数理解析研究所講究録
1489巻 2006年 1-7

確率時間オートマトンの確率時間弱模倣検証理論

Verification Theory of Probabilistic Timed Weak Simulation for Probabilistic Timed Automata (Extended Abstraction)

橋爪裕樹* 山根智†
Yuki Hashizume Satoshi Yamane
金沢大学 工学部 情報システム工学科
Department of Infomation and Systems Engineering,Faculty of Engineering,
Kanazawa University

概要

Probabilistic behaviors are requested to be exhibited immediately for real-time systems such as wireless protocols because immediacy is important for their securities. Moreover, as their components behave concurrently, it is difficult to assure their reliabilities. In this paper, we propose a probabilistic timed weak simulation verification and its decidability on the models of Probabilistic Timed Automata. To this purpose, we formalize real-time systems by Probabilistic Timed Automata. Then, the conditions (described in the specification) are kept about its implementation in a timed and probabilistic setting for the behaivors worked with their environment. It is useful for the stepwise refinement.

Keywords; probabilistic real-time systems, probabilistic timed weak simulation, Probabilistic Timed Automaton, stepwise refinement

1 まえがき

1.1 研究の背景

近年，巨大化・並列化・分散化などコンピュータソフトウェアやシステムの複雑化が進んでいる．また，それらへの社会環境の依存度の高さから，その信頼性保証の要求がより高まりつつある．その要求に応えうる一つの手段として行われているものが，形式的検証法である．形式的検証は，実在の検証対象のシステムをオートマトンやグラフなどの数学モデルで抽象的に記述し，状態空間で網羅的検証を行うことでバグを発見する方法として期待されている．

本論文では，形式的検証の対象として確率時間オートマトンというモデルを用いる．また，ソフトウェアやシステムを確率時間オートマトンでモデル化する方法については述べず，既にモデル化されたものについての検証法を述べる．確率時間オートマトンは，即時性が求められかつランダム動作を行う，確率的なリアルタイムソフトウェアやシステム（通信プロトコルなど）の検証を可能とする数学モデルである [6]．このモデルは，時間制約（5単位時間内以内に動作を完了するなど）と確率条件（90%でデータの衝突が発生しないなど）をオートマトン上に記述することで，PTCTLという式 [6] で記述されたシステムの動作（初期状態から20単位時間内に80%以上で送信完了状態に到達可能など）を自動的に解析可能である．理論的には，ω オートマトンを拡張した時間オートマトン [1] を，更に確率動作に対応できるよう拡張したという背景がある．

ここで，前述のサブシステムの設計では、以下に挙げる事柄により，設計が困難となる．

1. 各サブシステムは他のサブシステムと協調動作して，全体としての確率的リアルタイム処理を行う．このとき仕様記述で，外部の環境と相互作用する動作を**外部動作**，その他の動作を**内部動作**として記述する．この際，外部観測可能な外部動作と内部動作で区別して，サブシステムの仕様記述を行うべきである．
2. 確率的リアルタイムシステム全体は複雑なため，抽象化された各サブシステムの上位の仕様から，詳細化記述を行った下位の仕様を段階的

*E-mail: hashizume@csl.ec.t.kanazawa-u.ac.jp
†E-mail: syamane@is.t.kanazawa-u.ac.jp
‡〒 920-1192 金沢市角間町 金沢大学工学部情報システム工学科

に設計する．この際，下位の仕様は上位の仕様を満たす（整合性を保証する）必要がある．

以上の点を踏まえ，本論文では外部動作と内部動作の区別がある，非決定性確率時間オートマトンで各サブシステムの仕様を記述する．また，確率的リアルタイムシステム全体は，全サブシステムの並列合成により構成可能とする．そして，仕様の階層間の整合性を保つ検証法として，確率時間弱模倣検証を提案し，その決定可能性を示す．

確率時間弱模倣検証とは，外部観測・時間制約・確率条件の三つの観点から，下位の仕様が上位の仕様を満たしているかを判定する検証法である．具体的には，下位の仕様があるタイミング（確率），ある外部イベントにより動作するとき，上位の仕様は同じタイミング（確率），同じ外部イベントにより動作可能である．なお，本論文では非決定性動作を決定性動作にすることなどで動作を狭めることや，モデルの動作を具体化して，内部動作の追加や削除が発生するようなものを詳細化の作業とする．

1.2 関連研究

本研究と関連する，形式的手法により確率的システムを記述し，その正当性を検証する方法については，以下のような重要な既存研究が存在する．

1. 1995年，R.Segalaらは，強・弱の（双）確率模倣関係が確率オートマトン上で保存する動作をPCTL式やWPCTL式という式で示した[4]。
2. 1999年，M.Kwiatkowskaらにより，確率時間オートマトンが提案され，そのモデルのModel-Checkingアルゴリズムが提案された[6].
3. 2003年，C.Baierらは，有限状態のマルコフ連鎖上で，確率弱模倣関係が多項式時間で決定可能であることを示した[7]．しかし，(非決定性を含む）確率オートマトン上での弱模倣関係の計算については述べられていない．
4. 2003年，R.Lanotteらは“確率分布の非決定性”や“状態（本論文ではロケーションと呼ぶ）上での時間制約”を持たない，確率時間オートマトン上で弱双模倣関係を定義し，その関係を計算するアルゴリズムを提案した[3]．ただし，双模倣関係は段階的詳細化には適用できず，上記の理由からモデルの表現力が低い．
5. 2003年，S.Yamaneが確率リージョングラフ上での，確率時間オートマトンの確率時間強模倣関係の決定可能性を示した[8]。
6. 2005年，H.Koderaが確率時間オートマトン上の確率時間強模倣関係の定義とその計算アルゴリズムを示した[10].

