論文審査の結果の要旨

氏名　山本光晴

システムが仕様を満たしていることを検証する方法論の1つであるモデル検査は高度に自動化された手法であり，これまでハードウェア検証などの分野で成功をおさめてきた．しかし，モデル検査は状態空間の網羅的探索を基本としているため，そのままでは無限の状態空間を扱うことができない．このため，無限の状態空間を抽象化して，有限個の抽象状態の上でモデル検査を行う抽象モデル検査が提案されているが，抽象モデル検査における探索空間のサイズの爆発が問題で，それを乗り越えて無限状態システム上の探索によって検証を実現し，それを最適化することに関する方法論が必要となっていた．

本論文は，まさしくこの抽象モデル検査における探索空間の縮小を目的とし，無限状態システム上の探索による検証とその最適化に関する研究を行ったものである．まず，抽象モデル検査のあるクラスを含む抽象到達可能性検査を提案し，定式化とその上での最適化を行っている．最適化手法としては，A*アルゴリズムが用いられている．次に，これを無限状態システムの例である時間を扱うシステムに応用している．そこでは最早A*アルゴリズムは自明でなく，本論文のアプローチによって始めてこの場合のA*アルゴリズムが得られ，その正当性が証明されている．また，証明検証系でこのような探索アルゴリズムや，その最適化アルゴリズムの正当性を形式的に検証する手法について考察している．

具体的には，まず実際に証明検証系HOLの上で，最短路問題やデータフロー解析などを含む基本的なグラフ探索アルゴリズムおよび最適化アルゴリズムの検証を行っている．ここで軸となるのがA*アルゴリズムである．この際，基本アルゴリズムと最適化アルゴリズムの検証を全く独立に行うのではなく，前者の検証に用いた証明を後者の検証に用いることが可能であることを示し，これを利用して労力の軽減を図っている．また，証明検証系による形式的証明において，基本アルゴリズムに関する証明から最適化アルゴリズムに関する証明を容易に得るための機構として，帰納的定義の発展を導入する．

次に抽象モデル検査のあるクラスを含む抽象到達可能性検査を提案し，定式化とその上での最適化を行っている．これは抽象モデル検査アルゴリズムのあるクラスの他，上で検証した基本的なグラフ探索アルゴリズムを包括する抽象的なアルゴリズムである．抽象的なアルゴリズムの上で正当性を議論し，さらに最適化アルゴリズムを定義することにより，様々な具体的アルゴリズムに対する最適化および正当性の証明を，本論文の提唱する統一的な方法で得ることが可能となっている．

最後に抽象到達可能性検査を無限状態システムの問題が取り組み，時間を扱う無

限状態システムに応用している．具体的には，実時間システムの代表例である時間オートマトンの拡張であるコスト付き時間オートマトンの最小コスト問題に対し，上記の最適化を適用している．また，時間を扱うシステムに関連して，時間オートマトンと時間ペトリネットの拡張となる時間付き多重集合書き換え系を導入し，その性質について述べる．このように無限状態システムを，まず有限の探索空間に限る理論を構築し，さらに探索を効率化することに成功している．

以上をまとめるに，本論文提出者は，実際の証明系で有限状態の探索をモデル化してその最適化を扱う理論を構築し，抽象モデル検査における探索空間の縮小を実現して，無限状態システム上の探索による検証とその最適化に関する研究について成果をあげた．これは，情報科学，特にモデル検証の分野に重要な貢献をなすものである．また本論文は，萩谷昌己氏，玉井哲雄氏，西崎真也氏，高橋孝一氏，Jean-Marie Cottin 氏との共著論文の内容を含むが，本論文提出者が主体となって研究遂行したものであると認められる．

以上により，審査員一同は，博士 (理学) の学位を授与するに十分値するものと判定した．