JAIST Repository
https://dspace.jaist.ac.jp/

Title	証明スコア法に基づく革新的仕様検証システムの構築
Author(s)	二木，厚吉
Citation	科学研究費助成事業研究成果報告書: 1-5
Issue Date	2016-05-18
Type	Research Paper
Text version	publisher
URL	http://hdl.handle.net/10119/13692
Rights	
Description	基盤研究(S)，研究期間：2011～2015，課題番号：23220002，研究者番号：50251971，研究分野：形式手法、仕様検証、ソフトウェア工学

JAIST
JAPAN
ADVANCED INSTITUTE OF
SCIENCE AND TECHNOLOGY

Japan Advanced Institute of Science and Technology

様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２８ 年　 ５ 月 １８ 日現在

機関番号：１３３０２
研究種目：基盤研究(S)
研究期間：2011～2015
課題番号：２３２２０００２

研究課題名（和文）証明スコア法に基づく革新的仕様検証システムの構築

研究課題名（英文）Development of the Innovative Specification Verification System based on 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・ソフトウェア検証研究センター・特任教授

研究者番号：５０２５１９７１

交付決定額（研究期間全体）：（直接経費）　134,300,000円

研究成果の概要（和文）：仕様検証法の最重要課題として(1)適切な抽象度と(2)推論型×探索型検証を実現する技術の研究を、重要な仕様検証事例として(3)ソフトウェア自動更新と(4)車載OS標準の事例開発を、補完的に推進した。(1)-(4)の成果を、CafeOBJ仕様言語システムに統合することで、革新的仕様検証システムを実現した。本研究の成果である[革新的仕様検証システム=最新版CafeOBJ仕様言語システム]はホームページ(cafeobj.org)を通じてフリーウェアとして入手可能であり、UNIX/Linux, MacOS, Windowsの３つの主要なプラットホームで実行可能である。

研究成果の概要（英文）： Methods for (1)achieving an appropriate level of abstraction and (2)combining inference and search in verification are researched as most important issues of specification verification. Cases of (3)self-updating software and (4)international standard for automotive software are developed as most important cases of specification verification.
Quite a few versions of language system for specification verification has been researched and developed by incorporating the research achievements of (1)-(4) into the CafeOBJ specification language system. The targeted innovative specification verification system is realized as the latest version of CafeOBJ specification language system that supports newly developed verification methodology and includes newly developed verification cases.
The latest version of CafeOBJ specification language system is available as freeware from the CafeOBJ web page (cafeobj.org) and can be executed on UNIX/Linux, MacOS, and Windows.

研究分野：形式手法, 仕様検証、ソフトウェア工学

キーワード：仕様記述・仕様検証　形式手法　ソフトウェア工学　代数仕様　証明スコア　CafeOBJ　定理証明

１．研究開始当初の背景

ソフトウェア科学技術はあらゆる学術分野を横断する汎用科学技術となりその重要性はますます高まっている。

仕様（問題領域や応用領域における組織、規則、活動、処理のモデルの記述）の信頼性と安全性の確保は、２１世紀のソフトウェア科学技術の最重要課題の一つである。たとえば、現在多くの企業や行政組織は、顧客や住民の要求に迅速かつ的確に応えるべく、ネット上での新たなサービス提供に積極的に取り組んでおり、問題領域の要求を定式化した仕様の信頼性と安全性の確保が最重要の課題となっている。また、電気自動車への移行を想定した車載ソフトウェア分野では、OS（操作システム）などの基本ソフトウェアの機能やアーキテクチャを標準化し、多くのメーカーが柔軟に連携して高信頼で安全なソフトウェアを開発し得るオープンな体制の整備が急務であり、基本ソフトウェアの要件を定式化した標準（仕様）の信頼性と安全性の確保が最重要の課題である。

