氏名	長岡武志（ながおかたけし）
博士の専攻分野の名称	博士（情報科学）
学位記番号	第 24649 号
学位授与年月日	平成23年3月25日
学位授与の要件	学位規則第4条第1項該当 情報科学研究科コンピュータサイエンス専攻
学位論文名	Study on Model Abstraction for Model Checking of Real-time Systems （実時間システムに対するモデル検査のためのモデル抽象化に関する研究）
論文審査委員	（主査） 教授 楠本 真二 （副査） 教授 井上 克郎　教授 増澤 利光　准教授 岡野 浩三

論文内容の要旨

本論文は，情報システムの高信頼化技術であるモデル検査，特に実時間システムを対象とした検査に対して，検査コストの削減を目的とするモデル抽象化手法についての研究をまとめたものである．

まず，実時間システムをモデル化する時間オートマトンを対象としたモデル抽象化手法を提案している．提案手法では，モデルの抽象化にCEGAR(CounterExample-Guided Abstraction Refinement)の枠組みを利用し，適切な抽象モデルを自動的に生成する．提案手法ではまず最初に時間オートマトンが持つクロック変数を全て削除した抽象モデルを生成する．そしてモデル検査の結果得られた偽反例をもとに抽象モデルを洗練することを繰り返すことで，最終的に適切な抽象モデルを生成する．

さらに，提案した抽象化手法を，時間オートマトンに対して確率的な振る舞いを付加したモデルである確率時間オートマトンへ拡張した手法を提案している．一般的に確率的なモデル検査では，反例としてモデル上の具体的なパスを提示しないため，提案手法ではk最短路探索アルゴリズムを利用することで最大k個のパスを探索し，反例として提示する手法を用いている．さらに，確率時間オートマトンでは反例として提示する複数のパスが互いに両立可能でなければならないため，パスの両立性の検査，両立性を保つためのモデル変換手法を提案している．

次に，実時間分散システムを対象とした性能解析を確率モデル検査を用いて実現する手法を提案している．状態爆発の問題を回避するため，モデル検査におけるシミュレーション機能を利用した抽象化を提案している．提案手法ではまず，対象システムを詳細にモデル化したモデル上でシミュレーションを行い，振る舞いを詳細に解析する．そして得られた解析結果をもとに抽象モデルを生成し，確率モデル検査を適用する．

最後に，実時間システムの時間的なQoS(Quality of Service)を時間オートマトンを用いて検査する手法を提案している．提案手法では，QoSをシステム全体に要求される「要求QoS」と，システムを構成する各コンポーネントがそれぞれ提供す

ると期待される「提供QoS」に分割し，２ステップによる検査を行う．まず，提供QoSを前提にシステム全体をモデル化し，要求QoSの検査を行う．そして，各コンポーネントに対しては実際に提供QoSを満たすか否かを個別に検査を行う．

論文審査の結果の要旨

本論文は，実時間システムに対するモデル検査において，適切なモデル抽象化を行うことでモデルの状態空間を削減する手法を提案している．

時間オートマトンを用いて実時間システムを検証する場合，状態空間に時間の概念が組み込まれるため，一般的なモデル検査に比べて状態爆発の問題が深刻である．状態爆発の問題を回避する手法の一つにモデル抽象化手法があるが，提案手法ではCEGAR(CounterExample-Guided Abstraction Refinement)と呼ばれる枠組みを利用することで，時間の概念を自動的かつ適切に抽象化することができる．提案手法ではCEGARによるモデル検査，抽象モデルの洗練の繰り返し，に多くの時間を必要とするが，抽象化を適用しない場合に比べメモリ消費を大幅に削減できており，スケーラビリティ向上に有効であるといえる．

本論文では，更に提案手法の対象モデルを確率時間オートマトンに拡張している．確率時間オートマトンでは，時間の概念に加え確率的な振る舞いを考慮する必要があるため，状態爆発の問題がより深刻である．また，一般的な確率モデル検査では不具合検出時に具体的な反例を提示しないが，提案手法では具体的なパスの集合として反例を提示可能である．モデル検査で提示される反例は不具合修正の手掛かりとして利用されるため，反例を提示可能である提案手法は確率的な振る舞いを持つ実時間システムの設計に有用であると考えられる．また，提案手法は構築する状態空間の削減にも効果があることが実験により示されており，検証コストの削減についても貢献しているといえる．

実時間分散システムの性能評価では，シミュレーションと確率モデル検査を利用したハイブリッドなアプローチにより，確率モデル検査だけを利用した場合では状態爆発を引き起こすような規模のシステムに対して性能評価を実現している．またシミュレーションのみの評価では性能を十分に保証することができないが，提案手法はモデル検査により網羅的に解析を行うため分散システムの性能保証に有用だと考えられる．

最後に，本論文では，実時間システムの時間的なQoS(Quality of Service)を時間オートマトンを用いて検査する手法を提案している．従来手法では解析に線形計画法を利用するため，閉路や階層的な構造を含むようなシステムには適用できなかった．しかし提案手法では時間オートマトンを用いてシステムをモデル化し検査を行うことでこの問題を解決し，適用クラスの拡大に貢献している．また段階的に検査を適用することで状態爆発の問題を回避している．

以上のように、本論文は実時間システムを対象としたモデル検査のスケーラビリティを向上し，システムの高信頼化技術発展に貢献すると考えられ，博士（情報科学）の学位論文として価値のあるものと認める．