平成24年度 情報工学コース卒業研究報告要旨

結縁・寺内 研究室	氏　　名	西 木　悠
卒業研究題目	確率的モデル検査による実時間システムの検証	

モデル検査はシステムを網羅的に検証することで，人間の手では見つけることが困難な欠陥を検出する手法である．モデル検査に確率的拡張を施した確率的モデル検査は，確率的な振る舞いをするシステムの量的や質的な性質の検証を行うための手法である．システムはマルコフ連鎖やマルコフ決定過程，加えて確率時間オートマトンなどの確率・時間・非決定性を含むものでモデル化される．検証する性質の記述には確率的計算木論理などの確率と時間を記述できる時相論理を使用する．確率的モデル検査でシステムを解析することにより，信頼性の評価やパフォーマンスの測定などが可能である．

本研究は，確率的モデル検査により検証できるシステムの規模を調査することを目的としている．調査を行うため，バス型ネットワークを持つ通信プロトコルである Controller Area Network (CAN) を確率的システムとみなしたモデル化を行った．CAN はメッセージと呼ばれるデータの転送に時間制約が存在する実時間システムである．また，CAN はバスに接続された複数のノードが一つのバスを共有し，並行に動作する構造をしている．さらに，全ての CAN ノードはメッセージボックスと呼ばれるキューを備えている．したがって，CAN は並行性とキューを兼ね備えた実時間システムであると言える．これらはモデル検査において状態爆発を引き起こす要因として知られている．確率的モデル検査においても同様の状況を招くのであれば，CAN の厳密な確率的検証は非常に困難であることが予測される．条件の異なる複数のモデルを記述して実験を行うことによりキューや並行性の存在が CAN の確率的モデル検査をどのように難しくしているのかを調査した．

CAN は離散時間マルコフ連鎖でモデル化する．システムは全体でただ一つのクロック変数を持つものとし，各サイクルにおいて決められた手順を実行することにより CAN の振る舞いを再現する．また，CAN ノードで生成されるメッセージの種類は確率分布に従って選ばれるものとする．確率的モデル検査器には PRISM を使用したため，システムは PRISM 言語で記述した．

記述した CAN のモデルを確率的モデル検査により検証したところ，小さい規模の CAN のモデルに関しては確率的検証を行うことが可能であった．また状態数のスケールを調査する実験を行った結果，ノード数やキューの長さにより状態数は指数関数的なオーダーで増加することを観測した．この結果は，現在製品化されている典型的な CAN システムを確率的モデル検査により検証することが困難であることを示唆している．検証困難に陥った原因を考察した結果，CAN のモデルに対する数的なアプローチによる峻厳な検証は限界を向かえているという結論に至った．CAN のように厳密な検証が難しいモデルに対しては別のアプローチで検証を行う必要がある．そこでシミュレーションベースのモデル検査手法である統計的モデル検査に注目して，記述した CAN のモデルに適用可能であるか調査した．統計的モデル検査に適用できれば，一定の過誤は含むものの高い精度をもって大規模な CAN の検証が可能となる．