様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２８ 年　 ５ 月 ３０ 日現在

機関番号：１２６０１
研究種目：基盤研究(S)
研究期間：2011～2014
課題番号：２３２２０００１

研究課題名（和文）高階モデル検査とその応用

研究課題名（英文）Higher-Order Model Checking and its Applications

研究代表者
小林　直樹（Kobayashi, Naoki）

東京大学・情報理工学（系）研究科・教授

研究者番号：００２６２１５５

交付決定額（研究期間全体）：（直接経費）　　83,500,000円

研究成果の概要（和文）：本研究の中心テーマである高階モデル検査とは、代表的なシステム検証手法であるモデル検査の拡張であり、2009年に研究代表者の小林によって初めて現実的な高階モデル検査アルゴリズムおよびプログラム検証への応用が見出された。本研究課題はその結果を受けて行った研究であり、高階モデル検査器の大幅な高速化、高階モデル検査に基づく全自動プログラム検証器の構築、高階モデル検査のデータ圧縮への応用（データをそれを生成する関数型プログラムの形に圧縮し、圧縮したままのデータ操作を実現）などの成果を得た。

研究成果の概要（英文）：The main topic of this research project was higher-order model checking, which is an extension of model checking, a representative method for system verification. In 2009, Kobayashi, the leader of this project, has developed the first practical algorithm for higher-order model checking, and also shown that higher-order model checking is useful for program verification. This research project has been launched to extend his results. The major results include: the development of much faster higher-order model checkers, implementation of fully-automated tools for program verification, and applications to data compression (where data are compressed in the form of functional programs that generate them, and compressed data are manipulated without decompression).

研究分野：プログラミング言語

キーワード：高階モデル検査　プログラム検証　データ圧縮　高階文法　型システム

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要になっている。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た。

（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。それらを理論的に定式化するとともに実験によって有効性を検証する。

４．研究成果

前項の３つの項目に分けて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 およびそのさらなる改良版である HorSatZDD を構築した（論文⑰、⑦）。これら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た。HorSatZDD については、入力文法のサイズに対して固定パラメタ線形時間で動作するようにアルゴリズムを設計・実装し、実験的にそれを確認した。さらに、従来の高階モデル検査器が自明木オートマトンと呼ばれる、高階モデル検査の理論上扱える交代パリティ木オートマトンよりも小さなクラスのオートマトンで表現された性質しか扱えなかったのに対し、任意の交代パリティ木オートマトンを扱える高階モデル検査アルゴリズムおよびモデル検査器 APTRecS の開発にも成功した（論文⑯）。また、値呼び関数型プログラムの検証問題をより直接的に扱うため、高階モデル検査問題の変種として、値呼び高階ブーリアン関数プログラムの到達可能性問題を考え、この計算量が型の深さ n に関して n 重指数完全であることを証明した（論文⑫）。

以上の研究と並行して、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についての研究を行った。高階文法にはオーダーという指標があり、オーダーによって言語クラスが階層構造をなす。オーダー０、オーダー１、オーダー２の言語クラスがそれぞれ正規言語、文脈自由言語、インデックスト言語のクラスと一致することは知られていたが、それ以上のオーダーの言語クラスとチョムスキーの言語階層で文脈自由言語のクラスの上に位置する文脈依存言語のクラスとの関係はわかっていなかった。それに対し、我々は、オーダー３の高階文法によって生成される言語がすべて文脈依存言語に含まれることの証明に成功した（論文⑪）。また、無限木を生成する高階文法である高階再帰スキームの反復補題について、共通型の理論を用いて従来より簡明な別証を得ることに成功した（論文⑲）。

（２）プログラムの自動検証への応用
研究開始時点ですでに高階モデル検査に基づく関数型プログラム全自動検証器 MoCHi の開発に成功していたが、その時点では整数とブール値を扱う数行程度のプログラムのみしか扱えなかった。本研究において、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 MoCHi を拡張するとともに、高階モデル検査への帰着で必要となる述語発見手法なども改良し、より広範囲かつ大きな関数型プログラムの自動検証を可能にした（論文③、④、⑳、㉙）。また、検証できるプログラムの性質として、従来扱っていた到達可能性に加え、フロー情報、停止性、

