氏名	森岡澄夫（もりおかすみお）
博士の専攻分野の名称	博士（工学）
学位記番号	第 13222 号
学位授与年月日	平成9年3月25日
学位授与の要件	学位規則第4条第1項該当 基礎工学研究科物理系専攻
学位論文名	**プレスブルガー文真偽判定手続きを用いたプログラム正当性証明**
論文審査委員	（主査） 教授 谷口 健一 （副査） 教授 西川 清史　教授 井上 克郎

論文内容の要旨

本論文は，プログラムの正当性証明を，プレスブルガー文真偽判定手続きを用いて半自動で行う方法に関する研究をまとめたものである。従来から広く用いられているテスト手法では，要求仕様に書かれた入出力関係をプログラムが満たすこと（正当性）の保証が難しい。近年，形式的手法を用いて正当性を論理的に証明する手法（形式的検証）が注目されているが，一般に証明作業に手間がかかることが問題となっている。そこでプログラムの正当性を代数的手法を用いて証明する作業の効率化を目指し，以下を行った。

第一に，プログラムの仕様等の記述スタイルを制限し，そのもとで正当性証明を半自動で行える証明法を考案した。そのスタイルの制限の概略は「集合（配列）の各要素（または各要素間）に成り立つべき性質を一つの基本述語で表す」というものである。考案した証明法は次のようなものである。まずFloyd流の帰納表明法で用いる不変表明，および，プレスブルガー文で直接扱えない基本述語Pや基本関数Fに関する補題（補助定理）を検証者が考案する。ここで，プレスブルガー文とは整数の加減・比較演算と論理演算のみを持つ一階述語論理式のことであり，その真偽は決定可能である。次に，帰納法の各段階ごと，「PおよびFを自由解釈としたうえで，導入した補題のもとで不変表明等が成り立つ」ことを示す。このことは，上述のスタイル制限のもとでは，$\forall$で束縛された冠頭形のプレスブルガー文に対する真偽判定手続きにより直接示せる。

第二に，上述の冠頭形をしたプレスブルガー文の真偽判定を高速化するための方法を考案した。プレスブルガー文中の不等式から定まる幾つかの値を代入して変数を一つずつ消去していくCooper・直井の判定法に，(i)変数消去の度に，冗長な不等式をなるべく除去する，(ii)構文木の根に近い位置に出現する変数から先に消去する，(iii)変数が数個程度に減少したとき，実数上の線形計画法を利用して式の充足不能性を直接調べる，等のヒューリスティクスを追加した。それらのヒューリスティクスのもとで，実際の検証で現れるような多くのプレスブルガー文の真偽が数秒程度で判定できることを確認した。

第三に，マックスソートプログラムや酒屋在庫管理プログラムを例題に検証実験を行った。明らかに正しいと分かる単純な補題だけを用いて証明ができるよう，簡単な意味の基本述語・関数だけを用いて各プログラムの仕様を記述した。いずれのプログラムについても，どのような補題および不変表明を用いるかの検討に十数時間を要し，用いた補題は十数個，証明作業にかかった期間は約2日，証明に要した全CPU時間は数分であった。

論文審査の結果の要旨

プログラムの正当性の証明作業をなるべく自動化することが重要である。本論文では，仕様記述のスタイルを制限して，Floyd流の証明法における帰納法の各段階の証明を自動で行えるような，新しい証明方法を提案し，それに基づいた検証支援系を構成している。

提案方法は，帰納法の段階ごと，それぞれ次の方法で証明を行うものである。その段階に対応するプログラム命令列Cに対し，「Cの事後条件（不変表明等）が，Cの事前条件，Cの動作内容の定義，および，検証者が与えた述語・関数に関する補題のもとで成り立つ」ことを，補題等を含めて一つの論理式（検証条件）として表し，次に，その検証条件が成り立つことを，整数の加減・比較演算と論理演算のみを持つ一階述語論理式（プレスブルガー文）のうち，全称記号$\forall$だけで束縛された冠頭形のものに対する真偽判定手続きを用いて示す。

提案手法の利点は，検証条件の成立を自動で判定でき，従来のように検証者が対話的に論理式の変形等を行う必要がないことである。一方，上述の真偽判定手続きを用いて検証が行えるよう，「集合（配列）aの各要素（または各要素間）にある性質Pが成り立っているということを，述語Pと全称記号$\forall$を用いずに，aを引数とする一つの述語で表す」ように仕様等の記述スタイルを制限しているため，以下のような問題点が考えられる。(1)証明において述語に関する補題が多く必要となり，判定すべき論理式が大きくなるので，真偽判定に時間がかかること，(2)証明において補題は正しいものと仮定するので，正しいことが明らかな補題だけを用いねばならないが，そのような簡単な補題だけでは証明ができないこと，および，(3)証明を成功に導くために十分な補題を発見するまでに，何回も証明失敗を繰り返し，証明作業に手間がかかること。しかし，(1)に対しては，判定高速化に有効な幾つかのヒューリスティクスを新たに考案し，実際の証明で現れるようなかなり大きなプレスブルガー文の真偽判定を，数秒程度の短時間で行えるように工夫している。また，(2)，(3)に対しては，マックスソートプログラムや酒屋在庫管理プログラムなど典型的と思われる例題の検証実験を行って，簡単な補題を組み合わせるだけで証明が行え，かつ，証明作業全体にかかる時間が従来と比べてかなり短縮されることを実証している。

以上の研究成果は，ソフトウェアの形式的検証技術の進展に貢献しており，本論文は博士（工学）論文として価値あるものと認める。