設計自動化 72－15
(1994. 10. 28)

多重MISRの構成とそのエイリアス確率に関する二，三の考察

森井 昌克† 小野 竜一† 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

VLSIの自己テスト法として署名解析法が提案されている．署名解析法では誤り見逃し確率(エイリアス確率)が問題となる．シグネチャ回路として用いられるMISR(Multiple Input Signature Register)についてはGF(2^m)上のReed-Solomon(RS)符号の2元重み分布とそのエイリアス確率との関係が指摘されている．

署名解析法ではGF(2^m)上の原始元，bを非負の整数，生成多項式を$(x-\alpha^b)(x-\alpha^{b+1})\cdots(x-\alpha^{b+d-2})$としたRS符号を多項式基底$(1,\alpha,\alpha^2,\cdots,\alpha^{m-1})$により展開した符号に基づく$d-1$重MISRが提案されている．また最近，2重化MISRについて多項式基底でない他の基底により展開することによって，従来に比較してエイリアス確率を低減させ得ることが報告されている．

本稿では3重化MISRに対する展開基底とそのエイリアス確率との関係について考察を与える．

和文キーワード 組み込み自己テスト法，エイリアス確率，MISR，Reed-Solomon符号，VLSI

On aliasing probabilities for multiple input signature registers

Masakatu MORII† Ryuichi ONO† Kazuhiko IWASAKI‡

† Department of Computer Science, Ehime University
Matsuyama, 790 Japan
‡ Department of Information and Computer Science, Chiba University
Chiba,260 Japan

Abstract

The aliasing probability is a problem to VLSI built-in self-test(BIST). Recently the relation between the aliasing probability for MISR(Multiple Input Signature Register) and the binary weight distribution of Reed-Solomon(RS) codes has been studied actively.

This paper presents a few comments on the aliasing probability of MISR and the binary weight distribution of RS codes. Especially we give a triple MISR with 8 inputs which has the aliasing probability smaller than others.

英文 key words built-in self-test, aliasing probability, MISR, Reed-Solomon codes, VLSI

1 まえがき

VLSI の組み込み自己テスト法 [1][2] としての署名解析法 [3][4] では疑似ランダム誤りの回路応答である出力系列をシグネチャ回路と呼ばれる回路で圧縮し, 正常な回路の圧縮系列 (署名) と比較することにより回路の故障を検出する. しかしながら, この検査法では被検査回路に故障があるにも関わらず, 故障を見逃す可能性がある. この確率をエイリアス確率と呼ぶ [5]. エイリアス確率が低いという意味で優れた署名解析法の実現手法として符号理論に基づく構成手法が提案されている [6]. 特にシグネチャ回路として多入力シフトレジスタ (Multiple Input Shift Register,MISR) を多重化した回路 (多重化 MISR) を採用する署名解析法では, コンパクトディスク (CD), 光ディスクあるいは衛星通信等で用いられる Reed-Solomon(RS) 符号との関係が指摘され [8] [9] [10] エイリアス確率の評価法とともに優れたシグネチャ回路の構成を目的として研究が進められている.

多重化 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, 山口ら [9] は RS 符号に基づいた多重化 MISR を提案し, 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. 特に RS 符号の生成多項式において 1 を根として有する RS 符号に対応する 2 重化 MISR がビットエイリアス確率が低いという意味で優れていることを示した. 最近, 森井, 谷川, 岩崎ら [14] は RS 符号の 2 元重み分布を導出する際に必要となる展開基底に着目し, 従来提案されている 2 重化 MISR よりも優れた回路が存在することを示した. 展開基底は多重化 MISR の各シフトレジスタにおける回路構成に対応する.

本稿では 4 入力および 8 入力 3 重化 MISR に対する展開基底の効果について考察する. 本稿の結果から必ずしも 1 を根として含む RS 符号に対する 3 重化 MISR が優れていないことを示し, 2 重化 MISR の場合と同様, 基底の変化によってエイリアス確率のふるまいが異なることを示す.

