2 E － 5

遷移条件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の生存性検証

伊東 達雄　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　まえがき

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. 一般にシーケンス番号などのパラメータ値を状態で識別して取り扱おうとすると, 状態数が増加し状態爆発が起こる. 本稿では遷移条件が状態訪問回数に依存する有限状態機械モデル FSM/C を提案し, そのモデル上で状態爆発を回避した生存性の検証法を提案する. 本稿で議論する生存性は, FSM/C 対からなる通信系において, 各 FSM/C が初期状態からどのような遷移を行っても, いつかはもとの初期状態対に戻り, 各通信チャネルがもとの空の状態に戻ること, と定義する. その生存性の検証において, 整数線形計画法を用いて従来の可達解析で生じるような状態爆発の発生を防いでいる..

2　FSM/C モデル

本稿では, FSM が状態 s_i を訪問した回数を変数 C_{s_i} で記憶する. 提案する FSM/C モデルでは, 決定性 FSM の各遷移 $s_i \xrightarrow{a_h} s_j$ の実行可能性をその開始状態 s_i の状態訪問回数による上界制約 (下界制約) を用いて制限する. 条件付遷移 $s_i \overset{<(C_{s_i}<k),a_h>}{\longrightarrow} s_j$ ($s_i \overset{<(C_{s_i}\geq k),a_h>}{\longrightarrow} s_j$) は, 変数 C_{s_i} の値が k より小さい (k 以上の) ときのみ, つまり FSM が状態 s_i を訪問した回数が $k-1$ 回以下 (k 回以上) のときのみ, 状態 s_i で動作 a_h を実行できることを表す. また, 条件付遷移 $s_i \overset{<(mod(C_{s_i},m)<k),a_h>}{\longrightarrow} s_j$ は, 変数 C_{s_i} の値を整数 m で割った余りが k より小さいときのみ, 動作 a_h を実行できることを表す ($(mod(C_{s_i},m) \geq k)$ の場合も同様). 無条件遷移は $s_i \overset{<true,a_h>}{\longrightarrow} s_j$ のように書く. 以下, 議論を簡単にするため, FSM/C 仕様の任意の状態 s_i に対して, 状態 s_i から始まる条件付遷移があれば, その状態 s_i は 2 本の条件付遷移のみを持ち, かつ, それぞれの遷移の制約は $(C_{s_i} < k)$ と $(C_{s_i} \geq k)$, あるいは, $(mod(C_{s_i},m) < k)$ と $(mod(C_{s_i},m) \geq k)$ であると仮定する. また, 初期状態は自己ループや条件付遷移を持たない, 仕様は強連結である, ことを仮定する. 図 1 に FSM/C 仕様の例を付す. 図 1 では, 送信動作を a_h^-, 受信動作を a_h^+ のように表す.

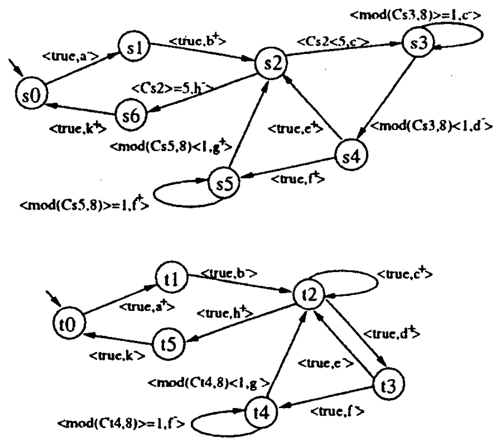

図 1: FSM/C 仕様 M1(上段), M2(下段)

3　単一の FSM/C 仕様に対する生存性検証

FSM/C 仕様 M の初期状態からの遷移系列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制約式を考える. 変数 $X_{s_i s_j a_h}$ で遷移 $s_i \overset{<cond,a_h>}{\longrightarrow} s_j$ を実行した回数を表すことにする. 変数 F_{s_i} は, M の現到達状態が 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. 本稿で採用する制約式としては, 次のようなものを考える.

