マルチメディア通信と分散処理 74－4
グループウェア 15－4
（1996. 1. 25）

複数個のFSMからなるプロトコル機械に対する適合性試験の一手法

鍛 忠司　東野 輝夫　谷口 健一

大阪大学 基礎工学部 情報工学科

あらまし　通信プロトコルに対する適合性試験は通信システムの信頼性を高めるために有効である．従来，適合性試験系列の生成に関する研究の多くは単一の有限状態機械 (FSM) によってモデル化されるソフトウェアを対象としている．しかし，複数のチャネルを持つ通信プロトコルなどでは，一つのチャネルの制御部を一つの決定性 FSM(DFSM) でモデル化し，システム全体を入力を奪い合いながら並行に動作する DFSM 群 (DFSMs の直積マシン) としてモデル化することが自然である．このようなシステムは全体としてもとの DFSM 群の状態数の積に比例する状態を持つ非決定性 FSM(NFSM) になる．このため，通常の NFSM に対する試験法を用いた場合，試験系列長がもとの DFSM 群の状態数の積に比例するオーダーになるという問題点があった．本稿では，そのような入力を奪い合いながら並行に動作する複数の DFSM 群としてモデル化されるような通信プロトコルのある部分クラスに対して，DFSM 群の状態数の和に比例する程度のコストで効率よく適合性試験を行えるようにするための一つの手法を提案する．提案する手法では，まず，W-法を用いて単独に各 DFSM の試験を行う場合に用いる先行系列の集合からシステム全体の試験を行うための先行系列の集合を生成する．また，各 DFSM に対する特性集合の和集合をシステム全体の試験を行うための特性集合とする．次に，与えられた各特性系列に対して正しく反応を返す可能性のある状態対をすべて列挙し，その関係を表す制約式を生成する．これらの制約式を満たす解（状態の組）が仕様として与えられた DFSM 群の状態対のみならば，与えられた先行系列の集合と特性集合に対して正しい反応を示す実装は仕様の DFSM 群と等価であることが保証される．

A Conformance Testing for Communication Protocols modeled as Coupled DFSMs

Tadashi Kaji　Teruo Higashino　Kenichi Taniguchi

Dept. of Information and Computer Sciences, Osaka University

Machikaneyama 1-3, Toyonaka, Osaka 560, Japan

Abstract　Conformance testing for communication protocols is useful for developing a highly reliable communication systems. Many researches have been done for test generation of the software modeled as a single finite-state machine (FSM). However, it is natural that the protocol with several channels is considered as a couple of DFSMs each of which controls a channel and competes with the others for common inputs. For this model, the existing methods have a problem that the derived test suite is proportional to the product of the numbers of states of DFSMs. In this paper, we propose an effective method of conformance testing for a subclass of protocols modeled as those couples of DFSMs. In our method, we find a state cover set for each DFSM, which is used to test the DFSM alone in W-method, and derive a state cover set for the total system from those sets. The characterization set for the total system is the union of those for the DFSMs. Then, we construct constraints representing the relation among tuples of states that have correct responses against the characterization set. If these constraints have only one solution, we guarantee that an IUT modeled as a couple of DFSMs which has correct responses against the state cover and characterization set is equivalent to the given specification.

1 はじめに

ソフトウェア開発の過程において, 試験は重要な位置を占めている. 通信ソフトウェアの分野では, 通信プロトコルの適合性試験を行うための手法が研究され, TT 法 [5], W-法 [1], Wp-法 [2], DS 法 [3], UIO 法 [6] など, 適合性試験系列を機械的に生成する手法が開発されてきた. このような試験系列生成を行う研究の多くは単一の決定性有限状態機械 (DFSM) によってモデル化されるソフトウェアを対象としたものであり, 非決定的な動作を行うモデルや並行に協調して動作する並行モデルに対する研究は十分には行われていない. 近年, 複数のチャネルを持つ通信プロトコルが数多く用いられるようになってきており, そのような通信プロトコルでは, 一つのチャネルの制御部を一つの DFSM でモデル化し, システム全体は並行に動作しながら, 共通する入力を奪い合うことにより非決定的な動作を行う, 複数の DFSM 群としてモデル化することが自然である. このような並行モデルの試験を行う一つの方法は, 与えられた DFSM 群全体の動作を表す単一の非決定性有限状態機械 (NFSM) に対して, GWp-法 [4] など NFSM に対する試験手法を適用することである. しかし, 全体の動作を表す NFSM の状態数は与えられた DFSM 群の状態数の積に比例するので, 状態数が爆発しそれに伴い試験系列長も長くなるという問題が生じる.

