離散確率分布を持つリアルタイムシステムの詳細化検証手法

山根 智†

近年，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．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も開発されている．本論文では，離散確率分布を持つ確率時間オートマトンの時間模倣関係の検証手法を開発して，リアルタイムシステムの段階的詳細化開発への適用を図る．

Formal Refinement Verification Method of Real-time Systems with Discrete Probability Distributions

Satoshi Yamane†

Generally, real-time systems have been specified using timed automata, and moreover model-checking methods of timed automata have been developed. On the other hand, recently, probabilistic timed automata have been developed in order to express the relative likelihood of the system exhibiting certain behavior. In this paper, we develope the verification method of simulation relation of probabilistic timed automata, and apply this method into stepwise refinement developments of real-time systems.

1. まえがき

近年，マイクロプロセッサの99%以上は組込み型システムに使われており，組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，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[2]が定着しており，その検証手法としてもモデル検査手法[3),4)]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[5]も開発されている．

本論文では，離散確率分布を持つ確率時間オートマトンの模倣関係の検証手法を開発して，リアルタイムシステムの段階的詳細化開発への適用を図る．従来の代表的な模倣関係による詳細化検証に関する研究としては，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[6]．
(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[7]．
(3) 1998年，Yamaneは時間オートマトンの ∀-時間模倣関係と ∃-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を示した[8]．

本論文では，新たに，離散確率分布を持つ確率時間オートマトンの時間模倣関係を定義して，そのアルゴリズムを開発して，リアルタイムシステムの段階的詳細化開発へ適用する．

以降の本論文の構成は以下のとおりである．2章では，諸定義を行う．3章では，確率時間オートマトンを定義する．4章では，確率時間オートマトンの時間模倣関係を定義する．5章では，確率時間オートマトンの時間模倣関係の検証手法を提案する．6章では，リアルタイムシステムの段階的詳細化開発への適用を図る．最後に，7章では，まとめと今後の課題を述べる．

2. 諸定義

本章では，本論文の以降で必要となる諸定義を行う．まず，確率分布を定義する．

Definition1（離散確率空間）

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

確率空間は $(\mathbf{\Omega}, \mathcal{F}, P)$ である．ここで，$\mathbf{\Omega}$ は集合，$\mathcal{F}$ は $\mathbf{\Omega}$ の部分集合の集まり，P は関数 $P : \mathcal{F} \to [0,1]$ である．ただし，$P[\mathbf{\Omega}] = 1$ であり，$\mathcal{F}$ の任意の集まり $\{C_i\}_i$ に対して $P[\cup_i C_i] = \sum_i P[C_i]$ である．なお，$\{C_i\}_i$ は互いに共通部分のない集合とする．P は確率測度と呼ばれて，$\mathcal{F}$ の各要素に測度を割り付ける関数である．

もし $\mathcal{F} = 2^{\mathbf{\Omega}}$ であり，各 $C \subseteq \mathbf{\Omega}$ に対して $P[C] = \sum_{x \in C} P[x]$ ならば，確率空間 $(\mathbf{\Omega}, \mathcal{F}, P)$ は離散である．有限集合 S に対して，離散確率空間 $(\mathbf{\Omega}, \mathcal{F}, P)$ の集合を $prob(S)$ と表記する．ここで，$\mathbf{\Omega}$ は S の部分集合である．s 上の Dirac 分布は唯一の要素 s を持つ確率空間であり，$D(s)$ と表記する．

2 つの離散確率空間 $(\mathbf{\Omega_1}, \mathcal{F}_1, P_1)$ と $(\mathbf{\Omega_2}, \mathcal{F}_2, P_2)$ との積は $(\mathbf{\Omega_1}, \mathcal{F}_1, P_1) \otimes (\mathbf{\Omega_2}, \mathcal{F}_2, P_2)$ と表記して，$(\mathbf{\Omega_1} \times \mathbf{\Omega_2}, 2^{\mathbf{\Omega_1} \times \mathbf{\Omega_2}}, P)$ である．ここで，任意の $(s_1, s_2) \in \mathbf{\Omega_1} \times \mathbf{\Omega_2}$ に対して，$P[(s_1, s_2)] = P_1[s_1] P_2[s_2]$ である． ■

次に，マルコフ決定プロセスを定義する．

Definition2（マルコフ決定プロセス）

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

マルコフ決定プロセスは $(Q, Steps)$ によって表記される．ただし，Q は状態の集合，$Steps : Q \to 2^{\mu(Q)}$ は各々の状態に確率分布の集合を割り付ける関数である．直感的には，状態 $q \in Q$ において，非決定的に確率分布 $p \in Steps(q)$ を選んで，状態 $q\prime \in Q$ に遷移する．この状態遷移は $q \xrightarrow{p} q\prime$ と表記される．

また，ある集合 Σ に対して，関数 $Steps$ は $Steps : Q \to 2^{\Sigma \times \mu(Q)}$ と拡張できる．この関数 $Steps$ は，各状態 $q \in Q$ に順序対 (σ, p) を割り付ける．すなわち，この状態遷移は $q \xrightarrow{\sigma, p} q\prime$ となる． ■

次に，パスを定義する．

Definition3（パス）

ラベル付きパスは非空な有限または無限なシーケンスであり，以下のとおりである．

$$\omega = q_0 \xrightarrow{l_0} q_1 \xrightarrow{l_1} q_2 \xrightarrow{l_2} \dots$$

ここで，q_i は状態であり，l_i はラベルである．

ω の最初の状態は $first(\omega)$ と表記して，ω の最後の状態は $last(\omega)$ と表記する．もし，$\omega = q_0 \xrightarrow{l_0} q_1 \xrightarrow{l_1} \dots \xrightarrow{l_{n-1}} q_n$ が有限のパス，かつ，$\omega\prime = q_0\prime \xrightarrow{l_0\prime} q_1\prime \xrightarrow{l_1\prime} \dots$ が有限または無限のパス，かつ，$last(\omega) = first(\omega\prime)$ ならば，ω と $\omega\prime$ の連接は以下である．

$$\omega\omega\prime = q_0 \xrightarrow{l_0} q_1 \xrightarrow{l_1} q_2 \dots \xrightarrow{l_{n-1}} q_n \xrightarrow{l_0\prime} q_1\prime \xrightarrow{l_1\prime} \dots$$

■

次に，クロックとクロック値を定義する．

Definition4（クロックとクロック値）

クロックは同じ速度で増加する，実数値を持つ変数である．$\chi = \{x_1, \dots, x_n\}$ をクロックの集合とする．$\nu : \chi \to \mathbf{R}$ は実数値をクロックの各々に割り当てる関数であり，クロック割当てと呼ばれる．χ のすべてのクロック割当ての集合を $\mathbf{R}^\chi$ と表記する．χ のすべてのクロックに 0 を割り付ける，クロック割当てを $\mathbf{0}$ とする．ある $X \subseteq \chi$ に対して，X の中のクロックに 0 を割り付けて，X 以外の χ の中のすべてのクロックは ν と一致するようなクロック割当てを $\nu[X := 0]$ と書く．さらに，任意の $t \in \mathbf{R}$ に対して，すべてのクロック $x \in \chi$ が $\nu(x) + t$ であることを $\nu + t$ と表記する． ■

次に，クロック制約を定義する．

Definition5（クロック制約）

χ のクロック制約は $x_i \sim c$ または $x_i - x_j \sim c$ で表現する．ここで，$1 \le i \ne j \le n$，$\sim \in \{<, \le, \ge, >\}$，$c \in \mathbf{N} \cup \{\infty\}$ である．また，x_0 は 0 とする． ■

次に，ゾーンを定義する．

Definition6（ゾーン）

χ のゾーンは ζ と書き，クロック制約の論理積によって表現される，$\mathbf{R}^\chi$ の凸状の部分集合である．形式的には，ゾーン ζ は以下を満たす，割当ての集合である．

$$\bigwedge_{0 \le i \ne j \le n} x_i - x_j \sim c_{ij}$$

χ のすべてのゾーンの集合は $\mathbf{Z}_\chi$ とする．ゾーン ζ の表現の中で使われる，最大の定数を $c_{max}(\zeta)$ と表記する．任意のゾーン $\zeta \in \mathbf{Z}_\chi$，$X \subseteq \chi$ と $\nu \in \mathbf{R}^\chi$ に対して，$\zeta[X := 0] = \{\nu[X := 0] | \nu \in \zeta\}$ である．ただし，$\nu \in \zeta$ はゾーン ζ の要素である，割当て ν を意味する．また，$\nu[X := 0]$ は，ある $X \subseteq \chi$ に対して X の中のクロックに 0 を割り当て，$\chi \setminus X$ の中のすべてのクロックの割当ては ν と一致することを意味する． ■

