

## 【基盤研究(S)】

### 総合・新領域系（総合領域）



#### 研究課題名 高階モデル検査とその応用

東北大学・大学院情報科学研究科・教授

こばやし なおき  
小林 直樹

研究分野：計算機科学

キーワード：プログラム検証、モデル検査、型理論

#### 【研究の背景・目的】

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、従来のモデル検査手法は、用いて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、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。本研究では、この高階モデル検査についての研究をさらに推進し、ソフトウェアの自動検証への応用のみならず、データ圧縮など他の分野への応用も試みる。

#### 【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) プログラム自動検証器の構築

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) 高階モデル検査の新しい応用分野の確立

高階モデル検査のプログラム検証以外にも多くの応用の可能性を探る。例えば、テキスト文書やXML文書、ゲノム配列など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。

#### 【期待される成果と意義】

本研究の遂行により、高階モデル検査に基づくソフトウェア検証という新しいソフトウェア検証技術を確認し、ソフトウェアの信頼性向上に貢献できると期待できる。また、学問的にも、本研究で扱う高階モデル検査とプログラム検証手法は、形式言語とオートマトン、型理論、モデル検査、ゲーム意味論、自動定理証明、プログラム変換など理論計算機科学の多岐にわたる分野を組み合わせ実現されており、本研究の遂行によって理論計算機科学分野の幅広い発展が期待できる。さらに、データ圧縮および知識発見への応用を通して、自然言語処理、ゲノム解析など他の学問分野への波及効果が得られる可能性がある。

#### 【当該研究課題と関連の深い論文・著書】

- Naoki Kobayashi, Types and Higher-Order Recursion Schemes for Verification of Higher-Order Programs, Proceedings of the 36<sup>th</sup> ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL 2009), pp.416–428, 2009.
- Naoki Kobayashi, Model-Checking Higher-Order Functions, Proceedings of the 11th International ACM SIGPLAN Conference on Principles and Practice of Declarative Programming (PPDP'09), pp. 25–36, 2009.

#### 【研究期間と研究経費】

平成23年度–27年度  
105,800千円

#### 【ホームページ等】

<http://www.kb.ecei.tohoku.ac.jp/>