離散確率分布を持つリアルタイムシステムの確率時間時相論理式の演繹的検証手法

山根 智†

近年，世界中で，リアルタイムシステムの仕様記述と検証の研究は大変にさかんであり，タイミング制約が記述可能な時間オートマトン，およびその検証手法としてもモデル検査手法などが開発されている．また，最近，リアルタイムシステムの不確かな動作を表現するために，離散確率分布を持つ確率時間オートマトンが開発されており，そのモデル検査手法や確率時間模倣検証手法も開発されている．本論文では，確率時間オートマトンを一般化することにより，確率時間遷移システムを開発して，その上に，確率時間時相論理の演繹的な検証規則を開発する．確率時間遷移システムは離散確率分布を持つリアルタイムシステムの一般的な計算モデルであり，従来よりも一般的な検証手法が確立できた．

Deductive Verification Method of Probabilistic Timed LTL of Real-time Systems with Discrete Probability Distributions

Satoshi Yamane†

Many people have studied formal specification and verification methods of real-time systems all over the world. We can specify real-time systems using timed automata, and verify them using model-checking. Especially, recently, probabilistic timed automata and their model-checking have been developed in order to express the relative likelihood of the system exhibiting certain behavior. Moreover, model-checking and probabilistic timed simulation verification methods of probabilistic timed automata have been developed. In this paper, we propose probabilistic timed transition system by generalizing probabilistic timed automata, and propose deductive verification rules of probabilistic timed temporal logic over probabilistic timed transition system. As our proposed probabilistic timed transition system is a general computational model, we have developed general verification method.

1. まえがき

近年，マイクロプロセッサの99%以上は組み込み型システムに使われており，組み込み型システムのほとんどはリアルタイムシステムである．リアルタイムシステムは非常に重要な計算機システムのパラダイムである．リアルタイムシステムはリアルタイムオペレーティングシステムとともに動作して，信頼性保証が難しいシステムであり，仕様記述と検証は重要である[1]．近年，世界中で，リアルタイムシステムの仕様記述と検証の研究は大変にさかんであり[2)~4)]，リアルタイムシステムの仕様記述言語としては，タイミング制約が記述可能な時間オートマトン[5]が定着しており，その検証手法としてもモデル検査手法[6),7)]などが開発されている．一方，最近，不確かな動作を表現するために，離散確率分布を持つ確率時間オートマトンが開発されており，そのモデル検査手法[8]や確率時間模倣検証手法[9]が開発されている．本論文では，確率時間オートマトンを一般化することにより，確率時間遷移システムを開発して，その上に，確率時間時相論理の演繹的な検証規則を開発する．確率時間遷移システムは離散確率分布を持つリアルタイムシステムの一般的な計算モデルであり，従来よりも一般的な検証手法が確立できる．

まず，以下では，確率システムやリアルタイムシステムの時相論理の形式的検証に関する，重要な既存の研究を以下に述べる．

(1) 1982年，A. Pnueli らは整礎順序集合を用いて，確率並行プログラムの活性の検証手法を提案したが，独立した原理のみを述べており，完全な検証問題の部分的な解決にしかなっていな

† 金沢大学工学部情報システム工学科
Department of Information and System Engineering, Kanazawa University

い[10]．この検証手法は以下のように拡張された[11),12)]．

(a) まず，Sharir らは確率分岐時相論理を基礎とした検証システム[11]を開発した．

(b) 次に，Lehmann らはやや特殊な線形時相論理を基礎とした検証システム[12]を開発した．

(c) さらに，Pnueli は標準的な線形時相論理を基礎とした検証システム[13]を開発した．

以上を発展させて，1986 年，Pnueli らは標準的な線形時相論理を基礎として，マルチ並行プロセスの検証システム[14]を開発して，ダイニングフィロソファーなどの本格的な検証事例を示した．

(2) 1991 年，Hansson は離散時間確率プロセス代数の双模倣関係検証および離散時間確率時相論理のモデル検査を初めて提案した[15]．この研究はプロセス代数を確率と離散時間で拡張して，その検証アルゴリズムを定義したものである．

(3) 1991 年，Alur らは稠密時間で確率システムを拡張した確率時間オートマトンを提案して，そのモデル検査を提案した[16),17)]．彼らのモデルは一般化されたセミマルコフプロセスであり，確率システムをリアルタイムシステムへ拡張した画期的な研究である．

(4) 1995 年，Segala が分散システムの一般的なモデルとして著名な I/O オートマトンを確率で拡張した確率 I/O オートマトンの双模倣関係と模倣関係[18]の公理系を初めて提案した．これは，上記の成果を一般化して，一般的な確率システムのモデルにおいて，双模倣関係と模倣関係を定義した意義がある．現在では，確率システムの最も標準的な双模倣関係の定義として引用されている．

(5) 1996 年，Kesten らは時間オートマトンを一般化したクロック遷移システムを提案して，実時間時相論理の検証規則を提案した[19]．

(6) 1999 年，Kwiatkowska らが離散確率分布を持つ確率時間オートマトンを提案して，確率時間時相論理のモデル検査を初めて提案した[8]．その後，Yamane が確率時間模倣関係を提案したり[9]，Kwiatkowska らが IEEE 1394 FireWire Root Contention Protocol の仕様記述と検証へ適用している[20]．

本論文では，確率時間オートマトンを一般化することにより，確率時間遷移システムを開発して，その上に，確率時間時相論理の演繹的な検証規則を開発する．確率時間遷移システムは離散確率分布を持つリアルタイムシステムの一般的な計算モデルであり，従来よりも一般的な検証手法が確立できる．なお，確率時間オートマトンの証明的な検証が未解決問題あることは，最近の Kwiatkowska の論文[21]においても指摘されている．

以降の本論文の構成は以下のとおりである．2 章では，確率時間オートマトンの一般的なモデルである確率時間遷移システムを定義する．3 章では，確率時間時相論理を定義する．4 章では，確率時間時相論理の安全性の検証規則を定義する．5 章では，確率時間時相論理の活性の検証規則を定義する．最後に，6 章では，まとめと今後の課題を述べる．

2. 離散確率分布を持つリアルタイムシステム

本章では，まず，確率時間オートマトン[8]を一般化して，確率時間遷移システムを定義する．

2.1 確率時間遷移システム

まず，離散確率分布を定義する．

Definition1（離散確率分布）

集合 Q 上の離散確率分布の集合を $\mu(Q)$ と表す．各 $p \in \mu(Q)$ は関数 $p : Q \to [0,1]$ である．ただし，$\sum_{q \in Q} p(q) = 1$ である．

■

次に，確率時間遷移システムを定義する．

まず，システム変数の有限集合を考える．システム変数は整数や実数などの型を持つ．我々はシステム変数にその型の値を割り付ける解釈として状態 s を定義する．すべての状態の集合を Σ とする．

Definition2（確率時間遷移システム）

確率時間遷移システムは，$\mathbf{PTS} = (V, \Theta, prob, \Pi)$ の 4 つ組で定義される．ここで，

(1) V：システム変数の有限集合．集合 $V = D \cup C$ は，離散変数の集合 $D = \{u_1, \ldots, u_n\}$ とクロック変数の集合 $C = \{t_1, \ldots, t_m, T\}$ に分類できる．離散変数は任意の型がありうるが，連続変数は実数型である．なお，$T \in C$ はリセットされないマスタクロックである．

(2) Θ：初期条件．これは，すべての初期状態を特徴付ける表明である．$\Theta \to t_1 = \ldots = t_m = T = 0$ が要求される．