3. 確率時間オートマトンの定義

本章では，確率時間オートマトン[5] を導入する．確率時間オートマトンは確率を持つリアルタイムシステムの仕様記述言語である．

3.1 確率時間オートマトンの構文と意味

まず，確率時間オートマトンの構文を定義する．確

率時間オートマトンは枝上の離散確率分布で時間オートマトンを拡張したものである．次のノードの選択は確率および非決定性である．

Definition7（確率時間オートマトンの構文）
確率時間オートマトンは $\mathbf{G} = (S, \Sigma, \overline{s}, \chi, inv, prob, < \tau_s >_{s \in S})$ の 7 つ組で定義される．ここで，

(1) ノードの有限集合 S.
(2) イベントの有限集合 Σ.
(3) 初期ノード $\overline{s} \in S$.
(4) クロックの有限集合 χ.
(5) 各ノードに不変性条件を割り付ける関数 $inv : S \to \mathbf{Z}_\chi$.
(6) 各ノードに $\Sigma \times S \times 2^\chi$ 上の離散確率分布の集合を割り付ける関数 $prob : S \to 2^{\mu(\Sigma \times S \times 2^\chi)}$. ただし，$2^\chi$ はリセットされるクロックの集合の集合である．なお，$prob(S)$ は離散確率空間 $(\mathbf{\Omega}, \mathcal{F}, P)$ の集合を表しており，$\mathbf{\Omega} \subseteq S$ である．
(7) 関数の族 $< \tau_s >_{s \in S}$．ここで，任意の $s \in S$ に対して，関数 $\tau_s : prob(s) \to \mathbf{Z}_\chi$ は任意の $p \in prob(s)$ に遷移可能な条件を割り付ける．ただし，$p \in \mu(\Sigma \times S \times 2^\chi)$ である．

■

次に，確率時間オートマトンの意味を非形式的に定義する．確率時間オートマトン $\mathbf{G} = (S, \Sigma, \overline{s}, \chi, inv, prob, < \tau_s >_{s \in S})$ の状態は順序対 $< s, \nu >$ として定義される．ここで，$s \in S$ はノードであり，$\nu \in \mathbf{R}^\chi$ はクロック割当てである．なお，$\nu \in inv(s)$ である．また，$< s, \nu >$ の集合を Ω と表す．

確率時間オートマトンの任意の状態において，可能な遷移は以下である：

(1) 現在のクロック割当て $\nu \in \mathbf{R}^\chi$ に $\delta \in \mathbf{R}^\chi$ を追加したクロック割当てが現在のノード s の不変性条件 $inv(s)$ を満たすときに限り，時間経過 $\delta \in \mathbf{R}^\chi$ は可能である．より形式的には，もし，$< s, \nu >$ が現在の状態で，$\nu + \delta \in inv(s)$ ならば，状態 $< s, \nu + \delta >$ への $\delta \in \mathbf{R}^\chi$ の時間経過の遷移は可能である．
(2) もし，確率分布 p が現在のノードの確率分布の集合に属して，現在のクロック割当てが $\tau_s(p)$ を満たすときに限り，確率分布 p に対応する確率遷移は可能である．より形式的には，もし，$< s, \nu >$ が現在の状態で，$p \in prob(s)$ であり，$\tau_s(p)$ が ν で満たされるならば，確率分布 p に対応する確率遷移は可能である．

Example1（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 $s1$ からイベント a で状態 $s1$ へは確率 0.3 で遷移して，状態 $s2$ へは確率 0.7 で遷移する．また，状態 $s2$ から状態 $s1$ へは $x = 1$ か $y = 1$ の条件に従って非決定的に遷移する．ここで，図 1 の確率時間オートマトン $\mathbf{G} = (S, \Sigma, \overline{s}, \chi, inv, prob, < \tau_s >_{s \in S})$ の各組を定義する：

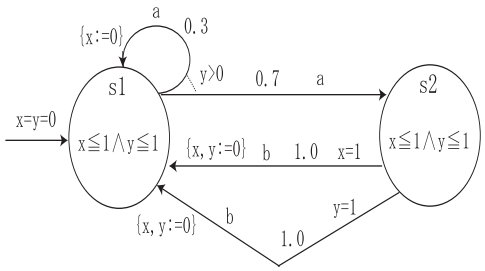


図 1 確率時間オートマトンの例
Fig. 1 Example of probabilistic timed automaton.

(1) $S = \{s1, s2\}$.
(2) $\Sigma = \{a, b\}$.
(3) $\overline{s} = s1$.
(4) $\chi = \{x, y\}$.
(5) $inv(s1) = x \leq 1 \wedge y \leq 1$. $inv(s2) = x \leq 1 \wedge y \leq 1$.
(6) $prob(s1) = \{{p_{s1}}^1\}$，ここで ${p_{s1}}^1(s1) = 0.3$, ${p_{s1}}^1(s2) = 0.7$.
$prob(s2) = \{{p_{s2}}^1, {p_{s2}}^2\}$，ここで ${p_{s2}}^1(s1) = 1.0$, ${p_{s2}}^2(s1) = 1.0$.
(7) $\tau_{s1}({p_{s1}}^1) = y > 0$. $\tau_{s2}({p_{s2}}^1) = x = 1$. $\tau_{s2}({p_{s2}}^2) = y = 1$.

■

3.2 確率時間オートマトンの並列合成

次に，確率時間オートマトンの並列合成を定義する．

Definition8（確率時間オートマトンの並列合成）
2 つの確率時間オートマトン $\mathbf{G_1} = (S_1, \Sigma_1, \overline{s}_1, \chi_1, inv_1, prob_1, < \tau_{s_1} >_{s_1 \in S_1})$ と $\mathbf{G_2} = (S_2, \Sigma_2, \overline{s}_2, \chi_2, inv_2, prob_2, < \tau_{s_2} >_{s_2 \in S_2})$ が与えられたとする．$\mathbf{G_1}$ と $\mathbf{G_2}$ の並列合成 $\mathbf{G_1} \parallel \mathbf{G_2}$ は，$\mathbf{G} = (S, \Sigma, \overline{s}, \chi, inv, prob, < \tau_s >_{s \in S})$ である．

(1) $S = S_1 \times S_2$.
(2) $\Sigma = \Sigma_1 \cup \Sigma_2$.
(3) $\overline{s} = \overline{s}_1 \times \overline{s}_2$.
(4) $\chi = \chi_1 \cup \chi_2$.
(5) $inv((s_1, s_2)) = inv_1(s_1) \wedge inv_2(s_2)$.
(6) $prob : S \to 2^{\mu(\Sigma \times S \times 2^\chi)}$ は以下のとおりである．
(a) $a \in \Sigma_1$ かつ $a \in \Sigma_2$ のとき
$a \in \Sigma_1$ のとき $p_1 \in prob_1(s_1)$ として，

$a \in \Sigma_2$ のとき $p_2 \in prob_2(s_2)$ とする．$p = p_1 \otimes p_2$ である $p \in prob(s)$ が存在する．ただし，$s_1 \in S_1$，$s_2 \in S_2$，$s \in S$ である．

(b) $a \in \Sigma_1$ かつ $b \in \Sigma_2 (a \neq b)$ のとき
$a \in \Sigma_1$ のとき $p_1 \in prob_1(s_1)$ として，$b \in \Sigma_2$ のとき $p_2 \in prob_2(s_2)$ とする．$p \in prob(s)$ なる $p = p_1$ および $p \in prob(s)$ なる $p = p_2$ が存在する．ただし，$s_1 \in S_1$，$s_2 \in S_2$，$s \in S$ である．

