

離散確率分布を持つリアルタイムシステムの 確率時間双模倣関係と確率時間時相論理式の保存

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る。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が定着しており、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。とりわけ、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も開発されている。さらに、最近、我々は確率時間オートマトンの確率時間模倣関係を開発して、段階的詳細化開発へ適用した。本論文では、より一般的な確率時間双模倣関係を新たに定義して、その確率時間双模倣関係にある2つの確率時間オートマトンは確率時間時相論理式の同じ集合を満たすことを示す。この種の双模倣関係は確率時間オートマトンの抽象化を保証するための重要な道具となりうる。

Probabilistic Timed Bisimulation Relation and Its Preservation of Probabilistic Timed CTL Formulas 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 generally specify real-time systems using timed automata, and verify them using model-checking. Timed automata are augmented with a finite set of clocks. 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, we have developed probabilistic timed simulation relation and applied our proposed methods to stepwise refinement. In this paper, we define general probabilistic timed bisimulation relation, and we show that two probabilistic timed bisimilar probabilistic timed automata must satisfy the same set of probabilistic timed CTL formulas. This kind of bisimilarity is a valuable tool to guarantee abstractions of probabilistic timed automata.

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、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⁾も開発されている。さらに、最近、我々は確率時間オートマトンの確率時間模倣関係を開発して、段階的詳細化開発へ適用した⁹⁾。我々の知る限りでは、この研究⁹⁾が確率時間オートマトンの確率時間模倣関係に関する最初の研究である。本論文では、確率時間オートマトンの確率時間双模倣関係に関する重要な性質を明らかにする。

まず、以下では、確率システムやリアルタイムシステムの模倣関係と双模倣関係に関する、重要な既存の研究を述べる。

確率システムの模倣関係と双模倣関係に関連する代表的な既存研究としては、以下がある：

(1) 1991年、K.G. Larsen らが確率システムの最

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

初の双模倣関係の研究として、確率プロセス代数の双模倣関係¹⁰⁾を初めて提案した。この研究は確率分布の同値関係を考慮した双模倣関係の提案であり、以降の確率システムの双模倣関係の標準的な方法となった。

- (2) 1991年, Hansson は確率離散時間プロセス代数の双模倣関係¹¹⁾とその検証アルゴリズムを初めて提案した。この研究はプロセス代数を確率と離散時間で拡張して、その双模倣関係の検証アルゴリズムを定義したものである。
- (3) 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¹²⁾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。

一方、リアルタイムシステムの代表的な双模倣関係と模倣関係による検証に関する既存研究としては、以下がある。

- (1) 1992年, Cerans は時間オートマトンの時間双模倣関係の決定可能性を示した¹³⁾。従来までは、時間オートマトンの言語包含検証のアルゴリズムが存在しないことが示されており、時間オートマトンの時間双模倣関係の決定性アルゴリズムが存在しないと予想されていた。この成果は驚くべきことであり、時間オートマトンの時間双模倣関係の設計問題への適用を促進した。
- (2) 1996年, Tasiran らは時間オートマトンの時間模倣関係により、非同期回路の段階的詳細化開発を示した¹⁴⁾。彼らは、世界で初めて、時間模倣関係を実際の設計問題へ適用した。
- (3) 1998年, Tasiran らの影響を受けて, Yamane は時間オートマトンの $\forall$ -時間模倣関係と $\exists$ -時間模倣関係を開発して、通信プロトコルの段階的詳細化開発へ適用した¹⁵⁾。

本論文は、これらの既存研究とまったく異なり、離散確率分布と稠密なタイミング制約の記述で拡張した、確率時間オートマトンの確率時間双模倣関係における確率時間相論理式の保存性に関する研究である。

本論文では、世界で最初に、確率時間オートマトンの一般的な確率時間双模倣関係を定義した。そして、その確率時間双模倣関係にある2つの確率時間オートマトンが、確率時間相論理式の同じ集合を満たすこ

とを示す。この種の双模倣関係は確率時間オートマトンの抽象化を保証するための重要な道具となりえて、実用上からも非常に価値がある。

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と Adversary を定義する。3章では、確率時間相論理を定義する。4章では、確率時間双模倣関係を定義して、確率時間相論理式の保存性を示す。最後に、5章でまとめと今後の課題を述べる。

2. 確率時間オートマトンと Adversary

本章では、まず、確率時間オートマトンを定義して、次に、Adversary を定義する⁸⁾。

2.1 確率時間オートマトン

まず、離散確率分布を定義する。

Definition 1 (離散確率分布)

有限集合 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 $p: Q \rightarrow [0, 1]$ である。ただし、 $\sum_{q \in Q} p(q) = 1$ である。

次に、確率時間オートマトン⁸⁾を定義する。

Definition 2 (確率時間オートマトン)

確率時間オートマトンは $M = (Q, Steps, L)$ によって表記される。ただし、

- (1) Q は状態の集合である。
- (2) $Steps: Q \rightarrow 2^{R \times \mu(Q)}$ であり、 $Steps$ は順序対 (t, p) の集合 $Steps(q)$ を任意の状態 $q \in Q$ に割り付ける関数である。ただし、 $t \in \mathbb{R}$ と $p \in \mu(Q)$ である。
- (3) $L: Q \rightarrow 2^{AP}$ である。ただし、 AP は原子命題の集合である。