(3) $prob$：状態遷移の有限集合．関数 $prob : \Sigma \to 2^{\mu(\Sigma)}$ であり，各状態 $s \in \Sigma$ に離散確率分布の集合 $\mu(\Sigma)$ の部分集合を写像する．ただし，すべて

の状態の集合を Σ とする．ここで，$p \in prob(s)$ とすると，$p(s\prime)$ の確率により，状態 s から状態 $s\prime$ に遷移する．この確率 $p(s\prime)$ による状態遷移 $\tau_{p(s\prime)}$ に関連する関数は一階述語論理の表明 $\rho_{\tau_{p(s\prime)}}(V, V\prime)$ により表現される．ただし，$V\prime$ は状態 $s\prime$ におけるシステム変数を表し，V は状態 s におけるシステム変数を表す．$\rho_{\tau_{p(s\prime)}}(V, V\prime)$ は状態遷移関係と呼び，状態 $s \in \Sigma$ を $\tau_{p(s\prime)}$-successor $s\prime \in \tau_{p(s\prime)}(s)$ に関係付ける．ただし，状態 s は V の型整合解釈であり，各変数 $v \in V$ に値 $s[v]$ を割り付ける．なお，システム変数の値は s の中の値や $s\prime$ の中の値として参照する．また，状態遷移 $\tau_{p(s\prime)}$ の集合を $\mathcal{T}$ とする．任意の $\tau_{p(s\prime)} \in \mathcal{T}$ に対して，$\rho_\tau \rightarrow T\prime = T$ が要求される．ただし，$T\prime$ は状態 $s\prime$ におけるマスタクロックを表し，T は状態 s におけるマスタクロックを表す．

(4) Π：時間前進条件．これは時間前進の制限を表現するために使われる．つまり，状態に割り付けられた変数の制約条件である．

■

また，確率時間遷移システム $\mathbf{PTS} = (V, \Theta, prob, \Pi)$ に対して，以下のように，状態遷移の集合 $\mathcal{T}$ を $\mathcal{T}_H$ に拡張する：

Definition3（拡張確率時間遷移システム）

確率時間遷移システム $\mathbf{PTS} = (V, \Theta, prob, \Pi)$ に対して，以下のように，状態遷移の集合 $\mathcal{T}$ を $\mathcal{T}_H$ に拡張する：

$\mathcal{T}_H = \mathcal{T} \cup tick.$

$tick$ の状態遷移関係は以下のように与えられる：

$\rho_{tick} : \exists \triangle > 0.\Omega(\triangle) \wedge D\prime = D \wedge C\prime = C + \triangle$

なお，$\Omega(\triangle)$ は以下のように定義される：

$\Omega(\triangle) : \triangle > 0 \wedge \forall t \in [0, \triangle).\Pi(D, C + t).$

ここで，$D = \{u_1, \ldots, u_m\}$ は離散変数の集合であり，$C = \{t_1, \ldots, t_k, T\}$ はクロック変数の集合である．$C\prime = C + \triangle$ は

$t_1\prime = t_1 + \triangle \wedge \ldots \wedge t_k\prime = t_k + \triangle \wedge T\prime = T + \triangle$

を意味して，$\Pi(D, C + t)$ は

$\Pi(u_1, \ldots, u_m, t_1 + t, \ldots, t_k + t, T + t)$

を意味する．■

次に，パスを定義する．

Definition4（パス）

確率時間遷移システムのパスは，非決定的な選択と確率的な選択の両方を解決することによって，発生する．確率時間遷移システムのパスは非空な無限なシーケンスであり，以下のとおりである．

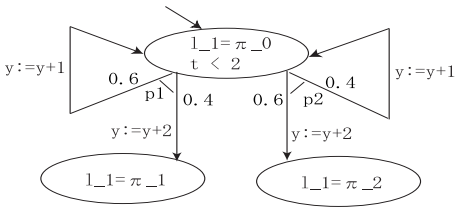


図 1 確率時間遷移システムの例—その 1

Fig. 1 Example of probabilistic timed transition system—part 1.

$$\omega = s_0 \xrightarrow{p_0} s_1 \xrightarrow{tick_1} s_2 \xrightarrow{p_2} s_3 \xrightarrow{tick_3} s_4 \ldots\ldots$$

ここで，$s_i \in \Sigma$ であり，確率の状態遷移のときは $s_i \in \tau_{p_{i-1}(s_i)}(s_{i-1})$ であり，$tick_{i-1}$ の状態遷移のときは $s_i = s_{i-1} + \triangle_{i-1}$ である．ただし，$s_i = s_{i-1} + \triangle_{i-1}$ はクロック変数の集合のみを $\triangle_{i-1}$ 増加させて，離散変数の集合は変化しないことを意味する．なお，パス ω の k 番目の状態を $\omega(k)$ と表記する．

$Path_{fin}$ は有限なパスの集合であり，$Path_{fin}(s)$ は $\omega(0) = s$ なる $Path_{fin}$ の中のパスの集合である．$Path_{ful}$ は無限なパスの集合であり，$Path_{ful}(s)$ は $\omega(0) = s$ なる $Path_{ful}$ の中のパスの集合である．

また，確率時間遷移システムのパス ω は以下の条件を満たす：

(1) 初期条件：$s_0 \models \Theta$.

(2) 連続条件：

(a) 確率の状態遷移のときは，任意の $\tau_{p_j(s_{j+1})} \in \mathcal{T}$ に対して，$s_{j+1} \in \tau_{p_j(s_{j+1})}(s_j)$ である．

(b) $tick$ の状態遷移のときは，$s_i = s_{i-1} + \triangle_{i-1}$ である．

(3) 時間の発散性：列 $s_0[T]$,$s_1[T]$,...,$s_i[T]$,... は際限なく大きくなる．ただし，$s_i[T]$ は状態 s_i における T の値である．

■

Example1（確率時間遷移システムの事例）

図 1 に確率時間遷移システムの例を示す．ロケーション l_0 からロケーション l_1 へは確率 0.6 で遷移して，ロケーション l_0 からロケーション l_0 へは確率 0.4 で遷移する．ここで，図 1 の確率時間遷移システム $\mathbf{PTS} = (V, \Theta, prob, \Pi)$ の各組を定義する：

(1) $V = \{\pi, y, t, T\}$.

(2) $\Theta : \pi = l_0 \wedge y = t = T = 0.$

(3) $\mathcal{T} : \{\tau_{p(\pi=l_0)}, \tau_{p(\pi=l_1)}\}$.

