

# 観測不可能な非決定動作を含む並行 DFISM 群として モデル化される通信プロトコルの適合性試験法

深田 敦史<sup>†</sup> 森 亮憲<sup>†</sup> 中田 明夫<sup>†</sup>  
北道 淳司<sup>††</sup> 樋口 昌宏<sup>†††</sup> 東野 輝夫<sup>†</sup>

高速ネットワークの発展にともない、多くの通信プロトコルが提案されている。そのようなプロトコルのいくつかは、複数個の決定性 FSM (DFISM) 群が協調して動作し、それらの DFISM 群が共通の入力を奪い合って非決定的に動作するようにモデル化できる。そのようなモデルでは、システム全体の動作として、観測不可能な非決定的動作を含む場合がある。本論文では、そのような観測不可能な非決定的動作を含む並行 DFISM 群に対して、GWp-法に基づく 1 つの適合性試験手法を提案する。

## Conformance Testing for Communication Protocols Modeled as Concurrent DFISMs with Non-observable Non-deterministic Behavior

ATSUSHI FUKADA,<sup>†</sup> TAKANORI MORI,<sup>†</sup> AKIO NAKATA,<sup>†</sup>  
JUNJI KITAMICHI,<sup>††</sup> MASAHIRO HIGUCHI<sup>†††</sup> and TERUO HIGASHINO<sup>†</sup>

According to the progress of high-speed networks, many communication protocols are specified as concurrent systems. Such systems can be modeled as concurrent deterministic DFISMs (DFISMs). In those protocols, a common input may be taken by some of concurrent DFISMs competitively (non-deterministically). In such a case, the global behaviour becomes non-observable non-deterministic in general. In this paper, we propose a conformance testing method based on GWp-method for a sub-class of non-observable non-deterministic DFISMs (NDFISMs). The proposed method can be used not only for testing NDFISMs directly but also for testing concurrent DFISMs whose global behavior is non-observable non-deterministic.

### 1. ま え が き

高速ネットワークの発展にともない、並列に複数のプロセスが動作するような通信プロトコルが数多く提案されている。そのようなプロトコルは、協調して動作する複数個の決定性 FSM (DFISM) 群でモデル化されることが多い。このようなプロトコルでは、複数の DFISM に共通する入力信号がある。そのような信号が入力された場合、いずれか 1 つの DFISM が信号を受け取るが、どの DFISM が信号を受け取るかは予測できない。よって、プロトコルは非決定的な動作をする。一般に、非決定性 FSM (NFSM) には、観測可能な NFSM と観測不可能な NFSM がある。ある状

態  $s$  から  $s \xrightarrow{a/b} s'$  と  $s \xrightarrow{a/c} s''$  の 2 つの遷移があるとき、観測可能な NFSM では共通の入力  $a$  に対する出力  $b$  と  $c$  は異ならなければならないが、観測不可能な NFSM では出力  $b$  と  $c$  は同じでもよい。並行 DFISM 群にそのような共通の入力がある場合、 $s \xrightarrow{a/b} s'$  と  $s \xrightarrow{a/c} s''$  のような観測不可能な非決定性の遷移が存在する可能性があり、その場合システム全体は観測不可能な NFSM になる。従来、NFSM に対する適合性試験について、いくつかの研究<sup>1)~7)</sup>がある。しかし、これらの研究では、仕様も実装 (IUT, Implementation Under Test) もすべて観測可能な NFSM としてモデル化されることを想定しており、並行 DFISM 群のように、仕様や実装が観測不可能な NFSM としてモデル化されるような場合の効果的な試験法は知られていない。

観測不可能な NFSM を試験する場合、一般には、その観測不可能な NFSM  $M$  を、それと等価で状態数最小の観測可能な NFSM  $M'$  (標準形と呼ぶ) に変換してから、状態と遷移の実装の正しさをそれぞれ試験す

<sup>†</sup> 大阪大学大学院基礎工学研究科  
Graduate School of Engineering Science, Osaka University

<sup>††</sup> 大阪大学サイバーメディアセンター  
Cybermedia Center, Osaka University

<sup>†††</sup> 近畿大学理工学部  
School of Science and Engineering, Kinki University

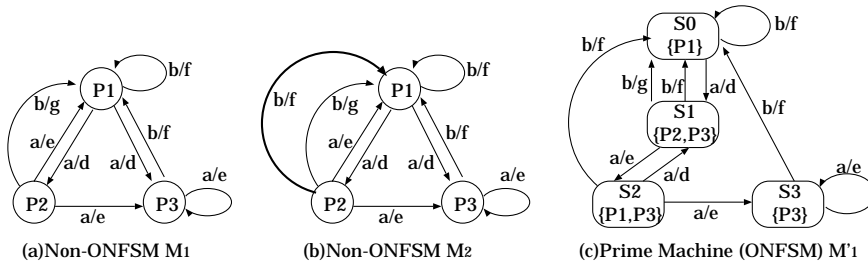


図1 Non-ONFSM とその標準形  
Fig. 1 Non-ONFSMs and their prime machines.

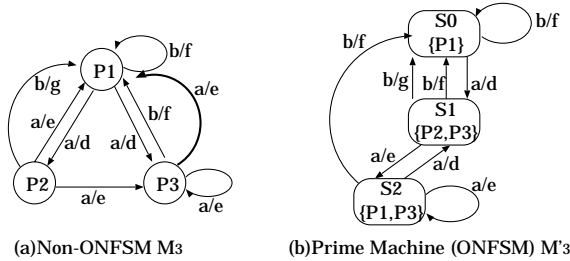


図2 類似の Non-ONFSM とその標準形  
Fig. 2 Similar Non-ONFSM and its prime machine.

