遷移の選択が状態訪問回数に依存する有限状態機械対からなる通信系に対する生存性検証システム

3Bb－5

水野 健太郎　中田 明夫　東野 輝夫　谷口 健一
大阪大学 基礎工学部 情報工学科

1　はじめに

通信プロトコルは有限状態機械 (FSM) 等によってモデル化され検証される場合が多いが，パラメータ値の取り扱いを考えるとFSMの状態数が多くなり状態爆発が生じる．そこで，我々は従来より実行される遷移が状態訪問回数に依存して定まる有限状態機械モデル FSM/C の上で，整数線形計画法を用いて状態爆発を回避した生存性の検証法を提案してきた [1].

本稿ではこの手法にもとづき，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報告する．また，従来 [1] で提案した手法では多くの場合において検証者が付加的な情報を与えて半自動で検証を行っていたのに対し，本稿では検証手法を改良し，文献 [1] と同じ例については検証手順を完全に機械的に行えるようにした．

2　モデル FSM/C と生存性

FSM/C では，FSM が S_i を訪問した回数を変数 C_{si} で記憶する．各遷移は無条件に実行可能なものと条件付遷移に分けられる．条件付遷移の場合，各状態を訪問した回数 C_{si}(もしくは C_{si} を m で割った剰余 Cr_{si}) の大小によって遷移が決まり，S_i からの遷移は変数 C_{si} (もしくは Cr_{si}) の値が k より小さいときのみ実行可能な遷移と k 以上のときのみ実行可能な遷移の２つで構成されるものとし，いずれか一方の遷移が決定的に選ばれる．また，初期状態は自己ループや条件付遷移を持たず，仕様は強連結である，と仮定する．

図１に FSM/C 仕様の例を示す．図１では，送信動作を a_{h-}，受信動作を a_{h+} のように表している．双方の機械 S, T は FIFO キュー (信頼でき，容量無限) で繋がっているものとし，T の初期状態は符号の受信以外の遷移が不可能な状態であると仮定する．

このモデル上での生存性は，

- ２つの FSM/C が初期状態から遷移したとき，いつかはもとの初期状態対に戻り，かつそのとき通信路が空になるような性質

とする．

3　生存性の検証と制約式の生成

FSM/C 仕様が次の条件を全て満たせば，上述の生存性が成り立つことが保証される．

- 通信系がデッドロックに陥らない
- 各 FSM/C が初期状態に戻るまでの遷移系列の長さが常に有限
- S がはじめて初期状態に戻ったとき，T が初期状態に戻っており，その訪問回数は１回 (はじめて戻る)
- 初期状態対に戻ったときは常に通信路が空

本稿では，このうち通信系がデッドロックに陥らないことを証明する方法について主に述べる．

Verification System of Liveness Property for C-FSM's with Transitions depending on State Visiting Numbers
Kentaro MIZUNO , Akio NAKATA , Teruo HIGASHINO and Kenichi TANIGUCHI
Dept. of Information and Computer Sciences, Osaka University,Toyonaka-shi, Osaka 560 , Japan

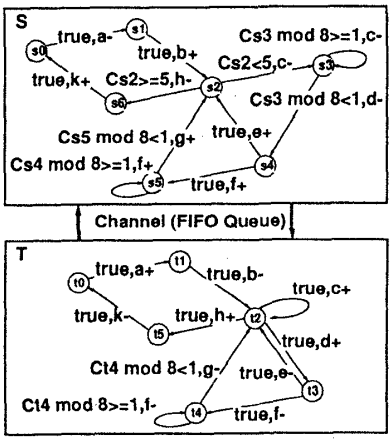

図 1: FSM/C 仕様 S(上段)，T(下段)

提案する手法では，FSM/C 仕様 M の初期状態からのある遷移系列 γ における各遷移の実行回数や各状態の訪問回数が満たすべき条件を線形不等式 (制約式) で表す．S_i から S_j へ遷移し，a_h を送信 (もしくは受信) した回数を変数 X_{sisjah} で表すことにする．変数 F_{si} は γ の現到達状態 (最後の状態) が S_i であるとき１，そうでなければ０になる変数とする．以降，すべての変数は非負整数とする．

