氏名	横川智教（よこがわともゆき）
博士の専攻分野の名称	博士（工学）
学位記番号	第 18815 号
学位授与年月日	平成16年3月25日
学位授与の要件	学位規則第4条第1項該当 基礎工学研究科情報数理系専攻
学位論文名	Formal Verification for Dependable Systems by Model Checking （モデル検査手法によるディペンダブルシステムの形式的検証に関する研究）
論文審査委員	（主査） 教授 菊野 亨 （副査） 教授 井上 克郎　教授 増澤 利光

論文内容の要旨

近年、システムの信頼性に対する要求はますます高まっており、システムを形式的に検証することが求められている。形式的検証のための手法は大きく定理証明とモデル検査の２つに分類される。定理証明は従来の形式的検証の主流であった手法であるが、多大な時間を要する手法で自動化もできず、実際に適用することは困難である。それに対してモデル検査は、対象は有限状態システムに限定されるものの、完全自動化が可能であるため非常に有効な手法である。本論文では、モデル検査を用いて(1)システムの耐故障性の検証と(2)一般電話システムにおける機能競合の検出という２つの問題を解く枠組みを示す。

まず、モデル検査を用いてシステムの耐故障性を検証する手法を提案する。ツールとしては記号モデル検査ツールSMV を用いる。本手法では、システムがガード付きコマンドに基づいてモデル化されていると仮定し、そのモデルからSMV の入力言語へ変換を行うことでSMV による耐故障性の自動検証を実現する。

同様に記号モデル検査を用いて電話システムにおける機能競合を検出する手法を示す。機能競合とは、複数の機能を同時に導入することで互いが干渉し、システムが意図しない動作を行ってしまう状況である。ここでは、STR と呼ばれるモデルに基づく機能記述を対象とし、そこからSMV 言語への変換を行うことで機能競合の検出を行う。

次に、限定モデル検査を用いて機能競合の検出を行う手法を提案する。限定モデル検査とは、検出問題を論理式の充足可能性判定問題へと帰着して解く手法である。従来の限定モデル検査では、電話システムのような非同期システムを対象とする場合、論理式のサイズが大きくなるため充足可能性の判定に時間がかかり、検証が困難となるという問題がある。これを解決するため新たな論理式の生成法を提案する。この生成法を用いることにより論理式のサイズが小さくなり、短い時間で検証を行うことが可能となる。提案法を用いることにより、他のモデル検査手法では１時間以上要していた問題を数秒程度で解くなどの大幅な改善が見られた。

論文審査の結果の要旨

ほとんどの社会システムが情報システムとして開発される傾向にあり、情報システムの信頼性に対する要求はますます高くなってきている。それに伴い、情報システムを形式的に検証することが求められている。一般に形式的検証の手法は定理証明とモデル検査に分けられる。定理証明は対象を限定しないが、多大な時間と労力を要するため実際の問題に適用することは困難である。一方、モデル検査は対象を有限状態システムに限定するが、完全自動化が可能であり非常に有効な手法である。モデル検査の実用化を目指して限定モデル検査が提案され、検証を充足可能性判定問題に帰着させて解いている。本論文の成果は次のように要約される。

(1)モデル検査を用いた情報システム検証の環境整備……検証にモデル検査ツール SMV を用いることを前提にして、モデル化されたシステム記述から SMV の入力言語（SMV 言語と呼ぶ）への変換手法を与えた。対象としてシステムの耐故障性の検証と機能競合の検出に注目している。まず耐故障性については、ガード付きコマンドでモデル化されていると仮定し、モデル記述から SMV 言語への変換を行っている。次に、機能競合の検出については、STR モデルに基づく機能記述が与えられるとして、SMV 言語への変換を行っている。評価実験の結果、ある典型的なシステムの例では直接求めた SMV 言語の記述には約 11000 トークンを要するのに対し、提案する変換によると約 2000 トークンで済んでいる。

(2)機能競合に対する限定モデル検査を用いた検出手法の提案……対象として機能競合の検出を選び、限定モデル検査の適用による高速化を目指す。非同期システムを対象とする場合、従来の限定モデル検査では式のサイズが大きくなるため判定に多くの時間がかかっていた。これを解決するためにシステムの動作を反映した論理式の生成法を新しく提案している。これにより式のサイズを大幅に削減することが可能になり、例えば、従来手法で１時間以上を要していたものを数秒程度で解けるようにしている。

以上のように、本論文はモデル検査手法を用いた情報システムの形式的検証に関して重要な成果を示しており、情報科学、特にディペンダブルシステムの設計に関する理論分野に貢献するところが大きい。よって本論文を博士（工学）の学位論文として価値のあるものと認める。