科学研究費助成事業　　研究成果報告書

平成　２６　年　　４　月　２１　日現在

機関番号：　１４４０１
研究種目：　基盤研究(C)
研究期間：　2009～2013
課題番号：　２１５０００３６

研究課題名（和文）モデル検査技術を活用したソフトウェア設計方法に関する研究

研究課題名（英文）Software Design using Model Cheking

研究代表者
岡野　浩三（Okano, Kozo）

大阪大学・情報科学研究科・准教授

研究者番号：７０２５２６３２

交付決定額（研究期間全体）：（直接経費）　　3,300,000円、（間接経費）　　990,000円

研究成果の概要（和文）：本研究では以下のことを行い、ソフトウェア設計へのフォーマルアプローチの適用可能性、有用性を調べた.
1.時間オートマトンンのCEGARloopの適用アルゴリズムの考案と評価．2．OCL-JML総合変換アルゴリズムの考案と実用性の評価．3.時間オートマトンをライントレースロボットに適用して検証の有効性を示した．4.既存ソフトウェアに対してJML記述をループ構造に対して数学的解析を行うことにより，より精度度良く自動生成する方法論を新たに提案しその有効性を示した．5.Javaのequals メソッドとhashCodeメソッドの整合性を自動検証する手法を考案し，その有効性を示した.

研究成果の概要（英文）：This research investigates formal approach on software, especially design of software and its correctness.
The research mainly researches:
1 CEGAR loop algorithm for timed automaton; 2. JML-OCL conversion and its application to open softwares; 3. modelchecing of timed automata and its application to a line tracing robot; 4. JML assertion generation from ordinal program code using mathematical analysis on loop structure; and 5. automatic verification on consistency between equals method and hasCode method in Java programs.

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：　モデル検査　モデル　形式手法　時間オートマトン　CEGAR　OCL　JML

１．研究開始当初の背景

近年，形式手法を用いたソフトウェア開発方法に関する期待が高まっている．仕様レベルの品質保証のための基本技術としては実時間性については時間オートマトンが重要視されている．また，一般のソフトウェア開発においては DbC（Design by Contract）の概念に基づいた仕様記述法，とりわけ OCL や JML などが注目を浴びている．

時間オートマトンを用いて記述すれば，検証ツールにより時間的性質の妥当性が論理的に保証されると言う利点がある．時間オートマトンの検証の１つの大きな課題は，大きな記述に対する検証コストの爆発である．一般に大きな状態数やクロックを持つ時間オートマトンを計算機上で検証すると状態爆発が起こり，有意な時間内に検証を行うことが不可能となる．この問題を解決する方法として，モデル抽象化技法があり，多くの研究がなされている．

Clarke らは一般のオートマトンで記述されたシステムに対し，このような抽象化や，抽象化の改良過程を計算機上において全自動で行う手法を考案し，その方法が有用であることを示した.Clarke の提案する抽象化改良ループ(CEGAR)は一般のオートマトンに有限値を持つレジスタを加えた拡張オートマトンに対するものであり，実数領域のクロック変数を持つ時間オートマトンに対する方法は提案されていなかった．申請者の研究グループは最近，CEGAR を UPPAAL という時間オートマトンの最もポピュラーな検証ツールで採用されている時間オートマトンのサブクラスに適用する具体的なアルゴリズムを考案し，研究会で発表した．本研究はこのアルゴリズムの改良および，実用例題適用を通じて提案手法の有用性を明らかにする．

一方，OCL や JML の活用については多くの研究が活発になされている．申請者の研究グループは最近，既存のソフトウェアに対する JML アサーションの自動導出の研究を開始している．このアイディアを掘り下げ，ソフトウェア設計法への展開をはかり，別途研究を開始した OCL からの JML 変換法とともにソフトウェア開発支援を総合的に行う開発支援システムの提案と構築を考えている．このシステムの有用性を評価することにより，提案手法の有用性を評価していく．