3.1　任意の遷移系列について成り立つ制約式

まず，単一の FSM/C について，初期状態からの任意の遷移系列γについて次のような制約式が成り立つ．

(1) γの現到達状態は１つであることから，たとえば

$$F_{s0} + F_{s1} + ... + F_{s6} = 1$$

(2) S_iに入る (S_iから出る) 遷移の実行回数と C_{si} の関係から

$$X_{s2s3c} + X_{s3s3c} = C_{s3}$$

$$C_{s3} = X_{s3s3c} + X_{s3s4e} + F_{s3}$$

(3) 条件遷移を持つ状態を訪れた回数とその状態から出る遷移を実行した回数について成り立つ関係より

$$(C_{s2} < 5) \rightarrow (X_{s2s6h} = 0)$$

$$(C_{s2} \geqq 5) \rightarrow (X_{s2s3c} = 4)$$

また，図２のように，単一 FSM/C の遷移条件の真偽のみに着目した到達可能性木を作成する．初期状態とその時点で

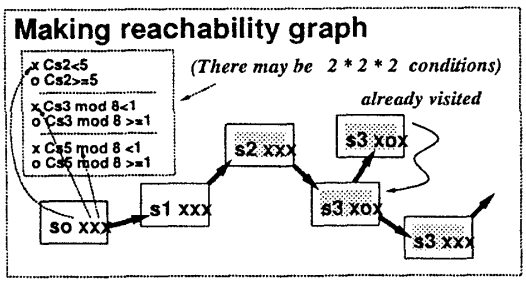

図 2: 到達可能性木の作成

成り立つ遷移条件群との組から木の生成を開始し，その時点までに生成されていない状態と遷移条件群との組に到達した

ときは，その状態からの遷移によって到達しうるすべての状態と遷移条件群との組を自身の子頂点として付加する．そして，各々の子頂点について，すでに調べた状態と遷移条件群の組に到達するか初期状態に戻るまで，同様に木の生成と探索を続ける．木の各頂点には現到達状態と遷移条件群をラベルとして格納しておく．このような方法により，遷移条件のすべての組合せについて，それらの遷移条件が成り立つときの現到達状態を絞り込むことができる．この方法は遷移条件が変化しうるかどうかのみに着目しているので，到達可能性木の大きさは遷移条件に書かれた具体的な kや m の値に依存しない(従来の可達解析では，到達可能性木の大きさは kや m の値に大きく依存する)．この探索の結果から，

(4) 各遷移条件の組に対してそれらの条件を満たす状態が限定できるので，たとえば

$$((C_{s2} \geqq 5) \wedge (C_{s3} mod 8 < 1) \wedge (C_{s5} mod 8 < 1)) \rightarrow (F_{s0} + F_{s2} + F_{s6} = 1)$$

のような制約式が成り立つことが分かる．

次に FSM/C 対について考える．一般に受信動作 a_{h+} は通信路に a_h が存在するときしか実行できないので，各符号について

(5) 符号の送信回数が受信回数以上になることを表す

$$X_{s2s3c} + X_{s3s3c} \geqq X_{t2t2c}$$

のような制約式を考えればよい．

3.2 デッドロックがないことの証明

通信系におけるデッドロックには，空チャネルデッドロック(双方の FSM/C がともに符号の受信しかできない状態に入り，通信路が双方向ともに空) と未定義受信 (通信路の先頭の符号が受信できず，受信以外の遷移が不可能) がある．FSM/C においては

- その状態からの遷移がすべて受信である場合
- 遷移条件により受信遷移のみが実行可能になる場合

は符号の受信以外の動作が不可能である．このような状態を受信状態と呼ぶことにする．チャネルが空であることを表すには，各符号について

(5') 符号の送信回数が受信回数と等しいことを表す

$$X_{s2s3c} + X_{s3s3c} = X_{t2t2c}$$

のような制約式を加える．

たとえば空チャネルデッドロックに陥らないことを証明するには，S，T のそれぞれについて受信状態を抽出し，すべての受信状態対$< S_i, T_j >$について，(1)〜(4) および (5') の制約式に，双方の受信状態に対応する変数 F の値が 1 になるような制約式 $(F_{si} = F_{tj} = 1)$ を加えたものを考える．どの受信状態対についてもこの制約式全体を満たす解が存在しなければ，S と T からなる通信系が空チャネルデッドロックに陥らないことが保証される．

