遷移の選択が状態訪問回数で決まる有限状態機械対からなる通信系に対する生存性の検証

水野 健太郎[†] 中田 明夫[††] 岡野 浩三[†]
東野 輝夫[†] 谷口 健一[†]

本論文では，各状態からの遷移条件がその状態の訪問回数で決まる有限状態機械モデルの上で生存性の検証を機械的に行う1つの方法を提案する．通信プロトコルは有限状態機械（FSM）によってモデル化され検証される場合が多いが，一般にシーケンス番号などのパラメータ値の変化を直接状態で区別して表そうとするとFSMの状態数が多くなり，状態爆発が起こる．我々は各遷移の実行可能性がその遷移の開始状態の訪問回数で決まるような有限状態機械モデルFSM/Cを提案し，このFSM/Cモデルの上で整数線形計画法を用いることにより状態爆発を回避した生存性の検証法を提案する．FSM/Cモデルでいくつかの通信プロトコルの仕様を記述できる．また，この手法に基づき，FSM/Cからなる通信系の生存性を検証するシステムを作成した結果についても報告する．

Verification of Liveness Property for C-FSM's with Transitions depending on State Visiting Numbers

KENTARO MIZUNO,[†] AKIO NAKATA,[††] KOZO OKANO,[†]
TERUO HIGASHINO[†] and KENICHI TANIGUCHI[†]

Many communication protocols are modeled as finite state machines (FSM's). In general, since the size of states becomes large in order to treat parameter values such as sequence numbers, the state explosion problem may occur. In this paper, we will propose an *FSM/C model* where the execution of each transition may depend on the number that its starting state has been visited, and propose a technique for verifying a liveness property. In this model, a counter C_{s_i} holds the number that state s_i has been visited. Many communication protocols can be modeled in our FSM/C model. If two communicating FSM/C's eventually return to the pair of their initial states and the communication channels become empty, then we say that they have the liveness property. For verifying the liveness property, we use an integer linear programming technique so that the state explosion problem does not occur.

1. まえがき

多くの通信プロトコルは有限状態機械（FSM）や拡張有限状態機械（EFSM）によってモデル化される．EFSMモデルではシーケンス番号などのパラメータ値を扱う仕様を簡潔に表現できるが，一般に検証の機械化は困難である．一方，FSMモデルでは「安全性」や「生存性」などの機械的な検証法が数多く提案されている．EFSMが保持するレジスタ（変数）値が有界なら，それらの値を有限状態で区別することにより等価なFSMに変換できるが，多くの場合，変換後のFSMの状態数が多くなり状態爆発が起こる．このため，状態爆発を回避するためのさまざまな方法が研究されている．たとえば，文献5)~8)では，いくつかの状態をひとまとめに扱うことにより検証時の検索領域を減らす工夫を行っている．また，プロトコル機械間のメッセージの送受信関係などを整数線形不等式などで表し，整数線形計画法の手法を用いて直接安全性や生存性などの性質の検証を行う研究も提案されている[2)~4)]．しかし，いずれの手法もEFSM仕様から直接検証を行うわけではなく，いったんFSMに変換してEFSM仕様の検証を行うため，取り扱うパラメータ値に検証時間が大きく依存し，その値が大きくなると検証が困難になる，などの問題点がある．

† 大阪大学基礎工学部情報科学科
Department of Information and Computer Sciences, School of Engineering Science, Osaka University
†† 広島市立大学情報科学部情報数理学科
Department of Computer Science, Faculty of Information Sciences, Hiroshima City University

本論文では，各状態からの遷移条件がその状態の訪問回数で決まる拡張有限状態機械モデルFSM/Cを提案し，そのモデル上でパラメータ値に検証時間が依存しない「生存性」の検証法を提案する．

このモデルの各状態 s_i は，その状態の訪問回数を表すカウンタ C_{s_i} を持つ．FSM/Cの遷移には，無条件に実行可能な遷移と条件付き遷移とがある．状態 s_i からの条件付き遷移は，カウンタ C_{s_i} の値（もしくは C_{s_i} の値をある整数 m_{s_i} で割った剰余 Cr_{s_i}）がある整数 k_{s_i} 未満のときのみ実行可能な遷移と k_{s_i} 以上のときのみ実行可能な遷移の2つからなり，いずれか一方の遷移が決定的に選ばれる．k_{s_i} や m_{s_i} を用いることにより，FSM/Cモデルで，シーケンス番号などのパラメータ値を扱った通信プロトコルのいくつかを簡潔に記述できる．

以下，2つのFSM/Cが双方向の通信路で結ばれ，各通信路がFIFOキューとしてモデル化できるような通信系を考え，そのモデル上での生存性を「各通信路が空で，かつ2つのFSM/Cがそれぞれの初期状態から遷移を開始したとき，いつかはもとの初期状態対に戻り，かつそのときの各通信路が空となるような性質」と定義する．

提案している検証手法では，FSM/C対からなる通信系の各遷移の実行回数とカウンタ C_{s_i} の値との関係（遷移の接続関係や実行回数などに関する条件，ならびに，各符号の受信回数が送信回数を上回らないことなどFSM/C間の通信路の制約に関する条件）などを整数線形不等式（制約式）の集合 ψ で表す．これらの制約式に対して，遷移系列の長さを表す目的関数の最大値が有限である（ライブロックがない）ことや，デッドロックに陥る遷移系列が必ず満たすような制約式 ξ（各FSM/Cが受信しかできない状態にあり，かつ通信路が空，あるいは通信路の先頭の符号を受信できない状況にあることを表す式）と上述の ψ をともに満足するような解が存在しないこと，などを整数線形計画法を用いて機械的に証明することにより，生存性の検証を行う．なお，ξ や ψ などの制約式は任意の遷移系列が必ず満足する性質（十分条件）を不等式の形で記述したものである．このため，たとえ ξ と ψ をともに満足するような解が存在して生存性の検証に失敗してもデッドロックに陥る遷移系列が存在しない場合もある．その意味で提案する手法は生存性の1つの十分条件を機械的に証明していることに相当する．このように提案する手法は生存性の十分条件の検証法であるが，2章で示すような典型的な相互通信プロトコルの検証に利用することが可能である．また，カウンタ C_{s_i} の値を有限状態で区別して従来の可達解析を用いて上記の生存性の検証を行った場合，検証時間は各遷移の遷移条件に含まれる k_{s_i} や m_{s_i} などのパラメータ値に大きく依存するが，本手法の検証時間はその値に依存せず，短時間で行える．なお，ここで議論する「生存性」は，文献8)で議論されている「安定性（Stabilizing Property）」と関連深い．文献8)では，特定の状態対を安定な状態対とし，有限回数の遷移の実行により必ず安定な状態対に戻ることを証明する．本論文では初期状態対と空チャネルの組を安定な状態対と考えている．また，3章で与える「生存性」の十分条件と類似の十分条件は文献3)などで用いられている．