る．一般に，与えられた NFSMM から状態数最小の観測可能な NFSM  $M'$  はただ 1 つに定まるが， $M'$  と等価で観測不可能な NFSM は数多く存在する．そのため， $M'$  から生成した試験系列を使っても， $M'$  と等価で観測不可能な NFSM をただ 1 つに特定できない．これが，観測不可能な NFSM を直接試験できない主な理由である．しかし，並行 DFSM 群としてモデル化されるいくつかのプロトコルでは，実装 (IUT) の状態数を制限すると，標準形  $M'$  と等価な NFSM (並行 DFSM 群) がただ 1 つとなる (単一性 (uniqueness property) が成り立つ) ことを証明できる場合がある．

そこで，本論文では，仕様として与えられた状態数  $n$  の観測不可能な NFSM (もしくは並行 DFSM 群)  $M$  と，その標準形  $M'$  に対し，最大  $n$  個の状態からなる観測不可能な NFSM の中に  $M'$  と等価な NFSM が  $M$  以外には存在しないことを保証するための 1 つの手法を提案し，その手法と従来の NFSM に対する適合性試験法の 1 つである GWp-法<sup>3)</sup>を組み合わせる．観測不可能な NFSM の適合性試験を行う方法を提案する．

## 2. 関連研究と課題

一般的な NFSM の試験法として Wp-法 (もしくは，W-法) が知られている<sup>3)</sup>．これらの手法の概略は次のとおりである．

(1) 観測不可能な NFSM (Non-ONFSM)  $M$  に対

して，それと等価で状態数最小 (その状態数を  $n'$  とする) の観測可能な NFSM (ONFSM)  $M'$  ( $M$  の標準形，prime machine) を構成する．  
(2)  $M'$  の先行系列の集合を  $V'$ ， $W$  集合を  $W'$  とする． $m' \geq n'$  を満たす任意の整数  $m'$  について， $TS_{M'} = V'X^{m'-n'+1}W'$ ， $X^1 = X \cup \{\epsilon\}$  とする．このとき， $TS_{M'}$  はただか  $m'$  個の状態からなる ONFSM モデルの IUT に対して，100% の誤り検出能力を持つ試験系列となる．特に  $m' = n'$  が成り立つ場合， $TS_{M'} = V'X^1W' = V'W' \cup V'XW'$  である．

この試験法は，(i)  $TS_{M'}$  は 100% の誤り検出能力を持つ，(ii) 適用可能なモデルに対する制約がない，(iii) これまでこれ以外の効果的な試験法が提案されていない，などの利点がある．しかし，仕様と IUT は ONFSM でモデル化されていなければならない，前章で述べたように，Non-ONFSM でモデル化されている場合に直接この試験法を適用できない，などの問題点がある．たとえば，図 1 (a) の  $M_1$  と図 1 (b) の  $M_2$  の標準形はともに図 1 (c) の  $M'_1$  になってしまい， $TS_{M'_1}$  でこれら  $M_1$  と  $M_2$  を区別できない．また，図 1 (a) の  $M_1$  と図 2 (a) の  $M_3$  を考えると，これらに対応する標準形は，それぞれ図 1 (c) の  $M'_1$  と図 2 (b) の  $M'_3$  になる．図 2 (a) の  $M_3$  は， $M_1$  に状態  $P_3$  から  $P_1$  に至る遷移  $a/e$  を余分に付け加えたものである．しかし，対応する標準形  $M'_1$  と  $M'_3$  は

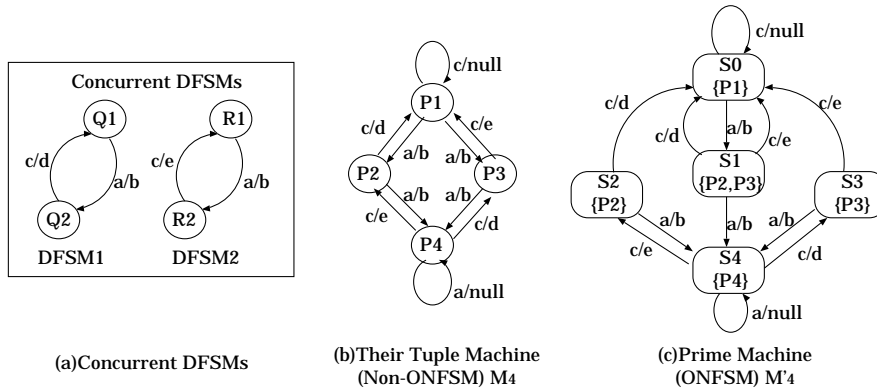


図3 並行 DFSM 群と対応する直積マシンと標準形  
Fig. 3 Concurrent DFSMs and corresponding NFSMs.

その状態数が異なっている．もし  $M_1$  と  $M_3$  (正確には  $M'_1$  と  $M'_3$ ) を区別するのに,  $M'_1$  から生成した  $TS_{M'_1} = V'X^1W'_1$  を用いて試験する場合,  $TS_{M'_1}$  は 4 状態までの ONFSM なら区別することができるので, これら  $M_1$  と  $M_3$  を区別できる．しかし,  $M'_3$  から生成した  $TS_{M'_3} = V'X^1W'_3$  を使用する場合, 3 状態までの ONFSM しか区別できないため, これらを区別できない可能性がある．区別したい場合,  $V'X^2W'_3$  を使用しなければならない． $n$  状態の Non-ONFSM を標準形に変換した場合, その状態数は最悪で  $O(2^n)$  になってしまい,  $TS_{M'} = V'X^{O(2^n)}W'$  の試験系列が必要となる．