1.3 研究の目的

本論文では，M.Kwiatkowskaらの確率時間オートマトンに変更を加え，確率時間弱模倣関係の定義を与える．そして，その確率リージョングラフ上での決定可能性とその例を示す．

1.4 構成

以降の本論文の構成は以下の通りである．まず2節で確率時間オートマトンと確率時間弱模倣関係を定義し，その決定可能性を与える．次に，3節で確率時間弱模倣関係を例を用い説明する．最後に4節で結論と今後の課題を述べる．

2 確率時間オートマトンと確率時間弱模倣関係の定義

本節では，確率時間オートマトンと確率時間弱模倣関係の定義を行い，その決定可能性を示す．

2.1 確率時間オートマトンのSyntaxとSemanticsの定義

オートマトンは形式的な構造を示す**構文(Syntax)**と，その構造上での動作を示す**意味(Semantics)**から成る．**確率時間オートマトン**(Probabilistic Timed Automaton;PTA)[6,10]は，時間オートマトン(TA)[1]に**離散確率分布**を加え，拡張したモデルであり，TAは，有限オートマトンに時間を示す**クロック変数**による制約を付加したモデルである．

PTA上のロケーションや辺には**時間制約**が与えられる．ここで，時間制約を満たすクロック値の集合は，以下に示される**ゾーン**と呼ばれる凸集合で定式的に示される．凸集合とは，その集合上の任意の二つの元を結ぶ線分上のどの点もまた，その集合の元であるような空間上の部分集合である．

Definition 1(Zoneの Syntax)
Xを非負の実数変数の有限集合，$|X|$を変数の総数とする時，以下の集合を$Zone$とする。

$$\mathbf{Z}_X=\left\{\left.\bigwedge_{0\le i\neq j\le|X|} x_i-x_j\prec c_{ij}\;\right|\;\begin{array}{l}x_0=0,x_i,x_j\in X,\\(i,j\in\{1,\ldots,|X|\})\\\prec\in\{<,\le\},\\c_{ij}\in\mathbb{Z}\cup\{\infty\}\end{array}\right\}$$

一つのZone（$\mathbf{Z}_X$の要素）が一つの時間制約を表す．

次に，Zone の意味する内容 (Semantics) を以下の定義により与える．

Definition 2(Zone の Semantics)
$[\![\cdot]\!] : \mathbf{Z}_X \to 2^{\mathbb{R}^{|X|}_{\geq 0}}$ を Zone の Semantics，$1 \leq i \neq j \leq |X|$ として次式で定義する．

$$[\![x_i - x_j \prec c_{ij}]\!] = \Big\{(a_1, a_2, \ldots, a_{|X|}) \in \mathbb{R}^{|X|}_{\geq 0} \mid a_i - a_j \prec c_{ij}, 1 \leq k \leq |X| \text{ に対して } a_k \in \mathbb{R}_{\geq 0}\Big\}$$

また，辺に与えられる離散確率分布は以下のように定義される．

Definition 3(離散確率分布)
U を空でない集合として，U 上の離散確率分布の集合を次式で定義する．

$$Dist(U) = \left\{ \mu \,\middle|\, \mu : U \to [0,1]\ s.t. \sum_{s \in U} \mu(s) = 1 \right\}$$

以上の定義を元に，PTA の Syntax を与える．

Definition 4(PTA の Syntax)
PTA $\mathcal{A}$ は，以下の 7 つの組 $\langle S, \bar{s}, \Sigma, X, inv, prob, \langle g_s \rangle_{s \in S} \rangle$ で定義される．

1. ロケーションの有限集合 S.
2. 初期ロケーション $\bar{s} \in S$.
3. アクションラベルの有限集合 $\Sigma = EXT \cup \{\tau\}$. (ここで，$EXT$ は外部イベントの有限集合．τ は内部イベントである)．
4. クロック変数と呼ばれる非負実数値を取る変数の有限集合 X.
5. 各ロケーションに時間制約（不変条件）を与える関数 $inv : S \to \mathbf{Z}_X$.
6. 各ロケーションに対し，そのロケーションから外向きに出る辺の集合を与える関数 $prob : S \to 2^{\Sigma \times 2^X \times Dist(S)}$ (ここで，辺はアクションラベル，リセットされるクロックの集合，離散確率分布の 3 つ組となる)．
7. ロケーション s から外向きに出ている各辺 $e \in prob(s)$ の集合に対し，時間制約（遷移可能条件）の集合を与える関数 $g_s : prob(s) \to \mathbf{Z}_X$ の有限集合（関数族）$\langle g_s \rangle_{s \in S}$.