関数の等価性など、より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（論文①、②、⑤、⑥、⑩、⑬、㉓）。さらに、関数引数の自動追加などの検証手法の改良を行い、改良後の検証手法がある仮定の下で（相対）完全性を満たすことを理論的に示すとともに、改良手法に基づいて実際に自動検証器 MoCHi を拡張し、より多くのプログラムの自動検証を可能にした（論文㉑）。また、関数型プログラム以外への応用として、高階モデル検査がロックを同期プリミティブとして持つマルチスレッドプログラムの自動検証にも適用可能であることを示した（論文⑧）。
さらに、一般の並行プログラムやオブジェクト指向プログラムの自動検証を可能にするため、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」問題を考え、その手続き（決定不能問題であるため、完全な「アルゴリズム」は存在しない）を与え、それがある種の相対完全性を満たすことを証明した。さらに、提案手続きに基づいて実際に拡張高階モデル検査器を構築し、その上に（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を構築した（論文⑱）。

（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、高階モデル検査およびその拡張を用いることで、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（論文㉒、㉔）。
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。圧縮については、文法圧縮アルゴリズムの一つである RePair のアルゴリズムにヒントを得て、入力データに対してほぼ線形時間で動作する高階圧縮アルゴリズムを得た。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（論文⑭）。

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。

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 29 件）

① Hiroshi Unno, Naoshi Tabuchi, Naoki Kobayashi, Verification of tree-processing program via higher-order mode checking, Mathematical Structures in Computer Science 25, pp.841-866, 2015（査読有）
DOI: 10.1017/S0960129513000054

② Takuya Kuwahara, Ryosuke Sato, Hiroshi Unno, Naoki Kobayashi, Predicate Abstraction and CEGAR for Disproving Termination of Higher-Order Functional Programs, Proceeding of CAV 2015, LNCS 9207, pp.287-303, 2015(査読有)
DOI: 10.1007/978-3-319-21668-3_17

③ Hiroshi Unno and Tachio Terauchi, Inferring Simple Solutions to Recursion-free Horn Clauses via Sampling, Proceedings of TACAS 2015, LINCS 9035, pp.149-163, 2015 (査読有)
DOI: 10.1007/978-3-662-46681-0_10

④ Tachio Terauchi and Hiroshi Unno, Relaxed Stratification: A New Approach to Practical Complete Predicate Refinement, Proceedings of ESOP 2015, LNCS 9032, pp.610-633, 2015 (査読有)
DOI: 10.1007/978-3-662-46669-8_25

⑤ 松本　雄磨、小林　直樹, 海野　広志、高階木変換器の自動検証のための反例発見と抽象化改良、コンピュータ・ソフトウェア　32(1), pp.161-178, 2015 (査読有)
DOI: 10.11309/jssst.32.1_161

⑥ Hiroshi Unno, Naoshi Tabuchi, and Naoki Kobayashi, Verification of Tree-Processing Programs via Higher-Order Model Checking, Mathematical Structures in Computer Science 25(4), APLAS 2010 special issue, pp.841-866, 2015（査読有）
DOI: 10.1017/S0960129513000054

⑦ Taku Terao, Naoki Kobayashi, A ZDD-Based Efficient Higher-Order Model Checking Algorithm, Proceedings of APLAS 2014, LNCS 8858, pp.354-371, 2014 (査読有)
DOI: 10.1007/978-3-319-12736-1_19

⑧ Kazuhide Yasukata, Naoki Kobayashi, Kazutaka Matsuda, Pairwise Reachability Analysis for Higher Order Concurrent Programs by Higher-Order Model Checking. Proceedings of CONCUR 2014, LNCS 8704, pp. 312-326, 2014 (査読有).