２．研究の目的

上記を念頭に本研究では以下のことを行う．

（１） まず時間オートマトンの CEGAR ループの抽象化手法を例題に適用し， 有用性を示す．

（２） 提案抽象化手法の並列実行アルゴリズムを提案し， 有用性を示す．

（３） 既存ソフトウェアに対して JML 記述を自動で付加する処理系を提案手法に基づいて作成する．

（４） UML/OCL 記述から JML 記述を自動導出する方法をもとに（3）とあわせてソフトウェア開発支援システムのプロトタイプを作成する．

（５） UML/OCL 記述から時間オートマトンへ変換する方法と組み合わせ，それらをもとに総合的な設計開発法への展開をはかる．

以上により，信頼性が高いシステムの上位設計技法を確立することが研究目標である．

３．研究の方法

本研究は平成21-25 年の5 年研究として実施する．

４．研究成果

時間オートマトンの CEGAR ループの抽象化手法について論文にまとめられた．

既存ソフトウェアに対して JML 記述を自動で付加する処理系などを提案手法に基づいて作成し，いくつかの例題に適用することができた. UML/OCL 記述から JML 記述を相互的に自動導出する方法を提案しその有効性を示した．

その他、いくつかの派生研究を行えた．

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 12 件）

小林和貴, 佐々木幸広, 岡野浩三, 楠本真二: “PDG とSMT ソルバを利用した表明自動導出手法の提案と評価”, 電子情報通信学会論文誌, Vol.J96D, No.11, pp.2657-2668 (2013) (ソフトウェア基礎・応用特集号)

森恵弥佳, 岡野浩三, 楠本真二: “Alloy Analyzer を用いた表明に関する欠陥の検出手法—JML による表明記述に対して—”, 日本ソフトウェア科学会学会誌コンピュー

タソフトウェア, Vol.30, No.3, pp.3-187-3-193 (2013)

Kozo Okano, Toshifusa Sekizawa, Hiroaki Shimba, Hideki Kawai, Kentaro Hanada, Yukihiro Sasaki, and Shinji Kusumoto: "Verification of Safety Properties of a Program for Line Tracing Robot using a Timed Automaton Model," International Journal of Informatics Society, Vol.5, No.3, pp.147-155 (2013)

Kentaro Hanada, Hiroaki Shimba, Kozo Okano, and Shinji Kusumoto: "Implementation of a Prototype Bi-directinal Translation Tool between Ocl and Jml," International Journal of Informatics Society, Vol.5, No.2, pp.89-96 (2013)

Kiyoyuki Miyazawa, Kozo Okano, and Shinji Kusumoto: "LASP—a Learning Assistant System for Formal Proof," International Journal of Informatics Society, Vol.4, No.2, pp.85-92 (2012)

Takeshi Nagaoka, Akihiko Ito, Toshiaki Tanaka, Kozo Okano, and Shinji Kusumoto: "A Model Abstraction Technique for Probabilistic Real-Time Systems Based on CEGAR for Timed Automata," International Journal of Informatics Society, Vol.3, No.1, pp.11-20 (2011)

Yuko Muto, Kozo Okano, and Shinji Kusumoto: "A Visualization Technique for Unit Testing and Static Checking with Caller-Callee Relationships," Journal of Convergences, Vol.2, No. 2, pp.1-8 (2011)

宮本敬三, **堀直哉**, **岡野浩三**, **楠本真二**: "Daikon **生成表明改善のためのテストケース自動生成手法とその評価実験**",**日本ソフトウェア科学会学会誌コンピュータソフトウェア**, Vol. 28, No. 4, pp.4-306-4-317 (2011)

Takeshi Nagaoka, Akihiko Ito, Kozo Okano, and Shinji Kusumoto: "QoS Analysis of Real-time Distributed System Based on Hybrid Analysis of Probabilistic Model Checking," IEICE Transactions on Information and Systems, Vol.E94-D, No.5, pp.958-966 (2011) (**フォーマルアプローチ特集号**)

Takeshi Nagaoka, Kozo Okano, and Shinji Kusumoto: "An Abstraction Refinement Technique for Timed Automata Based on Counterexample-Guided Abstraction Refinement Loop," IEICE Transactions on Information and Systems, Vol.E93-D, No.5, pp.994-1005 (2010) (**フォーマルアプローチ特集号**)

尾鷲方志, **岡野浩三**, **楠本真二**: "**メソッドの自動生成を用いた**OCL **の**JML **への変換**",**日本ソフトウェア科学会学会誌コンピュータソフトウェア**, Vol. 27, No. 2, pp.2-106-2.111 (2010)

Takeshi Nagaoka, Eigo Nagai, Kozo Okano, and Shinji Kusumoto: "Stepwise Approach to Design of Real-Time Systems based UML/OCL with Formal Verification," International Journal of Informatics Society, Vol.1, No.2, pp.37-44 (2009)