次に，ある時刻，あるイベント列実行後の動作範囲を規定する状態を定義する．PTA 上の状態はロケーションと各クロック変数の値の組で構成される．

Definition 5(PTA の状態)
PTA $\mathcal{A}$ の状態を集合 $states(\mathcal{A}) = \bigcup_{s \in S_\mathcal{A}} \{\langle s, \mathbf{a} \rangle | \mathbf{a} \in [\![inv_\mathcal{A}(s)]\!]\} \subseteq S_\mathcal{A} \times \mathbb{R}^{|X|}_{\geq 0}$ の元とする．

Definition 6(PTA の初期状態)
任意の PTA $\mathcal{A}$ に対し，$\bar{q} = \langle \bar{s}, (0, \ldots, 0) \rangle \in states(\mathcal{A})$ となる状態（初期ロケーションと全クロック値 0 の組）が存在するとし，これを初期状態と呼ぶ．

さらに，PTA の動作を定義するため，状態遷移を以下のように定義する．

Definition 7(PTA の Semantics)
PTA の遷移には時間遷移と離散遷移の二通りがある．

1. 時間遷移 (Timed Transition)
状態 $\langle s, \mathbf{a} \rangle$ において，ある $\delta \in \mathbb{R}_{>0}$ に対し，条件 $\mathbf{a} \in [\![inv_\mathcal{A}(s)]\!] \wedge \mathbf{a} + (\delta, \ldots, \delta) \in [\![inv_\mathcal{A}(s)]\!]$ が真である時，状態 $\langle s, \mathbf{a} \rangle$ から時間経過量 δ の時間遷移が可能と言い，
$$\langle s, \mathbf{a} \rangle \xrightarrow{\delta} \langle s, \mathbf{a} + (\delta, \ldots, \delta) \rangle$$
と書く．
2. 離散遷移 (Discrete Transition)
   - （遷移可能条件）$(\sigma, \lambda, \mu) \in prob(s)$ とし ($\sigma \in \Sigma, \lambda \subset X$)，状態 $q = \langle s, \mathbf{a} \rangle$ にて，$\mathbf{a} \in [\![g_s((\sigma, \lambda, \mu))]\!]$ を満たす辺 $e = (\sigma, \lambda, \mu)$ が選択される．
   - （状態上の確率分布）s' と $\mathbf{a}[\lambda := 0]$（各クロック変数の値 $\mathbf{a}$ について $\lambda \subset X$ で指定されるクロック変数の値を全てリセットしたもの）に対し，
   $$p^e_q(\langle s', \mathbf{a}[\lambda := 0] \rangle) = \mu(s')$$
   として，$S_\mathcal{A}$ から引数をとる μ を元に，$States(\mathcal{A})$ から引数をとる状態上の離散確率分布 $p^e_q \in Dist(S_\mathcal{A} \times \mathbb{R}^{|X|}_{\geq 0})$ を構成．
   - 確率的メカニズムに従い，$p^e_q(\langle s', \mathbf{a}[\lambda := 0] \rangle) > 0$ を満たす遷移先の状態が選択される．

ここで，遷移可能条件を満たしても，遷移先の不変条件が満たされていない時，モデル化が間違っているとみなす．上記の遷移は次の条件を満たす時に行われる．

$$\mathbf{a} \in [\![g_s((\sigma, \lambda, \mu))]\!] \ \wedge\ \exists \langle s', \mathbf{a}[\lambda := 0] \rangle \in states(\mathcal{A})$$
$$s.t. \{\mathbf{a}[\lambda := 0] \in [\![inv(s')]\!] \ \wedge\ p^q_e(\langle s', \mathbf{a}[\lambda := 0] \rangle) > 0\}$$

このとき，条件を満たす離散遷移を以下のように書く．

$$\langle s, \mathbf{a} \rangle \xrightarrow{\sigma} \langle s', \mathbf{a}[\lambda := 0] \rangle$$

また，ある確率分布 p に遷移したとし，到達しうる全状態を考慮する時，$\langle s, \mathbf{a} \rangle \xrightarrow{\sigma} p$ と書く．

2.2 確率時間弱模倣関係

まず弱遷移 [4] について説明を行う．弱遷移は内部の計算が環境や他のシステムに影響しないことから，

遷移列を可観測の遷移にのみ注目し，まとめたものである．一般に$(\xrightarrow{\tau})^*$を$\Longrightarrow$で，$(\xrightarrow{\tau})^* \xrightarrow{a} (\xrightarrow{\tau})^*$を$\overset{a}{\Longrightarrow}$で表記する。ここで$\Longrightarrow$は内部遷移さえ実行しないことがある．また，ある弱遷移を経て，全体としてある確率分布pが得られた時，弱遷移により分布pに到達したとし，$\langle s, \mathbf{a}\rangle \overset{\sigma}{\Longrightarrow} p$と書く．

