数理解析研究所講究録
950巻 1996年 200-206

1996年2月2日 冬のLAシンポジウム
於：京都大学数理解析研究所

時間値による状態爆発を回避した時間的双模倣等価性検証法

中田 明夫　東野 輝夫　谷口 健一
Akio NAKATA　Teruo HIGASHINO　Kenichi TANIGUCHI
大阪大学 基礎工学部 情報工学科
E-mail:{nakata,higashino,taniguchi}@ics.es.osaka-u.ac.jp

あらまし
時間制約付きプロセスの双模倣等価性の検証は，遅延による状態遷移を各値毎に分けることによって，時間を考慮しない場合に帰着して行うことができるが，遅延の値毎に状態を分けたことによる状態爆発により現実には困難であった．そこで我々は，計算量が遅延の具体的な値に依存しない手法によって，時間制約付きプロセス代数の時間的双模倣等価性を検証する手法を提案する．本提案ではモデルとして，遅延量を一つの記号で代表させる交替性時間付き記号的LTS(交替性TSLTS)を考える．交替性TSLTSの各状態はパラメータ変数を持ち，それらの変数への具体的な値の代入に対して動きが定まる．提案する手法では交替性TSLTSの状態対に対してそれらの動きが時間的双模倣等価となるような代入が満たすべき最も弱い条件mgbを出力する．

1 まえがき

時間性が記述可能なプロセス代数の体系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[1, 2, 3]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，時間制約付CCSを対象とした文献[1],Timed Automata[4]を対象にした文献[2, 3]の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[5]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．

提案する方法は，以下の2ステップから構成される：

1. 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$x+5$秒からy秒後までに動作aを実行する，などといった変数を用いた条件を記述できる．データの入出力は本稿では考慮しない．
2. 文献[5]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[5]と呼ぶ)を求める．その条件式が恒真なら任意のパラメータ値に関して時間的双模倣等価である．また，充足可能ならば2状態を時間的双模倣等価にするようなパラメータ値の決め方が存在する．充足不能ならばそれらは決して時間的双模倣等価にはならない．

例えば$x+5$秒後～y秒後までならaを実行し，y秒後～$x+10$秒後までならbを実行するプロセスPと，10秒後～z秒後までにaを実行するプロセスQが時間的双模倣等価であるためには“$(x+5=10)\wedge(y=z)\wedge(y>x+10)$”なる条件が成り立つ必要がある(“$(y>x+10)$”なら$b$は実行不能)．一方,$P$,$Q$が時間的双模倣等価とはならないようなどんな$x,y,z$の値に対してもこの条件は成り立たない．このような条件式が求めるmgbである．提案する手法ではP,Qが再帰を含むような無限プロセスであっても，対応するTSLTSが有限ならmgbを求めることが出来る．mgbが求まれば，その状態対が与えられた代入に対して時間的双模倣等価であるか否かの判定は，代入がmgbを充足するか否かの判定に帰着される．

まず最初に，時間による状態遷移をモデル化する方法を考える．我々は [1] などにみられるように, 遅延量を表す変数 d をパラメータとして持つような遅延遷移$\xrightarrow{e(d)}$を採用する．この表現法は, 時間を (遅延量が入力されるとみなすことによって) 入出力データと同等に扱うことができるので，本稿では時間のみを扱うが，時間とデータを同時に扱うモデルへも容易に拡張できる．また, 各遅延遷移$\xrightarrow{e(d)}$および動作による遷移$\xrightarrow{a}$には, その遷移を実行可能とする条件として, 一般に遅延量変数 d およびパラメータ変数 (過去の遅延遷移における遅延量変数を含む) を用いた論理式を記述できる．このように時間性を扱えるように LTS を拡張したモデルを Timed Symbolic Labelled Transition System(TSLTS) と呼ぶ．