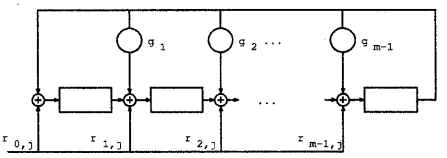

図 1: MISR(multiple-input signature register)

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

署名解析法では被検査回路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, 被検査回路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

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

に対応させたとき, GF(2^m) 上の多項式を

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

一次多項式

$$x - \alpha \quad (3)$$

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

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

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

一般的には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

$$(x-\alpha^b)(x-\alpha^{b+1})\cdots(x-\alpha^{b+d-2}) \qquad (5)$$

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(5)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．

被検査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(いわゆる2元対称通信路)と仮定した場合，式(5)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．

2.3 2重化MISRのエイリアス確率

岩崎，山口らは8入力2重化MISRのエイリアス確率を導出し，RS符号の生成多項式として1を有する場合に対応する2重化MISRが，低いビットエイリアス確率を有するという意味で優れていることを示した．森井，谷川，岩崎らはRS符号の2元重みを求める際に必要となる展開基底について着目し，多項式基底以外の基底を採用することにより，従来より優れた2重化MISRを導出している．例えば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を導出している．すなわち生成多項式

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

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2はそれぞれ

(a) 生成多項式として$(x-\alpha)(x-\alpha^2)$を採用し，基底$(1,\alpha^3,\alpha^6,\alpha^9)$により2元展開されたRS符号に基づく2重化MISRのエイリアス確率

(b) 生成多項式として$(x-1)(x-\alpha)$を採用し，多項式基底$(1,\alpha,\alpha^2,\alpha^3)$により2元展開されたRS符号に基づく2重化MISRのエイリアス確率

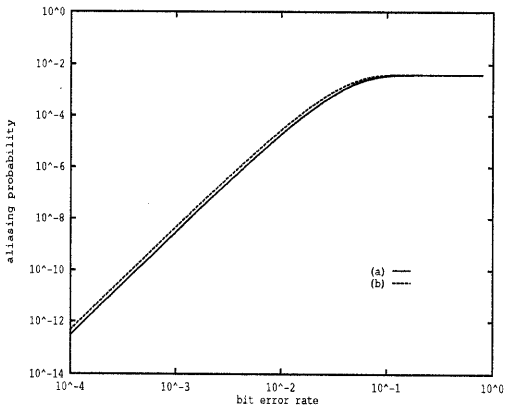

図2: 4入力2重化MISRのビットエイリアス確率

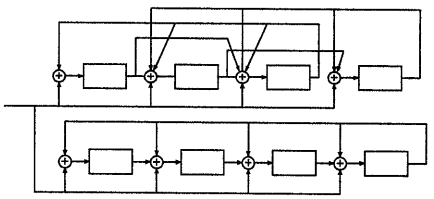

図3: ビットエイリアス確率が最も低いRS符号に基づく4入力2重化MISR

を与えている．すなわち

(a) 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

(b) 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

となっている．

図3は図2において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．

3 3重化MISRのエイリアス確率

3.1 4入力3重化MISRのエイリアス確率

原始多項式$\alpha^4+\alpha+1=0$により導かれたGF(2^4)上のRS符号に基づくテスト長（シンボル長）11の3重化MISRに対するビットエイリアス確率を導出する．図4はそれぞれ

(a) 生成多項式として$(x-1)(x-\alpha)(x-\alpha^2)$を採用し，多項式基底$(1,\alpha,\alpha^2,\alpha^3)$により2元展開されたRS符号に基づく3重化MISRのエイリアス確率

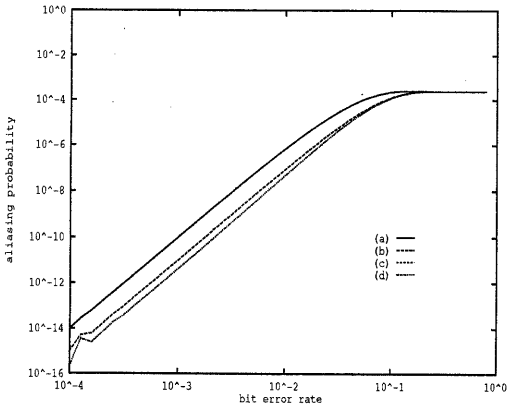

図 4: 4 入力 3 重化 MISR のビットエイリアス確率 (1)

(b) 生成多項式として $(x-\alpha^4)(x-\alpha^5)(x-\alpha^6)$ を採用し，多項式基底 $(1,\alpha,\alpha^2,\alpha^3)$ により 2 元展開された RS 符号に基づく 3 重化 MISR のエイリアス確率

(c) 生成多項式として $(x-1)(x-\alpha)(x-\alpha^2)$ を採用し，基底 $(1,\alpha,\alpha^3,\alpha^{10})$ により 2 元展開された RS 符号に基づく 3 重化 MISR のエイリアス確率

(d) 生成多項式として $(x-\alpha^5)(x-\alpha^6)(x-\alpha^7)$ を採用し，基底 $(1,\alpha,\alpha^9,\alpha^{13})$ により 2 元展開された RS 符号に基づく 3 重化 MISR のエイリアス確率