(7) 関数の族 $< \tau_s >_{s \in S}$．ここで，任意の $s \in S$ に対して，関数 $\tau_s : prob(s) \rightarrow \mathbf{Z}_\chi$ は任意の $p \in prob(s)$ に遷移可能な条件を割り付ける．ただし，$\sigma \in \Sigma$ である．

■

4. 確率時間オートマトンの時間模倣関係

本章では，2つの確率時間オートマトンの間に時間模倣関係を定義する．

Definition9（確率時間オートマトンの時間模倣関係）

2つの確率時間オートマトン $\mathbf{G_1} = (S_1, \Sigma_1, \overline{s}_1, \chi_1, inv_1, prob_1, < \tau_{s_1} >_{s_1 \in S_1})$ と $\mathbf{G_2} = (S_2, \Sigma_2, \overline{s}_2, \chi_2, inv_2, prob_2, < \tau_{s_2} >_{s_2 \in S_2})$ が与えられたとする．以下の2つの条件を満たす $R \subseteq \Omega_1 \times \Omega_2$ を，$\mathbf{G_1}$ から $\mathbf{G_2}$ への時間模倣関係と呼び，そのような関係 R が存在するとき，$\mathbf{G_1} \preceq \mathbf{G_2}$ と記述する．なお，Ω_1 は状態 $< s_1, \nu_1 >$ の集合であり，Ω_2 は状態 $< s_2, \nu_2 >$ の集合である．ただし，$s_1 \in S_1$，$\nu_1 : \chi_1 \rightarrow \mathbf{R}$，$s_2 \in S_2$，$\nu_2 : \chi_2 \rightarrow \mathbf{R}$，$\Sigma_1 = \Sigma_2$ である．

(1) 時間模倣条件
$(< s_1, \nu_1 >, < s_2, \nu_2 >) \in R$ ならば，任意の $\sigma \in \Sigma_1$ について，τ が遷移可能な条件であり，

$$< s_1, \nu_1 > \xrightarrow{\sigma, p, \tau} < s_1\prime, \nu_1\prime >$$

である $< s_1\prime, \nu_1\prime >$ が存在するならば，

$$< s_2, \nu_2 > \xrightarrow{\sigma, p, \tau} < s_2\prime, \nu_2\prime >$$

である $< s_2\prime, \nu_2\prime >$ が存在して，$(< s_1\prime, \nu_1\prime >, < s_2\prime, \nu_2\prime >) \in R$ である．なお，$s_1, s_1\prime \in S_1$，$s_2, s_2\prime \in S_2$ である．ただし，$\tau \subseteq \tau_{s_1}(p)$ かつ $\tau \subseteq \tau_{s_2}(p)$ である．

(2) 初期条件
$< \overline{s}_1, \mathbf{0} >$ に対して，$(< \overline{s}_1, \mathbf{0} >, < \overline{s}_2, \mathbf{0} >) \in R$ を満たす $< \overline{s}_2, \mathbf{0} >$ が存在する．

■

5. 確率時間オートマトンの時間模倣関係の検証手法

本章では，確率時間オートマトンの時間模倣関係の検証手法を提案する．

5.1 クロック値の同値関係

まず，クロック値の同値関係を定義する[5]．

Definition10（クロック値の整数部分の一致）

任意の $t \in \mathbf{R}$ に対して，$\lfloor t \rfloor$ は t の整数部分を表記する．任意の $t, t\prime \in \mathbf{R}$ に対して，以下のときに限り，t と $t\prime$ の整数部分が一致する．

(1) $\lfloor t \rfloor = \lfloor t\prime \rfloor$
かつ
(2) t と $t\prime$ の両方が整数か，整数でない．

■

Definition11（クロックの等価性）

割当て $\nu, \nu\prime \in \mathbf{R}^\chi$ が以下の条件を満たすときに限り，ν と $\nu\prime$ は等しい．これを $\nu \cong \nu\prime$ と表記する．

(1) $\forall x \in \chi$ に対して，$\nu(x)$ と $\nu\prime(x)$ の整数部分が一致するか，または，$\nu(x) > c$ かつ $\nu\prime(x) > c$ である．
かつ
(2) $\forall x, x\prime \in \chi$ に対して，$\nu(x) - \nu(x\prime)$ と $\nu\prime(x) - \nu\prime(x\prime)$ の整数部分が一致するか，または，$\nu(x) - \nu(x\prime) > c$ かつ $\nu\prime(x) - \nu\prime(x\prime) > c$ である．

■

ν が属する $\cong$ の同値クラスを $[\nu]$ と表記する．リージョンは $< s, [\nu] >$ と表記される．

ここで，以下のように，クロック値の同値関係 $\cong$ をリージョンの同値関係 $\cong$ に拡張する：

$< s, \nu > \cong < t, \nu\prime >$ iff $s = t$ かつ $\nu \cong \nu\prime$.

5.2 リージョングラフ

次に，リージョングラフを定義する[5]．

Definition12（リージョンの分類）

α と β は $\mathbf{R}^\chi$ の別の同値クラスとする．同値クラスは以下の3つに分類できる．

(1) **successor クラス**
各 $\nu \in \alpha$ に対して，ある $t \in \mathbf{R}$ が存在して，すべての $t\prime \leq t$ に対して，$\nu + t \in \beta$ かつ $\nu + t\prime \in \alpha \cup \beta$ であるときに限り，同値クラス β は α の successor であると呼ばれる．

(2) **x-zero クラス**
クロック $x \in \chi$ に対して，各 $\nu \in \alpha$ に対して $\nu(x) = 0$ のときに限り，同値クラス α は x-zero と呼ばれる．

(3) **x-unbounded クラス**

クロック $x \in \chi$ に対して，各 $\nu \in \alpha$ に対して $\nu(x) > c_{max}(\mathbf{G})$ のときに限り，同値クラス α は x-unbounded と呼ばれる．ただし，$C_{max}(G)$ はオートマトン $\mathbf{G}$ の中のゾーンを構成する定数 c_{ij} の中で最大の定数である．

■

次に，確率の遷移と時間経過の遷移から構成されるリージョングラフを定義する．リージョングラフはマルコフ決定プロセスである．

Definition13（リージョングラフ）

確率時間オートマトン $\mathbf{G} = (S, \Sigma, \overline{s}, \chi, inv, prob, < \tau_s >_{s \in S})$ に対して，リージョングラフ $\mathbf{R(G)}$ はマルコフ決定プロセス $(V^*, Steps^*)$ として定義される．ここで，V^* はリージョンの集合であり，$Steps^* : V^* \to 2^{\mu(\Sigma\prime \times V^*)}$ である．$Steps^* : V^* \to 2^{\mu(\Sigma\prime \times V^*)}$ は 2 つのタイプの遷移を含む．ただし，$\Sigma\prime = \Sigma \cup \{succ\}$ である．各リージョン $< s, \alpha > \in V^*$ に対して遷移は以下である：

(1) **時間経過の遷移**

もし不変性条件 $inv(s)$ が $succ(\alpha)$ により満たされるならば，$p^{s,\alpha}_{succ} \in Steps^*(< s, \alpha >)$ である．なお，$succ(\alpha)$ は α の successor である．ここで，任意の $< s\prime, \beta > \in V^*$ に対して，以下である：

$$p^{s,\alpha}_{succ} = \begin{cases} 1 & if \quad < s\prime, \beta > = < s, succ(\alpha) > \\ 0 & otherwise. \end{cases}$$

なお，$< s\prime, \beta > = < s, succ(\alpha) >$ のとき，$< s, \alpha > \xrightarrow{succ} < s\prime, \beta >$ と表記する．

(2) **離散の確率の遷移**

もし $p \in prob(s)$ が存在して α が遷移可能条件 $\tau_s(p)$ を満たすならば，$p^{s,\alpha} \in Steps^*(< s, \alpha >)$ である．ここで，任意の $s\prime \in S$ と同値クラス β に対して以下である：

$$p^{s,\alpha} = \sum_{X \subseteq \chi \quad and \quad \alpha[X:=0]=\beta} p(s\prime, X).$$

