東海大学紀要

情報理工学部

Vol.20 2020

目次

PROCEEDINGS

OF THE

SCHOOL OF INFORMATION SCIENCE AND TECHNOLOGY TOKAI UNIVERSITY

SERIES J

CONTENTS

VOL.20 2020

Papers

東海大学紀要情報理工学部
Vol.20 , 2020, pp. 1–10
DOI: 10.18995/24352152. 20-1. 1

2 次元格子システムに対する最適配置問題とその解法

中村 太信 †1

Component Assignment Problem of Two-dimensional Lattice Systems and Its Solution

by

Taishin Nakamura

Abstract

現代社会には我々の社会や暮らしを支えている多くのシステムが存在する．これらのシステムをいかに安定的に稼働させるかが重要であり，システムが期待通りに動作し続けられる性質である信頼性の確保は課題となっている．信頼性工学 (特に，信頼性数理) の分野では，現実システムの特徴を捉えたシステムモデルが数多く提案されており，そのシステムモデルに対して，システムの性能評価方法，最適設計や最適保全方策などについての数理的手法の開発が行われている．本稿では，システムを構成する要素の集中故障を評価する “2 次元格子システム” を紹介し，筆者がこれまでに行った研究を紹介する．特に，信頼性工学分野において，困難かつ重要な問題である最適配置問題の関連研究と効率的な最適配置探索アルゴリズムについて詳しく説明する．高性能な計算機やソフトウェアが利用できる環境が整ってきているとしても，現実には手に負えない問題は数多く存在するが，問題が持つ数理的な性質を利用することで，工夫を凝らした効率的なアルゴリズムを構築することが可能となり，様々な現実問題の解決につながる．

Keywords: 信頼性工学，2 次元格子システム，最適配置問題，アルゴリズム

1 は じ め に

現代社会には我々の社会や暮らしを支えている多くのシステムが存在する．これらのシステムは障害が発生することなく機能し続けることはなく，いずれ故障し，要求された機能を発揮できなくなる．特に，原子力発電所や航空機が故障した場合には，単なる経済的損失に留まらず，人命を奪い，我々の生活に広範囲かつ甚大な被害をもたらす可能性がある．従って，システムをいかに安定的に稼働させるかが重要であり，システムが期待通りに動作し続けられる性質である信頼性の確保は課題となっている．信頼性工学が目指すのは，工学が関与しているあらゆるものづくりに関して，故障や誤作動せずに，期待どおりの機能を発揮する視点から，画一的に信頼性を付与することである [1].

現実のシステムを効率的・効果的に運用するためには，信頼度 (正常に稼働する確率) を適切な方法で評価し，システムの設計・運用段階に何らかの対策を講じることが必要となる．信頼性工学 (特に，信頼性数理) の分野では，現実システムの特徴を捉えたシステムモデルが数多く提案されており，そのシステムモデルに対して，システムの性能評価方法，最適設計や最適保全方策などについての数理的手法の開発が行われている．本稿では，システムを構成する要素の集中故障を評価する “2 次元格子システム” を紹介し，筆者がこれまでに行った研究を紹介する．特に，信頼性工学分野において，困難かつ重要な問題である最適配置問題の関連研究と効率的な最適配置探索アルゴリズムについて詳しく説明する．

2 2 次元格子システム

2 次元格子システムとは，システムの構成要素であるコンポーネントが 2 次元格子状に配置され，それらのコンポーネントが一定範囲に集中して故障するとシステム全体に影響を与えるシステム・現象を表現するシステムモデルである．現実には，コンポーネントがまばらに故障しても，周囲のコンポーネントが故障し

†1 情報理工学部 コンピュータ応用工学科

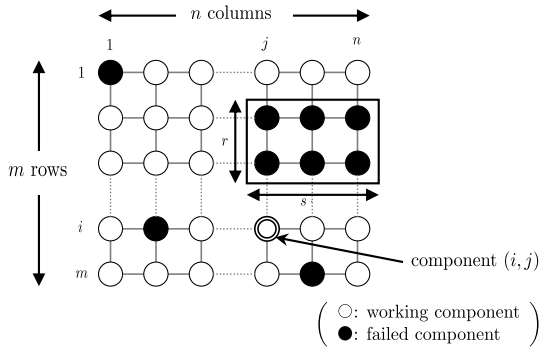

図 1　長方形型システム [3]

たコンポーネントの機能を補完するなどの理由により，システム全体としては正常に機能するが，コンポーネントが集中して故障するとシステムが正常に機能しなくなるという特徴を有するシステム (または，現象) が存在する．2 次元格子システムは，このような「コンポーネントが一定範囲に集中して故障すると故障する」というシステムの特徴を捉えたシステムモデルである．2 次元格子システムは,「システム形状」と「故障条件」により様々なバリエーションが存在する．本稿では「システム形状」の観点から分類した

- 長方形型システム
- 円筒型システム
- トーラス型システム

をそれぞれ紹介し，筆者がこれまでに行った研究を簡単に紹介する．

2.1　長方形型システム

長方形型 connected-**X**-out-of-(m,n):F システム (以下，長方形型システム) は，m 行 n 列の格子状にコンポーネントが配置されているシステムで，**X** はシステム故障の条件となるコンポーネントの故障形状を表す．例えば，**X** が (r,s) の場合，図 1 に示すように，r 行 s 列のコンポーネントがすべて故障する場合に故障となるシステムを表現できる [2]．また，**X** が $(1,2)$-or-$(2,1)$ の場合,「1 行 2 列のコンポーネントが故障する」もしくは「2 行 1 列のコンポーネントが故障する」(つまり，隣接した 2 つのコンポーネントが連続故障する) 場合に故障となるシステムを表現できる [2].

長方形型システムは，センサが (近似的に) 格子状に配置されたセンシングシステムを表現できる．センシングシステムとは，監視対象にセンサを配置することで，情報を収集し，その検出された情報に基づき，有用な情報を提供するシステムである．円形の監視範囲を持つセンサを監視範囲が重複するように格子状に配置することで，あるセンサが故障しても，周囲のセンサが監視範囲を補うため，領域全体を監視することができる．一方，センサが集中して故障すると，監視不可範囲が生じ，センシングシステムは正常に機能しなくなる．長方形型システムを用いることで，このようなセンシングシステムの信頼度評価・設計を実施することができる．その他にも，長方形型システムは液晶等の表示システムや部屋の照明などに適用できる [4].

信頼性工学の主要な問題の 1 つに信頼度算出問題がある．この問題は，コンポーネントの信頼度 (正常に動作する確率) が与えられたときに，システム全体の信頼度を算出する問題である．システムの設計段階において，システム信頼度を算出し，運用に先立って問題点を知ることは非常に有用である．一般的に，N 個のコンポーネントからなるシステム信頼度を求める場合には，コンポーネント故障が独立に生起するならば，すべてコンポーネントの状態を列挙し，それらの確率の総和によりシステム信頼度を求められる．しかし，その総数は 2^N であり，コンポーネント数が多い場合には膨大な計算時間を要する．そこで，Nakamura 他 [5] は，特別な場合の長方形型システムの信頼度を求める際，再帰方程式 [6] を行列表現に書き換え，行列のべき乗計算を工夫したことで高速に信頼度が求められることを示した．

既存方法 [7, 8] により信頼度の厳密値を求めることは理論的に可能であっても，システムの規模が大きいため，計算時間や記憶容量等，計算機の制約で計算実行が困難な場合が多く，信頼度算出可能なシステムのサイズは限定的である．そこで，Nakamura 他 [9] は，長方形型システムに対して，厳密方法と比べて短い時間で計算可能なシステム信頼度の上限値及び下限値を導出した．ここで，信頼度の上下限値とは，システムの信頼度がこの値以上でない，あるいはこの値以下でないことを保証する数値である．システム信頼度の厳密値は上限と下限の範囲内に収まっているため，上下限値が一致した場合にはその範囲においてシステム信頼度の厳密値とみなすことができる．

Nakamura 他 [10] は，Increasing Failure Rate (IFR) 保存問題に取り組んだ．この問題は，コンポーネントが IFR である (コンポーネントの故障率が時刻に対して単調増加する) ことがシステムにも保存されること，すなわち，システムも必ず IFR となることを明らかにする問題である．信頼性解析において，エージングは重要な概念であり，故障率関数の形状を把握することが求められる．コンポーネントが IFR であることがシステムにも保存されることが明らかにな

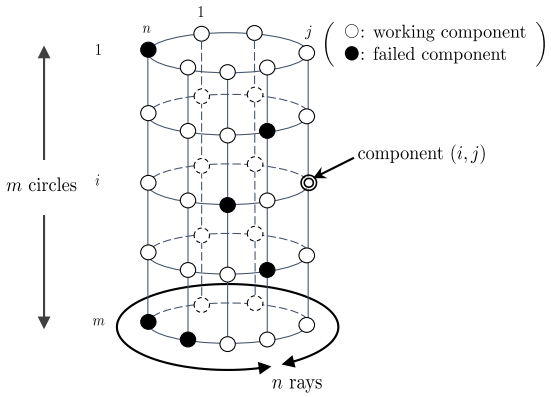

図 2　円筒型システム [3]

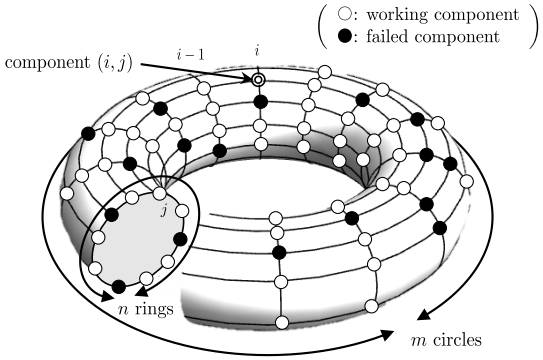

図 3　トーラス型システム [3]

れば，コンポーネントが任意の寿命分布を持つ場合における最適保全方策の提案 [11–13] などに寄与する．Nakamura 他 [10] では，システムの行数が $2, 3, 4$ の場合 (列数は任意) において，コンポーネントの IFR が保存されるシステムが 3 種類存在することを解析的に示した．システムの行数と列数がともに 5 以上のシステムに対しては，数値実験を行い，実験の範囲内ではコンポーネントの IFR が保存されるシステムが一つも存在しないことを確認した．

筆者は，最適配置問題にも取り組んできた．最適配置問題とは，各コンポーネントの信頼度が同一でない場合に，コンポーネントをどのように配置すればシステム信頼度が最大になるかという問題である．ここで，コンポーネントを自由に入れ替えてもシステムの機能としては問題がないことを前提とする．最適配置を求めることは，信頼性を保証したシステムを経済的に設計する上で重要となる．長方形型システムに対する最適配置問題に関しては 3 章で詳しく述べる．

2.2　円筒型システム

円筒型 connected-**X**-out-of-(m, n):F システム (以下，円筒型システム) は，長方形型システムの両端 2 辺を連結した構造を持ち，コンポーネントが m 円 n 放射の円筒状に配置されている (図 2)．

円筒型システムは，原子炉内の監視システムに適用できる．このシステムは円筒物の表面を覆うように温度センサが取り付けられており，領域内の温度分布を計測する．熱源の位置や形状を推定する際，熱源にある程度の大きさがあると考えると，複数の隣接したセンサの情報により熱源の位置や形状を検知することができる．しかし，センサが集中して故障すると，熱源を検知することができなくなり，システム故障となる．

Nakamura 他 [14] では，Finite Markov Chain Imbedding Approach (FMCIA) を用いて，円筒型システムに対する信頼度算出問題に取り組んだ．FMCIA とは,「システム故障が発生しないように，システムサイズを大きくする過程」を「マルコフ連鎖における状態遷移」に帰着させることで，マルコフ連鎖の考え方を利用したシステム信頼度算出方法である [15, 16]．具体的には，円筒型システムの構造を基にマルコフ連鎖を構築し，推移確率行列を求めた後，チャップマン＝コルモゴロフ方程式を用いることで，システム信頼度を得た．更に，効率的な信頼度算出を可能にするために，円筒型システムの特徴に応じた 2 種類の方法を提案した．数値実験により，特に，コンポーネント信頼度が同一である場合，提案方法は効率的にシステム信頼度を算出できることがわかった．これは，コンポーネント信頼度が同一である場合，すべての推移確率行列が等しくなるためである．

2.3　トーラス型システム

Nakamura 他 [17] は従来の長方形型システムや円筒型システムを拡張したコンポーネントがトーラス状に配置されたトーラス型 connected-**X**-out-of-(m, n):F システム (以下，トーラス型システム) を提案した．このシステムは，長方形型システムの上下と左右の 2 辺をそれぞれ連結した構造を持ち，コンポーネントが m 円 n 環のトーラス状に配置されている (図 2)．トーラス型の実システムには，荷電粒子加速器や,「京」「富岳」に採用されたアーキテクチャ [18] などの例がある．

Nakamura 他 [19] では，トーラス型システムに対して FMCIA を用いた信頼度算出方法を提案した．更に，Nakamura 他 [20] では，信頼度算出のための再帰方程式を導出し，それを利用したアルゴリズムを提案した．具体的には，トーラス型システムの信頼度を一部のコンポーネントの状態を与えた小さなシステムの和で表

すことで，再帰的にシステム信頼度を算出した．

2 次元格子システムに関する研究は，Kuo and Zuo [21], Yamamoto and Akiba [22], Akiba 他 [4], Cui 他 [23] などにまとめられている．

3 Lin/$(r,s)/(m,n)$:F システムに対する最適配置問題

本章では，長方形型 connected-(r,s)-out-of-(m,n):F システム (以下，Lin/$(r,s)/(m,n)$:F システム) に対する最適配置問題に関する関連研究を紹介し，筆者が行った研究での成果を示す．ここで，Lin/$(r,s)/(m,n)$:F システムとは，コンポーネントが m 行 n 列の格子状に配置されており，システム内の任意の位置において r 行 s 列内のコンポーネントがすべて故障するときにシステム故障となるシステムである (図 1)．また，最適配置問題とは，システム信頼度を目的関数として，それを最大化するコンポーネント配置を探索する問題である．対象とするシステムのコンポーネントを適切に並び替えることで，システム信頼度向上を実現し，安定的な運用が可能となる．3 章と 4 章では