(I) 現到達状態はたかだか 1 つしかないので ($\{s_0,\ldots,s_n\}$ を状態集合とし, s_0 を初期状態とする),

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

(II) 各状態の入出力遷移の実行回数と, C_{s_i} の値の関係 ($\{a_1,\ldots,a_m\}$ を動作の集合とする),

$$\sum_{j=0}^{n}\sum_{h=1}^{m} X_{s_j s_i a_h} = C_{s_i} = \sum_{j=0}^{n}\sum_{h=1}^{m} X_{s_i s_j a_h} + F_{s_i} \quad (i \neq 0)$$

$$\sum_{j=0}^{n}\sum_{h=1}^{m} X_{s_j s_0 a_h} = C_{s_0} = \sum_{j=0}^{n}\sum_{h=1}^{m} X_{s_0 s_j a_h} + F_{s_i} - 1$$

この式は状態 s_i を訪問した回数 C_{s_i} と, 状態 s_i の各入力遷移の実行回数の和が等しいことを表している. また

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

状態 s_iの出力遷移の実行回数の和は現到達状態が s_iの場合 C_{s_i}の値より 1 回少なく, 現到達状態が s_iでない場合 C_{s_i}の値と等しいことを表している.

(III) $s_i \xrightarrow{<(C_{s_i}<k),a_p>} s_v$, $s_i \xrightarrow{<(C_{s_i}\geq k),a_q>} s_u$ なる条件付遷移を持つ状態 s_iにおいて, 次の制約式が成り立つ.

$$(C_{s_i} < k) \Rightarrow (X_{s_i s_u a_q} = 0)$$

$$(C_{s_i} \geq k) \Rightarrow (C_{s_i} = X_{s_i s_u a_q} + k - 1)$$

$(mod(C_{s_i}, m) < k)$ と $(mod(C_{s_i}, m) \geq k$の場合は次の制約式が成り立つ (Cd_{s_i},Cr_{s_i}は新しく導入した変数).

$$(C_{s_i} = m * Cd_{s_i} + Cr_{s_i}) \wedge (m - 1 \geq Cr_{s_i} \geq 0)$$

$$(Cr_{s_i} < k) \Rightarrow (X_{s_i s_u a_q} = (m - k) * Cd_{s_i})$$

$$(Cr_{s_i} \geq k) \Rightarrow (X_{s_i s_v a_p} = k * Cd_{s_i} + (k - 1))$$

(IV) 条件付遷移に含まれる条件式がどの状態で成り立つかを考える. また, どのような状態でも成り立たないような条件式の組を見つける. 例えば, 図 1 の例では, 条件式 $(C_{s_2} < 5)$,$(Cr_{s_3} \geq 1)$,$(Cr_{s_5} < 1)$ が共に成立すれば, その遷移系列の最終状態は必ず状態 s_3であり, 条件式 $(C_{s_2} \geq 5)$,$(Cr_{s_3} \geq 1)$,$(Cr_{s_5} \geq 1)$ が共に成り立つことはない. このような場合, 次の制約を加える.

$$((C_{s_2} < 5) \wedge (Cr_{s_3} \geq 1) \wedge (Cr_{s_5} < 1)) \Rightarrow (F_{s_3} = 1)$$

$$not((C_{s_2} \geq 5) \wedge (Cr_{s_3} \geq 1) \wedge (Cr_{s_5} \geq 1))$$

以上の制約式の論理積を $CE(M)$ で表す. 初期状態から始まる任意の遷移系列の各遷移の実行回数や状態訪問回数は $CE(M)$ を満たす. しかし, $CE(M)$ を満たす解が実際の遷移系列に対応するとは限らない.