上記を前提とし，確率時間弱模倣関係の定義を行う．それは時間弱模倣関係 [9] と確率弱模倣関係 [4] の組み合わせとして与えられる．

Definition 8(確率時間弱模倣関係)
PTA $\mathcal{A} = (S_A, \bar{s}_A, \Sigma_A, X_A, inv_A, prob_A, \langle g_s^A\rangle_{s\in S_A})$, $\mathcal{B} = (S_B, \bar{s}_B, \Sigma_B, X_B, inv_B, prob_B, \langle g_s^B\rangle_{s\in S_B})$ の2つの状態集合上で次の条件を満たす二項関係 $R \subset states(\mathcal{A}) \times states(\mathcal{B})$ を確率時間弱模倣関係と言う．また，確率時間弱模倣関係 R の中で最大の集合を $R_{[\mathcal{A}\times\mathcal{B}]}$ で表す．ここで，$\lambda \subset X$ を時間遷移実行前の弱遷移によりリセットされるクロック変数の集合，$\lambda' \subset X$ を時間遷移実行後の弱遷移によりリセットされるクロック変数の集合，$q_1 = \langle s_1, \mathbf{a} + (\delta, \ldots, \delta)\rangle, q_2 = \langle s_3, (\mathbf{b}[\lambda := 0] + (\delta, \ldots, \delta))[\lambda' := 0]\rangle$ とする．全ての $(\langle s_1, \mathbf{a}\rangle, \langle s_2, \mathbf{b}\rangle) \in R$ に対し，

1. 時間模倣条件:
$\forall \delta \in \mathbb{R}^{>0}, \langle s_1, \mathbf{a}\rangle \xrightarrow{\delta} q_1$ならば，
$\exists \langle s_2, \mathbf{b}\rangle \overset{\delta}{\Longrightarrow} p \wedge (\forall q_2 (p(q_2) > 0), (q_1, q_2) \in R)$
2. 確率模倣条件:
全ての $e_1 = (\sigma, \lambda, \mu_1) \in prob_A(s_1)$ に対し，
$\langle s_1, \mathbf{a}\rangle \xrightarrow{\sigma} p_1$ならば，$\exists \langle s_2, \mathbf{b}\rangle \overset{\sigma}{\Longrightarrow} p_2$ $s.t. (p_1 \sqsubseteq_R p_2)$

ここで条件 1. と 2. の連言が模倣な状態である条件である．また，$p_1 \in Dist(S \times \mathbb{R}_{\geq 0}^{|X|}), p_2 \in Dist(S \times \mathbb{R}_{\geq 0}^{|X|})$ に対し，

$$p_1 \sqsubseteq_R p_2 \Longleftrightarrow \exists w : states(\mathcal{A}) \times states(\mathcal{B}) \to [0,1]\ s.t.$$
$$\begin{cases} 1)\ \forall q_1 \in states(\mathcal{A}), \sum_{q_2 \in states(\mathcal{B})} w(q_1, q_2) = p_1(q_1), \\ 2)\ \forall q_2 \in states(\mathcal{B}), \sum_{q_1 \in states(\mathcal{A})} w(q_1, q_2) = p_2(q_2), \\ 3)\ \text{全ての } (q_1, q_2) \in states(\mathcal{A}) \times states(\mathcal{B}) \text{ に対し，} \\ \quad w(q_1, q_2) > 0 \text{ ならば } (q_1, q_2) \in R \end{cases}$$

この関数 w を**重み関数**と言う．

次に，上記の各条件の成立例を図を用いて説明する．

図1は時間模倣条件の成立例である．このように，仕様側の内部遷移後に，確率1で実装側の時間遷移を模倣できる時，時間模倣条件は成立する．

次に，図2により確率模倣条件の成立例を説明する．図2は離散遷移 a に関する確率模倣条件を示す．

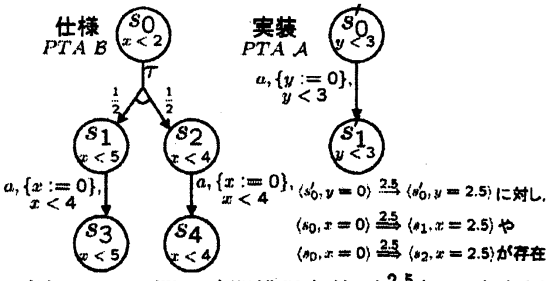

図 1: PTA 間の時間模倣条件 ($\xrightarrow{2.5}$) の成立例

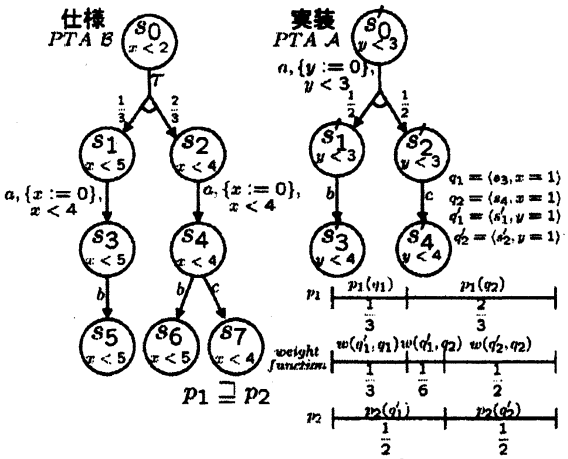

図 2: PTA 間の確率模倣条件 ($\xrightarrow{a}$) の成立例

$(q_1', q_1), (q_1', q_2), (q_2', q_2) \in R$ と p_1, p_2 の確率分布に対し，図のような重み関数が存在する．故に，確率模倣条件が成立していると言える．

