様式 C-19

科学研究費補助金研究成果報告書

平成２１年　５月　２７日現在

研究種目：若手研究（Ｂ）
研究期間：2006～2008
課題番号：１８７０００１８
研究課題名（和文）　対話的定理証明によるソフトウェアの精密な検証

研究課題名（英文）　Verification of Software with Interactive Theorem Proving

研究代表者
南出 靖彦（MINAMIDE YASUHIKO）
筑波大学・大学院システム情報工学研究科・准教授
研究者番号：５０２５２５３１

研究成果の概要：
対話的定理証明によるソフトウェアの検証について、様々な角度から研究を行い、事例研究を通じ、小規模なソフトウェアやソフトウェアの核となる部分については、対話的定理証明による検証が可能であることを示した。特に、本研究の代表者が開発しているウェブプログラムの検証ツール PHP 文字列解析器について、その核となるアルゴリズムの定式化・検証を行い、正当性を検証済みのプログラムを得ることに成功した。

交付額

（金額単位：円）

	直接経費	間接経費	合　計
2006 年度	1,100,000	0	1,100,000
2007 年度	1,000,000	0	1,000,000
2008 年度	1,000,000	300,000	1,300,000
年度			
年度			
総　計	3,100,000	300,000	3,400,000

研究分野：情報科学
科研費の分科・細目：情報学・ソフトウェア
キーワード：ソフトウェア検証, 定理証明系, ホーア論理

１．研究開始当初の背景

現代の社会では、ソフトウェアが至る所で使われており、その障害は深刻な影響をもたらす。そのためソフトウェアの安全性や正しさを検証することが重要な課題になっている。ソフトウェアを検証するアプローチとしては、モデル検査などの自動的な解析による検査と対話的な証明を行うアプローチが考えられる。前者は、ロックの安全性などのソフトウェアが満たすべき部分的性質の検証に非常に有効であり、近年、盛んに研究が行われ、デバイスドライバの検査などで実用になりつつある。しかし、ソフトウェアの正しさなど、より詳細、精密な性質の検証は、モデル検査では不可能である。

もう一つのアプローチが、定理証明系（証明支援系）を用いて対話的証明を行うアプローチである。このアプローチで、C言語など通常のプログラミング言語で書かれたプログラムを検証するためには、検証条件生成ツールと定理証明系の組み合わせを用いる。検証条件生成ツールは、仕様を表明として付加したプログラムに対して、プログラムが仕様を満たすための条件（検証条件）を生成する。生成された検証条件を、定理証明系を用いて対話的に証明すれば、プログラムの正しさを証明

できる。このような検証条件生成ツールとして、C言語のためのCaduceusやJavaのためのKrakatoaなどが開発されている。
これまでに、これらの検証条件生成ツールが、基本的なアルゴリズムの実装や小規模なソフトウェアの検証に用いられて、成功している。しかし、規模の大きなソフトウェアに関しては、証明の人的コストや、証明のスケーラビリティの問題があり、実用にはまだ隔たりがあるのが現状である。

２．研究の目的
対話的定理証明によりソフトウェアの性質を精密に検証し、信頼性の高いソフトウェアを構築する手法を確立することを目指す。具体的には、以下の研究を行う。
(1)　対話的定理証明による検証の事例研究として、基本アルゴリズムの検証を行う。この事例研究により対話的定理証明によるソフトウェア検証の問題点を明らかにする。定理証明系上で定式化したアルゴリズムの検証及びC言語による実装の検証の二つのレベルで行い、それぞれの弱点、利点を明らかにする。また、抽象度の高い検証から実装の検証を導く方法を研究する。
(2)　ソフトウェア検証のアプローチとして、ソフトウェアの核となる部分を定理証明系上でモデル化、検証し、モデル上のプログラムから、実際のソフトウェアの一部として利用できるプログラムを生成するアプローチについて研究する。このアプローチでは、実際のプログラミング言語上の実装に比べて、抽象度が高い検証が可能になるが、効率的なプログラムを得る手法が確立されておらず、研究課題となる。