以下，2章で本論文で対象とするモデルFSM/Cと，FSM/C対からなる通信系に対する生存性を形式的に定義する．3章では，提案する生存性の検証手法について述べる．4章では，本論文の手法に基づいて作成した生存性検証システムと，そのシステムを用いた検証実験の結果について述べる．5章で提案する手法の限界などについて議論する．

2. FSM/Cモデルと生存性

2.1 FSM/Cモデル

［定義2.1（FSM/Cモデル）］FSM/Cモデルを5字組 $\langle \mathrm{S,A,C},\delta,s_0\rangle$ で定義する．

S： 状態の集合 $\{s_0,\cdots,s_n\}$

A： 遷移の集合 $\{a_1,\cdots,a_m\}$
各動作は送受信動作と送受信に無関係な動作（ローカル動作）に分かれる．動作 a_h が符号 a の送信（受信）動作なら $a_h^-(a_h^+)$ と記述する．

C： カウンタの集合 $\{C_{s_0},\cdots,C_{s_n}\}$
カウンタ C_{s_i} は，FSM/Cが状態 s_i を訪れた回数を保持する．カウンタ C_{s_i} の値は初期値が0で，各状態に入るごとに1増える．FSM/Cが初期状態に戻ったときにはすべてのカウンタの値が0にリセットされるものとする．

δ： $\mathrm{S}\times\mathrm{A}\rightarrow\mathrm{S}$：状態遷移関数
各遷移は $s_i \overset{\langle cond,a_h\rangle}{\longrightarrow} s_j$ のように記述する．
条件 $cond$ は true，$(C_{s_i} < k_{s_i})$，$(C_{s_i} \geq k_{s_i})$，$(C_{s_i} \bmod m_{s_i} < k_{s_i})$，$(C_{s_i} \bmod m_{s_i} \geq k_{s_i})$ のいずれかである．$cond$ がtrueの場合は，状態 s_i で動作 a_h がつねに実行可能で，FSMは動作 a_h を実行した後，状態 s_j に移る．$cond$ が $(C_{s_i} < k_{s_i})$，$(C_{s_i} \geq k_{s_i})$，$(C_{s_i} \bmod m_{s_i} < k_{s_i})$，$(C_{s_i} \bmod m_{s_i} \geq k_{s_i})$ の場合は，その条件が成り立つときのみ動作 a_h が実行可能となる．

s_0 : 初期状態

本論文では，条件 $(C_{s_i} \geq k_{s_i})$ および $(C_{s_i} \bmod m_{s_i} \geq k_{s_i})$ を上界制約，$(C_{s_i} < k_{s_i})$ および $(C_{s_i} \bmod m_{s_i} < k_{s_i})$ を下界制約と呼ぶ．これらをあわせて，遷移条件と呼ぶことにする．また，そのような制約条件が付随している遷移を条件付き遷移と呼ぶ．

本論文で対象とする通信FSM/Cは，2つのFSM/Cが信頼できる容量無限のFIFOキューで相互接続されたものとする．

2.2 FSM/Cに対する制約

ここで議論を簡単にするために，単体のFSM/Cに対して次の4つの制約を与える．

(A1) 任意の状態 s_i について，もし状態 s_i から始まる条件付き遷移があるなら，その状態 s_i は2本の条件付き遷移のみを持ち，かつそれぞれの遷移条件は $(C_{s_i} < k_{s_i})$ と $(C_{s_i} \geq k_{s_i})$，もしくは，$(C_{s_i} \bmod m_{s_i} < k_{s_i})$ と $(C_{s_i} \bmod m_{s_i} \geq k_{s_i})$ である．

(A2) 初期状態は自己ループや条件付き遷移を持たない．

(A3) 強連結である．

(A4) $s_i \xrightarrow{\langle cond, a_h \rangle} s_j$，$s_i \xrightarrow{\langle cond', a'_h \rangle} s_{j'}$ なる遷移があれば，$a_h \neq a'_h$ である（この条件によりFSM/Cは決定的に遷移する）．

また，通信FSM/C $\langle S, T \rangle$ について，以下の制約を与える．

(A5) T の初期状態からは，受信以外の遷移が不可能であるとする．すなわち，S および T が初期状態対から遷移を開始するとき，先に S が遷移を開始し，T は S が送信した符号を受信することにより初めて遷移を開始する．

2.3 通信FSM/Cの例

通信FSM/C $\langle S, T \rangle$ の例を**図1**に示す．この例はトランスポート層などにおける一般的なシーケンスを抽象化したものである．S と T は初期状態 s_0，t_0 から遷移を開始する．S は符号 a を送り，T から b を受け取ってコネクションを確立する．データの送受信を行う部分では，c を8回送ったあと d を送り，T から符号が送られてくるのを待つ．T は e を送るか，f を8回送ったあとに g を送り，S から符号が送られてくるのを待つ．このようなデータのやりとりを4回行ったあと，S がコネクション開放のための符号 h を送り，T から k を受け取って初期状態対に戻る．

この例は，通常のプロトコル機械において頻繁に見られる以下の特徴を持つ．

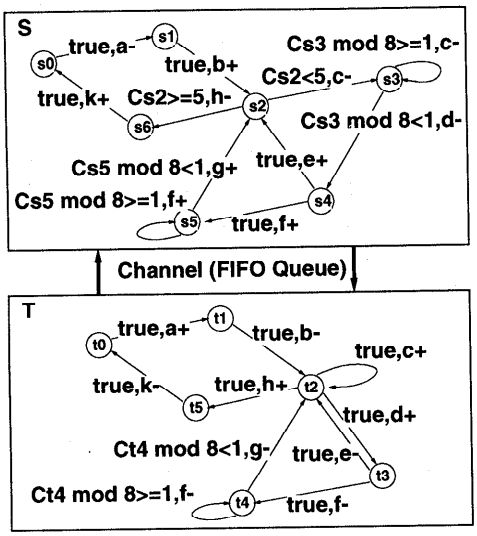


図1 FSM/C仕様 S（上段），T（下段）
Fig. 1 Example FSM/C specifications S and T.