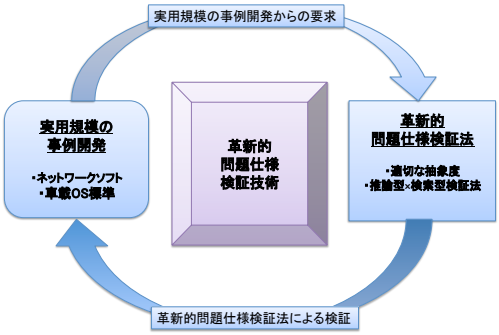
信頼性や安全性を重要な要件として仕様を作成しそれを検証する技術は、最重要のソフトウェア技術である。こうした技術は、ソフトウェア工学分野における、ドメイン技術、要求技術、仕様技術、検証技術などに属するが、仕様の信頼性や安全性を検証し得る技術はいまだに確立されていない。CafeOBJ仕様言語システムと証明スコア法は、信頼性や安全性が検証可能な形式仕様を作成し得る、革新的仕様検証システムを実現するための独創性の高い研究成果を有する。

２．研究の目的

信頼性や安全性を重要な要件として仕様(問題領域や応用領域における組織、規則、活動、処理のモデルの記述)を検証するための革新的な仕様検証技術を研究開発する。
具体的には、研究代表者二木と研究分担者緒方が研究開発してきたCafeOBJ証明スコア法に基づく検証技術と、研究分担者青木が研究開発してきた車載 OS の検証技術の研究成果に基づき、実用的に重要な事例開発と仕様検証法の研究を相互補完的に展開することで、実用規模の仕様を系統的に作成しかつ検証し得る、革新的な仕様検証システムを構築する。これにより、信頼性と安全性の確保が最重要の要件となる 21 世紀のソフトウェア科学技術に対して本質的かつ独創的な貢献を成す。

３．研究の方法

実規模の事例に対し適切な抽象度の仕様を作成し、それを推論型と探索型をシームレスに融合した推論型×探索型検証法で検証することで、仕様検証技術を確立する。具体的には、自動更新ソフトウェアなどのネットワークソフトウェアと、車載 OS 標準の２つの事例を取り上げ、事例開発と仕様検証法研究の２つを相互補完的に展開することで、研究開発を推進する。これにより、実規模の仕様の作成法と検証法を実証的に明らかにし、それらの研究成果を CafeOBJ 言語システムに統合することで、革新的仕様検証システムを実現する。研究成果はネットワークを通じて世界に広く発信する。



４．研究成果

仕様検証の中核技術として、(1)適切な抽象度と(2)推論型×探索型検証を実現する技術の研究を推進し、以下のような成果を得た。実用的に重要な事例として、(3)ソフトウェア自動更新事例と(4)車載OS標準事例の研究開発を推進し、以下のような成果を得た。それらの成果をCafeOBJ仕様言語システムに統合することで、(5)革新的仕様検証システムを構築した。

(1)適切な抽象度の実現

仕様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。適切な抽象度の実現は仕様検証のための最大の課題であるが、いままで十分に一般的でかつ有効な方法は体系化されていない。本研究では、事例開発を通じて、OTS (Observational Transition System)のスキーマに基づき、データ型とプロセス型を適切に切り分けつつ、 適切な抽象度を実現する方法を開発した。具体的には、(i)CafeOBJ 言語の順序ソート(order sort)機能とモジュール化機能を使い OTS の観測子(observer) の引数の詳細化を系統的に行う技術と、(ii)OTS の状態を観測子の集合(set)または列(sequence)とすることで観測子を必要な詳細度で参照・捨象する技術を研究開発した。とくに(i)の技術は車載 OS 標準事例を通じてその有効性が確認された。

新たな知見： OTS のスキーマ、順序ソート、状態の集合や列によるモデル化などを通じて適切な抽象度を客観的に定式化できた点に新規性があり、再利用可能な新たな知見として体系化できた。

学術的インパクト： 適切な抽象度を客観的に実現する技術は、我々の知る限りいままで存在せず、学術的な意義は大きい。

可能性： 適切な抽象度の実現は、仕様検証の大前提であり、今後この技術を支える理論とより広範な事例の研究開発により、仕様検証の重要な基盤科学技術に発展する可能性を有する。

(2)推論型×探索型検証の実現

仕様検証には、初期段階から検証を試み、できる限り早い時期に反例を発見し正当性を確認することを繰り返すことで、仕様の作成と検証を相互補完的に展開し、問題領域のモデル化の信頼性を高めることが重要である。本研究では、探索型検証で反例発見(反証)を推論型検証で仕様の正当性の確認（証明）を行う、推論型と探索型をシームレスに融合した推論型×探索型検証法の研究開発を目指し、状態パタンと trans 規則に基づく検証技術の研究開発を行った。