特にこのことは, 並行 DFSM 群の試験においては深刻な問題となる．例として, 図 3 (a) の DFSM 群を考える．図 3 (a) の DFSM1 と DFSM2 は並行に動作する．初期状態の組  $\langle Q1, R1 \rangle$  に対して入力  $a$  が与えられると, どちらか 1 つの DFSM がそれを受け取り,  $b$  を出力する．ただし, 入力  $a$  をどちらの DFSM が受け取るのかは特定できないものとする．また, 1 つの DFSM がある入力を受け取ることができ, もう 1 つの DFSM がその入力を受け取れない場合, 前者の DFSM が必ずその入力を受け取るものとする．このため, 状態組  $\langle Q2, R1 \rangle$  に対して入力  $a$  を与えた場合, 必ず DFSM2 がそれを受け取るものとする．もし, 両方の DFSM がある入力をもとに受け取れない場合, システムはその入力に対して  $null$  を出力し状態組は変化しないものとする．これらの仮定のもとで, システム全体の動作を表す直積マシン (tuple machine) を構成する．図 3 (b) にその例を示す．状態  $P1, P2, P3, P4$  はそれぞれ状態組  $\langle Q1, R1 \rangle, \langle Q2, R1 \rangle, \langle Q1, R2 \rangle, \langle Q2, R2 \rangle$  に対応する．直積マシンは 4 状態の Non-ONFSM で表される．一方, こ

れに対応する標準形は図 3 (c) のようになり, 5 状態となる．

図 3 (a) の並行 DFSM 群の動作は, たとえ各 DFSM にいくつかの実装誤りがあったとしても, 各 DFSM の状態数に変化がなければ, それらの直積マシンは図 3 (b) のような 4 状態の Non-ONFSM としてモデル化される．しかし, 従来の適合性試験法では, IUT は ONFSM としてモデル化されなければならない．上述のように 4 状態の Non-ONFSM でモデル化された (誤りを含むかもしれない) いくつかの IUT に対する標準形の状態数は異なっている．このため, 協調して動作する DFSM 群が観測不可能な非決定性の動作を行う場合の適合性試験 (等価でない DFSM 群の検出) は非常に困難になってしまう．文献 (6), (8), (9) に並行システムの適合性試験における問題点や解決法が述べられている．

### 3. 提案する試験法

#### 3.1 単一性と試験手法の概要

$n$  個の状態を持つ Non-ONFSM を  $M$ , その標準形 (状態数最小の ONFSM) を  $M'$  とする．もし,  $M$  が  $n$  個以下の状態を持つ NFSM のクラスの中で唯一  $M'$  と等価な NFSM であるなら,  $n$  個までの状態からなる  $M'$  と等価なすべての NFSM は  $M$  と同形になる．このとき,  $M$  は  $n$  個以下の状態を持つ NFSM のクラスの中で単一性 (uniqueness property) が成り立つという．そこで, 単一性に基づく次のような試験法を提案する．

- (1)  $n$  状態の NFSM としてモデル化されている仕様  $M$  に対して, 対応する ONFSM の標準形  $M'$  を構成する．
- (2)  $M'$  の 1 つの W 集合を  $W_{M'}$  とする． $M, M',$

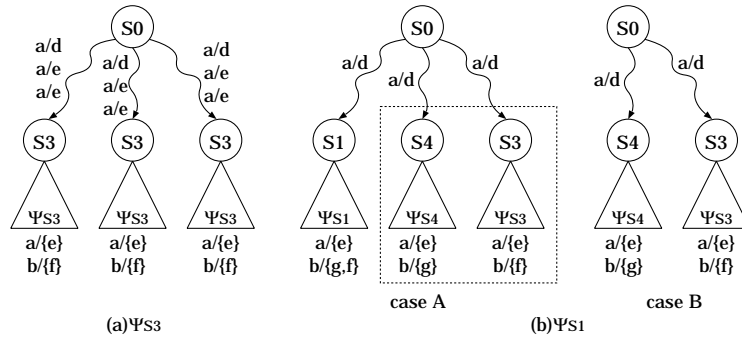


図4 テスト系列の実行  
Fig. 4 Execution of test sequences.

$W_{M'}$ , 状態数  $n$  から,  $M$  がたかだか  $n$  個の状態を持つ NFSM のクラスの中で単一性が成り立つ ( $M'$  と等価なただ 1 つの NFSM) かどうかを判定する. NFSM の単一性の判定は, 次節以降で述べる状態の単一性と遷移の単一性に分けて判定する.

- (3)  $M$  の単一性が成り立つ場合,  $V'$  を  $M'$  の先行系列の集合とし, 入力記号の集合  $X$  に対し,  $TS_{M'} = V'X^1W_{M'} = V'W_{M'} \cup V'XW_{M'}$  を試験系列集合として構成する. IUT は  $n$  個以下の状態を持つ NFSM としてモデル化されているという仮定のもとで, 与えられた IUT がこの試験系列  $TS_{M'}$  をパスすれば,  $M$  と同形であると判断する.

3.2 状態の単一性の判定法

まず,  $TS_{M'} = V'W_{M'} \cup V'XW_{M'}$  の前半の  $V'W_{M'}$  を用いて状態存在の確認を行う.

説明の例として, 図 1(a) の NFSM  $M_1$  を考える. NFSM  $M_1$  に対応する標準形  $M'_1$  は図 1(c) である. 今,  $W_{M'_1}$  として  $\{a, b\}$  なる入力系列の集合を選んだとする. このとき,  $W_{M'_1}$  に含まれる入力系列を  $M'_1$  の各状態  $t$  に与えたときに得られる入出力系列の集合を,  $\Psi_t$  とする. 図 1(c) の  $M'_1$  に対して, 次のような  $\Psi_t$  が得られる.

- $\Psi_{S0} : a/{d} \quad b/{f}$
- $\Psi_{S1} : a/{e} \quad b/{g, f}$
- $\Psi_{S2} : a/{d, e} \quad b/{f}$
- $\Psi_{S3} : a/{e} \quad b/{f}$

以下, 2 通りの場合に分けて考える.