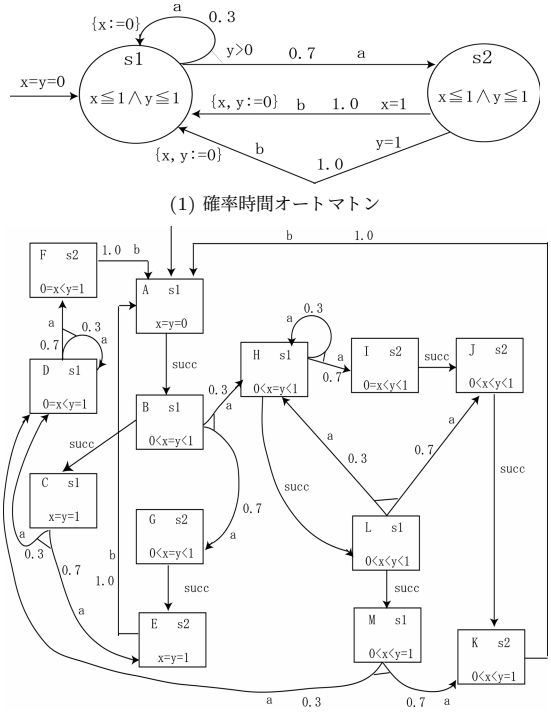
ここで，$p(s\prime, X)$ は，任意の $s\prime \in S$ と $X \subseteq \chi$ に対して，ノード $s\prime$ に遷移して X をリセットする確率を表記する．

なお，$< s, \alpha > \xrightarrow{\sigma, p^{s,\alpha}} < s\prime, \beta >$ と表記する．ただし，$\sigma \in \Sigma$ である．

■

Definition14（リージョングラフのパス）

リージョン $< s, \alpha >$ が与えられたとき，$< s, \alpha >$-パスは以下の形式の有限または無限のパスである．



(1) 確率時間オートマトン

(2) 確率時間オートマトンのリージョングラフ

図 2 リージョングラフの事例
Fig. 2 Example of region graph.

$$\omega^* = < s_0, \alpha_0 > \xrightarrow{\sigma_0, p^{s_0,\alpha_0}} < s_1, \alpha_1 > \xrightarrow{\sigma_1, p^{s_1,\alpha_1}} < s_2, \alpha_2 > \xrightarrow{\sigma_2, p^{s_2,\alpha_2}} \ldots$$

ここで，$< s_0, \alpha_0 > = < s, \alpha >$，$s_i \in S$，$\alpha_i$ は $\mathbf{R}^\chi$ 上の $\cong$ の同値クラスであり，$\sigma_i \in \Sigma\prime$ であり，$p^{s_i,\alpha_i} \in Steps^*(< s_i, \alpha_i >)$ である．

■

Example2（リージョングラフの事例）

図 2 では，リージョングラフの例を示す．図 2 (1) の確率時間オートマトン $\mathbf{G}$ に対して，図 2 (2) のリージョングラフ $\mathbf{R(G)}$ はマルコフ決定プロセス $(V^*, Steps^*)$ として定義される．

(1) $V^* = \{< s1, [x = y = 0] >, < s1, [0 < x = y < 1] >, < s1, [x = y = 1] >, < s2, [0 = x < y = 1] >, < s2, [x = y = 1] >, < s2, [0 = x < y = 1] >, < s2, [0 < x = y < 1] >, < s1, [0 < x = y < 1] >, < s2, [0 < x < y < 1] >, < s2, [0 < x < y = 1] >, < s1, [0 < x < y < 1] >, < s1, [0 < x < y = 1] >\}$.

(2)
- $Steps^*(< s1, [x = y = 0] >) = \{p^{s1,[x=y=0]}_{succ}\}$，ここで $p^{s1,[x=y=0]}_{succ} = 1.0$ である．
- $Steps^*(< s1, [0 < x = y < 1] >) =$

$\{p^{s1,[0<x=y<1]}, p_{succ}^{s1,[0<x=y<1]}\}$，ここで $p^{s1,[0<x=y<1]} = p(s1,x) + p(s2,\{\})$ と $p_{succ}^{s1,[0<x=y<1]} = 1.0$ である．なお，$p(s1,\{x\}) = 0.3$ と $p(s2,\{\}) = 0.7$ である．

. . . . . .

. . . . . .

. . . . . .

- $Steps^*(< s1,[0 < x < y = 1] >) = \{p^{s1,[0<x<y=1]}\}$，ここで $p^{s1,[0<x<y=1]} = p(s1,\{x\}) + p(s2,\{\})$ である．なお，$p(s1,\{x\}) = 0.3$ と $p(s2,\{\}) = 0.7$ である．

■

5.3 リージョン模倣関係

まず，リージョングラフ上のリージョン模倣関係を定義して，次に，確率時間オートマトン上の時間模倣関係の存在性問題はリージョングラフ上のリージョン模倣関係の存在性問題に帰着できることを示す．

まず，2つの確率時間オートマトン $\mathbf{G_1} = (S_1, \Sigma, \overline{s}_1, \chi_1, inv_1, prob_1, < \tau_{s_1} >_{s_1 \in S_1})$ と $\mathbf{G_2} = (S_2, \Sigma, \overline{s}_2, \chi_2, inv_2, prob_2, < \tau_{s_2} >_{s_2 \in S_2})$ が与えられたとする．$\mathbf{G_1}$ と $\mathbf{G_2}$ の並列合成 $\mathbf{G_1} \parallel \mathbf{G_2}$ は，$\mathbf{G} = (S, \Sigma, \overline{s}, \chi, inv, prob, < \tau_s >_{s \in S})$ である．

このとき，リージョングラフ $\mathbf{R}(\mathbf{G_1} \parallel \mathbf{G_2})$ を定義する．なお，以下の定義は **Definition 13** の $\mathbf{G}$ を $\mathbf{G_1} \parallel \mathbf{G_2}$ で置き換えたものである．

Definition15（リージョングラフ $\mathbf{R}(\mathbf{G_1} \parallel \mathbf{G_2})$）
確率時間オートマトン $\mathbf{G_1} \parallel \mathbf{G_2}$ に対して，リージョングラフ $\mathbf{R}(\mathbf{G_1} \parallel \mathbf{G_2})$ はマルコフ決定プロセス $(V^*, Steps^*)$ として定義される．ここで，V^* はリージョンの集合であり，$Steps^* : V^* \to 2^{\mu(\Sigma \times V^*)}$ である．$Steps^* : V^* \to 2^{\mu(\Sigma \times V^*)}$ は2つのタイプの遷移を含む．各リージョン $< (s_1, s_2), \alpha > \in V^*$ に対して以下である：

(1) **時間経過の遷移**
もし不変性条件 $inv((s_1, s_2))$ が $succ(\alpha)$ により満たされるならば，$p_{succ}^{(s_1,s_2),\alpha} \in Steps^*(< (s_1, s_2), \alpha >)$ である．ただし，α は $\mathbf{R}^{\chi}$ の同値クラスであり，$\chi = \chi_1 \cup \chi_2$ とする．ここで，任意の $< (s_1\prime, s_2\prime), \beta > \in V^*$ に対して，以下である：

$$p_{succ}^{(s_1,s_2),\alpha} = \begin{cases} 1 & if \quad < (s_1\prime, s_2\prime), \beta > \\ & \quad =< (s_1, s_2), succ(\alpha) > \\ 0 & otherwise. \end{cases}$$

なお，$< (s_1\prime, s_2\prime), \beta > =< (s_1, s_2), succ(\alpha) >$ のとき，
$< (s_1, s_2), \alpha > \xrightarrow{succ} < (s_1\prime, s_2\prime), \beta >$ と表記する．

(2) **離散の確率の遷移**
もし $p \in prob((s_1, s_2))$ が存在して α が遷移可能条件 $\tau_s(p)$ を満たすならば，$p^{(s_1,s_2),\alpha} \in Steps^*(< (s_1, s_2), \alpha >)$ である．ここで，任意の $(s_1\prime, s_2\prime) \in S$ と同値クラス β に対して以下である：

$$p^{(s_1,s_2),\alpha} = \sum_{X \subseteq \chi \quad and \quad \alpha[X:=0]=\beta} p((s_1\prime, s_2\prime), X).$$

