様式 C-19

科学研究費補助金研究成果報告書

平成２２年４月１０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

研究成果の概要（和文）：「帰納法」と「場合分け」は、問題モデル（問題領域や応用領域におけるモデル）の証明スコアによる検証法の基本技術である。本研究では、多様な応用分野で有効な帰納法と場合分けについて以下の成果を得た。(1) 帰納法をデータ型・プロセス型の帰納的な構造に基づき定式化した。(2) 場合分けを構成子からの項の生成に基づき定式化した。(3) (1),(2)に基づき、汎用的な証明規則を定式化するとともに、推論と探索を融合した強力な検証法を開発した。

研究成果の概要（英文）：″Induction″ and ″case-splitting″ are fundamentals of verifications of problem models (models in problem or application domains) by proof scores. The following research achievements are gotten about induction and case-splitting which are effective in many areas. (1) Induction is formalized based on recursive structures of data or process types. (2) Case-splitting is formalized based on generations of terms from generators. (3) Based on (1) and (2), universal proof rules are formalized, and a powerful verification method which harmonize inference and search is developed.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2006 年度	2,900,000	870,000	3,770,000
2007 年度	4,100,000	1,230,000	5,330,000
2008 年度	4,100,000	1,230,000	5,330,000
2009 年度	4,100,000	1,230,000	5,330,000
年度			
総　計	15,200,000	4,560,000	19,760,000

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、形式手法、問題モデル、証明スコア、帰納法、場合分け

１．研究開始当初の背景

地球規模の情報ネットワークが最重要の社会基盤となったネットワーク情報社会においては、「新たな問題解決のためのシステム開発への要求が増大」していた。例えば，多くの中小企業・商店はネット上でのビジネスに積極的に乗り出し、自らの事業・商売を「ネット時代」にあわせて再編・改良しつつ、自らを他と差別化する新たなシステム開発に積極的に取り組んでいた。また、行政サービスの電子化の進展にともない、行政の現場でも新たなサービスを実現するシステム開

発が進展しつつあった。こうしたシステムは必然的に不特定多数のユーザに開かれたネットワークが基盤となるので、電子商取引システムなどが典型例であるように、その「安全性と信頼性を確保する技術」が重要であった。

安全性や信頼性を重要な要件として、新たな問題解決のためのシステム開発を進めるためには、問題モデル（問題領域や応用領域におけるモデル）を構築しそれを検証する技術が必要であった。問題モデル検証技術は、ソフトウェア工学分野における、要求技術、仕様技術、検証技術といったカテゴリに属するが、問題モデルの仕様を記述しそれを検証する技術は確立されていなかった。本研究は、研究代表者のグループが研究成果を蓄積してきた CafeOBJ 言語を用いた証明スコアによる検証法に基づき、問題モデルの検証技術の研究開発を目指したものであった。

２．研究の目的

問題モデルの検証には、具体的な問題領域や応用領域について各々の問題の特質を分析することが重要である。本研究では、研究代表者のグループが検証事例を蓄積している、鉄道信号システム、分散アルゴリズム、分散オブジェクト、実時間・ハイブリッドシステム、認証プロトコル、電子商取引プロトコル、ワークフローモデル、失敗木解析モデルなどの問題領域について、個々の結果を精密に分析することで、問題モデルの検証技術を研究開発することとした。具体的には、問題モデル検証技術の最重要の課題である「帰納法」と「場合分け」に焦点を絞り、以下の２つを研究の目的とした。

(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。

３．研究の方法

以下の２つの観点から各々の事例における証明スコアの作成法を分析することで、多様な問題領域で有効な「帰納法」と「場合分け」を明らかにする方法をとった。

(1) データ型とプロセス型： システムのモデルは一般には問題領域や解析すべき性質の種類に応じて多様ではあるが、外界とデータを交換しつつ状態を変化させて動作する状態遷移モデルは、ソフトウェア工学やシステム工学において有効な汎用モデルであり、それに基づくシステムの性質の解析や検証の実績も豊富である。CafeOBJ は代数仕様言語に分類される形式仕様言語であるが、状態などの動的なものの集まり(型(type)；代数仕様ではこれをソート(sort)と呼ぶ) を隠蔽ソート(hidden sort)として導入し、データの集まり(型)である可視ソート(visible sort)と区別することで、状態遷移モデルを実現し，記述力と解析力・検証力を高めている。可視ソートはデータ型、隠蔽ソートはプロセス型とも呼ばれる。問題モデルの定義・形式仕様の中で、データ型とプロセス型を適切に区別して使うことで、適切な抽象度を持った仕様が開発しやすく検証もしやすいことが先行研究により明らかになっていた。ここで、適切な抽象度とは、関心がある性質を解析・検証するのに必要十分な問題モデルの抽象化のレベルのことである。問題モデルが適切な抽象度を持たないと、望みの性質が検証できないか、または検証が不必要に煩雑かつ非効率になる。