(a) コンポーネントとシステムは稼働か故障の 2 状態を取り，
(b) コンポーネントは独立に故障し，
(c) コンポーネント信頼度は与えられており，
(d) コンポーネントは任意の位置に割り当てられる

ことを仮定する．

3.1 最適配置問題の定式化

本節では，Lin/$(r,s)/(m,n)$:F システムに対する最適配置問題の定式化を行う．$i = 1,2,\ldots,m$ と $j = 1,2,\ldots,n$ に対して，(i,j) をシステム内の i 行 j 列の位置とする．$\pi(i,j)$ $(\in \{1,2,\ldots,mn\})$ を位置 (i,j) に割り当てられたコンポーネント番号とすると，$m \times n$ 個のコンポーネントの配置は

$$\Pi = (\pi(i,j))_{1\le i\le m, 1\le j\le n} \tag{1}$$

によって表現される．コンポーネント番号を τ $(\in \{1,2,\ldots,mn\})$ とすると，コンポーネント τ の信頼度は p_τ と表され，一般性を失うことなく，$p_1 < p_2 < \ldots < p_{mn}$ とする．つまり，p_τ は τ 番目に信頼度の低いコンポーネントの信頼度を意味している．また，ベクトル $\boldsymbol{p} = (p_1, p_2, \ldots, p_{mn})$ を定義する．更に，$\boldsymbol{p}$ が与えられており，配置が Π である Lin/$(r,s)/(m,n)$:F システムの信頼度を $R((r,s),(m,n),\boldsymbol{p};\Pi)$ とする．これらの記号を用いて，Lin/$(r,s)/(m,n)$:F システムの最適配置問題は以下のように定式化される．

$$\Pi^* = \arg\max_{\Pi\in\Omega} R((r,s),(m,n),\boldsymbol{p};\Pi) \tag{2}$$

ただし，Ω はすべての配置 Π の集合とする．

3.2 最適配置問題に関する関連研究

本節では，Lin/$(r,s)/(m,n)$:F システムの最適配置問題に関する関連研究を紹介する．Lin/$(r,s)/(m,n)$:F システムの最適配置問題に関する研究は (A) 最適配置が持つ性質の調査と (B) 最適配置探索アルゴリズムの開発に大別される．

(A) 最適配置が持つ性質の調査　Zuo [24] は，$r = m$ もしくは $s = n$ の場合における Lin/$(r,s)/(m,n)$:F システムに対して最適配置が満足すべき必要条件を導出した．その後，Koutras 他 [25] は，Lin/$(r,s)/(m,n)$:F システムの最適配置が満足すべき必要条件を導出した．

定理 1 (Koutras 他 [25])**.** Lin/$(r,s)/(m,n)$:F システムにおいて，Π が最適配置である必要条件は

(a) $2 \le j \le \min\{s, n-s+1\}$ ならば，$i = 1,2,\ldots,m$ に対して，
$$\pi(i,j-1) < \pi(i,j)$$
(b) $\max\{n-s+2, s+1\} \le j \le n$ ならば，$i = 1,2,\ldots,m$ に対して，
$$\pi(i,j-1) > \pi(i,j)$$
(c) $2 \le i \le \min\{r, m-r+1\}$ ならば，$j = 1,2,\ldots,n$ に対して，
$$\pi(i-1,j) < \pi(i,j)$$
(d) $\max\{m-r+2, r+1\} \le i \le m$ ならば，$j = 1,2,\ldots,n$ に対して，
$$\pi(i-1,j) > \pi(i,j)$$

である．

ここで，$\pi(i,j-1) < \pi(i,j)$ は $p_{\pi(i,j-1)} < p_{\pi(i,j)}$，つまり，位置 $(i,j-1)$ よりも位置 (i,j) に信頼度の高いコンポーネントを割り当てることを意味している．必要条件を満たさない配置は，より目的関数値 (信頼度) が大きい配置が存在するため，最適配置になりえないことがわかる．最適配置を探索する際，必要条件を用いることで劣解を排除して解探索空間を削減することができる．そのため，必要条件は効率的に最適配置を探索する上で有用である．

信頼度を目的関数とする最適配置問題には「不変性」という概念がある．不変性とは最適配置がコンポーネント信頼度の値に依存せず，各コンポーネント信頼度の大小関係のみに依存する性質である．ほとんどのシ

ステムにおいては，最適配置はコンポーネント信頼度の値に依存する (不変な最適配置が認められない) ことが確認されているが，中には，不変な最適配置を認めるシステムが存在する．その場合，コンポーネント信頼度の大小関係がわかれば，計算機を用いることなく，最適配置を決定することができる．Hwang and Dinghua [26] は，以下の定理により，$r = m$ $(s = n)$ の場合における Lin/(r, s)/(m, n):F システムの不変性の存在条件を明らかにしている．

定理 2 (Hwang and Dinghua [26])．(a) $r = 2$ かつ $s = n - 1$，(b) $r = 2$ かつ $s = 1$，(c) $s = n$ のいずれかの場合においては，Lin/(r, s)/(r, n):F システムは不変な最適配置を認める．

例えば，Lin/$(2, 1)$/$(2, 5)$:F システム ((b) の場合) の最適配置は

$$\Pi^* = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 10 & 9 & 8 & 7 & 6 \end{pmatrix} \qquad (3)$$

である．ここで，行列内の値はコンポーネント番号であり，$p_1 < p_2 < \ldots < p_{10}$ である．

(B) 最適配置探索アルゴリズムの開発　計算機の性能向上に伴い，問題例によっては多少の時間はかかるとしても，最適性が保証された解を得ることが可能となった．しかし，最適配置問題は NP 困難な組合せ最適化問題であるため，実用的な規模の問題例に対しては分枝限定法などの汎用的手法を単に適用するだけでは最適配置を得ることは難しい．そこで，与えられる入力ケースの性質を利用した効率的な最適配置探索アルゴリズムは開発されてきた．Omura 他 [27] は分枝限定法をベースとして，$r = m - 1$ かつ $2s > n$ の場合におけるアルゴリズムを開発した．

また，対象とするシステムを取り扱いが容易なシステムに帰着させることで，最適配置探索の効率化を行った研究もおこなわれている．このことは，単純化されたシステムの最適配置を求められれば，元の Lin/(r, s)/(m, n):F システムの最適配置も求まることを意味する．Omura 他 [28] は，$r = m$ かつ $s = 2$ の場合において，Lin/(r, s)/(m, n):F システムを単純なシステムに帰着させ，そのシステムが持つ不変性を使用した最適配置探索アルゴリズムを開発した．Nakamura 他 [29] は，$r = m$ の場合における Lin/(r, s)/(m, n):F システムを単純なシステムに帰着させ，効率的なアルゴリズムを提案した．Nakamura 他 [30] は，$r = m - 1$ かつ $s = n - 1$ の場合に特化したアルゴリズムを提案した．基本的な考え方としては，Lin/(r, s)/(m, n):F システムが $r = m - 1$ かつ $s = n - 1$ の条件を満たすとき，定理 1 [25] を用いることで「mn 個のコンポーネントで構成された Lin/(r, s)/(m, n):F システム」は「$2(m + n) - 5$ 個のコンポーネントが円状に配置されたシステム」に帰着可能であることを理論的に示した．Nakamura 他 [30] は，この単純化されたシステムに対する最適配置探索アルゴリズムを提案した．

このように最適配置を効率よく探索するアルゴリズムの開発は行われてきた．しかし，Nakamura 他 [29] のアルゴリズムは $r = m$ の場合，Nakamura 他 [30] のアルゴリズムは $r = m - 1$ かつ $s = n - 1$ の場合のように既存のアルゴリズムは故障条件が限定されており，一般的な Lin/(r, s)/(m, n):F システムには適用することができなかった．そこで，Nakamura and Yamamoto [31] により，一般的な Lin/(r, s)/(m, n):F システムに対して，効率的に最適配置を探索するアルゴリズムの開発が行われた．

4 Lin/(r, s)/(m, n):F システムに対する最適配置探索アルゴリズム

本章では，Nakamura and Yamamoto [31] により提案された Lin/(r, s)/(m, n):F システムに対する最適配置探索アルゴリズムを紹介する．

4.1 基本となるアイデア

まず，アルゴリズムの基本となるアイデアを述べる．探索木を用いて，すべての配置 (解候補) を列挙し，その中から最適配置を見つける場合，多くの計算量を要し，実用的な時間で最適配置を求めることは困難である．特に，Lin/(r, s)/(m, n):F システムに対する最適配置問題の場合，目的関数の計算に大きな計算コストが必要となる．これを回避するためには，最適配置となる見込みのない配置を可能な限り列挙しないことが重要である．分枝限定法では，基本的には全列挙と同様に探索木を用いた探索を行うが，その過程で最適配置になりえないことが何らかの理由によって示される場合，それ以上の探索を行わない．これを限定操作，もしくは，枝刈りという．Nakamura and Yamamoto [31] により提案されたアルゴリズムでは，分枝限定法をベースに限定操作により，探索する配置数を抑えることで効率的に最適配置を探索する．具体的には，以下の 3 種類の枝刈り条件により限定操作を行う．

- 必要条件に基づく枝刈り条件
- 対称配置を排除する枝刈り条件
- システム信頼度に基づく枝刈り条件

更に，前処理を行うことで，割り当てるコンポーネン

ト数を減じ，予め問題の規模を小さくする．

4.2 前 処 理

本節では，分枝限定法を実行する前に実施する前処理を説明する．定理 1 [25] により，最適性を失うことなく，以下の前処理によって割り当てるコンポーネント数を減らすことができる．

系 1. $2r > m$ かつ $2s > n$ ならば，最も信頼度の低いコンポーネントは位置 $(1,1)$ に，信頼度の高い $(2r-m)(2s-n)$ 個のコンポーネントは以下の集合 C の要素である位置に割り当てる．

$$C = \{(i,j) \mid m-r+1 \le i \le r, n-s+1 \le j \le s\}.$$

Lin/(r,s)/(m,n):F システムが $2r > m$ かつ $2s > n$ を満たすならば，この前処理を行うことで，割り当てるコンポーネント数を mn 個から $(mn-(2r-m)(2s-n)-1)$ 個まで減じることができる．

4.3 必要条件に基づく枝刈り条件

本節では，最適配置が満足すべき必要条件 [25] に基づく枝刈り条件を示す．

まず，位置 $(1,1)$ に割り当てられるコンポーネントを限定するための条件を与える．

枝刈り条件 1. 位置 $(1,1)$ にコンポーネントが割り当てられたとき，

(i) $2r \ge m$ かつ $2s \ge n$ ならば，$\pi(1,1) = 1$

(ii) $2r \ge m$ かつ $2s < n$ ならば，

$$\pi(1,1) \le mn - 2sm + 1$$

(iii) $2r < m$ かつ $2s \ge n$ ならば，

$$\pi(1,1) \le mn - 2rn + 1$$

(iv) $2r < m$ かつ $2s < n$ ならば，

$$\pi(1,1) \le mn - 4rs + 1$$

を満たさなければ，枝刈りを行う．

例えば，$2r \ge m$ かつ $2s < n$ ならば，τ 番目に信頼度の低いコンポーネント $(1 \le \tau \le mn - 2sm + 1)$ を位置 $(1,1)$ に割り当てる．

次に，最適配置において位置 (i,j) に割り当てられるコンポーネントは以下の条件を満たす．

枝刈り条件 2. 位置 (i,j) にコンポーネントが割り当てられたとき，

(i) $i = 1,2,\ldots,m$ に対して，$2 \le j \le s$ ならば，

$$\pi(i,j-1) < \pi(i,j)$$

(ii) $i = 1,2,\ldots,m$ に対して，$\max\{n-s+2, s+1\} \le j \le n$ ならば，

$$\pi(i,j-1) > \pi(i,j)$$

(iii) $j = 1,2,\ldots,n$ に対して，$2 \le i \le r$ ならば，

$$\pi(i-1,j) < \pi(i,j)$$

(iv) $j = 1,2,\ldots,n$ に対して，$\max\{m-r+2, r+1\} \le i \le m$ ならば，

$$\pi(i-1,j) > \pi(i,j)$$

を満たさなければ，枝刈りを行う．

4.4 対称配置を排除する枝刈り条件

Lin/(r,s)/(m,n):F システムにおいて，コンポーネント信頼度が与えられたとき，システム信頼度はコンポーネントの相対的な配置によって決まる．すなわち，回転や反転の操作により，同じシステム信頼度を持つ本質的に等価な複数の配置が現れる．従って，最適配置を求める場合には，本質的に等価な配置のうち 1 つの配置を列挙すれば，他の配置を列挙する必要はない．そのため，提案するアルゴリズムでは，以下の条件を満足する配置のみを考える．

枝刈り条件 3.

