論文審査の結果の要旨

氏名　高橋孝一

システム状態の自動的な探索を基礎とするモデル検査法は，システムが正しく動作することを検証する技術の一つとして，ハードウェア検証の分野で広く利用されている。一方、セイフティ・クリティカルなソフトウエアシステムが増えるに従って，ソフトウェア検証の重要性はますます大きくなり、モデル検査法をソフトシステムの検証法として用いることが期待されている。しかし，ソフトウェアはハードウェアに比べて状態空間が巨大であり，ソフトウェア検証に対してモデル検査法を直接には適用できない場合が多い。従って，ソフトウェアのモデル検査を成功させるためには，状態空間を小さくする技術が不可欠である。

本論文は、ソフトウェア検証を行うための抽象化の技術を付加したモデル検査法，すなわち，抽象モデル検査法についての新しい知見を報告したもので、全体は１０章より構成されている。はじめの２章においてソフトウエア検証の重要性とモデル検査法の発展等を述べ，終章の第１０章では、結語と将来の研究方向を述べている。

第３章では，モデル検査法における抽象化の有効性を調べるために，実用性においても重要であり、かつアルゴリズムの正しさがわかりにくい，並行ごみ集めのアルゴリズムをとりあげ、それにモデル検証法を適用し問題点を検討している。この結果、抽象モデル検査における二つの重要な課題を明らかにしている。一つは，抽象化によって元のアルゴリズムの性質が失われないこと保証するという課題であり、今ひとつは、問題に応じて適切な抽象化をどのように構成するかという課題である。

第４章では，上の第一の課題に答えるもので、抽象モデル検査の理論的基礎を与えている。ここでは、プログラム意味論の分野で研究されていた詳細化の理論を適用することによって，モデル検査と抽象化の関係を理論的に解明している。

第５章は、第３章で述べた二番目の課題の一つの答えを与えている。並行ごみ集めアルゴリズムを検証するケーススタディでは，ヒープの状態を抽象化する必要がある。ヒープは複雑なリンク構造をしており抽象化の可能性も無限にあるため，ヒープの抽象化をどのように定義すべきか自明ではない。本章では、リンク構造を抽象化するための一般的な技術を開発し、正則表現を用いることにより，並行ごみ集めアルゴリズムの抽象モデル検査に用いた抽象化を一般化している。

第６章では，アルゴリズムを自動合成することを目標に，モデル検査を用いてアルゴリズムの変種を探索する方法を提案している。

第７章では，アルゴリズムの探索の効率を上げるために，シンボリックなモデル検査法をアルゴリズムの集合に適用している。この方法を用いることにより，モデル検査の一回の実行でアルゴリズムの集合を探索することが可能となる。さらに探索空間を小さくするため，この方法に抽象化技術を適用している。

最後の２章においては、抽象モデル検査法の全プロセスの正しさを形式的に証明することを目指す研究について述べている。第８章では，並行ごみ集めに対する抽象モデル検査で用いられた抽象化の正しさを、形式的に証明している。形式的証明は，HOL と呼ばれる証明支援系の上で開発された。

第９章では，第８章でもちいた HOL 証明支援系のための環境に関する研究について述べており、 "proving as editing paradigm"と呼ぶ考えを提案している。この考えは，第８章での形式的証明に際して実際に活用されたものである。また，プログラム意味論の分野で多く使われる可換図をそのまま扱うことのできるグラフィカル・ユーザ・インタフェースについても述べている。

以上要するに、本論文は、ソフトウエアやアルゴリズムの正しさを検証する手段として、モデル検証法を用いる際に大きな問題となっていた状態数の爆発的増加を、抽象化の技法を援用することにより軽減する方法を提案し、それを発展させたもので、理学上の貢献が大と言える。なお、本論文の第３、５，６，７，９章は萩谷昌巳氏と、また第４、９章は木下佳樹氏との共同研究であるが、論文提出者が主体となった研究であり、本人の貢献は十分であると考えられる。　よって、本論文は理学博士を与えるに十分な内容を有すると判定した。