様式 C-19

科学研究費補助金研究成果報告書

平成２３年５月３１日現在

機関番号：６２６１５
研究種目：基盤研究（C）
研究期間：２００８～２０１０
課題番号：２０５００００４２
研究課題名（和文）　代数仕様を用いた要求モデルの自動検査に関する研究

研究課題名（英文）　Automatic Analysis of Requirements Model with Algebraic Specification Techniques

研究代表者
中島　震（NAKAJIMA SHIN）
国立情報学研究所・アーキテクチャ科学研究系・教授
研究者番号：６０３５０２１１

研究成果の概要（和文）：
「利用者の誤使用も製造者の責任」、といわれ、どのような機能を提供すべきかを決める作業が大きな課題になっている。この問題に対して、開発の初期段階で作成する要求モデルの検査を行う方法がある。本研究課題では、Event-B と呼ぶ手法で作成した要求モデルの正しさを自動検証する技術の研究を行った。考案した抽象化に基づく自動検査は、従来の検査方法と補完的な役割を果たす。正しさを検査する基準として新しい視点を導入できたといえる。

研究成果の概要（英文）：
Since it is said that even misusage of clients is what developers should be responsible for, the task of specifying what features the system provides becomes a major issue. According to Software Engineering, such a problem is to be resolved by checking of rigorous requirements models constructed at early stages of the development. In this research project, we investigated a new method of automated analysis of requirements models written in Event-B. The proposed method makes use of abstraction techniques, and provides a new correctness criteria complementary to existing methods,

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００８年度	1,100,000	330,000	1,430,000
２００９年度	1,300,000	390,000	1,690,000
２０１０年度	1,100,000	330,000	1,430,000
年度			
年度			
総　計	3,500,000	1,050,000	4,550,000

研究分野：ソフトウェア工学
科研費の分科・細目：情報学・ソフトウェア
キーワード：ソフトウェア工学、ソフトウェア開発効率化・安定化

１．研究開始当初の背景

ソフトウェア技術を利用したシステムが社会基盤に浸透すると共に、高い信頼性を達成する方法への関心が高まっている。複雑なシステムの本質的な側面を簡潔に表現することで見通しの良い設計を行う技術を提供す

る形式手法への期待が大きい。特に、システムが満たすべき事項を整理する要求モデリングへの適用を目的とする Event-B が注目されている。

Event-B は、先行する B メソッドとの比較では、非決定並行システムの記述を可能とした新しい形式手法といえる。ところが、並行システムを表現可能という特徴が、逆に、従来の方法での正しさの検証を難しくしている。時系列的な処理順序の性質を論じる振る舞い仕様の正しさを確認する系統的な方法が必要となっている。

２．研究の目的

本研究課題では、要求モデリングの正しさを確認する方法に注目する。具体的には、形式手法 Event-B を対象とする振る舞い仕様の系統的な検査方法を中心に研究を進める。

現状の技術では、Event-B の振る舞い仕様の確認は、仕様アニメータ（AnimB）あるいはモデル検査（ProB）を利用する。AnimB はテストデータを与えての「シミュレーション」を行うツールであって系統的な正しさの確認が難しい。ProB は有限集合を扱う Event-B サブセットを取り扱い、さらに、検証対象の大きさを限定することでモデル検査を可能とした。いずれもツールも、正しさの確認という点で過小近似の方法になっており、したがって、不具合の見逃しという問題点を抱えた方法である。

本研究課題では、Event-B に過大近似を導入したモデル検査の方法を確立することで、上記現状技術の補完方法を考案する。さらに、過大近似では一般に、見かけの不具合（本当の不具合ではない）が発生する。これを極力少なくする工夫を行う。

３．研究の方法

Event-B は、現在、欧州フレームワークプログラム（FP7）の DEPLOY プロジェクトで研究開発が進行中の新しい形式手法である。Event-B を使った要求モデリングについても標準的な方法が確立されていない。そこで、(a) 過大近似の方法、(b) 要求モデリングの方法、の２つの観点からの研究が必要となる。以下、具体的な内容を説明する。