$Steps(q)$ は状態 $q \in Q$ の中で非決定的に選択される遷移の集合である。各遷移は順序対 (t, p) であり、 t は遷移の滞留時間を表して、 p は次の状態の集合上の確率分布を表す。ゆえに、状態 q の中の $(t, p) \in Steps(q)$ の非決定的な選択が与えられたとき、 t 時刻経過した後、確率 $p(q')$ を有する状態 q' への確率遷移が起きる。

次に、パスを定義する。

Definition 3 (パス)

確率時間オートマトンのパスは、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。確率時間オートマトンのパスは非空有限または無限のシーケンスであり、以下のとおりである。

$$\omega = q_0 \xrightarrow{p_0} q_1 \xrightarrow{p_1} q_2 \xrightarrow{p_2} q_3 \cdots \xrightarrow{p_{n-1}} q_n \cdots$$

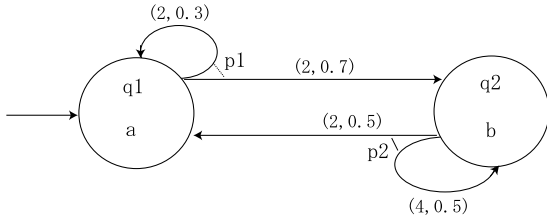


図 1 確率時間オートマトンの例

Fig. 1 Example of probabilistic timed automaton.

ここで, $q_i \in Q$, $(t_i, p_i) \in \text{Steps}(q_i)$ である. n 番目の遷移の発生時間は $\sum_{i=0}^{n-1} t_i$ であり, $\tau(n)$ と表記する. ω の位置は順序対 $(i, t) \in \mathbf{N} \times \mathbf{R}$ であり, $t \leq t_i$ である. パス ω のすべての位置の集合を $\Pi(\omega)$ と表記する. 位置 $(i, t) \in \Pi(\omega)$ の発生時間は $\tau_\omega((i, t))$ と表記して, $\tau_\omega(i) + t$ として定義される. 位置 $(i, t) \in \Pi(\omega)$ が与えられたとき, その位置 (i, t) の状態は $\omega((i, t))$ として表記されて, 確率時間オートマトンの状態 q_i において滞留時間 t が経過したことを意味し, これを $q_i + t$ と表記する.

以下のように, $\Pi(\omega)$ 上に全順序 $<_{\omega}$ を定義する:

$$(i, t) <_{\omega} (j, t') \iff i < j \vee (i = j \wedge t \leq t')$$

Example 1 (確率時間オートマトンの事例)

図 1 に確率時間オートマトンの例を示す. 状態 q_1 から状態 q_1 へは遅延時間 2 で確率 0.3 で遷移して, 状態 q_1 から状態 q_2 へは遅延時間 2 で確率 0.7 で遷移する. 状態 q_2 から状態 q_1 へは遅延時間 2 で確率 0.5 で遷移して, 状態 q_2 から状態 q_2 へは遅延時間 4 で確率 0.5 で遷移する. ここで, 図 1 の確率時間オートマトン $M = (Q, \text{Steps}, L)$ の各組を定義する:

- (1) $Q = \{q_1, q_2\}$.
- (2) $AP = \{a, b\}$.
- (3) $\text{Steps}(q_1) = \{(2, 0.7), (2, 0.3)\}$
 $\text{Steps}(q_2) = \{(2, 0.5), (4, 0.5)\}$
- (4) $L(q_1) = \{a\}$. $L(q_2) = \{b\}$.

この確率時間オートマトンには, 以下のようなパスが存在する:

$$\omega = q_1 \xrightarrow{p_1^1} q_1 \xrightarrow{p_2^1} q_2 \xrightarrow{p_2^2} q_2 \xrightarrow{p_4^2} q_1 \dots$$

ただし, p_1 と p_2 は離散確率分布であり, $p_1(q_1) = 0.3$, $p_1(q_2) = 0.7$, $p_2(q_1) = 0.5$, $p_2(q_2) = 0.5$ である.

2.2 Adversary

確率時間オートマトンの非決定性を解決するために, Adversary⁸⁾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, Vardi¹⁶⁾により提案された.

Definition 4 (確率時間オートマトンの Adversary)

確率時間オートマトン $M = (Q, \text{Steps}, L)$ の Adversary は順序対 (t, p) をすべての有限なパス ω に割り付ける関数 A である. ただし, $A(\omega) \in \text{Steps}(\text{last}(\omega))$ であり, $\text{last}(\omega)$ は ω の最後の状態である.

確率時間オートマトン $M = (Q, \text{Steps}, L)$ の Adversary A に対して, Path_{fin}^A を有限のパスの集合とし, Path_{ful}^A をパスの集合とする.

Adversary A によって, 確率時間オートマトン M 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 が確率時間オートマトン M の Adversary ならば, $\text{MC}^A = (\text{Path}_{fin}^A, \mathbf{P}^A)$ はマルコフ連鎖である. ここで,

$$\mathbf{P}^A(\omega, \omega') = \begin{cases} p(q) & \text{if } A(\omega) = (t, p) \\ & \text{and } \omega' = \omega \xrightarrow{p_t} q \\ 0 & \text{otherwise.} \end{cases}$$

任意の確率時間オートマトンに対して, $\mathcal{F}^{path}$ 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 $\omega' \in \text{Path}_{ful}$ に対して

$\{\omega | \omega \in \text{Path}_{ful} \text{ であり, } \omega' \text{ は } \omega \text{ のプレフィックスである}\}$

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.