(a) $\rho_{\tau_{p(\pi=l_0)}} : \pi = \pi\prime = l_0 \wedge y\prime = y+1 \wedge t\prime = t \wedge T\prime = T$

(b) $\rho_{\tau_{p(\pi=l_1)}} : \pi = l_0 \wedge \pi\prime = l_1 \wedge y\prime = y+2 \wedge t\prime = t \wedge T\prime = T$

(4) $\Pi : \pi = l_0 \rightarrow t < 2.$

ここで，$tick$ の状態遷移関係は以下のように定義できる：

$$\rho_{tick} : \exists \triangle > 0.\pi\prime = \pi \wedge y\prime = y \wedge t\prime = t+\triangle \wedge T\prime = T+\triangle \wedge \pi = l_0 \rightarrow t+\triangle \leq 2$$

この確率時間遷移システムには，以下のようなパスが存在する：

$$< \pi : l_0, y : 0, t : 0, T : 0 > \stackrel{tick(1)}{\longrightarrow}$$
$$< \pi : l_0, y : 0, t : 1, T : 1 > \stackrel{\tau_{p(\pi=l_0)}}{\longrightarrow}$$
$$< \pi : l_0, y : 1, t : 1, T : 1 > \stackrel{tick(0.5)}{\longrightarrow}$$
$$< \pi : l_1, y : 1, t : 1.5, T : 1.5 > \stackrel{\tau_{p(\pi=l_1)}}{\longrightarrow}$$
$$< \pi : l_1, y : 3, t : 1.5, T : 1.5 > \stackrel{tick(0.5)}{\longrightarrow}$$
$$< \pi : l_1, y : 3, t : 2, T : 2 > \stackrel{tick(0.5)}{\longrightarrow} \ldots\ldots$$

ただし，$tick(0.5)$ は 0.5 時間の経過を意味する．

■

2.2 Adversary

確率時間遷移システムの非決定性を解決するために，Adversary[8] を導入する．非決定的選択と確率的選択の両方を含むシステムでは，この Adversary の概念は標準的なものであり，A. Pnueli[10] や Vardi[22] らにより提案された．

Definition5 （確率時間遷移システムの Adversary）

確率時間遷移システム $\mathbf{PTS} = (V, \Theta, prob, \Pi)$ の Adversary は $p \in prob(s)$ にすべてのパス ω を割り付ける関数 A である．なお，s は状態とする．ただし，$A(\omega) \in prob(last(\omega))$ であり，$last(\omega)$ は ω の最後の状態である．

■

確率時間遷移システム $\mathbf{PTS} = (V, \Theta, prob, \Pi)$ の Adversary A に対して，$Path^A_{fin}$ を有限のパスの集合とし，$Path^A_{ful}$ をパスの集合とする．

Adversary A によって，確率時間遷移システム **PTS** のパスの集合は逐次マルコフ連鎖と見なせる．形式的には，A が確率時間遷移システム **PTS** の Adversary ならば，$\mathbf{MC}^A$=$(Path^A_{fin}, \mathbf{P}^A)$ はマルコフ連鎖である．ここで，

$$\mathbf{P}^A(\omega, \omega\prime) = \begin{cases} p(s) & if\ A(\omega) = p\ and\ \omega\prime = \omega \stackrel{p}{\longrightarrow} s \\ 0 & otherwise. \end{cases}$$

任意の確率時間遷移システムに対して，$\mathcal{F}^{path}$ は以下の集合を含む $Path_{ful}$ 上の最小の σ-代数である：

すべての $\omega\prime \in Path_{ful}$ に対して

$\{\omega | \omega \in Path_{ful}$ であり，$\omega\prime$ は ω のプレフィックスである $\}$

ここで，σ-代数 $\mathcal{F}^{path}$ 上の測度 $Prob$ を定義する．まず，$Path_{ful}$ 上の関数を定義して，次に，測度 $Prob$ を定義する．

Definition6（関数 $Prob^A_{fin}$）

A を確率時間遷移システム **PTS** の Adversary とする．$Prob^A_{fin} : Path^A_{fin} \rightarrow [0,1]$ は $Path^A_{fin}$ の中のパスの長さ上で帰納的に定義される関数である．$Prob^A_{fin}$ は，以下のように定義される：

(1) $|\omega| = 0$ ならば，$Prob^A_{fin}(\omega) = 1$ である．

(2) $|\omega| \neq 0$ のときは以下である．$\omega\prime \in Path^A_{fin}$ は A のパスとする．もし，ある $\omega \in Path^A_{fin}$ に対して $\omega\prime = \omega \stackrel{p}{\longrightarrow} s$ ならば，

$$Prob^A_{fin}(\omega\prime) = Prob^A_{fin}(\omega) \cdot \mathbf{P}^A(\omega, \omega\prime)$$

である．

■

Definition7（測度 $Prob^A$）

$\mathcal{F}^{path^A}$ 上の測度 $Prob^A$ は以下のようなユニークな測度である：

$$Prob^A\{\omega | \omega \in path^A_{ful} \text{ かつ } \omega\prime \text{ は } \omega \text{ のプレフィックスである } \} = Prob^A_{fin}(\omega\prime).$$

■

Example2 （確率時間遷移システムのマルコフ連鎖の事例）

ある Adversary A に対して，図 1 の確率時間遷移システムのマルコフ連鎖 $\mathbf{MC}^A$=$(Path^A_{fin}, \mathbf{P}^A)$ を以下のように構成する．

(1) まず，

$$\omega = < \pi : l_0, y : 0, t : 0, T : 0 > \stackrel{tick(0.5)}{\longrightarrow} < \pi : l_0, y : 0, t : 0.5, T : 0.5 >$$

とする．

(2) 次に，$last(\omega) = < \pi : l_0, y : 0, t : 0.5, T : 0.5 >$ であり，$A(< \pi : l_0, y : 0, t : 0.5, T : 0.5 >) = p$ とする．

ただし，$\omega\prime = \omega \stackrel{p}{\longrightarrow} < \pi : l_0, y : 1, t : 0.5, T : 0.5 >$ と $p(< \pi : l_0, y : 1, t : 0.5, T : 0.5 >) = 0.4$ とする．

(3) 次に，$\omega\prime\prime = \omega\prime \stackrel{tick(1)}{\longrightarrow} < \pi : l_0, y : 1, t : 1.5, T : 1.5 >$ とする．

(4) 次に，$last(\omega\prime\prime) = < \pi : l_0, y : 1, t : 1.5, T : 1.5 >$ であり，$A(< \pi : l_0, y : 1, t : 1.5, T : 1.5 >) = p$ とする．

ただし，$\omega\prime\prime\prime = \omega\prime\prime \stackrel{p}{\longrightarrow} < \pi : l_1, y : 3, t :$

$1.5, T:1.5>$ と $p(<\pi:l_1, y:3, t:1.5, T:1.5>)=0.6$ とする．

(5) 次に，$\omega'''' = \omega''' \xrightarrow{tick(1)} <\pi:l_1, y:3, t:2.5, T:2.5>$ とする．

ゆえに，マルコフ連鎖 $\mathbf{MC}^A$=$(Path^A_{fin}, \mathbf{P}^A)$ は以下のとおりである：

(1) $Path^A_{fin} = <\pi:l_0, y:0, t:0, T:0> \xrightarrow{tick(0.5)} <\pi:l_0, y:0, t:0.5, T:0.5> \xrightarrow{p} <\pi:l_0, y:1, t:0.5, T:0.5> \xrightarrow{tick(1)} <\pi:l_0, y:1, t:1.5, T:1.5> \xrightarrow{p} <\pi:l_1, y:3, t:1.5, T:1.5> \xrightarrow{tick(1)} <\pi:l_1, y:3, t:2.5, T:2.5>$

(2) $\mathbf{P}^A$ は以下のように定義される：

(a) $\mathbf{P}^A(\omega, \omega') = 0.4$

(b) $\mathbf{P}^A(\omega', \omega''') = 0.6$

■

3. 確率時間線形時相論理

本章では，確率時間線形時相論理を導入する．我々は線形時相論理[23] のサブセットを時間と確率の概念で拡張する．

まず，確率時間線形時相論理の構文を定義する．

Definition8（確率時間線形時相論理の構文）

確率時間線形時相論理の構文は以下のように定義される：

(1) q は一階述語論理の表明であり，確率時間線形時相論理式である．

(2) $[\Box q]_{\sqsupseteq\lambda}$ は確率時間線形時相論理式である．ただし，q は一階述語論理の表明であり，$\lambda \in [0,1]$，$\sqsupseteq$ は $\geq$ または $>$ である．なお，$[\Box q]_{\sqsupseteq\lambda}$ の直感的な意味は，確率 $\sqsupseteq \lambda$ を満たして，つねに q が成り立つことである．