〔**学会発表**〕（**計　24 件**）

Emsaib Geepalla, Behzad Bordbar, Kozo Okano, and Seyedhamed Seyedali: "AC2Uppaal: A Tool for automatic

Generation of Timed Automata for Analysis of Cyber-Physical Systems," in the proceedings of the World Congress on Internet Security (WorldCIS-2013) IEEE, (December 2013)

Hiroaki Shimba, Kentaro Hanada, Kozo Okano, and Shinji Kusumoto: "Bidirectional Translation between OCL and JML for Round-trip Engineering," Accepted in the 5th International Workshop on Empirical Software Engineering in Practice (IWESEP2013), (December 2013)

Toshifusa Sekizawa, Kozo Okano, Ayako Ogawa, and Shinji Kusumoto: "Verification of a Control Program for a Line Tracing Robot using UPPAAL Considering General Aspects," In Proceedings of International Workshop on Informatics 2013 (IWIN2013), pp.153-162 (September 2013)

Yuko Muto, Yukihiro Sasaki, Takafumi Ohta, Kozo Okano, Shinji Kusumoto, and Kazuki Yoshioka: "Variable Coverage: A Metric to Evaluate the Exhaustiveness for Program Specifications Based on DbC," In Proceedings of International Workshop on Informatics 2013 (IWIN2013), pp.113-132 (September 2013)

Emsaieb Geepalla, Behzad Bordbar, and Kozo Okano: "Verification of Spatio-Temporal Role Based Access Control using Timed Automata," In Proceedings of IEEE International Workshop on Design, Analysis and Tools for Integrated Circuits and Systems, pp.1-6 (December, 2012).

Kozo Okano, Toshifusa Sekizawa, Hiroaki Shimba, Hideki Kawai, Kentaro Hanada, Yukihiro Sasaki, and Shinji Kusumoto: "Verification of Safety Property of Line Tracer Program Using Timed Automaton Model," In Proceedings of International Workshop on Informatics 2012 (IWIN2012), pp.147-156 (September 2012)

Kentaro Hanada, Hiroaki Shimba, Kozo Okano, and Shinji Kusumoto: "Implementation of a Prototype Bi-Directinal Translation Tool between Ocl and Jml," In Proceedings of International Workshop on Informatics 2012 (IWIN2012), pp.131-138 (September 2012)

Kentaro Hanada, Kozo Okano, Shinji Kusumoto, and Kiyoyuki Miyazawa: "Practical Application of a Translation Tool from Uml/Ocl to Java Skeleton with Jml Annotation," In Proceedings of 14th International Conference on Enterprise Information Systems (ICEIS2012), pp. 389-394 (June 2012)

Kozo Okano, Behzad Bordbar, and Takeshi Nagaoka: "Clock Number Reduction Abstraction on CEGAR Loop Approach to Timed Automaton," In proceedings of the 2nd International Conference on Networking and Computing, pp.235-242, DOI 10.1109/ICNC.2011.42 (December 2011)

Kiyoyuki Miyazawa, Kozo Okano, and Shinji Kusumoto: "LASP - a Learning Assistant System for Formal Proof," In Proceedings of International Workshop on Informatics 2011 (IWIN2011), pp.158-165 (September 2011)

Yuko Muto, Kozo Okano, and Shinji

Kusumoto: “Improvement of a Visualization Technique for the Passage Rate of Unit Testing and Static Checking and its Evaluation,” In proceedings of The Joint Conference of the 21th International Workshop on Software Measurement (IWSM2011) and the 6th International Conference on Software Process and Product Measurement (Mensura), pp. 279-284 (November 2011)

Yuko Muto, Kozo Okano, and Shinji Kusumoto: “A Visualization Technique for the Passage Rate of Unit Testing and Static Checking with Caller-Callee Relationships,” International Conference on Advanced Software Engineering 2011, pp.336-341, DOI : 10.1109/ISPAW. 2011.54 (May 2011)

Takeshi Nagaoka, Akihiko Ito, Toshiaki Tanaka, Kozo Okano, and Shinji Kusumoto: “Reachability Analysis of Probabilistic Timed Automata Based on an Abstraction Refinement Technique,” International Workshop on Empirical Software Engineering in Practice 2010, pp.33-38 (December 2010)

Takeshi Nagaoka, Akihiko Ito, Kozo Okano, and Shinji Kusumoto: “ Reachability Analysis of Probabilistic Real-Time Systems Based on CEGAR for Timed Automata,” In Proceedings of International Workshop on Informatics 2010 (IWIN2010), pp.18-26 (September 2010)