上で述べた方法によってデッドロックに陥らないことが証明できれば，次に

- 初期状態へ戻るまでの遷移系列の長さが，どちらの FSM/C についても常に有限であること
- $((F_{s0} = 1) \wedge (C_{s0} = 1)) \rightarrow ((F_{t0} = 1) \wedge (C_{t0} = 1))$
- $((F_{s0} = 1) \wedge (F_{t0} = 1)) \rightarrow$ (各符号の送信数=受信数)

の各条件が成り立つことを証明することにより，2つの FSM/C からなる通信系が生存性を満たすことが証明できる．

3.3 検証手法の改良

従来文献 [1] で提案した手法では，図 1 の検証例を含め，多くの場合において符号の送受信の順序などに関する制約式を検証者が手動で付加して (半自動で) 検証を行っていた．これに対し，本稿では，単一の FSM/C の現到達状態と遷移条件群との関係に注目することにより，より多くの例に対してデッドロックがないことを自動的に証明できるようにする．

普通に受信状態と遷移条件群とのすべての組合せについて考えると，3.1 および 3.2 で考えた制約式が対応する遷移系列が存在しないような解を持ち，検証に失敗することが多くなる．ここで，図 2 の探索結果から得られた表 (図 3) より，実際には S の受信状態 S_1，S_4，S_6 に入ったときに成り立つような遷移条件の組合せはそれぞれ高々 1 つ，S_5 については高々 2 つであることが分かるので，これらの組合せのみについて考えれば十分である．図 1 の例では，この手法で受信状態と遷移条件群との組合せを絞り込むことにより，機械的に検証を行うことができる．

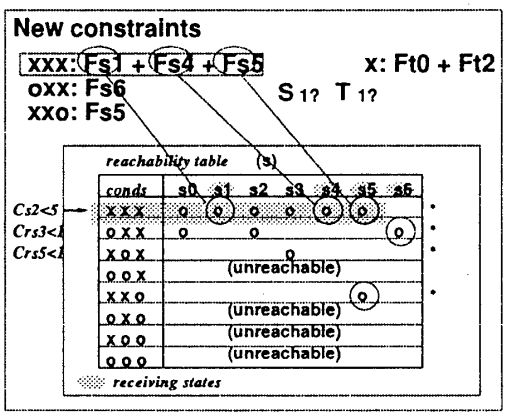

図 3: 受信状態と遷移条件群の関係

3.4 検証システムの作成と実験結果

本稿では，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 章で述べた制約式および受信状態対を出力する．それらの組合せすべてについて，その出力を整数線形計画問題を解くプログラム LINDO [2] に入力し，どの入力に対しても解が存在しなければデッドロックに陥らないことが証明できる．

このとき，同じ条件群に属する受信状態群はまとめて，各々の状態に対応する変数 F の和が 1 になるような解がないことを証明すればよいので (図 1 の例では，S について

$$((C_{s2} < 5) \wedge (C_{s3} mod 8 < 1) \wedge (C_{s5} mod 8 < 1)) \rightarrow (F_{s1} + F_{s4} + F_{s5} = 1)$$

のような制約式を加える)，実際には考慮すべき組合せの数はかなり抑えられる．

図 1 の例について検証実験を行った結果，検証に約 10 秒を要した (CPU:Pentium 100MHz)．

4 おわりに

本稿では，FSM/C 対からなる通信系が生存性を満たすことを機械的に検証するシステムを作成した．また，デッドロックの検出においては検証手法を改良し，文献 [1] の例について検証の自動化を行った．

今後の課題としては，実用的なプロトコル仕様を FSM/C で記述して生存性の検証を行うこと，他のモデルや性質に今回の手法を応用することなどがある．

参考文献

[1] T.Higashino, Akio Nakata, Tatsuo Ito and Kenichi Taniguchi : "Verification of Liveness Property for Communicating FSM's with Conditional Transitions depending on State Visiting Numbers", Proc. FORTE'95,Oct. 1995.

[2] LINDO : Linear INteractive and Discrete Optimizer for Linear , Ingeger , and Quadratic Programming Problems , LINDO Systems , Inc.