CafeOBJ を用いた
ハイブリッドシステムの形式的な仕様記述と検証

山岸 大悟 (210097)

北陸先端科学技術大学院大学 情報科学研究科

2004 年 2 月 13 日

キーワード: CafeOBJ, ハイブリッドシステム, HOTS, アクティビティ, モデル化.

1 はじめに

組み込みシステム等, アナログ事象にデジタル事象が組み込まれたシステムのことをハイブリッドシステムと呼ぶ. ハイブリッドシステムは高信頼性を求められるものが多く, システム記述の際には信頼性を保証することが重要である. 本研究の目的は, ハイブリッドシステムが検証可能な数学モデルを提案することである. さらに, 提案されたモデルが有効であることを確かめるために, ある例題に対してモデル化されたシステムを, 代数仕様言語 CafeOBJ を用いて記述し, 検証を行う.

CafeOBJ が属する代数仕様言語は, 代数に基づいて記述された仕様を用いて, 数学による証明を用いた検証を行うことが可能である. 特に CafeOBJ では, 隠蔽代数を用いて抽象機械を記述, 検証することが可能である. CafeOBJ で抽象機械を表現するための数学モデルとして観測遷移機械 (OTS : Observational Transition System) がすでに提案されており, プロトコルの検証や, 制御システムの検証等で成果があげられている. ハイブリッドシステムのモデル化については, そのサブクラスであるリアルタイムシステムに関して, OTS にある時間制約を持たせた拡張が行われている (TOTS : Timed OTS). しかしながらこのモデルは, 時間のみを実数として扱っているため, ある物理変数が常微分方程式に従って変化するようなシステムには対応していない.

そこで本研究では, 観測遷移機械を拡張し, ハイブリッドシステムに対して適応可能な HOTS : Hybrid OTS を新たに提案した. 提案した手法の有効性を確認するために, 2 つの例題を用いて事例研究を行った. そして CafeOBJ を用いて, モデル化されたシステムの記述を行い, 安全性の検証を行った.

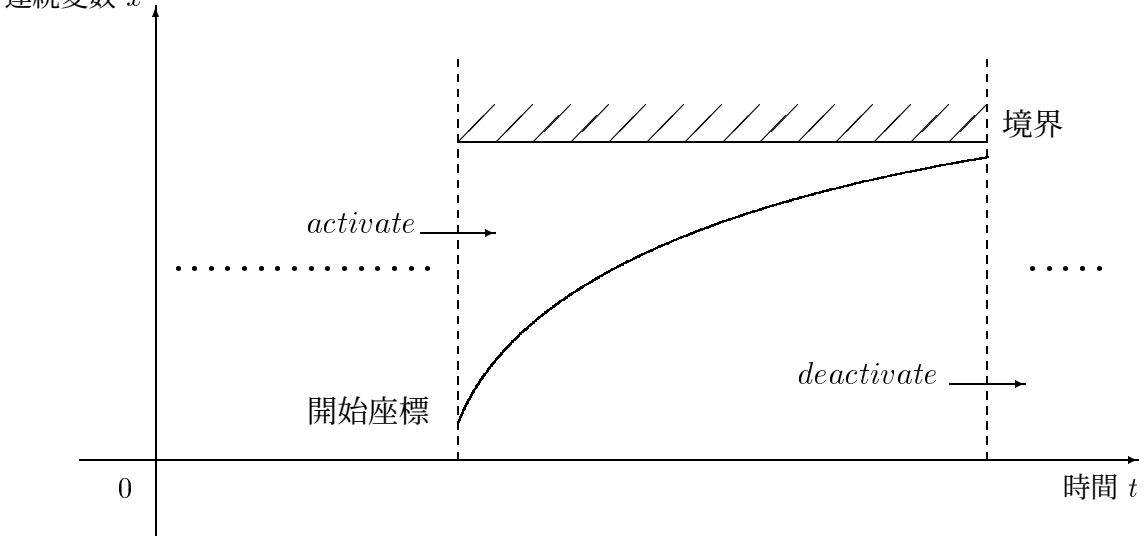

図 1: アクティビティ概念図

2 モデルの概要

本研究では, まず始めに OTS にアナログ事象を持たせた HOTS を提案した. HOTS が持つアナログ事象は, アクティビティによって決定される. アクティビティにおいて重要な要素は, アクティビティの開始座標と, 境界, 常微分方程式である. アクティビティ概念図を図 1 に示す.

- 図 1 における $activate$ は遷移規則であり, 対象とするアクティビティ内の連続変数を動作可能にする.
- $activate$ が生じると, アクティビティ内の連続変数は, 開始座標に設定される.
- 開始座標に設定された連続変数の進化は遷移規則 $deactivate$ が生じるまで行われる.
- 開始座標から, 境界を越えない範囲で, アクティビティが持つ常微分方程式に従って, 時間前進に伴い進化する.
- $deactivate$ が生じると, 対象となるアクティビティ内における動作中の連続変数は, 動作を停止する.

3 成果, 今後の課題

HOTS を用いて, 2 つの例題に対するモデル化, CafeOBJ による記述, 安全性の検証を行った. 例題として用いたシステムは, サーモスタット (自動温度制御システム) と交差点問題である. 両例題の違いは, 独立した制御対象の数である. サーモスタットは 1 つであるが, 交差点問題はある 2 つの制御対象が合成された分散システムである. モデル化は両例題共 HOTS を用いて記述が可能であった, CafeOBJ を用いた記述, 帰納法を用いた安全性検証では, HOTS において連続変数を動作させる唯一の遷移規則 $tick$ について, アク

ティビティ, 境界に対する記述者の推論, さらに補題の適用が必要であった. 交差点問題に関しては, 変数の時間前進に関して, 記述者が合成システムの解軌道予測をしなければならないことが例題から判明した.

以上の結果より, 本研究で提案した HOTS は, 事例研究に限れば, HOTS でモデル化されたシステムを CafeOBJ で記述, 処理系を用いた検証を行うことが満足できた. 従って, 現時点において, HOTS でモデル化し, CafeOBJ を用いて記述されたものに関して, 検証可能なものは,

- 1 階線形微分方程式であるもの

であることが推測できる.

さらに別の結論として, ハイブリッドシステムを記述するためのモデルの 1 つであるハイブリッドオートマトンを用いて記述された, サーモスタット例題の定義を, HOTS の定義で解釈することが可能であった. このことから, 意味的なモデルであるハイブリッドオートマトンを, HOTS を用いることで, CafeOBJ で記述し, 検証支援系を用いた簡約による証明を行える可能性が示唆できた.

今後の課題は, より汎用的なハイブリッドシステムを CafeOBJ で記述するために,

- n 階微分の結果が定数であるもの

を記述可能にするための手法を提案することである.

もう 1 つの課題は, 連続システムから離散遷移システムへの抽象化手法を HOTS に適用させること, さらに実数に関する述語を用いた決定手続きを考えだし, 実装を行い, 実装結果を CafeOBJ に反映させること等である.