科学研究費助成事業（基盤研究（Ｓ））公表用資料
〔平成３０年度研究進捗評価用〕

平成２７年度採択分
平成３０年３月８日現在

高階モデル検査の深化と発展

Refinement and Extension of Higher-Order Model Checking

課題番号：15H05706

小林　直樹（KOBAYASHI NAOKI）

東京大学・大学院情報理工学系研究科・教授

研究の概要

システム検証手法であるモデル検査の一般化の高階モデル検査について、その理論を発展させるとともに、それに基づくプログラム検証やデータ圧縮への応用を行う。理論面では高階モデル検査の計算量の量的評価や高階文法の未解決問題に取り組み、応用面では、これまでよりも大規模かつ広範囲のプログラムの自動検証を可能にする。

研　究　分　野：理論計算機科学

キ　ー　ワ　ー　ド：プログラム検証、高階モデル検査、データ圧縮

１．研究開始当初の背景

交通や金融システムなどの様々な重要な社会基盤が計算機によって制御されている今日、計算機システム、とりわけソフトウェアの信頼性の担保が重要な課題である。本課題で扱う高階モデル検査は、システム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モデル検査の一般化であり、従来の有限状態モデル検査よりも強力で大きな可能性を秘めている。

研究開始当初の時点で、我々は、世界初の高階モデル検査器を実現するとともに、その上に関数型プログラムの全自動検証器を構築し、その有用性を示していた。また、データをそれを生成するプログラムの形に圧縮することにより、高階モデル検査の理論を用いて、圧縮したままの形で検索などの様々な操作を施せることも示していた。

２．研究の目的

本課題では、これらの成果をさらに飛躍的に発展させ、高階モデル検査の理論的基盤を確固たるものにするとともに、自動検証できるプログラムの規模、高階モデル検査に基づくデータ圧縮の性能などを飛躍的に増大させることを目指す。

３．研究の方法

以下の４つの柱を設け、それらについて並行して研究を進めた。

（１）高階モデル検査の理論の整備

高階モデル検査とは、高階再帰スキームと呼ばれる木文法によって生成される無限木の性質を判定する問題であるが、この木文法について重要な未解決問題が残っており、その解決に取り組む。また、高階モデル検査問題が一般には多重指数完全という計算量理論的には手に負えない問題のクラスに属しながらも、多くの入力に対して現実的な時間で解けることについて、理論的な保証を与えることを目指す。また、それらの理論的結果を基に、高階モデル検査アルゴリズムのさらなる高速化を目指す。

（２）関数型プログラムの自動検証への応用

関数型プログラムの様々な検証問題を高階モデル検査問題に帰着することにより、関数型プログラムの全自動検証器を構築することができる。研究開始当初の時点ですでにそのような検証器 MoCHi を構築済みだが、これをさらに改良し、扱えるプログラムのサイズや機能、検証する性質を拡げる。

（３）拡張高階モデル検査とオブジェクト指向・並行プログラムの検証への応用

高階モデル検査をさらに拡張した、拡張高階モデル検査のための効率のよい手法を考案し、それを基にオブジェクト指向プログラムや並行プログラムの全自動検証器を構築する。

（４）データ圧縮への応用

研究目的の項で述べたとおり、高階モデル検査の理論を用いることにより、プログラム形式で圧縮されたデータを、解凍することなく、様々な操作を施すことができる。この考え方に基づいたデータの圧縮・変換器のプロトタイプは作成ずみだが、本課題ではこれをさらに改良し、実用的なレベルの圧縮・変換

器を作成するとともに、その知識発見などへの応用を目指す。

４．これまでの成果

前項の４つの柱ごとにこれまでの主要成果を記述する。

（１）高階文法に関する未解決問題として、オーダー３の言語の反復補題を証明するとともに、任意のオーダーについてもある予想（クラスカルの木定理の高階版）の下に成立することを証明した[4]。これまで知られていた結果は 1973 年の林によるオーダー２の言語の場合であり、40 年以上ぶりに進展が得られた。また、高階モデル検査の計算量の量的評価への取り組みとして、関連する問題である型付きラムダ項の簡約列の長さの量的評価に成功した[3]。さらに、高階モデル検査アルゴリズムの改良を行い、入力によっては数十万行からなる問題を数分で解けるなど、既存の高階モデル検査器に比べて飛躍的な性能向上を達成した。

