2K-8

THA の到達可能性解析によるハイブリッドシステムの検証について

栗田 淳　　中村 勝則　　房岡 璋
立命館大学情報理工学部知能情報学科

1　はじめに

本研究では，先に提案した新しいオートマトンの枠組みである THA(Transfinite Hybrid Automaton) [1] に対する到達可能性解析手法を提案する．到達可能性解析とは，システムが初期状態から目標状態へと遷移し得るか否かを判定する問題であり，例えば，システムの安全性は危険状態への到達不可能性を示すことで検証可能である．

THA では, 非標準解析を用いることにより, 対象システムの連続的なダイナミクスを超離散化された差分方程式で記述するため, 離散的な手法のみでハイブリッドシステムの挙動を扱うことができる．また, Büchi の Transfinite Automaton の考え方を用いることにより, 無限回の離散的状態変化の後のシステム状態を表す．本稿ではこの THA の到達可能性解析によりシステムの検証を簡単に取り扱うことができることを示す.

2　問題設定

2.1　非決定性システム

先の報告 [2] では，ある状況下において状態の遷移先が一つに定まる一意なシステムを対象としたが，本研究では一つの状態に対して次の動作が決まらない非決定性を含むシステムを対象とする．

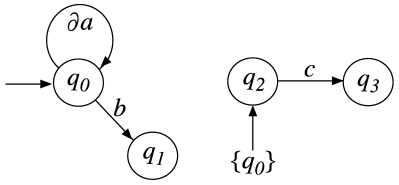

図 1: THA における非決定性モデル

図 1 のモデルは，状態 q_0 において無限小アクション ∂a の無限反復の後，状態 q_2 への極限遷移が起こることを表している一方，∂a の有限回の繰り返し中にアクション b が起こり, 状態 q_1 への遷移が可能であることも表している．このアクション b を例外的なアクションとし，また, その遷移先である状態 q_1 を異常状態とすることにより非決定性システムの表現を行うものとする．このような非決定性を含むシステムの動作は，上記アクションからなるアクションスキーマ

$$(\partial a)^{\omega} c + (\partial a)^{\omega'} b \quad (\omega' < \omega)$$

として表現できる．

Verification of Hybrid System on Reachability Analysis of Transfinite Hybrid Automaton
Jun Kurita, Katsunori Nakamura, Akira Fusaoka
Dept. of Human and Computer Intelligence,
Ritsumeikan University

2.2　Nondeterministic Transfinite Hybrid Automaton

非決定性システムの記述においては，一般に状態遷移の振る舞いに多様性が生じる．そこで，Nondeterministic Transfinite Hybrid Automaton $\mathcal{A}$ を形式的に次の 8 組で定義する．

$$\mathcal{A} =< Q, A, E, I, F, X, X_0, D > \tag{1}$$

Q : 有限個の状態からなる集合
A : 有限個の無限小アクションからなる集合
E : 有限個の状態遷移ルールからなる集合
　$q \in P$ のときに $(P, q) \notin E$ であるとして,
　$E \subseteq (Q \times A \to \mathcal{P}(Q)) \cup (\mathcal{P}(Q) \to \mathcal{P}(Q))$
$Inf(q_1, q_2, \cdots, q_n)$:
　状態遷移 $q_1, q_2, \cdots, q_n$の無限反復後の状態
I_0 : 初期状態の集合 ($I_0 \subseteq Q$)
F : 終了状態の集合 ($F \subseteq Q$)
X : 状態変数の集合 (Situation)
　$X \subseteq \mathbf{R}^m$, $m \in \mathbf{N}$ でシステムの物理的状態を表す.
　特に時刻を表す変数 t を含む.
X_0 : X の要素である初期状態の集合
D : A の各要素のアクションの定義からなる集合
　$x, x' \in X$ において非標準の算術操作 f を用いて
　$x' = f(x)$ と表される.

ここで，Q, A, F, X, X_0, D の意味は決定性 THA の場合と同じであるが，I_0 が初期状態の集合であり，I_0 に属する任意の状態を初期状態にすることができること，及び状態遷移関数が Q の冪集合への関数となっており，任意の Q の部分集合の要素への遷移できる点が拡張点である．

3　到達可能性解析

3.1　後ろ向き解析

本研究では, 式 (1) で与えられるシステムに対し, 目標状態に到達可能な全状態を逆向きに戻って求め，初期状態との充足可能性を調べることにより, システムが目標状態に至るかどうか判定する．

ここで THA の遷移関係において，現在の状態へ 1 度の遷移で到達できるような，現在から 1 回分過去に戻った全状態集合を求める関数 pre を定義する．THA における状態と Situation の対集合を region $R(= \bigcup_{q_i \in Q}(q_i, x_i))$ とし，この region 単位で到達可能性の解析を行う．

spre(R)：同一状態内において Situation x_i を時間後継とする状態集合

演算子 spre は，単一の状態 $q_i \in Q$ における現在の Situation x_i に対して，1 度の無限小アクションで x_i に遷移可能な，過去の Situation の集合を与える．

$$\mathrm{spre}(q, x_i) = (q, x_{i-1}) \text{ where } ((q, \partial a, q) \in E \wedge x_i = \partial a(x_{i-1}))$$