(i) $m \ne n$ もしくは $r \ne s$ ならば，

$$\pi(1,1) = \min\left\{ \begin{array}{l} \pi(1,1), \pi(m,1), \\ \pi(1,n), \pi(m,n) \end{array} \right\} \tag{4}$$

(ii) $m = n$ かつ $r = s$ ならば，式 (4) と

$$\pi(m,1) < \pi(1,n) \tag{5}$$

を満たさなければ，枝刈りを行う．

ここで，式 (4) は，位置 $(1,1), (m,1), (1,n), (m,n)$ に割り当てられるコンポーネントの中で最も信頼度の低いコンポーネントを位置 $(1,1)$ に割り当てることを意味する．

4.5 システム信頼度の計算

最適配置探索アルゴリズムでは，位置 (m,j) $(j = 1,2,\ldots,n)$ にコンポーネントが割り当てられた時点において，Yamamoto and Miyakawa [6] が導出した再

帰方程式を用いて部分的にシステム信頼度を計算する．その再帰方程式は紙面の都合上，割愛する．

最適配置問題を解く際，効率的な信頼度算出方法を用いても，多くの信頼度計算が求められるため，多くの計算時間を要する．従って，わずかな時間であってもシステム信頼度の計算時間を短縮することは非常に重要となる．そこで，分枝操作では一部のコンポーネントのみが異なる配置が逐次的に列挙されることに着目し，異なる部分に対して差分計算することで信頼度計算の高速を実現する．

例として，Lin/(2,2)/(3,5):F システムにおいて，以下の配置 Π_A, Π_B を持つ 2 つのシステムを考える．

$$\Pi_A = \left(\begin{array}{ccc|c|c} 1 & 8 & 5 & 10 & \cdot \\ 12 & 15 & 13 & 14 & \cdot \\ 2 & 7 & 6 & 9 & \cdot \end{array}\right) \tag{6}$$

$$\Pi_B = \left(\begin{array}{ccc|c|c} 1 & 8 & 5 & 9 & \cdot \\ 12 & 15 & 13 & 11 & \cdot \\ 2 & 7 & 6 & 4 & \cdot \end{array}\right) \tag{7}$$

ここで，行列内の “$\cdot$” はコンポーネントが割り当てられていないことを意味する．式 (6) と式 (7) に示すように，$R((2,2),(3,5),\boldsymbol{p};\Pi_A)$ と $R((2,2),(3,5),\boldsymbol{p};\Pi_B)$ では 1 列目から 3 列目の配置は共通である．よって，一方の信頼度を求める際に共通となる値を記憶しておくことで，もう一方の信頼度を少ない計算量で求めることができる．このように，多くの配置に対応するシステム信頼度を計算する際には，特定の値を記憶し，利用することで冗長な計算を回避し，効率的な信頼度計算が可能となる．

また，システム信頼度を用いた限定操作を実施する．システム信頼度は列 n に対して非増加関数であるため，部分的にコンポーネントが配置されたシステムの信頼度がこれまでの探索で得られた最良の配置に対応するシステム信頼度を下回った場合は，さらにコンポーネントを割り当てても信頼度は増加しない．つまり，それ以上コンポーネントを割り当てる必要はない．そこで，提案アルゴリズムでは，システム信頼度に基づく枝刈りを実施する．

枝刈り条件 4. $j = s, s+1, \ldots, n$ に対して，位置 (m,j) にコンポーネントが割り当てられたとき，

$$\mathbf{Rmax} \leq R((r,s),(m,j),\boldsymbol{p};\Pi) \tag{8}$$

を満たさなければ，枝刈りを行う．ここで，**Rmax** はこれまでの探索で得られた最良の配置に対応するシステム信頼度である．

4.6 最適配置探索アルゴリズムの手順

次に，分枝限定法を用いた提案アルゴリズムの手順を簡単に説明する．具体的な手順は，Nakamura and Yamamoto [31] を参照されたい．

まず，$2r > m$ かつ $2s > n$ を満たすのであれば，系 1 の前処理を行う．その後，コンポーネントを $(2,1),(3,1),\ldots,(m,1),(1,2),\ldots,(m,2),(1,3),\ldots,(m,n)$ の順に割り当てる．このとき，前処理により既にコンポーネントが割り当てられているならば，その位置への割り当てはスキップする．分枝限定法により割り当てられるコンポーネント数を α とすると，

$$\alpha = \begin{cases} mn - (2r-m)(2s-n) - 1 & \\ \qquad\qquad 2r > m \text{ かつ } 2s > n \text{ の場合} & \\ mn \qquad \text{その他} & \end{cases} \tag{9}$$

となる．上記の順にコンポーネントを割り当てるとき，$k = 1, 2, \ldots, \alpha$ に対して，DFS(k) を k 番目の位置にコンポーネント割り当てるための処理ルーチンとする．処理ルーチン DFS(k) の流れは以下のとおりである．

STEP 1: 枝刈り条件 1 を用いて限定操作を行う．
STEP 2: 枝刈り条件 2 を用いて限定操作を行う．
STEP 3: 枝刈り条件 3 を用いて限定操作を行う．
STEP 4: m 行目にコンポーネントが割り当てられたとき，再帰方程式 [6] を用いてシステム信頼度を算出する．
STEP 5: 枝刈り条件 4 を用いて限定操作を行う．
STEP 6: mn 個すべてのコンポーネントが割り当てられた配置が **Rmax** よりも大きければ，その配置を保存し，**Rmax** を更新する．

上記の操作をすべての配置を列挙するまで繰り返し，すべての配置を列挙し終えた後，システム信頼度が **Rmax** である配置が最適配置となる．

4.7 数値実験の結果

本節では，Nakamura and Yamamoto [31] のアルゴリズムと Omura 他 [27] のアルゴリズムを計算時間の観点から比較する．本来，アルゴリズム [27] は，$r = m-1$ かつ $2s > n$ の場合にのみ探索可能であるが，比較のため，一般化を行った．表 1 にアルゴリズム [31] のアルゴリズム [27] の計算時間の比較結果を示す．表中の “N/A” は最適配置の探索に 24 時間以上要することを意味する．表 1 に示すように，アルゴリズム [31] は，アルゴリズム [27] に比べて，短い時間で最適配置が求められる．以上のことから，枝刈り条件による限定操作が有効に機能していることがわかる．

表 1 計算時間比較 (秒) [3]

(r,s)	$(2,2)$	$(3,2)$	$(3,3)$	$(3,3)$	$(3,4)$	$(3,3)$	$(4,4)$	$(4,5)$	$(5,4)$	$(5,5)$
(m,n)	$(4,4)$	$(4,4)$	$(4,4)$	$(4,5)$	$(4,5)$	$(5,4)$	$(5,5)$	$(5,6)$	$(6,5)$	$(6,6)$
(A) アルゴリズム [31]	408.81	52.84	0.08	3686.04	2.30	4548.24	40.84	1144.77	1532.19	19645.68
(B) アルゴリズム [27]	462.77	72.45	7.23	19529.64	6066.08	41857.86	N/A	N/A	N/A	N/A
(A)/(B)	88.34%	72.93%	1.12%	18.87%	0.04%	10.87%	—	—	—	—
システム信頼度	0.328	0.782	0.960	0.943	0.989	0.943	0.998	0.992	0.992	0.997

4.8 ま と め

本章では，Lin/(r,s)/(m,n):F システムに対して，分枝限定法をベースとして，必要条件に基づく枝刈り条件，対称配置を排除する枝刈り条件，システム信頼度に基づく枝刈り条件を組み込んだ最適配置探索アルゴリズムを紹介した．更に，前処理によって最適性を失うことなく割り当てるコンポーネント数を減らした．加えて，分枝操作では一部のコンポーネントのみが異なる配置が逐次的に列挙されることに着目し，異なる部分に対して差分計算することで信頼度計算の高速を実現した．Nakamura and Yamamoto [31] で実施された計算機実験では，このアルゴリズムは，既存アルゴリズム [27] と比較して，短時間で最適配置が得られることを確認した．

Nakamura and Yamamoto [31] で得られた成果の 1 つは，最も信頼度が高い (故障に強い) コンポーネント配置が得られることである．先行研究 [27–30] では，適用可能なシステムに制限があったが，提案アルゴリズムでは，(理論的には) 一般的な Lin/(r,s)/(m,n):F システムの最適配置を得ることができる．最適配置が得られることで，信頼性を保証したシステムを経済的に設計することが可能となり，現実のシステムを設計・運用するための指針が従来よりも的確に提案可能になると考えられる．センシングシステムに限らず,「構成要素の集中異常がシステム全体に影響を与える」という現象は様々なところで見られるため，Lin/(r,s)/(m,n):F システムとして表現可能な多様な現実システムの信頼度向上が期待できる．

しかし，現実に現れる問題例は規模が大きいことが多く，その場合，提案アルゴリズムを用いても最適配置を得ることが極めて困難となる．実務上，常に最適解が求められているわけではないため，良質な準最適解を出来るだけ効率良く求めることを目指す発見的解法の構築が求められる．その際，遺伝的アルゴリズムやアントコロニー最適化などの汎用的なメタ戦略を単に適用するのではなく，Nakamura and Yamamoto [31] で導出した枝刈り条件を組み込むことで，解探索空間を狭め，探索効率の向上が期待できる．更に，提案アルゴリズムで得られる解は最適性が保証されているため，発見的解法の評価に理論的裏打ちを与えることができる．このように，発見的解法の構築及び評価においても Nakamura and Yamamoto [31] は貢献可能であると考えている．

5 お わ り に

本稿では，長方形型・円筒型・トーラス型システムを紹介し，それらに対してこれまでに行ってきた研究を簡単に紹介した．更に，これまでの研究成果の 1 つとして，信頼性工学分野において，困難かつ重要な問題である最適配置問題に対する効率的な最適配置探索アルゴリズムを説明した．高性能な計算機やソフトウェアが利用できる環境が整ってきているとしても，現実には手に負えない問題は数多く存在する．しかし，問題が持つ数理的な性質を利用し，工夫を凝らした効率的なアルゴリズムを構築することで，様々な現実問題の解決に貢献できると考えている．

近年，第 4 次産業革命ともいわれる，IoT, ビッグデータ，AI をはじめとするデータ利活用の技術が急速に進展してきており，これらの技術により，収集されたデータをもとに瞬時に判断することが可能になりつつある．信頼性工学の分野においても，IoT によるデータ収集が行われており，これまで解析が困難であった部材や部品の製造状況や製品の使用状況のデータを容易に収集することが可能となっている [32]．このような変化に伴って新たな課題が生じており，その課題に対する解決策の提供が求められる．AI やデータを軸とする第 4 次産業革命に対応すべく，今後も信頼性工学における諸問題に取り組んでいく．

参 考 文 献

[1] 福井 泰好,『入門 信頼性工学 (第 2 版) 確率・統計の信頼性への適用』，森北出版株式会社，2016.

[2] T. K. Boehme, A. Kossow, and W. Preuss, “A generalization of consecutive-k-out-of-n:F systems,” *IEEE Transactions on Reliability*, vol. 41, no. 3, pp. 451–457, 1992.

[3] T. Nakamura, “Study on reliability evaluation and

optimal design of connected-**X**-out-of-(m, n):F lattice systems," 首都大学東京大学院システムデザイン研究科博士論文，2020.

[4] T. Akiba, T. Nakamura, X. Xiao, and H. Yamamoto, "Evaluation methods for reliability of consecutive-k systems," in *Systems Engineering: Reliability Analysis Using k-out-of-n Structures*, M. Ram and T. Dohi, Eds. CRC Press, 2019, ch. 1, pp. 1–24.

[5] T. Nakamura, H. Yamamoto, and X. Xiao, "Fast calculation methods for reliability of connected-(r, s)-out-of-(m, n):F lattice system in special cases," *International Journal of Mathematical, Engineering and Management Sciences*, vol. 3, no. 2, pp. 113–122, 2018.

[6] H. Yamamoto and M. Miyakawa, "Reliability of a linear connected-(r, s)-out-of-(m, n):F lattice system," *IEEE Transactions on Reliability*, vol. 44, no. 2, pp. 333–336, 1995.

[7] Y. Higashiyama, "An algorithm for exact reliability of consecutive 2-out-of-(m, n):F system with un-equal component probability," in *Proceedings of the IEEE Region 10 Conference*, vol. 2, 1999, pp. 990–993.

[8] H. Yamamoto, T. Akiba, H. Nagatsuka, and Y. Moriyama, "Recursive algorithm for the reliability of a connected-$(1, 2)$-or-$(2, 1)$-out-of-(m, n):F lattice system," *European Journal of Operational Research*, vol. 188, no. 3, pp. 854–864, 2008.

[9] T. Nakamura, H. Yamamoto, T. Shinzato, and T. Akiba, "Upper and lower bounds for reliability of connected-$(1, 2)$-or-$(2, 1)$-out-of-(m, n):F lattice system," in *Proceedings of the 19th Asia Pacific Industrial Engineering and Management Systems*, 6 pages, 2018.

[10] T. Nakamura, H. Yamamoto, X. Xiao, and T. Akiba, "The increasing failure rate property of connected-$(1, 2)$-or-$(2, 1)$-out-of-(m, n):F lattice systems — the case of $m = 2, 3, 4$ —," in *Proceedings of the 8th Asia-Pacific International Symposium on Advanced Reliability and Maintenance Modeling*, pp. 45–51, 2018.

[11] W. Y. Yun and A. J. Endharta, "Preventive maintenance of consecutive multi-unit systems," in *Advances in Reliability and System Engineering*, M. Ram and J. P. Davim, Eds. Springer, 2017, pp. 27–51.

[12] L. Zhou, H. Yamamoto, T. Nakamura, and X. Xiao, "Optimization problems for consecutive-2-out-of-n:G system," *Communications in Statistics - Theory and Methods*, vol. 49, no. 15, pp. 3792–3807, 2020.

[13] L. Zhou, H. Yamamoto, T. Nakamura, and X. Xiao, "Optimization problems for consecutive-k-out-of-n:G systems," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E103-A, no. 5, pp. 741–748, 2020.

[14] T. Nakamura, H. Yamamoto, T. Shinzato, X. Xiao, and T. Akiba, "Reliability of a circular connected-$(1, 2)$-or-$(2, 1)$-out-of-(m, n):F lattice system with identical components," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E100-A, no. 4, pp. 1029–1036, 2017.

[15] L. Cui, Y. Xu, and X. Zhao, "Developments and applications of the finite Markov chain imbedding approach in reliability," *IEEE Transactions on Reliability*, vol. 59, no. 4, pp. 685–690, 2010.

[16] L. Cui, C. Lin, and H. Yang, "Analysis for a qualification test procedure with FMCIA (finite Markov chain imbedding approach)," in *Mathematics Applied to Engineering*, M. Ram and J. P. Davim, Eds. Academic Press, 2017, ch. 1, pp. 1–20.