（１） 過大近似の方法

① Event-B の振る舞い仕様を考察する上で基本となる言語要素はイベントである。イベントには 2 種類の書き方がある。最初に短縮形式（when）を考察し、次に、一般形式（any）についての過大近似の導入方法を検討する。

② 過大近似の基本的な方法として述語抽象を用いる。通常の述語抽象では状態遷移を対象とするので、遷移の事前・事後、両方の情報を用いた抽象化を行う。一方、イベント記述は事前状態の正確な情報を持たない。したがって、新しい方法を考案する必要がある。

③ 抽象化の結果を既存のモデル検査ツールで検証する方法を検討する。特に、代数仕様技術に基づく Maude を用いる方法によってプロトタイピングを行い問題の本質を考察する。次いで、他モデル検査ツールを適用する場合についても検討することで一般的な技術とする。

（２） 要求モデリングの方法

① 前項（１）で考案する方法の妥当性を確認することを目的とした適切な Event-B 記述例が必要となる。DEPLOY プロジェクト資料には基本的な方法を考察する小規模例題が掲載されているだけである。中規模の記述例が必須である。そこで、そのような Event-B 記述を得る手順（モデリン

グ手順）を考案する。

② モデリング手順にしたがって、一般形式のイベントを用いる中規模例題を作成する。これを検討の例題とする。

4．研究成果

（1） 過大近似の方法

① イベントに対する述語抽象として、事前状態の情報を用いない方法を定式化した。一方、この方法では情報不足によって冗長な処理が混入する。そこで、冗長となる述語を決定する方法を考案することで問題点を解決した。冗長な述語は見かけの不具合の原因となる。

② 述語抽象では抽象化の対象となる述語の選択方法が重要となる。素朴には、イベントが持つガード条件の構成述語を対象とすればよい。実際、短縮形式（when）イベントでは、この方法が有効である。一方、一般形式イベント（any）では、ガード条件の述語を多様な意図で用いることから、素朴な方法ではうまくいかない。そこで、述語の使い方の目的を分類し、適切な述語だけを抽象化対象とする方法を考案した。残念ながら、述語の構文的な情報だけでは十分な分類ができないことも判明した。

③ 抽象化の計算は、述語論理式の充足性判定として定式化することができる。対象論理式を構成する述語、変数、定数、などは、Event-B の構文で表現されている。そこで、Event-B のツールである RODIN を用いて充足性判定を行う方法を考案した。

④ 抽象化後のイベントは命題論理の範囲で表現可能な Event-B サブセット記述になる。これに対して、構文的な変換を行うことで、代数仕様言語 Maude で表現する方法を考案した。Maude を用いて EventB イベントの遷移の仕組みを定義することで、目的を達成した。他モデル検査ツールも同様な方法で適用可能となる。具体例として、SPIN を用いる場合を実験した。

（2） 要求モデリングの方法

① Event-B 仕様を作成する前の段階で事前スケッチを行う方法として整理した。第 1 に問題記述からイベントを抽出する方法にオブジェクト指向モデリングの考え方を導入、第 2 にリファインメントの進め方を事前に検討するプランシートを考案、である。事前スケッチを行うことで、Event-B 仕様作成だけでなく検証作業の無駄も省けるような工夫を行った。

② 具体的な事例として、組込みシステムの典型例である割り込み制御と、設計方法論の検討で用いられる標準的な問題「酒屋在庫問題」を作成した。特に、後者の例題をもとに、一般形式に対する過大近似の方法が妥当であるかを確認した。

（3） 国内での位置づけ

① 集合論および述語論理に基づく Event-B と状態遷移系を対象とするロジック・モデル検査を融合する本研究は、広範な技術を要することから、国内で他に類をみない。