本稿では, そのような並行に動作しながら共通する入力を奪い合う, 複数の DFSM 群としてモデル化されるような通信プロトコルのある部分クラスに対して, DFSM 群の状態数の和に比例する程度のコストで効率よく適合性試験を行えるようにするための一つの手法を提案する.

提案する手法では, まず, W-法によって部分仕様である各 DFSM を単独に試験を行う場合に用いる先行系列の集合からシステム全体の試験を行うための先行系列の集合を生成する. また, 各 DFSM に対する特性集合の和集合をシステム全体の試験を行うための特性集合として用いる. 一般にここで考えているモデルでは, DFSM 間で一つの入力を奪い合うため, ある DFSM に対する一つの特性系列を与えても, その系列の一部を他の DFSM が奪って同じような反応を返してしまう可能性がある. そこで, 与えられた各特性系列に対して正しく反応を返す可能性のある状態対をすべて列挙し, その関係を表す制約式を生成する. 一般に一つの特性系列に対する反応から状態対を特定することは出来なくても, 複数の特性系列に対する反応から状態を特定できる場合が多い. そこで, 提案する手法では, この制約式を満たす解 (状態の組) が仕様として与えられた DFSM 群の状態対のみであることを示せる場合には, 与えられた先行系列の集合と特性集合に対して正しい反応を示す実装 (IUT) は (IUT がもとの DFSM 群と同じ状態数の DFSM 群で構成されているという仮定の下で) もとの DFSM 群と等価であることを保証する. なお, 提案する手法は, 本質的に区別不可能であるような状態対が与えられた DFSM 群に含まれていないことなど, DFSM 群に対して若干の制約 (上述の制約式を満たす解が一意であること) を課してクラスを制限しているが, かなりのクラスの通信プロトコルに対して適用可能である.

以下, 2章で本稿で取り扱うモデル, Coupled DFSMs を定義し, 関連する概念について説明を行う. 3章では, 従来提案されている手法を Coupled DFSMs に対して適用する場合の問題点とその問題点を回避する場合に新たに問題となる点について述べる. 4章では, 提案する試験手法の概要について説明し, 5章で試験系列生成のアルゴリズムについて説明する. 最後にまとめを6章で述べる.

2 Coupled DFSMs

2.1 準備

有限状態機械 (FSM) は, 形式的には

$$A = (S, X, Y, \delta, \lambda, s_0)$$

として定義される. S, X, Yは, それぞれ, A の状態, 入力, 出力の集合である. また, δは $S \times X \rightarrow S$で定義される遷移関数の集合であり, λは $S \times X \rightarrow Y$で定義される出力関数の集合である. s_0は A の初期状態である.

FSM が最小であるとは, その機械の相異なる二つの状態が等価でないことである. FSM が完全であるとは, 任意の状態について, 任意の入力に対する遷移関数, 出力関数が共に定義されているものをいう. 本稿では, 与えられた FSM が完全でない場合, 遷移関数, 出力関数が定義されていない状態 s と入力 x に対し, 何も出力しないことを表す特殊な出力記号 (ε) を出力し, s 自身に遷移するような遷移を付け加えて完全な FSM とみなす. 以下, このようなε遷移が存在する場合, 状態 s は入力 x を無視するという. また, FSM が初期状態から連結であるとは, その機械の任意の状態に対して, 初期状態からその状態への遷移系列が存在することである. ただし, 遷移系列には空系列 (ϵ) も含まれる. 一方, FSM が強連結であるとは, その機械のすべての状態に対して, 任意の状態からの遷移系列が存在することである.