[17] T. Nakamura, H. Yamamoto, X. Xiao, and T. Akiba, "Reliability of a toroidal connected-$(1, 2)$-or-$(2, 1)$-out-of-(m, n):F lattice system," in *Proceedings of the 7th Asia-Pacific International Symposium on Advanced Reliability and Maintenance Modeling*, pp. 399–406, 2016.

[18] 安島雄一郎，井上智宏，平本新哉，清水俊幸，"スーパーコンピュータ「京」の インターコネクト Tofu," *Fujitsu*, vol. 63, no. 3, pp. 260–264, 2012.

[19] T. Nakamura, H. Yamamoto, T. Shinzato, X. Xiao, and T. Akiba, "Proposal of calculation method for reliability of toroidal connected-$(1, 2)$-or-$(2, 1)$-out-of-(m, n):F lattice system with Markov chain," in *Reliability Modeling With Computer and Maintenance Applications*, S. Nakamura, C. H. Qian, and T. Nakagawa, Eds. World Scientific, 2017, ch. 7, pp. 139–153.

[20] T. Nakamura, H. Yamamoto, and T. Akiba, "Reliability of a toroidal connected-(r, s)-out-of-(m, n):F lattice system," *Journal of Risk and Reliability*, 10 pages, 2020 (Early Access).

[21] W. Kuo and M. J. Zuo, *Optimal Reliability Modeling: Principles and Applications*. John Wiley and Sons, 2003.

[22] H. Yamamoto and T. Akiba, "Survey of reliability studies of multi-dimensional consecutive-k-out-of-n:F systems," *Reliability Engineering Associ-*

ation of Japan, vol. 25, no. 8, pp. 783–796, 2003.

[23] L. Cui and D. Qinglai, "Consecutive k and Related Models—A Survey," in *International Conference of Celebrating Professor Jinhua Cao's 80th Birthday*, Q. L. Li, J. Wang, and H.B. Yu, Eds. Springer, 2019, ch. 1, pp. 3–18.

[24] M. Zuo, "Reliability & design of 2-dimensional consecutive-k-out-of-n systems," *IEEE Transactions on Reliability*, vol. 42, no. 3, pp. 488–490, 1993.

[25] M. V. Koutras, G. K. Papadopoulos, and S. G. Papastavridis, "Note: Pairwise rearrangements in reliability structures," *Naval Research Logistics*, vol. 41, no. 5, pp. 683–687, 1994.

[26] F. K. Hwang and S. Dinghua, "Redundant consecutive-k systems," *Operations Research Letters*, vol. 6, no. 6, pp. 293–296, 1987.

[27] T. Omura, H. Yamamoto, X. Xiao, and T. Akiba, "Algorithm for obtaining optimal arrangement of a connected-(r, s)-out-of-(m, n):F system — the case of $m = r + 1$ and $2s > n$ —," in *Proceedings of the 16th Asia Pacific Industrial Engineering and Management Systems Conference*, 2015, pp. 652–659.

[28] T. Omura, T. Akiba, H. Yamamoto, and X. Xiao, "Algorithm for obtaining optimal arrangement of a connected-(r, s)-out-of-(m, n):F system — the case of $m = r$ and $s = 2$ —," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E98-A, no. 10, pp. 2018–2024, 2015.

[29] T. Nakamura, H. Yamamoto, T. Akiba, and K. Shingyochi, "Algorithm for the component assignment problem in redundant consecutive-k-out-of-n:F systems," in *Proceedings of the 20th Asia Pacific Industrial Engineering and Management Systems Conference*, 2019, pp. 152–157.

[30] T. Nakamura, H. Yamamoto, and T. Akiba, "Fast algorithm for optimal arrangement in connected-$(m-1, n-1)$-out-of-(m, n):F lattice system," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E101-A, no. 12, pp. 2446–2453, 2018.

[31] T. Nakamura and H. Yamamoto, "Algorithm for solving optimal arrangement problem in connected-(r, s)-out-of-(m, n):F lattice system," *IEEE Transactions on Reliability*, vol. 69, no. 2, pp. 497–509, 2020.

[32] 斎藤 彰，"AI の進化は故障解析に何をもたらすのか ～その期待とリスク～," 日本信頼性学会誌　信頼性, vol. 40, no. 2, pp. 64–71, 2018.

東海大学紀要情報理工学部
Vol.20 , 2020, pp. 11–18
DOI: 10.18995/24352152. 20-1.11

Introduce the CyExec System for Cybersecurity Training Platform and Cybersecurity Research Trends Related to Data Analysis

by

Sanggyu Shin †1

Abstract

Recently, the threats of cyberattacks, mainly targeted attacks, are increasing rapidly, and many cybersecurity incidents are frequently occurring. On the other hand, capable personnel is much lacking, becoming an urgent issue that strengthens the systematic human resource development cultivating cybersecurity activities capabilities. Only a few universities and companies in Japan are conducting education using an effective training system on the market because of expensive and difficult to use that adopted and operation the training system like Cyber Range in higher education institutions and SMEs. In this paper, I introduce CyExec, an effective cybersecurity training platform that can be exercised at a lower cost and based on the open environment. Also, I introduce the cybersecurity research trends related to data analysis.

Keywords: CyExec, cybersecurity, training platform

1 Introduction

This paper introduces CyExec, a training platform for cybersecurity education based on a virtual environment [1]. Additionally, recapitulate the cybersecurity education curriculum and research trends related to data analysis.

It is the world problem that the growing workforce shortage of qualified cybersecurity professionals and practitioners. On the CSO website, both government and non-government sources project nearly 1.8 million cybersecurity-related positions going unfilled by 2022 [2]. The workforce demand is acute, immediate, and growing worldwide [3].

Cyberattacks are bringing profound social influences, causing vast cybersecurity incidents and even affecting business continuity. In Japan, $530 million of cryptocurrencies stolen occurred in January 2018, and cyberattacks targeted the organizations associated with the Pyeongchang Winter Olympics in February 2018 [4]. Kevin Morooney – former Vice Provost for Information Technology at Pennsylvania State University – told The New York Times that Penn State faced an average of 20 million attacks per day, an amount "typical for a research university [5]."

A recent study conducted by consulting firm Frost & Sullivan projects that there will be 1.8 million unfilled cybersecurity jobs by 2020 in America and that this talent shortage exists on a global scale, with nearly 70 percent of professionals globally saying there are too few cybersecurity workers on staff. With demand for cybersecurity talent far outpacing supply, companies often pay top dollar for cybersecurity expertise [6]. On cybersecurity strategy of the Government of Japan cited human resource development as a serious issue. The Japanese government also estimated the insufficiency of human resources of cybersecurity to grow at 190,000 by 2020. Additionally, the lack of technical knowledge and skill is worried even in personnel engaged in cybersecurity operations [7][8].

In an effort to develop a security workforce, some higher education institutions provide practical exercise-style education. For example, Cyber Range provides exercise environments that are similarly real-world for assuming an actual security incident [9][10]. Participants of the Cyber Range exercises learn practical defense technology against

†1 Tokai University, Kanagawa, Japan

an assumed cyberattack on the virtual environment network. Participants also learn the systematic correspondence method depending on the organization's roles by using possible realistic scenarios such as real malware infection. Therefore, high training effects can be expected [9].

However, universities have not enough exercise infrastructure to bring up a cybersecurity workforce because of the high cost of introducing the practical exercises system and the lack of personnel to maintain the practice environment. Therefore, it is strongly required in the universities that a cybersecurity exercise platform can promote joint development and typical use. These requirements are the reason why we developed a cybersecurity exercises platform, "Cybersecurity Exercises" (from now on referred to as CyExec), using a virtual computer environment of VirtualBox and Docker [11][12].

In this paper, I introduce the constitution of the cybersecurity exercises platform CyExec and the training contents we implemented on it. In Chapter 2, I introduce cybersecurity in higher education, including the topics that the international standard of cybersecurity education and information security education in Japan. Introduces an overview of the CyExec that cybersecurity exercise system in Chapter 3. Chapter 4 introduces the cybersecurity trends recently, and Chapter 5 introduces cybersecurity and data analytics.

2 Cybersecurity in Higher Education

Some strategies exist for combating the cyberattacks faced by society. Some involve strategies that higher education IT professionals must employ themselves, while others include strategies that everyone in the higher education community, including end-users, must implement. Though the cybersecurity challenges facing higher education are significant and the cost of solving them is steep, the potential financial and reputational risks that come with insufficient defense are likely even higher [6].

Cybersecurity education is an issue not only in advanced countries but also in developing nations. The ability to prevent successful cyberattacks against a nation ' s critical infrastructure depends on the availability of a skilled cyber-literate workforce, and therefore, on an educational system that can build such capabilities [13].

2.1 Standard of Cybersecurity Education

Whether developing full new programs, defining new concentrations within existing programs, or augmenting existing course content, these institutions need curricular guidance based on a comprehensive view of the cybersecurity field, the base discipline's specific demands, and the relationship between the curriculum and cybersecurity workforce frameworks. In August 2015, the Association for Computing Machinery (ACM) Education Board recognized this urgent need [14]. It took measures to assemble a Joint Task Force on Cybersecurity Education (CSEC2017) with other professional and scientific computing societies to develop comprehensive curricular guidance in cybersecurity education [15]. Based on this mission, the CSEC2017 JTF established the following goals for the curricular volume:

- To describe a vision of proficiency in cybersecurity,
- To define a structure for the cybersecurity discipline by developing a thought model that defines the boundaries of the domain and outlines critical dimensions of the curricular design,
- To support the alignment of academic programs with industry needs in cybersecurity,
- To involve a broad global audience of stakeholders through continuous community engagement during the development process,
- To develop curricular guidance that is comprehensive enough to support a wide range of program types, and
- To develop curricular advice grounded in fundamental principles that provide stability yet is structured to provide flexibility to support evolving program needs.

2.2 Information security education in Japan

The environment surrounding ICT in Japan has been changing day by day, and information security threat has increased. It can be said that about 147 million viruses have been detected so far; nearly 18 million new malware were found in the second quarter of 2013. In order to improve this environment, the education for information security is started in

the kindergarten stage in japan [16].

The primary cybersecurity education and training programs available in Higher Education, which we believe are mostly unknown outside the country. Typical training systems include Secure Eggs, enPiT-Security (also known as SecCap), and CYDER [17].

Secure Eggs is an introductory hands-on cybersecurity course offered by Nomura Research Institute (NRI) Secure Technologies. The word Eggs in the program title, an acronym for "Essentials and Global Guidance for Security," emphasizes the program's focus on necessary cybersecurity skills [18].

A consortium of five Japanese universities started the enPiT-Security training program: JAIST, Tohoku University, Nara Institute of Science and Technology, Keio University, and Institute of Information Security. The SecCap program is a curriculum for university students to develop the necessary skills needed by IT security engineers through courses and hands-on activities regarding security-related aspects of operating systems, software, networks, and malware-related countermeasures technologies. The program participants were selected based on their cybersecurity knowledge and interests among the students at the end of their studies in the five participating universities [17][19].

CYDER (CYber Defense Exercise with Recurrence) is a training program initiated in September 2013 by the Ministry of Internal Affairs and Communications in Japan [6]. The program focuses on the improvement of competence in dealing with cyberattacks of the IT and cybersecurity-related personnel of central government offices, independent administrative agencies, and large companies. The practical cybersecurity training conducted in the CYDER program takes place over two days, based on a training scenario defined by several organizing parties. Throughout the program, there is a focus on the use of hands-on training so that the trainees become able to handle potential cybersecurity incidents in real life [20].

2.3 Cybersecurity training in higher education

In order to know the state of cybersecurity education, Y. Seto, et al. researched the contents/courses of cyber attacking and defense exercises in educational institutes such as universities or specialized institutions. The survey method was conducted by interviewing six organizations and others, including public information, questionnaire surveys by concerned parties, and participating in exercises [21][22]. Table 1 shows the target organizations and a brief of their training. Based on the survey, we divided the practices into the following two forms.

(1) Exercises by the learning applications
(2) Exercises by the Cyber Range We confirmed each type's main contents.

According to a document from the Ministry of Economy, Trade and Industry of Japan, the security personnel needed in the future are as follow,

(1) advanced security technicians such as white hackers
(2) those who have acquired the security technologies necessary to create secure information systems
(3) those who manage the security of the company in cooperation with in-house security technicians.

3 CyExec - Cybersecurity Exercises Platform

The goal of CyExec is to provide an exercise system that learns the necessary technology of cyberattacks and defense intended for introduction in higher education institutions and small and medium enterprises [21]. The features of CyExec as follow.

3.1 Low cost, highly portable exercise environment

Most of the costs of building and maintaining the exercise system are equipment and the cost of licensing software. The system requires specialized skills to renew the exercise, and the price, such as labor cost, is substantial.

In order to reduce these costs, CyExec was built an exercise environment using virtualization technology to quickly implement the developed exercise program in an existing computer environment (client PC, server, etc.). Using VirtualBox, we implemented the exercise program operating environment in a virtual environment.

Table 1 Contents of the exercise and training to raise the security personnel resources

Name	Overview
Tokyo Institute of Technology	The university offered a specialized study program of Five courses from 2016 as their cybersecurity. External lecturers from cooperating companies assign exercise subjects. Training focuses on how to use tools and OWASP applications etc.
Institute of Information Security	IIS introduced a large-scale exercise system, operated in cooperation with companies. The learners can be mastering a wide range of practical security skills through exercises, from technical subjects to social science subjects, towards multi-talent security human resources.
enPiT	Covering a wide range of practical security skills, from technical entity to social science subject, toward the training of human security resources sought by industry. Learning security practical skills in various forms such as learning using learning applications, joint exercises, group exercises.
Tokyo Denki University	International Cyber Security Special Course "CySec" started in 2015. The graduate students and people aim to become senior security engineers or CISO engineers. Practice exercises on security technology, attack countermeasure, and network design.
The university of AIZU	Developed and implemented practical cyber defense exercises from 2016 for administrative agencies, local governments, independent executive agencies, and essential social infrastructure operators in the country as stipulated in the Cyber Security Basic Law. Practical exercises by constructing a virtual exercise environment at NICT "StarBED."
NICT (National Institute of Information and Communications Technology)	Developed and implemented practical cyber defence exercises from 2016 for administrative agencies, local governments, independent administrative agencies, and important social infrastructure operators in the country as stipulated in the Cyber Security Basic Law. Practical exercises by constructing a virtual exercise environment at NICT "StarBED."

