別紙 2

論文審査の結果の要旨

論文提出者氏名　熊澤 努

情報システムが現代社会の基盤を形成していることは今さら言うまでもないが，そのような情報システムの運用中に不具合が発生し，それが大きな社会的・経済的損失を引き起こす事例は枚挙に遑がない．したがって，情報システムの高信頼性を確保することは，IT 化社会における最重要課題の一つといえる．

ソフトウェアを核とするシステムの信頼性を高める開発方法として注目を集め，広く産業界でも実践が進められている方法に，「モデル駆動開発」がある．これはシステムに求められる要求を分析し，それに基づいて要求仕様を決定する段階で，構築すべきシステムのモデルを作成し，そのモデルを系統的な方法で設計モデルに変換し，さらに実装レベルのシステムにまで変換していく，という方法論である．この手法の成否は，初めに作成する要求モデルが，いかに正確でかつ適切であるかにかかっている．

本研究が対象とするのは，そのようなモデルの正当性，適切性を検証するための「モデル検査」技術である．モデル検査は論理回路設計や通信プロトコル設計に使われてきたが，より複雑な構造を持つ一般のソフトウェアに適用する研究や実践が活発に行われるようになったのは比較的新しく，この 10 年ほどのことである．モデル検査は対象とするモデルが論理式として与えられた性質(仕様)を満たすか否かを，自動的に検証するものである．検証に失敗した場合は反例が示されることがこの技術の特徴であるが，技術者にとっては提示された反例をどう解釈し，モデルをどう修正すべきかの判断が通常困難である．本研究はこの問題に取り組み，反例からモデルの誤りを特定し，モデルを修正する方法と，その作業を支援するツールを開発したものであり，学術的に高い価値が認められるとともに，実際的な意義も大きく，優れた研究成果として評価できる．

本論文は 6 章で構成されている．

第 1 章では上に述べたような研究背景と目的，その目的達成のために克服すべき課題が説明される．続く第 2 章では，モデル検査の現状技術が解説され，次章以降の研究内容を説明するための基盤を与えるとともに，既存の技術の何が問題であるかが検討される．

第 3 章では，本研究の主要な成果の一つである，反例に基づくモデル修正法が提案される．その手法は，入力として分析対象のモデルとモデル検査の結果として得られた反例，および検証に成功している性質集合が与えられたとして，反例が満たせなかった性質を満たすように修正されたモデルを，半自動的に求めるものである．手法を支援するツールが実装され，それを 3 つの事例に対して適用した結果が報告されている．事例の分析は詳細で，提案された手法の有効性について説得力をもつ．

第 4 章と第 5 章では，反例からモデル修正を行う際に必要となる誤りの特定方法について，2 つの独立した，しかし共通する技術に基づいた手法がそれぞれ提案される．第 4 章の

手法は簡略版であり，場合によっては第 5 章の手法で検出される誤りを見逃すことがありうるが，効率がよい．第 5 章の方法は，平均的には第 4 章の方法より計算時間を要するが，より正確な検出手法になっている．前者は LLL-F と名づけられてツールが開発されており，後者は LLL-S と名づけられてやはりツールが開発されている．いずれも 7 つのシステムを対象とした事例研究がなされ，求められた誤りの有効性，実行性能，などが評価分析されている．すなわち，新規性の高い手法を提案しただけでなく，きちんと実装し，実証的な評価を綿密に行っている点が，この 2 つの章で報告されている研究の大きな特徴である．

最後に第 6 章で，全体のまとめと今後の課題が述べられている．

このように，本研究は情報システムの信頼性確保という重要な課題に対して，精緻な手法の提案，実装と評価を正統的な方法で成し遂げたものとして，大きな学術的貢献があると認められる．

よって，本論文は博士(学術)の学位論文として相応しいものであると審査委員会は認め，合格と判定する．