FSM が決定的な動作を行うとは, 任意の状態, 任意の入力に対し, 一意の出力と遷移先の状態が定まることである. 決定的な動作を行う FSM を決定性 FSM(DFSM) といい, DFSM でないものを非決定性 FSM(NFSM) という. 非決定的な動作の中で, 出力の内容から一意に遷移先が定まる非決定的動作を観測可能な非決定的動作と呼び, 観測可能でない非決定的動作を含まない非決定性 FSM を観測可能な非決定性 FSM(ONFSM) という.

2.2 Coupled DFSMs

環境から与えられる入力を奪い合いながら並行に動作する, 決定的な動作を行う複数のコンポーネントによって構成されているとみなせる通信プロトコルは, 各コンポーネントをモデル化した DFSM の組 (以降, Coupled DFSMs と呼ぶ) として表されるものとする. このとき, 各コンポーネント自身は決定的な動作を行うが, プロトコル全体はコンポーネントが環境からの入力を奪い合うことによって非決定的な動

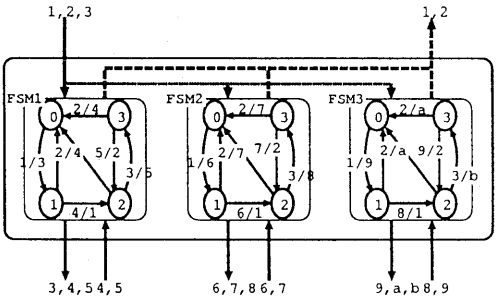

図 1: Multi-Link Protocol

表 1: 入力, 出力, 状態の意味

入力	意味	出力	意味
1	リンク増加要求	1	接続確立
2	リンク削減要求	2	データ受信確認
3	データ送信要求	3, 6, 9	接続指示
4, 6, 8	接続確立確認	4, 7, a	切断指示
5, 7, 9	データ受信確認	5, 8, b	データ送信指示

状態	意味
0	接続要求待ち
1	接続中
2	データ送信待ち
3	データ送信中

作を行う. ただし, ここでは入力に対して非決定的な動作を行うが, どのコンポーネントが遷移を行ったのかは対応する出力によって観測できるような仕様, すなわち, 仕様が ONFSM とみなせるクラスを対象とする.

図 1は, 動的に下位層とのリンクの数を変化させることができるプロトコル仕様である. このプロトコルでは上位層からの指示によって下位層と最大三個までのリンクを構成することができる. 単一のリンクに対応するプロトコルが一つの DFSM としてモデル化されている. 上位層からこのプロトコルに対してリンク増加要求が与えられると, 未だ下位層とリンクを持っていない DFSM の中の一つがリンクを構成する. 逆に, 上位層からリンク削減要求が与えられると, 下位層とリンクを持っている DFSM の中の一つがリンクを切断する. このようなリンクの数を増減させる要求は, 動作可能な DFSM が要求を奪い合うと考えることができる.

Coupled DFSMs として与えられるプロトコルの仕様 A は, 形式的には, k 個の DFSM の組,

$$A = (A_0, A_1, \ldots A_{k-1})$$

として与えられる. ここで, $A_0, A_1, \ldots, A_{k-1}$がそれぞれ, DFSM であり, A の部分仕様と呼ぶ.

部分仕様は, 形式的には,

$$A_i = (S_i, X_i, Y_i, \delta_i, \lambda_i, s_{i0})$$

として定義される, 完全, 初期状態から連結, 最小の DFSM である.

二つの部分仕様 A_iと A_jは入力アルファベット集合 X_i, X_jに重なりを持つことができる. $x \in X_i \cap X_j$ である入力 x が環境から与えられると, A_iと A_jの一方が非決定的に選ばれ, 状態遷移を行う. このような入力を共通する入力と呼ぶ. 共通する入力が与えられた場合は, A_iと A_jは異なる出力を行わなければならない. ただし,A_iでは入力 x を無視せず, A_jでは入力 x を無視する場合, 必ず A_iが入力 x を獲得し, 対応する状態遷移を行うものと定める.

2.3 Fault Model

本稿では, プロトコルの実装I も k 個の DFSM の組,

$$I = (I_0, I_1, \ldots, I_{k-1})$$

として与えられるものとする. I_jは部分仕様 A_jに対応する部分実装であり, A_jと同じ入出力アルファベットの集合 X_j, Y_jを持ち, 完全, 初期状態から連結, 最小の DFSM $I_j = (T_j, X_j, Y_j, \Delta_j, \Lambda_j, t_{j_0})$ であると仮定する. また, I_jは高々A_jの状態数 n_j 個以下の状態で実現されているものとする.