3.2 Exercise environment to secure joint development and use

The development of the training program curriculum requires a high level of expertise and time, and advances in the security technology field rapidly change. For these reasons, it is challenging to complete the exercise program development at a single higher education institution. Therefore, it needs to develop practice programs that several higher education institutions and private companies need to work together.

The CyEcex realizes joint development and exercise programs in multiple organizations by introducing the ecosystem concept. The ecosystem is not a single organization, but a word that indicates that the whole related organization develops through associated organizations ' collaboration. CyExec enriches the exercise program of CyExec not only by a single organization but also by joint development and use of related organizations.

For the training system, to realize joint development and utilization by multiple higher education institutions, it is necessary to develop and utilize exercise programs among different institutions quickly. To achieve this request, we implemented container technology using Docker.

The CyExec implemented Docker on the virtual environment configured with VirtualBox and install a container on Docker. By implementing vulnerability assessments and various exercise programs on attacks and defenses and running them on a Docker container, we could easily construct a practice environment for each purpose. The CyEcex can also be used jointly by creating an image file of a container that runs the developed exercise program and publishing it in related organizations. Table 2 shows the comparison of CyExec and other exercise systems.

Figure 1 shows the architecture of the CyExec exercise system. The exercise system's architecture is to install Docker on the guest OS running on VirtualBox on the host OS and implement the process on which the attack and defense exercise program runs on the container on Docker. The portability that can operate in the existing computer environment of VirtualBox and the Docker container's high ex-

Table 2 The comparison of CyExec and other exercise systems

	Exercise system example (Developer)		
	Proposed exercise system CyExec	WebGoat (OWASP), AppGoat (IPA)	CYBERIUM (Fujitsu), TAME Range (DNP)
Cost	· Program, text development free	· Text development cost	· Expensive system introduction operation cost
Exercise form	· Individual learning / Large-scale exercise · Operation of other exercise systems is also possible	· Individual learning/Small exercise	· Large scale exercise
Exercise content	· Can learn from the fundamentals of vulnerability detection to an organizational response method · Customizable according to study purpose	· Fixed exercise content · Update depends on the developer · Practice exercises concerning commentary/usage guides	· Personnel with expertise is required for operation · Update by development/provider (paid)
Feature	· High portability/extensibility with the ecosystem as a development concept · Improvement of the appropriate curriculum by cooperative development	· It can be carried out on student PCs and can be used on their own · Easy to introduce practical environment · Supplementary text required	· Exercise imitating the real environment · Practical exercises using actual malware

tensibility enable joint development and use of our exercise program.

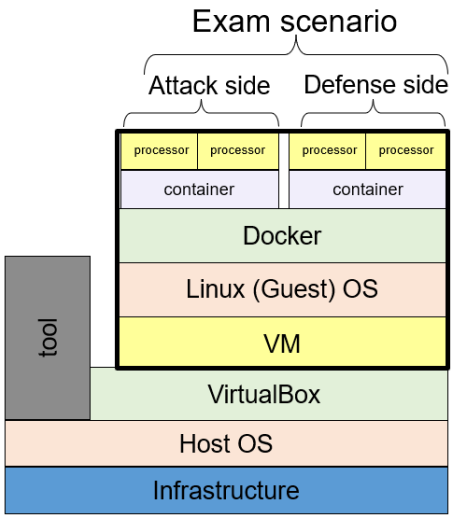

Figure 1 The architecture of the CyExec exercise system

3.3 Exercise example

Figure 2 shows the system configuration of the applied exercise. We implemented Docker on a virtual environment configured with VirtualBox and installed a container on Docker. Implementing various exercise programs related to attack and defense, such as virtual digital signage and trap server used by attackers, and running them on containers, it is possible to construct an exercise environment for each purpose easily. We built a physical environment that imitated digital signage using Raspberry Pi. By connecting via CyExec, it is possible to perform safe exercises in an isolated environment from the outside while using the actual machine. By preparing IoT devices as a rial physical environment, the learner could imagine the attack's actual situation. Therefore, we expect to enable easy-to-understand exercises with high educational effects. If a lecturer cannot prepare the physical environment, practices in virtual environments only are also possible.

4 Cybersecurity Trends

By the COVID-19, nearly 70 organizations surveyed by Skybox said over a third of their workforce would remain remote for at least the next 18 months [24].

Bitdefender researchers agree and say securing

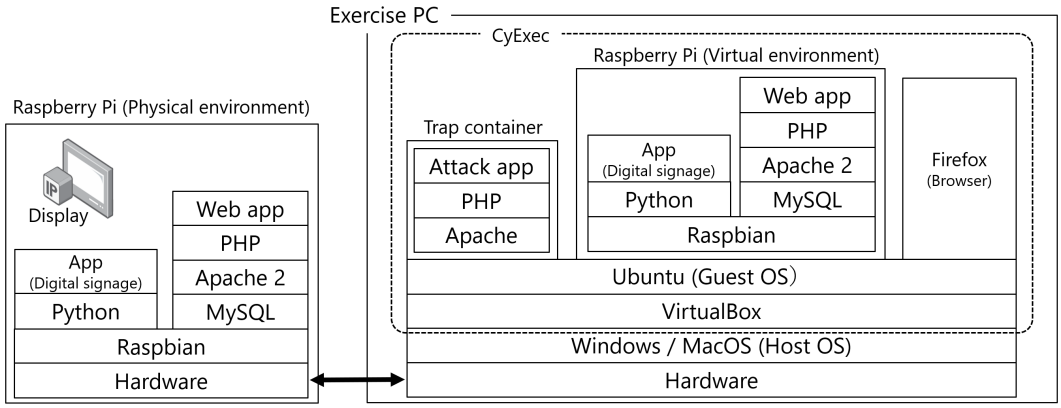

Figure 2 System configuration of the applied exercise

remote workers will become a primary focus for organizations. Cybersecurity is an essential issue since remote workers will continue to present a unique set of hackers' opportunities. Independent cybersecurity and data privacy consultancy Bridewell Consulting issued six predictions that will impact cybersecurity in 2021 [25].

Also, with the digital revolution around all businesses, small or large corporations, organizations, and even governments rely on computerized systems to manage their day-to-day activities, thus making cybersecurity a primary goal to safeguard data from various online attacks or any unauthorized access. Continuous change in technologies also implies a parallel shift in cybersecurity trends as news of data breach, ransomware, and hacks become the norm. N. Duggal and other workers who the cybersecurity field upped the issue of cybersecurity trends for 2021 [26].

5 Cybersecurity and data analytics

In general, cybersecurity is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. As a definition, cybersecurity analytics has its industry definition as "analyzing data to detect anomalies, unusual user behavior, and other threats". It aggregates data from across the entire enterprise ecosystem and turns that data into actionable insights — so that the IT team can promptly act on minimizing those risks. Advanced features like artificial intelligence (AI) and machine learning (ML) further help by automating the detection and remediation process." Cybersecurity analytics combines big data capabilities with threat intelligence to help detect, analyze and alleviate insider threats, as well as targeted attacks from bad external actors and persistent cyber threats [27].

The need for automated, scalable, machine-speed vulnerability detection and patching is large and growing fast as more and more systems—from household appliances to major military platforms—get connected to and become dependent upon the internet. To help overcome these challenges, DARPA launched the Cyber Grand Challenge, a competition to create automatic defensive systems capable of reasoning about flaws, formulating patches and deploying them on a network in real time [28].

There are two main ways to find software vulnerabilities using artificial intelligence technology. First, it is a method to extract patterns from vulnerability data and then find parts with code flows similar to this pattern in the program under analysis. The second method is to construct a framework that behaves like a single organism that explores, tracks, and validates the program's central part. The former is a data-driven technique, and the latter is an algorithm-driven technique. It is fast and effective in the former case, but only similarity patterns can be found, and its coverage is limited. In the latter case, it is a method of delegating all processes from vulnerability discovery to verification in the machine, which requires more consideration than data-driven techniques and is challenging to

implement. Some teams opened to the public their paper when they participated in the CGC [29][30].

S. Chr presented MAYHEM, a new system for automatically finding exploitable bugs in binary (i.e., executable) programs. Every bug reported by MAYHEM is accompanied by a working shell-spawning exploit. The working exploits ensure soundness and that each bug report is security-critical and actionable. MAYHEM works on raw binary code without debugging information [29].

Y. Shoshitaishvili discussed their cyber reasoning system, Mechanical Phish, which they have open-sourced; the lessons they learned in participating in this ground-breaking competition; and their system's performance as a tool in assisting humans during the DEF CON Capture-the-Flag competition, which followed the DARPA Cyber Grand Challenge [30].

6 Conclusion

Cyber-attacks such as targeted attacks are increasing, and it is becoming a problem of digital society. Human resource development, which has attack and defense technology, is an important theme. Therefore, the environment improvement to security human resource development has not progressed due to the exercise system's building cost and the shortage of personnel who maintain and manage the exercise environment. Therefore, this paper introduced CyExec that developed for the cybersecurity exercise system, an ecosystem consisting of virtual computer environments using VirtualBox and Docker. Additionally, through this paper, I introduced cybersecurity trends and cybersecurity and data analytics recently.

Acknowledgments

This work was supported by JSPS KAKENHI Grant Number JP 19K03006 and supported by Transcosmos fundation.

REFERENCES

[1] S. Shin, Y. Seto, CyExec – Training Platform for Cybersecurity Education Based on a Virtual Environment, IJLTLE. Vol. 3, No. 1, pp.1-20 (2020).

[2] CSO Online: https://www.csoonline.com/article/2953258/cybersecurity-job-market-figures-2015-to-2019-indicate-severe-workforce-shortage.html

[3] The 2015 (ISC)2 Global Information Security Workforce Study: https://www.boozallen.com/content/dam/boozallen/documents/Viewpoints/2015/04/frostsullivan-ISC2-global-information-security-workforce-2015.pdf

[4] Information and Security White Paper 2019 (in Japanese), white paper, Information-technology Promotion Agency, Japan (IPA) (2019).

[5] Penn State ' s College of Engineering Hit by Cyberattack: https://bits.blogs.nytimes.com/2015/05/15/penn-states-college-of-engineering-hit-by-cyberattack/?_r=0

[6] S. Campbell, Cybersecurity in Higher Education: Problems and Solutions: https://www.toptal.com/insights/innovation/cybersecurity-in-higher-education

[7] National Center of Incident and Strategy for Cybersecurity, Japan, Cybersecurity Strategy (2018): https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018-kakugikettei.pdf

[8] Ministry of Economy, Trade and Industry, Japan, Survey on latest trends and future estimates of IT personnel (in Japanese) (2016): https://www.meti.go.jp/committee/kenkyukai/shoujo/daiyoji_sangyo_skill/pdf/001_s02_00.pdf

[9] M. Edure, Practical Exercises for Cyber Attacks, Information processing, Vol. 55, No. 7, pp. 666-672 (2014).

[10] N. Ryotaro, H. Kumi and S. Yoichi, Development of Container-based virtual exercise system CyExec related to cyber-attack and defense, The 80th National Convention of IPSJ (2018).

[11] S. Toyoda, R. Nakata, K. Hasegawa, S. Shin, Y. Seto, Proposal of Cyber attack and defense Exercise system CyExec composed of ecosystem, Computer Security Symposium, Nagano (2018).

[12] Y. Kasai, Y. Seto, et al., Development of practice contents for cyber security exercise system CyExec, Symposium on Cryptography and Information Security, (2019)

[13] Frankie E. Catota, M. Granger Morgan1 and Douglas C. Sicker, Cybersecurity education in a developing nation: the Ecuadorian environment, J. of Cybersecurity, Vol. 5, Issue. 1 (2019).

[14] ACM Computing Disciplines Overview: https://www.acm.org/education/curricula-recommendations

[15] Cybersecurity Curricular Guidelines — CSEC 2017: https://cybered.hosting.acm.org/wp/
[16] Information security education for students in Japan: https://www.nier.go.jp/English/educationjapan/pdf/201403ISE.pdf
[17] R. Beuran, K. Chinen, Y. Tan, Y. Shinoda, Towards Effective Cybersecurity Education and Training, Research Report - School of Information Science (2016).
[18] Nomura Research Institute (NRI) Secure Technologies: http://www.nrisecure.com/.
[19] enPiT University Consortium. enPiT-Security (SecCap) Training Program: https://www.seccap.jp/
[20] Ministry of Internal Affairs and Communications, Japan. Cyber Defense Exercise with Recurrence (CYDER) Training Program (press release): http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Releases/Telecommunications/130925 02.html
[21] Ministry of Education, Culture, Sports, Science and Technology, Japan, Annual report 2016, enPiT (2017): http://www.enpit.jp/img_new/publications/enPiT_annualreport_uni_2017.pdf
[22] Cyber Defense Exercise with Recurrence: https://cyder.nict.go.jp/.
[23] T. Shinichi, et al., Proposal of Cyberattack and defense Exercise system CyExec composed of the ecosystem, CSS2018 (2018).
[24] Threatpost, 2021 Cybersecurity Trends: Bigger Budgets, Endpoint Emphasis and Cloud: https://threatpost.com/2021-cybersecurity-trends/162629/
[25] M Jones, Six cybersecurity trends heading our way in 2021: https://techhq.com/2020/12/six-cybersecurity-trends-heading-our-way-in-2021/
[26] N. Duggal, Top 10 Cyber Security Trends For 2021: https://www.simplilearn.com/top-cybersecurity-trends-article
[27] L, Sarker, et al., Cybersecurity data science: an overview from machine learning perspective, J. of Big Data, Vol. 7, No. 41 (2020).
[28] Cyber Grand Challenge (CGC): https://www.darpa.mil/program/cyber-grand-challenge
[29] S. Cha, T. Avgerinos, A. Rebert and D. Brumley, Unleashing MAYHEM on Binary Code, 2012 IEEE Symposium on Security and Privacy (2012).
[30] Y. Shoshitaishvili, Mechanical Phish: Resilient Autonomous Hacking, IEEE Security & Privacy, Vol. 16, Issue. 2 (2018).

