平成27年度 情報工学コース卒業研究報告要旨

結縁・中澤 研究室	氏　　名	市 橋　友 樹
卒業研究題目	Yampaプログラムの安全性検証のための振舞いモデル	

本研究では，Haskell言語のドメイン固有言語であるYampaプログラムの安全性を検証するための振舞いのモデルとして差分オートマトンを提案する．差分オートマトンはハイブリッドオートマトンにおける離散的・連続的な遷移の他に，微小時間経過による遷移を持つ．微小時間経過において変数には事前値と事後値の値割当を区別し，時間経過による遷移とロケーションの遷移の際の更新を行うことによって，Yampaの離散的な実行を表現する．

ハイブリッドシステムとは時間経過に伴う離散的変化と連続的変化が混在した動的システムであり，そのモデル化手法としてハイブリッドオートマトンがある．しかし，正しいものと判断したモデルからハイブリッドシステムを記述したプログラムを実際に動作させてみると意図しないエラーが発生することがある．これは，プログラムにおいて連続的な時間変化が実際の動作では離散的であることが原因である．よって実際に動作させるまでエラー発生の可能性に気づけず，原因を突き止めるために何度もテストをする必要が出てくる．こういったエラーが事前に分かれば，テストの負担を軽減することができる．

YampaとはFunctional Reactive Programming (FRP) というパラダイムの実装の1つである．FRPは連続的に時間変化する値behaviorと時間順に並べた事象発生の列eventという2つの概念を持つ．Yampaにおいては信号Signalと信号関数SFという2つの概念を持ち，関数型言語であるHaskell言語の枠組みでハイブリッドシステムを記述する．Signalは時間を引数に値を返す関数であり，SFは信号を引数として信号を返す関数である．離散的な遷移を表現するために信号に対するスイッチングを行う関数switchにより特定の事象が発生した際にSFを切り替える．

本研究では，末尾再帰を持つYampaで記述したプログラムから差分オートマトンを作成し，プログラムがモデルとなるハイブリッドオートマトンに従わない動作をする可能性があることをモデル化によって確認できた．Yampaプログラムにおいて理想的な動作は，連続的な時間変化に伴って処理が行われることである．Yampaプログラムが実際に動作する際には微小時間を次々と切り取って扱うことで実時間の近似を行っているため，エラーが発生する可能性があることを示している．