ここで，$p((s_1\prime, s_2\prime), X)$ は，任意の $(s_1\prime, s_2\prime) \in S$ と $X \subseteq \chi$ に対して，ノード $(s_1\prime, s_2\prime)$ に遷移して X をリセットする確率を表記する．
なお，$< (s_1, s_2), \alpha > \xrightarrow{\sigma, p^{(s_1,s_2),\alpha}} < (s_1\prime, s_2\prime), \beta >$ と表記する．ただし，$\sigma \in \Sigma$ である．

■

また，$\mathbf{R}(< \mathbf{s_1}, \nu_1 >, < \mathbf{s_2}, \nu_2 >)$ と $\mathbf{R_{G_1 \| G_2}}$ を定義する．

Definition16（$\mathbf{R}(< \mathbf{s_1}, \nu_1 >, < \mathbf{s_2}, \nu_2 >)$ と $\mathbf{R_{G_1 \| G_2}}$）
$\mathbf{R}(< \mathbf{s_1}, \nu_1 >, < \mathbf{s_2}, \nu_2 >)$ と $\mathbf{R_{G_1 \| G_2}}$ は以下のように定義される：

(1) $\mathbf{R}(< \mathbf{s_1}, \nu_1 >, < \mathbf{s_2}, \nu_2 >)$ は $< (s_1, s_2), [\nu] >$ または $\{< s_1, [\nu] >, < s_2, [\nu] >\}$ であり，状態の対 $(< (s_1, s_2), [\nu] >) \in \Omega_{\mathbf{G_1 \| G_2}}$ の同値クラスを表す．

(2) $\mathbf{R_{G_1 \| G_2}}$ は $\mathbf{G_1} \parallel \mathbf{G_2}$ 上のリージョンの同値クラスの集合である．

■

Definition17（リージョン模倣関係の定義）
$\eta \subseteq \mathbf{R}(\mathbf{G_1} \parallel \mathbf{G_2})$ が $\mathbf{G_1}$ から $\mathbf{G_2}$ へのリージョン模倣関係である必要十分条件は，任意の $\mathbf{R}(< \mathbf{s_1}, \nu_1 >, < \mathbf{s_2}, \nu_2 >) \in \eta$ に対して，以下の条件が満たされることである．
任意の σ に対して，もし

$$< s_1, \nu_1 > \xrightarrow{\sigma, p, \tau_{(s_1,s_2)}(p)} < s_1\prime, \nu_1\prime >$$

ならば，以下の2つが成り立つ．

(1) $\mathbf{R}(< \mathbf{s_1}\prime, \nu_1\prime >, < \mathbf{s_2}\prime, \nu_2\prime >) \in \eta$ であるような，ある $< s_2\prime, \nu_2\prime >$ に対して，$< s_2, \nu_2 > \xrightarrow{\sigma, p, \tau_{(s_1,s_2)}(p)} < s_2\prime, \nu_2\prime >$ が存在する．

(2) もし $\mathbf{G_1}$ が $< s_1, \nu_1 >$ において p と $\tau_{(s_1,s_2)}(p)$ を持つならば，$\mathbf{G_2}$ が $< s_2, \nu_2 >$

において p と $\tau_{(s_1,s_2)}(p)$ を持つ．

■

Theorem1（時間模倣関係とリージョン模倣関係） $\mathbf{R}(< \mathbf{s_1}, \nu_1 >, < \mathbf{s_2}, \nu_2 >) \in \eta$ に対して，$\mathbf{R}_\eta = \{(< s_1, \nu_1 >, < s_2, \nu_2 >) | R(< s_1, \nu_1 >, < s_2, \nu_2 >) \in \eta\}$ とする．η が $\mathbf{G_1}$ から $\mathbf{G_2}$ へのリージョン模倣関係である必要十分条件は，$\mathbf{R}_\eta$ が $\mathbf{G_1}$ から $\mathbf{G_2}$ への時間模倣関係 $\mathbf{G_1} \preceq \mathbf{G_2}$ である．

Proof1 次の 2 つに場合分けして証明する：

(1) $\mathbf{R}_\eta$ が時間模倣関係ならば η がリージョン模倣関係の証明：
$\mathbf{R}(< \mathbf{s_1}, \nu_1 >, < \mathbf{s_2}, \nu_2 >) \in \eta$，かつ，$< s_1, \nu_1 > \xrightarrow{\sigma, p, \tau_{(s_1,s_2)}(p)} < s_1\prime, \nu_1\prime >$ となるような $p \in prob((s_1, s_2))$ と $\tau_{(s_1,s_2)}(p)$ とする．$\mathbf{R}_\eta$ が時間模倣関係なので，$< s_2, \nu_2 > \xrightarrow{\sigma, p, \tau_{(s_1,s_2)}(p)} < s_2\prime, \nu_2\prime >$ である $< s_2\prime, \nu_2\prime >$ が存在する．この $< s_2\prime, \nu_2\prime >$ はリージョン模倣関係の条件を満たす．
ゆえに，η はリージョン模倣関係である．

(2) η がリージョン模倣関係ならば $\mathbf{R}_\eta$ が時間模倣関係の証明：
$(< s_1, \nu_1 >, < s_2, \nu_2 >) \in \mathbf{R}_\eta$ とする．そして，任意の σ について，$\tau_{(s_1,s_2)}(p)$ が遷移可能な条件であり，$< s_1, \nu_1 > \xrightarrow{\sigma, p, \tau_{(s_1,s_2)}(p)} < s_1\prime, \nu_1\prime >$ とする．この証明では，$(< s_1\prime, \nu_1\prime >, < s_2\prime, \nu_2\prime >) \in \mathbf{R}_\eta$ を示せばよい．
$(< s_1\prime, \nu_2\prime >, < s_2\prime, \nu_2\prime >) \in \mathbf{R}_\eta$ であるような $< s_2\prime, \nu_2\prime >$ に対して，$< s_1\prime, \nu_1\prime > \xrightarrow{\sigma, p, \tau} < s_2\prime, \nu_2\prime >$ とする．なお，あるタイミング制約を τ とする．ここで，τ を $\tau_{(s_1,s_2)}(p)$ とすれば，$< s_1\prime, \nu_1\prime > \xrightarrow{\sigma, p, \tau_{(s_1,s_2)}(p)} < s_2\prime, \nu_2\prime >$ となり，$(< s_1\prime, \nu_1\prime >, < s_2\prime, \nu_2\prime >) \in \mathbf{R}_\eta$ が示せる．
ゆえに，$\mathbf{R}_\eta$ は時間模倣関係である．

■

Example3（リージョン模倣関係の事例） **図 3** に確率時間オートマトンとその並列合成の例を示す．**図 4**，**5**，**6**，**7**，**8** にそのリージョン模倣関係の例を示す．
以下に，$\mathbf{G_1}$ から $\mathbf{G_2}$ へのリージョン模倣関係 η が存在することを示す．任意の $\mathbf{R}(< \mathbf{s_1}\prime, \nu_1 >, < \mathbf{s_1}\prime\prime, \nu_2 >) \in \eta$ に対して，以下が成り立つことを示す．

(1) $\mathbf{R}(< \mathbf{s_1}\prime, \mathbf{x = 0} >, < \mathbf{s_1}\prime\prime, \mathbf{y = 0} >) \in \eta$ に対して，$< s_1\prime, x = 0 > \xrightarrow{succ, 1.0, x \leq 1 \wedge y \leq 1} < s_1\prime, 0 < x < 1 >$ である．このとき，以下が成り立つ．

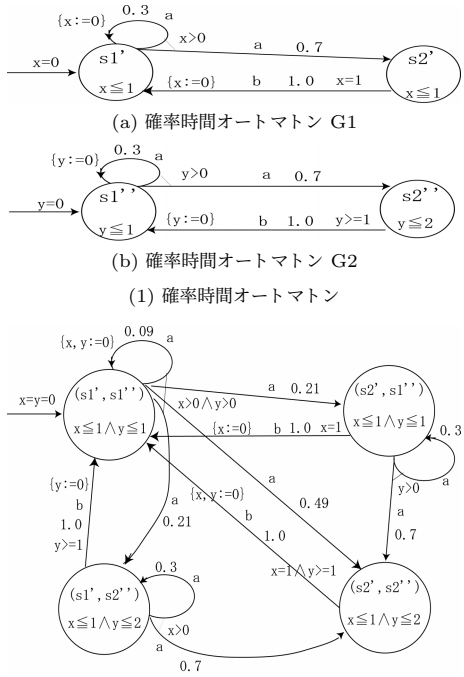


図 3 確率時間オートマトンとその並列合成の例
Fig. 3 Example of probabilistic timed automaton and its parallel composition.