TSLTS で文献 [5] 同様の symbolic bisimulation を考えたとき，次の問題を生じる．すなわち，遅延量 d の遅延遷移$\xrightarrow{e(d)}$は$\xrightarrow{e(d_1)}\xrightarrow{e(d_2)}\cdots\xrightarrow{e(d_n)}(d_1+d_2+\cdots+d_n=d)$ なる遷移系列と等価であるため，双模倣関係の構成にあたり 2 つのプロセスの遷移の対応関係をとるとき，遅延遷移に関しては一般に不定長の系列間の対応をとる必要が生じる．そこで，我々はプロセスのモデルを以下に示すような交替性を持つものに制限することによって，この問題を回避する．つまり，プロセスの状態を休止状態 (idle state) と活動状態 (active state) に 2 分割する．プロセスは休止状態からは遅延遷移のみが可能で，必ず活動状態に遷移する．逆に活動状態からは遅延遷移以外の遷移のみが可能で，必ず休止状態に遷移する．この制限によって，双模倣関係を構成するときの遅延遷移の対応を 1 対 1 にすることができる．なお，モデルを交替性に制限しても, ゼロ遅延を許すことによって，表現可能なプロセスのクラスは変化しない．

提案するモデル, 交替性 TSLTS に対して文献 [5] と同様のアルゴリズムを適用することによって, 状態対に対してそれらを時間的記号双模倣等価にする最弱の条件を求めることができる．さらに，我々は本手法が動作の生起時刻が一致しなくても良い双模倣等価性，非時間的双模倣等価性の判定法へも容易に拡張可能であることを示す．

本稿は以下のように構成される．まず，2章では時間制約を持つプロセスのモデルである交替性 TSLTS の定義を述べる．3章では, 交替性 TSLTS に対して時間的双模倣等価性を定義する．4章では，交替性 TSLTS においては時間的双模倣等価性の判定が文献 [5] と同様のアルゴリズムに帰着されることを示す．5章では，非時間的双模倣等価性の判定への拡張について述べる．6章では本稿の結論を述べる．

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)．遅延は Pを満たす d の値の最大値まで可能で，それを越えて時間が経過することはできない (time-deadlock[6], urgency[7])．また，遅延終了時には状態 s' 以降のパラメータ変数 d には Pを満たす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 (interleaving semantics[8, 9])．状態 s から遷移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．

例 1　図 1に TSLTS の例を示す．図において各状態には便宜上 $s_1, s_2, \ldots$ の順に，各遷移には $t_1, t_2, \ldots$ の順に名前を振ってある．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．各遷移名の隣には $a[P]$(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．　□

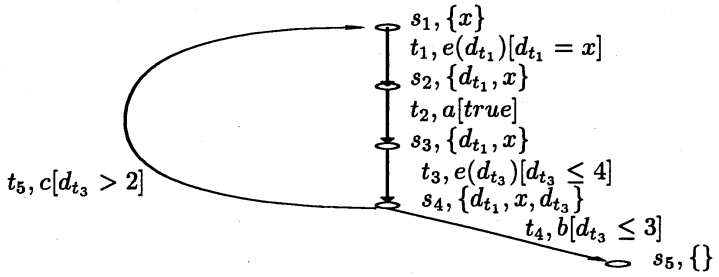

図 1: TSLTS の例

TSLTS では連続した遅延遷移が 1 つの遅延遷移と対応することがあり，そのままでは双模倣性を考えることが難しい．そこで，連続した遅延遷移を行えないように，状態を休止状態 (idle state) および活動状態 (active state) に 2 分割し，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とした TSLTS のサブセットを考え，これを交替性 TSLTS と呼ぶ．なお，交替性 TSLTS の着想は文献 [10] から得た．

以下の議論では TSLTS はすべて交替性であること, および，時間決定的 (time-deterministic), すなわち，各状態から出る遅延遷移はたかだか 1 本であることを仮定する．時間決定性は現実のプロセスを考える上で妥当な仮定であり，他の多くの研究もこれを仮定している [6, 8, 9]．

例 2　例 1の TSLTS は，休止状態：$\{s_1, s_3, s_5\}$, 活動状態：$\{s_2, s_4\}$ の分割が可能なので，交替性 TSLTS である．また，例 1の TSLTS は時間決定的でもある．　□