[定理 1] 与えられた FSM/C 仕様 Mに対して, 制約式 $Live(M)$ を次のように定義する.

$$Live(M) \equiv CE(M) \wedge (C_{s_0} = 1) \wedge (F_{s_0} = 1)$$

また, 各遷移の実行回数 $X_{s_i s_j a_h}$の総和を $L(M)$ とする. このとき $Live(M)$ が充足可能で, $L(M)$ の最大値が有限であれば, Mはいつかは初期状態に戻る. □

4 FSM/C 対に対する生存性検証

以下, 信頼できる容量無限の FIFO キューでつながっている FSM/C 対 M_s,M_tからなる通信系の生存性検証を考える. 検証は上述の制約式 $CE(M_s)$, $CE(M_t)$ と M_s,M_t間のチャネルに関する制約 $CH(M_s, M_t)$ を用いて証明する. 一般に受信動作 a_h^+は通信チャネルに a_hが存在しない限り実行できない. よって, M_sの送信動作 a_h^-を実行した合計回数は M_tの受信動作 a_h^+を実行した合計回数以上でなければならない. すなわち,

$$N(a_h) = \sum_{i=0}^{n_s}\sum_{j=0}^{n_s} X_{s_i s_j a_h} - \sum_{i=0}^{n_t}\sum_{j=0}^{n_t} X_{t_i t_j a_h} \geq 0$$

また, もとの FSM/C 仕様から各記号の受信回数の間に一定の関係が成り立つことがわかる場合がある. 例えば, 図 1 の M1 は記号 c を 8 回送信してからしか記号 d を送信しないので, M2 で c を受信した回数と d を受信した回数の間には次のような関係が成り立つ.

$$X_{t_2 t_2 c} - 8 * X_{t_2 t_3 d} \geq 0$$

以下, これらの制約式の論理積を $CH(M_s, M_t)$ とする [2]. $CH(M_s, M_t)$ における記号間の受信回数に関する制約式は検証者が与える. この部分の制約式を多く与えれば与えるほど, 証明に成功する可能性が高くなる.

[定理 2] M_s, M_tから成る通信系がデッドロック状態を含まないと仮定する. また M_tの初期状態が受信動作のみが可能な状態とする. このとき, 制約式

$$Prog(M_s, M_t) = Prog(M_s) \wedge CE(M_t) \wedge CH(M_s, M_t)$$

$$Prog2(M_s, M_t) = Live(M_s) \wedge (C_{s_0} = 1) \wedge (F_{s_0} = 1)$$

に対して, 次の 5 つの条件

(1-1) $Prog(M_s, M_t)$ が充足可能,

(1-2) $L(M_s), L(M_t)$ の最大値が有限,

(2-1) $Prog2$ に対する F_{t_0}の最小値が 1,

(2-2) C_{t_0}の最大値が 1,

(2-3) $N(M_s, M_t) = \sum_{h=1}^{m} N(a_h)$ の最大値が 0

が共に成立すれば, M_s, M_tから成る通信系は生存性を満たす. □

デッドロック状態を含まないことの証明法については文献 [2] 参照.

5 あとがき

本稿では, 通信 FSM/C's に対する生存性の一検証法を提案した. 従来の可達解析では, 条件付制約式に含まれる上下界制約値の積に比例する状態が生成される. しかし, 本手法ではそれらの値に依存しない. 制約式 $Prog(M_1, M_2)$ の充足可能性を判定し, $L(M_1)$ の最大値を求めるのに約 3.0 秒 (CPU : INTEL DX4) 要した. 提案する手法に基づいた検証システムを開発し, 提案する手法の有効性を確認することなどが今後の課題である.

参考文献

[1] J.C. Corbett : "Verifying General Safety and Liveness Properties With Integer Programming", Proc. CAV '92, pp.337-348, 1992.

[2] T. Higashino, et. al. : "Verification of Liveness Property for Communicating FSM's with Conditional Transitions depending on State Visiting Numbers", Proc. FORTE'95, Oct. 1995 (to appear).