6A-3

頻度オペレータを導入したProbabilictic CTL とそのモデル検査アルゴリズム

冨田 尭　萩原 茂樹　樋浦 信　伊藤 宗平　米崎 直樹
東京工業大学大学院　情報理工学研究科　計算工学専攻

確率的なシステムの性質の記述にはしばしば確率計算木論理 Probabilistic Computation Tree Logic (PCTL) が用いられている。PCTL では、「いつかイベントが生起する」や「ずっとイベントが生起し続けている」などの性質を満たすパスの生起確率に言及できる。しかし、「80% 以上の頻度でイベントが生起する」などのイベントの生起頻度に関する性質を記述することはできない。本稿では、イベントの生起頻度を記述できるように PCTL を拡張した確率-頻度計算木論理を提案し、そのモデル検査アルゴリズムの概略を示す。

1　はじめに

確率的モデルの性質の記述にはしばしば確率計算木論理 Probabilistic Computation Tree Logic (PCTL) あるいはそれを拡張した Continuous Stochastic Logic (CSL) が用いられている [1]。それらの論理では「いつかイベント φ が生起する」($\mathbf{F}\varphi$) や「ずっとイベント φ が生起し続けている」($\mathbf{G}\varphi$)、「いつかイベント φ_2 を満たし、かつ、それまでの間ずっとイベント φ_1 が生起し続ける」($\varphi_1\mathbf{U}\varphi_2$) のような性質を満たすパスが生起する確率の制約を記述できが、パス上でのイベント生起頻度の制約を記述することはできなかった。また、報酬構造による拡張 [1] でも、頻度の期待値についての記述はできても、「イベント生起頻度が 80%以上であるパスの生起確率が 90%以上」のような性質は捉えられなかった。

本稿では新たに頻度オペレータ $\mathbf{Q}$ (freQuently) と一般化した Until 式 $\mathbf{U}$ (frequently Until) を導入した確率-頻度計算木論理 PQCTL を提案し、そのモデル検査について数値計算によるアルゴリズムと統計的手法によるアルゴリズムの概略を示す。

2　確率-頻度計算木論理 PQCTL

本章では、確率-頻度計算木論理 PQCTL の構文と意味論の定義を示す。

定義 2.1 (構文)**.** a を原子命題集合の要素とする。確率-頻度計算木論理 PQCTL は以下のように定義される状態式 φ の集合である。

$$\text{[状態式] } \varphi ::= \mathtt{true} \mid a \mid \neg\varphi \mid \varphi_1 \wedge \varphi_2 \mid \mathbf{P}_{\sim p}\psi$$
$$\text{[パス式] } \psi ::= \mathbf{Q}^{\leq k}_{\bowtie q}\ \varphi \mid \varphi_1 \mathbf{U}^{\leq k}_{\bowtie q}\ \varphi_2$$

ただし、$\sim, \bowtie \in \{<, >, \leq, \geq\}$、$p, q \in [0,1]$、$k \in \mathbb{N} \cup \{\infty\}$。

直観的には、$\mathbf{Q}^{\leq k}_{\bowtie q}\varphi$ は、パスの k ステップ以内での φ を満たす状態の頻度が制約 $\bowtie q$ を満たすことを表し、$\varphi_1\mathbf{U}^{\leq k}_{\bowtie q}\varphi_2$ は、パスの k ステップ以内に φ_2 を満たす状態に初めて到達しかつそれまでの間の φ_1 を満たす状態の頻度が制約 $\bowtie q$ を満たすことを表す。また、$\mathbf{P}_{\sim p}\psi$ は PCTL と同様に、その状態を始点とし ψ を満たすパスが生起する確率が制約 $\sim p$ を満たすことを表す。通常の時間論理の Until 式 $\varphi_1\mathbf{U}\varphi_2$ は $\varphi_1\mathbf{U}^{\leq\infty}_{=1}\varphi_2$ と等価であり、他の通常の時間演算子 $\mathbf{F}$ ($\mathbf{F}\varphi \equiv \mathtt{true}\mathbf{U}\varphi$)、$\mathbf{G}$ ($\mathbf{G}\varphi \equiv \neg\mathbf{F}\neg\varphi$)、通常の命題論理の演算子 $\vee$、$\leftrightarrow$ と合わせて略記として用いてよい。また、$k = \infty$ のときには時間制約 $\leq \infty$ は省略する。