CafeOBJ 仕様言語は、順序ソート等式論理、振舞論理(隠ぺい論理)、書換え論理に基づき設計されている。これまでは、分散システムを OTS(観測遷移システム)でモデル化し、OTS の振舞仕様を順序ソート等式論理により記述してきた。等式のみを用いて記述した OTS 仕様は証明スコア法に基づく推論型検証に向いているが、探索型検証には不向きである。この問題点を解消するために、OTS の状態を観測子の集合または列として表現し、状態遷移をその状態表現（状態パタン）上の書換え規則(trans 規則)として表す方法を考案した。これにより、OTS の全ての可能な状態（一般には無限）をもれなくカバーする有限の状態パタンを系統的に生成し、その全てについて望みの性質が成り立つことをチェックすることが可能となった。また、この状態パタンにより、ある数以下の状態遷移でたどり着ける全ての状態を探索する従来の探索型検証（有界モデル検査）も可能となった。

新たな知見： 有界モデル検査（探索型検証）と定理証明（推論型検証）が、状態を観測子の集合または列として表現することで、シームレスに融合できることが明らかになった。また、全状態をもれなくカバーする有限の状態パタンを系統的に生成することで、状態遷移の時間軸だけでなく、状態空間の空間軸についても探索型検証が出来ることが明らかになった。

学術的インパクト： 時間軸だけでなく空間軸にたいする探索型検証を推論型検証とシームレスに融合した本検証法は、全く新規のものであり、学術的な意義は大きい。

可能性： CafeOBJ の trans 規則を用いて記述した OTS は、直観的で解析しやすい記述となりうることがいくつかの事例により示されている。この利点を活用することで、より実用性の高い仕様記述検証技術を実現できることが期待できる。さらに、これまで主に不変性(invariant)の検証に用いてきた CafeOBJ のサーチ述語を、不変性のみならず活性(livness)の検証にも応用できることが明らかになった。また、(1)で述べた(i)CafeOBJ 言語の順序ソート機能を使い OTS の観測子の引数の詳細化を系統的に行う技術と、(ii)OTS の状態を観測子の集合または列とすることで観測子を必要な詳細度で参照・捨象する技術は、本検証法と表裏一体をなすものである。これらは、本検証法の大きな発展可能性を示している。

(3)ソフトウェア自動更新事例

Apple の iOS や Tesla Motors の Model S 電気自動車で採用されている over-the-air update(OTA 更新)などを含む次世代のソフトウェア更新技術の形式化ならびに形式検証の技術基盤を開発した。旧来の更新技術との違いは、更新手続きが人手によらずプログラム化・自動化されていること、稼働中のソフトウェアを本質的に停止することなく更新を行えること(動的ソフトウェア更新)である。

新たな知見： 次世代ソフトウェア更新を状態遷移システムで形式化できることがわかった。これにより、分散システム等の形式検証にとって有効であることが実証されてきた対話的定理証明（推論型検証）やモデル検査（探索型検証）の技術を次世代ソフトウェア更新の形式検証に対しても有効に利用できるとの知見を得た。

学術的インパクト： ソフトウェア工学の他分野と同じく、Apple の iOS や Tesla Motors の Model S 電気自動車の例からもわかるとおり、ソフトウェア更新に関しても理論研究より実践のほうが先んじている。このため次世代ソフトウェア更新の有効性については実証されつつあるが、安全性等の面で真に信頼し得る成熟した技術にするための理論研究が不足していることは否めない。本研究は、既に実用化が始まっている次世代ソフトウェア更新の形式検証の基盤を提供するものであり、学術的意義は大きい。

可能性： 研究成果となる次世代ソフトウェア更新の形式化ならびに形式検証法は

学術的研究として閉じるものではなく、Apple の iOS や Tesla Motors の Model S 電気自動車で採用されている OTA 更新に対しても適用できる見通しである。すでに実用化がすすみつつあるが、OTA 更新の安全性・信頼性は理論的には保障されていないのが実状である。OTA 更新を含む次世代ソフトウェア更新は複雑化の一途をたどるソフトウェアの保守・進化を支える技術として不可欠であること、社会の安全性・信頼性はソフトウェアに大きく依存しており今後その傾向はますます強くなることから、本研究は、OTA 更新を含む次世代ソフトウェア更新を理論的に保障(形式検証)する可能性を開くものである。