東海大学紀要情報理工学部
Vol.20 , 2020, pp. 19–21
DOI: 10.18995/24352152. 20-1.19

研究紹介：情報科学科　高橋研究室

高橋　智博 [†1],

Introduction of Research: Takahashi laboratry

by

Tomohiro Takahashi

Abstract

本研究室では画像処理と音声・音楽処理を中心に研究を行なっている．本稿では特に，image inpainting と呼ばれる欠損画素補間について平易に解説し，東海大学における今後の研究教育について展望を述べる．

Keywords: ディジタル信号処理, 画像修復, 行列ランク最小化

1 は じ め に

行列完成問題は様々な応用を持つ数理最適化問題である．対象とする行列の多くの要素が欠損しており，それら欠損要素を欠損していない要素から推定し，修復する問題である．推薦システムはこの問題の代表的な応用先であり，Netflix Prize と呼ばれる優勝賞金 100 万ドルのアルゴリズムコンテストが行なわれたのは 2006 年のことである [1]．各行がインターネット動画配信サービス Netflix が扱う映画のタイトル，各列が登録ユーザーに対応したデータ行列が与えられ，この行列の各要素はどのユーザーがどの映画を 5 段階でどのように評価したかを表している．このとき，まだ評価されていない空白の要素の値を高い精度で推定することが目標となる．これが可能になれば，任意のユーザーに対して，そのユーザーが高く評価するであろう映画を推薦することが出来るようになり，顧客満足度やレンタル率の向上が期待できる．

では具体的にどうやってまだ評価されていない要素を推定するのであろうか．多くのアプローチがあるが，行列の低ランク性に着目する方法は代表的な方法の一つである．例えば，スターウォーズが好きな人はスタートレックや銀河英雄伝説も好きであろうし，同様にロードオブザリングが好きな人はゲームオブスローンズやハリーポッターも好きであろう．これは人間の映画に対する嗜好は，宇宙 SF 好き，ファンタジー好きといったより低次元な説明変数でデータを表現できることを示している．もしそれらの説明変数とデータの間に線形あるいはアフィンな関係があれば，データ行列は低ランク行列で十分に近似可能である．観測データが存在する要素については十分それに従い，かつ低ランクとなる行列を求める手法は多く提案されており，適当な手法を用いて推薦システムを実現することが出来る．

図 1　ランダム欠損画像の修復例

本研究室ではこうしたデータ予測･補間の技術をディジタル信号処理の分野に応用した，画像の修復や音声の歪み除去のためのアルゴリズムについて研究している．特に，image inpainting と呼ばれる欠損画素補間は，図 1 のように画像の一部が欠損している（図左側）場合に，その周囲の非欠損画素から欠損画素を推定し，復元する（図右側）技術である．本稿ではランク最小化に基づく画像修復法について平易に解説し，今後の

[†1] E-mail:takahashi.tomohiro.r@tokai.ac.jp

研究について展望を述べる．

2 行列のランク最小化に基づく画像修復

2 次の微分方程式で表される現象を離散的にモデル化[1]する方法として，以下のような自己回帰（Autoregressive:AR）モデルがよく知られている．

$$x_i = \sum_{j=1}^{r} a_j x_{i-j} + e_i, \tag{1}$$

このとき，x_i は第 i 時刻の信号値を表し，a_j は j 時刻ずれた信号に対する重み，e_i は第 i 時刻のモデル化残差をそれぞれ表している．この式の意味するところは，ある時刻の信号はそれより前の時刻の信号の線形結合によって表されるということである．このような信号のモデル化を行なう上で重要となるのがモデル次数と呼ばれるパラメータであり，式では r で表されている．一般的にモデル推定を行なうためには，モデル次数 r をあらかじめ適当に決定した上で観測信号から a_j を推定する必要がある．モデルの「質」はこのモデル次数の決定に大きく依存するため，モデル次数の決定は重要であり，AIC をはじめとする様々な方法が提案されてきた．

ここで，信号が 2 次元的な広がりを持つ場合，すなわち画像等であった場合はどのようにモデル化すれば良いであろうか．画像に対する AR モデルは以下のように定義されることが多い．

$$x_{i,j} = \sum_{l=-K}^{K} \sum_{m=-K}^{K} a_{l,m} x_{i+l,j+m} + e_{i,j}, \tag{2}$$

式 (1) と対比すれば，各変数の対応は明らかであろう．ただし，ここでは $a_{0,0} = 0$ と定義されている．また，式 (2) では K をモデル次数と呼ぶことにする．このとき時間信号の場合と同じく，モデル次数 K の決定がモデル化にとって重要である事は変わらない．

さて，本節で考えようとしている問題は image inpainting，すなわち画像の一部が欠損している問題であった．それは重み $a_{l,m}$ のみならず $x_{i,j}$ の一部も観測できない事を意味している．もし欠損が画像の一部分に集中しているならば，欠損していない部分だけを上手く取り出すことでモデルの推定が可能かもしれない．しかしながら，図 1 のように画像全体にわたって欠損箇所が散らばっている場合には，欠損していない領域だけを集めてくることは不可能である．ある画素を中心とする $2K+1 \times 2K+1$ 平方ピクセルの領域にはほぼ例外なく欠損画素が含まれてしまい，重みを推定することは難しい．正しいモデル次数 K も，モデルの重み $a_{l,m}$ も，そして画像 $x_{i,j}$ の一部すら分からないというこの状況下において，どのようにして画像の欠損部分を修復すれば良いであろうか．

結論としては，“ある構造化行列のランク”と“AR モデルの次数”の間にある特別な関係が，“ランク最小化に基づくデータ予測”と“AR モデルに基づく信号の修復”とを全く等価なものとして結びつけてくれる．時間信号においてモデル化残差が無視できる場合，AR モデルに基づく信号からなる Hankel 行列のランク（階数）はモデル次数 r に等しい [2] ことが知られている．画像の場合においても同様に，そのランクがモデル次数 K の増加関数となるような構造化行列が存在する [3]．そのような構造化行列の集合の中で，非欠損画素は観測された値がそのままで，かつ行列のランクが最小となるような構造化行列を見つけることは，最小次数でモデル化可能な画像を見つけることに等しい．もしモデル次数の選択基準として「与えられた信号を十分に表現可能で，かつ最小限」なものを良いとするのであれば，この方法は理に適っているだろう．この方法には，モデル化に基づく一般的な信号・画像修復法と大きく異なる点がある．それは重み $a_{l,m}$ を推定しないこととモデル次数の事前決定を行なう必要が無いことである．重みを推定しないということは，後から同じような特徴を持った画像が入力されても以前の計算結果を使い回すことが出来ないということであり，モデル残差を再計算することが困難でもある．信号処理の応用においては，これらの点は欠点にもなり得るので，本手法適用の是非は慎重に検討しなくてはならない．

3 東海大学における研究と今後の展望

本研究室は 2018 年に出来た新しい研究室であり，2020 年 3 月に初めての卒業生を送り出した．第 1 期生の卒業研究発表タイトルは以下の通りである．

- 分岐管付き声道音響モデルによる声道断面積の推定法
- 着色済み画像に対する操作者の事前情報を用いた再着色法
- 雲による欠損を含む衛星データからのクロロフィル a 濃度推定
- 音響スパイクノイズ抑圧のためのディジタルフィルタ
- ラインスキャン画像における計測必要箇所のリアルタイム判別
- ニューラルネットワークを用いたリアルタイム表情認識
- 美顔処理における肌領域高精度抽出

[1] 数式で表すこと

- 圧縮センシングに基づく音声符号化
- 同一地点で撮影された被災地写真の自動仕分けに関する基礎検討

以上のように，画像処理と音声・音楽処理を中心に研究しており，古典的なディジタルフィルタやニューラルネットワークを使った物まで問題に応じた手法を学生自身に自由に検討させることを目指している．また，著者が得意とする画像修復技術を東海大学（情報科学科，および情報技術センター）の強みである衛星リモートセンシングへと応用した研究も行なっている．東海大学には広域な学問分野をカバーする多くの学部・学科が設置されているが，学部・学科の壁を越えた共同研究が非常に盛んであると感じている．今後は学内外でそうした学際領域における信号処理・信号修復の応用を開拓し，信号処理分野における新たな知見を他大学の研究者に先駆けて発見できるよう務める所存である．

参 考 文 献

[1] Netflix Prize Home, https://www.netflixprize.com/

[2] M. Fazel, H. Hindi and S. P. Boyd, "A rank minimization heuristic with application to minimum order system approximation," the 2001 American Control Conference, Arlington, VA, USA, 2001, pp. 4734-4739 vol.6, doi: 10.1109/ACC.2001.945730.

[3] T. Takahashi, K. Konishi and T. Furukawa, "Structured matrix rank minimization approach to image inpainting," 2012 IEEE 55th International Midwest Symposium on Circuits and Systems (MWSCAS), Boise, ID, 2012, pp. 860-863, doi: 10.1109/MWSCAS.2012.6292156.

東海大学紀要情報理工学部
Vol.20 , 2020, pp. 22–27
DOI: 10.18995/24352152. 20-1.22

LSI 出荷時におけるテストの高速化および信頼性向上に関する研究紹介

土屋秀和

Research introduction on speedup and improving reliability of testing for executing at LSI shipment

by

Hidekazu TSUCHIYA*1

(received & accepted)

Abstract

Recently, LSIs have been used in various products such as smartphones and automobiles etc. are indispensable parts in modern society. Also, the operating speed of LSI is faster and the scale of circuit for LSI is larger. LSIs are always tested on an individual basis at the time of shipment, these induce increasing power dissipation and the amount of test data for testing. For the reduction of these factors, we research the testing method that adjustable for power dissipation and test data size during testing by applying the clock control. The testing method achieve to reduce the test data size by using the method to mix pseudo random vector and ATPG (Automatic Test Pattern Generation) vector. In addition, the testing method achieve to reduce for power dissipation of CUT (Circuit Under Test) during testing by applying the clock control. In this paper, we introduce our research for LSI testing method.

Keywords: LSI Testing, Test pattern generation, Low power

1. はじめに

現在，LSI はあらゆる電子機器に組み込まれ，我々の生活にとって必要不可欠な電子デバイスとなっている.これまで，LSI は製造技術の進歩により，回路の大規模化による高機能化や動作速度の高速化などの発展を遂げてきた．しかし，現在の製造技術において極僅かな異物や環境の変化などの様々な要因によって，各々の LSI 全てを良品として製造することが困難となっている [1]．そのため，LSI 製造時における選別テストが必須となっている．また，LSI の回路の大規模化が進むにつれて，回路が複雑となり完全テストが困難になっている．そして，この事態は LSI メーカが抱える問題の一つとなっている．例えば，組込み用のマイコンを例に挙げると，売価は数百円のものも存在する．しかしながら，そのマイコンをテストするためには，数千万円～数億円の高性能 LSI テスタを使用して,長い時間テストを行なわなくてはならない.さらに，LSI の実動作速度でのテストに対応するためには，より高性能な LSI テスタが必要となることから，テストコストも増加する．また，性能が伴わない LSI テスタを使用してテストを行なった場合は，実動作速度テストが行なえずにテスト品質の低下を招く.

一方，近年の LSI の大規模化によって，システムの大部分を 1 つのチップに搭載する SOC(System On Chip)化が進んでいる．これらの高機能化された LSI に対しては，より多くのテスト項目を必要とし，テスト時間が長大化する [2]．その結果，LSI テスタの使用時間増加による出荷効率の低下によってテストコストが増加する．また，不完全にテストが行なわれた場合は，テスト品質の低下のため，出荷後の不良率が増加する恐れがある．これらの現状を改善する手法の一つとして，BIST(Built In Self Test)[3][4]と呼ばれる手法が挙げられる．BIST は，LSI テストの一部または全てを LSI 内に組込むことで，自己テストを実現する手法であり，自己テストによって LSI テスタの使用時間の削減を実現し，テストコストを削減することが可能である．また，実動作速度テストおよび完全テストの実施によって，テスト品質の向上を実現することが可能である．BIST には，実動作速度テストや高い故障検出率を実現する高品質テストの実現，テスト時間の短縮による更なるテストコストの削減との両立が要求されている.