(3) $[\Box(q \rightarrow \Diamond r)]_{\sqsupseteq\lambda}$ は確率時間線形時相論理式である．ただし，q，r は一階述語論理の表明である．なお，$[\Box(q \rightarrow \Diamond r)]_{\sqsupseteq\lambda}$ の直感的な意味は，確率 $\sqsupseteq \lambda$ を満たして，つねに q が終局的に r を引き起こすことである．

■

次に，確率時間線形時相論理の意味を定義する．

Definition9（確率時間線形時相論理の意味）

確率時間遷移システム **PTS** および **PTS** の adversary の集合 $\mathcal{A}$ が与えられたとき，**PTS** の任意の状態 s と確率時間線形時相論理式 ϕ に対して，充足関係 $s \models_{\mathcal{A}} \phi$ は帰納的に定義される：

(1) $s \models_{\mathcal{A}} q$

$\Longleftrightarrow$

$s \models q$.

なお，$s \models q$ は表明 q が状態 s 上で成り立つことを意味する．

(2) $s \models_{\mathcal{A}} [\Box q]_{\sqsupseteq\lambda}$

$\Longleftrightarrow$

すべての $A \in \mathcal{A}$ に対して，

$Prob(\{\omega | \omega \in Path^A_{ful}(s)$, かつ，$\forall i$ に対して $\omega(i) \models_{\mathcal{A}} q\}) \sqsupseteq \lambda$.

(3) $s \models_{\mathcal{A}} [\Box(q \rightarrow \Diamond r)]_{\sqsupseteq\lambda}$

$\Longleftrightarrow$

すべての $A \in \mathcal{A}$ に対して，

$Prob(\{\omega | \omega \in Path^A_{ful}(s)$, かつ，すべての i に対して $\omega(i) \models_{\mathcal{A}} q$ は $j \geq i$ なる $\omega(j) \models_{\mathcal{A}} r$ が続く $\}) \sqsupseteq \lambda$.

■

次に，恒真と状態恒真の概念を定義する：

確率時間遷移システム **PTS** および **PTS** の adversary の集合 $\mathcal{A}$ が与えられたとき，**PTS** の任意の状態 s と任意の adversary $A \in \mathcal{A}$ に対して，$s \models_{\mathcal{A}} \phi$ ならば，確率時間線形時相論理式 ϕ は **PTS** 上で恒真であると呼ばれる．また，**PTS** の任意のアクセス可能な状態 s と任意の adversary $A \in \mathcal{A}$ に対して，$s \models_{\mathcal{A}} \phi$ ならば，確率時間線形時相論理式 ϕ は **PTS** 上で状態恒真であると呼ばれる．

4. 安全性の演繹的検証系

本章では，確率時間遷移システム上の安全性，すなわち，$[\Box q]_{\sqsupseteq\lambda}$ を検証する手法を述べる．我々は，Manna らのリアクティブシステムの安全性の検証手法[23] を拡張して，確率時間遷移システム上の安全性の検証手法を開発する．

最初に，安全性の演繹的検証系を定義する．

Definition10（安全性の演繹的検証ルール）

確率時間遷移システム $\mathbf{PTS} = (V, \Theta, prob, \Pi)$ のすべての Adversary A に対して，表明 φ と q について以下が成り立つ：

1. $\Theta \rightarrow \varphi$
2. $\varphi \rightarrow q$
3. $\forall \tau \in \mathcal{T}_H$ に対して以下が成り立つ：
   $\rho_\tau \wedge \varphi \rightarrow \varphi'$
4. $\forall \tau_{p(s')} \in \mathcal{T}$ に対して以下が成り立つ：
   $p \cdot p(s')$ で更新した p が $\sqsupseteq \lambda$ を満たす
   ただし，p の初期値は 1 である．
5. ――――――――――――――――――――――――
6. $[\Box q]_{\sqsupseteq\lambda}$

これは安全性を証明するルールであり，1，2，3，4 を満たすとき，6 のように $[\Box q]_{\sqsupseteq\lambda}$ が証明されることを意味する．なお，$\rho_\tau \wedge \varphi \rightarrow \varphi\prime$ は $\varphi\{\tau\}\varphi\prime$ を意味しており，$\varphi\prime$ は状態遷移 ρ_τ 後の状態 $s\prime$ における表明であり，φ のシステム変数の集合 V を $V\prime$ に変えたものである．

■

次に，安全性の演繹的検証ルールの健全性を述べる．

Theorem1（安全性の検証ルールの健全性）
確率時間遷移システム **PTS** 上において，安全性の検証ルールの前提条件が状態恒真であるならば，論理式 $[\Box q]_{\sqsupseteq\lambda}$ は恒真である．

Proof1 前提条件 1. が状態恒真であるので，初期状態において φ は成り立つ．前提条件 3. が状態恒真であるので，初期状態から遷移規則を適用すると，すべての **PTS** の状態において φ は成り立つ．また，前提条件 4. が成り立つので，確率の条件 $\sqsupseteq \lambda$ を満たす．また，前提条件 2. が状態恒真であるので，すべての状態において q は成り立つ．ゆえに，$[\Box q]_{\sqsupseteq\lambda}$ は恒真である．

■

次に，安全性の演繹的検証の事例を述べる．

Example3（安全性の演繹的検証の事例）
Example1 の確率時間遷移システムにおいて，以下の性質が成り立つことを証明する．

$$[\Box((\pi = l_1 \wedge y = 3 \wedge t < 2 \wedge T < 2) \rightarrow (\pi = l_1 \wedge y = 3 \wedge t > 5 \wedge T > 5))]_{\geq 0.2}$$

ここで，

$$q = (\pi = l_1 \wedge y = 3 \wedge t < 2 \wedge T < 2) \rightarrow (\pi = l_1 \wedge y = 3 \wedge t > 5 \wedge T > 5)$$

とすると，証明すべき論理式は $[\Box q]_{\geq 0.2}$ である．

(1) $\Theta \rightarrow \varphi$:
$\Theta = (\pi = l_0 \wedge y = t = T = 0)$ であり，
$\varphi = q = (\pi = l_1 \wedge y = 3 \wedge t < 2 \wedge T < 2) \rightarrow (\pi = l_1 \wedge y = 3 \wedge t > 5 \wedge T > 5)$
とする．
ここで，$\Theta \rightarrow \varphi$ は成り立つ．

(2) $\varphi \rightarrow q$:
$\varphi = q$ とするので，$\varphi \rightarrow q$ は成り立つ．

(3) $\forall \tau \in \mathcal{T}_H$ に対して $\rho_\tau \wedge \varphi \rightarrow \varphi\prime$:

(a) $(\pi = \pi\prime = l_0 \wedge y\prime = y + 1 \wedge t\prime = t \wedge T\prime = T)$
$\wedge$
$((\pi = l_1 \wedge y = 3 \wedge t < 2 \wedge T < 2) \rightarrow (\pi = l_1 \wedge y = 3 \wedge t > 5 \wedge T > 5))$
$\rightarrow$
$((\pi\prime = l_1 \wedge y\prime = 3 \wedge t\prime < 2 \wedge T\prime < 2) \rightarrow (\pi\prime = l_1 \wedge y\prime = 3 \wedge t\prime > 5 \wedge T\prime > 5))$