(2) 推論型検証と探索型検証: 推論型と探索型の検証は対照的な原理に基づいており、互いに補完する。研究代表者のグループによる先行研究でも、推論型検証法である証明スコア法による検証において、検索方検証方であるモデル検査器を用いた自動検証と反例発見を適切に使うこと検証能力を高めることができる、との知見を得ていた。

４．研究成果

多様な応用分野で有効な帰納法と場合分けについて以下の成果を得た。

(1) 帰納法のデータ型・プロセス型の帰納的な構造に基づく定式化： CafeOBJ 仕様のデータ型やプロセス型は構成子から生成される項の集合として定義することが出来る。従って、データ型・プロセス型に対してある命題が成立することは、その命題がそのデータ型・プロセス型に属する全ての項について成立することとして定義できる。これから、データ型・プロセス型に対してある命題が成り立つことを証明するための帰納法は、そのデータ型・プロセス型を構成する項の集合の帰納的な構造、すなわち構成子が帰納的に項を生成する構造、に基づき定式化することができる。この帰納法の定式化は、仕様のモデルとして「構成子から生成される項だけから成るモデル」（到達可能モデル）を対象とする限り，多様な応用分野で有効な汎用的なものである。

(2) 場合分けの構成子からの項の生成に基づく定式化： 仕様中に現れる命題（つまりブール値(true,false)を返値とする関数）に基づき、仕様が定義するシステムの可能性を、返値が true な場合と返値が false な場合の、２つの場合に切り分けることは、最も典型的な場合分けである。これは、ブールデータ型を定義する２つの構成子 true と false に基づき、場合分けを定義したと見なすことが出来る。仕様に現れる全てのデータ型とプロセス型が構成子から生成されると仮定すると、全ての場合分けを、このブール値に基づく場合分けと同様に、構成子に基づき定式化できる。この場合分の定式化は、仕様のモデルとして「構成子から生成される項だけから成るモデル」（到達可能モデル）を対象とする限り，多様な応用分野で有効な汎用的なものである。

(3) (1),(2)に基づく、①完全な証明規則の定式化、②推論と探索を融合した強力な検証法の開発：

① 完全な証明規則の定式化： CafeOBJ 言語による証明スコア法の基本操作は、帰納法と場合分け、さらにそれらから導出される規則の適用である。これらの基本操作が健全(sound)、つまり論理的に正しいものである、ことは検証法であるための必要条件である。一方、基本操作が検証操作として完全(complete)、つまり検証可能な命題は基本操作により検証できる、ことは検証法が持つことが望ましい性質ではあるが、この性質を有する検証法は稀である。証明スコア法の基本操作が完全であることを理論的に示した。この結果は、CafeOBJ 仕様に基づく証明スコア法が、極めて強力な検証法であることを示すものである。

② 推論と探索を融合した強力な検証法の開発： スコア法は対話的検証法であり、その一部を自動化して検証の自動化率を向上することは本基盤研究の最大の目標の一つであった。無限状態を有限状態に帰着させる抽象化の正しさを証明スコア法で対話的に検証し，有限状態については全ての場合を探索ツールで網羅的調べる、ことで無限状態に対する検証を行う方法を定式化し、そのためのツールを開発した。

以上の①と②の成果のうち、①の理論的な成果は当初は予想しなかったものであるが、かなり一般的な形で証明スコア法の完全性を保証する理論的な成果を得ることが出来た。②は計画したとおりの成果であり、本基盤研究の成果の中でも最も重要なものの一つである。これら２つの成果は、それらに基づきさらに強力な問題モデル検証技術を構築できる可能性があり、今後の発展が期待できる。

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 44 件）

(査読有 44 件、査読無 0 件)

① Masaki Nakamura, Kazuhiro Ogata, Kokichi Futatsugi: Reducibility of operation symbols in term rewriting systems and its application to behavioral specifications. J. Symb. Comput. 45(5): 551-573 (2010)（査読有）