Definition 5 (関数 Prob_{fin}^A)

A を確率時間オートマトン M の Adversary とする. $\text{Prob}_{fin}^A : \text{Path}_{fin}^A \rightarrow [0, 1]$ は Path_{fin}^A 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_{fin}^A は, 以下のように定義される:

- (1) $|\omega| = 0$ ならば, $\text{Prob}_{fin}^A(\omega) = 1$ である.
- (2) $|\omega| \neq 0$ のときは以下である. $\omega' \in \text{Path}_{fin}^A$ は A のパスとする. もし, ある $\omega \in \text{Path}_{fin}^A$ に對して $\omega' = \omega \xrightarrow{p_t} q$ ならば,

$$\text{Prob}_{fin}^A(\omega') = \text{Prob}_{fin}^A(\omega) \cdot \mathbf{P}^A(\omega, \omega')$$

である.

Definition 6 (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:

$$\begin{aligned} & \text{Prob}^A\{\omega | \omega \in \text{path}_{ful}^A \text{ かつ} \\ & \quad \omega' \text{ は } \omega \text{ のプレフィックスである}\} \\ & = \text{Prob}_{fin}^A(\omega'). \end{aligned}$$

Example 2 (確率時間オートマトンのマルコフ連鎖の事例)

ある Adversary A に対して, 図 1 の確率時間オートマトンのマルコフ連鎖 $MC^A = (Path_{fin}^A, P^A)$ を以下のように構成する.

- (1) もし $last(\omega) = q_1$ ならば, $A(q_1) = (2, 0.3)$ とする.
ただし, $\omega' = q_1 \xrightarrow{0.3} q_1$ とする.
- (2) ここで $last(\omega'') = q_1$ であり, $A(q_1) = (2, 0.7)$ とする.
ただし, $\omega'' = \omega' \xrightarrow{0.7} q_2$ とする.
- (3) ここで $last(\omega''') = q_2$ であり, $A(q_1) = (4, 0.5)$ とする.
ただし, $\omega''' = \omega'' \xrightarrow{0.5} q_2$ とする.
- (4) ここで $last(\omega''') = q_2$ であり, $A(q_2) = (2, 0.5)$ とする.
ただし, $\omega'''' = \omega''' \xrightarrow{0.5} q_1$ とする.

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

- (1) $Path_{fin}^A = q_1 \xrightarrow{0.3} q_1 \xrightarrow{0.7} q_2 \xrightarrow{0.5} q_2 \xrightarrow{0.5} q_1$
- (2) P^A は以下のように定義される:
 - (a) $P^A(\omega, \omega') = 0.3$
 - (b) $P^A(\omega', \omega'') = 0.7$
 - (c) $P^A(\omega'', \omega''') = 0.5$
 - (d) $P^A(\omega''', \omega''') = 0.5$

3. 確率時間時相論理

本章では, 確率時間時相論理を導入する. 我々は時間時相論理 TCTL⁶⁾ を確率の概念で拡張する.

Definition 7 (確率時間時相論理の構文)

形式 $[c, c']$, $[c, c')$, $(c, c']$, (c, c') , (c, ∞) , $[c, \infty)$ の実数のインターバルの集合を I とする. ここで, $c, c' \in \mathbb{N}$ (自然数) とする.

確率時間時相論理の構文は以下のように定義される:

$$\phi ::= true \mid a \mid \phi_1 \wedge \phi_2 \mid \neg \phi_1 \mid [\phi_1 \exists U_{\delta} \phi_2]_{\geq \lambda} \mid [\phi_1 \forall U_{\delta} \phi_2]_{\geq \lambda}$$

ここで, $a \in AP$ は原子命題, $\lambda \in [0, 1]$, $\delta \in I$, $\geq \in \{\geq, >\}$ である.

Definition 8 (確率時間時相論理の意味)

確率時間オートマトン M と M の adversary の集合 $\mathcal{A}$ が与えられたとき, M の任意の状態 q と確率時間時相論理式 ϕ に対して, 充足関係 $q \models_{\mathcal{A}} \phi$ は帰納的に定義される:

- (1) $q \models_{\mathcal{A}} true$
- (2) $q \models_{\mathcal{A}} a \iff q(a) = true$
- (3) $q \models_{\mathcal{A}} \phi_1 \wedge \phi_2 \iff q \models_{\mathcal{A}} \phi_1$ かつ $q \models_{\mathcal{A}} \phi_2$
- (4) $q \models_{\mathcal{A}} \neg \phi_1 \iff q \not\models_{\mathcal{A}} \phi_1$
- (5) $q \models_{\mathcal{A}} [\phi_1 \exists U_{\delta} \phi_2]_{\geq \lambda} \iff$ ある $A \in \mathcal{A}$ に対して, $Prob(\{\omega \mid \omega \in Path_{ful}^A(q) \text{ かつ } \omega \models_{\mathcal{A}} \phi_1 U_{\delta} \phi_2\}) \geq \lambda$
- (6) $q \models_{\mathcal{A}} [\phi_1 \forall U_{\delta} \phi_2]_{\geq \lambda} \iff$ すべての $A \in \mathcal{A}$ に対して, $Prob(\{\omega \mid \omega \in Path_{ful}^A(q) \text{ かつ } \omega \models_{\mathcal{A}} \phi_1 U_{\delta} \phi_2\}) \geq \lambda$

ただし,

$\omega \models_{\mathcal{A}} \phi_1 U_{\delta} \phi_2 \iff \tau_{\omega}((i, t)) \in \delta$ かつ $\omega((i, t)) \models \phi_2$ であるような ω の位置 (i, t) が存在する. そして, $(j, t_j) <_{\omega} (i, t)$ のすべての (j, t_j) に対して, $\omega((j, t_j)) \models \phi_1 \vee \phi_2$ である.