⑨ Elena Giachino, Naoki Kobayashi, Cosimo Laneve, Deadlock Analysis of Unbounded Process Networks,

Proceedings of CONCUR 2014, LNCS 8704, pp.63-77, 2014 (**査読有**)
DOI: 10.1007/978-3-662-44584-6_6

⑩ Kazuyuki Asada, Ryosuke Sato, Naoki Kobayashi, Verifying Relational Properties of Functional Programs by First-Oder Refinement, Proceedings of PEPM 2015, pp.61-72, 2014(**査読有**)
DOI: 10.1145/2678015.2682546

⑪ Naoki Kobayashi, Kazuhiro Inaba, and Takeshi Tsukada, Unsafe Order-2 Tree Languages are Context-Sensitive, Proceedings of FOSSACS 2014, Springer LNCS 8412, pp.149-163, 2014（**査読有、**EATCS Best Paper Award **を受賞**）
DOI:10.100/978-3-642-54830-7_10

⑫ Takeshi Tsukada and Naoki Kobayashi, Complexity of Model-Checking Call-by-Value Programs, Proceedings of FOSSACS 2014, Springer LNCS, pp.180-194, 2014. （**査読有**）
DOI: 10.1007/F978-3-642-54830-7_12

⑬ Takuya Kuwahara, Tachio Terauchi, Hiroshi Unno and Naoki Kobayashi, Automatic Termination Verification for Higher-Order Functional Programs, Proceedings of ESOP 2014, Springer LNCS 8410, pp.392-411, 2014 （**査読有**）
DOI:10.1007/978-3-642-54833-8_21

⑭ Kazuya Yaguchi, Naoki Kobayashi, and Ayumi Shinohara, Efficient Algorithm and Coding for Higher-Order Compression (poster presentation), Proceedings of Data Compression Conference (DCC 2014), 434, 2014（**査読有**）
DOI: 10.1109/DCC.2014.63

⑮ Naoki Kobayashi, Model Checking Higher-Order Programs, Journal of the ACM, 60(3:20), 62 pages, 2013（**査読有**)
DOI: 10.1145/2487241.2487246

⑯ Koichi Fujima, Sohei Ito, and Naoki Kobayashi, Practical Alternating Parity Tree Automata Model Checking of Higher-Order Recursion Schemes, Proceedings of APLAS 2013, Springer LNCS 8301, pp.17-32, 2013. （**査読有**）
DOI: 10.1007/978-3-319-03542-0_2

⑰ Christopher H. Broadbent, and Naoki Kobayashi, Saturation-Based Model Checking of Higher-Order Recursion Schemes, Proceedings of CSL 2013, pp.129-148, 2013. （**査読有**）
DOI: 10.4230/LIPIcs.CSL.2013.129

⑱ Naoki Kobayashi and Atsushi Igarashi, Model-Checking Higher-Order Programs with Recursive Types, Proceedings of ESOP 2013, Springer LNCS 7792, 431-450, 2013（**査読有**）
DOI:10.1007/978-3-642-37036-6_24

⑲ Naoki Kobayashi, Pumping by Typing, Proceedings of LICS 2013, pp.398-407, 2013. (**査読有**)
DOI:10.1109/LICS.2013.46

⑳ Ryosuke Sato, Hiroshi Unno, and Naoki Kobayashi, Towards a scalable software model checker for higher-order programs, Proceedings of PEPM 2013, pp.53-62, 2013. （**査読有**）
DOI:10.1145/2426890.2426900

㉑ Hiroshi Unno, Tachio Terauchi, and Naoki Kobayashi, Automating relatively complete verification of higher-order functional programs, Proceedings of POPL 2013, pp.75-86, 2013. (**査読有**)
DOI: 10.1145/2480359.2429081

㉒ Naoki Kobayashi, Kazutaka Matsuda, Ayumi Shinohara, and Kazuya Yaguchi, Functional programs as compressed data, Higher-Order and Symbolic Computation 25(1), Special Issue on PEPM 2012, pp.39-84, 2012 （**査読有**）
DOI: 10.1007/10990-013-9093-z

㉓ Yoshihiro Tobita, Takeshi Tsukada, and Naoki Kobayashi, Exact Flow Analysis by Higher-Order Model Checking, Proceedings of FLOPS 2012, LNCS 7294, .pp.275-289.(**査読有**)
DOI: 10.1007/978-3-642-29822-6_22