② 本研究課題実施中の 2009 年秋に産業界 5 社が集まった DSF（ディペンダブル・ソフトウェア・フォーラム）設立に関わった。DSF では新しい技術として Event-B に注目し、当該技術の調査研究を実施している。本研究課題の成果である「要求モデリングの方法」を

DSF に移管した。中規模以上の Event-B仕様構築に必須の考え方となっている。

（4） 海外との連携

Event-B は DEPLOY プロジェクトで研究が進行中の技術であることから、欧州の研究者との交流を積極的に行うことで、最新の情報に基づく研究を進める工夫を行った。また、日本での Event-B 関連活動（上記 DSF を参照）と欧州のコミュニティの交流を行った。

① フランスで Event-B 関連研究を進めているナント大学から学生を受け入れ共同研究を実施した。当該学生は卒業後、DEPLOY プロジェクト参加企業に就職し、現在も、同プロジェクトで活躍している。

② 日本人の研究者としてはじめて、B/Event-B関連の国際学会で研究発表を行った。

③ B/Event-B の考案者である Jean-Raymond Abrial 氏を招聘し、セミナー講演、研究打ち合わせを行った。セミナー講演は一般公開し国内産業界の方々を集めた。

（5） 今後の展望

Event-Bは単純な形式仕様言語である一方、書き方の自由度が高く、使いこなすことが難しい。本研究課題が着目した振る舞い仕様検証のための抽象化の中でも、ガード条件の使い方を明らかにする必要がある等、言語の構文的な情報のみから自動的な情報抽出が難しい。このことは、逆に、典型的な使い方を整理したイディオムや、応用領域ごとの特別な構文の工夫などが重要であることを示唆している。

また、Event-B 仕様記述の作成に先立つ事前スケッチを中心とする要求モデリングの方法は、中規模以上の記述を作成する上で必須のノウハウであることがわかった。同時に、DSF の活動など、産業界において、Event-B をどのように使えば効果的かといった調査研究が広がりを見せている。

本研究課題の成果は、形式手法の分野では、抽象化等の基本的な技術の研究と、モデリングを含む利用技術の研究を両輪で進めていくことの大切さを示しているといってよい。

５．主な発表論文等

〔雑誌論文〕（計３件）

① Shin Nakajima, Masaki Ishiguro, and Kazuyuki Tanaka 、 Rewriting Logic Approach to Modeling and Analysis of Client Behavior in Open Systems 、 Proceedings of 8th IFIP Workshop on Software Technology for Future Embedded and Ubiquitous Systems、査読有、2010、pp.83-94

② 中島震、ソフトウェア品質確保の技術動向、自動車研究、査読無、Vol.32、No.10、2010、pp.561-565

③ 中島震、形式手法の潮流：アーキテクチャへの関心、システム／制御／情報、査読無、Vol.52、No.9、2008、pp.310-315

〔学会発表〕（計７件）

① 中島震、Event-B で書かれたシステム要求仕様の妥当性検査、電子情報通信学会ソフトウェアサイエンス研究会、2010.8.7、旭川

② Shin Nakajima、A Refinement Planning Sheet 、 RODIN User and Developer Workshop 2010、2010.9.15、デユッセルドルフ

③ Shin Nakajima and Hironobu Kuruma、Abstraction Aided Model Checking for Validation of Event-B Descriptions, IM_FMT 2009、2009.2.16、デユッセルドルフ

〔図書〕（計３件）

① M.Ben-Ari（著）、中島震（監訳）、谷津弘一、野中哲、足立太郎（訳）、オーム社、SPIN モデル検査入門、2010、241

② 中島震、鷲崎弘宜（編）、近代科学社、ソフトウェア工学の基礎 XVI、2009、336

③ 中島震（著）、近代科学社、SPIN モデル検査、2008、238

〔その他〕
ホームページ等
http://research.nii.ac.jp/~nkjm/

６．研究組織
(1)研究代表者
中島　震（NAKAJIMA SHIN）
国立情報学研究所・アーキテクチャ科学研究系・教授
研究者番号：６０３５０２１１