これにより以下のような性質が記述できる。

$\mathbf{P}_{=1}\mathbf{Q}_{=1}\mathbf{P}_{=1}\mathbf{Q}^{\leq 10}_{\geq 0.9}\varphi$

– 10 ステップ中の 90%以上で φ を満たすようなパスを必ず生起する状態がすべてのパス上のほとんどいたるところで生起する。

$\mathbf{P}_{\geq 0.75}\mathbf{Q}^{\leq 10}_{\geq 0.9}\varphi_1 \Rightarrow \mathbf{P}_{\geq 0.85}(\varphi_1 \vee \varphi_2)\mathbf{U}_{\geq 0.95}\mathbf{P}_{=1}\mathbf{Q}^{\leq 20}_{=0.8}\varphi_2$

– 初期状態から 10 ステップ中の 90%以上の状態で φ_1 を満たすパスが 75%以上の確率で生起されるならば、20 ステップ中の 80%以上の状態で φ_2 を満たすパスが必ず生起される状態にいつか到達し、かつ、その間 φ_1 または φ_2 を 95%以上の頻度で満たすパスが 85%以上の確率で生起する。

このように、「だいたい φ を満たしている」や「だいたい φ_1 を満たす状況からだいたい φ_2 を満たす状況へ変化する」という性質について PCTL ではできないような詳細な記述が可能になる。

次に意味論を与える。状態式についてはPCTLと同様なため、頻度オペレータの意味のみを示す。頻度を考慮する領域が有限である場合には単純に頻度が決まるが、$\mathbf{Q}_{\bowtie q}$ では無限パス上の式を満たす状態の出現頻度を捉える必要がある。一般に無限集合の大きさは濃度で定義するが、ここで捉えたい大きさは濃度ではないため極限を用いて定義する。

定義 2.2 (頻度オペレータの意味)**.** 状態 $s_i \in S$ からなる無限パス $\omega = s_0 s_1 \ldots$ に対して $\omega(i) = s_i$ としたとき、$\mathbf{Q}$ 式と一般化した $\mathbf{U}$ 式に関する充足関係 $\models$ は以下のように定義する。

$$\omega \models \mathbf{Q}^{\leq k}_{\bowtie q}\ \varphi \Leftrightarrow$$

$$\begin{cases} \limsup_{k'\to\infty} \frac{|\{i \in \mathbb{N}^{\leq k'} | \omega(i) \models \varphi\}|}{k'+1} \bowtie q & \text{if } k = \infty \wedge \\ & \qquad \bowtie \in \{<, \leq\} \\ \liminf_{k'\to\infty} \frac{|\{i \in \mathbb{N}^{\leq k'} | \omega(i) \models \varphi\}|}{k'+1} \bowtie q & \text{if } k = \infty \wedge \\ & \qquad \bowtie \in \{>, \geq\} \\ \frac{|\{i \in \mathbb{N}^{\leq k} | \omega(i) \models \varphi\}|}{k+1} \bowtie q & \text{otherwise.} \end{cases}$$

$$\omega \models \varphi_1 \mathbf{U}^{\leq k}_{\bowtie q} \varphi_2 \Leftrightarrow$$
$$\exists k' \in \mathbb{N}^{\leq k}.(k' = \min\{i \in \mathbb{N} | \omega(i) \models \varphi_2\}$$
$$\wedge (k' = 0 \vee \omega \models \mathbf{Q}^{\leq k'-1}_{\bowtie q}\ \varphi_1))$$