仕様 S, 実装 Iがともに Coupled DFSMs であるとし, 任意の I_jが S_jに対して誤りを持たないとき, Iと Sは等価であるという. Iと Sが等価でないならば, I は次に示すような誤りを持っている.

- 出力誤り : DFSM のある状態において, ある入力に対して定義された出力が誤っているもの.
- 遷移誤り : DFSM のある状態において, ある入力に対して定義された遷移先の状態が誤っているもの. ただし, 遷移先の状態はその DFSM のある状態に限られる.
- 複合誤り : 出力誤りと遷移誤りが同時に起こるもの

ただし, I には上述の誤りが複数個存在しても良いとする.

以下では, このような Fault Model に対し, I が A と等価でない時に, その誤りを発見できるような試験法を考える.

3 問題点

従来, Coupled DFSMs として与えられる仕様 A から効率よく試験系列を生成する手法は存在しなかった. 従来提案されている手法では, 例えば, 与えられた Coupled DFSMs 全体の動作を表す単一の ONFSM に対して GWp-法を用いて試験系列を生成する.

この方法では, 全体の動作を表す ONFSM の状態数が各 DFSM の状態数の積に比例するオーダーになるため, 生成された試験系列長も各 DFSM の状態数の積に比例する長さを持つことになる. したがって, 並行に動作する DFSM の数が増加するに従い, 試験を行うことが困難になるという問題が生じる.

本稿では, 各 DFSM が正しく実現されていることを独立に保証する方法を考える. この方法では, 各 DFSM に対して個々に試験を行う場合の試験系列を

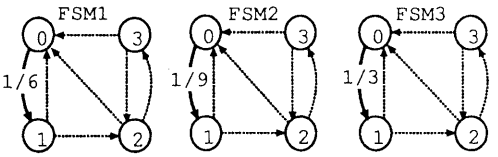

図 2: 図 1 の初期状態と同じ反応を示す例

求め, その試験系列に対して期待通りの反応が返ってきた場合に, そのDFSMが正しく実装されていると判断する. この方法を用いれば, 全体として試験系列長は各DFSMの状態数の和に比例する程度に抑えることができる.

しかし, この方法を用いる場合は, "他のDFSMが入力を奪う" ことから生じる問題を解決する必要がある.

まず, 正しく実現されたIに対して, あるDFSMに対する試験系列を与えた場合に期待通りの反応が返ってこないことが考えられる. これは, 他のDFSMが試験系列に含まれている共通する入力を奪ってしまうことによるものである. 例えば, あるDFSMで, 共通する入力を無視する定義されてる状態sが存在すると仮定する. このとき, 他のDFSMが同じ入力に対して何らかの出力を行う状態にあれば, sでの共通する入力を無視することは確認できない.

同様に, あるDFSMに対する試験系列を与えて期待通りの反応が返ってきた場合でも, IがAに対して正しく実現されていることを保証できない場合がある. 例えば, 図1の初期状態対を考えると, FSM1の初期状態は$\{1/3, 4/\varepsilon, 5/\varepsilon\}$という反応を示す状態として識別される. しかし, 入力1は共通する入力であるため, 1/3という入出力は*FSM1* (以下, *FSMi* はFSMiに対応する実装を表す) が行ったものではないかもしれない. 図2のように, 各DFSMの間で1に対する出力が入れ代わっているCoupled DFSMsの初期状態対は, $\{1/3, 4/\varepsilon, 5/\varepsilon\}$という反応を示す.

4 試験法

本章では, 本稿で提案する試験法について述べる. 本手法はW-法をもとにした試験法である. W-法で用いられる試験系列は, 先行系列の集合(V)と入力アルファベットの集合(X), 状態確認のための特性集合(W)を用いて, $VX^1W(=VW \cup VXW)$で表現される. ここで, VWは各DFSMの状態が存在することを確認する系列の集合になり, VXWは各DFSMの遷移が正しく実現されていることを確認する系列の集合になる.

