signature analysis testing with multiple-input shift-registers", European Test Conf.in Paris, pp.346-353 (Apr. 1989)

[IwaYa88] 岩崎一彦，山口昇：" リードソロモン符号の2元重み分布とそのBISTへの応用"，信学技報，**R88-29**, pp.35-40 (1988-11)

[Iwasaki90] 岩崎一彦：" 距離2の最大距離分離符号の2元重み分布とそのVLSI自己テストへの応用"，信学論 (A)，**J73-A**, no.11, pp.1851-1857 (1990-11)

[IwaYa90] K.Iwasaki and N.Yamaguchi, "Design of signature circuits based on weight distribution of error-correcting codes", Int'l Test Conf., pp.779-785 (1990-09)

[MoToKa87] 森井，常盤，笠原：" Reed-Solomon符号の2元重み分布に関する二，三の考察"，信学技報，**IT86-118**, pp.21-26 (1987-03)

[MoTa90] 森井昌克，高松雄三：" MISRのエイリアス確率とMDS符号及びその基底展開について"，第23回FTS研究会，山形 (1990-07)

[ImYoNa85] 今村，吉田，中村，" GF(2^m)上のReed-Solomon符号の2元符号としての重み分布について"，情報理論とその応用研究会第8回シンポジウム資料，pp.135-139 (1985-12)