科学研究費助成事業（基盤研究（Ｓ））公表用資料
〔令和４(2022)年度 中間評価用〕

令和４年３月３１日現在

研究期間	：２０２０年度～２０２４年度
課題番号	：20H05703
研究課題名	：ＡＩ時代を見据えたプログラム検証技術
研究代表者氏名（ローマ字）	：小林 直樹（KOBAYASHI Naoki）
所属研究機関・部局・職	：東京大学・大学院情報理工学系研究科・教授
研究者番号	：00262155

研究の概要：

ソフトウェアの高信頼性を保証するためのプログラム検証技術は従来から重要であるが、近年の AI 技術の台頭によるソフトウェアの質の変化などへの対応を迫られつつある。そこで、本研究では高階モデル検査などのプログラム検証技術をさらに発展させ、そのボトルネックであった不変条件の発見などに機械学習を応用とともに、ソフトウェアの質の変化に対応するための研究にも取り組む。

研究分野：プログラム理論、プログラミング言語、機械学習

キーワード：高階モデル検査、プログラム検証、機械学習

１．研究開始当初の背景

ソフトウェアの高信頼性を保証するためのプログラム検証技術は従来から重要であるが、近年の AI 技術の台頭によって以下の観点から大きな変革を迫られつつある。（１）コンピュータによる社会システムの制御がますます進み、ソフトウェアの欠陥が従来以上に重要な影響を及ぼすため、ソフトウェアの信頼性保証のためのプログラム検証技術の重要性が増している。（２）一方で、プログラム検証は究極には定理証明の一種であり、その一部に AI 技術を活用することによって大きな進展が望める可能性がある。（３）人間に代わって AI によってソフトウェアが生成される時代が来ると、ソフトウェアの質および規模に大きな変化がもたらされ、これまでの検証技術では太刀打ちできなくなる可能性がある。

２．研究の目的

上記の背景をふまえ、本研究では研究代表者らがこれまで世界をリードして研究してきた高階モデル検査などのプログラム検証技術をさらに発展させつつ、そのボトルネックであった不変条件の発見などに機械学習を導入することによって上記（３）の「規模」の問題に対処するとともに、「質」の問題に対処するため、確率付きプログラムや機械学習コンポーネントを組み込んだソフトウェアなど、これまで十分に扱ってこなかったプログラム検証技術の研究に取り組む。

３．研究の方法

次の３つの大項目について並行して研究を進める。研究の比重は、A に 6 割、B と C に 2 割ずつを予定している。

(A) 高階モデル検査をはじめとするプログラム検証技術のさらなる発展。

高階モデル検査とは、有用なシステム検証手法としてチューリング賞の対象にもなった「モデル検査」の拡張であり、高レベル言語で記述されたプログラムの有効な検証手法として、本課題の代表者らが 10 年来、世界をリードして進展させてきたものである。高階モデル検査には HORS モデル検査と HFL モデル検査の 2 種類があり、当初は前者に基づいて研究を進めてきたが、最近になって HFL モデル検査に基づく手法がより有効であることが判明した。そこで本項目では、HFL モデル検査に基づくプログラム検証手法の確立・発展および他のプログラム検証手法との融合を進める。また、高階モデル検査の理論に関する重要な未解決問題にも取り組む。

(B) 機械学習技術のプログラム検証への応用。

高階モデル検査は理論上の最悪の計算コストが極めて高い検証手法であるが、これまでの高階モデル検査に関する研究の進展の結果、現在ではプログラム検証器の主なボトルネックは、高階モデル検査自体よりも検証対象のプログラムの近似に用いる述語の発見などの、ヒューリスティックスが関わる部分になっている。この部分に機械学習の技術を取り入れることでプログラム検証器の性能向上を目指す。

(C) 質の変化したプログラムの検証技術：

機械学習コンポーネントを組み込んだソフトウェアは、これまでのような人間が書いたソフトウェ

アとは質が異なる。例えば、機械学習コンポーネントが常に正しい答えを出力するわけではなく、確率的に振る舞うシステムとしてモデル化、検証する必要がある。そこで高階モデル検査の拡張として確率付き高階モデル検査の理論を構築するなどの研究を行う。また、実際に機械学習コンポーネントを組み込んだシステムの検証実験を通して新たな課題の洗い出しおよび対処を行う。