- ハンドシェイクでのコネクションの確立および解放
- 状態訪問に一定の順序関係や局所性がある
- 機械が多重ループを持つ
- 双方の機械でループ構造が異なる
- ループ回数などの制御を片方の機械が一方的に行う場合がある☆

仕様 S および T は，前述の制約(A1)～(A5)を満たしている．

2.4 生存性の定義

本論文で対象とする通信FSM/C上での生存性は，「通信路が空で各FSM/Cがそれぞれ初期状態から遷移を始めたとき，どのように遷移を行ってもいつかはもとの初期状態対に戻り，かつ通信路も空の状態に戻っているような性質」と定義する．

3. 生存性の検証法

以下では次のような十分条件が成り立つことを示すことにより，生存性の検証を行う．

［生存性の検証］S および T からなる通信FSM/Cが以下の条件をすべて満たせば，生存性が成り立つ．

(B1) デッドロック（S, T ともにどの遷移も実行できないこと）がない

(B2) S が初期状態に戻らずに，S, T が無限の動作を実行することはない

(B3) S が初めて初期状態に戻ったとき，T も初期状態に戻っている

☆ T では受信動作 c, d の実行回数の制御は行っていない．

(B4) S, T が初期状態対に戻ってきたときには，つねに両チャネルが空である

上記 4 条件の証明は，与えられた通信 FSM/C が必ず満たすような制約式を以降で述べるような整数線形不等式からなる論理式で表し，それらの充足不能性や目的関数の最大値が有限であることなどを示すことにより行う．

3.1 制約式の生成

3.1.1 遷移の接続関係から得られる制約式

はじめに，FSM/C 仕様 $S(T)$ を独立に考えたときに，各遷移系列が満たす（$S(T)$ 上の任意の遷移系列について成り立つ）条件（制約式）について考える．いま S がある遷移系列を実行して状態 s_i に達したと考え，この状態を現到達状態とする．まず変数 $X_{s_is_ja_h}$ と F_{s_i} を導入する．変数 $X_{s_is_ja_h}$ は s_i から s_j への遷移 a_h を実行した回数を保持する（遷移そのものが存在しない場合は 0）．変数 F_{s_i} は，S の現到達状態が s_i のときに 1，それ以外のときに 0 になるような変数とする．以降，すべての変数は非負整数と仮定する．

本論文では，次のような制約式を考える．

(FS) 遷移の最終状態は 1 つであるから

$$\sum_{i=0}^{n} F_{s_i} = 1$$

(Si) s_i に入る遷移の実行回数の総和は s_i の訪問回数 C_{s_i} と等しい．一方，s_i から出る遷移の実行回数の総和は，s_i が現到達状態となるときのみ s_i の訪問回数 C_{s_i} より 1 少なくなるが，その他のときは C_{s_i} の値に等しくなる．よって

$$\sum_{j=0}^{n}\sum_{h=1}^{m} X_{s_js_ia_h} = C_{s_i} = \sum_{j=0}^{n}\sum_{h=1}^{m} X_{s_is_ja_h} + F_{s_i}$$

例外として，初期状態 s_0 については

$$\sum_{j=0}^{n}\sum_{h=1}^{m} X_{s_js_0a_h} = C_{s_0} = \sum_{j=0}^{n}\sum_{h=1}^{m} X_{s_0s_ja_h} + F_{s_0} - 1$$

(Si-cond) $s_i \xrightarrow{\langle (C_{s_i} < k_{s_i}), a_q\rangle} s_u$，$s_i \xrightarrow{\langle (C_{s_i} \geq k_{s_i}), a_p\rangle} s_v$ のように状態 s_i の訪問回数 C_{s_i} と k_{s_i} の大小により遷移が決まるような条件付き遷移を持つ状態 s_i については，C_{s_i} の値と 2 つの遷移の実行回数の関係から次のような制約式が成り立つ．

$$(C_{s_i} < k_{s_i}) \Rightarrow (X_{s_is_ua_q} = C_{s_i} - F_{s_i})$$
$$(C_{s_i} < k_{s_i}) \Rightarrow (X_{s_is_va_p} = 0)$$
$$(C_{s_i} \geq k_{s_i}) \Rightarrow (X_{s_is_ua_q} = k_{s_i} - 1)$$
$$(C_{s_i} \geq k_{s_i}) \Rightarrow (X_{s_is_va_p} = C_{s_i} - F_{s_i} - (k_{s_i} - 1))$$

(Si-cond') $s_i \xrightarrow{\langle (C_{s_i} \bmod m_{s_i} < k_{s_i}), a_q\rangle} s_u$，および $s_i \xrightarrow{\langle (C_{s_i} \bmod m_{s_i} \geq k_{s_i}), a_p\rangle} s_v$ なる遷移がある状態 s_i については，C_{s_i} を m_{s_i} で割った商 Cd_{s_i} と剰余 Cr_{s_i} の間に次のような制約式が成り立つ．

$$C_{s_i} = m_{s_i} \times Cd_{s_i} + Cr_{s_i}$$
$$m_{s_i} - 1 \geq Cr_{s_i} \geq 0$$

（C_{s_i} に対して Cd_{s_i} と Cr_{s_i} は一意に定まる）また，Si-cond と同様に，次のような制約式が成り立つ．

$$(Cr_{s_i} < k_{s_i}) \Rightarrow (X_{s_is_ua_q} = k_{s_i} \times Cd_{s_i} + Cr_{s_i} - F_{s_i})$$
$$(Cr_{s_i} < k_{s_i}) \Rightarrow (X_{s_is_va_p} = (m_{s_i} - k_{s_i}) \times Cd_{s_i})$$
$$(Cr_{s_i} \geq k_{s_i}) \Rightarrow (X_{s_is_ua_q} = k_{s_i} \times Cd_{s_i} + k_{s_i} - 1)$$
$$(Cr_{s_i} \geq k_{s_i}) \Rightarrow (X_{s_is_va_p} = (m_{s_i} - k_{s_i}) \times Cd_{s_i} + Cr_{s_i} - F_{s_i} - (k_{s_i} - 1))$$

以下，FSM/C 仕様 S に対する上述の制約式の集合（論理積）を $CE(S)$ で表すことにする．図 1 の FSM/C 仕様 S に対して，**図 2** で示すような制約式の集合 $CE(S)$ が得られる．$CE(S)$ では，$(C_{s_i} \bmod m_{s_i} < k_{s_i})$ の形の遷移条件は $(Cr_{s_i} < k_{s_i})$ の形の条件で表されている．以降，$(Cr_{s_i} < k_{s_i})$ の形の条件も遷移条件と呼ぶことにする．

