東京大学
担当部署連絡先：研究推進部研究資金戦略課　Kakenhi.adm@gs.mail.u-tokyo.ac.jp
作成日：2020年　2月19日
更新日：―
科研費 KAKENHI

ソフトウェアの全自動検証を目指して

研究者所属・職名：
大学院情報理工学系研究科・教授

ふりがな　こばやし　なおき
氏名：小林　直樹

主な採択課題：
- 基盤研究(A)「ソフトウェアの安全性向上のための型理論の深化と応用」(2008-2010)
- 基盤研究(S)「高階モデル検査とその応用」(2011-2015)
- 基盤研究(S)「高階モデル検査の深化と発展」(2015-2019)

分野：情報学基礎、ソフトウェア

キーワード：プログラム検証、高階モデル検査、関数型プログラム、データ圧縮

課題

●なぜこの研究をおこなったのか？（研究の背景・目的）
現代では、金融システムから交通システムに至るまで世の中の重要な社会基盤の多くがコンピュータによって制御されている。この傾向は空前のAIブームの高まりとともに今後ますます強まるものと予想され、コンピュータに対する指令書であるソフトウェアの信頼性が今後さらに重要となる。そこで本研究では、ソフトウェアが期待通りの動作を行うことを、高階モデル検査をはじめとする様々な数理科学的手法を用いて自動検証を行うことを目指している。

●研究するにあたっての苦労や工夫（研究の手法）
システムの自動検証のための代表的な手法として有限状態モデル検査と呼ばれるものがあり、「コンピュータサイエンス分野のノーベル賞」と呼ばれるチューリング賞を2007年に提唱者らが受賞しているが、高レベルソフトウェアの検証には非力であった。本研究では、有限状態モデル検査の本質的な拡張であり、当初は理論家の間のみで興味を持たれていた「高階モデル検査」に着目し、それをソフトウェアの自動検証に応用した。高階モデル検査は多重指数完全問題と呼ばれる現実的な時間では解けないとされている問題のクラスに属するため、それをいかに克服するかが大きな壁であった。

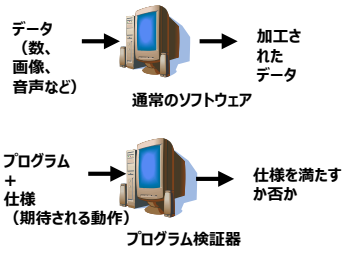

図1　プログラム検証のイメージ図

東京大学
担当部署連絡先：研究推進部研究資金戦略課　Kakenhi.adm@gs.mail.u-tokyo.ac.jp

作成日：2020年　2月19日
更新日：―

ソフトウェアの全自動検証を目指して

研究成果

●どんな成果がでたか？どんな発見があったか？

2009年に、それまで理論家の間でのみ着目されていた高階モデル検査が、実はソフトウェアの自動検証に有効であることを世界に先駆けて示した。同じ年に、現実的な時間では解くことができないと考えられていた高階モデル検査について、典型的な問題については効率よく解くことができるようなアルゴリズムを世界に先駆けて示し、世界初の高階モデル検査ツールTRecSの開発に成功した。2011年には、TRecSを利用した関数型プログラムの全自動検証器（プログラムを入力し、ボタンを押すだけでプログラムにバグがあるか否かを全自動で検証するツール）MoCHiの開発に成功した（図2）。

その後も高階モデル検査ツールおよびMoCHiの改良を続け、2013年には、より優れた高階モデル検査アルゴリズムを発見し、それに基づく新しい高階モデル検査ツールHorSatの開発に成功している。現在、その改良版であるHorSat2が世界で最速の高階モデル検査ツールである。その他の様々な研究成果を積み重ねた結果、現在では、簡単な仕様の検証であれば、数百から千行程度のプログラムの全自動検証も可能になってきている。

さらに、高階モデル検査に関する研究の副産物として、データ圧縮への応用が得られた。文字列や木構造データなどをそれを生成するプログラムの形で圧縮することによって理論的には最適な圧縮率が得られることは以前から知られていたが、高階モデル検査の発展・応用することによって、そのように得られた圧縮データを解凍することなく、圧縮されたままの形で検索やデータの変換などを行えることがわかった（図3）。

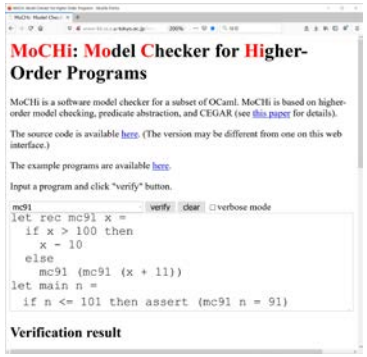

図2　全自動プログラム検証器MoCHiのWebインターフェース画面

今後の展望

●今後の展望・期待される効果

上で述べたソフトウェアの自動検証の成果はコンピュータによって制御されるシステムの信頼性向上にとって役立つものであり、データ圧縮に関する成果は今後ますます加速するビッグデータ時代における効率的なデータの格納・処理に役立つものと期待できる。

ただし実用化の観点からは研究はまだ道半ばであり、理論と実践の両面から今後さらに研究を加速させていきたいと考えている。

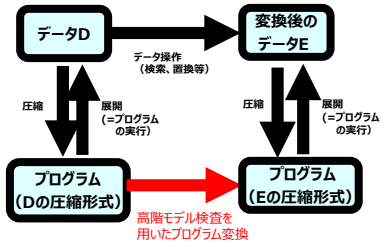

図3　データ圧縮への応用