PTA 間の確率時間弱模倣関係を上記の確率時間弱模倣関係を用いて，次のように定義できる．

Definition 9(PTA 間の確率時間弱模倣関係)
初期状態対 $(\bar{q}_A, \bar{q}_B)$ が $R_{[\mathcal{A}\times\mathcal{B}]}$ に含まれているとき，$\mathcal{A} \preceq_{ptws} \mathcal{B}$ と書き，PTA $\mathcal{A}$ は PTA $\mathcal{B}$ に確率時間弱模倣されると言う．

2つの PTA の確率時間弱模倣関係検証は，以下のように定義される．

Definition 10(確率時間弱模倣検証)
入力:二つの PTA $\mathcal{A}, \mathcal{B}$.
出力:$\mathcal{A} \prec_{ptws} \mathcal{B}$ ならば *yes* ／でなければ *no*.

2.3 確率時間弱模倣検証問題の決定可能性

前述の定義の状態と状態間の辺を構成しようとすると，時間稠密性からそれらが無限に存在するため，確率時間弱模倣関係が決定できない．例えば，図3における時間遷移は 0.5 と 0.51 の間ですら 0.505 や 0.501 など無限に存在する．そこで，クロックリージョン [1] により，状態や辺を有限の範囲で考える．

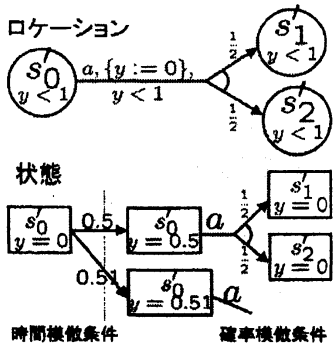

図 3: PTA と対応する状態と遷移のグラフ例

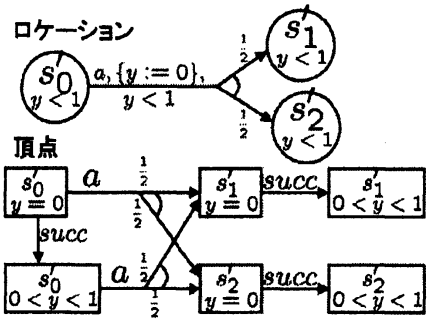

図 4: PTA と対応する確率リージョングラフの例

図 3 の状態や遷移を時間についてクロックリージョンでまとめると，六つの頂点（ロケーションとクロックリージョンの組）と五つの辺のみで表せる（図 4）．ここで，$\xrightarrow{succ}$ 遷移とは，現時の頂点と異なる，時間的に連続な頂点に到達する時の辺を指す．そして，このようなグラフを確率リージョングラフと呼ぶ．

Definition 11(頂点)
状態 $\langle s_1, \mathbf{a}\rangle$ について，同一ロケーションを持ち，同一なクロックリージョンに属するクロック値を持つ状態をまとめたものを頂点 $\langle s_1, [\mathbf{a}]\rangle$ と定義する．

Definition 12(時間とリセットの successor)
あるリージョン ρ に時間的に連続であり，時間経過で到達できるリージョン ρ' を ρ の**時間 successor** と言い，$\rho' = succ(\rho)$ とする．また，あるリージョン ρ について，$\lambda \subseteq X$ に属するクロック変数がリセットされた時の，リセット後のクロックリージョンを**リセット successor** と言い，$\rho[\lambda := 0]$ とする．

Definition 13(確率リージョングラフ)
リージョンの集合 $\mathcal{V}$ は，PTA $\mathcal{A}$ の条件式 $(\mathbf{Z}_X)$ に表れる最大の整数 C_A とクロック変数の集合 X_A を与えることで決まる．ここで PTA を $\mathcal{A}$，頂点の集合を $V \subseteq S_A \times \mathcal{V}_{(X_A \times C_A)}$，辺の集合を $E \subseteq V \times (\Sigma_A \cup \{succ\}) \times Dist(V)$ として，グラフ (V, X) を $\mathcal{A}$ に対する確率リージョングラフと言い，$\mathcal{R}_A$ と書く．ここで，$\overline{p} \in Dist(V)$ について以下のように定義する．

