平成２３年度採択分
平成２６年３月２４日現在

高階モデル検査とその応用

Higher-Order Model Checking and its Applications

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

高階モデル検査は、システム検証手法であるモデル検査の一般化であり、最近になってその有用性が代表者の小林らによって明らかにされた。本研究では高階モデル検査の理論を発展させ、それに基づいて高速な高階モデル検査器を構築するとともに、その応用として、高レベルプログラムの自動検証器の構築、データ圧縮への応用などを行う。

研　究　分　野：総合領域

科研費の分科・細目：情報学・情報学基礎

キ　ー　ワ　ー　ド：プログラム理論、プログラム検証

１．研究開始当初の背景

近年、交通システムや金融システムなど、重要な社会基盤がコンピュータによって制御されており、ソフトウェアの信頼性が重用になっている。モデル検査は、ソフトウェアの検証手法として有望視されている手法の一つであるが、従来のモデル検査は、検証対象として用いる数学的モデルの表現力が弱く、高レベル言語で記述されたソフトウェアの検証には適さない。

そこで我々は、数年前まで理論家の間で純粋に理論的な興味から研究されていた高階モデル検査と呼ばれる従来のモデル検査の拡張に着目し、最近になって、（１）プログラム検証問題の多くが高階モデル検査問題に帰着できること、（２）高階モデル検査の最悪の入力に対する計算コストが極めて高い（n 重指数完全）にもかかわらず多くの入力に対して効率よく解くことができることを示し、世界初の高階モデル検査器の実現、およびそれに基づくプログラム自動検証器の試作に成功した。

２．研究の目的

本研究では、上記の高階モデル検査の研究をさらに推進し、高階モデル検査の理論を発展させて高速な高階モデル検査器を実現すること、およびその応用として、高レベルプログラムの自動検証器の構築、データ圧縮など他の分野への応用も試みる。

３．研究の方法

以下の３つの柱を設け、それらについて並行して研究を進める。

（１）高階モデル検査の理論および実装技術

高階モデル検査の理論をさらに発展させ、それに基づいて高階モデル検査のアルゴリズムおよび実装技術を改良する。また、高階モデル検査に関連するいくつかの未解決問題にも取り組む。

（２）プログラムの自動検証への応用

すでに試作済みの高階モデル検査に基づくプログラム自動検証器を拡張し、より効率が良く、再帰データ型やオブジェクトなど多くのプログラミング言語機能を扱えるものにする。

（３）データ圧縮への応用

テキスト文書、XML 文書、ゲノム配列などの文字列や木構造データを、それを生成するプログラムの形で圧縮することにより、高い圧縮率が期待できるとともに、高階モデル検査に基づいて圧縮データを展開することなくパターンマッチなどの操作を施すことが可能である。また、データを極限まで圧縮することによってそこからデータに隠された知識を発見できる可能性もある。

４．これまでの成果

前項の３つの項目に分けてこれまでの主要成果を記述する。

（１）高階モデル検査の理論および実装技術

新しい高階モデル検査アルゴリズムおよびそれに基づくモデル検査器 HorSat を構築した。これは我々自身が以前に開発していた TRecS や GTRecS を大きく上回る性能を示し、入力によっては 1000 倍以上の性能向上を達成している。

また、高階モデル検査の検証対象のモデルである高階文法の性質に関する理論的性質の解明を行い、反復補題や文脈依存文法との関連など、未解決問題の部分的解決や既存の結果の簡明な別証を与えることに成功した。

（2）プログラムの自動検証への応用

研究開始当初、整数とブール値を扱うプログラムのみしか扱えなかった関数型プログラム用自動検証器 MoCHi を拡張し、リストや木などのデータ構造や例外処理などの言語機能を扱えるようにし、より広範囲の関数型プログラムの自動検証を可能にした。また、検証する性質として、これまでのアサーション検査のみならず、フロー情報、停止性、関数の等価性など広範囲の性質を高階モデル検査を用いて検証する手法を確立した。加えて、検証手法の改良を行い、ある仮定の下での検証手法の（相対）完全性を示した。

さらに、高階モデル検査のモデルに再帰型を加えて拡張した「拡張高階モデル検査」のアルゴリズムを考案し、それに基づいて（副作用のない）オブジェクト指向プログラムの自動検証器の構築にも成功した。

（3）データ圧縮への応用

木構造データを、それを生成する関数型プログラムの形で表現することにより、理論的に最適な圧縮率が得られることを示すとともに、高階モデル検査を用いることで、圧縮データに対する文字列検索、パターンマッチ、置換などの操作をデータを展開することなしに高速に行えることを示した。

また、上記の理論を実証するため、実際に木構造データを関数型プログラムの形に圧縮するアルゴリズムの開発、高階モデル検査器の拡張による圧縮データの変換器の構築、などを行った。さらに、データ圧縮アルゴリズムをゲノム配列などに適用し、入力によっては既存の文法圧縮手法を上回る圧縮率が得られることを確認した。

以上の成果は、コンピュータサイエンス分野のトップジャーナルである Journal of the ACM に掲載された 60 ページ以上にわたる論文、プログラム理論分野のトップ国際会議である POPL や LICS に採択された論文などで発表済みである。また、構築したプログラム自動検証器などは、ホームページから試すことができるようにしている。

５．今後の計画

上記 3 本の柱にそって引き続き研究を続け、高階モデル検査および高階文法の理論を整備しながら、高階モデル検査器やその上のプログラム全自動検証器の拡張・改良を行う。研究期間の終わりまでに 1 万行規模の高階文法に対するモデル検査、1000 行規模の関数型プログラムの自動検証を達成することを目指す。理論面では高階文法に関する残された未解決問題の解決、高階モデル検査の計算量に関するより詳しい分析を試みる。

データ圧縮については、圧縮性能の向上とともに、圧縮を通してゲノムデータや自然言語の文章からの知識発見への応用も試みる。

６．これまでの発表論文等（受賞等も含む）

[1] Naoki Kobayashi, Kazutaka Matsuda, Ayumi Shinohara, and Kazuya Yaguchi, Functional programs as compressed data, Higher-Order and Symbolic Computation, Special Issue on PEPM 2012, 46 pages, 2014.

[2] Naoki Kobayashi, Model Checking Higher-Order Programs, Journal of the ACM, 60(3:20), 62 pages, 2013.

[3] Christopher H. Broadbent, and *Naoki Kobayashi, Saturation-Based Model Checking of Higher-Order Recursion Schemes, Proceedings of CSL 2013, pp.129-148, 2013.

[4] Naoki Kobayashi and Atsushi Igarashi, Model-Checking Higher-Order Programs with Recursive Types, Proceedings of ESOP 2013, Springer LNCS 7792, pp.431-450, 2013.

[5] Hiroshi Unno, Tachio Terauchi, and Naoki Kobayashi, Automating relatively complete verification of higher-order functional programs, Proceedings of POPL 2013, pp. 75-86, 2013.

[6] Naoki Kobayashi, Program Certification by Higher-Order Model Checking, Second International Conference on Certified Programs and Proofs (CPP 2012), 招待講演, 2012 年 12 月.

[7] Naoki Kobayashi, Higher-Order Model Checking: From Theory to Practice, the 26th Annual IEEE Symposium on Logic in Computer Science (LICS 2011), 招待講演, 2011 年 6 月.

ホームページ等

http://www-kb.is.s.u-tokyo.ac.jp/~koba/hmc