様式 C-7-2

自己評価報告書

平成２１年５月１日現在

研究種目：基盤研究（Ｂ）
研究期間：2006～2009
課題番号：18300008
研究課題名（和文）　証明スコアによる問題モデルの検証技術

研究課題名（英文）　Verification of Problem Models with Proof Scores

研究代表者
二木 厚吉 （FUTATSUGI Kokichi）
北陸先端科学技術大学院大学・情報科学研究科・教授
研究者番号： 50251971

研究分野： 総合領域
科研費の分科・細目： 情報学・ソフトウェア
キーワード： 仕様記述、仕様検証、システム検証、安全性、信頼性、形式手法、問題モデル

１．研究計画の概要

ドメイン仕様や要求仕様などの問題モデルの検証技術の実用化を目指し、証明スコア法に基づく対話型検証法の最重要の技術課題である帰納法と場合分けに関し以下の研究開発を行う。

(1) 多様な問題領域で有効な帰納法の開発: 証明スコア法による検証法の基本的な推論スキーマは、再帰的に定義されたデータ型やプロセス型に関する数学的帰納法である。すでに多くの応用領域において帰納法による検証事例を蓄積しているが、それらにおける帰納法は個々の問題ごとに個別的になる傾向がある。これを改善し、実用的な検証技術を開発するために、蓄積した事例における帰納法の適用法を分析・体系化することで、より汎用的な帰納法を開発する。

(2) 多様な問題領域で有効な場合分けの方法の開発： 証明スコア法による検証の要点は、問題モデルの定義(形式仕様)に基づきすべての可能な場合を洗い出し、それらをもれ無く記述し、その各々について論理的なチェックを行うコードを確実に実行することで、検証を完成することである。このような場合分けに基づく証明スコア法が、多くの問題モデルに対して有効であることを事例研究で確認しているが、場合分けは個々の問題ごとに個別的で煩瑣になることが多い。これを改善し実用的な検証技術を開発するために、多様な問題領域で有効な汎用的な場合分けの方法を開発する。

２．研究の進捗状況

色々な問題領域において形式仕様と証明スコアを開発し、それを分析することで、以下のような成果を得た。

(1) 帰納法については、データ型とプロセス型に共通な、形式仕様からの帰納スキーマの導出法を明らかにし、それに基づき帰納法による検証を行う証明スコアの作製法を整理体系化することで、多様な問題領域で有効な汎用的な帰納法を定式化した。

(2) 場合分けについては、形式仕様に現れる型構成子や命題に基づく場合分けの方法を明らかにし、それに基づき場合分けを行う証明スコアの作製法を整理体系化することで、多様な問題領域で有効な汎用的な場合分けの方法を定式化した。

(3) (1)(2)に基づき、(帰納法に基づく) 推論と探索を融合した検証法を体系化し、「証明スコア作成ツール」を設計し一部システム化した。ツールの設計と開発は、「人間と機械が各々の優れた能力を発揮しつつ協力して行う検証を支援する」という

方針に従い、場合分けを自動的に行う探索を支援する機能に焦点を絞って行った。

上記の研究開発を通じて、以下のような知見を、具体的な事例とともに得ることができた。

(1) 帰納法を用いた推論に基づく検証は、帰納スキーマの選択、帰納命題（帰納法で証明すべき命題）や補題の特定、などの検証すべき問題に関する深い理解を必要とするので、人間が証明スコアを作成しつつ対話的に行うのが適当である。
(2) 場合分けの中には、探索により自動化できシステムに支援させるのが適当であるようなものが存在する。
(3) 抽象化などにより、検証を自動化可能な網羅的な場合分けの探索に帰着させるためには、一般的には帰納法による推論が必要である。この部分は人間が証明スコアを作成しつつ対話的に行うのが適当である。

３．現在までの達成度

①当初の計画以上に進展している。

（理由）

当初計画していた、汎用的な帰納法と場合分けの技法は、帰納法と場合分けを行う証明スコアの作製法を体系化するという形で、開発できた。その成果の一部は日本ソフトウェア科学会の論文誌に６回に渡りチュートリアルという形で発表した。

方法論のツール化については、場合分けの自動化に役立つ検索ツールに焦点を絞り、システム化をほぼ終了した。

「目標とする命題の検証を、証明スコアの作成を通じて帰納法の推論を行うことで、自動化し得る検索に帰着させる」という方法論は、汎用的な帰納法と場合分けの技法の研究開発の中から生まれた、当初計画では想定していなかった重要な成果である。この成果は最終年度であるH21年度に一層の進展が期待できる。

以上に述べたごとく、本研究は当初の計画以上に進展している。

４．今後の研究の推進方策

証明スコア法による検証技術をより実用的なものとするために、以下のような研究を推進し本研究をより発展させる予定である。

(1) 形式仕様と証明スコアの正しさを半自動的にチェック・検証するシステムの開発。
(2) 推論と探索を組み合わせたより強力な検証技術の開発。

５．代表的な研究成果

（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21件、2006.4-2009.3）
（査読有21件、査読無0件）

① 二木厚吉, 緒方和博, 中村正樹：CafeOBJ 入門(1) - 形式手法とCafeOBJ, コンピュータソフトウェア(日本ソフトウェア科学会論文誌), 25(2)： 1-13, 2008.（査読有）
② Kokichi Futatsugi, Joseph A. Goguen and Kazuhiro Ogata: Verifying Design with Proof Scores, 1st VSTTE, LNCS 4171, Springer, pp.277-290, 2008.（査読有）
③ Masahiro Nakano, Kazuhiro Ogata, Masaki Nakamura and Kokichi Futatsugi: Creme: An Automatic Invariant Prover of Behavioral Specifications, International Journal of Software Engineering and Knowledge Engineering, Vol.17, No.6, pp.783-804, World Scientific, 2007.（査読有）
④ Kazuhiro Ogata and Kokichi Futatsugi: Modeling and verification of real-time systems based on equations, Science of Computer Programming, 66(2): 162-180, Elsevier, 2007.（査読有）

〔学会発表〕（計26件、2006.4-2009.3）
（査読有19件、査読無7件）

① Kokichi Futatsugi: Verifying Specifications with Proof Scores in CafeOBJ (invited keynote paper at ASE 2006, 20 September 2006, Tokyo), Proc. of 21st International Conference on Automated Software Engineering, IEEE, pp. 3-10, 2006.（査読無）

〔その他〕

以下のウェッブページを通じて、開発したシステムと例題、発表論文などを公開している。

http://www.ldl.jaist.ac.jp/cafeobj