この論理式は成り立つ．

(b) $(\pi = l_0 \wedge \pi\prime = l_1 \wedge y\prime = y + 2 \wedge t\prime = t \wedge T\prime = T)$
$\wedge$
$((\pi = l_1 \wedge y = 3 \wedge t < 2 \wedge T < 2) \rightarrow (\pi = l_1 \wedge y = 3 \wedge t > 5 \wedge T > 5))$
$\rightarrow$
$((\pi\prime = l_1 \wedge y\prime = 3 \wedge t\prime < 2 \wedge T\prime < 2) \rightarrow (\pi\prime = l_1 \wedge y\prime = 3 \wedge t\prime > 5 \wedge T\prime > 5))$

この論理式は成り立つ．

(c) $(\triangle > 0.\pi\prime = \pi \wedge y\prime = y \wedge t\prime = t + \triangle \wedge T\prime = T + \triangle \wedge \pi = l_0 \rightarrow t + \triangle \leq 2)$
$\wedge$
$((\pi = l_1 \wedge y = 3 \wedge t < 2 \wedge T < 2) \rightarrow (\pi = l_1 \wedge y = 3 \wedge t > 5 \wedge T > 5))$
$\rightarrow$
$((\pi\prime = l_1 \wedge y\prime = 3 \wedge t\prime < 2 \wedge T\prime < 2) \rightarrow (\pi\prime = l_1 \wedge y\prime = 3 \wedge t\prime > 5 \wedge T\prime > 5))$

この論理式は成り立つ．

(4) $\forall \tau_{p(s\prime)} \in \mathcal{T}$ に対して $p \cdot p(s\prime)$ で更新した p が $\sqsupseteq \lambda$ を満たす：
(a) まず，$p = p \cdot p(\pi = l_0) = 1 \cdot 0.4 = 0.4$ である．ただし，$p(\pi = l_0) = 0.4$ である．
(b) 次に，$p = p \cdot p(\pi = l_1) = 0.4 \cdot 0.6 = 0.24$ である．ただし，$p(\pi = l_1) = 0.6$ である．
以上より，$p = p \cdot p(\pi = l_1) = 0.4 \cdot 0.6 = 0.24 \geq 0.2$ が成り立つ．

ゆえに，**Example1** の確率時間遷移システムにおいて，

$$[\Box((\pi = l_1 \wedge y = 3 \wedge t < 2 \wedge T < 2) \rightarrow (\pi = l_1 \wedge y = 3 \wedge t > 5 \wedge T > 5))]_{\geq 0.2}$$

が成り立つことを証明できた．

■

5. 活性の演繹的検証系

本章では，確率時間遷移システム上の活性，すなわち，$[\Box(q \rightarrow \Diamond r)]_{\sqsupseteq\lambda}$ を検証する手法を述べる．我々は，Manna らのリアクティブシステムの活性の検証

手法[24] を拡張して，確率時間遷移システム上の活性の検証手法を開発する．

最初に，活性の演繹的検証系を定義する．検証系を形式的に定義する前に，まず，検証系を簡単に以下に説明する：

検証ルールは補助的な表明 $\varphi_1,\ldots,\varphi_m$ を使い，φ_0 として表明 r を定義する．各表明 φ_i にクロック変数 $t_i \in C$ と実数値上限 b_i を結び付ける．これは，φ_i を満たす状態にいる間，クロック変数 t_i は b_i により制限されて，リセットされないことを意図する．計算の時間は際限なく大きくなるので，φ_i を満たす状態に長くとどまれないことを意味する．また，すべての i に対して，φ_i を満たす状態は，終局的には，φ_j を満たす状態に到達しなければならないことを示す．ただし，$j \leq i$ とする．

では，次に，活性の演繹的検証系を形式的に定義する．

Definition11（活性の演繹的検証ルール）
確率時間遷移システム $\mathbf{PTS} = (V, \Theta, prob, \Pi)$ のすべての Adversary A に対して，表明 q，r と $\varphi_0 = r,\varphi_1,\ldots,\varphi_m$，クロック変数 $t_1,\ldots,t_m \in C$ と定数 $b_1,\ldots,b_m \in \mathbf{R}$ について，以下が成り立つ：

1. $q \rightarrow \bigvee_{j=0}^{m} \varphi_j$

   $i = 1,\ldots,m$ に対して，以下の 3 つの仮定 2.，3.，4. が成り立つ：

2. $\forall \tau \in \mathcal{T}_H$ に対して以下が成り立つ：

   $\rho_\tau \wedge \varphi_i \rightarrow (\varphi\prime_i \wedge t_i\prime \geq t_i) \vee \bigvee_{j<i} \varphi\prime_j$

3. $\forall \tau_{p(s\prime)} \in \mathcal{T}$ に対して以下が成り立つ：

   $p \cdot p(s\prime)$ で更新した p が $\sqsupseteq \lambda$ を満たす

   ただし，p の初期値は 1 である．

4. $\varphi_i \rightarrow t_i \leq b_i$

5. −−−−−−−−−−−−−−−−−−−−−−−−

6. $[\Box(q \rightarrow \Diamond r)]_{\sqsupseteq\lambda}$

これは活性を証明するルールであり，1. から 4. を満たすとき，6. のように $[\Box(q \rightarrow \Diamond r)]_{\sqsupseteq\lambda}$ が証明されることを意味する．

以下に，各仮定の意味を簡単に説明する：

1. 表明 q が成り立つ状態は $\varphi_0 = r,\varphi_1,\ldots,\varphi_m$ の 1 つを満たす．

   $i = 1,\ldots,m$ に対して，以下の 3 つの仮定が成り立つ：

2. φ_i の成り立つ状態 s の τ-successor $(\forall \tau \in \mathcal{T})$ は φ_j が成り立つ．ただし，$j \leq i$ である．τ-successor 状態が φ_i を満たす場合，この状態遷移は t_i の値を減少させない．

3. 任意の状態遷移 ρ_{τ_i} する確率が $\sqsupseteq \lambda$ を満たす．

4. 表明 φ_i ならば，t_i は b_i 以下におさえられる．

なお，$\varphi_i\prime$ は状態遷移 ρ_τ 後の状態 $s\prime$ における表明であり，φ_i のシステム変数の集合 V を $V\prime$ に変えたものである．

■

次に，活性の演繹的検証ルールの健全性を述べる．

Theorem2（活性の検証ルールの健全性）
確率時間遷移システム **PTS** 上において，活性の検証ルールの前提条件が状態恒真であるならば，論理式 $[\Box(q \rightarrow \Diamond r)]_{\sqsupseteq\lambda}$ は恒真である．

Proof2 検証ルールの前提条件が状態恒真であり，**PTS** のパスを ω とする．すべての Adversary $A \in \mathcal{A}$ に対して，$Prob(\{\omega | \omega \in Path^A_{ful}(s),$ かつ，すべての k に対して $\omega(k) \models q$ は $i \geq k$ なる $\omega(i) \models r$ が続く $\}) \sqsupseteq \lambda$ が成り立つことを示す．

ここで，$\omega(k) \models q$ であり，$i \geq k$ において $\omega(i) \models r$ が成り立たないと仮定する．

前提条件 1. により，ある φ_j が $\omega(k) \models \varphi_j$ である．$\omega(k) \models \varphi_{j_k}$ であるような最小のインデックスを j_k とする．