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．その前に幾つかの準備を行う．

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．　□

TSLTS の操作的意味は, 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, 以下のように形式的に定義される．

定義 2　TSLTS Mと代入ρに対して LTSM'を以下のように定義し，ρに関する Mの意味 LTS(semantic LTS) と呼ぶ:

- M'の状態集合は Mの全ての状態のインスタンスの全体 $\{\rho(s)|s$:状態, ρ:代入 $\}$ である．
- M'の遷移のラベルは Mの任意の動作名 a または任意の非負の時間値 t である．
- Mの遷移 $s \xrightarrow{a,P} s'$と，代入ρに対して，$\rho \models P$ならば M'は遷移$\rho(s) \xrightarrow{a} \rho(s')$ を持つ．
- Mの遷移 $s \xrightarrow{e(d),P} s'$と任意の時間値 t に対して, $\rho[d = t] \models \exists d'[d \leq d' \wedge P\{d'/d\}]$ ならば,M'は遷移 $\rho(s) \xrightarrow{t} \rho[d = t](s')$ を持つ ($P\{d'/d\}$ は Pに現れる自由変数 d を d'で置き換えた式)．さらに,$t' \leq t$ なる任意の時間値 t'に対して，M'は遷移$\rho[d = t'](s') \xrightarrow{t-t'} \rho[d = t](s')$ を持つ．　□

定義 2のように遅延量が関連づけられた状態遷移を考えた実時間プロセスのモデル化は [8, 9] などと同様のものである．

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 3 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:
  - 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 $(\rho_i'(s_i'), \rho_j'(s_j')) \in R$,
  - 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. また, 特に$\rho(s_i) \sim_t \rho(s_j)$ ならば, 状態 s_i,s_jは代入 ρに関して時間的双模倣等価であるということにする. □

4 等価性判定

交替性 TSLTS の状態対 (s_i, s_j) に対して$\rho \models P$ならば,$\rho(s_i) \sim_t \rho(s_j)$ であるような最も弱い条件 P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各遅延遷移は遅延量も含めて 1 対 1 に対応する. 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 $s_i \xrightarrow{e(d_i), d_i \leq x} s_i'$,$s_j \xrightarrow{e(d_j), d_j \leq y} s_j$ならば $\forall d[d \leq x \Rightarrow [d \leq y \wedge ((s_i'[d_i \to d], s_j'[d_j \to d])$ 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.

一方,s_iと s_jが等価とならない変数の値に対しては, s_iは s_jには不可能な値の遅延が可能であるか, あるいは,s_i',s_j'が等価にならないかのどちらかであり, いずれにせよ, 式 (1) は成り立たない. したがって式 (1) は休止状態対 s_iと s_jを等価にするような最も弱い条件, つまり mgb である.

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 [5].

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

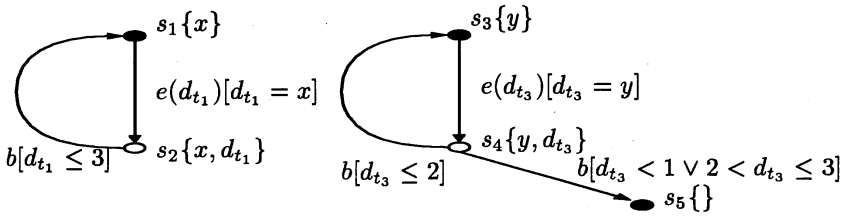

図 2: $mgb(s_1, s_3) = [x = y \wedge 1 \leq x \leq 2]$ である状態対 (s_1, s_3)

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

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

と表せる [5]. 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. 一方,s_iと s_jが等価でなくなるような変数の値に関しては, ある動作 a に関して例えば遷移 $s_i \xrightarrow{a,P_k} s_{i_k}$が実行可能で, かつ, 任意の lに関して $s_j \xrightarrow{a,Q_l} s_{j_l}$が実行不能であるか遷移先 (s_{i_k}, s_{j_l}) が等価でないかのどちらかが成り立つはずである. この場合, 式 (2) は満足されない. したがって式 (2) は動作 a に関して活動状態対 (s_i, s_j) を等価にするような最も弱い条件, つまり mgb である. 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.

