平成29年度 情報工学コース卒業研究報告要旨

高田 研究室	氏　　名	清 水　貴 裕
卒業研究題目	シンボリック実行に基づく状態遷移モデルの抽出	

組込みシステム開発の現場では，設計書やテストケースが存在しない，もしくは更新されていないレガシーコードが存在する．このような状況では，ソースコードの保守や再利用が困難になる．一方，組込みシステム開発の現場では，開発期間短縮や低コスト化の要求がある．よって，リバースエンジニアリングによりレガシーコードの設計を明らかにすることができれば，組込みシステム開発の生産性を向上させることができる．

多くの組込みシステムには，イベント・状態・動作・遷移が存在し，これら 4 つの要素から構成されるモデルを表現した状態遷移表によって，システムの振舞いを表現可能である．そこで，組込みシステム向けのソースコードに対するリバースエンジニアリングの方法の 1 つとして，状態遷移表を抽出することが提案されている．先行研究において，状態遷移表抽出ツールが開発された（以下，既存ツール）．既存ツールでは，イベントが発生する条件（イベント条件）や状態遷移が発生する条件（遷移条件）の抽出を，専用のソースコード解析器を開発して実現している．しかし，既存ツールには以下の問題点がある．1 つ目の問題点は，開発したソースコード解析器は C 言語専用のものであるため，対応可能プログラミング言語を増やすためには，専用のソースコード解析器を言語ごとに開発する必要があることである．2 つ目の問題点は，不等式を含む条件式の解析が複雑になるため，条件式に不等式を含むソースコードに対応できていないことである．

シンボリック実行とは，ある変数に対して具体的な値ではなく，シンボルを割り当てて疑似的に実行することである．シンボリック実行により，ある実行における条件と処理を知ることができる．シンボリック実行ツールにより得られた条件と処理について木形式でまとめたものを，シンボリック実行木と呼ぶこととする．シンボリック実行木のノードはソースコード中の位置を表す．エッジは実行経路を表し，分岐となるノードのあとのエッジには条件が，処理が存在するエッジにはその処理が書かれている．

本研究では，上述の 2 つの問題点の軽減を目的とする．目的を達成するべく，プログラムの解析を既存のシンボリック実行ツールによって行い，その解析結果から状態遷移表抽出手法を提案する．提案手法では，まずシンボリック実行ツールによってソースコードからシンボリック実行木を抽出する．次に，抽出したシンボリック実行木を深さ優先探索でたどっていき，イベント条件や遷移条件，それらに対応する処理を抽出する．抽出したイベント条件や遷移条件およびユーザが選択した状態変数を基に，状態遷移表を抽出する．抽出された状態遷移表では，冗長な表現が見られたため状態遷移表抽出後にツール内で修正を行った．本研究で用いるシンボリック実行法は，様々な言語に対して正確な解析を行うことができる実装が公開されている．そのため，それらを利用することで上述の 2 つの問題点を軽減できると考えられる．

提案手法を実装し，状態遷移表を抽出するツールを開発した．また，本ツールについて適用実験を行った結果，状態遷移およびイベントの発生の両者が表現されている 11 個のソースコードのうち，10 個のソースコードについて状態遷移表を抽出することができた．

今後の課題は，様々な言語で記述されたソースコードに対して本ツールを適用し，抽出された状態遷移表の正確さを確認することである．また，本ツールを組込みシステム技術者に使用してもらうことにより，有用性の評価および改善を行いたいと考えている．