を与えている．

我々は，3 重化 MISR に対応する符号長 11 シンボルである GF(2^4) 上の RS 符号についてすべての生成多項式，およびすべての基底についてビットエイリアス確率を導出している．図 4ではそれぞれ

(a) 展開基底を多項式基底とし，すべての生成多項式を考慮した場合のビットエイリアス確率が最も高い 3 重化 MISR

(b) 展開基底を多項式基底とし，すべての生成多項式を考慮した場合のビットエイリアス確率が最も低い 3 重化 MISR

(c) すべての生成多項式および展開基底を考慮した場合のビットエイリアス確率が最も高い 3 重化 MISR

(d) すべての生成多項式および展開基底を考慮した場合のビットエイリアス確率が最も低い 3 重化 MISR

となっている．なお，図 4においては (a) と (c) はほぼ同一の値を与えている．

従来，多項式基底により展開された 2 元 RS 符号に基づく MISR について考察が行なわれてきた．しかしながら，図 4に与えるように基底を変え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より優れた 3 重化 MISR を構成することができる．また図 4(a) で与えられる多項式基底で 2 元展開された RS 符号に基づく 3 重化 MISR が最悪な 3 重化 MISR(図 4(c)) のビットエイリアス確率にほぼ等しいことに注意されたい．

図 4はビット誤り確率が 0.5 から極めて小さい値についてエイリアス確率を求めたものである．逆にビット誤り確率が 0.5 から極めて 1 に近い値をとる場合を考えることができる．図 5はビット誤り確率が 1 に近い場合に対する結果を与えている．すなわち

(a) 生成多項式として $(x-\alpha^4)(x-\alpha^5)(x-\alpha^6)$ を採用し，多項式基底 $(1,\alpha,\alpha^2,\alpha^3)$ により 2 元展開された RS 符号に基づく 3 重化 MISR のエイリアス確率

(b) 生成多項式として $(x-1)(x-\alpha)(x-\alpha^2)$ を採用し，多項式基底 $(1,\alpha,\alpha^2,\alpha^3)$ により 2 元展開された RS 符号に基づく 3 重化 MISR のエイリアス確率

(c) 生成多項式として $(x-\alpha^6)(x-\alpha^7)(x-\alpha^8)$ を採用し，基底 $(1,\alpha,\alpha^6,\alpha^9)$ により 2 元展開された RS 符号に基づく 3 重化 MISR のエイリアス確率

(d) 生成多項式として $(x-\alpha)(x-\alpha^2)(x-\alpha^3)$ を採用し，基底 $(1,\alpha^3,\alpha^6,\alpha^9)$ により 2 元展開された RS 符号に基づく 3 重化 MISR のエイリアス確率

を与えている．各 MISR の意味は図 4と同様である．すなわち，(d) はすべての生成多項式および展開基底を考慮した場合，ビット誤り確率が 0.5 から 0.9999 の範囲において，ビットエイリアス確率が最も低い 4 入力 3 重化 MISR である．

3.2 8 入力 3 重化 MISR のエイリアス確率

原始多項式$\alpha^8+\alpha^4+\alpha^3+\alpha^2+1=0$ により導かれた GF(2^8) 上の RS 符号に基づくテスト長 (シンボル長)200 の 3 重化 MISR に対するビットエイリアス確率を導出する．図 6はそれぞれ

(a) 生成多項式として $(x-1)(x-\alpha)(x-\alpha^2)$ を採用し，多項式基底により 2 元展開された RS 符号に基づく 3 重化 MISR のエイリアス確率

(b) 生成多項式として $(x-\alpha)(x-\alpha^2)(x-\alpha^3)$ を採用し，多項式基底により 2 元展開された RS 符号に基づく 3 重化 MISR のエイリアス確率

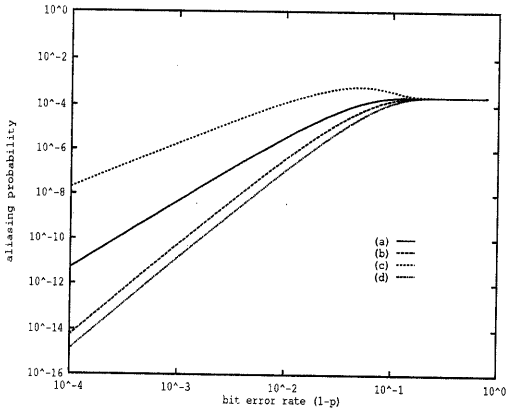

図 5: 4 入力 3 重化 MISR のビットエイリアス確率 (2)

