50－1　イベント間の時間制約を論理式で記述できるラベル付き遷移システムとその双模倣等価性検証

中田明夫　東野輝夫　谷口健一

大阪大学 基礎工学部 情報科学科

1　まえがき

時間制約が指定された通信プロセスに対する双模倣等価性の判定は，時間性に起因する状態爆発により一般には困難である．時間性に関しては，文献 [4, 2, 1] などに状態爆発を回避する等価性判定法の提案がある．しかし，それらの提案ではいずれも時間制約としては限られたクラスの記述しか出来ない．一方，最近，データ受渡しを記述できるプロセスモデルに関して，データの具体的な値を考えずに値が満たす条件式を用いて等価性を判定する方法が [3] で提案された．この手法は，(1) 判定コストがデータの領域や具体値に依存しない，(2) データに依存する動作の遷移条件を記述する言語として任意の決定可能な論理式の体系を採ってよい，という利点をもつ．時間性を考慮したプロセスの等価性判定にも同様の利点を持った判定法があることが望ましい．

本稿では，時間制約が記述可能な一つのプロセスモデルを提案し，そのモデルで記述されたプロセスに対して，上記のような手法によって状態爆発を回避して双模倣等価性を判定する方法を提案する．

まず，時間制約を記述するモデルとして，交替性Timed Symbolic Labelled Transition System(以下交替性TSLTSと略す)を導入する．交替性 TSLTS の各状態は幾つかのパラメータ変数 (例えば x,y) を持ち，各遷移には，例えば，$x+5$ 秒間から y 秒間待つ，待った時間が $y-3$ 秒以内なら動作 a を実行し，さもなければ動作 b を実行する，などといった条件を変数を用いて記述できる．

提案する方法では，文献 [3] と同様のアルゴリズムによって，交替性 TSLTS モデルで記述されたプロセスの 2 状態に対して，それらを時間的双模倣等価にするような最弱の条件式 (most general boolean, 以下 mgb[3] と呼ぶ) を求める．

2　TSLTS モデル

TSLTS は LTS の各状態 s にパラメータ変数の集合 $DVar(s)$ を付加し，遷移として，遷移条件 P が付いた動作遷移 $s \xrightarrow{a,P} s'$(a は動作名)，および，遅延遷移 $s \xrightarrow{e(d),P} s'$($d$ は遅延量を表す任意の変数) を持つものであると定義する．P は $DVar(s)$ に含まれる変数 (および d(遅延遷移の場合)) を引数に持つことのできる述語である．直観的には遅延遷移 $s \xrightarrow{e(d),P} s'$は条件 P を満たすような d の値だけ時間遅延した後に s'に遷移することを表す (d は状態 s'以降のパラメータ変数に用いることができる)．また，遅延遷移終了時には状態 s' 以降のパラメータ変数 d にはそのときの 遅延値が代入される．動作遷移 $s \xrightarrow{a,P} s'$は s のパラメータ変数 $DVar(s)$ が条件 P を満たすときに動作 a を瞬時に実行することを表す．状態 s から遷移

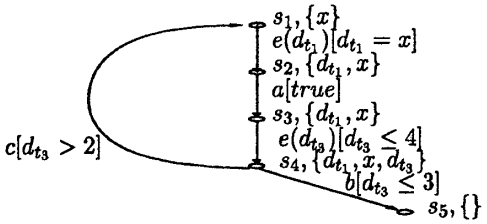

図 1: 交替性 TSLTS の例

可能な動作が複数ある場合はそれらの 1 つが非決定的に選択実行される．

さらに，TSLTS の状態が休止状態 (idle state) および活動状態 (active state) に 2 分割され，休止状態からは遅延遷移のみ，活動状態からは遅延遷移以外の遷移のみが実行可能であるものを，交替性 TSLTS と呼ぶ．交替性を仮定することによって，連続した遅延遷移が 1 つの遅延遷移と対応する場合を考慮する必要がなくなるので，双模倣関係を考えることが容易になる．