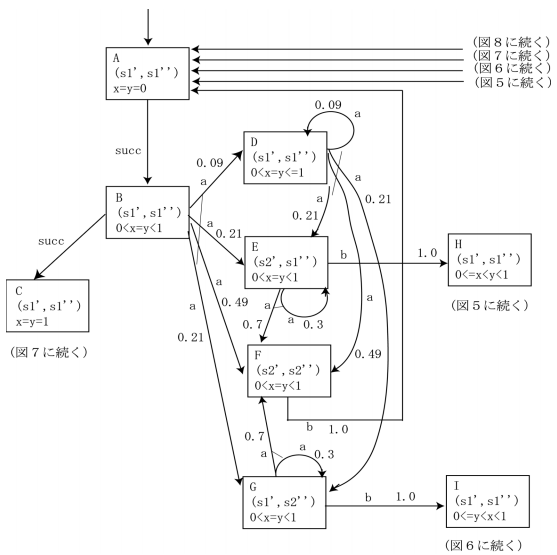


図 4 確率時間オートマトン G1‖G2 のリージョングラフ（その 1）
Fig. 4 Example of region graph of probabilistic timed automaton G1‖G2 (part1).

(a) $\mathbf{R}(< \mathbf{s_1}\prime, \mathbf{0 < x < 1} >, < \mathbf{s_1}\prime\prime, \mathbf{0 < y < 1} >) \in \eta$ であるような，ある $< s_1\prime\prime, 0 < y < 1 >$ に対して，$< s_1\prime\prime, y = 0 > \xrightarrow{succ, 1.0, x \leq 1 \wedge y \leq 1} < s_1\prime\prime, 0 < y < 1 >$ が存在する．

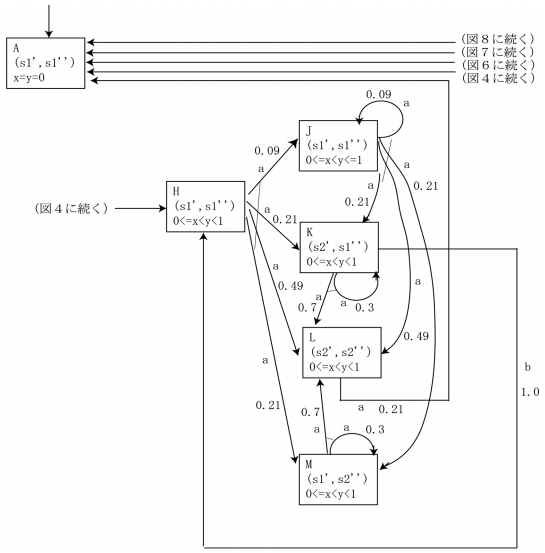


図 5 確率時間オートマトン G1‖G2 のリージョングラフ（その 2）
Fig. 5 Example of region graph of probabilistic timed automaton G1‖G2 (part2).

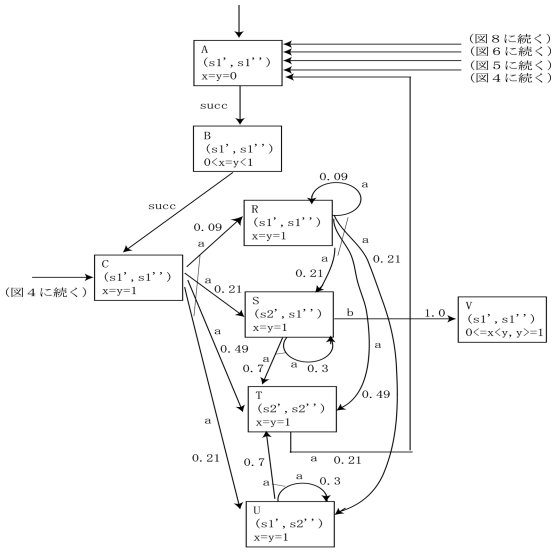


図 7 確率時間オートマトン G1‖G2 のリージョングラフ（その 4）
Fig. 7 Example of region graph of probabilistic timed automaton G1‖G2 (part4).

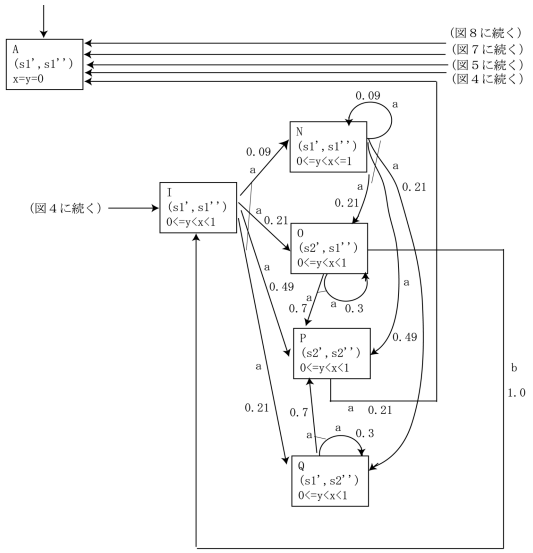


図 6 確率時間オートマトン G1‖G2 のリージョングラフ（その 3）
Fig. 6 Example of region graph of probabilistic timed automaton G1‖G2 (part3).

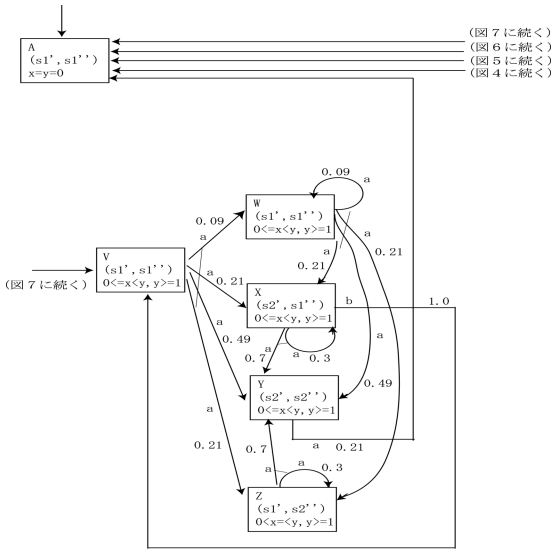


図 8 確率時間オートマトン G1‖G2 のリージョングラフ（その 5）
Fig. 8 Example of region graph of probabilistic timed automaton G1‖G2 (part5).

(b) もし $\mathbf{G_1}$ が $< s_1\prime, x = 0 >$ において確率 1.0 と $x \leq 1 \wedge y \leq 1$ を持つならば，$\mathbf{G_2}$ が $< s_1\prime\prime, y = 0 >$ において確率 1.0 と $x \leq 1 \wedge y \leq 1$ を持つ．

(2) $\mathbf{R}(<\mathbf{s_1\prime}, \mathbf{0} < \mathbf{x} < \mathbf{1}>, <\mathbf{s_1\prime\prime}, \mathbf{0} < \mathbf{y} < \mathbf{1}>) \in \eta$ に対して，$< s_1\prime, 0 < x < 1 > \xrightarrow{succ, 1.0, x \leq 1 \wedge y \leq 1} < s_1\prime, x = 1 >$ である．このとき，以下が成り立つ．

(a) $\mathbf{R}(< \mathbf{s_1\prime}, \mathbf{x = 1} >, < \mathbf{s_1\prime\prime}, \mathbf{y = 1} >) \in \eta$ であるような，ある $< s_1\prime\prime, y = 1 >$ に対して，$< s_1\prime\prime, 0 < y < 1 > \xrightarrow{succ, 1.0, x \leq 1 \wedge y \leq 1} < s_1\prime\prime, y = 1 >$ が存在する．

(b) もし $\mathbf{G_1}$ が $< s_1\prime, 0 < x < 1 >$ において確率 1.0 と $x \leq 1 \wedge y \leq 1$ を持つならば，$\mathbf{G_2}$ が $< s_1\prime\prime, 0 < y < 1 >$ において確率 1.0 と $x \leq 1 \wedge y \leq 1$ を持つ．