3.1.2 可達解析情報から得られる制約式

一般に 1 つの FSM/C に複数の遷移条件付き遷移があったとしても，各状態で取りうる可能性のある遷移条件の組はかなり限定される．たとえば，図 1 の FSM/C 仕様 S では 3 つの遷移条件 $(C_{s_2} < 5)$, $(Cr_{s_3} < 1)$, $(Cr_{s_5} < 1)$（ならびにそれらの否定）がある．詳細は後で述べるが，S がどのような遷移系列を実行しても，状態 s_3 に到達したときの遷移条件 $(C_{s_2} < 5)$, $(Cr_{s_5} < 1)$ の値はつねに真であることが保証される．このため，図 2 の制約式 $CE(S)$ を考える場合も，現到達状態が s_3 の場合，$CE(S)$ の制約式のうち $(C_{s_2} < 5)$ と $(Cr_{s_5} < 1)$ がともに真の場合に成り立つ制約式のみを考えればよいことになり，以降の検証の際に考えるべき条件の組合せを減らすことができる．

一般にFSM/Cモデルでの厳密な可達解析は困難であるので，以下では次のような簡易な可達解析（十分条件）を用いて，各状態で可達でない遷移条件の組を見つけることにする．まず，単一FSM/Cの状態と遷移条件群の真偽のみに着目して**図3**のような可達解析木を構成する．この可達解析木の各節点は，現到達状態とその状態で成り立つ遷移条件群の組を要素として持つ．木の根ノードは初期状態と初期状態で成り立つ遷移条件群の組であり，各節点の状態から実行可能な遷移を実行したあとの状態と遷移条件群の組を子節点として付加する．任意の遷移系列を実行した際の状態と遷移条件の真偽の組はこの到達可能性木に書かれた状態と遷移条件の組のいずれかであり，この可達解析木に現れない状態と遷移条件の組には遷移しないことが保証できる．可達解析木の生成は以下のように行う．まず，選んだ遷移が条件付き遷移でないときは，現節点の状態名のみをその遷移を実行して遷移する状態名に置き換えた組を子節点とする．選んだ遷移が条件付き遷移の場合は，遷移条件の真理値が変化する場合（たとえば，$(C_{s_i} < k_{s_i})$ の値が真であるような状況から $(C_{s_i} \geq k_{s_i})$ の値が真であるような状況へ変化する場合）と変化しない場合の2通りに相当する子節点を作る（ただし，現在の節点ですでに $(C_{s_i} \geq k_{s_i})$ の値が真である場合は，$(C_{s_i} < k_{s_i})$ の値が真になるような子節点は作らない）．根ノードから順次子節点の生成を繰り返すが，すでに調べた状態と遷移条件群の組を生成した場合，あるいは，初期状態と遷移条件群の組に到達した場合は，その時点で子ノードの生成を打ち切る．一般に子節点の生成に際して，遷移条件の真理値が必ず変化するとは限らないので生成した可達解析木のすべての節点に相当する状態と遷移条件の組に到達するとは限らないが，上述のように生成した可達解析木に現れない状態と遷移条件の組には絶対に

(FS)	$F_{s_0} + F_{s_1} + F_{s_2} + F_{s_3} + F_{s_4} + F_{s_5} + F_{s_6} = 1$
(S0-1)	$X_{s_6 s_0 k} = C_{s_0} = X_{s_0 s_1 a} + F_{s_0} - 1$
(S1-1)	$X_{s_0 s_1 a} = C_{s_1} = X_{s_1 s_2 b} + F_{s_1}$
(S2-1)	$X_{s_1 s_2 b} + X_{s_4 s_2 c} + X_{s_5 s_2 g} = C_{s_2}$
(S2-2)	$C_{s_2} = X_{s_2 s_3 c} + X_{s_2 s_6 h} + F_{s_2}$
(S2-3)	$(Cs_2 < 5) \Rightarrow (X_{s_2 s_6 h} = 0)$
(S2-4)	$(Cs_2 < 5) \Rightarrow (X_{s_2 s_3 c} = C_{s_2} - F_{s_2})$
(S2-5)	$(Cs_2 \geq 5) \Rightarrow (X_{s_2 s_3 c} = 4)$
(S2-6)	$(Cs_2 \geq 5) \Rightarrow (X_{s_2 s_6 h} = C_{s_2} - F_{s_2} - 4)$
(S3-1)	$X_{s_2 s_3 c} + X_{s_3 s_3 c} = C_{s_3}$
(S3-2)	$C_{s_3} = X_{s_3 s_3 c} + X_{s_2 s_6 h} + F_{s_2}$
(S3-3)	$C_{s_3} = 8Cd_{s_3} + Cr_{s_3}$
(S3-4)	$7 \geq Cr_{s_3} \geq 0$
(S3-5)	$(Cr_{s_3} < 1) \Rightarrow (X_{s_3 s_3 c} = 7Cd_{s_3})$
(S3-6)	$(Cr_{s_3} < 1) \Rightarrow (X_{s_3 s_4 d} = Cd_{s_3} + Cr_{s_3} - F_{s_3})$
(S3-7)	$(Cr_{s_3} \geq 1) \Rightarrow (X_{s_3 s_4 d} = Cd_{s_3})$
(S3-8)	$(Cr_{s_3} \geq 1) \Rightarrow (X_{s_3 s_3 c} = 7Cd_{s_3} + Cr_{s_3} - F_{s_3})$
(S4-1)	$X_{s_3 s_4 d} = C_{s_4} = X_{s_4 s_5 f} + F_{s_4}$
(S5-1)	$X_{s_4 s_5 f} + X_{s_5 s_5 f} = C_{s_5}$
(S5-2)	$C_{s_5} = X_{s_5 s_5 f} + X_{s_5 s_2 g} + F_{s_5}$
(S5-3)	$C_{s_5} = 8Cd_{s_5} + Cr_{s_5}$
(S5-4)	$7 \geq Cr_{s_5} \geq 0$
(S5-5)	$(Cr_{s_5} < 1) \Rightarrow (X_{s_5 s_5 f} = 7Cd_{s_5})$
(S5-6)	$(Cr_{s_5} < 1) \Rightarrow (X_{s_5 s_2 g} = Cd_{s_5} + Cr_{s_5} - F_{s_5})$
(S5-7)	$(Cr_{s_5} \geq 1) \Rightarrow (X_{s_5 s_2 g} = Cd_{s_5})$
(S5-8)	$(Cr_{s_5} \geq 1) \Rightarrow (X_{s_5 s_5 f} = 7Cd_{s_5} + Cr_{s_5} - F_{s_5})$
(S6-1)	$X_{s_2 s_6 h} = C_{s_6}$
(S6-2)	$C_{s_6} = X_{s_6 s_0 k} + F_{s_6}$

図2 S の遷移関係から得られる制約式 $CE(S)$
Fig. 2 Constraints $CE(S)$ obtained from spec. S.