1.$\mathbf{a} \in \rho(\in \mathcal{V}_{(X_A \times C_A)})$ について $\mathbf{a}$ のいずれかのクロック値 $x_1 \in X_A$ について $x_1 \leq C_A$ であり，かつ $succ(\rho) \subseteq [\![inv_A(s)]\!]$ である時，辺 $(\langle s, \rho\rangle, succ, \overline{p}^{\langle s,\rho\rangle}_{succ}) \in E$ により到達可能な確率分布 $\overline{p}^{\langle s,\rho\rangle}_{succ} \in Dist(V)$ について，

$$\overline{p}^{\langle s,\rho\rangle}_{succ}(\langle s', \rho'\rangle) = \begin{cases} 1 & (if\ s' = s \wedge \rho' = succ(\rho)) \\ 0 & (otherwise) \end{cases}$$

2.$\exists(\sigma, \lambda, \mu) \in prob_A(s)$ **s.t.** $\rho \subseteq [\![\tau^A_s(\sigma, \lambda, \mu)]\!]$ が成立つ時，辺 $(\langle s, \rho\rangle, \sigma, \overline{p}^{\langle s,\rho\rangle}_{(\sigma,\lambda,\mu)}) \in E$ により到達可能な確率分布 $\overline{p}^{\langle s,\rho\rangle}_{(\sigma,\lambda,\mu)} \in Dist(V)$ について，

$$\overline{p}^{\langle s,\rho\rangle}_{(\sigma,\lambda,\mu)}(\langle s', \rho'\rangle) = \begin{cases} \mu(s') & (if\ \rho[\lambda := 0] = \rho') \\ 0 & (otherwise) \end{cases}$$

Definition 14(確率リージョングラフ上の遷移)
確率リージョングラフ $\mathcal{R}(\mathcal{A}) = (V, E)$ 上において，次の 2 種類の遷移を定義する．

1. 抽象化時間遷移

$(\langle s, \rho\rangle, succ, \overline{p}) \in E$ かつ $\rho' = succ(\rho)$ かつ $\overline{p}(\langle s, \rho'\rangle) = 1$ の場合（かつその場合に限り），$\langle s, \rho\rangle \xrightarrow{succ} \langle s, \rho'\rangle$ と書き，これを抽象化時間遷移と呼ぶ．

2. 抽象化離散遷移

$\sigma \neq succ$ とし，$(\langle s, \rho\rangle, \sigma, \overline{p}') \in E$ の場合（かつその場合に限り），$\langle s, \rho\rangle \xrightarrow{\sigma} \overline{p}'$ と書き，これを抽象化離散遷移と呼ぶ．

Definition 15(確率リージョングラフ上の確率弱模倣関係)
$\xrightarrow{succ}$ を n 回実行する遷移を $(\xrightarrow{succ})^n$ とする。また，弱遷移について $\overset{(succ)^n}{\Longrightarrow} = (\xrightarrow{\tau})^*(\xrightarrow{succ})^n(\xrightarrow{\tau})^*$ と定義する．PTA $\mathcal{A}, \mathcal{B}$ が与えられた時，その確率リージョングラフ $\mathcal{R}(\mathcal{A}) = (V_A, E_A), \mathcal{R}(\mathcal{B}) = (V_B, E_B)$ の二つの頂点集合上で次の条件を満たす二項関係 $\overline{R} \subseteq V_A \times V_B$ を確率弱模倣関係と言う．全ての $(\langle s_1, \rho_1\rangle, \langle s_2, \rho_2\rangle) \in \overline{R}$ に対し，

1. 時間模倣条件:
$\forall n \geq 1, \langle s_1, \rho_1\rangle(\xrightarrow{succ})^n v_1$ ならば，

$\exists \langle s_2, \rho_2\rangle \overset{(succ)^n}{\Longrightarrow} \overline{p} \wedge (\forall v_2(\overline{p}(v_2) > 0), (v_1, v_2) \in R)$

2. 確率模倣条件:
全ての $e_2 = (\langle s_1, \rho_1\rangle, \sigma, \overline{p}_1) \in E_A$ に対し，

$\langle s_1, \rho_1\rangle \xrightarrow{\sigma} \overline{p}_1$ ならば，$\exists \langle s_2, \rho_2\rangle \overset{\sigma}{\Longrightarrow} \overline{p}_2$ $s.t.(\overline{p}_1 \sqsubseteq_R \overline{p}_2)$

条件 1. と 2. の連言が模倣な状態である条件である．ここで，以下の定理が成り立つ．

Theorem 1(確率時間弱模倣関係の決定可能性)
2つのPTA $\mathcal{A},\mathcal{B}$ が与えられた時，確率時間弱模倣関係が存在する，iff, 2つのPTA $\mathcal{A},\mathcal{B}$ の確率リージョングラフ間に確率弱模倣関係が存在する．

