様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２９　年　　５　月　３１　日現在

機関番号：　１３３０２
研究種目：　基盤研究(C)（一般）
研究期間：　2014～2016
課題番号：　２６３３００８２

研究課題名（和文）高階プログラミング言語で記述された大規模ソフトウェアの検証

研究課題名（英文）Large scale verification of higher-order programs

研究代表者
寺内　多智弘（Terauchi, Tachio）

北陸先端科学技術大学院大学・先端科学技術研究科・教授

研究者番号：７０４４７１５０

交付決定額（研究期間全体）：（直接経費）　　3,700,000円

研究成果の概要（和文）：本課題の目標は、関数型プログラミング言語など、高階関数を含むプログラミング言語で記述された大規模ソフトウェアに対して有効な自動検証手法の確立である。特に、近年、国内外において高く注目されている依存型型システムを用いたソフトウェアモデル検査による手法を研究した。

主な研究成果は以下である：1.)よりよい抽象詳細化(ソフトウェアモデル検査に用いられる技術)の手法、2.)高階関数型プログラムのための停止性・活性仕様など時相論理仕様の自動検証手法。

研究成果の概要（英文）：The goal of the research is to advance the state of the art on automatic verification techniques of higher-order functional programs. We have especially focused on the techniques based on software model checking via dependent type inference, that has gained popularity in the recent years.

The main contributions of the research are as follows: 1.) New, improved abstraction refinement methods (abstraction refinement is a technique used in software model checking), 2.) New automatic methods for verification of temporal properties (such as termination and liveness) of higher-order functional programs.

研究分野：　ソフトウェア

キーワード：　プログラム検証　モデル検査　高階関数　述語論理　型システム　抽象詳細化　時相論理

１．研究開始当初の背景

今日の情報化社会において、コンピュータソフトウェアは生活基盤のいたる所に活用されており、その重要度は計り知れない。また、近年、ソフトウェアシステムの不具合は社会的に大きな問題として取り沙汰され、ソフトウェアプログラムの検証が非常に高い関心を集めている。モデル検査はハードウェア、ソフトウェアを問わずシステムの検証手法として最も有望視されている手法の一つである。2007 年にはモデル検査の提唱者の Clarke らが、コンピュータサイエンスにおけるノーベル賞といわれるチューリング賞を受賞している。また、マイクロソフト社はモデル検査に基づくソフトウェア自動検証ツール SLAM を構築し、Windows 用デバイスドライバの検証に実用化している。

しかし、SLAM を含め、従来のソフトウェアモデル検査の技術は、C 言語など低レベルなプログラミング言語で記述されたプログラムを対象としており、高階プログラムに対しては著しく精度を落とす。「高階プログラム」とは Lisp、ML、Haskell などの関数型プログラミング言語や Java、C++ などのオブジェクト指向言語に代表される、関数やオブジェクトをデータとして扱えるプログラムのことを指す。Java、C#、F# を始め、高階の機能を備えたプログラミング言語の普及が進む今、高階プログラムの検証は現実的に重要な課題であると考えられる。

近年、高階プログラム検証の有効な手段として、型システムの枠組みを用いたソフトウェアモデル検査が高い関心を集めている。型理論、モデル検査などプログラム検証およびプログラミング言語分野を横断し、国内外の研究グループがこの手法を取り入れ研究を推進している。

これらは、自動抽象化など、従来の（高階でない）ソフトウェアモデル検査の技術を、型システムを通じて高階プログラム検証に応用するという試みである。本課題研究代表者の寺内は、この枠組みで、世界で初めて反例を用いた自動抽象化の実現に成功するなど画期的な業績を挙げており、この研究の専門家である。

しかし、現在の高階プログラムに対するソフトウェアモデル検査は計算コストが高く、数十行程度の小規模なプログラムの検証に用いることが限界である。現在では、高階プログラミング言語の普及が進み、数万行以上にもなる大規模な高階プログラムも珍しくない。

２．研究の目的

本課題は、高階ソフトウェアモデル検査技術をベースとし、高階プログラミング言語で記述された大規模ソフトウェアに対する検証技術の確立を目指す。具体的には、以下のテーマを主な目的として研究を推進する。

(１) 高階ソフトウェアモデル検査の基盤となる抽象状態探索および抽象詳細化アルゴリズムを改良し、検証器の大幅な性能の向上を図る。また、依存関係解析によるスライシングなど大規模ソフトウェアに対して有効なプログラム解析の技術も取り入れる。