- (case-i)  $W_{M'_1}$  の各入力系列に対する出力系列がただ 1 つの場合:

$\Psi_{S0}$  と  $\Psi_{S3}$  は, 各入力系列に対する出力系列がただ 1 つに定まっている. この場合, 初期状態から状

態  $t$  に遷移させるための先行系列を与えた後,  $W_{M'_1}$  に含まれる各入力系列を与え, その出力系列を調べることで, 状態  $t$  の存在を確認できる. ただし, 図 4(a) のように, 状態  $t$  と等価な状態が 2 つ以上存在するかもしれない.

- (case-ii)  $W_{M'_1}$  の各入力系列に対する出力系列が 2 つ以上ある場合:

$\Psi_{S1}$  と  $\Psi_{S2}$  は, 各入力系列に対する出力系列がただ 1 つではない. 今,  $S1$  への先行系列を与えたとする. この状態から  $\Psi_{S1}$  の入出力系列が観測できた場合, 次の 2 つの可能性が考えられる. 次の  $\Psi_{S4}$  のような反応を返す,  $M'_1$  に含まれない新たな状態を  $S4$  とする.

$$\Psi_{S4} : a/{e} \quad b/{g}$$

1 つの可能性は, 図 4(b) の case A のように,  $\Psi_{S1}$  のような反応を返す  $S1$  に対応する状態が少なくとも 1 つ存在する場合である. もう 1 つの可能性は, 図 4(b) の case B のように,  $M'_1$  に含まれない新たな状態  $S4$  に対応する状態が少なくとも 1 つあり, かつ,  $S3$  に対応する状態も少なくとも 1 つあるような場合である. これは,  $\Psi_{S4}$  と  $\Psi_{S3}$  の和集合が  $\Psi_{S1}$  になるためである. case A の場合でも,  $S4$  と  $S3$  の両方の状態が存在する場合もありうる (和集合が等しいため).

先に述べたように (case-ii) のように出力系列がただ 1 つに定まらない場合, 出力系列の和集合が等しいすべての可能な状態の組を考慮する. ここで,  $\psi_{Si}$  を  $\Psi_{Si}$  のような入出力系列を持つ状態が少なくとも 1 つ存在するとき真となるような論理変数とする. 各状態について, どんな  $\psi_{Si}$  の組合せが真になるかを考え, 可能な組合せに関する論理式を構成する. すなわち, 各  $\Psi_{Si}$  の入出力系列をもとに, 可能性のあるすべての  $\psi_{Si}$  の組合せを構成する. もし, 可能性のある状

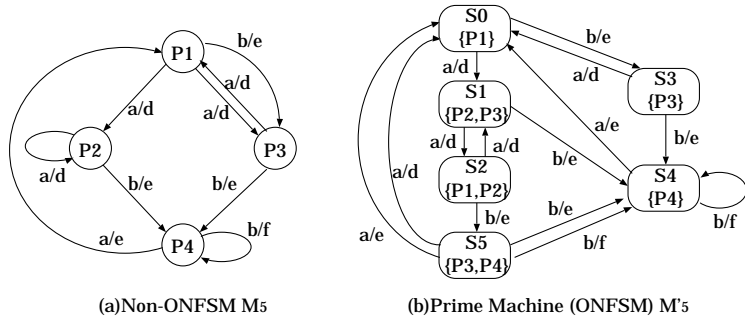


図 5 状態の単一性を持つ Non-ONFSM  
Fig. 5 Non-ONFSM with uniqueness of states.

態の組合せがただ 1 つであれば，与えられた NFSM の状態の存在が確認される。

図 1(c) の  $M'_1$  の場合，次のような可能性を考えることができる。

- 状態  $S_0$  について： $C_0 = \psi_{S_0}$
- 状態  $S_1$  について： $C_1 = \psi_{S_1} \vee (\psi_{S_4} \wedge \psi_{S_3})$
- 状態  $S_2$  について： $C_2 = \psi_{S_2} \vee (\psi_{S_0} \wedge \psi_{S_3})$
- 状態  $S_3$  について： $C_3 = \psi_{S_3}$

ここで，仕様の NFSM が図 1(a) や図 1(b) の NFSM のように 3 状態以下の Non-ONFSM でモデル化されていると仮定する。 $AtMost(X, n)$  を  $X$  中のたかだか  $n$  個の論理変数が真のときのみ真になるような論理式とする。たとえば， $AtMost(\{x, y, z\}, 2) = \neg(x \wedge y \wedge z)$  である。ここで，次の条件式がただ 1 つの解を持つかどうかを調べてみる。

$$C_0 \wedge C_1 \wedge C_2 \wedge C_3 \wedge AtMost(ST'_1, 3)$$

ただし， $ST'_1 = \{\psi_{S_i} | S_i \text{ は ONFSM } M'_1 \text{ と } W_{M'_1} \text{ から上述の方法で生成可能な状態}\}$  である。以下では，上述の論理式を状態の単一性を判定する論理式と呼ぶ。

上の論理式は， $\{\psi_{S_0}, \psi_{S_4}, \psi_{S_3}\}$  と  $\{\psi_{S_0}, \psi_{S_1}, \psi_{S_3}\}$  の 2 つの解を持つ。 $M_1$  の場合， $\psi_{S_0} = \psi_{P_1}$ ， $\psi_{S_1} = \psi_{\{P_2, P_3\}}$ ， $\psi_{S_3} = \psi_{P_3}$ ， $\psi_{S_4} = \psi_{P_2}$  が成り立つため，次の解が得られる。

$$\begin{aligned} \{\psi_{S_0}, \psi_{S_4}, \psi_{S_3}\} &= \{\psi_{P_1}, \psi_{P_2}, \psi_{P_3}\} \\ \{\psi_{S_0}, \psi_{S_1}, \psi_{S_3}\} &= \{\psi_{P_1}, \psi_{\{P_2, P_3\}}, \psi_{P_3}\} \end{aligned}$$