これまで，LSI テストの多くは故障モデルの一つである単一縮退故障を対象として故障検出を行ない，良品を選別してきた [1][2]．この単一縮退故障とは，被テスト回路中の信号線のうち,いずれか 1 つの信号線の論理値が 0 または 1 に固定（縮退）されてしまう故障である [2]．ここで，NMOS インバータを例に挙げると, Fig.1 のようにドレインとソースが短絡した場合, 入力 X の状態を問わず出力 Z より論理値 0 が出力され，この状態を 0 縮退故障と呼ぶ．一方で，Fig.2 のようにドレインまたはゲートが断線した場合，入力 X の状態を問わず出力

*1　コンピュータ応用工学科　助教
Department of Applied Computer Engineering,
Assistant Professor

Z より論理値 1 が出力され，この状態を 1 縮退故障と呼ぶ．組み合わせ回路に対する単一縮退故障は，ATPG(Automatic Test Pattern Generator)と呼ばれる被テスト対象の回路構成情報に基づくコンピュータシミュレーションより生成されるテストパターンや，LFSR（Linear Feedback Shift Register）と呼ばれるシフトレジスタのビット列の一部を取り出し排他的論理和を取り，入力ビットとしてフィードバックすることで生成される疑似ランダムなテストパターンを用いて検出することができる. しかし, 多くの LSI は一般的に順序回路であり，組み合わせ回路の他に記憶回路としてフリップフロップが実装されている．

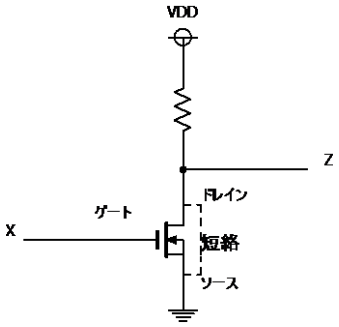

Fig.1 Stuck-at 0 fault

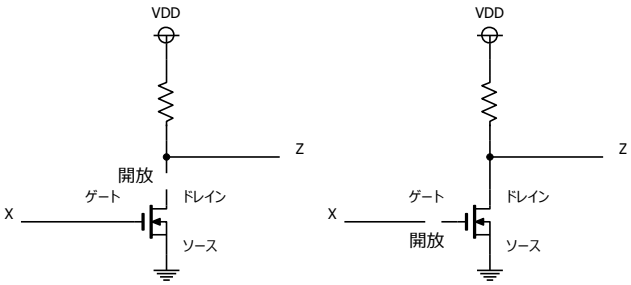

Fig.2 Stuck-at 1 fault

そこで，テストパターンを任意の回路箇所に印加するためには，このフリップフロップの状態を外部より制御できる必要があり，スキャンテストが広く用いられている．これは，Fig.3 に示すように, テスト時には回路内のフリップフロップ FF をシリアル接続に構成し, スキャンチェインと呼ばれるシフトレジスタとして動作させる．スキャンテストでは，テストパターンをシリアルデータとしてスキャンチェインに入力（スキャンイン）し，テストパターンに対する被テスト回路の出力応答を LSI の外部へ出力（スキャンアウト）することができる．このように，本来の機能を維持した状態で，テストが容易になるように LSI の構造の一部に変更を加えた設計手法をテスト容易化設計と呼ぶ．テスト容易化設計では，同期して多くの回路を強制的に動作させることもできる．この場合は，テスト時間を短縮することが可能であるが，通常使用時と比べてテスト時の消費電力は増加し，発熱による誤動作や故障，さらに回路の破壊に繋がる恐れがある．また，エレクトロマイグレーションと呼ばれる，イオンが徐々に移動し，半導体内部の構造が欠損していく現象による信頼性の低下も問題となる．

そこで，本稿では LSI 評価の高速化および信頼性向上に関する研究において,「テスト時の消費電力を抑制するテストパターン生成技術」として，テスト時の消費電力を抑制することで歩留まり低下を抑制し，短いテスト時間で高い故障検出率を達成することにより高いテスト品質の実現と共にテストコストを削減し，実動作速度でテストパターンを発生することで高いテスト品質を実現するテストパターン発生器の回路構成およびテストパターン生成法 [5)6)]について紹介させて頂く．

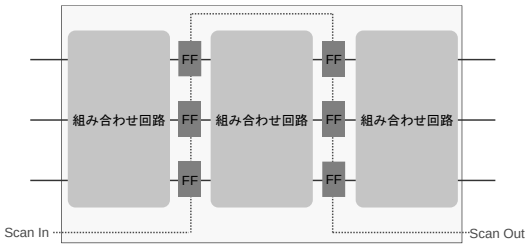

Fig.3 Structure of scan testing

2. テスト時の消費電力を抑制するテストパターン生成技術

2.1 準備

BIST では Fig.4 のように被テスト回路に加えてテストパターン発生器，テストパターンに対する出力応答のデータ圧縮を行なう出力応答圧縮器，テストパターンの出力応答とその期待値を比較するテスト結果比較器によって構成される．

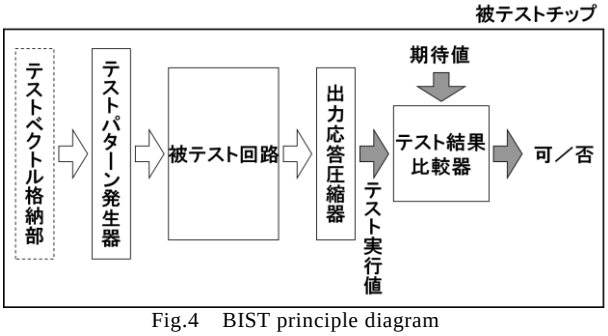

Fig.4 BIST principle diagram

更に，ATPG によって生成したテストパターンの部分集合など，あるテストベクトルを元にテストパターンを生成する場合は，ROM などのテストベクトル格納部の併設や外部の LSI テスタのメモリを使用する．また，BIST にはテストベクトル格納部などから元となるテストベクトルを利用してテストパターンを生成する方式や，元となるテストベクトルを利用せずに，LFSR（Linear Feedback Shift Register: 線形フィードバックレジスタ）やカウンタなどのハードウェアによってテストパターンを生成する方式がある．生成されたテストパターンは被テスト回路に印加され，そのテストパターンに対する出力応答が MISR（Multiple Input Signature Register: 多入力シグネチャシフトレジスタ）などの出力応答圧縮器によって圧縮される．全てのテストベクトルを ROM などに格納すると大容量のメモリが必要になってしまうため, BIST では出力応答を LFSR やカウンタなどの出力応答圧縮器で圧縮し，圧縮した出力応答（シグネチャ）と正しい期待値を圧縮した値とを比較してテストを行なう．このように出力応答圧縮器を用いて圧縮した出力応答と正しい期待値を圧縮した値を比

較するテスト方式をシグネチャ解析と言い，圧縮器をシグネチャレジスタまたはシグネチャアナライザと言う．この中でも，BIST 用テストパターン発生器（TPG：Test Pattern Generator）は，BIST の構成要素の中でもテストの品質を左右する部分であり，より少ないハードウェア量で効率的なテストパターンを生成し，高い故障検出率を達成することが課題とされている．LFSR のみによって擬似ランダムベクトルを生成する場合は，被テスト回路の構成を考慮しないため，故障検出に貢献しないテストベクトルが多く生成されてしまう．従って，高い故障検出率を達成するための膨大なテストパターン数を縮小することが課題となっている．加えて，高い故障検出率を達成できない場合がある．また，ATPG ベクトルと擬似ランダムベクトルを混在させたテストパターンを生成する場合は，ATPG ベクトルの出現頻度を高めることによって，短いテスト長で高い故障検出効率を達成する可能性がある．しかし，ATPG ベクトルを格納するためには ROM などのメモリが必要となるため，短いテスト長で高い故障検出効率を達成しながらも，ATPG ベクトルを格納するメモリ量を削減することが課題である．

TPG に関しては，LFSR による擬似ランダムベクトル系列による故障検出効率を改善するための手法として，重み付き擬似ランダムパターン手法 [7]，ビットフィックス手法 [8]，ビットフリッピング手法 [9] などが提案されている．また，擬似ランダムベクトルと ATPG ベクトルを混在させる手法として，LFSR の初期値を可変するリシード手法 [10]，ATPG ベクトルの部分集合を元にし，分割シフトパターンを生成する分割シフト法 [11]，分割スキャンチェインをローテッドスキャンするパーシャルスキャン手法 [12] などが提案されている．一方，近年における動作速度の高速化や回路の大規模化に伴って，テスト時の消費電力が問題となっている．これらの改善については，いくつかの Gated Clock 手法が研究され報告されている [13)~16)]．Gated Clock 手法では，分割した回路ごとにクロック供給を制御することによって，消費電力を削減することができる．本稿では，擬似ランダムベクトルと ATPG ベクトルを混在させる手法として，Gated Clock 手法を適用した分割シフト法 TPG の回路構成とテストパターン生成法を提案し，高い故障検出率の達成に必要なテスト長とメモリ量，平均電流，総消費電力に関して，SR の分割数及び Gated Clock による動作率と特性との関係を評価した．CUT には ISCAS’85 ベンチマーク回路を用い，比較対象は，ATPG 及び LFSR とした．

2.2 テストパターン発生器の回路構成

Fig.5 に Gated Clock によりテスト時の消費電力を抑制するテストパターン技術を適用したテストパターン発生器 TPG の回路構成を示す．ここで，シフトレジスタ SR の分割数を k，同時に動作する SR 数を g，被テスト回路 CUT の入力数を m とする．TPG はメモリ MR とクロック制御部 CP と k 個に分割されクロック制御が適用されたシフトレジスタ SR により構成される．MR は k ビットのバス幅を持ち，ATPG ベクトルの部分集合が格納され，格納されたデータがクロック制御に従って各 SR に分配される．CP の入力であるイネーブル信号(enable_1～enable_k)の組み合わせにより，SR 毎にクロック制御が行なわれ，CUT において分割した回路毎にクロック供給のタイミングを制御することで，消費電力を削減可能である．TPG において，ランダムパターンで検出困難な故障である rpr(random pattern resistant)故障の検出を疑似ランダムなテストパターンのみで試みた場合，膨大なテストパターンが必要となることや，検出できずに故障検出率の低下を招き出荷後の動作不良の発生率が高くなる可能性がある．そこで，本技術を適用した TPG ではクロック制御が適用された SR により，周期的に出現する被テスト回路の回路構成を考慮し生成した ATPG ベクトルの部分集合を用いることで，rpr 故障を検出する．また，rpr 故障以外の故障は SR のシフト動作による疑似ランダムベクトルを使用して検出する．このように，rpr 故障以外の故障検出には擬似ランダムベクトルを使用し，rpr 故障検出には ATPG ベクトルを使用することで，ATPG ベクトルの全てをメモリに格納せず，その部分集合のみをメモリに格納するため，メモリに格納する ATPG ベクトル数の削減が可能である．これにより，LSI テスタのメモリ増設が必要となる頻度を低減可能であり，コスト削減に寄与する．また，rpr 故障を ATPG ベクトルで検出することで，故障検出に冗長なテストベクトルを削減可能となり，短いテスト長で高い故障検出率の達成が可能である．

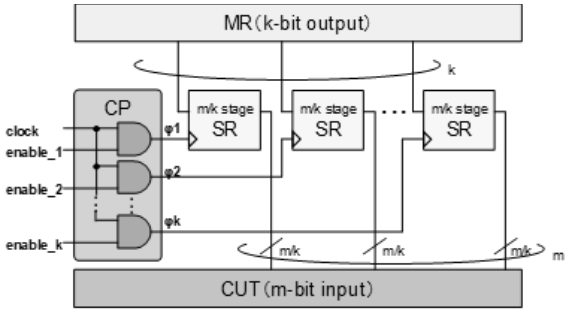

Fig.5　Circuit structure for test pattern generator

2.3 テストパターンの生成

本技術では，スキャンテストが適用された回路の単一縮退故障を対象とし，故障検出効率を次式で定義する．

$$\text{故障検出効率} = \frac{\text{検出故障数}}{\text{全故障数} - \text{冗長故障数}} \times 100\% \quad (2.1)$$

本技術によるテストパターン生成について述べる．テストパターンの生成は，大きく分けて 2 つの工程で構成される．ATPG ベクトルの部分集合の選択では，実テスト時間および必要なメモリ量を削減するために，ATPG ベクトルの部分集合を求める操作と共に圧縮操作を行なう．この操作は，大きく分けて 4 つのステップで構成される．また，TPG によるテストパターン生成では，実際に被テスト回路にテストパターンを印加するために，ATPG ベクトルの部分集合を元にして TPG によりテストパターンを生成する．この操作は，大きく分けて 2 つのステップで構成される．以下に各操作の詳細を示す．

①ATPG ベクトルの部分集合の選択

Step 1 : ATPG ツールを使用して，被テスト回路に対する高い故障検出効率を達成する ATPG ベクトル集合を生成す

る.

Step 2 : 分割数 k および同時に動作する SR 数 g の構成に基づいて，分割シフト動作によって分割シフトされたテストパターンを求める.

Step 3 : 分割シフトされたテストパターンを使用して，故障シミュレーションを行ない，高い故障検出効率を達成するまでに使用された部分集合から，元となる ATPG ベクトルの部分集合を求める．選択した部分集合が前回求めた ATPG ベクトルの部分集合と比較し，同量または縮小された場合は Step 4 に移り，それ以外は前回求めた ATPG ベクトルの部分集合を最小とみなし確定する.

Step 4 : 求めた ATPG ベクトルの部分集合の最後に位置するベクトルを rpr 故障検出に必要なベクトルと期待し，Fig.6 のように先頭に並び替えた後 Step 2 に戻り, この手順を繰り返す.

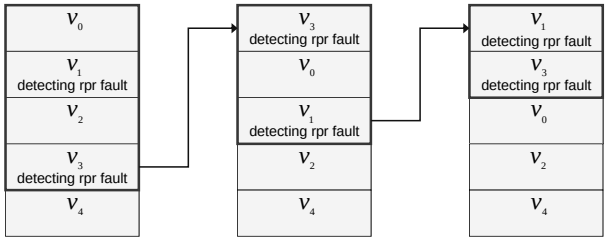

Fig.6　Reordering vectors

②TPG によるテストパターン生成

Step 1 : “①ATPG ベクトルの部分集合の選択” で求めた部分集合をメモリに格納する.

Step 2 : ATPG ベクトルの部分集合を元にクロック制御が適用された k 個の SR により，分割シフトされたビット幅が m ビットのテストパターンが生成される. テストパターンには，シフト動作によって生成される擬似ランダムベクトルと ATPG ベクトルが混在する.

ここで, 同時に動作する SR 数を g とした時の SR の動 A.R を次式で定義する.

$$\text{動作率 A.R.} = \frac{g}{k} \times 100\%, \quad 1 \le g \le k \quad (2.2)$$

元になる ATPG ベクトルは，分割された k 個の SR によってシフトされる. すなわち, それぞれの SR において ATPG ベクトルは m/k シフトごとに出現する. また, それぞれの SR は Gated Clock によって k/g ごとにシフトする．すなわち，分割シフト法 TPG において ATPG ベクトルは(m/k) × (k/g) = m/g 回ごとに出現する. 元となるベクトル数を q としたときに生成可能なテストベクトル数及びその中に含まれる ATPG ベクトル数，擬似ランダムベクトル数は以下に示される.