前提条件 2. により，状態 s_{k+1} において，ある $j(0 < j \leq j_k)$ に対して，$s_{k+1} \models \varphi_j$ である．j_{k+1} はそのような最小のインデックスである．この方法を続けることにより，すべての $i > k$ に対して，ある φ_{j_i} について，$s_i \models \varphi_{j_i}$ である．ここで，$j_i > 0$，$j_k \geq j_{k+1} \geq j_{k+2} \geq \ldots$ である．

我々は無限に減少する自然数の無限な増加しない列を持つことができないので，以下のような $w(w \geq k)$ が存在する：

$$j_w = j_{w+1} = j_{w+2} = \ldots.$$

我々は，$u = j_w$ によって，この終局的に安定な表明のインデックスの値を表す．

状態 $s_i(i \geq w)$ において，クロック変数 t_u の値を考慮する．前提条件 2. により，t_u の値は減少しない．また，増分 $\triangle$ の tick 遷移が起こるときはいつも，t_u が $\triangle$ で増加する．前提条件 4. により，マスタクロック T は状態 s_w における値から，$b_u - s_w[t_u]$ より大きな増加はできない．これは，パス ω において，マスタクロック T が際限なく大きくなるという時間の発散性の事実と矛盾する．

以上の矛盾により，どんな r が成り立つ状態にも続かれない q が成り立つ状態が存在するという仮定が間違っていると結論する．

また，前提条件 3. により，確率の条件を満たすこ

とは明白である．

結局，もし前提条件が成り立つならば，すべての q が成り立つ状態は r が成り立つ状態に続けられて，確率の条件を満たす．

■

次に，活性の演繹的検証の事例を述べる．

Example4（活性の演繹的検証の事例）

図 2 に確率時間遷移システムの例を示す．たとえば，ロケーション $\pi_1 = l_0 \wedge \pi_2 = m_0$ からロケーション $\pi_1 = l_1 \wedge \pi_2 = m_0$ へは確率 0.8 で遷移し，ロケーション $\pi_1 = l_0 \wedge \pi_2 = m_0$ からロケーション $\pi_1 = l_2 \wedge \pi_2 = m_0$ へは確率 0.1 で遷移し，ロケーション $\pi_1 = l_0 \wedge \pi_2 = m_0$ からロケーション $\pi_1 = l_0 \wedge \pi_2 = m_1$ へは確率 0.1 で遷移する．また，$t_1 \geq 3$, $t_1 := 0$, $y := y+1$ は，$t_1 \geq 3$ ならば $t_1 := 0$ と $y := y+1$ を実行することを意味する．

ここで，図 2 の確率時間遷移システム $\mathbf{PTS} = (V, \Theta, prob, \Pi)$ の各組を定義する：

(1) $V = \{\pi_1, \pi_2, x, y, t_1, t_2, T\}$.
ここで，π_1 と π_2 はロケーションを表す変数であり，x と y はデータを表す変数であり，t_1 と t_2 はタイミング制約を表すクロック変数であり，T はグローバル時間を表すクロック変数である．

(2) $\Theta : \pi_1 = l_0 \wedge \pi_2 = m_0 \wedge x = y = 0 \wedge t_1 = t_2 = T = 0$.

(3) $\mathcal{T} : \{\tau_{p_1(\pi_1=l_1\wedge\pi_2=m_0)}, \tau_{p_1(\pi_1=l_2\wedge\pi_2=m_0)}, \tau_{p_1(\pi_1=l_0\wedge\pi_2=m_1)}, \tau_{p_2(\pi_1=l_0\wedge\pi_2=m_0)}, \tau_{p_2(\pi_1=l_1\wedge\pi_2=m_1)}, \tau_{p_3(\pi_1=l_0\wedge\pi_2=m_1)}, \tau_{p_4(\pi_1=l_2\wedge\pi_2=m_1)}, \tau_{p_5(\pi_1=l_2\wedge\pi_2=m_1)}\}$.

(a) $\rho_{\tau_{p_1(\pi_1=l_1\wedge\pi_2=m_0)}} : \pi_1 = l_0 \wedge \pi_1\prime = l_1 \wedge \pi_2 = \pi_2\prime = m_0 \wedge x = x\prime \wedge y = y\prime \wedge t_1 \geq 3 \wedge t_1\prime = 0 \wedge t_2\prime = t_2 \wedge T\prime = T$

(b) $\rho_{\tau_{p_1(\pi_1=l_2\wedge\pi_2=m_0)}} : \pi_1 = l_0 \wedge \pi\prime = l_2 \wedge \pi_2 = \pi_2\prime = m_0 \wedge x = x\prime \wedge y = y\prime \wedge t_1 \geq 3 \wedge t_1\prime = 0 \wedge t_2\prime = t_2 \wedge T\prime = T$

(c) $\rho_{\tau_{p_1(\pi_1=l_0\wedge\pi_2=m_1)}} : \pi_1 = \pi_1\prime = l_0 \wedge \pi_2 = m_0 \wedge \pi_2\prime = m_1 \wedge x\prime = 1 \wedge y = y\prime \wedge t_1\prime = t_1 \wedge t_2 \geq 3 \wedge t_2\prime = 0 \wedge T\prime = T$

(d) $\rho_{\tau_{p_2(\pi_1=l_0\wedge\pi_2=m_0)}} : \pi_1 = l_1 \wedge \pi_1\prime = l_0 \wedge \pi_2 = \pi_2\prime = m_0 \wedge x = x\prime \wedge y \leq 2 \wedge y\prime = y+1 \wedge t_1 \geq 3 \wedge t_1\prime = 0 \wedge t_2\prime = t_2 \wedge T\prime = T$

(e) $\rho_{\tau_{p_2(\pi_1=l_1\wedge\pi_2=m_1)}} : \pi_1 = \pi_1\prime = l_1 \wedge \pi_2 = m_0 \wedge \pi_2\prime = m_1 \wedge x\prime = 1 \wedge y = y\prime \wedge t_2 = t_2\prime \wedge t_2 \geq 3 \wedge t_2\prime = 0 \wedge T\prime = T$

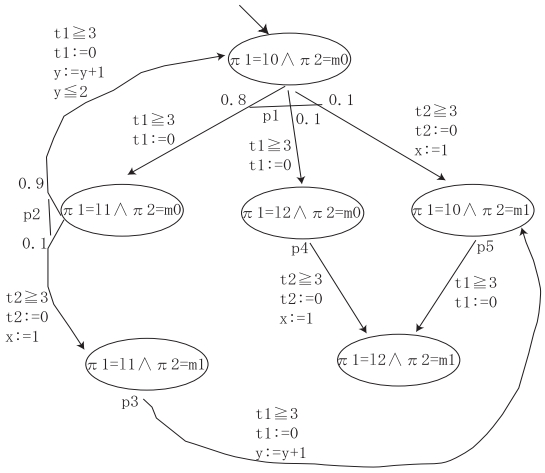


図 2 確率時間遷移システムの例—その 2
Fig. 2 Example of probabilistic timed transition system—part 2.