(3) $\mathbf{R}(<\mathbf{s_1\prime}, \mathbf{0} < \mathbf{x} < \mathbf{1}>, <\mathbf{s_1\prime\prime}, \mathbf{0} < \mathbf{y} < \mathbf{1}>) \in \eta$

に対して，$< s_1\prime, 0 < x < 1 > \overset{a,0.09,x\leq 1\wedge y\leq 1}{\longrightarrow} < s_1\prime, 0 < x <= 1 >$ である．このとき，以下が成り立つ．

(a) $\mathbf{R}(< \mathbf{s_1\prime}, \mathbf{0 < x <= 1} >, < \mathbf{s_1\prime\prime}, \mathbf{0 < y <= 1} >) \in \eta$ であるような，ある $< s_1\prime\prime, < y <= 1 >$ に対して，$< s_1\prime\prime, 0 < y < 1 > \overset{a,1.0,x\leq 1\wedge y\leq 1}{\longrightarrow} < s_1\prime\prime, 0 < y <= 1 >$ が存在する．

(b) もし $\mathbf{G_1}$ が $< s_1\prime, 0 < x < 1 >$ において確率 0.09 と $x \leq 1 \wedge y \leq 1$ を持つならば，$\mathbf{G_2}$ が $< s_1\prime\prime, 0 < y < 1 >$ において確率 0.09 と $x \leq 1 \wedge y \leq 1$ を持つ．

. . . . . .

. . . . . .

. . . . . .

. . . . . .

以上より，$\eta \subseteq \mathbf{R}(\mathbf{G_1} \parallel \mathbf{G_2})$ は $\mathbf{G_1}$ から $\mathbf{G_2}$ へのリージョン模倣関係である．

■

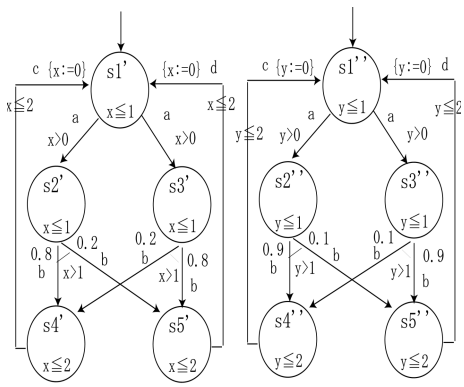
6. リアルタイムシステムの段階的詳細化開発への適用

一般的に，我々は段階的詳細化により，リアルタイムシステムを開発する．つまり，抽象的な仕様から，段階的に詳細化しながら，具体的な仕様を開発する．本章では，前章の結果を拡張して，それをリアルタイムシステムの段階的詳細化開発へ適用する．本章では，プロセス代数[9]の意味における，内部動作を考慮して，時間弱模倣関係を考えて，以下のように段階的詳細化を考える．

(1) まず，リアルタイムシステムの段階的詳細化開発では，抽象的な仕様を詳細化して，内部動作を追加しながら具体的な仕様を開発すると考える．

(2) 次に，具体的な仕様は抽象的な仕様に弱模倣されると考える．つまり，具体的な仕様から抽象的な仕様へ弱模倣関係が存在すると考える．この根拠は，観測可能な動作において，具体的な仕様は，抽象的な仕様が規定する範囲内で設計されるべきであるからである．

(3) さらに，**図 9** の場合を考える．前章の時間模倣関係では，$\mathbf{G_1}$ から $\mathbf{G_2}$ への時間模倣関係は存在しない．しかし，$\mathbf{G_1}$ では，確率 1.0 で $s2\prime$ と $s3\prime$ から $s4\prime$ へ遷移して，確率 1.0 で $s2\prime$ と $s3\prime$ から $s5\prime$ へ遷移する．一方，$\mathbf{G_2}$ では，確率 1.0 で $s2\prime\prime$ と $s3\prime\prime$ から $s4\prime\prime$ へ遷移して，確率 1.0 で $s2\prime\prime$ と $s3\prime\prime$ から $s5\prime\prime$ へ遷移する．現実の問題への適用を考えると，時間模倣関係を拡張して，上記場合でも模倣関係があると考えたほうがよい．つまり，組合せ遷移（後に定義する）を考慮する．これを確率時間模倣関係と呼ぶ．



(1) 確率時間オートマトン G1 (2) 確率時間オートマトン G2

図 9 確率時間模倣関係

Fig. 9 Probabilistic timed simulation relation.

以上の考察より，確率時間弱模倣関係を定義して，リアルタイムシステムの段階的詳細化開発への適用を図る．

6.1 確率時間弱模倣関係

確率時間弱模倣関係により，リアルタイムシステムの段階的詳細化開発を実現する．確率時間弱模倣関係では，組合せ遷移と内部イベント i を考慮する．直感的には，確率時間弱模倣関係では，**図 10** の $\mathbf{G_1}$ から $\mathbf{G_2}$ への確率時間弱模倣関係が存在する．ここで，$\mathbf{G_1}$ は具体的な仕様であり，$\mathbf{G_2}$ は抽象的な仕様である．

まず，組合せ遷移を定義する．

Definition18（組合せ遷移の定義）

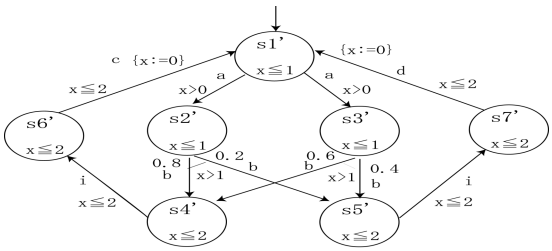
確率時間オートマトン $\mathbf{G}$ に対して，$prob(\Sigma \times S \times 2^X)$ の確率分布の有限集合 $\{\mu_i\}_i$ と重み $p_i > 0$ に対して，μ_i の組合せ $\sum_i p_i\mu_i$ は以下のような確率空間 $(\mathbf{\Omega}, \mathcal{F}, P)$ である．

(1) $\mathbf{\Omega} = \cup_i \mathbf{\Omega}_i$.

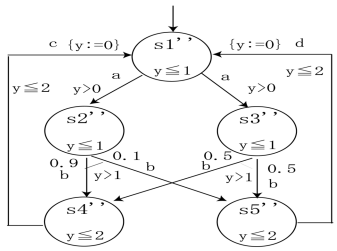
(2) $\mathcal{F} = 2^{\mathbf{\Omega}}$.

(3) 各 $(\sigma, s, \{x\}) \in \mathbf{\Omega}$ に対して，
$P[(\sigma, s, \{x\})] = \sum_{\{i|(\sigma,s,\{x\})\in\mathbf{\Omega}_i\}} p_i\mu_i[(\sigma, s, \{x\})]$.
ただし，$\sigma \in \Sigma$，$s \in S$，$\chi = \{x\}$ である．

もし遷移の族 $\{(s, \mu_i)\}_i$ と重み $\{p_i\}_i$ の集合が存在して $\mathcal{P} = \sum_i p_i\mu_i$ ならば，$(s, \mathcal{P})$ は $\mathbf{G}$ の組合せ遷移



(1) 確率時間オートマトン G1



(2) 確率時間オートマトン G2

図 10 確率時間弱模倣関係
Fig. 10 Probabilistic timed weak simulation relation.