Example 3 (確率時間時相論理式の事例)

以下に確率時間時相論理式の例を示す.

- (1) $[true \exists U_{[0, 2]} full]_{\geq 0.5}$
この論理式は, 2 時間以内に, キューが満杯になる確率が 0.5 以上である場合が存在することを意味する.
- (2) $[\neg repair \forall U_{[0, 200]} success]_{\geq 0.98}$
この論理式は, すべての場合に, 200 時間以内に, システムが repair することなく, システムが success する確率が 0.98 以上であることを意味する.

上記は代表的な例であり, 確率と実時間性により, 記述能力が向上して, リアルタイムシステムの面白い性質が記述できる.

4. 確率時間双模倣関係と確率時間時相論理

本章では, 確率時間オートマトンの確率時間双模倣関係を定義し, 確率時間双模倣関係にある 2 つの確率時間オートマトンは確率時間時相論理式と同じ集合を満たすことを示す.

4.1 確率時間双模倣関係

本論文では, 確率時間双模倣関係にある 2 つの確率時間オートマトンが確率時間時相論理式と同じ集合を満たすために, 確率時間双模倣関係が確率と時間の性質を完全にとらえる必要がある. ゆえに, 提案する確率時間双模倣関係では, 2 つの確率時間オートマトンの離散確率分布が同値関係にあり, かつ, 2 つの確率時間オートマトンの状態遷移の経過時間の長さが同じであるような確率時間双模倣関係を定義する.

なお、既存の研究としては、リアルタイムシステムにおいて、経過時間の長さを考慮しない強時間抽象双模倣関係が定義されており、強時間抽象双模倣関係にある2つの時間オートマトンが分岐時相論理式(CTL)の同じ集合を満たすことが示されている¹⁷⁾。この強時間抽象双模倣関係では、経過時間の長さを考慮しないために、強時間抽象双模倣関係にある2つの時間オートマトンは時間分岐時相論理式(TCTL)の同じ集合を満たさない。我々は確率時間時相論理式の保存性を示すために、経過時間の長さを考慮する必要があり、強時間抽象双模倣関係ではなく、強時間双模倣関係とする。

以下では、確率時間オートマトンに対して、確率時間時相論理式を保存する、確率時間双模倣関係を定義する。

4.1.1 離散確率分布の同値関係と強時間双模倣関係
まず、文献 18), 19) に従って、離散確率分布の間の同値関係を定義する。

Definition 9 (離散確率分布の間の同値関係)
集合 Q 上の同値関係を $\mathcal{R}$ とする。 $\mu(Q)$ の2つの離散確率分布 p_1 と p_2 が $\mathcal{R}$ -同値の必要十分条件は以下である：

商集合 $Q/\mathcal{R}$ の任意の同値類 C に対して、

$$\sum_{q \in C} p_1(q) = \sum_{q \in C} p_2(q)$$

すなわち、もし p_1 と p_2 が商集合 $Q/\mathcal{R}$ の同値類 C に同じ確率を割り付けるならば、 p_1 と p_2 は $\mathcal{R}$ -同値である。

なお、 p_1 と p_2 が $\mathcal{R}$ -同値であることを $p_1 \equiv_{\mathcal{R}} p_2$ と表記する。

Example 4 (離散確率分布の間の同値関係の事例)

まず、 $Q = \{x_1, x_2, x', y, y'\}$ とし、 Q 上の同値関係を $\mathcal{R}$ とする。また、商集合 $Q/\mathcal{R}$ の同値類の集合を $\{C_x, C_y\}$ として、 $C_x = \{x_1, x_2, x'\}$ と $C_y = \{y, y'\}$ とする。ここで、 p_1 と p_2 は離散確率分布とする。ただし、 $p_1(x_1) = \frac{1}{8}$ 、 $p_1(x_2) = \frac{3}{8}$ 、 $p_1(y) = \frac{1}{2}$ 、 $p_2(x') = \frac{1}{2}$ 、 $p_2(y') = \frac{1}{2}$ とする。以下が成り立つ：

$$(1) \quad p_1[C_x] = p_1(x_1) + p_1(x_2) + p_1(x') = \frac{1}{8} + \frac{3}{8} + 0 = \frac{1}{2} = p_2(x_1) + p_2(x_2) + p_2(x') = 0 + 0 + \frac{1}{2} = p_2[C_x]$$

$$(2) \quad p_1[C_y] = p_1(y) + p_1(y') = 0 + \frac{1}{2} = \frac{1}{2} = p_2(y) + p_2(y') = 0 + \frac{1}{2} = p_2[C_y]$$

以上より、 $p_1 \equiv_{\mathcal{R}} p_2$ である。

次に、時間オートマトンの強時間双模倣関係を定義する。

Definition 10 (時間オートマトンの強時間双模倣関係)

まず、時間オートマトンを定義する。時間オートマトンを $M^t = (Q^t, Steps^t, L^t)$ とする。ただし、

- (1) Q^t は状態の集合である。
- (2) $Steps^t : Q^t \rightarrow 2^{\mathbf{R}}$ であり、 $Steps^t$ は t の集合 $Steps^t(q)$ を任意の状態 $q \in Q^t$ に割り付ける関数である。ただし、 $t \in \mathbf{R}$ である。
- (3) $L^t : Q^t \rightarrow 2^{AP}$ である。ただし、 AP は原子命題の集合である。

なお、時間オートマトンのパス ω は以下のとおりである：

$$\omega = q_0 \longrightarrow_{t_0} q_1 \longrightarrow_{t_1} q_2 \longrightarrow_{t_2} q_3 \cdots \longrightarrow_{t_{n-1}} q_n \cdots$$