例 1　図 1に交替性 TSLTS の例を示す．図において $s_1, s_2, \ldots$ は状態名である．各状態名の隣に書かれた集合はその状態における $DVar()$ の値を示す．各遷移には $a[P]$(または $e(d)[P]$) という形で，動作 (遅延) およびその条件を示してある．図 1の TSLTS において，状態 s_1の変数 x にパラメータ値 v が与えられたときの動作は次の通り．まず，v 単位時間経過した後 (このとき d_{t_1}には v が代入される)，動作 a を実行する．次に a の動作後 4 単位時間以内に b または c を実行する．b は 3 単位時間以内のときに実行され，状態 s_5に遷移し停止する．2 単位時間以上のときは c も実行可能で，この場合は s_1に戻り，上と同様の動作を繰り返す．　□

3　時間的双模倣等価性

本節では TSLTS に対して時間的双模倣等価性を定義する．

定義 1　各変数への値の代入を ρ, ρ'などで表記する．論理式 P へ代入ρを施した式が真であることを $\rho \models P$ と表記する．$\rho[x = e]$ を変数 x に e を代入する以外はρと同じ代入であると定義する．TSLTS の状態 s と代入ρの対 (s, ρ) を $\rho(s_1)$ と表記し，代入ρによる s のインスタンスと呼ぶ．インスタンスは直観的には変数の値も含めた状態のことである．　□

TSLTS の実際の動きは与えられた代入に関して TSLTS を各状態のインスタンス間の動作遷移および具体的な時間値による遅延遷移が定義された通常の LTS に対応させることによって定義される．TSLTS の動作遷移 $s \xrightarrow{a,P} s'$と $\rho \models P$ なるρに対して，$\rho(s) \xrightarrow{a} \rho(s')$ というインスタンス間の遷移が対応する．遅延遷移 $s \xrightarrow{e(d),P} s'$ に関しては遅延変数への具体的な値の代入が生じるので，$\rho[d = t] \models P$ なるρに対して，インスタンス間の遷移$\rho(s) \xrightarrow{t} \rho[d = t](s')$ が対応する．

交替性 TSLTS の 2 つのインスタンスに対してそれらの時間的双模倣等価性は，対応する意味 LTS に対して従来同様の双模倣関係を考えることによって，以下のように定義される．

定義 2　交替性 TSLTS の状態のインスタンスの集合 $\{\rho(s) |$ s:状態, ρ:代入 $\}$ の上の対称な 2 項関係 R で以下の条件を満

Labelled Transition System with Timing Constraints among Events specified in 1st-order Logic and its Verification of Bisimulation Equivalence

Akio NAKATA, Teruo HIGASHINO, Kenichi TANIGUCHI
Department of Information and Computer Sciences,
Faculty of Engineering Science, Osaka University
Toyonaka, 560 Japan

足するものを時間的双模倣関係と呼ぶ：$(\rho_i(s_i), \rho_j(s_j)) \in R$ ならば，以下の条件をすべて満たす：(1). 任意の時間値 t に対して，もし $\rho_i(s_i) \xrightarrow{t} \rho_i'(s_i')$ ならば，ある s_j',ρ_j'が存在して $\rho_j(s_j) \xrightarrow{t} \rho_j'(s_j')$ かつ $(\rho_i'(s_i'), \rho_j'(s_j')) \in R$, (2). 任意の $a \in Act$ に対して，もし $\rho_i(s_i) \xrightarrow{a} \rho_i'(s_i')$ ならば，ある s_j',ρ_j'が存在して $\rho_j(s_j) \xrightarrow{a} \rho_j'(s_j')$ かつ $(\rho_i'(s_i'), \rho_j'(s_j')) \in R$. このとき，ある時間的双模倣関係 R が存在して $(\rho_i(s_i), \rho_j(s_j)) \in R$ となるならば，$\rho_i(s_i)$ と $\rho_j(s_j)$ は時間的双模倣等価であると定義し，$\rho_i(s_i) \sim_t \rho_j(s_j)$ と表記する. □

4 等価性判定

交替性 TSLTS の状態対 (s_i, s_j) に対して $\rho(s_i) \sim_t \rho(s_j)$ であるような ρ が満たすべき必要十分条件を状態対 (s_i, s_j) の mgb と呼ぶ. 状態対の mgb を求めることができれば，代入 ρ に対して $\rho(s_i)$ と $\rho(s_j)$ が時間的双模倣等価であるかの判定は論理式の真偽判定に帰着できる. 交替性 TSLTS の状態対 (s_i, s_j) の mgb を $mgb(s_i, s_j)$ と表記する. mgb は以下のようにして求めることが出来る.