従来のW-法をもとにしたDFSMに対する試験手法の多くは, 試験を行う実装(IUT)に対して入力系列σ_iを与え, 期待した系列σ_oを出力しない場合に, IUTは誤りを含んでいると判断した.

しかし, 一般に非決定的な動作を伴うモデルではσ_iを与えたときの出力系列は複数存在するため, σ_oとは異なる系列が出力される可能性が存在する. このため, 試験は複数回σ_iを与えることにより行う. その際, もし何回試験してもσ_o以外の出力系列しか出力しなければ,IUTに誤りが含まれていると判断できる. しかし, 何回かの試験の中でσ_oが出力された場合は, IUTに誤りが含まれているとは判断できない.

ただし, 本手法で扱うモデルにおいては, 入力系列σ_iに対して得られた出力系列を調べることによって, 現在の状態を判断できる. したがって, DFSMを目的の状態に遷移させるための先行系列vは, IUTに与える入力系列v_iとそれに対して期待される出力の系列v_oの組v_i/v_oであると考えることができる.

本手法では, IUTにv_iを与えた場合の反応がv_o以外の出力系列であった場合には, IUTが目的の状態に達していないと判断するのみで, IUTに誤りが含まれるかどうかの判断には利用しない. したがって, v_oと異なる出力を得た時点で, 初期状態からv_iを与え直す. v_iを十分な回数与えたとしても, v_oが観測されない場合には, IUTには誤りが存在し, v_i/v_oによって遷移する状態は存在しないと判断する.

一方, 入力$x \in X$や特性集合の系列$w \in W$に対しては, 先行系列によって遷移した先の状態対が正しく実現されている場合に出力するすべての出力系列を予め列挙しておく. したがって, 期待しない出力が得られた場合や十分な回数与えたあとも期待した出力が得られない場合にはIUTが誤っていると判断する.

5 試験系列選択アルゴリズム

本章では, 各DFSMの状態数の和に比例する長さを持つ試験系列を選択するアルゴリズムを説明する.

試験系列生成のアルゴリズムは次に示すとおりである.

1. 各DFSMの先行系列の集合, 特性集合生成

   DFSM A_iを単独で試験を行う場合の先行系列の集合V_iと特性集合W_iをそれぞれ計算する.

2. 先行系列生成

   DFSM A_iの状態sへの先行系列vを他のDFSMも状態sが動作したことを確認できる状態へ遷移させる系列を付加した先行系列v'に置き換える (複数の先行系列v',...,v''に置き換える場合もある).

3. 特性集合に対する制約式の確認

   仕様Aに対する特性集合WをW_iの和集合として考え, 2で生成した先行系列の集合Vによって遷移させたあと, Wを与えたときに示す反応に関する制約式を生成し, その制約式が唯一つの解を持つことを示す.

4. 遷移の確認のための試験系列追加

   共通する入力を無視することを確認するための試験系列を追加する.

以降, 図1に示されるCoupled DFSMsを用いて説明を行っていく.

5.1 各DFSMに対する先行系列, 特性集合の生成

各DFSM A_iをW-法によって単独に試験を行う場合に用いられる先行系列の集合V_iと特性集合W_iを

	V_i	W_i
FSM1	$\{\varepsilon, 1/3, 14/31, 143/315\}$	$\{1, 4, 5\}$
FSM2	$\{\varepsilon, 1/6, 16/61, 163/618\}$	$\{1, 6, 7\}$
FSM3	$\{\varepsilon, 1/9, 18/91, 183/91b\}$	$\{1, 8, 9\}$

表 2: 各 DFSM の先行系列, 特性集合

計算する. 例えば, 図1では, 表2に示す先行系列の集合と特性集合が計算される.

5.2 先行系列の生成

DFSM A_iのある状態 s が存在することを調べるために, W-法をもとにした手法では状態 s に遷移を行うような系列 vを与え, その後, 特性集合を与える.

Coupled DFSMs の場合には, 状態 s が存在することを調べる場合に, 他の DFSM が共通する入力を奪う可能性を考慮しなければならない. 例えば, 状態 s が共通する入力 x を無視する状態であった場合, 他の DFSM が x に対して zを出力するが状態は変化しないような遷移を持つ状態にある場合には, 状態 s に入力 x に対して zを出力するような誤りを持っていても期待する反応を示すため, 誤りを検出できない. また, 状態 s が入力 x に対して yを出力する状態であった場合には, 状態 s が zを出力し, 他の DFSM が yを出力するというような誤りを持っていても期待する反応を示す.