ここで、 $q_i \in Q^t$ 、 $t_i \in Steps^t(q_i)$ である。

次に、時間オートマトンの強時間双模倣関係を定義する。

$\mathcal{R}$ が強時間双模倣関係である必要十分条件は、もし $(q_1, q_3) \in \mathcal{R}$ ならば、任意の $t \in \mathbf{R}_{\geq 0}$ に対して、以下の2つの条件が成り立つことである。

- (1) $(q_1, q_3) \in \mathcal{R}$ かつ $q_1 \longrightarrow_{t_1} q_2$ であるときはいつも、ある q_4 が存在して、 $q_3 \longrightarrow_{t_3} q_4$ かつ $(q_2, q_4) \in \mathcal{R}$ である。
さらに、 $L(q_1) = L(q_3)$ かつ $L(q_2) = L(q_4)$ である。
- (2) $(q_1, q_3) \in \mathcal{R}$ かつ $q_3 \longrightarrow_{t_3} q_4$ であるときはいつも、ある q_2 が存在して、 $q_1 \longrightarrow_{t_1} q_2$ かつ $(q_2, q_4) \in \mathcal{R}$ である。
さらに、 $L(q_1) = L(q_3)$ かつ $L(q_2) = L(q_4)$ である。

4.1.2 確率時間双模倣関係の定義

次に、離散確率分布の同値関係と強時間双模倣関係を融合して、確率時間双模倣関係を定義する。

Definition 11 (確率時間双模倣関係)

同値関係 $\mathcal{R} \subseteq Q \times Q$ が確率時間オートマトン $M = (Q, Steps, L)$ の確率時間双模倣関係である必要十分条件は、もし $(q, r) \in \mathcal{R}$ ならば、任意の $t \in \mathbf{R}_{\geq 0}$ に対して、以下の2つの条件が成り立つことである：

- (1) $(q, r) \in \mathcal{R}$ かつ $q \longrightarrow_t^{p_q}$ であるときはいつも、 $r \longrightarrow_t^{p_r}$ かつ $p_q \equiv_{\mathcal{R}} p_r$ である。
さらに、 $L(q) = L(r)$ である。
- (2) $(q, r) \in \mathcal{R}$ と $r \longrightarrow_t^{p_r}$ であるときはいつも、 $q \longrightarrow_t^{p_q}$ かつ $p_r \equiv_{\mathcal{R}} p_q$ である。
さらに、 $L(r) = L(q)$ である。

この1つの確率時間オートマトン上の確率時間双模倣関係の定義は、容易に、2つの確率時間オートマトン間の確率時間双模倣関係の定義に拡張できる。

Definition 12 (確率時間オートマトン間の確率時間双模倣等価)

同じ原子命題の集合を持つ2つの確率時間オートマトンを $M = (Q, Steps, L)$ と $M' = (Q', Steps', L')$ とする。以下の条件を満たすような、 M と M' の状態集合のカルテジアン積上の同値関係である確率時間双模倣関係 $\mathcal{R} \subseteq Q \times Q'$ が存在するならば、2つの確率時間オートマトン M と M' は確率時間双模倣等価である ($M \equiv M'$ と表記する) :

- (1) M' が M を確率時間模倣する場合 :
 - (a) $(q, q') \in \mathcal{R}$ かつ $q \xrightarrow{p_q}_t$ であるときはいつも、 $q' \xrightarrow{p_{q'}}_t$ かつ $p_q \equiv_{\mathcal{R}} p_{q'}$ である。さらに、 $L(q) = L'(q')$ である。
 - (b) M のすべての初期状態 $q_0 \in Q$ に対して、 $(q_0, q'_0) \in \mathcal{R}$ となる M' の初期状態 $q'_0 \in Q'$ が存在する。
- (2) M が M' を確率時間模倣する場合 :
 - (a) $(q, q') \in \mathcal{R}$ かつ $q' \xrightarrow{p_{q'}}_t$ であるときはいつも、 $q \xrightarrow{p_q}_t$ かつ $p_{q'} \equiv_{\mathcal{R}} p_q$ である。さらに、 $L'(q') = L(q)$ である。
 - (b) M' のすべての初期状態 $q'_0 \in Q'$ に対して、 $(q_0, q'_0) \in \mathcal{R}$ となる M の初期状態 $q_0 \in Q$ が存在する。

■

次に、確率時間双模倣等価の事例を示す。

Example 5 (確率時間双模倣等価の事例)

図2の2つの確率時間オートマトン $M_1 = (Q_1, Steps_1, L_1)$ と $M_2 = (Q_2, Steps_2, L_2)$ を考える。2つの確率時間オートマトンが確率時間双模倣等価であることを示す。

関係 $\mathcal{R} \subseteq Q_1 \times Q_2$ が以下の条件を満たすことを示す。

1. まず、 M_2 が M_1 を確率時間模倣することを調べる。

- (1) $(q, r) \in \mathcal{R}$ と $q \xrightarrow{p_q}_2$ に対して、 $r \xrightarrow{p_r}_2$ かつ $p_q \equiv_{\mathcal{R}} p_r$ である。
さらに、 $L_1(q) = L_2(r) = a$ である。
以下に、 $p_q \equiv_{\mathcal{R}} p_r$ を示す：
まず、 $Q = \{q_1, q_2, r_1, q_3, r_2\}$ とし、 Q 上の同値関係を $\mathcal{R}$ とする。また、商集合 $Q/\mathcal{R}$ の同値類の集合を $\{C_x, C_y\}$ として、 $C_x = \{q_1, r_1\}$ と $C_y = \{q_2, q_3, r_2\}$ とする。ただし、 $p_q(q_1) = \frac{1}{2}$ 、 $p_q(q_2) = \frac{1}{8}$ 、 $p_q(q_3) = \frac{3}{8}$ 、 $p_r(r_1) = \frac{1}{2}$ 、