これは，もともとの NFSM の状態には 2 つの可能性を示している。つまり，この例では状態の単一性は成り立たないと判定できる。図 1(a) と図 1(b) の  $M_1$  と  $M_2$  が上の 2 つの状態の集合に対応しており，図 1(c) のように，その両方が標準形である  $M'_1$  と等価である。

次に状態の単一性が成り立つ例を紹介する。図 5(a) の NFSM  $M_5$  を考える。対応する ONFSM  $M'_5$  は図 5(b) のようになる。 $M_5$  に対する  $W$  集合として，

$W_{M'_5} = \{abb, ba\}$  なる入力系列の集合を選ぶとする。このとき  $\Psi_t$  は次のようになる。

- $\Psi_{S_0}$  :  $abb/\{def\}$        $ba/\{ed\}$
- $\Psi_{S_1}$  :  $abb/\{dee, def\}$        $ba/\{ee\}$
- $\Psi_{S_2}$  :  $abb/\{def\}$        $ba/\{ee, ed\}$
- $\Psi_{S_3}$  :  $abb/\{dee\}$        $ba/\{ee\}$
- $\Psi_{S_4}$  :  $abb/\{eee\}$        $ba/\{fe\}$
- $\Psi_{S_5}$  :  $abb/\{eee, dee\}$        $ba/\{ee, fe\}$

$M'_5$  に含まれない可能な状態を列挙すると，次のようなものが考えられる。

- $\Psi_{S_6}$  :  $abb/\{def\}$        $ba/\{ee\}$
- $\Psi_{S_7}$  :  $abb/\{eee, dee\}$        $ba/\{ee\}$
- $\Psi_{S_8}$  :  $abb/\{eee, dee\}$        $ba/\{fe\}$
- $\Psi_{S_9}$  :  $abb/\{eee\}$        $ba/\{ee, fe\}$
- $\Psi_{S_{10}}$  :  $abb/\{dee\}$        $ba/\{ee, fe\}$
- $\Psi_{S_{11}}$  :  $abb/\{eee\}$        $ba/\{ee\}$
- $\Psi_{S_{12}}$  :  $abb/\{dee\}$        $ba/\{fe\}$

このとき，次の関係式が成り立つ。

$$\begin{aligned} \Psi_{S_0} &= \Psi_{P_1}, \Psi_{S_6} = \Psi_{P_2}, \\ \Psi_{S_3} &= \Psi_{P_3}, \Psi_{S_4} = \Psi_{P_4} \end{aligned}$$

各状態の入出力系列から，4 状態までの NFSM のクラスに対する状態の単一性を判定する論理式を構成し，その解が一意となるかどうかを調べる。上述の場合，ただ 1 つの解  $\{\psi_{S_0}, \psi_{S_6}, \psi_{S_3}, \psi_{S_4}\}$  が得られる。これは  $\{\psi_{P_1}, \psi_{P_2}, \psi_{P_3}, \psi_{P_4}\}$  に対応している。よって， $M_5$  は 4 状態以下の NFSM のクラスの中で状態の単一性が成り立つと判定できる。

### 3.3 遷移の単一性の判定法

前節では状態の存在の確認を行った。しかし，状態の確認では，試験系列  $V'W_{M'}$  に含まれない入力系列に対する反応については何も保証されていない。NFSM の単一性を保証するためには，遷移の実装の正しさの

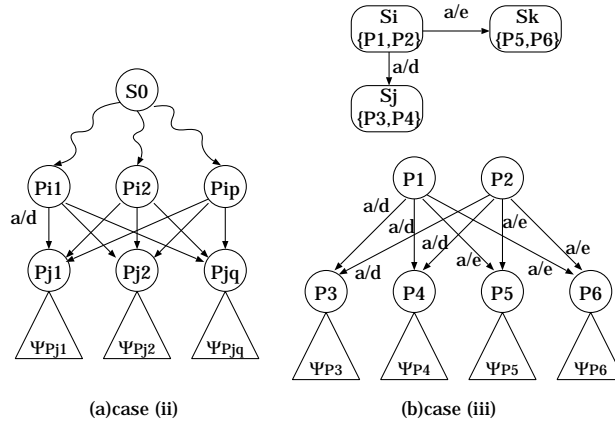


図6 NFSMの遷移の実装の正しさの試験  
Fig. 6 Testing transitions in NFSMs.

確認も行う必要がある。遷移の実装の正しさの確認は、次のように試験系列  $V'XW_{M'}$  を用いて、状態の存在の確認の方法と類似した方法で行う。なお、以下の議論では状態の存在は確認されているものとして議論を進める。

まず、標準形の各遷移  $S_i \xrightarrow{\alpha/\beta} S_j$  に対して試験系列  $V'XW_{M'}$  を与える。今、 $S_i$  と  $S_j$  は標準形の状態を表し、 $P_{i'}$  と  $P_{j'}$  はもとのNFSMの状態を表すとする。このとき、次の3つの場合が考えられる。

(i)  $\psi_{S_i} = \psi_{P_{i'}}$ ,  $\psi_{S_j} = \psi_{P_{j'}}$  が成り立ち、状態  $S_i$  から入力  $\alpha$  で遷移するような他の遷移は存在しない場合(たとえば、図5(b)の  $S_0 \xrightarrow{b/e} S_3$  は、図5(a)の  $P_1 \xrightarrow{b/e} P_3$  に対応している)：