(4)車載 OS 標準事例

車載オペレーティングシステムの国際標準 OSEK/VDX (Operating System 2.2.3、英文 86 ページの文書) は自然言語と図表で記述され公開された標準文書である。本研究では、この文書を形式化して、CafeOBJ により記述された形式仕様を作成した。国際標準の形式仕様は、可読性が高く、かつ容易に拡張できなければならない。高い可読性は、様々な人から参照されること、拡張容易性は、継続的にメンテナンスされることからの要求である。一方、形式仕様では、厳密に仕様を記述することから、必要以上に複雑になり、これらの要求を満たせなくなりがちである。そこで、(1)で述べた適切な抽象度を実現する技術、(i)CafeOBJ 言語の部分ソート機能を使い OTS の観測子(observer) の引数の詳細化を系統的に行う技術、を用いて CafeOBJ 形式仕様の基本的な構造を決定し、形式仕様を開発した。これにより、厳密であるだけでなく、読みやすく、かつ拡張容易な形式仕様を作成できた。

OSEK/VDX は、デッドロックや優先度逆転が発生しないことを保証すると言明している。作成した形式仕様に基づき、これらの性質の検証を行った。証明が容易になるよう一般化および抽象化を行い、これらの性質が成立することを、CafeOBJ システムを用いて証明した。さらに、抽象化した振る舞いと具体的な OSEK/VDX の振る舞いを対応づけることにより、OSEK/VDX においても、それらの問題が発生しないことを示した。

新たな知見： 国際標準 OSEK/VDX の形式仕様は現在まで開発されておらず、新規性があり、その作成を通じて、(1)で述べた適切な抽象度を実現する技術などの、多くの知見が得られた。

学術的インパクト： OSEK/VDX の形式仕様に基づきデッドロックや優先度逆転が発生しないことを示した事例は存在せず、新規性があり、大きな学術的インパクトを持つ。

可能性： 本事例研究の中で提案した証明の枠組みは、OSEK/VDX 固有のものではなく、同様のスケジューリングを伴う OS にも適用可能なように一般化されている。対象となる OS の仕様と抽象化した振る舞いとの対応関係を決めることで、OS が望ましい性質を持つことを検証するための汎用的な枠組に発展し得る。

(5)革新的仕様検証システム

証明スコア法による仕様の作成と検証は、仕様と証明スコアの2種類の CafeOBJ 言語の文書を作成しつつ、適宜それらを実行するという対話的かつ総合的な作業により行われる。こうした作業を、特定の環境やツールに依存せず支援するために、広く使われ定評のある UNIX/Linux, MacOS, Windows や Emacs, Eclips などの OS やエディターからなる標準的な開発環境を前提として、仕様検証システムを実現した。具体的には、上記(1)-(4)の研究成果を、研究の進展に並行して、標準的な環境を前提として、CafeOBJ 仕様言語システムに統合することで、汎用性の高い革新的仕様検証システムを実現した。

研究成果が統合された CafeOBJ 言語システムは BSD ライセンスに基づくフリーウェアとしてホームページ:

https://cafeobj.org/

を通じて入手可能であり、UNIX/Linux, MacOS, Windows の3つの主要なプラットホームで実行可能である。

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 66 件）

① Adrian Riesco, Kazuhiro Ogata, Kokichi Futatsugi: CafeInMaude: A CafeOBJ Interpreter in Maude. Springer Lecture Notes in Computer Science, Vol.9633 (Fundamental Approaches to Software Engineering, 19th FASE), Refereed, 2016, pp.377-380.

② Kokichi Futatsugi: Generic Proof Scores for Generate & Check Method in CafeOBJ. Springer Lecture Note in Computer Science, Vol.9200 (Logic, Rewriting, and Concurrency), Refereed, 2015, pp.287-310.

③ Hiroyuki Yoshida, Kokichi Futatsugi, Kazuhiro Ogata: Formalization and Verification of Declarative Cloud Orchestration. Springer Lecture Note in Computer Science, Vol.9407 (Formal Methods and Software Engineering, 17th ICFEM), Refereed, 2015, pp.33-49.