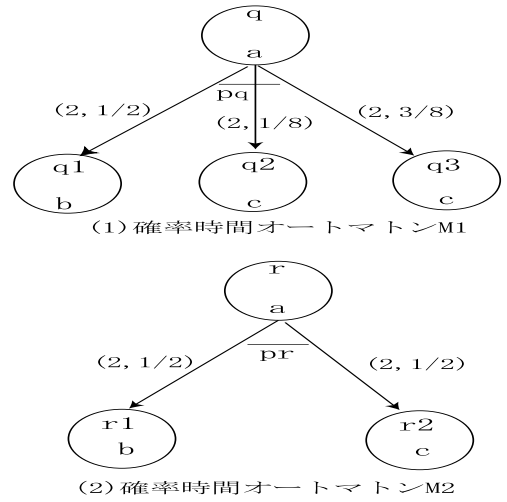


図2 確率時間双模倣等価の例

Fig. 2 Example of probabilistic timed bisimulation equivalence.

$p_r(r_2) = \frac{1}{2}$ とする。以下が成り立つ：

- (a) $p_q[C_x] = p_q(q_1) + p_q(r_1) = \frac{1}{2} + 0 = \frac{1}{2} = p_r(q_1) + p_r(r_1) = 0 + \frac{1}{2} = p_r[C_x]$
- (b) $p_q[C_y] = p_q(q_2) + p_q(q_3) + p_q(r_2) = 0 + \frac{1}{8} + \frac{3}{8} + 0 = \frac{1}{2} = p_r(q_2) + p_r(q_3) + p_r(r_2) = 0 + 0 + \frac{1}{2} = p_r[C_y]$

以上より、 $p_q \equiv_{\mathcal{R}} p_r$ である。

- (2) $(q_1, r_1) \in \mathcal{R}$ と $q_1 \xrightarrow{p_{q_1}}_1$ に対して、 $r_1 \xrightarrow{p_{r_1}}_1$ かつ $p_{q_1} \equiv_{\mathcal{R}} p_{r_1}$ である。
さらに、 $L_1(q_1) = L_2(r_1) = b$ である。
- (3) $(q_3, r_2) \in \mathcal{R}$ と $q_3 \xrightarrow{p_{q_3}}_3$ に対して、 $r_2 \xrightarrow{p_{r_2}}_3$ かつ $p_{q_3} \equiv_{\mathcal{R}} p_{r_2}$ である。
さらに、 $L_1(q_3) = L_2(r_2) = b$ である。

また、 M_1 の初期状態 $q \in Q_1$ に対して、 $(q, r) \in \mathcal{R}$ となる M_2 の初期状態 $r \in Q_2$ が存在する。

以上より、 M_2 が M_1 を確率時間模倣する。

2. 次に、 M_1 が M_2 を確率時間模倣することを調べる。

- (1) $(r, q) \in \mathcal{R}$ と $r \xrightarrow{p_r}_2$ に対して、 $q \xrightarrow{p_q}_2$ かつ $p_r \equiv_{\mathcal{R}} p_q$ である。
さらに、 $L_2(r) = L_1(q) = a$ である。
- (2) $(r_1, q_1) \in \mathcal{R}$ と $r_1 \xrightarrow{p_{r_1}}_1$ に対して、 $q_1 \xrightarrow{p_{q_1}}_1$ かつ $p_{r_1} \equiv_{\mathcal{R}} p_{q_1}$ である。
さらに、 $L_2(r_1) = L_1(q_1) = b$ である。
- (3) $(r_2, q_3) \in \mathcal{R}$ と $r_2 \xrightarrow{p_{r_2}}_3$ に対して、 $q_3 \xrightarrow{p_{q_3}}_3$ かつ $p_{r_2} \equiv_{\mathcal{R}} p_{q_3}$ である。
さらに、 $L_2(r_2) = L_1(q_3) = b$ である。

また、 M_2 の初期状態 $r \in Q_2$ に対して、 $(r, q) \in \mathcal{R}$ となる M_1 の初期状態 $q \in Q_1$ が存在する。

以上より, M_1 が M_2 を確率時間模倣する.

以上の 1. と 2. より, 2 つの確率時間オートマトン M_1 と M_2 は確率時間双模倣等価にある.

■

4.2 確率時間双模倣関係による確率時間時相論理式の保存

ここでは, 確率時間双模倣関係にある 2 つの確率時間オートマトンは確率時間時相論理式の同じ集合を満たすことを示す. ここでは, 双模倣関係による CTL^* の保存性の証明²⁰⁾ を基礎として, 以下に証明を行う.

以下の Lemma は確率時間時相論理と確率時間双模倣関係との結び付きを構築するときに重要である. 同じ原子命題の集合を持つ 2 つの確率時間オートマトンを $M = (Q, Steps, L)$ と $M' = (Q', Steps', L')$ とする. また, 2 つの確率時間オートマトン M と M' の確率時間双模倣関係を R とする.