(c) 生成多項式として $(x-\alpha^2)(x-\alpha^3)(x-\alpha^4)$ を採用し，多項式基底により 2 元展開された RS 符号に基づく 3 重化 MISR のエイリアス確率

(d) 生成多項式として $(x-\alpha^3)(x-\alpha^4)(x-\alpha^5)$ を採用し，多項式基底により 2 元展開された RS 符号に基づく 3 重化 MISR のエイリアス確率

を与えている．さらに図 7は図 6と同様，8 入力 3 重化 MISR についてビット誤り確率が極めて 1 に近い場合のエイリアス確率のふるまいを与えている．

基底を多項式基底に固定した場合の RS 符号に対応する 8 入力 2 重化 MISR のエイリアス確率に関して，文献 [5][13] において生成多項式が 1 を根として含み，ビット誤り確率が小さい値の場合，他の MISR に比べて優れ，逆にビット誤り確率が 1 に近い値の場合，劣ることが報告されている．8 入力 3 重化 MISR においては，ビット誤り確率の値が 1 に近い場合も含めて，そのエイリアス確率が劣悪であることが示され，極めて 1 に近い 0.9999 程度になってから，他の MISR に比較して優れた値を示すという興味深い結果が得られた．

図 8では生成多項式を $(x-\alpha^3)(x-\alpha^4)(x-\alpha^5)$ に固定し，基底を変化させた場合の RS 符号に対応する 8 入力 3 重化 MISR のエイリアス確率のふるまいを与えている．具体的には

(a) 多項式基底 $(1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7)$ により 2 元展開された RS 符号に基づく 3 重化 MISR

(b) 基底 $(\alpha^{53}, \alpha^{77}, \alpha^{83}, \alpha^{106}, \alpha^{154}, \alpha^{166}, \alpha^{169}, \alpha^{212})$ により 2 元展開された RS 符号に基づく 3 重化 MISR

(c) 基底 $(\alpha^{15}, \alpha^{30}, \alpha^{60}, \alpha^{120}, \alpha^{135}, \alpha^{195}, \alpha^{225}, \alpha^{240})$ により 2 元展開された RS 符号に基づく 3 重化 MISR

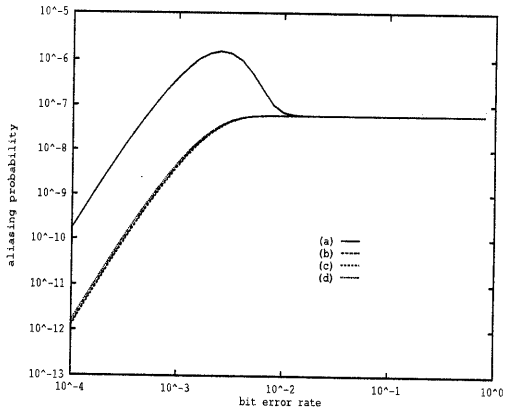

図 6: 8 入力 3 重化 MISR のビットエイリアス確率 (1)

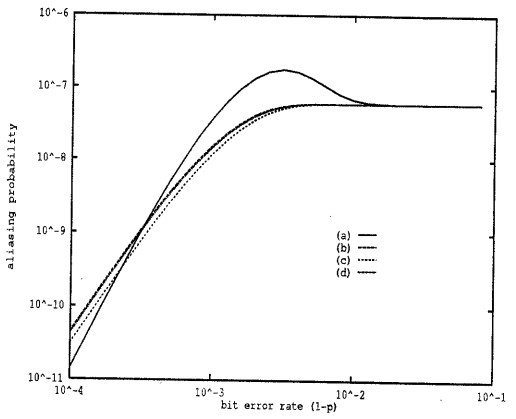

図 7: 8 入力 3 重化 MISR のビットエイリアス確率 (2)

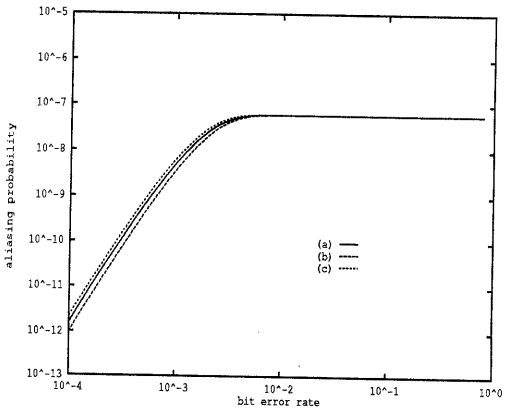

図 8: 8 入力 3 重化 MISR のビットエイリアス確率 (3)