休止状態対 (s_i, s_j) に対しては，mgb は以下のように表される. まず，交替性 TSLTS の性質および時間決定性より，s_i と s_j が等価ならばそれぞれから出る遅延遷移は値も含めて 1 対 1 に対応するはずである. そこで遅延変数名を 1 つに統合する. その変数名は s_i, s_jどちらのパラメータにも使われていない必要があるので，$DVar(s_i) \cup DVar(s_j)$ に属さない新しい変数名 d を選ぶ. まず，s_i と s_jが時間的双模倣等価ならば，s_iで可能な任意の遅延値 d の遅延遷移に対して，s_j も同じだけの遅延遷移が可能で，各遷移先 s_i', s_j'は同じ d の値の下で時間的双模倣等価であるはずである. つまり，例えば $s_i \xrightarrow{e(d_i), d_i \le x} s_i', s_j \xrightarrow{e(d_j), d_j \le y} s_j$ ならば $\forall d[d \le x \Rightarrow [d \le y \wedge ((s_i'[d_i \to d], s_j'[d_j \to d])$ の mgb)] が成り立つ. ここで，状態 s_iからでる遷移およびそれ以降の遷移の条件に現れる変数 d_i を d へ置き換えることを $s_i[d_i \to d]$ と表す. (s_i', s_j') の mgb は変数 d ではなく一般に変数 d_i および d_j を含む. そこで (s_i', s_j') の代わりに $(s_i'[d_i \to d], s_j'[d_j \to d])$ の mgb を考える. $(s_i'[d_i \to d], s_j'[d_j \to d])$ の mgb は一般に自由変数 d を含む論理式であり，共通の遅延量 d を前提にした時の (s_i', s_j') の mgb を表す.

s_i と s_j を入れ換えても上と同様のことがいえる. 従って，休止状態対 (s_i, s_j) が時間的双模倣等価とするような条件は $(s_i'[d_i \to d], s_j'[d_j \to d])$ の mgb,$M_{i',j'}$ を用いて

$$\forall d[P_i\{d/d_i\} \Rightarrow [P_j\{d/d_j\} \wedge M_{i',j'}]] \\ \wedge \forall d[P_j\{d/d_j\} \Rightarrow [P_i\{d/d_i\} \wedge M_{i',j'}]] \quad (1)$$

と表される.

活動状態対 (s_i, s_j) に対する mgb は以下のように表される [3]. まず，s_i と s_jがある代入 ρ に関して時間的双模倣等価ならば，動作の集合 Act に属する任意の動作 a に対して以下の条件が成り立つ必要がある. s_iにおいて，代入 ρがその遷移条件 P_k を満たすような (ρにおいて遷移可能な) 任意の遷移において動作 a を実行したとき，s_jにおいても ρが遷移条件 Q_j を満たすある遷移が存在して，その遷移で動作 a を実行可能で，各遷移先 s_i', s_j'は ρの下で時間的双模倣等価 (=ρは状態対 (s_i', s_j') の mgb を満たす) であるはずである. s_i,s_jの立場を逆にしても同様. したがって，$K = \{k | s_i \xrightarrow{a, P_k} s_{i_k}\}$, $L = \{l | s_j \xrightarrow{a, Q_l} s_{j_l}\}$ とし，(s_{i_k}, s_{j_l}) の mgb を $M_{k,l}$とすれば，(動作 a のみに着目した時に)(s_i, s_j) を等価とする条件は

$$\bigwedge_{k \in K} \{P_k \Rightarrow \bigvee_{l \in L} \{Q_l \wedge M_{k,l}\}\} \wedge \bigwedge_{l \in L} \{Q_l \Rightarrow \bigvee_{k \in K} \{P_k \wedge M_{k,l}\}\} \quad (2)$$

と表せる [3]. この条件を任意の動作 a に対して求めて論理積で結合すれば任意の動作に対する活動状態対 (s_i, s_j) を等価とするような条件となる. すべての動作 $a \in Act$ に対する式 (2) を論理積で結合した式が活動状態対 (s_i, s_j) の mgb となる.