はじめに先行系列の集合  $V'$  中の系列によって状態  $S_i$  に遷移させる。そこで入力  $\alpha$  を与え、その出力が  $\beta$  であるかどうかを調べる。その後、 $W_{M'}$  中の系列を与える。もし入出力系列の集合が  $\Psi_{S_j}$  と同じであれば、 $\Psi_{S_j}$  の入出力系列を実行できる状態は  $S_j$  以外にありえないことから、遷移先の状態は  $S_j$  であると判断できる。

ここで、遷移の実装の正しさを確認するための新たな論理変数  $\Phi_{\alpha\beta i'j'}$  を導入する。これは、ももとのNFSMに  $P_{i'} \xrightarrow{\alpha/\beta} P_{j'}$  なる遷移が存在するとき真になる変数とする。(i)の場合、IUTが  $S_i \xrightarrow{\alpha/\beta} S_j$  に対する試験系列をパスすれば、次の論理式を得ることができる。

$$\Phi_{\alpha\beta i'j'} = 1 \tag{i.1}$$

また、この遷移を実行したときは  $\beta$  が出力されるだけなので、 $\beta$  以外のすべての出力  $\gamma$  に対して、次の論理式も得られる。

$$\Phi_{\alpha\gamma i'j'} = 0 \tag{i.2}$$

状態  $S_i(P_{i'})$  からの遷移には、 $S_i \xrightarrow{\alpha/\beta}$  以外の遷移は存在しないので、すべての出力  $\delta$  と  $P_{j'}$  以外のすべての状態  $P_{j''}$  に対して、次の論理式も成り立つ。

$$\Phi_{\alpha\delta i'j''} = 0 \tag{i.3}$$

(ii)  $\psi_{S_i} = \psi_{P_{i1}} \cup \psi_{P_{i2}} \cup \dots \cup \psi_{P_{ip}}$  または  $\psi_{S_j} = \psi_{P_{j1}} \cup \psi_{P_{j2}} \dots \cup \psi_{P_{jq}}$  が成り立つ場合で、図5(b)の  $S_1 \xrightarrow{a/d} S_2$  のように入力  $\alpha$  で遷移するような他の遷移が存在しない場合：

試験法は(i)と同じであって、先行系列集合  $V'$  中の系列によって状態  $S_i$  に遷移させると、図6(a)のように、もとのNFSMでは  $P_{i1}, P_{i2}, \dots$  もしくは  $P_{ip}$  のいずれかの状態に遷移している。また、状態の存在が確認されているので、 $V'$  の系列によって  $P_{i1}, \dots, P_{ip}$  のいずれの状態にも遷移できる。これらの状態から  $\alpha/\beta$  が実行できるので、次の論理式が成り立つ。

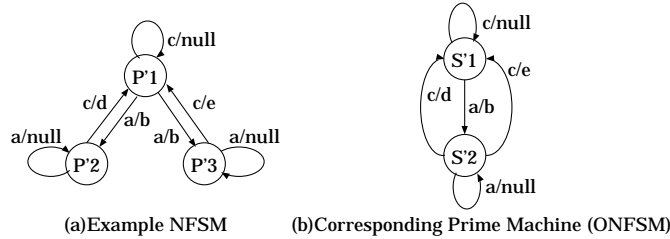
$$\Phi_{\alpha\beta i1j1} \vee \Phi_{\alpha\beta i1j2} \vee \dots \vee \Phi_{\alpha\beta i1jq} = 1 \tag{ii.1}$$

$$\Phi_{\alpha\beta ipj1} \vee \Phi_{\alpha\beta ipj2} \vee \dots \vee \Phi_{\alpha\beta ipjq} = 1$$

$\alpha/\beta$  を実行した後、 $\Psi_{S_j}$  が観測できた場合、もとのNFSMは  $P_{j1}, P_{j2}, \dots$  もしくは  $P_{jq}$  のいずれかの状態に遷移している。このとき、各  $P_{j_h} \in \{P_{j1}, \dots, P_{jq}\}$  に対して  $\psi_{S_i} - \psi_{P_{j_h}} \neq \psi_{S_i}$  が成り立てば、 $P_{i1}, \dots, P_{ip}$  のいずれかの状態から  $P_{j_h}$  への  $\alpha/\beta$  遷移が存在する。すべての  $P_{j_h}$  に対してこの条件が成立する場合、以下の論理式が成立する。

$$\Phi_{\alpha\beta i1j1} \vee \Phi_{\alpha\beta i2j1} \vee \dots \vee \Phi_{\alpha\beta ipj1} = 1 \tag{ii.2}$$

$$\Phi_{\alpha\beta i1jq} \vee \Phi_{\alpha\beta i2jq} \vee \dots \vee \Phi_{\alpha\beta ipjq} = 1$$



(a)Example NFSM (b)Corresponding Prime Machine (ONFSM)

図7 標準形より状態数の多いNFSMの例

Fig.7 NFSM whose number of states exceeds that of corresponding prime machine.

同様に,  $\beta$  以外のすべての出力  $\gamma$  と  $i \in \{i_1, \dots, ip\}$  および  $j \in \{j_1, \dots, jq\}$  の組に対して, 以下の論理式も成立する.

$$\Phi_{\alpha\gamma ij} = 0 \quad (\text{ii.3})$$

また, すべての出力  $\delta$  とすべての  $i \in \{i_1, \dots, ip\}$  および  $\{P_{j1}, \dots, P_{jq}\}$  以外のすべての  $P_j$  の組に対して, 以下の論理式が成立する.

$$\Phi_{\alpha\delta ij} = 0 \quad (\text{ii.4})$$

(iii) 図6(b)のように, ある状態から同じ入力に対して異なる出力をする2つ以上の遷移  $S_i \xrightarrow{\alpha/\beta_1} S_{j1}$  と  $S_i \xrightarrow{\alpha/\beta_2} S_{j2}$  がある場合:

この場合の制約条件は以下の点を除いて, (ii) の場合とほぼ同じである. 図6(b)において, 入力  $a$  に対する状態  $S_i$  ( $\{P1, P2\}$  に相当) からの遷移が  $S_i \xrightarrow{a/d} S_j$  と  $S_i \xrightarrow{a/e} S_k$  の2つあるので, 条件(ii.1)は  $a/d$  または  $a/e$  の遷移の存在を表す次のような論理式に修正する.

$$\Phi_{ad13} \vee \Phi_{ad14} \vee \Phi_{ae15} \vee \Phi_{ae16} = 1 \quad (\text{iii.1})$$

同様に (ii.2) も同じような修正を施した論理式を作成する. すなわち, もし  $\psi_{S_i} = \psi_{P_3} \cup \psi_{P_4}$  が  $\psi_{S_i} \neq \psi_{S_i} - \psi_{P_3}$ ,  $\psi_{S_i} \neq \psi_{S_i} - \psi_{P_4}$  の2つの条件を満足するなら,  $a/d$  の実行後は  $P_3$  にも  $P_4$  にも遷移する. また,  $a/e$  の実行後は  $P_5$  にも  $P_6$  にも遷移する. よって, 条件(ii.2) は次のような論理式に修正する.

$$\begin{aligned} \Phi_{ad13} \vee \Phi_{ad23} &= 1 \\ \Phi_{ad14} \vee \Phi_{ad24} &= 1 \\ \Phi_{ae15} \vee \Phi_{ae25} &= 1 \\ \Phi_{ae16} \vee \Phi_{ae26} &= 1 \end{aligned} \quad (\text{iii.2})$$

また, 論理式(ii.3), (ii.4)に相当する論理式も同様に構成できる.

以上のような構成法で得られたすべての論理式の論理積を遷移の単一性を判定する論理式と呼ぶことにする. この論理式がただ1つの解を持てば, 遷移の単一性が成り立つと判定できる.

たとえば, 図5のNFSM  $M_5$  は4状態までのNFSMのクラスで単一性を持っていることを証明できる. 概略は次のようになる. 状態  $S_5$  に遷移させる先行系列を与えると, もとのNFSMでは  $P_3$  か  $P_4$  のいずれかに遷移している. このとき, 入力  $b$  を与えると,  $b/e$  と  $b/f$  が観測できるので,  $P_4$  は余分な遷移  $P_4 \xrightarrow{b/e} P_4$  を持っているかもしれないと考えられる. しかし, 状態  $S_4$  に遷移させて, そこで入力  $b$  に対する出力を観測すると  $P_4 \xrightarrow{b/e} P_4$  という遷移は存在しないことが分かる. 状態  $S_1$  に遷移させた後, 入力  $a$  と  $W$  集合を与え, その出力を観測すると, 余分な遷移  $P_2 \xrightarrow{a/d} P_1$  が存在するかもしれないと考えられる. しかし, 状態  $S_2$  に遷移させ, そこで入力  $a$  と  $W$  集合を与え, その出力を観測すると, そのような遷移  $P_2 \xrightarrow{a/d} P_1$  が存在しないことが分かる. 先に述べた制約条件は, このような状況を表している.

#### 4. 議 論

2章でも述べたように, 図3のような典型的なDFSM群に対しては, その直積マシンとなるNFSMの単一性を証明できる. しかし, 一般に与えられたDFSM群が必ず単一性を持つという保証はない. また, 与えられたNFSMがその標準形のONFSMより状態数が多い場合, 単一性は成り立たず, 本手法は適用できない. 以下では, そのような場合に対する1つの対応策を与える.

まず, 最初にそのような例を示す. 2章で説明した図3(a)のDFSM群では, つねに2つのDFSMは並行に動作すると仮定していた. 以下では, このDFSM群に対して, 一方のDFSMが入力  $a$  を読み込んだ場合, そのDFSMが次の入力  $c$  を読み込むまで, もう一方のDFSMは入力  $a$  を読み込むことができないと仮定する. その場合, 全体の動作を表す直積マシンは図7(a)のように表される. 図7(a)状態  $P'1, P'2, P'3$  はそれぞれ  $\langle Q1, R1 \rangle, \langle Q2, R1 \rangle, \langle Q1, R2 \rangle$  に対応する. 直積マシンは3状態でNon-ONFSMである.

他方, 対応する標準形の ONFSM は図 7(b) のようになり, 2 状態である. このため, 図 7(a) の Non-ONFSM は 3 状態までの NFSM のクラスの中で単一性を持たない.

図 7(b) の標準形に対して, 次の 2 つの  $\Psi_t$  が得られる.

$$\begin{aligned}\Psi_{S'1} &: a/\{b\} & c/\{\text{null}\} \\ \Psi_{S'2} &: a/\{\text{null}\} & c/\{d, e\}\end{aligned}$$

しかし, この章では, 与えられた DFSM 群に対して, 一方の DFSM が入力  $a$  を読み込んだ場合, その DFSM が次の入力  $c$  を読み込むまでもう一方の DFSM は入力  $a$  を読み込むことができないと仮定している. このような場合, どちらか一方の DFSM し入力  $c$  を読み込むことができない. この場合, 直積マシンに  $\Psi_{S'2}$  のように入力  $c$  に対して  $d$  と  $e$  の両方を返すような状態は存在しない. この仮定のもとでは, 次のような 3 つの反応を返す状態しか存在しない.

$$\begin{aligned}\Psi_{S'1} &: a/\{b\} & c/\{\text{null}\} \\ \Psi_{S'3} &: a/\{\text{null}\} & c/\{d\} \\ \Psi_{S'4} &: a/\{\text{null}\} & c/\{e\}\end{aligned}$$

これらの状態は, 図 7(a) の  $P'1, P'2, P'3$  の 3 状態に対応している. このように, 与えられた DFSM 群の動作を表す直積マシンの状態に対して, 何らかの仮定を与えると, 与えられた NFSM がその標準形の ONFSM より状態数が多いような場合でも, 単一性が保証できる場合があり, そのような場合, 提案する手法で, 与えられた IUT と仕様との等価性が保証できる.

