平成２３年度採択分
平成２６年３月２５日現在

証明スコア法に基づく革新的仕様検証システムの構築

Development of the Innovative Specification Verification System based on Proof Scores

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

研究の概要
問題仕様（問題領域や応用領域における組織、規則、活動、処理の仕様やモデル）の信頼性と安全性の確保を目指し、CafeOBJ 形式仕様言語システムとそれに基づく証明スコア法を発展させ、革新的仕様検証システムを構築する。これによりソフトウェア科学技術に対して基本的で独創性の高い貢献を成す。

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、問題仕様、CafeOBJ、証明スコア

１．研究開始当初の背景

問題仕様（問題領域や応用領域における組織、規則、活動、処理の仕様やモデル）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、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、操作システム(OS)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（問題仕様）の信頼性と安全性の確保が最重要の課題である。

２．研究の目的

信頼性や安全性を重要な要件として問題仕様を検証するための仕様検証技術を研究開発する。具体的には、研究代表者のグループが研究開発してきた CafeOBJ 言語システムと証明スコア法を発展させ、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する基本的かつ独創的な貢献を成す。

３．研究の方法

現在までの研究の蓄積に基づき、ソフトウェア自動更新と車載 OS 標準の２つの性格の異なる事例について、実用規模の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により、革新的仕様検証システムの研究開発を推進する。

４．これまでの成果

証明スコア法による仕様検証の中核技術として、(A)適切な抽象度と(B)推論型×探索型検証法を実現する技術の研究を進めるとともに、実用的に重要な事例として、(C)ソフトウェア自動更新事例と(D)車載 OS 標準事例の研究開発を進め、それらの成果を CafeOBJ 形式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構築しつつある。各々の研究成果は以下の通りである。

(A) 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確立されていない。本研究では、H25 年度までに、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(D)の車載OS標準事例を通じてその有効性が確認された。

(B) 推論型×探索型検証法

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､H25 年度までに状態パタンと trans 規則に基づく検証技術の研究開発を行った。

これまでは、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状態表現を系統的に生成し、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、この状態表現により、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）も可能となる。

(C) 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)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。

(D) 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 は自然言語(英語)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。標準仕様は、読みやすく、かつ、容易に拡張できなければならない。前者は、様々な人から参照されること、後者は､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、(A)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、整った構造の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。これにより、開発した抽象的な形式仕様の詳細化である具体的な OSEK/VDX の振る舞いにたいしても、デッドロックや優先度逆転が発生しないことが保証される。

５．今後の計画

(A) 適切な抽象度の実現

(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、の２つを融合した技術を研究開発する。

(B) 推論型×探索型検証法

時間的探索と空間的探索を推論型検証とシームレスに融合する推論型×探索型検証法を研究開発する。

(C) ソフトウェア自動更新事例

次世代ソフトウェア自動更新の形式検証を完成する。

(D) 車載OS標準事例

車載 OS 国際標準 OSEK/VDX Operating System 2.2.3 (英文 86 ページの国際標準)の CafeOBJ 形式仕様を完成しネットを通じて世界に発信する。

６.これまでの発表論文等(受賞等も含む)

[1] Kokichi Futatsugi, Daniel Gaina and Kazuhiro Ogata: Principles of proof scores in CafeOBJ. Theoretical Computer Science (TCS), 464: 90-112, Elsevier, 2012. (査読有)

[2] Daniel Gaina, Kokichi Futatsugi and Kazuhiro Ogata: Constructor-based Logics. The Journal of Universal Computer Science (J. UCS), 18(16): 2204-2233, J.UCS consortium, 2012. (査読有)

[3] Kazuhiro Ogata, Kokichi Futatsugi: Theorem Proving Based on Proof Scores for Rewrite Theory Specifications of OTSs, Specification, Algebra, and Software, SAS 2014, LNCS 8373, Springer, pp.630-656, 2014. (査読有) (to appear)

ホームページ等

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