M のパス $\omega = q_0 \xrightarrow{p_0} q_1 \xrightarrow{p_1} q_2 \xrightarrow{p_2} q_3 \dots \xrightarrow{p_{n-1}} q_n \dots$ と M' のパス $\omega' = q_0' \xrightarrow{p_0'} q_1' \xrightarrow{p_1'} q_2' \xrightarrow{p_2'} q_3' \dots \xrightarrow{p_{n-1}'} q_n' \dots$ が対応する必要十分条件は, 任意の $i \geq 0$ に対して $(q_i, q_i') \in R$ である.

Lemma 1 (対応するパスの存在性)

同じ原子命題の集合を持つ 2 つの確率時間オートマトンを $M = (Q, Steps, L)$ と $M' = (Q', Steps', L')$ が確率時間双模倣関係 R にあるとする. ここで, $(q, q') \in R$ となる 2 つの状態を q と q' とする. q から始まるすべてのパスに対して, q' から始まる対応するパスが存在して, かつ, q' から始まるすべてのパスに対して, q から始まる対応するパスが存在する.

Proof 1 (1) まず, q から始まるすべてのパスに対して, q' から始まる対応するパスを構成する.

ここで, $(q, q') \in R$ であり, $q = q_0$ から始まるパス

$$\omega = q_0 \xrightarrow{p_0} q_1 \xrightarrow{p_1} q_2 \xrightarrow{p_2} \dots$$

とする.

以下では, $q' = q_0'$ から始まるパス

$$\omega' = q_0' \xrightarrow{p_0'} q_1' \xrightarrow{p_1'} q_2' \xrightarrow{p_2'} \dots$$

を帰納的に構成する.

- (a) まず, 明らかに, $(q_0, q_0') \in R$ である.
- (b) 次に, ある $i > 0$ に対して, $(q_i, q_i') \in R$ を仮定する. $(q_i, q_i') \in R$ かつ $q_i \xrightarrow{p_i} q_{i+1}$ なので, $q_i' \xrightarrow{p_i'} q_{i+1}'$ かつ $p_i' \equiv_{\mathcal{R}} p_i$ と $t_i = t_i'$ であり, $L(q_{i+1}) = L'(q_{i+1}')$ である q_{i+1}' が存在して, $(q_{i+1}, q_{i+1}') \in R$ となる.

以上を繰り返すと,

ω と対応するパス

$$\omega' = q_0' \xrightarrow{p_0'} q_1' \xrightarrow{p_1'} q_2' \xrightarrow{p_2'} \dots$$

が構成できる.

- (2) 次に, q' から始まるすべてのパスに対して, q から始まる対応するパスを構成する. 上記と同様に構成できるので, ここでは省略する.

■

Lemma 2 (確率時間時相論理式の充足性の保存) 確率時間オートマトン M , M の adversary の集合 $\mathcal{A}$ と確率時間時相論理式 ϕ が与えられたとする. R は確率時間双模倣関係であり, q と q' は確率時間双模倣な状態 $(q, q') \in R$ とする. このとき, $q \models_{\mathcal{A}} \phi \iff q' \models_{\mathcal{A}} \phi$ が成り立つ.

Proof 2 我々は ϕ の構造に関する帰納法によって補題を証明する.

- (1) $\phi = \text{true}$ のとき
 $(q, q') \in R$ なので, $L(q) = L(q')$ である.
 ゆえに, $q \models_{\mathcal{A}} \text{true} \iff q' \models_{\mathcal{A}} \text{true}$ が成り立つ.
- (2) $\phi = a$ のとき
 $(q, q') \in R$ なので, $L(q) = L(q')$ である.
 ゆえに, $q \models_{\mathcal{A}} a \iff q' \models_{\mathcal{A}} a$ が成り立つ.
- (3) $\phi = \phi_1 \wedge \phi_2$ のとき
 このとき, 以下がいえる:
 $q \models_{\mathcal{A}} \phi_1 \wedge \phi_2 \iff q \models_{\mathcal{A}} \phi_1 \text{ かつ } q \models_{\mathcal{A}} \phi_2$
 $\iff q' \models_{\mathcal{A}} \phi_1 \text{ かつ } q' \models_{\mathcal{A}} \phi_2$ (帰納法の仮定)
 $\iff q' \models_{\mathcal{A}} \phi_1 \wedge \phi_2$.
- (4) $\phi = \neg \phi_1$ のとき
 このとき, 以下がいえる:
 $q \models_{\mathcal{A}} \neg \phi_1 \iff q \not\models_{\mathcal{A}} \phi_1$
 $\iff q' \not\models_{\mathcal{A}} \phi_1$ (帰納法の仮定)
 $\iff q' \models_{\mathcal{A}} \neg \phi_1$.
- (5) $\phi = [\phi_1 \exists U_{\delta} \phi_2]_{\geq \lambda}$ のとき

このとき, ある $A \in \mathcal{A}$ に対して, $\text{Prob}(\{\omega | \omega \in \text{Path}_{f_{ui}}^A(q) \text{ かつ } \omega \models_{\mathcal{A}} \phi_1 U_{\delta} \phi_2\}) \geq \lambda$ であり, $\omega \models_{\mathcal{A}} \phi_1 U_{\delta} \phi_2$ は以下のパス ω が存在することを意味する:

$\tau_{\omega}((i, t_i)) \in \delta$ かつ $\omega((i, t_i)) \models \phi_2$ であるような ω の位置 (i, t_i) が存在する. そして, $(j, t_j) <_{\omega} (i, t_i)$ のすべての (j, t_j) に対して, $\omega((j, t_j)) \models \phi_1 \vee \phi_2$ である.