（証明の方針）Zoneはクロック同値類より，細かく取ることはできない[10]（Zoneの最小単位がクロック同値類である）．

（PTAの確率時間弱模倣→確率リージョングラフの確率弱模倣）実装の $\langle s_1,\mathbf{a}\rangle \xrightarrow{\delta} \langle s_1,\mathbf{a}+(\delta,\ldots,\delta)\rangle$ が仕様側の $\langle s_2,\mathbf{b}\rangle \stackrel{\delta}{\Longrightarrow} p$ により模倣される時，確率リージョングラフの実装の $\langle s_1,\mathbf{a}\rangle$ を含む頂点からの $(\xrightarrow{succ})^n$ 遷移に対し，仕様側の $\langle s_2,\mathbf{b}\rangle$ を含む頂点から $\stackrel{(succ)^n}{\Longrightarrow}$ による弱遷移が存在する．その理由として，同じ頂点に属する状態は，遷移可能条件や不変条件に同様な真偽値を返すことが言える．故に，状態上の確率時間弱模倣関係から，$\langle s_2,\mathbf{b}\rangle$ を含む頂点は仕様側の τ による離散遷移について同様に実行できる．そして $succ$ 遷移の部分は強模倣関係時と同様に実行が保証される[8,10]．以上から時間模倣条件は保存される．

また，実装の $\langle s_1,\mathbf{a}\rangle \xrightarrow{\sigma} p_1$ が仕様側の $\langle s_2,\mathbf{b}\rangle \stackrel{\sigma}{\Longrightarrow} p_2$ に模倣される時，確率リージョングラフの実装の $\langle s_1,\mathbf{a}\rangle$ を含む頂点からの遷移 $\xrightarrow{\sigma}$ に対し，仕様側の $\langle s_2,\mathbf{b}\rangle$ を含む頂点から $\stackrel{\sigma}{\Longrightarrow}$ による弱遷移が存在する．これは離散遷移について上述の事実があるからである．

（確率リージョングラフの確率時間弱模倣→PTAの確率弱模倣）確率リージョングラフの実装の $\langle s_1,[\mathbf{a}]\rangle(\xrightarrow{succ})^n\langle s_1,[\mathbf{c}]\rangle$ が仕様側の $\langle s_2,[\mathbf{b}]\rangle \stackrel{(succ)^n}{\Longrightarrow} \overline{p}$ により模倣される時，実装の $\langle s_1,[\mathbf{a}]\rangle$ に含まれる状態の遷移 $\xrightarrow{\delta}$ に対し，仕様側の $\langle s_2,[\mathbf{b}]\rangle$ に含まれる状態から $\stackrel{\delta}{\Longrightarrow}$ による弱遷移が存在する．その理由として，頂点上の遷移可能条件や不変条件に対する真偽から，それに含まれる状態上でも離散遷移の実行が同様に保証される．故に，頂点上の模倣関係から，$\langle s_2,\mathbf{b}\rangle$ に含まれる状態は，仕様側の τ による離散遷移について同様に実行できる．そして $\xrightarrow{\delta}$ 遷移の部分は強模倣関係時と同様に実行が保証される[8,10]．以上から時間模倣条件は保存される．

また，実装の $\langle s_1,[\mathbf{a}]\rangle \xrightarrow{\sigma} \overline{p}_1$ が仕様側の $\langle s_2,[\mathbf{b}]\rangle \stackrel{\sigma}{\Longrightarrow} \overline{p}_2$ に模倣される時，実装の頂点 $\langle s_1,[\mathbf{a}]\rangle$ に含まれる状態からの遷移 $\xrightarrow{\sigma}$ に対し，仕様側の頂点 $\langle s_2,[\mathbf{b}]\rangle$ に含まれる状態から $\stackrel{\sigma}{\Longrightarrow}$ による弱遷移が存在する．これは離散遷移について上述の事実があるからである．

ここで，確率リージョングラフ上では，時間制約が全て頂点と辺の有無により表現されているため，PTA間の**確率時間弱模倣関係**の計算は，単なるグラフ間の**確率弱模倣関係**の計算となる．

3 確率時間弱模倣関係の例

この節では，実際に確率時間弱模倣関係にある確率時間オートマトンのモデル例を示し，保存されているいくつかの動作についての説明を行う．また，構成された確率リージョングラフ間で時間模倣条件・確率模倣条件が満たされていることを確認する．

3.1 確率時間弱模倣関係のPTA間での検討

まず，図5に確率時間弱模倣関係にある二つのPTAの例を示す．

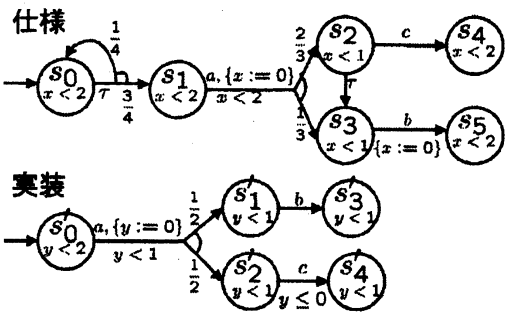

図5: 確率時間弱模倣関係にあるPTAの例

実装側では外部イベント a が確率1，時間単位1未満で実行される記述がある．これに対し，仕様側では時間遷移を行うことなく内部イベント τ を実行し（このとき s_0 に戻った場合，再び τ の実行が繰り返されるなら結局 s_1 に到達する確率は1に収束），s_1 から確率1，時間単位1未満で a を実行可能である．また，仕様側ではさらに時間単位1以上から2未満の間も a を実行できる．