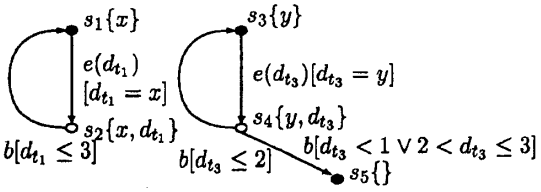

図 2: $mgb(s_1, s_3) = [x = y \wedge 1 \le x \le 2]$ である状態対 (s_1, s_3)

式 (1) および式 (2) にしたがって，各休止状態対および活動状態対に対して文献 [3] と同様のアルゴリズムを適用すれば，mgb を再帰的に求めることができる. 繰り返しを含む無限プロセスに対しても，訪問済みの状態対をマークし，マーク済みの状態対に対しては *true* を返すようにすれば mgb が求められる (詳細は [5] 参照).

例 2 図 2の交替性 TSLTS の状態対 (s_1, s_3) に対して，$mgb(s_1, s_3)$ は以下のように求められる.

$mgb(s_1, s_3) = \forall d_1[d_1 = x \Rightarrow [d_1 = y \wedge M_{24}]] \wedge \forall d_1[d_1 = y \Rightarrow [d_1 = x \wedge M_{24}]]$ ただし，M_{24} $[d_1 \le 3 \Rightarrow [d_1 \le 2 \wedge M_{13} \vee (d_1 < 1 \vee 2 < d_1 \le 3) \wedge M_{15}]] \wedge [d_1 \le 2 \Rightarrow [d_1 \le 3 \wedge M_{13}\,]]$ $[(d_1 < 1 \vee 2 < d_1 \le 3) \Rightarrow [d_1 \le 3 \wedge M_{15}]]$, $M_{13} = mgb(s_1, s_3)$ $M_{15} = false$. $mgb(s_1, s_3)$ は上の連立方程式の解になるが，[5] に示すアルゴリズムによって解 $mgb(s_1, s_3)$ を求めることが可能である. その解は簡約化すれば，$mgb(s_1, s_3) \equiv [x = y] \wedge [1 \le x \le 2]$ となる. □

5 あとがき

本稿では，時間的性質を記述可能なプロセスのモデル，交替性 TSLTS を提案し，時間性を考慮した双模倣等価性を [3] と同様の手法によって状態爆発を回避して判定できることを示した.

なお，[5] では本稿の結果をさらに押し進めて，仕様記述言語 LOTOS を時間制約を記述できるように拡張した言語 LOTOS/T の記述から交替性 TSLTS への変換法を与え，本稿の結果がプロセスを構造的に記述する言語にも適用可能であることを示している.

今後の課題は，内部動作を考慮した等価性判定ができるように拡張することと，等価性判定アルゴリズムを計算機に実装し，実際的な十分大きなプロセスの記述に対して，等価性判定の効率を定量的に評価することである.

参考文献

[1] ALUR, R., COURCOUBETIS, C. and HENZINGER, T. A. The Observational Power of Clocks, Proc. of CONCUR'94, LNCS 836, Springer-Verlag (1994).

[2] ĆERĀNS, K. Decidability of bisimulation equivalence for parallel timer processes, Proc. of 4th CAV, LNCS 663, Springer-Verlag (1992).

[3] HENNESSY, M. and LIN, M. Symbolic bisimulations, *Theoret. Comput. Sci.*, **138** (1995), 353–389.

[4] HOLMER, U., LARSEN, K. and WANG, Y. Deciding properties of regular timed processes, Proc. of 3rd CAV, LNCS 575, Springer-Verlag (1991).

[5] NAKATA, A., HIGASHINO, T. and TANIGUCHI, K. Time-Action Alternating Model for Timed LOTOS and its Sympolic Verification of Bisimulation Equivalence, Proc. of FORTE/PSTV'96, Chapman & Hall (Oct. 1996), to appear.