である．なお，組合せ遷移は $< s_1, \nu_1 > \stackrel{\sigma,\mathcal{P},\tau_{s_1}(\mathcal{P})}{\longrightarrow}_C < s_1\prime, \nu_1\prime >$ と表記する．なお，各記号の意味は前章のとおりである．

■

次に，内部イベントによる遷移を含む遷移を定義する．

Definition19（内部イベントによる遷移を含む遷移の定義）

状態遷移 $< s_1, \nu_1 > \stackrel{\sigma,p,\tau_{s_1}(p)}{\Longrightarrow} < s_2, \nu_2 >$ は以下のときに存在する．

$$< s_1, \nu_1 > \stackrel{i,p\prime,\tau_{s_1}(p\prime)}{\longrightarrow} \ldots < s_1\prime, \nu_1\prime > \stackrel{i,p\prime\prime,\tau_{s_1\prime}(p\prime\prime)}{\longrightarrow} < s_1\prime\prime, \nu_1\prime\prime > \stackrel{\sigma,p,\tau_{s_1}(p)}{\longrightarrow} < s_2, \nu_2 >$$

■

最後に，確率時間弱模倣関係を定義する．

Definition20（確率時間弱模倣関係の定義）

2 つの確率時間オートマトン $\mathbf{G_1} = (S_1, \Sigma_1, \overline{s}_1, \chi_1, inv_1, prob_1, < \tau_{s_1} >_{s_1 \in S_1})$ と $\mathbf{G_2} = (S_2, \Sigma_2, \overline{s}_2, \chi_2, inv_2, prob_2, < \tau_{s_2} >_{s_2 \in S_2})$ が与えられたとする．以下の 2 つの条件を満たす $R \subseteq \Omega_1 \times \Omega_2$ を，$\mathbf{G_1}$ から $\mathbf{G_2}$ への確率時間弱模倣関係と呼び，そのような関係 R が存在するとき，$\mathbf{G_1} \preceq \mathbf{G_2}$ と記述する．ここで，$\mathbf{G_1}$ は具体的な仕様であり，$\mathbf{G_2}$ は抽象的な仕様である．なお，Ω_1 は状態 $< s_1, \nu_1 >$ の集合であり，Ω_2 は状態 $< s_2, \nu_2 >$ の集合である．ただし，$s_1 \in S_1$，$\nu_1 : \chi_1 \to \mathbf{R}$，$s_2 \in S_2$，$\nu_2 : \chi_2 \to \mathbf{R}$ である．Σ_1 と Σ_2 は外部から観測不能なイベント i を含む．

(1) 確率時間弱模倣条件

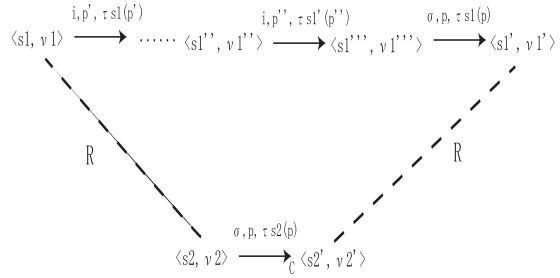


図 11 確率時間弱模倣条件
Fig. 11 Condition of probabilistic timed weak simulation relation.

$(< s_1, \nu_1 >, < s_2, \nu_2 >) \in R$ ならば，任意の σ について，$\tau_{s_1}(p)$ が遷移可能な条件であり，

$$< s_1, \nu_1 > \stackrel{\sigma,p,\tau_{s_1}(p)}{\Longrightarrow} < s_1\prime, \nu_1\prime >$$

である $< s_1\prime, \nu_1\prime >$ が存在するならば，

$$< s_2, \nu_2 > \stackrel{\sigma,p,\tau_{s_1}(p)}{\longrightarrow}_C < s_2\prime, \nu_2\prime >$$

である $< s_2\prime, \nu_2\prime >$ が存在して，$(< s_1\prime, \nu_1\prime >, < s_2\prime, \nu_2\prime >) \in R$ である．なお，$s_1, s_1\prime \in S_1$，$s_2, s_2\prime \in S_2$ である．

以上を**図 11** に図示する．

(2) 初期条件

$< \overline{s}_1, \mathbf{0} >$ に対して，$(< \overline{s}_1, \mathbf{0} >, < \overline{s}_2, \mathbf{0} >) \in R$ を満たす $< \overline{s}_2, \mathbf{0} >$ が存在する．

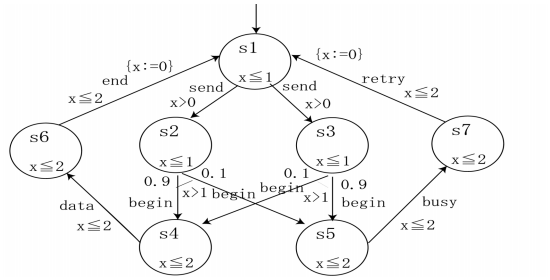
■

6.2 段階的詳細化開発の事例

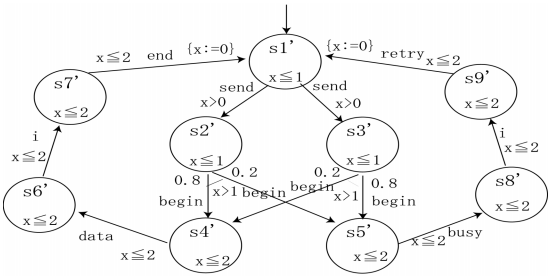
本論文では，簡単なリアルタイムシステムの段階的詳細化開発の事例を示す．イーサネットの CSMA/CD プロトコル[10] では，送信局と受信局からなる．ここでは，簡単な送信局の抽象的な仕様と具体的な仕様を記述して，具体的な仕様から抽象的な仕様への確率時間模倣関係が存在する例を示す．すなわち，具体的な仕様は抽象的な仕様の範囲内で動作する例を示す．

図 12 (1) の抽象的な仕様では，データ送信モードに遷移して ($s1 \to s2$)，データ送信を開始したら ($s2 \to s4$)，データ送信中になり ($s4 \to s6$)，データ送信中が終了する ($s6 \to s1$) 場合もあるが，回線がビジー ($s5 \to s7$) ならば，再び送信を試みる．ここで，データ送信モードへの遷移は非決定性の動作 ($s1 \to s2$ または $s1 \to s3$) である．また，データ送信の開始は確率的に起きるものとする．

図 12 (2) の具体的な仕様では，データ送信中において，新たな内部動作 ($s6\prime \to s7\prime$) を追加して詳細化したり，回線がビジーのときにおいても，新たな内部動作 ($s8\prime \to s9\prime$) を追加して詳細化したりする．



(1) 抽象的な送信局 S



(2) 具体的な送信局 S

図 12 リアルタイムシステムの段階的詳細化開発の事例
Fig. 12 Example of stepwise refinement development of real-time systems.

前述の確率時間模倣関係を使えば，送信局の具体的な仕様から抽象的な仕様への確率時間模倣関係が存在することが分かる．すなわち，送信局の具体的な仕様は抽象的な仕様の範囲内で動作する．これは正しく詳細化開発できたことを示している．

7. ま と め

本論文では，離散確率分布を持つ確率時間オートマトンの模倣関係を定義して，模倣関係の検証手法を定義した．さらに，リアルタイムシステムの段階的詳細化開発への適用が容易な確率時間模倣関係を定義して，実問題への適用方法を示した．今後の課題として，現在，以下の研究を進めている：

(1) 効率的な模倣関係の検証アルゴリズムの実装
(2) 本手法の実問題への適用
(3) モデル検査[5] と確率時間模倣関係との関係の明確化

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）の援助のもとで実施されました．

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) Alur, R. and Dill, D.L.: A theory of timed automata, *Theoretical Computer Science*, Vol.126, pp.183–235 (1994).
3) Alur, R., Courcoubetis, C. and Dill, D.L.: Model-Checking in Dense Real-Time, *Information and Computation*, Vol.104, pp.2–34 (1993).
4) 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).
5) Kwiatkowska, M., Norman, G., Segala, R. and Sproston, J.: Automatic verification of real-time systems with discrete probability distributions, *Theoretical Computer Science* (2002).
6) Cerans, K.: Decidability of Bisimulation Equivalences for Processes with Parallel Timers, LNCS 663, pp.302–315 (1992).
7) Tasiran, S., Alur, R., Kurshan, R.P. and Brayton, R.K.: Verifying abstractions of timed systems, LNCS 1119, pp.546–562 (1996).
8) Yamane, S.: A Practical Hierarchical Design by Timed Simulation Relations for Real-Time Systems, LNCS 1641, pp.151–167 (1998).
9) Milner, R.: *Communication and Concurrency*, Prentice Hall, New York (1989).
10) IEEE. ANSI/IEEE 802.3,ISO/DIS 8802/3. IEEE computer society (1985).

(平成 14 年 12 月 19 日受付)
(平成 15 年 6 月 3 日採録)

山根 智（正会員）
1984 年京都大学大学院修了．鹿児島大学を経て，現在，金沢大学工学部情報システム工学科勤務．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．