Takeshi Nagaoka, Akihiko Ito, Kozo Okano, and Shinji Kusumoto: “Qualitative Analysis of Real-time Distributed Systems Considering Network Congestion by Probabilistic Model Checker PRISM,” In Proceedings of International Workshop on Empirical Software Engineering in Practice 2009 (IWESEP2009), pp.104-113 (October 2009)

Takeshi Nagaoka, Akihiko Ito, Kozo Okano, and Shinji Kusumoto: “Qos Evaluation for Real-Time Distributed Systems Using the Probabilistic Model Checker Prism,” In Proceedings of International Workshop on Informatics 2009 (IWIN2009), pp.60-66 (September 2009)

Kozo Okano, Kazuki Yoshioka, and Shinji Kusumoto: “Empirical Experiments on Software Assertion and Qualities,” Symposium on Advanced Information Systems (SAIS2013), Copenhagen, Denmark (September 2013).

Kentaro Hanada, Hiroaki Shimba, Kozo Okano, and Shinji Kusumoto: “A Bi-directional Translation Tool between OCL and JML considering Reverse Translation,” The 4th International Workshop on Empirical Software Engineering in Practice (IWESEP2012), poster presentation, Osaka Japan (October 2012)

佐々木幸広, **岡野浩三**, **楠本真二**: “SMT **を活用した**Java **プログラム解析フレームワークの設計**”, **日本ソフトウェア科学会「ソフトウェア工学の基礎」研究会第**19 **回ワークショップ**FOSE2012, **レクチャーノート・ソフトウェア学**38 **ソフトウェア工学の基礎**XIX, pp.33-38 (2012-12)

武藤祐子, **岡野浩三**, **楠本真二**: “**呼び出し関係を用いた単体テストおよび静的検査の**

可視化手法の改善とその評価", 日本ソフトウェア科学会「ソフトウェア工学の基礎」研究会第18 回ワークショップFOSE2011, レクチャーノート・ソフトウェア学37 ソフトウェア工学の基礎XVIII, pp.163-168 (2011-11)

小林和貴, 宮本敬三, 岡野浩三, 楠本真二: "アサーション動的生成を目的としたテストケース制約のESC/Java2 を利用した導出", 日本ソフトウェア科学会「ソフトウェア工学の基礎」研究会第17 回ワークショップFOSE2010, レクチャーノート・ソフトウェア学36 ソフトウェア工学の基礎XVII, pp.44-54 (2010-11)

武藤祐子, 岡野浩三, 楠本真二: "クラス間関係を利用した単体テストおよび静的検査の網羅率可視化手法", 情報処理学会ソフトウェア工学研究会ワークショップ SES2010, ソフトウェアエンジニアリング最前線2010, pp.107-112 (2010-09)

宮本敬三, 堀直哉, 岡野浩三, 楠本真二, 西本哲: "アサーション動的生成のためのテストケース自動生成手法の生成アサーションの妥当性評価", 日本ソフトウェア科学会「ソフトウェア工学の基礎」研究会第16 回ワークショップFOSE2009, レクチャーノート・ソフトウェア学35 ソフトウェア工学の基礎XVI, pp.183-190 (2009-11)

尾鷲方志, 岡野浩三, 楠本真二: "メソッドの自動生成を用いたOCL のJML への変換ツールの設計", 日本ソフトウェア科学会「ソフトウェア工学の基礎」研究会第16 回ワークショップFOSE2009, レクチャーノート・ソフトウェア学35 ソフトウェア工学の基礎XVI, pp.191-198 (2009-11)

宮澤清介, 岡野浩三, 楠本真二: "フォーマルアプローチの基本技術習得のための学習支援システムの試作", 情報処理学会ソフトウェア工学研究会ワークショップ SES2009,ソフトウェアエンジニアリング最前線2009, pp.69-74 (2009-09)

その他　研究会発表　39件

〔図書〕（計　0件）

〔産業財産権〕
○出願状況（計　0 件）

○取得状況（計　0 件）

〔その他〕
ホームページ等

6. 研究組織
(1)研究代表者
岡野 浩三　（オカノ コウゾウ）

研究者番号:
70252632
(2)研究分担者
谷口 健一　（タニグチ ケンイチ）

研究者番号:
00029513
(3)連携研究者
（　　）

研究者番号：