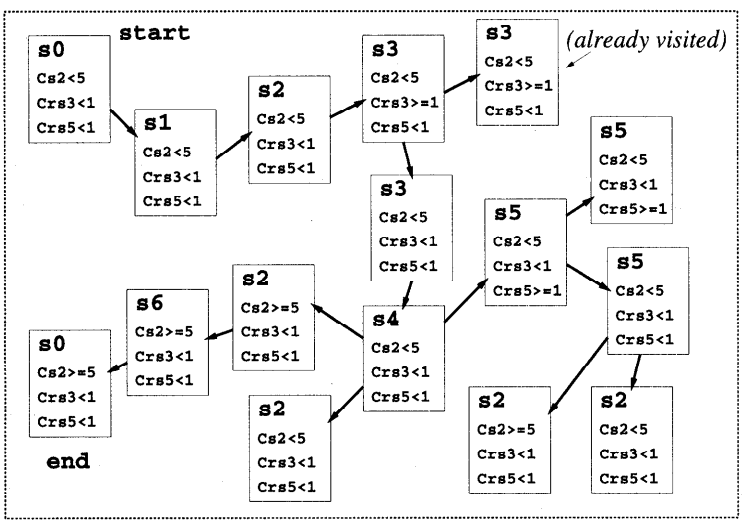


図3 S の可達解析木
Fig. 3 Reachability graph for spec. S.

reachability table of S

conditions			states						
Cs2	Crs3	Crs5	s0	s1	s2	s3	s4	s5	s6
<5	<1	<1	o	o	o	o	o	o	
>=5	<1	<1	o		o				o
<5	>=1	<1				o			
>=5	>=1	<1	(unreachable)						
<5	<1	>=1						o	
>=5	<1	>=1	(unreachable)						
<5	>=1	>=1	(unreachable)						
>=5	>=1	>=1	(unreachable)						

図4 S の可達解析結果
Fig. 4 Reachability table of spec. S.

(UN-1) $\mathrm{not}((C_{s_2} \geq 5) \wedge (Cr_{s_3} \geq 1) \wedge (Cr_{s_5} < 1))$
(UN-2~4) 他の3通りの到達不能な条件組の場合も(UN-1)と同様.
(RE-1) $((C_{s_2} < 5) \wedge (Cr_{s_3} < 1) \wedge (Cr_{s_5} < 1)) \Rightarrow (F_{s_0} + F_{s_1} + F_{s_2} + F_{s_3} + F_{s_4} + F_{s_5} = 1)$
(RE-2) $((C_{s_2} \geq 5) \wedge (Cr_{s_3} < 1) \wedge (Cr_{s_5} < 1)) \Rightarrow (F_{s_0} + F_{s_2} + F_{s_6}) = 1$
(RE-3,4) 他の2通りの条件組の場合も同様.

図5 S の可達解析から得られる制約式 $RA(S)$
Fig. 5 Constraints $RA(S)$ obtained from reachability table of spec. S.

到達しない．この性質を利用して，可達でない遷移条件の組を検出する．なお，この可達解析木のサイズはたかだか

$$O(\text{状態数} \times 2^P)$$

P = 条件付き遷移を持つ状態の数

で抑えられ，具体的なパラメータ値（遷移条件に書かれている k_{s_i} や m_{s_i} の値）には依存しない．

図3のような可達解析木の内容から，各遷移条件群に対して，その遷移条件群の値をすべて真にするような可能性のある状態を求めることができる．**図4**はその結果である．○印の状態では左側に列挙した遷移条件群の値がすべて真になる可能性があり，無印の状態では左側に列挙した遷移条件群の値がすべて真になることはない（unreachableの行はすべての状態で，左側に列挙した遷移条件群の値がすべて真になることはない，ことを表している）．

図4の可達解析結果から，**図5**のような制約式の集合（以下，$RA(S)$ と書く）が得られる．

3.1.3 送受信回数から得られる制約式

次に，符号の送信回数と受信回数が満たす制約式を考える．$S \rightarrow T$ 方向の通信チャネルを考えたとき，すべての送受信符号 a_h について，T が a_h を受信した回数は S が a_h を送信した回数を超えることはないので，任意の遷移系列について次の制約式が成り立つ（$T \rightarrow S$ 側についても同様）．

[$S \rightarrow T$ 側について]
(Ch1-a) $X_{s_0 s_1 a} - X_{t_0 t_1 a} \geq 0$
(Ch1-c) $X_{s_2 s_3 c} + X_{s_3 s_3 c} - X_{t_2 t_2 c} \geq 0$
(Ch1-d) $X_{s_2 s_6 h} - X_{t_2 t_5 h} \geq 0$
(Ch1-h) $X_{s_3 s_4 d} - X_{t_2 t_3 d} \geq 0$
[$T \rightarrow S$ 側について]（省略）

図6 S と T 間のチャネルに関する制約式 $CH_{\geq}(S,T)$
Fig. 6 Constrains $CH_{\geq}(S,T)$ for channels between S and T.