④ Kokichi Futatsugi: Generate&Check Method for Verifying Transition Systems in CafeOBJ. Springer Lecture Notes in Computer Science, Vol.8950 (Software, Services, and Systems), Refereed, 2015, pp.171-192.
⑤ Daniel Gaina, Kokichi Futatsugi: Initial semantics in logics with constructors. Journal of Logic and Computation, 25 (1), Refereed, 2015, pp.95-116
⑥ Iakovos Ouranos, Petros Stefaneas, Kazuhiro Ogata: TESLA source authentication protocol verification experiment in the Timed OTS/CafeOBJ method: Experiences and Lessons Learned. IEICE TRANSACTIONS on Information and Systems, E97-D(5), Refereed, 2014, pp.1160-1170.
⑦ Masaki Nakamura, Kazuhiro Ogata, Kokichi Futatsugi: Incremental proofs of termination, confluence and sufficient completeness of OBJ specifications. Springer Lecture Notes in Computer Science, Vol.8373 (Specification, Algebra, and Software), Refereed, 2014, pp.92-109.
⑧ Haitao Zhang, Toshiaki Aoki, Yuki Chiba: A Spin-based Approach for Checking OSEK/VDX Applications. Proc. of 3rd Intl. Workshop on Formal Techniques for Safety-Critical Systems (FTSCS), Refereed, 2014, pp.187-202.
⑨ Daniel Gaina, Dorel Lucanu, Kazuhiro Ogata, Kokichi Futatsugi: On Automation of OTS/CafeOBJ Method. Springer Lecture Notes in Computer Science, Vol.8373 (Specification, Algebra, and Software), Refereed, 2014 pp.578-602.
⑩ Norbert Preining, Kazuhiro Ogata, Kokichi Futatsugi: Liveness Properties in CafeOBJ - A Case Study for Meta-Level Specifications. Springer Lecture Notes in Computer Science, Vol.8981 (Logic-Based Program Synthesis and Transformation, 24th LOPSTR), Refereed, 2014, pp.182-198.
⑪ Kokichi Futatsugi, Daniel Gaina, Kazuhiro Ogata: Principles of proof scores in CafeOBJ. Theoretical Computer Science (TCS), 464, Refereed, 2012, pp.90-112.

〔学会発表〕（計 20 件）
① Kokichi Futatsugi: Recent Developments on Algebraic Specification and Verification in CafeOBJ. 2nd International Symposium on Dependable Computing and Internet of Things (DICT 2015), 16-18 November 2015, Wuhan, China.
② Kokichi Futatsugi: Generate & Check Method for Verifying Transition Systems in CafeOBJ (an overview). Science and Practice of Engineering Trustworthy Cyber-Physical Systems, Shonan Meeting 26-30 October 2014, Hayama, Kanagawa, Japan.

〔図書〕（計 2 件）
① Shusaku Iida, Jose Meseguer, Kazuhiro Ogata (Eds), Springer, Specification, Algebra, and Software: Essays Dedicated to Kokichi Futatsugi. Springer Lecture Notes in Computer Science, Vol. 8373, 2014, 657p.

〔その他〕
ホームページ等
https://cafeobj.org/

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・ソフトウェア検証研究センター・特任教授
研究者番号：５０２５１９１７

(2)研究分担者
緒方 和博 (OGATA,KAZUHIRO)
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：３０２７２９９１

青木 利晃 (AOKI,TOSHIAKI)
北陸先端科学技術大学院大学･情報科学研究科・准教授
研究者番号：２０３１３７０２

中村 正樹 (NAKAMURA,MASAKI)
富山県立大学・工学部・講師
研究者番号：４０３４５６５８

(3)連携研究者
千葉 勇輝 (CHIBA,YUKI)
北陸先端科学技術大学院大学･情報科学研究科・助教
研究者番号：１０５０９７５６

清野 貴博 (SEINO,TAKAHIRO)
産業技術総合研究所・社会知能研究ラボ・特別研究員
研究者番号：１０３９７２２６

(4)研究協力者
PREINING,Norbert
北陸先端科学技術大学院大学･ソフトウェア検証研究センター・准教授
研究者番号：６０５７１２４７

GAINA,Daniel
北陸先端科学技術大学院大学･ソフトウェア検証研究センター・助教
研究者番号：８０５９５７７８