３．研究の方法
対話的定理証明によるソフトウェアの検証の様々なアプローチについて、事例研究を通じ、その問題点を明らかにする。また、ソフトウェア検証の基礎となるアルゴリズムの検証、プログラミング言語の意味論の定理証明系による定式化の研究を行いソフトウェア検証の基礎とする。本研究では、対話的定理証明系として、Isabelle/HOLを用いる。
(1)　ソフトウェア検証の基礎となるプログラミング言語の意味論の研究を行う。特に、プログラミング言語を定理証明系上で定式化する場合に問題となる束縛変数の扱いについて重点的に研究を行う。また、ウェブソフトウェアの検証に向けて、ウェブプログラミング言語の意味論やウェブプログラムの実行環境の定式化の研究を行う。
(2)　ソフトウェア検証の基礎となるアルゴリズム検証の研究を行う。本研究では、特に、定理証明系上での定式化が難しいグラフアルゴリズムについて、研究を行う。グラフアルゴリズムの基礎となる深さ優先探索の精密な検証からはじめ、最短経路アルゴリズムの検証に発展させる。
(3)　検証条件生成ツールCaduceusと定理証明系Isabelle/HOLを用いたC言語プログラムの検証の研究を行う。基本的なアルゴリズムのC言語による実装を検証する事例研究からはじめ、より規模の大きいプログラムの検証を行う。
(4)　Isabelle/HOLなどの定理証明系では、定理証明系上で関数プログラムを記述することができる。Isabelle/HOLでは、この機能を用いて記述したプログラムを、Objective CamlやHaskellなどに変換することができ、通常のプログラムとして実行可能である。この手法により、実用的なレベルの実行効率を持つプログラム構築する手法を明らかにする。

４．研究成果
対話的定理証明によるソフトウェアの検証について、様々な角度から研究を行い、事例研究を通じ、小規模なソフトウェアやソフトウェアの核となる部分については、対話的定理証明による検証が可能であることを示した。

(1)　検証条件生成ツールと対話的定理証明を用いたＣプログラムの検証について以下の研究成果を得た。
①　Cプログラムに対する検証条件生成ツールCaduceusを定理証明系Isabelleの最新のバージョンに対応させる実装を行った。これにより最新のバージョンのIsabelleに導入された機能を用いた効率的な検証が可能になった。
②　KMP法による文字列照合のＣ言語による実装の正しさを検証した。検証には、検証条件生成ツールCaduceusを用いた。ループ不変条件を決定するには、プログラムの精密な分析が必要であったが、検証条件の証明自体は、比較的容易であった。また、検証の過程でアルゴリズムの教科書に掲載されているC言語によるKMP法の実装の誤りを発見することができた。

(2)　アルゴリズム検証については、グラフ探索アルゴリズムについて重点的に研究を行い以下の研究成果を得た。
①　深さ優先探索の検証の精密化を行った。先行研究で既に深さ優先探索アルゴリズムの検証をIsabelle/HOLを用いて行っていたが、グラフ探索アルゴリズムを用いたプログラムの検証を進める上で、より精密な性質の検証が必要であることが分かった。そこで、深さ優先探索アルゴリズムの原理をより精密にとらえ、探索の各ステップが保存する性質を明らかにし、その検証を行った。

② 重み付きグラフに対して最短経路を求めるBellman-Fordアルゴリズムの形式化及び検証を行った。アルゴリズムの教科書では、重みとして実数など具体的な代数構造を仮定してアルゴリズムの形式化が行われる。一方、本研究では、必要最低限の性質を仮定し形式化を行った。代数的な構造としてどのような性質が必要かを、厳密な証明をすることで明確にすることができた。また、グラフの経路の形式化をリストの構造に対応するように行うことで、グラフアルゴリズムの形式化が扱いやすくなることが分かった。

(3) ソフトウェア検証の基礎としてプログラミング言語意味論とその検証の研究を行い以下の成果を得た。
① 関数型言語のコンパイラで用いられるCPS変換と呼ばれるプログラム変換の形式化と検証を行った。形式化と検証には、束縛変数に関する同値性を直接扱えるNominal Logicに基づく定理証明系Nominal Isabelleを用いた。CPS変換をNominal Isabelleで形式化する場合、変換が導入する新しい束縛変数の扱いが難しく、紙の上の証明をそのまま翻訳することができない。本研究では、必要となる補題を系統的に準備して証明を行うことで、定義や証明の主要な部分を自然な形で記述するができることを示した。
② ウェブソフトウェアの検証の基礎として、スクリプト言語PHPの操作的意味論の研究を行った。PHPは、値を代入するときにコピーを行う代入時コピー（Copy-on-Assignment）が基礎となっている。一方、実装には、書き込みの時にコピーを行うCopy-on-Writeが用いられている。本研究では、これら二つの評価戦略に対して、グラフ書き換えによる操作的意味論を与えた。また、操作的意味論の核となる部分を定理証明系Isabelle/HOLにより形式化し、基礎的な性質の証明を行った。

