氏　　名	橋本　祐介
学位（専攻分野）	博士（情報学）
学位記番号	総研大甲第1514号
学位授与の日付	平成２４年３月２３日
学位授与の要件	複合科学研究科　情報学専攻 学位規則第６条第１項該当
学位論文題目	有界モデル検査を用いた逐次Ｃプログラムのモジュラー検証に関する研究
論文審査委員	主　査　教授　中島　震 准教授　細部　博史 助教　日高　宗一郎 教授　劉　少英　法政大学 准教授　岡野　浩三　大阪大学

論文内容の要旨

近年，身の回りの消費者向け製品や社会基盤システムでは，多くの機能がソフトウェアで実現されている．製品やシステムの障害が社会的関心事となり，ソフトウェアにも高い品質が求められている．産業界ではソフトウェアの品質確保をプログラム・テスティングで行っており，開発期間の半分以上を費やすこともある．ソフトウェア品質向上の新しい技術が求められている．

自動検証の技術にロジック・モデル検査の方法がある．有限状態遷移系として表現された検証対象と時相論理で表した検証性質を与えると，有限状態空間上の実行可能な全経路を網羅探索して，検証性質が満たされることを調べる．モデル検査には，「状態爆発」と呼ばれる，検証対象の規模に関して指数的に計算資源を消費するスケーラビリティの問題がある．有界モデル検査（BMC）は，探索範囲を限定して状態爆発を緩和し，効率的に不具合を発見する手法である．プログラムを対象とするソフトウェアモデル検査は，プログラムを有限状態遷移系に変換してモデル検査を行う．自動検証かつ網羅性が高いことから，産業界に導入しやすい品質向上手段といえる．しかし，実用的なプログラムでは BMC でも状態爆発が起こる．従来のプログラム・テスティングとの関係も明らかでない．ソフトウェアモデル検査の実用化では，これらの問題を解決する必要がある．

プログラム検証の考え方にモジュラー検証がある．C プログラムの場合，関数に事前・事後条件を，大域変数に不変条件を付記し，事前・不変条件を満たす状態から関数を実行し，実行後の状態が事後・不変条件を満たすことを静的に調べる．個々の関数を検証単位とするので，大規模なプログラムも扱える．しかし，関数に閉じて検証するので，コールシーケンスに関わる情報の不足から，不具合の見逃しや誤警告が起こりうる．

本研究では，逐次 C プログラムの新しい品質向上手段として，BMC とモジュラー検証を組み合わせたソフトウェアモデル検査技術を提案する．モジュラー検証の導入により BMC のスケーラビリティを向上する．この BMC を用いたモジュラー検証を本研究の基本的な技術として，さらにモジュラー検証の課題と BMC の課題についてそれぞれ解決方法を提案し，その有効性を実験により確認する．

BMC を用いたモジュラー検証では，事前・事後・不変条件を，assert や assume といった BMC の検証プリミティブに変換して対象プログラムに埋め込む．そして，事前・不変条件を満たす初期状態から到達可能な状態が事後・不変条件を満たすことを，BMC の方法で調べる．産業界の製品プログラムを用いた実験を行い，別途実施した単体テストで見つかった不具合を再発見することにより提案方法の基本的な有効性を確認した．

C プログラムでは，モジュールへの再入や関数ポインタを用いた間接呼び出しといった従来の静的なモジュラー検証では不具合を見逃す状況が発生する．特定の機能を実現する関数の集まりをモジュールと呼ぶとき，あるモジュールから呼ばれたモジュールが，呼び出し元モジュールを呼び返すことを，モジュール再入と呼ぶ．モジュール再入はコールバック型プログラムでは頻繁に起こる．再入箇所で不変条件違反が起きる場合に，関数を検証単位とするモジュラー検証では不具合を見逃す．本研究では，ファイルをモジュールとみなし，あるファイルに定義された不変条件をそのファイルに限定して検証するための記

法と，ファイル限定の不変条件から検証プリミティブへの変換方法を考案した．これを用いて，検証単位をコールシーケンスに拡張する BMC のインライン展開機能と組み合わせた検証方法を提案する．提案方法の実験を行い，モジュール再入箇所において，ファイル限定不変条件への違反を精度良く発見できることを示した．

関数ポインタを用いた間接呼出しでは，実際に呼ばれる関数は，そのアドレスを関数ポインタに実行時代入することで決まるので，静的に特定することが難しい．また，間接呼び出し側と実際に呼ばれる側が独立に開発されることから，前者の検査を行う際に後者のコードや事前・事後条件を利用できないことが多い．本研究では，関数ポインタ変数に事前・事後条件を定義する記法を導入したモジュラー検証と，関数ポインタと実際に呼ばれる関数の置換可能性検査との 2 段階からなる検証方法を提案する．関数ポインタと実際に呼ばれる関数の置換可能性検査には，オブジェクト指向プログラミングにおけるスーパー・サブタイプの置換可能性の考え方を応用した．オープンソースの OS である MINIX を用いて提案方法の実験を行い，関数ポインタの事前・事後条件によって誤警告を減少できることを確認し，間接呼び出しに関わる未発見バグの検出に成功した．

BMC は，プログラムを有限状態遷移系に変換する際に，抽象化を行わず，精度の高い検証を行う．しかし，変換時の過小近似によって，有限状態空間上の経路が少なくなり，元のプログラムに存在する不具合を見逃すことがある．そこで探索しない過小近似箇所を見つけて，別の手段で検査する必要がある．本研究では，BMC の過小近似箇所を自動検知する方法を考案し，検知した場合に，事前・事後条件からテストケースを自動生成して，単体テストで補う方法を提案する．過小近似検知の網羅度と単体テスト実行の網羅度は，産業界で高信頼ソフトウェアのテスティングに用いる MCDC 基準にしたがって測定する．MINIX を用いて提案方法の実験を行い，BMC の過小近似箇所を MCDC 基準で検知できることと，BMC と自動生成した少数のテストケースによる単体テストを合わせて MCDC 基準を 100%達成できることを示した．