## 5. ま と め

本論文では, 観測不可能な NFSM のサブクラスに対して  $\text{GW}_p$ -法に基づく適合性試験法を提案した. 提案する試験法は, NFSM を直接試験するだけでなく, 全体として観測不可能な非決定性の動作を行いながら協調して動作する DFSM 群の試験にも適用できる. NFSM の適合性試験についてはいくつか研究が行われているが, ほとんどの試験法が観測可能な NFSM としてモデル化された仕様を対象としており, 観測不可能な NFSM を直接試験しようとする研究はほとんどない. 本論文では, 状態数  $n$  個までの NFSM のクラスで単一性を持つような NFSM に対する適合性試験法を提案している. 現在, この単一性を機械的にチェックするツールを開発中である. 今後は, 実用的なアプリケーションに本手法を適用し, その有用性を

評価することが課題である.

## 参 考 文 献

- 1) Kloosterman, H.: Test Derivation from Non-deterministic Finite State Machines, *Proc. 5th IFIP International Workshop on Protocol Test Systems (IWPTS'92)*, pp.297–308 (1992).
- 2) Lee, D., Sabnani, K.K., Kristol, D.M. and Paul, S.: Conformance Testing of Protocols Specified as Communicating FSMs, *Proc. IEEE INFOCOM'93*, pp.115–127 (1993).
- 3) Luo, G., Bochmann, G.V. and Petrenko, A.: Test Selection Based on Communicating Non-deterministic Finite State Machines using a Generalized Wp-method, *IEEE Trans. Softw. Eng.*, Vol.20, No.2, pp.149–162 (1994).
- 4) Tripathy, P. and Naik, K.: Generation of Adaptive Test Cases from Nondeterministic Finite State Models, *Proc. 5th IFIP International Workshop on Protocol Test Systems (IWPTS'92)*, pp.309–320 (1992).
- 5) Ulrich, A. and Chanson, S.T.: An Approach to Testing Distributed Software Systems, *Proc. 15th IFIP International Symposium on Protocol Specification, Testing and Verification*, pp.121–136 (1995).
- 6) Fukada, A., Kaji, T., Higashino, T., Taniguchi, K. and Mori, M.: A Conformance Testing for Communication Protocols Modeled as A Set of DFSMs with Common Inputs, *Proc. 10th IFIP International Workshop on Testing of Communicating Systems (IWTCS'97)*, pp.239–254 (1997).
- 7) Petrenko, A., Yevtushenko, N. and Bochmann, G.V.: Testing Deterministic Implementations from Nondeterministic FSM Specifications, *Proc. 9th IFIP International Workshop on Testing of Communicating Systems (IWTCS'96)*, pp.125–140 (1996).
- 8) Yevtushenko, N., Cavalli, A. and Anido, R.: Test Suite Minimization for Embedded Non-deterministic Finite State Machines, *Proc. 12th IFIP International Workshop on Testing of Communicating Systems (IWTCS'99)*, pp.237–250 (1999).
- 9) Toro, M.: Decision on Testing Configuration for Multiparty Testing, *Proc. 12th IFIP International Workshop on Testing of Communicating Systems (IWTCS'99)*, pp.109–128 (1999).

(平成 13 年 5 月 21 日受付)

(平成 13 年 10 月 16 日採録)





深田 敦史

平成 10 年大阪大学大学院基礎工学研究科博士前期課程修了。同年、ヤマハ(株)勤務、現在に至る。平成 12 年より大阪大学大学院基礎工学研究科博士後期課程在学中。電子音楽やマルチメディア、通信プロトコル等に関する研究に従事。



森 亮憲(学生会員)

平成 10 年大阪大学基礎工学部情報工学科卒業。平成 12 年同大学大学院博士前期課程修了。現在、同大学院博士後期課程在学中。通信プロトコルの適合性試験、検証法等の研究に従事。



中田 明夫(正会員)

平成 4 年大阪大学基礎工学部情報工学科卒業。平成 9 年同大学大学院基礎工学研究科物理系専攻博士後期課程修了。同年広島市立大学情報科学部助手。現在、大阪大学大学院基礎工学研究科助手。博士(工学)。実時間システムや分散システムの仕様記述と検証法、プロセス代数、時相論理等の研究に従事。



北道 淳司(正会員)

1965 年生。1988 年大阪大学基礎工学部情報工学科卒業。1991 年同大学大学院博士後期課程中退。同年大阪大学基礎工学部情報科学科助手。1999 年同大学大学院基礎工学研究科講師。現在同大学サイバーメディアセンター講師。工学博士。ハードウェアの形式的検証、動的再構成可能 FPGA およびコンピュータリテラシに関する研究に従事。



樋口 昌宏(正会員)

昭和 58 年大阪大学基礎工学部情報工学科卒業。昭和 60 年同大学大学院博士前期課程修了(株)富士通研究所勤務、大阪大学助手、講師を経て、現在近畿大学理工学部電気工学科助教授。博士(工学)。通信プロトコル等の並行処理系の検証、試験に関する研究に従事。



東野 輝夫(正会員)

昭和 54 年大阪大学基礎工学部情報工学科卒業。昭和 59 年同大学大学院博士課程修了。同年大阪大学助手。平成 2,6 年モンテリオール大学客員研究員。現在、大阪大学大学院基礎工学研究科教授。工学博士。分散システム、通信プロトコル等の研究に従事。電子情報通信学会、ACM 各会員。IEEE Senior Member。