(4) 本研究の研究代表者が開発しているウェブプログラムの検証ツールPHP文字列解析器の核となるアルゴリズムの検証を行い、Isabelle/HOLの実行コード生成機能を用いて検証済みプログラムの生成を行った。PHP文字列解析器では、サーバサイドプログラムの性質を検査するために文脈自由言語に関するさまざまな判定アルゴリズムを用いている。本研究では、Isabelle/HOL上で文脈自由言語を形式化し、以下の三つの決定アルゴリズムの検証を行った。
① 文脈自由言語と正則言語の包含関係の決定アルゴリズム
② 与えられた文脈自由言語に属する語がすべてバランスが取れているか決定するアルゴリズム
③ 文脈自由言語と正則生垣言語の包含関係の決定アルゴリズム
これらのアルゴリズムに対して、Isabelleの実行コード生成機能により実行可能なプログラムを得た。PHP文字列解析に組み込み実験を行ったところ、得られたプログラムは、実用的にならないほど非効率的であることが分かった。この問題を解決するために、アルゴリズムの定式化を大きく変更することなく、より効率的プログラムを得ることができる手法を開発し、最終的には、実用的な実行効率をもつプログラムを得ることができた。

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計８件）

① A. Tozawa, M. Tatsubori, T. Onodera, Y. Minamide, Copy-on-Write in the PHP Language, In Proc. POPL: The Symposium on Principles of Programming Languages, pp. 200-212, 2009. 査読有

② Y. Minamide, Approximation of String Operations in the PHP String Analyzer, Proc. of Symbolic Computation in Software Science Austrian-Japanese Workshop, RISC Technical Report 08-08, pp. 137-147, 2008. 査読無

③ T. Nishiyama, Y. Minamide, A Translation from the HTML DTD into a Regular Hedge Grammar, In Proc. of the 13th International Conference on Implementation and Application of Automata, LNCS 5148, pp.122-131, 2008. 査読有

④ 松本宗太郎, 南出靖彦, 多相レコード型に基づくRubyプログラムの型推論, 情報処理学会論文誌:プログラミング, Vol.49, No. SIG 3, PRO 36, pages 39-54, 2008. 査読有

⑤ 南出靖彦, ソフトウェア解説：Cプログラムの検証ツール Caduceus, コンピュータソフトウェア, Vol. 24, No. 3, pp.15-19, 2007. 査読有

⑥ Y.Minamide, Verified Decision Procedures on Context-Free Grammars, In Proc. of the 20th International Conference on Theorem Proving in Higher Order Logics, LNCS 4732, pages

173-188, 2007.　査読有

⑦ A.Tozawa, Y. Minamide, Complexity Results on Balanced Context-Free Languages, In Proc. of the Tenth International Conference on Foundations of Software Science and Computation Structures, LNCS 4423, pages 346-360, Springer, 2007. 査読有

⑧ Y. Minamide, A. Tozawa, XML Validation for Context-Free Grammars, In Proceedings of the Fourth Asian Symposium on Programming Languages and Systems (APLAS), LNCS 4279, pages 357-373, Springer, 2006. 査読有

〔学会発表〕(計３件)

① 安田峰悠, 松本宗太郎, 南出靖彦, ブラウザにおけるJavaScript 実行のモデル化, 日本ソフトウェア科学会第 25 回大会, 2008 年 9 月 10 日, 筑波大学東京キャンパス

② 西山拓哉, 南出靖彦, 動的に生成されるHTML文書の妥当性検査, 日本ソフトウェア科学会第 25 回大会, 2008 年 9 月 10 日, 筑波大学東京キャンパス

③ 松本宗太郎, 南出靖彦, 多相型レコードに基づくRubyオブジェクトの型推論に関する考察, 日本ソフトウェア科学会第 23 回大会, 2006 年 9 月 15 日, 東京大学

〔その他〕
ホームページ等
http://www.score.cs.tsukuba.ac.jp/~minamide/verification.html

６．研究組織
(1)研究代表者
南出　靖彦 (MINAMIDE YASUHIKO)
筑波大学・大学院システム情報工学研究科・准教授
研究者番号：　５０２５２５３１