４．これまでの成果

項目 A については、HFL 方式に基づく新しいプログラム検証手法を考案・実装し、プログラムの安全性(エラー状態に陥らないこと)、停止性(プログラムがいかなる入力に対しても正常に停止すること)、非停止性、公平停止性など、さまざまなプログラムの性質を統一的に検証できる枠組み、ツール（高階不動点論理用妥当性検証器 MuHFL）の構築に成功した。従来の検証方式では、検証する性質ごとに異なる検証器を構築していたが、新方式に基づく検証器ではそれらすべての性質を統一的に扱え、かつ実験的にも、従来の個々の性質に特化した検証器を上回る性能が得られた[1]。以上の中心となる成果の他、(i) ポインタを持つプログラムの検証手法の考案[2]、(ii) HFL のような不動点論理における証明手法として有効な循環証明と、一階のモデル検査手法として主流の PDR との関係の理論的解明[3]、(iii)再帰データ型を持つプログラムの自動検証のための形式言語理論的アプローチ[4]、などについて研究を行い、大きな進展が得られた。

項目 B, C に共通する取り組みとして、ニューラルネットワークをグレイボックスとして用いて与えられた制約を充足する論理式を合成する、NeuGuS (Neural-Network-Guided Synthesis)という枠組みを考案した[5]。 この方式を実際にプログラム自動検証の鍵となる不変条件（ループの先頭や関数呼び出しの前後など、特定のプログラムポイントで常に成り立つ性質）の発見に応用し、プログラム検証器の性能向上を確認できた。さらに項目 C の一環として、(i)確率付き高階不動点論理に関する研究[6]、(ii)機械学習プログラムのテンソル形状の誤りを検出するための型システムの研究などを行い、大きな進展が得られた。

５．今後の計画

以下の通り、引き続き A～C の大項目について並行して研究を進める。また、それらの結果の集大成として、自動運転用のオープンソースソフトウェアなどを対象にソフトウェアの自動検証実験を行う。

A: 引き続き高階不動点論理 HFL などに基づくプログラム検証理論・技術の発展のために、(i)高階不動点論理妥当性検証器 MuHFL のさらなる改良および理論的基礎の補強、(ii)大規模プログラムの検証のための分割検証手法、(iii)ポインタやオブジェクト、並行プリミティブを用いる、広範囲のプログラムの自動検証、などについて研究を進める。

B: NeuGuS の枠組みをさらに発展させ、再帰データ型等を含むより広いクラスのプログラムの不変条件の発見に、機械学習技術を応用する。

C: 機械学習コンポーネントを含んだソフトウェアシステムの検証のために、ニューラルネットワークから論理式を合成する NeuGuS の枠組みをさらに拡張し、再帰の入ったプログラムの合成するための手法を考案する。これによって、機械学習コンポーネント部分を通常のプログラムに置き換えることができ、項目 A および B で発展させるプログラム自動検証手法が適用可能になると期待される。

６．これまでの発表論文等（受賞等も含む）

[1] Kento Tanahashi, Naoki Kobayashi, Ryosuke Sato, “Automatic HFL(Z) Validity Checking for Program Verification”, CoRR abs/2203.07601, 32 pages, 2022

[2] Yusuke Matsushita, Takeshi Tsukada, and Naoki Kobayashi, “RustHorn: CHC-based Verification for Rust Programs”, ACM Trans. Program. Lang. Syst. 43(4), pp.15:1-15:54, 2021

[3] Takeshi Tsukada and Hiroshi Unno, “Software Model-Checking as Cyclic-Proof Search”, Proceedings of the ACM on Programming Languages (POPL 2022), Volume 6, Issue POPL, ACM, pp.63:1-63:29, January 2022.

[4] Takumi Shimoda, Naoki Kobayashi, Ken Sakayori, and Ryosuke Sato, “Symbolic Automatic Relations and Their Applications to SMT and CHC Solving”, Proceedings of SAS 2021, Springer LNCS 12913, pp.405-428, 2021

[5] Naoki Kobayashi, Taro Sekiyama, Issei Sato, and Hiroshi Unno, “Toward Neural-Network-Guided Program Synthesis and Verification”, Proceedings of SAS 2021, Springer LNCS 12913, pp.236-260, 2021

[6] Yo Mitani, Naoki Kobayashi, and Takeshi Tsukada, “A Probabilistic Higher-order Fixpoint Logic”, Logical Methods in Computer Science, December 2, 2021, Volume 17, Issue 4

7. ホームページ等

https://www-kb.is.s.u-tokyo.ac.jp/~koba/hmcai/