このような問題を回避するためには, 状態 s が存在することを調べるための先行系列を与える場合に他の DFSM も s が動作したことを観測できる状態に遷移させればよい. つまり, 状態 s が共通する入力 x を無視するならば, 他の DFSM も x を無視する状態に遷移させる. s が x を無視しないならば, 他の DFSM を x に対して相異なる出力を行うような二つの状態に遷移させる.

これは, 他の各 DFSM の各状態が x に対してどのような出力を行うかを調べ, 該当する状態への先行系列を vに連結した系列を先行系列として用いればよい. ここで扱うモデルにおいては, 共通する入力に対しても出力によって遷移を実行した機械が特定できるため, 各 DFSM の先行系列を連結する順序によって到達する状態が変化することはない. したがって, 生成する先行系列は, 機械的に $v_0 \cdots v_{i-1} \cdot v \cdot v_{i+1} \cdots v_{k-1}$ と連結することによって得ることができる (v_jは他の DFSM A_jを該当する状態へ遷移させる系列).

例えば, 図1の例において, FSM1 の状態 0 は共通する入力 1 に対して 3 を出力する状態である. したがって, 1 に対して相異なる出力を行う二つの状態に FSM2 と FSM3 を遷移させる. つまり, FSM1 の状態 0 への先行系列εは FSM2 と FSM3 をともに 1 に対して出力を行う状態 (状態 0) に遷移させる系列εと FSM2 と FSM3 をともに 1 を無視する状態 (状態 1) に遷移させる系列 11/69 の二つの先行系列に置き換える. また, FSM1 の状態 1 への先行系列 1/3 は, 状態 1 が 1 を無視する状態であるから, FSM2 と FSM3 も 1 を無視する状態へ遷移させる. つまり, FSM1 の状態 1 への先行系列は系列 11/69 を付加し, 系列 111/369 に置き換える.

状態変数	反応	状態変数	反応
A1	$\{1/3, 4/\varepsilon, 5/\varepsilon\}$	A2	$\{1/6, 4/\varepsilon, 5/\varepsilon\}$
A3	$\{1/9, 4/\varepsilon, 5/\varepsilon\}$	A4	$\{1/\varepsilon, 4/\varepsilon, 5/\varepsilon\}$
B1	$\{1/3, 6/\varepsilon, 7/\varepsilon\}$	B2	$\{1/6, 6/\varepsilon, 7/\varepsilon\}$
B3	$\{1/9, 6/\varepsilon, 7/\varepsilon\}$	B4	$\{1/\varepsilon, 6/1, 7/\varepsilon\}$
B5	$\{1/3, 6/1, 7/\varepsilon\}$	C1	$\{1/3, 8/\varepsilon, 9/\varepsilon\}$
C2	$\{1/6, 8/\varepsilon, 9/\varepsilon\}$	C3	$\{1/9, 8/\varepsilon, 9/\varepsilon\}$
C4	$\{1/\varepsilon, 8/1, 9/\varepsilon\}$	C5	$\{1/3, 8/1, 9/\varepsilon\}$

表 3: 状態変数

同様の操作をすべての FSM のすべての状態に対して行うと,

$$\begin{aligned} V = \{&\varepsilon, 11/69, 11/39, 11/36, 111/369, \\ &1411/3169, 1161/3619, 1118/3691, \\ &14311/31569, 11631/36189, 11183/3691b\} \end{aligned}$$

という先行系列が得られる.

5.3 特性集合に対する制約式の確認

前節で生成した先行系列の集合 Vと各 DFSM に対する特性集合 W_iの和集合 Wに対して IUT が期待する反応を示したとしても, 各 DFSM が期待する反応を示す状態のみから構成されていることが保証されるわけではない. ある遷移系列によって遷移した状態対に対して, A_iの状態を調べるために, 特性集合 W_i に含まれる系列$\alpha s \beta$ (α, βは入力系列, s は共通する入力) を与えたときに, 期待する出力$\gamma t \delta$が得られたとする. しかし, 入力 s に対する出力は A_i以外の DFSM が行ったものであるかもしれないからである.