(CE-S) $CE(S)$
(CE-T) $CE(T)$
(RA-S) $RA(S)$
(RA-T) $RA(T)$
(CH-ST) $CH_{\geq}(S,T)$

図7 通信FSM/C $\langle S,T \rangle$ 全体の制約式 $Cons\_CFSM(S,T)$
Fig. 7 Constrains $Cons\_CFSM(S,T)$ for communicating FSM/C $\langle S,T \rangle$.

$$\sum_{i=0}^{n}\sum_{j=0}^{n} X_{s_i s_j a_h} - \sum_{i'=0}^{n'}\sum_{j'=0}^{n'} X_{t'_i t'_j a_h} \geq 0$$

図1の S と T からは，**図6**のような制約式の集合（以下，$CH_{\geq}(S,T)$ と書く）が得られる．

与えられた通信FSM/C $\langle S,T \rangle$ に対して，通信系全体として，**図7**のような制約式の集合を生成する．以下，これらの制約式の集合を $Cons\_CFSM(S,T)$ で表す．

3.2 デッドロックがないことの証明

ここでは，与えられた通信FSM/C $\langle S,T \rangle$ にデッドロック（S, T ともにどの遷移も実行できないような状況）がないことの証明を機械的に行う1つの方法について述べる．提案する手法では，通信系がデッドロックに陥るような遷移系列が必ず満たすような制約式を考え，それらの制約式と前節で述べた通信系全体の制約式 $Cons\_CFSM(S,T)$ とを同時に満たすような解がないことを示すことにより，与えられた通信FSM/Cにデッドロックがないことを保証する．

以下では，ある遷移条件が成り立つときは受信動作しか実行できなくなるような状態を「受信状態」とよぶ☆．

3.2.1 デッドロックの定義

通信FSM/C $\langle S,T \rangle$ がデッドロックに陥る場合，次の2つの状況のいずれかである．

空チャネルデッドロック：S, T がともに受信状態に入り，かつそのときにチャネルがともに空でどの遷移も実行できなくなるようなデッドロック
未定義受信：S, T がともに受信状態に入り，かつ S

☆ 図1の S の受信状態は s_1, s_4, s_5, s_6 の4つである．

または T，あるいはその両方が，入力チャネルの先頭の符号を受信できなくなることにより生じるデッドロック

3.2.2 空チャネルデッドロックがないことの証明

空チャネルデッドロックに陥った場合，(1) S と T の現到達状態がともに受信状態であり，かつ，(2) すべての符号 a_h について，その符号の送信回数と受信回数が等しくなる．このため，次のような制約式が成り立つ．

$$\sum_{s_i \in S\text{の受信状態の集合}} F_{s_i} = 1$$

$$\sum_{t_j \in T\text{の受信状態の集合}} F_{t_j} = 1$$

また，$(C_{s_i} < k_{s_i})$ が成り立つときは受信動作しか実行できないが，$(C_{s_i} \geq k_{s_i})$ が成り立つときは受信動作以外の遷移が実行可能であるような状態 s_i では次のような制約式も成り立つ（逆の場合も同様）．

$$(F_{s_i} = 1) \Rightarrow (C_{s_i} < k_{s_i})$$

同様に $(C_{s_i} \bmod m_{s_i} < k_{s_i})$ が成り立つときは受信動作しか実行できない場合は，制約式

$$(F_{s_i} = 1) \Rightarrow (Cr_{s_i} < k_{s_i})$$

が成り立つ．

(2) については，各符号 a_h について以下が成り立つ．

$$\sum_{i=0}^{n}\sum_{j=0}^{n} X_{s_i s_j a_h} - \sum_{i'=0}^{n'}\sum_{j'=0}^{n'} X_{t'_i t'_j a_h} = 0$$

この制約式は，図6のようなチャネルに関する制約式 $CH_{\geq}(S,T)$ の $\geq$ を $=$ で置き換えたものである．

以上の制約式の集合を $EC\_DL(S,T)$ とする．$Cons\_CFSM(S,T) \wedge EC\_DL(S,T)$ の充足不能性は整数線形計画法の手法を用いて機械的に判定できる．

3.2.3 未定義受信がないことの証明

次に，未定義受信について考える．モデルの性質より，未定義受信に陥る遷移系列 α があれば，必ず

- 送信側：ある符号 a_h の送信が可能な状態
- 受信側：a_h が受信不可能な受信状態
- 送信側から受信側へのチャネル：空

のような状態対に至る遷移系列 α' が存在する．

（証明） いま，通信FSM/C $\langle S,T\rangle$ に対して，ある遷移系列 α を実行することにより，状態対 $\langle s_i, t_j\rangle$ に遷移し，$T \rightarrow S$ 方向のチャネルの先頭に a_h が存在したとする．系列 α の内，T がその符号 a_h を送信するまでに S,T で実行された遷移系列を γ，a_h の送信後に実行された遷移系列を β とする（$\alpha = \gamma \cdot a_h^{-} \cdot \beta$）．また，系列 γ を実行して T が状態 $t_{j'}$ に入ったとする．β が空のときは，$\alpha' = \gamma$ の実行により状態対 $\langle s_i, t_{j'}\rangle$ に遷移し，この状態対で上の命題が成り立つ．β が空でないとき，遷移系列 β の中から T の動作を除いた遷移系列を β' とすると，遷移系列 $\alpha' = \gamma \cdot \beta'$ も実行可能であり，この系列 α' の実行により，通信FSM/C $\langle S,T\rangle$ は状態対 $\langle s_i, t_{j'}\rangle$ に遷移し，$T \rightarrow S$ 方向のチャネルは空となる．よって上の命題が成り立つ． （証明終）

ゆえに，このような状態対に陥ることがないことさえ保証できれば，未定義受信により生じるデッドロック状態に陥らないことが保証できる．各符号 a_h に対して，このような状態対に遷移する系列は下記のような制約式を満足する（T が符号 a_h を送信可能な場合）．

$$\sum_{s_i \in S\text{で符号 } a_h\text{の受信が不可能な受信状態集合}} F_{s_i} = 1$$

$$\sum_{t_j \in T\text{で符号 } a_h\text{の送信が可能な状態集合}} F_{t_j} = 1$$

また，すべての符号 a_k に対して，

$$\sum_{i=0}^{n}\sum_{j=0}^{n} X_{s_i s_j a_k} = \sum_{i'=0}^{n'}\sum_{j'=0}^{n'} X_{t'_i t'_j a_k}$$

が成り立つ．また，S が $(C_{s_i} < k_{s_i})$ なる条件式が成り立つときのみ符号 a_h の受信が不可能な受信状態となる場合などは，前項の空チャネルデッドロックの項で述べた次のような制約式も満足する．

$$(F_{s_i} = 1) \Rightarrow (C_{s_i} < k_{s_i})$$

以上のような制約式の集合を $Undef(S,T,a_h)$ とする．前項同様，すべての符号 a_h に対して，もし図7のような通信系全体の制約式の集合 $Cons\_CFSM(S,T)$ と未定義受信のときに成り立つ制約式の集合 $Undef(S,T,a_h)$ をともに満足するような解が存在しなければ，与えられた通信FSM/C$\langle S,T\rangle$ は未定義受信に陥らないことが保証される．

