平成21年度 情報工学コース卒業研究報告要旨

阿草 研究室	氏　　名	坂　知 樹
卒業研究題目	ソースコード解析に基づくTOPPERS/ASPカーネルにおけるタスク制御システムのUPPAALを用いたモデル化	

本研究では，TOPPERS/ASP カーネルにおけるタスク制御システムをソースコード解析に基づきモデル化し，UPPAAL を用いてその振る舞いを検証した．

航空機の姿勢制御システムや自動車のエンジン制御など，リアルタイム性が求められるシステムは，必ず一定時間内に処理を完了しなければならないなどの高度な時間制約が課せられる．それらリアルタイムシステム上に構築されているのがリアルタイム OS である．リアルタイム OS は，処理に優先度をつけて細かくスケジューリングする機能を持ち，応答時間が一定の範囲内にあることを保証する．

このような高信頼性が求められるシステムが誤った動作をしないことを示すために，モデル検査が用いられる．モデル検査は，検査したいシステムにおいて検査したい特徴を残して抽象化した「モデル」を作成し，そのモデルの振る舞いを網羅的に調べることでシステムの動作を証明する．

リアルタイム OS のひとつに，TOPPERS プロジェクトにより開発されている，TOPPERS/ASP カーネルがある．この OS の動作を保証する検査はコードレビューなど，人の手を用いて行われているにすぎず，内部にバグがないとは言い切れない．タスクのスケジューリングが正しく行われず，処理が一定時間内に終了しないと，システムは致命的な損害を受ける．

本研究では ASP カーネルのタスク制御システムを拡張時間オートマトンに変換することでモデル化を行い，モデル検査ツールである UPPAAL を用いてソフトウェアモデル検査を行った．モデル化はソースコード解析に基づいた．ソースコードを分割し，それぞれのブロックにおける分岐命令以外の命令が終了した時点を拡張時間オートマトンのそれぞれの状態とし，分岐命令をガード条件とした．このことから，モデル化する際の主観を排除し，モデルから本質が失われることを防ぐことができた．タスク制御システムは，多くの機能をもつが，本研究でモデル化し検査したのは，それらのうちの一部である．具体的には，タスクのスケジューリングが正しく行われているか，タスクの切り替えが不可分であるか，想定外の割込みが発生しないかである．

モデル検査の結果，タスク制御システムは仕様通りに動作することがわかり，システムに問題が無いことが確認された．しかし，本研究でのモデル規模は，タスク制御システムのすべての特徴をモデル化しているわけではないにもかかわらず，UPPAAL で検証できるモデル規模の限界値に近かった．これは，ソースコードからモデル化を行ったことにより，モデルが冗長になってしまったからである．そのため，今後は検証範囲を広げることを考えると共に，モデルの冗長性をなくし，状態数を減らすことも考えなければならない．

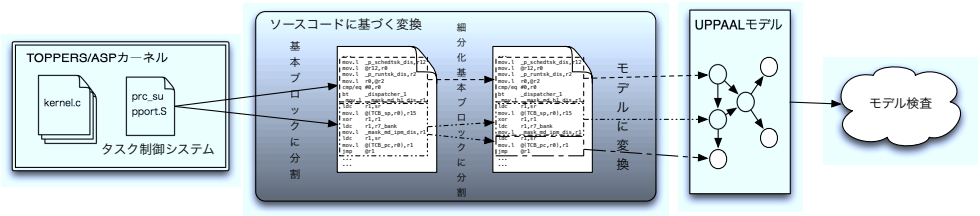

図:手法の概要