次に，b や c の実行確率についても，仕様側の s_2 において，非決定な遷移 τ と c をそれぞれ確率 $\frac{1}{4},\frac{3}{4}$ で実行するとし，s_3 から b を実行する確率と合わせて考えることができる．このとき b と c の実行確率はそれぞれ $\frac{1}{3}+\frac{2}{3}\cdot\frac{1}{4}=\frac{1}{2},\frac{2}{3}\cdot\frac{3}{4}=\frac{1}{2}$ となる．これは実装側でのイベントの実行確率と一致する．

このように動作を見ていくと，実装側でのイベントの確率やタイミングは仕様側で模倣することができる，すなわち仕様が実装を確率時間弱模倣していることがわかる．

3.2 確率時間弱模倣関係の確率リージョングラフ間での検討

さらに，図5のPTAの確率リージョングラフを構成すると，次の2つの図がそれぞれ構成される．ここで，実装側の時間遷移 (*succ* 遷移)，離散遷移

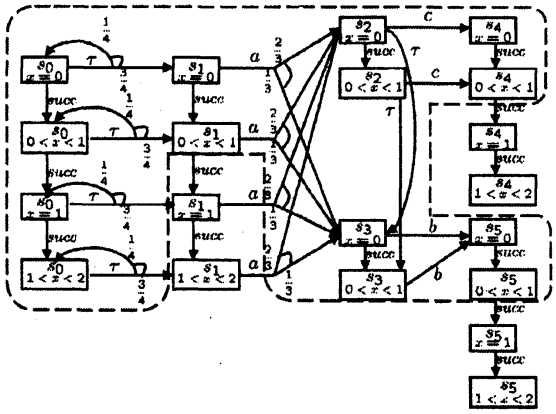

図 6: 仕様側の確率リージョングラフ

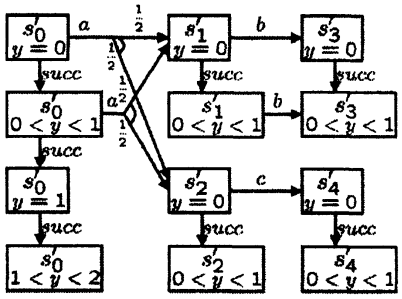

図 7: 実装側の確率リージョングラフ

は仕様側の破線部内の遷移により模倣されていることが分かる．このように，確率リージョングラフ上では，PTA上の不変条件や遷移可能条件から，ある頂点から起こりうる全遷移を構成する．また，時間模倣条件・確率模倣条件に関して共に満たされていることが，(条件式を見ることなく) 遷移のみにより確認でき，起こりうるクロック値のパターンも頂点により網羅している．単純にPTAを見るだけで，このようなクロック値のパターンの網羅を行うのは (クロック変数が複数の場合などで) 困難である．

4 結論・今後の課題

本研究の成果として，確率時間強模倣関係より検証において実用的な，確率時間弱模倣関係を定義することができた．また，その関係の確率リージョングラフ上での決定可能性を示せた．

一方で，今後の課題として，確率時間弱模倣関係の計算アルゴリズムを提案し，プログラムで実装することにより，検証器を開発することが挙げられる．また，開発した検証器により，詳細化における検証が正確に行われるかを，いくつかの例を対象として実験する必要が有る．

参考文献

[1] R.Alur; Timed Automata; LNCS 1633, pp. 8-22, Springer-Verlag,1999.

[2] Mariëlle Stoelinga; An Introduction to Probabilistic Automata; Bulletin of the EATCS 78: pp.176-198,2002.

[3] Ruggero Lanotte, Andrea Maggiolo-Schettini, Angelo Troina; Weak Bisimulation Probabilistic Timed Automata; SEFM'03, IEEE, pp. 34-43, 2003.

[4] Roberto Segala,Nancy A.Lynch: Probabilistic Simulations for Probabilistic Processes; Nordic Journal of Computing2(2): pp.250-273,1995.

[5] Christel Baier, Battina Engelen, Mila Majster-Cederbaum; Deciding Bisimilarity and Similarity for Probabilistic Processes; Journal of Computer and System Sciences, v.60 n.1, pp.187-231, Feb. 2000.

[6] M.Kwiatkowska, G.Norman, R.Segala, and J.Sproston; Automatic Verification of Real Time Systems with Discrete Probability Distributions; LNCS 1601, pp. 79-95, May 1999.

[7] Christel Baier, Holger Hemanns and Joost-Pieter Katoen; Probabilistic weak simulation is decidable in polynomial time; Information Processing Letters Volume 89,Issue 3 ,pp. 123 - 130,2004.

[8] S. Yamane; Probabilistic Timed Simulation Verification and its application to Stepwise Refinement of Real-Time Systems;LNCS 2896, pp.276-290, Springer-Verlag, 2003.

[9] 山根智, 中野善光; 時間弱模倣検証に基づくリアルタイムソフトウェアの詳細化設計手法, 電子情報学会論文誌 VOL.J88-D1 No.10,October 2005.

[10] 小寺広志、山根 智; "確率時間オートマトンの確率時間強模倣検証アルゴリズム", 数理解析研究所講究録 1426,pp.133-138, 京都大学数理解析研究所,2005.