例えば, 図1の初期状態対に対して, Wに対して期待する反応を示す可能性のある状態対を列挙すると,

$$\begin{aligned} &(\{1/3, 4/\varepsilon, 5/\varepsilon\}, \{1/6, 6/\varepsilon, 7/\varepsilon\}, \{1/9, 8/\varepsilon, 9/\varepsilon\}) \quad , \\ &(\{1/3, 4/\varepsilon, 5/\varepsilon\}, \{1/9, 6/\varepsilon, 7/\varepsilon\}, \{1/6, 8/\varepsilon, 9/\varepsilon\}) \quad , \\ &(\{1/6, 4/\varepsilon, 5/\varepsilon\}, \{1/3, 6/\varepsilon, 7/\varepsilon\}, \{1/9, 8/\varepsilon, 9/\varepsilon\}) \quad , \\ &(\{1/6, 4/\varepsilon, 5/\varepsilon\}, \{1/9, 6/\varepsilon, 7/\varepsilon\}, \{1/3, 8/\varepsilon, 9/\varepsilon\}) \quad , \\ &(\{1/9, 4/\varepsilon, 5/\varepsilon\}, \{1/6, 6/\varepsilon, 7/\varepsilon\}, \{1/3, 8/\varepsilon, 9/\varepsilon\}) \quad , \\ &(\{1/9, 4/\varepsilon, 5/\varepsilon\}, \{1/3, 6/\varepsilon, 7/\varepsilon\}, \{1/6, 8/\varepsilon, 9/\varepsilon\}) \end{aligned}$$

の 6 通りの状態対が考えられる.

ここで, ある反応を示す状態が存在するときに真となり, 存在しないときに偽となる論理変数を考える (表 3) と, 初期状態対に対しては, 論理式,

$$\begin{aligned} &(A1 \wedge B2 \wedge C3) \vee (A1 \wedge B3 \wedge C2) \\ \vee \quad &(A2 \wedge B1 \wedge C3) \vee (A2 \wedge B3 \wedge C1) \\ \vee \quad &(A3 \wedge B1 \wedge C2) \vee (A3 \wedge B2 \wedge C1) \end{aligned}$$

が真となる.

また, 図1で, 11/69 によって遷移する状態対を考える. この状態対は, FSM1 が状態 0, FSM2, FSM3 が状態 1 であり, 特性集合に対して, それぞれ, $\{1/3, 4/\varepsilon, 5/\varepsilon\}$, $\{1/\varepsilon, 6/1, 7/\varepsilon\}$, $\{1/\varepsilon, 8/1, 9/\varepsilon\}$ という反応を示す状態であるはずである. このとき, *FSM2* や *FSM3* は

1/3 という遷移を持つ状態にあるかもしれない. また, *FSM1* は 1/3 という遷移を持たない状態にあるかもしれない. 後者の場合には, *FSM2*, あるいは *FSM3* がある状態に 1/3 という遷移が存在する必要があり, *FSM1* は 1 では動作しない状態になければならない. したがって, この状態対に対しては, 論理式,

$$\begin{aligned} & (A1 \wedge (B4 \vee B5) \wedge (C4 \vee C5)) \\ \vee \quad & (A4 \wedge B4 \wedge C5) \vee (A4 \wedge B5 \wedge C4) \\ \vee \quad & (A4 \wedge B5 \wedge C5) \end{aligned}$$

が真となる.

このような制約式を V のすべての遷移系列によって遷移する状態対に対して特性集合を与えた場合の反応に対して求める. これらは各 DFSM に存在する状態の可能性に関する制約式と考えることができる.

また, 部分仕様 A_i に対応する部分実装 I_i の状態数は, A_i の状態数 n_i を越えないという仮定から, 各 DFSM の状態数に関する制約式を考える. このために, DFSM I_i の状態数が n_i 以下であるときに, 真となる述語, $AtMost(I_i, n_i)$ を導入する. 図 1の例に対しては $AtMost(\text{FSM1}, 4) \wedge AtMost(\text{FSM2}, 4) \wedge AtMost(\text{FSM3}, 4)$ が成り立つ.