(２) プログラム注釈を用いた検証支援体系を検証の枠組みに加える。具体的には、各プログラムモジュールの満たすべき動作を記述する体系を開発する。既存の高階ソフトウェアモデル検査器が型システムの枠組みを用いていることもあり、型を用いた柔軟な注釈体系を開発する。

(３) 検証ツールを作成し、ML 言語、Java 言語など高階プログラミング言語で記述された実際の大規模ソフトウェアに対して検証実験を行う。

３．研究の方法

ソフトウェアは整数など無限もしくは非常に大きな範囲のデータを扱うため、ソフトウェア検証には「抽象化」によるデータの近似が欠かせない。適切な抽象を選択するために、多くのソフトウェアモデル検査器で用いられるのが、CEGAR という手法である。この手法では、(1)抽象化されたプログラムが仕様を満たしているか検査する「抽象状態探索」と、(2)抽象状態探索で検出された反例パスの真偽を確かめ、偽反例を除去するよう抽象を適切に詳細化する「抽象詳細化」を反復的に行う。

通常、CEGAR では「述語抽象」と呼ばれる論理述語式による抽象化が用いられる。述語抽象における抽象詳細化アルゴリズムは、与えられた反例を否定するのに十分な述語式を推論する。しかし、同じ反例に対して、それを否定する無数の述語式の候補が存在する場合があり、推論される述語式の選択がソフトウェアモデル検査全体の性能に影響することが課題となっている。特に、既存の高階ソフトウェアモデル検査で用いられる述語式推論手法は、僅かな入力の変化が選ばれる式に大きく変化を及ぼし、結果、性能に大きく影響を及ぼすことが知られている。本研究では、テンプレートを用いた述語式推論の技術 などを取り入れ、より予測可能なより良い抽象詳細化の実現を目指す。

また、高階プログラムに対するソフトウェアモデル検査特有の課題にも取り組む。具体的

には、既存の型を用いた高階プログラムのためのソフトウェアモデル検査技術をベースにより大規模ソフトウェアに対して効果的な手法を開発する。

４．研究成果

抽象状態探索・抽象詳細化についての研究を行い、以下の成果を得た：(1)ソフトウェアモデル検査による検証プロセスの収束性を保証する抽象詳細化の手法の開発。(2)サンプリングを用いて、より単純な抽象詳細化を求める手法の開発。(3) 述語抽象による抽象状態探索・抽象詳細化が検証プロセス全体に与える影響の理論的考察。

また、ソフトウェアモデル検査による高階プログラムの検証が扱える仕様のクラスを拡大することに成功した。具体的には、停止性、活性(liveness)など時相論理仕様の自動検証の手法を開発した。これは、(無限データを扱う)高階プログラムに対し、このクラスの仕様の初の健全かつ完全な検証手法である。

これらの研究は International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS)、European Symposium on Programming (ESOP)、ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL)など、トップレベルの国際論文誌および国際会議に採録された。また、国際会議 Horn Clauses for Verification and Synthesis (HCVS)、および、NII 湘南会議、Dagstuhl セミナーなどに招待され講演も行った。

また、ML など関数型プログラミング言語であっても、現実の大規模ソフトウェアは(特に代数データ構造やオブジェクト等の再帰データ構造に対する)破壊的代入を含むものも多く、検証技術をそのようなプログラミング言語機能に拡張する必要があるという事実も確認した。今後の研究の展開のための課題とする。例えば、分離論理やエイリアス型など、データ構造に対する破壊的代入を扱うためのプログラム論理・型システム等のアイデアを参考に効果的な検証手法を考える。

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 7 件）

① Akihiro Murase, Tachio Terauchi, Naoki Kobayashi, Ryosuke Sato, and Hiroshi Unno. Temporal Verification of Higher-Order Functional Programs. In Proceedings of the 43rd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL 2016), ACM SIGPLAN Notices 51 (1), pp. 57-68, ACM, January, 2016. (査読有)

② Tachio Terauchi. Explaining the Effectiveness of Small Refinement Heuristics in Program Verification with CEGAR. In Proceedings of the 22nd International Static Analysis Symposium (SAS 2015), Lecture Notes in Computer Science 9291, pp. 128-144, Springer, September, 2015. (査読有)