② 二木厚吉，緒方和博，中村正樹：CafeOBJ 入門(1)-(6)、コンピュタソフトウェア(日本ソフトウェア科学会論文誌)，25(2)：1-13, 25(2)：14-27, 25(3)：69-80, 25(4)：68-84，26(1)：71-83，26(2)：93-106, 2008-2009.（査読有）

③ D.Gaina, K.Futatsugi, K.Ogata: Constructor-based institutions, Proc. of CALCO 2009, LNCS 5728, Springer, pp.398-412, 2009.（査読有）

④ Masaki Nakamura, Kazuhiro Ogata, Kokichi Futatsugi: User-Defined On-Demand Matching. IEICE Transactions

92-D(7): 1401-1411 (2009) (査読有)

⑤ 二木厚吉： フォーマルメソッドの新展開--検証進化可能電子社会の中核技術--,情報処理, Vol.49, No.5, pp.521-529, 情報処理学会, 2008. (査読有)

⑥ Yasuhito Arimoto, Yuji Watanabe, Michiharu Kudoh, Kokichi Futatsugi: Checking Assignments of Controls to Risks for Internal Control, Proc. of 2nd International Conference on Theory and Practice of Electronic Governance 2008, ACM, pp.98-104, 2008. (査読有)

⑦ K.Futatsugi, J.A.Goguen and K.Ogata: Verifying Design with Proof Scores, Proc. of 1st VSTTE, LNCS 4171, Springer, pp.277-290, 2008. (査読有)

⑧ Masaki Nakamura, Weiqiang Kong, Kazuhiro Ogata, Kokichi Futatsugi: A Specification Translation from Behavioral Specifications to Rewrite Specifications. IEICE Transactions 91-D(5): 1492-1503, 2008. (査読有)

⑨ Kazuhiro Ogata and Kokichi Futatsugi: Formal Analysis of the Bakery Protocol with Consideration of Nonatomic Reads and Writes, Proc. of the 10th Intl. Conference on Formal Engineering Methods (10th ICFEM), LNCS 5256, pp.187-206, Springer, 2008. (査読有)

⑩ Jianwen Xiang, Dines Bjorner, Kokichi Futatsugi: Formal digital license language with OTS/CafeOBJ method, Proc. of IEEE/ACS Intl. Conference on Computer Systems and Applications, pp.652-660, IEEE, 2008. (査読有)

⑪ Kazuhiro Ogata and Kokichi Futatsugi: Simulation-based verification for invariant properties in the OTS/CafeOBJ method, Refine 2007, ENTCS 201, Elsevier, pp.127-154, 2008. (査読有)

⑫ W.Kong, K.Ogata, K.Futatsugi: Specification and Verification of Workflows with RBAC Mechanism and SoD Constraints, Intl. J. of Software Eng. and Knowledge Eng., 17(1): pp.3-32, World Scientific, 2007. (査読有)

⑬ Masaki Nakamura and Kokichi Futatsugi, On equality predicates in algebraic specification languages, Proc. of the 4th International Colloquium on Theoretical Aspects of Computing (ICTAC 2007), LNCS 4711, Springer, pp.381-395, 2007. (査読有)

⑭ Kazuhiro Ogata and Kokichi Futatsugi: Modeling and verification of real-time systems based on equations, Sci. of Comp. Prog., 66(2): 162-180, Elsevier, 2007. (査読有)

〔学会発表〕(計 8 件)
(査読有 0 件、査読無 8 件)

① Kokichi FUTATSUGI, Verifying Specifications with Proof Scores in CafeOBJ, Proc. of 21st IEEE International Conference on Automated Software Engineering, pp. 3-10, 20 September 2006. Tokyo (an invited keynote talk)

〔図書〕(計 1 件)

① 二木厚吉, 緒方和博, 有本泰仁： 法令対象ドメインの形式記述と検証,片山卓也編「法令工学の提案」, JAIST Press, 第４章 (pp.71-93), 2007.

〔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

６．研究組織
(1)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

(2)研究分担者(2006.4-2008.3)
中村　正樹 (NAKAMURA MASAKI)
北陸先端科学技術大学院大学・情報科学研究科・助手
研究者番号：40345658

(3)連携研究者 (2008.4-2010.3)
中村　正樹 (NAKAMURA MASAKI)
金沢大学・理工研究域電子情報学系・助教
研究者番号：40345658