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 [5] 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 (文献 [5] 参照). 状態対のマークなどを含めたアルゴリズムの詳細は付録に示す.

例 3　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,

$$\begin{aligned} M_{24} &= [d_1 \leq 3 \Rightarrow [d_1 \leq 2 \wedge M_{13} \vee (d_1 < 1 \vee 2 < d_1 \leq 3) \wedge M_{15}]] \wedge \\ &\quad [d_1 \leq 2 \Rightarrow [d_1 \leq 3 \wedge M_{13}]] \wedge [(d_1 < 1 \vee 2 < d_1 \leq 3) \Rightarrow [d_1 \leq 3 \wedge M_{15}]], \\ M_{13} &= mgb(s_1, s_3) \\ M_{15} &= false. \end{aligned}$$

$mgb(s_1, s_3)$ は上の連立方程式の解になるが, 文献 [5] と同様にして解 $mgb(s_1, s_3)$ を求めることが可能である. その解は簡約化すれば, $mgb(s_1, s_3) \equiv [x = y] \wedge [1 \leq x \leq 2]$ となる. □

5　非時間的双模倣等価性およびその検証

時間制約の指定されたシステムの検証において, 動作のタイミングを変更しても, 動作の系列や実行可能性が変化しないか否かを判定することも有用である. そこで本節では前節の結果を拡張し, 動作の生起時刻が一致しなくても等価とみなす, 非時間的双模倣等価性の判定法を示す.

まず, 非時間的双模倣等価性を以下に正確に定義する.

定義 4　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で以下の条件を満足するものを非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:
  - 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, ある時間値 t', および, ある s'_j,ρ'_jが存在して$\rho_j(s_j) \xrightarrow{t'} \rho'_j(s'_j)$ かつ $(\rho'_i(s'_i), \rho'_j(s'_j)) \in R$,
  - 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, ある非時間的双模倣関係 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$\rho_j(s_j)$ は非時間的双模倣等価であると定義し,$\rho_i(s_i) \sim_u \rho_j(s_j)$ と表記する. □

前節までの結果は, 非時間的双模倣等価性の判定に容易に拡張可能である. そのためには, 遅延遷移の対応をとるときに遅延量が等しくなくてもよいように 式 (1) を以下のように変更すれば良い.

$$\forall d[P_i\{d/d_i\} \Rightarrow \exists d'[P_j\{d'/d_j\} \wedge M_{i',j'}]] \wedge \forall d'[P_j\{d'/d_j\} \Rightarrow \exists d[P_i\{d/d_i\} \wedge M_{i',j'}]] \quad (3)$$

ただし,d と d'は互いに異なる変数で, ともに $DVar(s_i) \cup DVar(s_j)$ に属さない新しい変数とする.

例 4　図 2の交替性 TSLTS の状態対 (s_1, s_3) に対して, 非時間的双模倣等価性に関する $mgb(s_1, s_3)$ は以下のように求められる.

$$mgb(s_1, s_3) = \forall d_1[d_1 = x \Rightarrow \exists d'_1[d'_1 = y \wedge M_{24}]] \wedge \forall d'_1[d'_1 = y \Rightarrow \exists d_1[d_1 = x \wedge M_{24}]]$$

ただし,

$$\begin{aligned} M_{24} &= [d_1 \leq 3 \Rightarrow [d'_1 \leq 2 \wedge M_{13} \vee (d'_1 < 1 \vee 2 < d'_1 \leq 3) \wedge M_{15}]] \wedge \\ &\quad [d'_1 \leq 2 \Rightarrow [d_1 \leq 3 \wedge M_{13}]] \wedge [(d'_1 < 1 \vee 2 < d'_1 \leq 3) \Rightarrow [d_1 \leq 3 \wedge M_{15}]], \\ M_{13} &= mgb(s_1, s_3) \\ M_{15} &= false. \end{aligned}$$

文献 [5] と同様にして $mgb(s_1, s_3)$ を求め, 簡約化すれば,$mgb(s_1, s_3) \equiv [x \leq 3] \Leftrightarrow [1 \leq y \leq 2]$ となる. □

6　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 [5] 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.