3 PQCTL のモデル検査

本章では、有限状態マルコフ連鎖に対するPQCTLのモデル検査アルゴリズムの概略を示す。

3.1 数値計算によるモデル検査

有限状態マルコフ連鎖は必ず1つ以上の閉強連結成分を持ち、すべてのパスはいつか閉強連結成分のうちの1つに到達し、状態の出現頻度はその定常分布となる。そのため、$\mathbf{P}_{\sim p}\mathbf{Q}_{\bowtie q}\varphi_1$ 式については有限状態マルコフ連鎖の閉強連結成分への到達確率とその定常分布からパス式を満たす確率を計算できる。また、$k \in \mathbb{N}$ の $\mathbf{P}_{\sim p}\mathbf{Q}^{\leq k}_{\bowtie q}\varphi_1$ 式、$\mathbf{P}_{\sim p}\varphi_1\mathbf{U}^{\leq k}_{\bowtie q}\varphi_2$ 式については、i 回の遷移で状態 s から状態 s' へ φ_1 を満たす状態を j 回訪れた上で到達する確率 $Pr^i_j(s, s')$ からパス式を満たす確率を計算できる。マルコフ連鎖の状態数を $|S|$ とすると、Pr^i_j は遷移確率行列と Pr^{i-1}_{j-1} と Pr^{i-1}_j から $\mathcal{O}(|S|^3)$ で計算できるため、全体の計算量は $\mathcal{O}(|S|^3 \cdot k^2)$ である。$\mathbf{P}_{\sim p}\varphi_1\mathbf{U}_{\bowtie q}\varphi_2$ 式では φ_2 を満たすまでの遷移数とそれまでに訪れた φ_1 を満たす状態数のどちらも数え上げる必要があるため、PCTLのように φ_2 または $\neg\varphi_1$ を満たす状態への到達確率から求めることはできない。$\mathtt{true}\mathbf{U}^{\leq n}_{=1}\varphi_2$ を満たす確率が $\mathtt{true}\mathbf{U}_{=1}\varphi_2$ を満たす確率に十分収束するステップ数 n で $\mathbf{P}_{\sim p}\varphi_1\mathbf{U}^{\leq n}_{\bowtie q}\varphi_2$ を検査すればよい。このステップ数 n は、φ_2 を満たす状態において確率1で自己ループさせるように変形した遷移確率行列における1未満の固有値の中で絶対値が最大の固有値 λ に対して、$\mathcal{O}(\frac{1}{-\log|\lambda|})$ のサイズである。

3.2 統計的手法によるモデル検査

統計的なモデル検査はすなわち検定であり、十分なサイズのサンプルを生成し、その偏りから $\mathbf{P}_{\sim p}\psi$ の真偽を判定する。[2] で行われている逐次確率比検定を用いた統計的モデル検査アルゴリズムはPQCTLでもそのまま適用でき、任意に設定した精度のもとでモデル検査できる。$k \in \mathbb{N}$ のときにはサンプルは計算量 $\mathcal{O}(k \cdot \log|S|)$ で生成でき、検定に必要なサンプルサイズのオーダーは要求する精度（多重検定になるため必要な検定数に応じたエラー率の補正は必要）で決まるため、すべての状態についての検定の計算量も $\mathcal{O}(k \cdot |S| \cdot \log|S|)$ に抑えることができる。この手法では、大きいモデル・パス長を検査する場合でも十分な検査精度を保ったまま計算量を抑えられ、「φ_1 の生起頻度より φ_2 の生起頻度の方が大きい」や「φ_1 の生起頻度と φ_2 の生起頻度がどちらも30%以上」などのパスの性質を記述できるように論理を拡張したとしても計算量が変わらないという利点がある。

4 まとめ

本稿では、イベントの生起頻度を記述できるようにPCTLを拡張した確率-頻度計算木論理PQCTLを提案し、数値計算手法と統計的手法によるモデル検査アルゴリズムの概略を示した。

また、連続時間の性質を記述できるCSLに対しても同様の拡張ができ、その場合の連続時間マルコフ連鎖に対するモデル検査も行うことができる。

参考文献

[1] M. Kwiatkowska, G. Norman and D. Parker. Stochastic Model Checking. SFM 2007, LNCS 4486, pp. 220-270, 2007.

[2] H. Younes, R. Simmons. Probabilistic Verification of Discrete Event System Using Acceptance Sampling. CAV 2002, LNCS 2404, pp. 223-235, 2002.