THA では, 一般的な有限状態遷移規則に加え, 集合内の全ての状態を無限回巡回した後, 次の状態への遷移を行う極限遷移規則を用いている．そこで, 現在の状態 $q_i \in Q$ に対して，1 回の有限状態遷移のみで q_i へ遷移可能な状態集合を与える関数 fpre と極限遷移により q_i へ遷移可能な状態集合を与える関数 lpre を次のように定義する．

fpre(R)：状態 q_i を有限状態遷移後継とする状態集合

$$\mathrm{fpre}(q_i, x_i) = \bigcup_{(q_{i-1}, a_{i-1}, q_i) \in E} (q_{i-1}, x_{i-1}) \text{ where } (p(x_{i-1}) \wedge x_i = x_{i-1})$$

ここで，$p(x_i)$ は Situation x_i においてアクション a_i を適用する事前条件とする．

lpre(R)：状態 q_i を極限遷移後継とする状態集合

$$\mathrm{lpre}(q_{i+1}, x_{i+1}) = \bigcup_{(\{q_{i1}, q_{i2}, \cdots q_{ir}\}, q_{i+1}) \in E} (q_{ij}, x_i) \text{ where } (0 < j < r \wedge x_{i+1} \approx x_{ij})$$

よって，現在の region $R = (q_i, x_i)$ へ 1 度の遷移で到達可能な全状態は

$$\mathrm{pre}(R) = \mathrm{spre}(R) \cup \mathrm{fpre}(R) \cup \mathrm{lpre}(R)$$

で与えられる．

ハイブリッドオートマトンでは, 連続的な状態変化と離散的な状態間遷移と 2 つの種類の異なるダイナミクスで対象システムの挙動を記述するため, 逆像計算の取り扱いが困難であるが, それに対し THA では, 非標準解析を用いて超離散化された差分方程式で対象システムのダイナミクスを記述するため, これらの逆像計算は超実数上の代数的な演算のみで求めることが可能である．

3.2 到達可能性判定

ここでは，前節で定義した逆像計算を用いて THA の目標状態 ψ_R への到達可能性判定を行う．$\psi_0 = \psi_R, i \geq 0$ を反復回数としたとき，ψ_R への到達可能な状態集合 ψ は次式の最小不動点として与えられる．

$$\psi_{i+1} = \psi_i \cup \mathrm{spre}(\psi_i) \cup \mathrm{fpre}(\psi_i) \cup \mathrm{lpre}(\psi_i) \qquad (2)$$

また THA の初期状態が ψ_I，目標状態が ψ_R であるとき，THA が目標状態に到達可能であることは次式を満たす ψ_i が存在することと同値であると言える．

$$\exists i[\psi_I \cap \psi_i \neq \emptyset]$$

よって，ψ_R への到達可能な全状態を逆像計算を繰り返し適用することにより求め，充足関係より初期状態からの到達可能性の判定を行う．

Reach：到達可能性判定

THA の初期状態を $\psi_I = (q_0, x_0)$，目標状態を ψ_R とするとき，$q_0 = q_i$, 及び $x_0 \wedge x_i \neq \emptyset$ を満たす ψ_i が ψ 内に存在する場合，Reach は真である (THA が目標状態へ到達可能) とする．

ここで, ψ_i は以下のように再帰的に求められる．

$$\begin{aligned}
\psi_i &= pre(\psi_{i-1}) \\
&= \psi_{i-1} \cup \mathrm{spre}(\psi_{i-1}) \cup \mathrm{fpre}(\psi_{i-1}) \cup \mathrm{lpre}(\psi_{i-1}) \\
\psi_{i-1} &= pre(\psi_{i-2}) \\
&= \psi_{i-2} \cup \mathrm{spre}(\psi_{i-2}) \cup \mathrm{fpre}(\psi_{i-2}) \cup \mathrm{lpre}(\psi_{i-2}) \\
&\vdots \\
\psi_1 &= pre(\psi_0) \\
&= \psi_0 \cup \mathrm{spre}(\psi_0) \cup \mathrm{fpre}(\psi_0) \cup \mathrm{lpre}(\psi_0)
\end{aligned}$$

この式より, $\psi_{i-1} \subseteq \psi_i$(単調増加) であり, ψ_i を求める際には $\psi_j (j = 0, 1, \cdots i-1)$ が既に得られているため, 反復計算ごとに新たに求められる $\mathrm{pre}(\psi_{i-1})(= \mathrm{pre}(\mathrm{pre}(\psi_{i-2})))$ に対してのみ初期状態との充足性を調べることで目標状態への到達可能性を判定でき, これよりシステムの検証が可能となる．

4 おわりに

本稿では，THA の到達可能性解析により代数的な手法のみでシステムの検証を行なう手法について定式化を行なった．今後は, 到達可能性解析に基づくシステムの安定性の検証などについて検討する予定である．

参考文献

[1] Katsunori NAKAMURA, Akira FUSAOKA, "On Transfinite Hybrid Automata", Hybrid Systems: Computation and Control, Proceedings of the 8th International Workshop, HSCC2005, LNCS3414 pp.495-510 Springer-Verlag, 2005

[2] 栗田淳，中村勝則，房岡璋．"On Transfinite Hybrid Automaton"，情報処理学会第 67 回全国大会講演論文集，1N-5，pp.255-256，2005

[3] R. Alur, C. Courcoubetis, N. Halbwachs, P.-H. Ho, X. Nicollin, A. Olivero, J. Sifakis, S. Yovine. "The Algorithmic Analysis of Hybrid Systems", Theoretical Computer Science, 138:3-34, 1995