これらの制約式を満たす解は V と W に対して, 期待通りの反応を返す状態の集合である. つまり, そのような状態から構成された DFSM 群は VW に対して期待する反応を示す. 各 I_i が A_i と等価なら, 各 I_i の状態の集合は必ずこれらの制約式を満足する. したがって, 制約式がそのような解のみを持つことを示すことができれば, VW によって, 各 I_i に対して A_i と同じ反応をする状態が存在することを確認できる.

5.4 遷移の確認のための試験系列追加

VW に対して生成した制約式が唯一つの解を持つことを示すことによって, VW に対して期待する反応を返す IUT には W_i に対して期待する反応を返す状態が存在することが確かめられた.

次に, DFSMs の各状態におけるすべての遷移が正しく実現されていることを確認しなければならない. W-法では, $vx(v \in V, x \in X)$ を与えて遷移させた状態が W に対して期待通りの反応を示すことによって遷移が正しく実現されていることを確認する.

しかし, Coupled DFSMs において, ある DFSM の状態 s が共通する入力 x を無視することを示したい場合には不十分であるかもしれない. 例えば, 他の DFSM が x に対して z を出力し, 状態は変化しないような遷移を持つ状態にある場合, 状態 s が x に対して z を出力し, s に遷移するような誤りを実装していたとしても, W に対して期待通りの反応を示すため, s が x を無視することは保証できない.

例えば, 図 3の状態 T が共通する入力 1 に対して動作しないことを示したいとする. このとき, DFSM A が状態 S にあるならば, T に 1/3 という入出力で T に戻ってくる誤りは発見できない.

この問題を避けるためには, 他の DFSM も x を無視する状態に遷移させ, x を無視することを調べればよい.

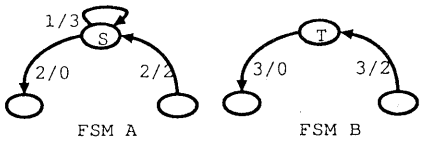

図 3: 誤りを発見できない状態対

また, DFSM A_j はすべての状態で x に対してなんらかの出力を行うと定義されているかもしれない. この場合には, 他の DFSM を x に対して相異なる出力 y_m, y_n を行うような二つの状態に遷移させ, 状態 s の存在を二度調べればよい.

例えば, 誤りを含む実装 I_i が状態 s で x に対して y_m を出力すると実装されていると仮定する. この場合, 相手の DFSM を y_n を出力する状態に遷移させ入力 x を与えると, y_n だけでなく y_m も観測されることになる. したがって, 誤りを持つことが示される. y_n を出力すると実装されている場合にも同様に誤りを持つことが示される.

以上のような系列を新たに先行系列として加えると, VX^1W は状態遷移の存在とその遷移先の状態確認を行う試験系列になる.

6 まとめ

本論文では, Coupled DFSMs として与えられる通信プロトコルに対して効率の良い適合性試験を行う手法を与えた. 現在, DFSM が互いに同期を行いながら並行に動作するようなモデルに対して本手法を拡張することを検討中である.

参考文献

[1] T. S. Chow, "Testing design modeled by finite-state machines," IEEE Trans. Software Eng. vol.4, pp.178–186, Mar. 1978

[2] S. Fujiwara, G. v. Bochmann, F. Khendek, M. Amalou, and A. Ghedamsi, "Test Selection Based on Finite State Models," IEEE Trans. Software Eng. vol.17, pp.591–603, June 1991

[3] G. Gonenc, "A method for the design of fault-detection experiments," IEEE Trans. Comput., vol. C-19, pp. 551–558, June 1970

[4] G. Luo, G. v. Bochmann, and A. Petrenko, "Test Selection Based on Communicating Nondeterministic Finite State Machines Using a Generalized Wp-Method", IEEE Trans. Software Eng. vol.20, pp.149–162, Feb. 1994

[5] S. Naito and M. Tsunoyama, "Fault detection for sequential machines by transition-tours," Proc. FTCS (Fault Tolerant Comput. Syst.), 1981, pp.238–243

[6] K. K. Sabnani and A. T. Dahbura, "A protocol testing procedure," Comput.Networks and ISDN Syst. Vol. 15, no.4, pp.285–297, 1988