3.3 S が初期状態に戻らずに無限個の遷移を続けることがないことの証明

前節の方法でデッドロックに陥らないことを保証できるので，以下では与えられた通信FSM/C $\langle S,T\rangle$ はデッドロックに陥らないと仮定する．デッドロックがないという仮定から，(1) S はいつかは初期状態に戻るか，あるいは，(2) 初期状態に戻らず永久に初期状態以外の状態間を遷移し続ける（ライブロックの場合などに相当する）かのいずれかである．(1)，(2) の状況では，論理式 $(F_{s_0} = 1 \wedge C_{s_0} = 1) \vee (C_{s_0} = 0)$

を満足する．この論理式と通信系全体の制約式の集合 $Cons\_CFSM(S,T)$ との論理積に対して，S, T それぞれについて，遷移の実行回数の総和 $\sum X_{s_i s_j a_h}$（あるいは $\sum X_{t_{i'} t_{j'} a_{h'}}$）を最大にするような解を整数線形計画法の手法を用いて求める．どちらについても，その総和が有限であれば，遷移系列の長さが有限であることが保証される．各状態では少なくとも1つの遷移が実行可能であるように仕様が書かれているので，遷移系列の長さが有限なら S はいつかは初期状態に戻る．

3.4 S が初めて初期状態に戻ったとき T も初期状態に戻っていることの証明

次に，S が初めて初期状態に戻ったとき，T がすでに初期状態に戻って S が初期状態に戻るのを待っていることをどのように証明するかについて述べる．S が初めて初期状態に戻ったとき，論理式 $(F_{s_0} = 1 \wedge C_{s_0} = 1)$ が成り立つ．また，T が初期状態以外の状態に遷移したり，S が初期状態に戻ったときに T が2回以上初期状態を通過した場合，制約式 $(F_{t_0} = 0 \vee C_{t_0} > 1)$ が成り立つ．このため，$(F_{s_0} = 1 \wedge C_{s_0} = 1)$ と $(F_{t_0} = 0 \vee C_{t_0} > 1)$，および通信系全体の制約式の集合 $Cons\_CFSM(S,T)$ の3つの制約式をともに満たすような解がなければ，T は S が初期状態に初めて戻ったときに必ず初期状態に初めて戻っていること（S より先に初期状態に戻って待っていること）が保証される．なお，2.2 節の (A5) で仮定した「T の初期状態が受信状態であること」が成り立たない場合，T は S より先に初期状態に戻れば，S を待たずに遷移を行えるので，この論文で議論している「生存性」は成り立たない．

3.5 初期状態対に戻ってきたときにつねに両チャネルが空であることの証明

ここでは，FSM/C が双方ともに初期状態に戻ったときにつねに両チャネルが空になっていることの証明について述べる．この性質の証明は，未定義受信がないことの証明法を応用する．もし，チャネルにメッセージが残るとすれば，

- 受信側：初めて初期状態に戻る
- 送信側：符号の送信が可能な状態
- 送信側から受信側へのチャネル：空

のような状態対に陥る遷移系列が必ず存在する．このような状態対に陥らないことを，未定義受信がないことの証明と同様に証明する．

4. 生存性検証システムの作成と検証実験結果

提案した手法の有用性を確認するため，以上の手法を自動で行うシステムを作成した．このシステムは，FSM/C 記述から 3.1 節で述べた制約式および可達解析結果，3.2〜3.5 節で述べた状態対などを自動生成したり，目的関数の最大値や最小値を自動的に計算する．このシステムから得られる整数線形計画問題を解くのには，市販のパッケージソフト LINDO[9] を用いた．

LINDO のような線形計画問題を解くプログラムの入力は，整数線形不等式の論理積の形で与える必要があるので，たとえば $(C_{s_2} < 5) \Rightarrow (X_{s_2 s_6 h} = 0)$ のような論理式や "∨" などを含む論理式を直接入力することはできない．そこで，実際に制約式を入力する際には場合分けを行う．たとえば，図1では，条件付き遷移を持つ状態が S には3状態，T には1状態あるので，最大 2^4 通りの場合について考える必要があるが，実際には，可達解析結果を用いることによって考えるべき場合分けの数をかなり抑えることが可能である．

図1の例を用いて検証実験を行った結果，検証に約 20 秒を要した（CPU: Pentium 100 MHz）．これは，FSM/C 記述から得られる 80 組程度の整数線形計画問題を解くのに要した時間の合計である．

5. 議　　論

以下では本論文で用いたモデルの制約条件の解消法や提案する手法の限界などについて議論する．

まず，本論文で用いるモデルでは，初期状態に戻ってきた際にはすべての状態訪問回数が0にリセットされると仮定している．すなわち，初期状態を特殊な状態と見なし，初期状態に戻ることにより，システムを初期化（最初の状況に戻す）している．しかし，実際には，初期状態をこのような特殊な状態と見なさずに仕様（たとえば1回目に初期状態に戻ってきたときの動作と2回目以降の動作が異なるような仕様）を記述したい場合がある．このような場合，たとえば，もとの初期状態 s_0 とは別に特別な状態 s_{INIT} を設け，この s_{INIT} を初期状態と見なして遷移を開始し，s_0 を普通の状態として仕様を記述することにより，もとの初期状態 s_0 を特別視しない仕様を記述できる．また，本論文では，条件付き遷移の数が一状態につき2本という制約を課しているが，この制約は本質的なものでない．たとえば，$s_1 \xrightarrow{\langle (C_{s_1} < 5), a \rangle} s_2$, $s_1 \xrightarrow{\langle (5 \le C_{s_1} < 8), b \rangle} s_3$, $s_1 \xrightarrow{\langle (8 \le C_{s_1}), c \rangle} s_4$ なる3分岐の条件付き遷移はダミー遷移（dummy）と新たな状態（たとえば s_5）を導入して，$s_1 \xrightarrow{\langle (C_{s_1} < 5), a \rangle} s_2$, $s_1 \xrightarrow{\langle (5 \le C_{s_1}), dummy \rangle} s_5$, なる2分岐と，$s_5 \xrightarrow{\langle (C_{s_5} < 4), b \rangle} s_3$, $s_5 \xrightarrow{\langle (4 \le C_{s_5}), c \rangle} s_4$ なる2分岐からなる FSM/C を構成する．このように変形