プログラムの事前・事後条件は入力データと期待結果と見なせるので，事前・事後条件の定義は単体テストの計画に相当する．また，BMC を用いたモジュラー検証は，単体テスト実施の自動化を実現する．さらに，単体テストと共通のカバレッジ基準を用いた BMC の過小近似検知と，BMC を事前・事後条件から生成したテストケースによる単体テストで補完する方法は，従来の単体テスト評価に相当する．本研究の提案方法は全体として，従来の単体テスト作業（計画・実施・評価）を効率化する．形式検証技術の産業界への移転を容易にする方法といえる．

博士論文の審査結果の要旨

本博士論文は，プログラムの品質確保を目的とした自動検査の新しい技術確立を目的としている．産業界では，プログラムの品質は膨大なテスティング作業によって確保しており，開発期間の半分以上を費やしている．形式検証技術に基礎を置くプログラム自動検証の研究が進んできたが，検査可能なプログラム規模が限定されること，現状のテスティング技術との関係が明らかでないこと，といった実用化への障壁があった．本研究は，自動検証の方法である有界モデル検査をもとに，プログラム単体テストを補完する新しい方法を提案し，その有効性を適用実験によって確認するものである．

本博士論文は，全７章からなる．第１章では，産業界で実施しているプログラム品質確保技術の状況を述べ，本研究の着眼点を整理する．自動検証の方法による検査結果とプログラム・テスティングによる結果の関係を明らかにすることが，自動検証技術を産業界で実用化する鍵となることを論じている．

第２章では，背景となる技術として２つの方法を説明する．自動検証の代表的な方法であるロジック・モデル検査では検証対象の大規模化に起因する「状態爆発の問題」を解決しなければならない．逐次プログラムを検査する方法として有界モデル検査（BMC と略す）が提案されたが，実用的なＣプログラムでは BMC でも状態爆発が起こる．一方，手続きや関数などのプログラム要素に検証対象を限定するモジュラー検証の考え方が提案されている．状態爆発の問題が生じない反面，検証の単位を限定することによる情報不足から不具合を見逃すことが問題となっていた．

第３章では，BMC とモジュラー検証を組み合わせる新しい自動検証の方法を提案する．具体的には，Ｃプログラム関数の機能仕様を事前・事後条件で，また参照するデータに関わる不変条件で表す方法（DbC 仕様と呼ぶ）を導入し，BMC の検査プリミティブに変換する方法を整理した．これによって，ライブラリ関数などのようにソースプログラムが入手できない場合でも自動検査を可能とした．産業界で開発されたプログラムを対象として，別途単体テストによって発見された不具合を再発見できたことで，本提案方式の基本的な有効性を確認した．

第４章では，モジュラー検証で問題となる「モジュール再入」に起因する誤りの見過ごしを抑止する方法を提案する．これは「コールバック関数」を用いるプログラミングで生じることが知られている．本研究では，第３章で導入した検査プリミティブの生成方法を工夫して BMC を適用することによって，この問題が解決できることを示した．モジュラー検証と BMC を組み合わせることの効果といえる．

第５章では，第３章で導入した基本的な DbC 仕様を拡張して，Ｃプログラムで頻繁に用いる関数ポインタを取り扱う方法を提案する．関数ポインタ変数を用いて関数起動しているプログラムに対して，関数ポインタ変数を具体的な関数で置き換えることが可能か否かを検査する「置き換え可能性規則」を導入するアイデアである．オープンソースの O/S である MINIX に提案方法を適用し，公開されている MINIX プログラムの未発見バグを見つけることに成功した．

第６章では，BMC の一般的な限界について問題分析を行い，テストデータ自動生成によって BMC を補う新しい方法を提案する．BMC では検査対象Ｃプログラムから有限状

態遷移系を得る際に行う近似変換によって，検査対象のプログラム箇所を見逃すという過小近似が生じる．本研究では，BMC を応用して過小近似の有無を自動検出する方法と，過小近似によって見逃すプログラム箇所をピンポイント的に検査するテスト入力データを DbC 仕様から自動生成する方法を考案した．特に，過小近似箇所の検出と自動生成テストデータによる検査に共通する基準として，産業界で用いている MCDC 基準を採用した．MINIX を用いた適用実験によって，BMC による自動検証と少数のテストケース実行を組み合わせることで，期待される検査網羅度が達成可能なことを示した．この方法によって，MCDC 基準に基づく検査網羅度の達成という観点から，BMC を用いる自動検証の技術とプログラム・テスティング技術の関係を明らかにすることに成功した．

第７章では，まとめとして，本研究成果を，産業界のプログラム品質確保に実適用する具体的な見通しを論じている．

本審査委員会では，上記の研究成果は，自動検証技術を産業界での実践に橋渡しするものであり，ソフトウェア研究の学位として相応しい内容を持つと判断した．また，第３章から第５章の研究成果については２件の国際学会発表ならびに１件の学術論文誌掲載，第６章については１件の学術論文誌掲載ならびに国内シンポジウム口頭発表での最優秀論文賞受賞がある．これらから，本博士論文の成果が，当該技術の研究分野で高く評価されていることがわかる．

以上，発表及び質疑応答と博士論文原稿，研究成果の内容に基づき，審査委員会全員によって審査した結果，博士論文として十分な水準にあると認められた．