ここで, Lemma 1 より, パス ω と対応するパス ω' が存在するので, パス ω の位置 (i, t_i)

に対応する, パス ω' の位置 $(i', t_{i'})$ およびパス ω の位置 (i_m, t_m) に対応する, パス ω' の位置 (i_m', t_m') が存在する.

(a) このとき, $(\omega'((i', t_{i'})), \omega((i, t))) \in \mathcal{R}$ かつ $\tau_{\omega'}((i', t_{i'})) = \tau_{\omega}((i, t)) \in \delta$ であり, 帰納法の仮定によって $\omega'((i', t_{i'})) \models \phi_2$ である.

(b) さらに, すべての $(i_m', t_m') <_{\omega'} (i', t_{i'})$ に対して, 位置 (i_m', t_m') に対応する位置 (i_m, t_m) が存在して, $(\omega'((i_m', t_m')), \omega((i_m, t_m))) \in \mathcal{R}$ であり, $(i_m', t_m') <_{\omega'} (i', t_{i'})$ なので, 帰納法の仮定により $\omega'((i_m', t_m')) \models \phi_1$ である.

以上より, $q' \models_{\mathcal{A}} [\phi_1 \exists U_{\delta} \phi_2]_{\exists \lambda}$ である.

(6) $\phi = [\phi_1 \forall U_{\delta} \phi_2]_{\exists \lambda}$ のとき
 $\phi = [\phi_1 \exists U_{\delta} \phi_2]_{\exists \lambda}$ のときと同様な方法で証明できる.

■

Theorem 1 (確率時間時相論理式の保存性)

2つの確率時間オートマトン $M_1 = (Q_1, Steps_1, L_1)$ と $M_2 = (Q_2, Steps_2, L_2)$, 確率時間時相論理式 ϕ が与えられたとする. もし, 2つの確率時間オートマトン M_1 と M_2 が確率時間双模倣等価であり, $(q_1, q_2) \in R$ ならば, $q_1 \models_{\mathcal{A}} \phi \iff q_2 \models_{\mathcal{A}} \phi$ である. ただし, R は確率時間双模倣関係であり, $q_1 \in Q_1$ と $q_2 \in Q_2$ である.

Proof 3 Lemma 2 の証明において, $(q, q') \in \mathcal{R}$ を $(q_1, q_2) \in \mathcal{R}$ と置き換えることにより, この定理の証明は得られるので, ここでは省略する.

■

5. ま と め

本論文では, 以下の2つの成果を述べた:

- (1) まず, 確率時間オートマトンの一般的な確率時間双模倣関係を世界で最初に定義した.
- (2) 次に, その確率時間双模倣関係にある2つの確率時間オートマトンは確率時間時相論理式の同じ集合を満たすことを示した.

この種の双模倣関係は確率時間オートマトンの抽象化を保証するための重要な道具となりえ, 実用上から非常に重要である.

今後の研究課題としては, 以下がある.

- (1) 本論文で提案した確率時間双模倣関係を用いて, 大規模なリアルタイムシステムから小規模な抽象的なリアルタイムシステムを構成して, 大

模なりリアルタイムシステムの正当性を検証する予定である. この場合, 確率時間双模倣な小規模システムをいかに効率的に構成するかが非常に重要となり, 今後の研究が必要な分野である.

(2) 内部動作を考慮した弱確率時間双模倣を定義して, 弱確率時間双模倣にある2つの確率時間オートマトンは確率時間時相論理式の同じ集合を満たすことを示す.

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み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 年度 ~ 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*, p.316, Kluwer Academic Pub. (1991).
- 2) de Bakker, J.W., 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*, Vol.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*, IEEE Computer Society, pp.79-82 (2003).

- 10) Jonsson, B. and Larsen, K.G.: Specification and Refinement of Probabilistic Processes, *International Symposium on Logic in Computer Science*, pp.266–277, IEEE Computer Society (1991).
- 11) Hansson, H.A.: Time and Probability in Formal Design of Distributed Systems, Ph.D. Thesis, Uppsala University (1991).
- 12) Segala, R.: Modeling and Verification of Randomized Distributed Real-Time Systems, Ph.D. Thesis, MIT (1995).
- 13) Cerans, K.: Decidability of Bisimulation Equivalences for Processes with Parallel Timers, *LNCS 663*, pp.302–315 (1992).
- 14) Tasiran, S., Alur, R., Kurshan, R.P. and Brayton, R.K.: Verifying abstractions of timed systems, *LNCS 1119*, pp.546–562 (1996).
- 15) Yamane, S.: A Practical Hierarchical Design by Timed Simulation Relations for Real-Time Systems, *LNCS 1641*, pp.151–167 (1998).
- 16) Vardi, M.Y.: Automatic verification of probabilistic concurrent finite-state systems, *Proc. 26th IEEE Symp. Found. of Comp. Sci.*, pp.327–338 (1985).
- 17) Tripakis, S. and Yovine, S.: Analysis of timed systems based on time-abstracting bisimulations, *Formal Methods in System Design*, Vol.18, pp.25–68, Kluwer Academic Publishers (2001).
- 18) Segala, R.: Verification of Randomized Distributed Algorithms, *LNCS 2090*, pp.232–260 (2001).
- 19) Jonsson, B., Yi, W. and Larsen, K.G.: Probabilistic Extensions of Process Algebra, *Handbook of Process Algebra*, North-Holland, pp.685–710 (1991).
- 20) Clarke, E.M., Grumberg, O. and Peled, D.A.: *Model Checking*, The MIT Press (1999).

(平成 15 年 7 月 1 日受付)

(平成 16 年 3 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。