③ Hiroshi Unno and Tachio Terauchi. Inferring Simple Solutions to Recursion-free Horn Clauses via Sampling. In Proceedings of the 21st International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS 2015), Lecture Notes in Computer Science 9035, pp. 149-163, Springer, April, 2015. (査読有)

④ Tachio Terauchi and Hiroshi Unno. Relaxed Stratification: A New Approach to Practical Complete Predicate Refinement. In Proceedings of the 24th European Symposium on Programming (ESOP 2015), Lecture Notes in Computer Science 9032, pp. 610-633, Springer, April, 2015. (査読有)

⑤ Eric Koskinen and Tachio Terauchi. Local Temporal Reasoning. In Proceedings of the Joint Meeting of the 23rd EACSL Annual Conference on Computer Science Logic and the 29th Annual ACM/IEEE Symposium on Logic in Computer Science (CSL-LICS 2014), pp. 59:1-59:10, ACM, July, 2014. (査読有)

⑥ Hirotoshi Yasuoka and Tachio Terauchi. Quantitative Information Flow as Safety and Liveness Hyperproperties. Theoretical Computer Science, Vol.538, pp. 167-182, Elsevier, June, 2014. (査読有)

⑦ Takuya Kuwahara, Tachio Terauchi, Hiroshi Unno, and Naoki Kobayashi. Automatic Termination Verification for Higher-Order Functional Programs. In Proceedings of the 23rd European Symposium on Programming (ESOP 2014),

Lecture Notes in Computer Science 8410, pp. 392-411, Springer, April, 2014. (査読有)

〔学会発表〕(計 9 件)

① Tachio Terauchi. On Predicate Refinement Heuristics in Program Verification with CEGAR. The 3rd Workshop on Horn Clauses for Verification and Synthesis (HCVS 2016), Eindhoven, Netherlands, April 3rd, 2016. (招待講演)

② Tachio Terauchi. Temporal Verification of Higher-Order Functional Programs. Dagstuhl Seminar 16131: Language Based Verification Tools for Functional Programs, Dagstuhl, Germany, March 31st, 2016. (招待講演)

③ Tachio Terauchi. Temporal Verification of Higher-Order Functional Programs. NII Shonan Meeting Seminar 078: Higher-Order Model Checking, Shonan Village Center, Hayamamachi, Kanagawa, Japan, March 15th, 2016. (招待講演)

④ Nam Mai and Tachio Terauchi. Verification of Object-Oriented Programs via Refinement Types. The 13th Asian Symposium on Programming Languages and Systems (APLAS 2015), Pohang, Korea, November 30th, 2015. (ポスター発表)

⑤ Tachio Terauchi. Predicate Refinement Heuristics in Program Verification with CEGAR. NII Shonan Meeting Seminar 063: Semantics and Verification of Object-Oriented Languages, Shonan Village Center, Hayamamachi, Kanagawa, Japan, September 22nd, 2015. (招待講演)

⑥ 山本真輝, 寺内多智弘. 効率の良い Leakage Resilient プログラムの自動生成に向けて. 日本ソフトウェア科学会第 17 回プログラミングおよびプログラミング言語ワークショップ (PPL 2015), 道後プリンスホテル愛媛県松山市, 2015 年 3 月 4 日. (ポスター発表)

⑦ Tachio Terauchi. Information Flow Analysis and Applications to Computer Security. NII Shonan Meeting Seminar 065: Low-level Code Analysis and Applications to Computer Security, Shonan Village Center, Hayamamachi, Kanagawa, Japan, March 3rd, 2015. (招待講演)

⑧ 寺内多智弘. プログラム検証とインバリアント生成. 日本ソフトウェア科学会第 31 回大会, 名古屋大学東山キャンパス愛知県名古屋市, 2014 年 9 月 9 日. (招待講演)

⑨ Takuya Kuwahara, Tachio Terauchi, Hiroshi Unno, and Naoki Kobayashi. Automatic Termination Verification for Higher-Order Functional Programs. 日本ソフトウェア科学会 第 16 回プログラミングおよびプログラミング言語ワークショップ (PPL 2014), 阿蘇の司ビラパークホテル熊本県阿蘇市, 2014 年 3 月 6 日.

〔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
寺内 多智弘 (TERAUCHI TACHIO)
北陸先端科学技術大学院大学・先端科学技術研究科・教授
研究者番号：70447150

(2)研究分担者
(　　)

研究者番号：

(3)連携研究者
(　　)

研究者番号：

(4)研究協力者
(　　)