（２）関数型プログラムの自動検証への応用として、(a)検証できるプログラム規模の拡大、(b)検証できる性質の拡充、に取り組んだ。(a)については、分割検証手法などの研究に取り組み[2]、千行規模のプログラムの自動検証に成功した。(b)については、活性（いずれ○○がおきる）など、これまで扱えなかった性質を検証する手法の開発に成功した[7]。

（３）新しい拡張高階モデル検査（μHORS モデル検査）アルゴリズムを考案し、それに基づくモデル検査器を実装して、既存のμHORS モデル検査器よりも大幅な性能向上を達成した。また、本課題の対象としていた HORS モデル検査と,もう一つの高階モデル検査の概念である HFL モデル検査との間に密接な関係があることを発見した。さらにそれに基づいて、拡張 HFL モデル検査を用いることによってプログラムの様々な性質の検証を統一的に行えることを発見した[1,5]。

（４）高階圧縮アルゴリズムおよびその要素技術の改良を進めた[8]。また、圧縮を通した知識発見の可能性を検討するため、自然言語の文章を題材として、圧縮を通して自然言語の文法が得られるかどうかの実験を行った。現在のところ肯定的な結果は得られていないが、形式言語の学習アルゴリズムなどを組み合わせて引き続き検討を行っている。

５．今後の計画

上記４本の柱にそって引き続き研究を続ける。（１）の高階モデル検査の理論については、一般の場合の反復補題で仮定しているクラスカルの木定理の高階版の証明に取り組む。また、ラムダ項の簡約列の長さに関する結果を拡張して高階モデル検査の計算量の量的評価に取り組む。（２）については、一万行規模の大規模プログラムの検証実験を行いながら分割検証などの要素技術の改良を続ける。（３）については、千行規模のオブジェクト指向プログラムの検証実験に取り組むとともに、拡張 HFL モデル検査に基づく統一的プログラム検証の枠組みを確立する。（４）のデータ圧縮への応用については、引き続き圧縮アルゴリズムの改良を行うとともに、自然言語文章を対象とした知識発見と高階圧縮の関係の解明を行う。

６.これまでの発表論文等(受賞等も含む)

[1] Naoki Kobayashi, Takeshi Tsukada, and Keiichi Watanabe, Higher-Order Program Verification via HFL Model Checking, Proceedings of ESOP 2018, Springer LNCS, 2018, 掲載決定.

[2] Ryosuke Sato and Naoki Kobayashi, Modular Verification of Higher-Order Functional Programs. ESOP 2017, Springer LNCS 10201, pp.831-854, 2017.

[3] Ryoma Sinya, Kazuyuki Asada, Naoki Kobayashi, and Takeshi Tsukada, Almost Every Simply Typed λ-Term Has a Long β-Reduction Sequence, FoSSaCS 2017, Springer LNCS 10203, pp. 53-68, 2017

[4] Kazuyuki Asada and Naoki Kobayashi, Pumping Lemma for Higher-order Languages. Proceedings of ICALP 2017, LIPIcs 80, pp.97:1-97:14, 2017.

[5] Naoki Kobayashi, Étienne Lozes, and Florian Bruse, On the relationship between higher-order recursion schemes and higher-order fixpoint logic. Proceedings of POPL 2017, pp.246-259, 2017.

[6] Naoki Kobayashi, On Two Higher-Order Extensions of Model Checking, FTSCS 2016, Tokyo, Japan, November 14, 2016, 招待講演.

[7] Akihiro Murase, Tachio Terauchi, Naoki Kobayashi, Ryosuke Sato, and Hiroshi Unno, Temporal verification of higher-order functional programs, Proceedings of POPL 2016, pp.57-68, 2016.

[8] Kotaro Takeda, Naoki Kobayashi, Kazuya Yaguchi, and Ayumi Shinohara, Compact bit encoding schemes for simply-typed lambda-terms, Proceedings of ICFP 2016, pp.146-157, 2016.

[9] Naoki Kobayashi and Xin Li, Automata-Based Abstraction Refinement for μHORS Model Checking,Proceedings of LICS 2015, pp.713-724, 2015

ホームページ等:
http://www-kb.is.s.u-tokyo.ac.jp/~koba/hmc