時間的プロセスに対する他の提案と異なり, 我々の提案では時間制約の記述言語として任意の論理式の体系をとることが可能である. このことにより, 時間制約を非常に柔軟に記述することができ, なおかつ, 時間的双模倣等価性を条件に現れる定数の絶対値に依存しないコストで判定することができる. また, TSLTS の通常動作に入出力値を持たせるように拡張すれば, 時間とデータを同時に扱える体系に対しても時間的双模倣等価性の判定が行えるように容易に拡張可能であると考える.

なお, [11] で提案した LOTOS/T などのように, 時間制約を持つプロセスを構造的に記述する言語に対しても本稿の結果を応用可能である. この場合, 言語の記述から交替性 TSLTS への変換規則を与えればよい.

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.

付録: mgb 導出アルゴリズム

時間的双模倣等価性に関する mgb は以下のアルゴリズムによって求めることが出来る.

$mgb(s_i, s_j) \stackrel{\text{def}}{=} mgb1(s_i, s_j, \emptyset)$

$mgb1(s_i, s_j, W) \stackrel{\text{def}}{=}$ if $(s_i, s_j) \in W$ then return true
else if (s_i, s_j) が休止状態対 then return $match\_delay(s_i, s_j, W)$
else if (s_i, s_j) が活動状態対 then return $match\_action(s_i, s_j, W)$
else return false

$match\_delay(s_i, s_j, W) \stackrel{\text{def}}{=}$ if $s_i \stackrel{e(d_i),P_i}{\longrightarrow} s_{i'}$ and $s_j \stackrel{e(d_j),P_j}{\longrightarrow} s_{j'}$
then let $\{d = new(DVar(s_i) \cup DVar(s_j)),$
$M_{i',j'} = mgb1(s_{i'}[d_i \to d], s_{j'}[d_j \to d], W \cup \{(s_i, s_j)\})\}$ in
return $\forall d[P_i\{d/d_i\} \Rightarrow [P_j\{d/d_j\} \wedge M_{i',j'}]] \wedge \forall d[P_j\{d/d_j\} \Rightarrow [P_i\{d/d_i\} \wedge M_{i',j'}]]$
else if $s_i \stackrel{e(d_i),P_i}{\not\longrightarrow}$ and $s_j \stackrel{e(d_j),P_j}{\not\longrightarrow}$ then return true else return false

$match\_action(s_i, s_j, W) \stackrel{\text{def}}{=}$ return $\bigwedge_{a \in Act}\{match\_action1(a, s_i, s_j, W)\}$

$match\_action1(a, s_i, s_j, W) \stackrel{\text{def}}{=}$ let $\{K = \{k | s_i \stackrel{a,P_k}{\longrightarrow} s_{i_k}\}, L = \{l | s_j \stackrel{a,Q_l}{\longrightarrow} s_{j_l}\},$
$M_{k,l} = mgb1(s_{i_k}, s_{j_l}, W \cup \{(s_i, s_j)\})\}$ in
return $\bigwedge_{k \in K}\{P_k \Rightarrow \bigvee_{l \in L}\{Q_l \wedge M_{k,l}\}\} \wedge \bigwedge_{l \in L}\{Q_l \Rightarrow \bigvee_{k \in K}\{P_k \wedge M_{k,l}\}\}$

ただし，変数集合 V に対して $new(V)$ を V に含まれない適当な新しい変数を返す関数とする．
また，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．