したFSM/Cは，ダミー遷移（dummy）を余分に行うことを除けば，生存性の議論には影響なく，もとのFSM/Cと同じ動作を行う．

本手法では，「一方のFSM/Cが初期状態において送信動作を行う場合，もう一方のFSM/Cは受信動作しか行えない」という制約を課している．しかし，初期状態でともに送信動作が行えるような対称構成をとるプロトコルではこの制約を満足しない．このようなプロトコルに対しては，本手法は直接適用できない．これは，本手法の適用限界の1つである．このような場合の対処法としては，たとえば，S, T の初期状態のコピーに相当する状態（最終状態）を新たに導入し，S, T の初期状態への遷移を新たに導入した最終状態への遷移に置き換え，「S, T の初期状態対と空のチャネルの組」から「S, T の最終状態対と空のチャネルの組」へ必ず戻るかどうかを議論する方法が考えられる．この場合，一方のFSM/Cが最終状態に入ったらそれ以上遷移できないので，S, T がともに最終状態に遷移することが証明できても，もとの通信FSM/Cでは，S, T の両方が初期状態に戻る前に一方のFSM/Cが初期状態から実行可能な送信動作を実行し始めるという可能性を否定できない．しかし，上述の証明結果は，少なくとも「（同時ではないかもしれないが）いつかは S, T ともに初期状態に戻る」ことは保証している．また，初期状態に戻った際の S, T の送信動作の実行に関して適当な仮定を置くことによって上述のような可能性を排除できる場合は，上記の証明によって生存性の検証を行うことができる．

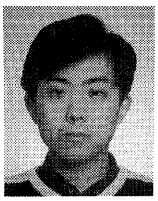
6. まとめ

本論文では，各状態 s_i を訪れたカウンタ C_{s_i} の値により遷移が決まるFSM/C対からなる通信系が生存性を満たすことを整数線形計画法を用いて機械的に検証する方法を提案し，提案した手法に基づき検証を行うシステムを作成した．本手法による検証はパラメータ値に依存しないため，状態爆発を回避する1つの手段として利用可能である．なお，本手法は十分条件の証明であるため，「生存性」が成り立つ場合でも必ず証明に成功するとは限らない．このため，たとえば，与えられた通信FSM/Cで成り立つ性質（不変式）を加えると証明に成功する可能性が高くなる．文献1)では，本論文で述べた可達解析結果に関する制約式を用いず，検証者が与えた性質（たとえば，「つねに符号 c の受信回数は符号 d の受信回数の8倍以上である」など）がすべての遷移系列に対して不変式として成り立つことを機械的に証明し，その結果を用いて「生存性」を証明している．この方法では，検証者が与えた不変式が可達解析結果に相当する制約式を与えていることになる．このように，検証者がその通信システムで成り立つと思われる性質を与え，その性質が不変式であることを機械的に証明し，証明した結果を加えて「生存性」の検証を行えば，さらに検証に成功する可能性を高めることができる．今後の課題としては，検証者が与えた性質を用いた検証系にシステムを拡張することや，他の性質の検証に本論文の検証手法を応用することなどが考えられる．

参考文献

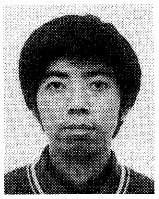
1) Higashino, T., Nakata, A., Itoh, T. and Taniguchi, K.: Verification of Liveness Property for Communicating FSM's with Conditional Transitions depending on State Visiting Numbers, *Proc. 8th IFIP Int. Conf. on Formal Description Technique* (*FORTE'95*), pp.431–438 (1995).
2) Avurnin, G.S., Buy, U.G., Corbett, J.C., Dillion, L.K. and Wileden, J.C.: Automated Analysis of Concurrent Systems with Constrained Expression Toolset, *IEEE Trans. Softw. Eng.*, Vol.17, No.11, pp.1204–1222 (1991).
3) Corbett, J.C.: Verifying General Safety and Liveness Properties With Integer Programming, *Proc. Computer Aided Verification '92* (*CAV'92*), pp.337–348 (1992).
4) Corbett, J.C.: Evaluating Deadlock Detection Methods for Concurrent Software, *IEEE Trans. Softw. Eng.*, Vol.22, No.3, pp.161–180 (1996).
5) Agarwal, S., Courcoubetis, C. and Wolper, P.: Adding Liveness Property to Coupled Finite-State Machines, *ACM Trans. Prog. Lang. and Syst.*, Vol.12, No.2, pp.303–339 (1986).
6) Blumer, T.P. and Sidhu, D.P.: Mechanical Verification and Automatic Implementation of Communication Protocol, *IEEE Trans. Softw. Eng.*, Vol.12, No.8, pp.827–843 (1986).
7) Gouda, M.G. and Chang, C.K.: Proving Liveness for Network of Communicating Finite State Machines, *ACM Trans. Prog. Lang. Syst.*, Vol.8, No.1, pp.154–182 (1986).
8) Gouda, M.G. and Multari, N.J.: Stabilizing Communication Protocols, *IEEE Trans. Comput.*, Vol.40, No.4, pp.448–458 (1991).
9) LINDO: Linear INteractive and Discrete Optimizer for Linear, Integer, and Quadratic Programming Problem, LINDO Systems, Inc.

(平成 9 年 5 月 12 日受付)
(平成 10 年 1 月 16 日採録)



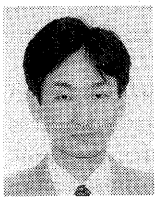
水野健太郎（学生会員）

平成7年大阪大学基礎工学部情報工学科中退（飛び級修了）．平成9年同大学院基礎工学研究科博士前期課程修了．現在同大学院博士後期課程在学中．分散システム，通信プロトコルの仕様記述と検証，ハードウェアの自動合成等の研究に従事．



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年同大学院博士後期課程修了．工学博士．同年広島市立大学情報科学部情報数理学科助手．分散システム，プロセス代数，時相論理等の研究に従事．



岡野　浩三（正会員）

平成2年大阪大学基礎工学部情報工学科卒業．平成5年同大学院博士後期課程中退．同年同大学情報工学科（現：情報科学科）助手．工学博士．代数的手法によるソフトウェア設計開発法，分散システム等の研究に従事．電子情報通信学会会員．

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年同大学院博士後期課程修了．工学博士．同年同大学助手．平成2年，6年モントリオール大学客員研究員．現在大阪大学情報科学科助教授．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，IEEE，ACM各会員．

谷口　健一（正会員）

昭和40年大阪大学工学部電子工学科卒業．昭和45年同大学院基礎工学研究科博士課程修了．工学博士．同年同大学基礎工学部助手．現在，同大学情報科学科教授．計算理論，ソフトウェアやハードウェアの仕様記述・実現・検証の代数的手法および支援システム，関数型言語の処理系，分散システムや通信プロトコルの設計・検証法等に関する研究に従事．