(f) $\rho_{\tau_{p_3(\pi_1=l_0\wedge\pi_2=m_1)}} : \pi_1 = l_1 \wedge \pi_1\prime = l_0 \wedge \pi_2 = \pi_2\prime = m_1 \wedge x = x\prime \wedge y\prime = y+1 \wedge t_1 \geq 3 \wedge t_1\prime = 0 \wedge t_2\prime = t_2 \wedge T\prime = T$

(g) $\rho_{\tau_{p_4(\pi_1=l_2\wedge\pi_2=m_1)}} : \pi_1 = \pi_1\prime = l_2 \wedge \pi_2 = m_0 \wedge \pi_2\prime = m_1 \wedge x\prime = 1 \wedge y = y\prime \wedge t_1\prime = t_1 \wedge t_2 \geq 3 \wedge t_2\prime = 0 \wedge T\prime = T$

(h) $\rho_{\tau_{p_5(\pi_1=l_2\wedge\pi_2=m_1)}} : \pi_1 = l_0 \wedge \pi\prime = l_2 \wedge \pi_2 = \pi_2\prime = m_1 \wedge x = x\prime \wedge y = y\prime \wedge t_1 \geq 3 \wedge t_1\prime = 0 \wedge t_2\prime = t_2 \wedge T\prime = T$

(4) $\Pi : ((\pi_1 = l_0 \vee \pi_2 = l_1) \rightarrow t_1 < 5) \wedge (\pi_1 = m_0 \rightarrow t_2 < 5)$.

ここで，$tick$ の状態遷移関係は以下のように定義できる：

$$\rho_{tick} : \exists \triangle > 0.(\pi_1 = \pi_1\prime \wedge \pi_2 = \pi_2\prime \wedge x = x\prime \wedge y = y\prime) \wedge (t_1\prime = t_1 + \triangle \wedge t_2\prime = t_2 + \triangle \wedge T\prime = T + \triangle) \wedge ((\pi_1 = l_0 \vee \pi_2 = l_1) \rightarrow t_1 < 5) \wedge (\pi_1 = m_0 \rightarrow t_2 < 5)$$

図 2 に確率時間遷移システムにおいて，以下の性質が成り立つことを証明する．

$$[\Box((\pi_1 = l_0 \wedge \pi_2 = m_0 \wedge x = t_1 = t_2 = T = 0) \rightarrow \Diamond(\pi_1 = l_2 \wedge \pi_2 = m_1))]_{\geq 0.04}$$

活性の演繹的検証ルールを適用するために，$(\pi_1 = l_0 \wedge \pi_2 = m_0 \wedge x = t_1 = t_2 = T = 0)$ を q として，$(\pi_1 = l_2 \wedge \pi_2 = m_1)$ を r とする．活性の演繹的検証ルールにおける表明，クロック変数，定数は以下である：

表明	クロック変数	定数
$\varphi_0 : \pi_1 = l_2 \wedge \pi_2 = m_1$	-	-
$\varphi_1 : \pi_1 = l_0 \wedge \pi_2 = m_1 \wedge x = 1 \wedge t_1 \leq 5$	$t_1 : t_1$	$b_1 : 5$
$\varphi_2 : \pi_1 = l_1 \wedge \pi_2 = m_1 \wedge x = 1 \wedge t_1 \leq 5$	$t_2 : t_1$	$b_2 : 5$
$\varphi_3 : (\pi_1 = l_0 \vee \pi_1 = l_1) \wedge \pi_2 = m_0$ $\wedge x = 0 \wedge t_1 \leq 5 \wedge t_2 \leq 5$	$t_3 : t_2$	$b_3 : 5$

以下に，活性の演繹的検証ルールに従って，性質の検証を進める：

1. $q \rightarrow \bigvee_{j=0}^{3} \varphi_j$ ：
$q = (\pi_1 = l_0 \wedge \pi_2 = m_0 \wedge x = t_1 = t_2 = T = 0)$ として，$\varphi_3 = ((\pi_1 = l_0 \vee \pi_1 = l_1) \wedge \pi_2 = m_0 \wedge x = 0 \wedge t_1 \leq 5 \wedge t_2 \leq 5)$ とする．
ここで，
$(\pi_1 = l_0 \wedge \pi_2 = m_0 \wedge x = t_1 = t_2 = T = 0) \rightarrow \ldots\ldots\ldots \vee ((\pi_1 = l_0 \vee \pi_1 = l_1) \wedge \pi_2 = m_0 \wedge x = 0 \wedge t_1 \leq 5 \wedge t_2 \leq 5)$
は明らかに成り立つ．

$i = 1, 2, 3$ に対して，以下の 3 つの仮定 2.，3.，4. が成り立つ：

2. $\forall \tau \in \mathcal{T}_H$ に対して以下が成り立つ：
$\rho_\tau \wedge \varphi_i \rightarrow (\varphi\prime_i \wedge t_i\prime \geq t_i) \vee \bigvee_{j<i} \varphi\prime_j$:
(1) $\forall \tau \in \mathcal{T}$ に対して：
紙面の都合上，$i = 3$ のときのある遷移について示す．
$\rho_{\tau_{p_1(\pi_1 = l_0 \wedge \pi_2 = m_1)}} \wedge \varphi_3 \rightarrow (\varphi_1\prime \vee \varphi_2\prime)$
上記式は成り立つ．
ここで，
$\rho_{\tau_{p_1(\pi_1 = l_0 \wedge \pi_2 = m_1)}} = \pi_1 = \pi_1\prime = l_0 \wedge \pi_2 = m_0 \wedge \pi_2\prime = m_1 \wedge x\prime = 1 \wedge y = y\prime \wedge t_1\prime = t_1 \wedge t_2 \geq 3 \wedge t_2\prime = 0 \wedge T\prime = T$, $\varphi_1\prime = (\pi_1\prime = l_0 \wedge \pi_2\prime = m_1 \wedge x\prime = 1 \wedge t_1\prime \leq 5)$, $\varphi_2\prime = (\pi_1\prime = l_1 \wedge \pi_2\prime = m_1 \wedge x\prime = 1 \wedge t_1\prime \leq 5)$, $\varphi_3 = ((\pi_1 = l_0 \vee \pi_1 = l_1) \wedge \pi_2 = m_0 \wedge x = 0 \wedge t_1 \leq 5 \wedge t_2 \leq 5)$
とする．
同様に，$i = 1, 2, 3$ のすべての遷移についても成り立つ．
(2) tick 遷移に対して：
紙面の都合上，$i = 2$ のときの tick 遷移について示す．
$\rho_{tick} \wedge \varphi_2 \rightarrow \varphi_2\prime \wedge t_1\prime \geq t_1$
上記式は成り立つ．
ここで，
$\rho_{tick} = \triangle > 0 \wedge (\pi_1 = \pi_1\prime \wedge \pi_2 = \pi_2\prime \wedge x = x\prime \wedge y = y\prime) \wedge (t_1\prime = t_1 + \triangle \wedge t_2\prime = t_2 + \triangle \wedge T\prime = T + \triangle) \wedge ((\pi_1 = l_0 \vee \pi_2 = l_1) \rightarrow t_1 < 5) \wedge (\pi_1 = m_0 \rightarrow t_2 < 5)$,
$\varphi_2 = (\pi_1 = l_1 \wedge \pi_2 = m_1 \wedge x = 1 \wedge t_1 \leq 5)$,
$\varphi_2\prime = (\pi_1\prime = l_1 \wedge \pi_2\prime = m_1 \wedge x\prime = 1 \wedge t_1\prime \leq 5)$
とする．
同様に，$i = 1, 3$ の tick 遷移についても成り立つ．