生成可能なベクトル数= (q − 1) × (m/g) + 1　(2.3)

ATPG ベクトル数= q　(2.4)

擬似ランダムベクトル数= (q−1)×(m/g)+1 −q　(2.5)

テストパターンの生成例を CUT の入力数 m=4, 分割数 k=2, 動作率 A.R.=50%として，Fig.6 に示す．$v_0(v_{00},v_{01},v_{02},v_{03})$ と $v_1(v_{10},v_{11},v_{12},v_{13})$ を元にして ATPG ベクトル 2 個$(v_{00},v_{01},v_{02},v_{03})$, $(v_{10},v_{11},v_{12},v_{13})$，擬似ランダムベクトル 3 個$(v_{11},v_{00},v_{02},v_{03})$, $(v_{11},v_{00},v_{13},v_{02})$，$(v_{10},v_{11},v_{13},v_{02})$を生成し，$v_1(v_{10},v_{11},v_{12},v_{13})$ と $v_2(v_{20},v_{21},v_{22},v_{23})$を元にして ATPG ベクトル 2 個$(v_{10},v_{11},v_{12},v_{13})$, $(v_{20},v_{21},v_{22},v_{23})$，擬似ランダムベクトル 3 個$(v_{21},v_{10},v_{12},v_{13})$, $(v_{21},v_{10},v_{23},v_{12})$，$(v_{20},v_{21},v_{23},v_{12})$を生成している．すなわち，ATPG ベクトル 1 個あたり ATPG ベクトル 1 個，疑似ランダムベクトル 3 個を生成している．このように，MR に格納された ATPG ベクトルの部分集合を, Gated Clock が適用された SR でシフトしながらテストパターンの生成を行うため, 実テストの面で以下の効果が期待される.

（1）高い故障検出効率の達成が可能である.

（2）実動作速度でのテストパターン生成が可能である.

（3）Gated Clock による SR の動作率の変更によって，テスト長と元となるベクトル数，テスト長と平均電流の各トレードオフを可能とする.

$$v_0 = (v_{00}\ v_{01} \mid v_{02}\ v_{03}) \qquad \begin{array}{c|c} (v_{00}\ v_{01} & v_{02}\ v_{03}) \\ (v_{11}\ v_{00} & v_{02}\ v_{03}) \\ (v_{11}\ v_{00} & v_{13}\ v_{02}) \\ (v_{10}\ v_{11} & v_{13}\ v_{02}) \end{array}$$

$$v_1 = (v_{10}\ v_{11} \mid v_{12}\ v_{13}) \Rightarrow \begin{array}{c|c} (v_{10}\ v_{11} & v_{12}\ v_{13}) \\ (v_{21}\ v_{10} & v_{12}\ v_{13}) \\ (v_{21}\ v_{10} & v_{23}\ v_{12}) \\ (v_{20}\ v_{21} & v_{23}\ v_{12}) \end{array}$$

$$v_2 = (v_{20}\ v_{21} \mid v_{22}\ v_{23}) \qquad (v_{20}\ v_{21} \mid v_{22}\ v_{23})$$

Fig.7　Example of the pattern generation

3.　評価方法

前述のテスト時の消費電力を抑制するテストパターン生成技術について, 分割数 k=1, 2, 4, 8, 動作率 A.R.[%]=100, 50, 25, 12.5 とし，評価尺度を高い故障検出効率の達成に必要なテスト長，元となるベクトル数，平均電流として SR の分割数およびクロック制御による動作率と特性との関係を評価した. 元となるベクトル集合は ATPG ツールで生成し, 2.3 項の手順で圧縮し選択を行なった．ターゲットデバイスとして，プログラムにより自在にディジタル回路を構成可能なデバイスである FPGA（Xilinx 製 Virtex-E:xcv405e-8fg676）に Xilinx 社製デザインツール ISE9.1i を用いて，評価対象の回路をインプリメントした．また，論理合成した CUT 及び TPG に対して, ISE9.1i に搭載されている消費電力シミュレータ（XPower）を用いて平均電流の評価を行った（ロジック部の電圧= 1.8V）. CUT には ISCAS’85 ベンチマーク回路を用いた．Table 1 に評価対象を示す．論理合成結果は，FPGA の論理ブロックである 4 入力 LUT（Look Up Table）数で示した．比較対象は, ATPG および原始 LFSR とした. また, 本技術を適用した TPG, ATPG，原始 LFSR によって生成されるテストパターンは，それぞれ高い故障検出効率を達成するものとした.

Table 1　Evaluation targets

CUT	機能	入力数	出力数	ゲート数	4 入力 LUT 数
C432	27 チャネル 割り込み コントローラ	36	7	160	91
C499	32 ビットシングル エラー訂正回路	41	32	202	78
C880	8 ビットALU	60	26	383	101
C1355	32 ビットシングル エラー訂正回路 （C499 のXOR を4 入力NAND に置換）	41	32	546	78
C1908	16 ビットエラー検出 ／訂正回路	33	25	880	130
C2670	12 ビットALU ／コントローラ	233	140	1193	158
C5315	9 ビットALU	178	123	2307	389
C6288	16 × 16 乗算器	32	32	2406	703
C7552	34 ビット加算器 ／入力パリティ チェック付き 大小比較器	207	108	3512	442

4.　評価結果

評価結果としてベンチマーク回路 C499 に着目し，Table 2 に示す．左の列から，CUT : ISCAS’85 ベンチマーク回路の回路名，#k : SR の分割数，%A.R. : 全体の SR に対して同時にシフト動作している SR 数の割合，%F.E. : 故障検出効率，#L : 高い故障検出効率を達成するために必要なテスト長，#MR : MR に格納される ATPG ベクトルの部分集合，#power : テスト実行時の平均電流を示す．この結果をもとに，ATPG および LFSR を対象として本技術について比較検討を行った．また，SR の分割数 k およびクロック制御による動作率 A.R. と特性との関係を検討した．

Table 2　Evaluation result (C499)

CUT	#k	% A.R.	% F.E.	#L	#MR	#power [mA]
C499	1	100	100	334	9	1.77
	2	50	100	578	15	0.89
		100	100	258	13	1.61
	4	25	100	535	14	0.54
		50	100	373	19	1.02
		100	100	231	24	2.03
	8	12.5	100	801	21	0.34
		25	100	521	27	0.61
		100	100	176	36	2.12
	41 (ATPG)	100	100	52	52	3.31
	LFSR	100	100	1167	0	2.15

4.1　ATPG との比較

ATPG に比べてテスト長は長くなるものの，元となるベクトル数および平均電流を大幅に低減可能である．先ず，元となるベクトルの縮小率すなわち ATPG ベクトルをすべて印加した場合に対する ATPG ベクトルの縮小の度合いに関しては，ATPG パターンをすべて印加した場合に比べて，少ない ATPG ベクトル数（平均 60.8%）で高い故障検出効率（99.5～100%）を達成することが可能である．また，平均電流の縮小率すなわち ATPG ベクトルをすべて印加した場合に対する平均電流の縮小の度合いに関しては，ATPG パターンをすべて印加した場合に比べて減少する（平均 42.4%）．

例えば C499 において，ATPG（分割数 k = 41）に対して k = 8 の場合を考える．動作率 A.R.=25%では，元となるベクトル数が 52 から 27 に減少し約 0.52 倍，平均電流は 3.31mA から 0.74mA に減少し約 0.22 倍に減少する．また，動作率 A.R.=12.5%では，元となるベクトル数が 52 から 21 に減少し約 0.40 倍，平均電流は 3.31mA から 0.47mA に減少し約 0.14 倍に減少する．

4.2　LFSR との比較

LFSR に比べて，元となるベクトルが必要となるが，テスト長を大幅に削減することが可能であり，平均電流も動作率 A.R. に応じて大幅に削減することができる．テスト長の縮小率すなわち LFSR のテスト長に対する縮小の度合いに関しては，LFSR で生成したパターンを印加した場合に比べて，短いテスト長（平均 35.9%）で高い故障検出効率（99.5～100%）を達成する．

例えば C499 において，LFSR に対して分割数 k=8 を比べると，動作率 A.R.=25%では，テスト長が 1167 から 521 に減少し約 0.45 倍，平均電流が 2.15mA から 0.74mA に減少し 0.34 倍に減少する．また，動作率 A.R.=12.5%の場合は，テスト長が 1167 から 801 に減少し約 0.69 倍，平均電流が 2.15mA から 0.47mA に減少し 0.22 倍に減少する．

4.3　分割数 k および動作率 A.R.

出力部の SR の分割数に応じて，ATPG ベクトルの出現頻度を変えることができる．すなわち，分割数 k の減少に従って，擬似ランダムベクトルの出現頻度が高まり，テスト長は長くなるものの，元となるベクトル数を削減することが可能である．

評価した範囲では，分割数が最大の k = m（ATPG）に対して分割数が最小の k = 1 の場合は，動作率 A.R. = 100%では，元となるベクトル数は平均 45.5%に減少する．また，動作率 A.R. に関しては，その率を低下させるに従って，テスト長は長くなるが，平均電流を削減することが可能である．評価した範囲では，分割数 k = 8 の場合，動作率が最大の A.R. = 100%に対して動作率が最小の A.R. = 12.5%の場合，平均電流は平均 18.5%に減少する．

5.　おわりに

本稿では，LSI の評価技術の現状および我々が取り組んでいる研究の一部を紹介した．研究として，Gated Clock 手法が適用可能な TPG について紹介し，高い故障検出効率を達成するテスト長，元となるベクトル数，平均電流について評価を行った．比較対象は，ATPG 及び原始 LFSR を，CUT には ISCAS’85 ベンチマーク回路を用いた．また，SR の分割数及び Gated Clock による動作率と特性との関係を評価した．評価した範囲では分割シフト法 TPG は ATPG と比較して，元となるベクトル数と平均電流を削減することが可能である．また，LFSR と比較して，テスト長と平均電流を削減することが可能である．今後は，引き続き「テスト時の消費電力を

抑制するテストパターン生成技術」に関して，単一縮退故障以外の故障への拡張対応などを行なっていきたい.

参考文献

1) LSI テスティング学会，LSI テスティングハンドブック，オーム社(2008).
2) 藤原秀雄，ディジタルシステムの設計とテスト，工学図書(2004).
3) S. Wang, “A BIST TPG for low power dissipation and high fault coverage,” IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol.15, no.7, pp.777–789 (2007).
4) P. Wohl, J.A. Waicukauski, S. Patel, and M.B. Amin, “X-tolerant compression and application of scan-atpg patterns in a bist architecture,” Proc. IEEE International Test Conference, vol.1, pp.727–736, Charlotte, USA (2003).
5) 土屋秀和，阿部高也，増田良介，浅川毅，” 擬似ランダムベクトルと ATPG ベクトルを利用した低電力指向 TPG，”電子情報通信学会論文誌 D，vol.J92-D，No.6，pp.777-783(2009).
6) Hidekazu Tsuchiya,” Testing method that adjustable for power dissipation and test data size during testing,” IEEE 19th Workshop on RTL and High Level Testing, Hefei, China (2018).
7) J. Dworak, “An analysis of defect detection for weighted random patterns generated with observation/excitation-aware partial fault targeting,” Proc.IEEE 25th VLSI Test Symposium, pp.205–210, Berkeley, USA (2007).
8) N.A. Touba and E.J. Mccluskey, “Bit-fixing in pseudorandom sequences for scan BIST,” IEEE Trans. Comput. Aided Des. Integr. Circuits Syst., vol.20, no.4, pp.545–555 (2001).
9) Y. Chaowen, S.M. Reddy, and I. Pomeranz, “Circuit independent weighted pseudo-random BIST pattern generator,” Proc. IEEE 14th Asian Test Symposium, pp.132–137, Calcutta, India (2005).
10) H.-S. Kim, Y. Kim, and S. Kang, “Testdecompression mechanism using a variable-length multiple-polynomial LFSR,” IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol.11, no.4, pp.687–690 (2003).
11) T. Asakawa and K. Iwasaki, “On using ATPG vectors for BIST TPG,” Proc. IEEE First Asia Pacific ASICs, pp.359–362, Seoul, Korea (1999).
12) S.M. Reddy and I. Pomeranz, “On undetectable faults in partial scan circuits using transparent-scan,” Proc. IEEE 22nd International Conference on Computer Design, pp.o82–o84, San Jose, USA (2004).
13) T.E. Yu, T. Yoneda, D. Zhao, and H. Fujiwara, “Using domain partitioning in wrapper design for IP cores under power constraints,” Proc. IEEE 25th VLSI Test Symposium, pp.369–374, Berkeley, USA (2007).
14) M. Pedram and J. Oh, “Gated clock routing for low-power microprocessor design,” IEEE Trans. Comput. Aided Des. Integr. Circuits Syst., vol.20, no.6, pp.715–722 (2001).
15) Y. Bonhomme, P. Girard, L. Guiller, C. Landrault, and S. Pravossoudovitch, “A Gated clock scheme for low power scan testing of logic ICs orembedded cores,” Proc. IEEE 10th Asian Test Symposium, pp.253–258 (2001).
16) 土屋秀和，阿部高也，浅川毅，“ATPG ベクトルを利用した TPG の電流評価，” 信学技報，DC2007-80 (2008).

本紀要の論文は、情報理工学部紀要委員会
掲載可と判定された原著論文である。

東　海　大　学　紀　要　　情報理工学部
Vol. 20 2020
2021年 3月31日　発　行
発行所　東海大学出版部
〒259-1292　神奈川県平塚市北金目4-1-1
tel　0463-58-7811

Printed in Japan　　（港北出版印刷株式会社）