平成26年度 情報工学コース卒業研究報告要旨

結縁研究室 研究室	氏　　名	稲垣 貴大
卒業研究題目	SpaceEX GUIから微分動的論理式への変換によるハイブリッドオートマトンの検証支援	

実世界におけるシステムの振舞いは状態の離散的な変化と値の連続的な変化によって特徴づけることができる．このようなシステムに対する制御プログラムは，プラントの連続的な値の変化と，制御部における離散的な状態の変化を扱う必要がある．本研究ではシステムの安全性の検証のために，離散的な値の更新に加えて，時間経過とともに連続的かつ自律的に更新される値の情報を持つ振舞いモデルを直接扱う．

ハイブリッドオートマトンは，有限オートマトンの状態に対して連続的に変化する値に関する微分方程式を加えることによって，離散と連続の両方の振舞いをモデル化する．ハイブリッドオートマトンの到達可能性に基づく検証を行うことで，エラー状態への到達可能性を排除し，安全性の検証が可能である．ハイブリッドオートマトンの到達可能性は一般に決定不能であるため，ハイブリッドオートマトンを用いた，システムの直接的な安全性検証は限定されたクラスにのみ可能である．

Platzer らによって提案されている微分動的論理は真偽値割り当てが決定可能な，連続的な値の変化と離散的な状態の変化を扱うシステムの形式的モデルである．微分動的論理は様相論理の拡張で，時間に関するシステムの性質を記述できる．また，微分動的論理の定理証明器 KeYmaera を用いることで微分動的論理式の厳密な証明が可能である．ここで，微分動的論理式は可読性が低く，直感的な定式化が容易でないことが問題である．

本研究では，ハイブリッドオートマトンのGUIであるSpaceEXで記述されたXMLファイルを微分動的論理式に自動変換する検証支援プログラムを作成した．SpaceEX の GUI による記述から，ハイブリッドオートマトンの変数情報，状態情報，遷移情報を抽出し，微分動的論理式を生成する．この論理式に対してループ不変式と検証したい振舞いを論理式で記述し，生成した微分動的論理式に加え，定理証明器KeYmaeraを用いて微分動的論理式の検証を行う．

本研究の手法を用いることで，直感的に設計したハイブリッドオートマトンの安全性の検証が可能となる．BouncingBall と WaterTank のモデルに対して本手法を適用し，安全性の検証証明を構成した．