3. $\forall \tau_{p(s\prime)} \in \mathcal{T}$ に対して以下が成り立つ：
$p \cdot p(s\prime)$ で更新した p が $\sqsupseteq \lambda$ を満たす
ただし，p の初期値は 1 である．：
ここでは，以下のように，最も確率の低いパスを考える：
$(\pi_1 = l_0 \wedge \pi_2 = m_0) \xrightarrow{p_1} (\pi_1 = l_1 \wedge \pi_2 = m_0) \xrightarrow{p_2}$
$(\pi_1 = l_0 \wedge \pi_2 = m_0) \xrightarrow{p_1} (\pi_1 = l_1 \wedge \pi_2 = m_0) \xrightarrow{p_2}$
$(\pi_1 = l_0 \wedge \pi_2 = m_0) \xrightarrow{p_1} (\pi_1 = l_1 \wedge \pi_2 = m_0) \xrightarrow{p_2}$
$(\pi_1 = l_1 \wedge \pi_2 = m_1) \xrightarrow{p_3} (\pi_1 = l_0 \wedge \pi_2 = m_1) \xrightarrow{p_5}$
$(\pi_1 = l_2 \wedge \pi_2 = m_1)$
この場合の確率 p は以下である：
$p = 1 \cdot 0.8 \cdot 0.9 \cdot 0.8 \cdot 0.9 \cdot 0.8 \cdot 0.1 \cdot 1 \cdot 1 = 0.041472$
$p > 0.04$ なので，確率は成り立つ．

4. $\varphi_i \rightarrow t_i \leq b_i$ ：
表明 φ_1，φ_2，φ_3 の中には，それぞれ $t_1 \leq b_1$，$t_2 \leq b_2$，$t_3 \leq b_3$ が含まれるので，上記式は明らかに成り立つ．

以上より，図 2 の確率時間遷移システムにおいて，以下の性質が成り立つことが証明できた．

$$[\Box((\pi_1 = l_0 \wedge \pi_2 = m_0 \wedge x = t_1 = t_2 = T = 0) \rightarrow \Diamond(\pi_1 = l_2 \wedge \pi_2 = m_1))]_{\geq 0.04}$$

■

6. ま と め

本論文では，確率時間オートマトンを一般化することにより，確率時間遷移システムを開発して，その上に，確率時間時相論理の演繹的な検証規則を開発した．確率時間遷移システムは離散確率分布を持つリアルタイムシステムの一般的な計算モデルであり，従来よりも一般的な検証手法が確立できた．

今後の研究課題としては，以下がある．

(1) 表明の自動生成や証明式の決定可能手続きの発見，GUI の向上などにより，演繹的証明作業の効率的な計算機支援を実現する．
(2) 確率時間遷移システムのモジュール化により，確率時間遷移モジュールを開発する．
(3) 抽象実行などの抽象化技術を適用することにより，確率時間遷移システムの自動検証を実現する．

謝辞 本研究は文部省科研費基盤 C「ハイブリッドモデルによる組込みシステムの高信頼性設計方法論の構築と支援環境の開発（副題：モジュール性と自律性を基礎とした Assume-Guarantee 型詳細化検証理論の構築）(代表：山根智)」（平成 14〜16 年度）の援助の下で実施されました.

参 考 文 献

1) Tilborg, A.M. and Koob, G.M.: *Foundations of Real-time Computing: Formal Specifications and Methods*, Kluwer Academic Pub., p.316 (1991).
2) de Bakker, J.W. and Huizing, C., de Roever, W.P. and Rozenberg, G.: *Time: Theory in Practice*, LNCS 600, Springer-Verlag (1992).
3) Kavi, K.M.: *Real-Time Systems Abstractions, Languages and Design Methodologies*, IEEE Computer Society Press (1992).
4) Inan, M.K. and Kurshan, R.P.: Verification of Digital and Hybrid Systems, *NATO ASI Series F: Computer and Systems Sciences*, Vol.170, Springer-Verlag (2000).
5) Alur, R. and Dill, D.L.: A theory of timed automata, *Theoretical Computer Science*, Vol.126, pp.183–235 (1994).
6) Alur, R., Courcoubetis, C. and Dill, D.L.: Model-Checking in Dense Real-Time, *Information and Computation*, Vol.104, pp.2–34 (1993).
7) Henzinger, T.A., Nicollin, X., Sifakis, J. and Yovine, S.: Symbolic model checking for real-time systems, *Information and Computation*, Vol.111, pp.193–244 (1994).
8) Kwiatkowska, M., Norman, G., Segala, R. and Sproston, J.: Automatic verification of real-time systems with discrete probability distributions, *Theoretical Computer Science 282*, pp.101–150 (2002).
9) Yamane, S.: Formal Probabilistic Refinement Verification Method of Embedded Real-Time Systems, *1st Workshop on Software Technologies for Future Embedded Systems*, pp.79–82, IEEE Computer Society (2003).
10) Hart, S., Sharir, M. and Pnueli, A.: Termination of Probabilistic Concurrent Programs, *ACM Trans. Programming Languages*, Vol.5, pp.356–380 (1983). (In: *Proc. 9th ACM Symposium Principles of Programming Languages* (*POPL 1982*), pp.1–6 (1982).)
11) Sharir, M. and Hart, S.: Probabilistic temporal logics for finite and bounded models, *Proc. 16th ACM Symposium on Theory of Computing*, pp.1–13 (1984).
12) Lehmann, D. and Shelah, S.: Reasoning about time and chance, *Information and Control*, Vol.53, pp.165–198 (1982).
13) Pnueli, A.: On the Extremely Fair Treatment of Probabilistic Algorithms, *Proc. 15th ACM Symposium Theory of Computing*, pp.278–290 (1983).
14) Pnueli, A. and Zuck, L.: Verification of multiprocess probabilistic protocols, *Distributed Computing*, Vol.1, No.1, pp.53–72 (1986).
15) Hansson, H.A.: Time and Probability in Formal Design of Distributed Systems, Ph.D. Thesis, Uppsala University (1991).
16) Alur, R., Courcoubetis, C. and Dill, D.L.: Verifying automata specifications of probabilistic real-time systems, *LNCS 600*, pp.28–44 (1991).
17) Alur, R., Courcoubetis, C. and Dill, D.L.: Model-checking for probabilistic real-time systems, *LNCS 510*, pp.115–136 (1991).
18) Segala, R.: Modeling and Verification of Randomized Distributed Real-Time Systems, Ph.D. Thesis, MIT (1995).
19) Kesten, Y., Manna, Z. and Pnueli, A.: Verifying Clocked Transition Systems, *LNCS 1066*, pp.13–40, Springer-Verlag (1996).
20) Kwiatkowska, M.Z., Norman, G. and Sproston, J.: Probabilistic Model Checking of Deadline Properties in the IEEE 1394 FireWire Root Contention Protocol, *Formal Aspects of Computing*, Vol.14, No.3, pp.295–318 (2003).
21) Kwiatkowska, M.Z.: Model Checking for Probability and Time: From Theory to Practice, Invited talk at LICS'03, pp.351–360 (2003).
22) Vardi, M.Y.: Automatic verification of probabilistic concurrent finite-state systems, *Proc. 26th IEEE Symp. Found. of Comp. Sci.*, pp.327–338 (1985).
23) Manna, Z. and Pnueli, A.: *Temporal Verification of Reactive Systems*: Safety, Springer-Verlag (1995).
24) Manna, Z. and Pnueli, A.: Temporal Verification of Reactive Systems: Progress, Unpublished, Stanford University (http://theory.stanford.edu/~zm/) (1996).

(平成 15 年 8 月 27 日受付)
(平成 16 年 4 月 5 日採録)



山根　智（正会員）

1984年京都大学大学院修了．現在，金沢大学工学部情報システム工学科教授．リアルタイム・ハイブリッドシステムの仕様記述と形式的検証の研究に従事．EATCS，ACM，IEEE等各会員．