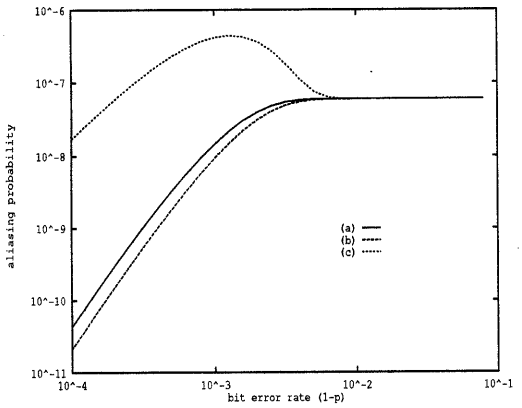

図 9: 8入力3重化 MISR のビットエイリアス確率 (4)

を与えている．GF(2) 上の GF(2^8) の基底は多数存在し，また8入力3重化 MISR に対応する RS 符号の重み分布を求める計算量が比較的大きいことからすべての基底に対してそのエイリアス確率を求めることは困難である．図8の結果はランダムに生成した100個の基底に対してそのエイリアス確率を導出し，エイリアス確率が低いという意味で優れた MISR とエイリアス確率が高いという意味で劣った MISR を与えている．またビット誤り確率が極めて1に近い場合のエイリアス確率のふるまいを図9に与える．図9はそれぞれ

(a) 多項式基底 $(1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7)$ により2元展開された RS 符号に基づく3重化 MISR

(b) 基底 $(\alpha^{39}, \alpha^{86}, \alpha^{112}, \alpha^{125}, \alpha^{169}, \alpha^{191}, \alpha^{194}, \alpha^{241})$ により2元展開された RS 符号に基づく3重化 MISR

(c) 基底 $(\alpha^{19}, \alpha^{28}, \alpha^{53}, \alpha^{134}, \alpha^{159}, \alpha^{200}, \alpha^{222}, \alpha^{227})$ により2元展開された RS 符号に基づく3重化 MISR

を与えている．

本稿で与える8入力3重化 MISR のエイリアス確率のふるまいから，8入力2重化 MISR のエイリアス確率同様，生成多項式が同一であっても基底を変えることにより，そのエイリアス確率のふるまいが変化することを確認した．またビット誤り確率が極めて1に近い場合，8入力3重化 MISR のエイリアス確率は基底によってそのふるまいが極めて特異なふるまいをすることが認められた．すなわち，生成多項式が同一であっても，基底が異なることによってそのエイリアス確率において1000倍以上の差となり得ることが示された．

4 むすび

本稿では回路の出力において生起する誤りが出力端子ごとに独立であると仮定し，シグネチャ回路として3重化 MISR を用いた場合のビットエイリアス確率について考察を与えた．2重化 MISR と同様，3重化 MISR においても異なる基底により2元展開することによりビットエイリアス確率が異なり，また基底を多項式基底に固定し生成多項式が1を根として含む場合のエイリアス確率が他に比較して特異なふるまいを与えることを指摘した．

参考文献

[1] P.K.Lala 著, 当麻善弘監訳," フォールト・トレランス入門", オーム社 (1985)

[2] 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)

[3] J.E.Smith," Measures of effectiveness of fault signature analysis", IEEE Trans.Computer.,vol.C-29,pp.510-514 (1980-06)

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

[5] 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」資料 (1991-05)

[6] 岩崎一彦, 西向井忠彦," 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)

[7] 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)

[8] 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(1990-04)

[9] 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", 信学技法,**R88-29**,pp.35-40(1988-11)

[10] M.Morii and K.Iwasaki, "A Note on Aliasing Probability for Multiple Input Signature Analyzer",IEEE Trans.on Computer,**42**,9,pp.1152(1993-09)

[11] 岩崎一彦," 距離2の最大距離分離符号の2元重みとその VLSI 自己テストへの応用", 信学論 (A),**J73-A**,no.11.pp.1851-1857(1990-09)

[12] 森井昌克, 常盤欣一朗, 笠原正雄,"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,(1987-08)

[13] 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)

[14] 森井昌克, 谷川晃一, 岩崎一彦," 多重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", 情報処理学会研究報告,91-DA-59,pp.1-8(1991-10)

[15] S.Feng,T.Fujiwara,T.Kasami and K.Iwasaki,"On the Maximum Value of Aliasing Probabilities for Single Input Signature Registers",VTS'93,pp.267-274(1993)