また，非時間的双模倣等価性に関しては上の関数 $match\_delay(s_i, s_j, W)$ を以下のように変更すれば良い．

$match\_delay(s_i, s_j, W) \stackrel{\text{def}}{=}$ if $s_i \stackrel{e(d_i),P_i}{\longrightarrow} s_{i'}$ and $s_j \stackrel{e(d_j),P_j}{\longrightarrow} s_{j'}$
then let $d = new(DVar(s_i) \cup DVar(s_j)),\ d' = new(DVar(s_i) \cup DVar(s_j) \cup \{d\}),$
$M_{i',j'} = mgb1(s_{i'}[d_i \to d], s_{j'}[d_j \to d'], W \cup \{(s_i, s_j)\})$ in
return $\forall d[P_i\{d/d_i\} \Rightarrow \exists d'[P_j\{d'/d_j\} \wedge M_{i',j'}]] \wedge \forall d'[P_j\{d'/d_j\} \Rightarrow \exists d[P_i\{d/d_i\} \wedge M_{i',j'}]]$
else if $s_i \stackrel{e(d_i),P_i}{\not\longrightarrow}$ and $s_j \stackrel{e(d_j),P_j}{\not\longrightarrow}$ then return true else return false

参考文献

[1] Holmer, U., Larsen, K. and Wang, Y.: "Deciding properties of regular timed processes", Proc. of 3rd CAV, Vol. 575 of Lecture Notes in Computer Science, Springer-Verlag, pp. 443–453 (1991).

[2] Ćerāns, K.: "Decidability of bisimulation equivalence for parallel timer processes", Proc. of 4th CAV, Vol. 663 of Lecture Notes in Computer Science, Springer-Verlag, pp. 302–315 (1992).

[3] Alur, R., Courcoubetis, C. and Henzinger, T. A.: "The observational power of clocks", Proc. of CONCUR'94, Vol. 836 of Lecture Notes in Computer Science, Springer-Verlag, pp. 162–177 (1994).

[4] Alur, R. and Dill, D.: "Automata for modelling real-time systems", Proc. of ICALP'90 (Ed. by Paterson, M. S.), Vol. 443 of Lecture Notes in Computer Science, Springer-Verlag, pp. 322–335 (1990).

[5] Hennessy, M. and Lin, M.: "Symbolic bisimulations", Theoret. Comput. Sci., **138**, pp. 353–389 (1995).

[6] Moller, F. and Tofts, C.: "A temporal calculus of communicating systems", Proc. of CONCUR '90 (Eds. by Baeten, J. C. M. and Klop, J. W.), Vol. 458 of Lecture Notes in Computer Science, Springer-Verlag, pp. 401–415 (1990).

[7] Bolognesi, T. and Lucidi, F.: "LOTOS-like process algebras with urgent or timed interactions", Formal Description Techniques, IV (Eds. by Parker, K. R. and Rose, G. A.), IFIP, Elsevier Science Publishers B.V.(North-Holland), pp. 249–264 (1992).

[8] Wang, Y.: "CCS + time = an interleaving model for real time systems", Proc. of ICALP '91 (Eds. by Leach Albert, J., Monien, B. and Rodríguez Artalejo, M.), Vol. 510 of Lecture Notes in Computer Science, Springer-Verlag, pp. 217–228 (1991).

[9] Chen, L.: "An interleaving model for real-time systems", Proc. of 2nd Int'l Symp. on Logical Foundations of Computer Science — Tver'92 (Eds. by Nerode, A. and Taitslin, M.), Vol. 620 of Lecture Notes in Computer Science, Springer-Verlag, pp. 81–92 (1992).

[10] Hansson, H. A.: "Time and Probability in Formal Design of Distributed Systems", Ph.D thesis DoCS 91/27, Dept. of Computer Systems, Uppsala University (1991).

[11] Nakata, A., Higashino, T. and Taniguchi, K.: "LOTOS enhancement to specify time constraints among nonadjacent actions using first order logic", Formal Description Techniques, VI (FORTE'93) (Eds. by Tenney, R. L., Amer, P. D. and Uyar, M. Ü.), IFIP, Elsevier Science Publishers B.V. (North-Holland), pp. 451–466 (1994).