㉔ Takeshi Tsukada, and Naoki Kobayashi, An Intersection Type System for Deterministic Pushdown Automata. Proceedings of IFIP TCS 2012, pp.357-371, 2012. (**査読有**)
DOI: 10.10078978-3-642-33475-7_25

㉕ Naoki Kobayashi, Kazutaka Matsuda, and Ayumi Shinohara, Functional programs as compressed data. Proceedings of PEPM 2012, pp. 121-130, 2012. (**査読有**)
DOI: 10.1145/2103746.2103770

㉖ Kohei Suenaga, Ryota Fukuda, and Atsushi Igarashi, Type-based safe resource deallocation for shared-memory concurrency, Proceedings of the ACM Conference on Object-Oriented Programming, Systems, Languages, and Applications (OOPSLA2012), pp. 1-20, 2012. (**査読有**)
DOI: 10.1145/2384616.2384618

㉗ Naoki Kobayashi, and C.-H. Luke Ong, Complexity of Model Checking Recursion Schemes for Fragments of

the Modal Mu-Calculus, Logical Methods in Computer Science, 7(4), 2011. (査読有)
DOI: 10.2168/LMCS-7(4:9)2011

㉘ Naoki Kobayashi, Higher-Order Model Checking: From Theory to Practice. Proceedings of LICS 2011, pp.219-224, IEEE Computer Society, 2011 (招待講演論文、査読無)
DOI: 10.1109/LICS.2011.15

㉙ Naoki Kobayashi, Ryosuke Sato, and Hiroshi Unno, Predicate abstraction and CEGAR for higher-order model checking. Proceedings of PLDI 2011, pp.222-233, 2011. (査読有)
DOI：10.1145/1993498.1993525

〔学会発表〕（計 8 件）

① 佐藤 亮介, 浅田 和之, 小林 直樹, 一階詳細化を用いた関数型プログラムの関係的性質の検証,第 16 回プログラミングおよびプログラミング言語ワークショップ（PPL2014）, ポスター発表, 2014 年 3 月 5 日, 阿蘇の司 ビラパークホテル（熊本県阿蘇市）

② 安酸 円秀, 小林 直樹, 松田 一孝, 高階モデル検査による高階並行プログラムの同時到達可能性の解析,第 16 回プログラミングおよびプログラミング言語ワークショップ（PPL2014）, ポスター発表, 2014 年 3 月 5 日, 阿蘇の司 ビラパークホテル（熊本県阿蘇市）

③ 寺尾 拓, 小林 直樹, BDD を用いた高階モデル検査アルゴリズム,第 16 回プログラミングおよびプログラミング言語ワークショップ（PPL2014）, ポスター発表, 2014 年 3 月 5 日, 阿蘇の司 ビラパークホテル（熊本県阿蘇市）

④ 武田広太郎, 小林 直樹, 松田一孝, RePair 流高階圧縮アルゴリズムの最適化, 日本ソフトウェア科学会大会, 2014 年 9 月 9 日, 名古屋大学 東山キャンパス（愛知県名古屋市）

⑤ Naoki Kobayashi, Behavioral Type Systems for Program Analysis: A Tutorial,1st International Workshop on Behavioural Types, 招待チュートリアル, 2013 年 1 月 22 日, ローマ（イタリア）

⑥ Naoki Kobayashi, Program Certification by Higher-Order Model Checking, CPP 2012, 招待講演, 2012 年 12 月 15 日, 京都市国際交流会館(京都府京都市)

⑦ Naoki Kobayashi, Higher-Order Model Checking: From Theory to Practice. LICS 2011, 招待講演, 2011 年 6 月 23 日, トロント（カナダ）

⑧ Naoki Kobayashi, Towards a software model checker for ML, ACM SIGPLAN Workshop on ML, 招待講演, 2011 年 9 月 18 日, 一橋記念講堂(東京都千代田区))

〔図書〕（計 0 件）

〔産業財産権〕
○出願状況（計 0 件）

○取得状況（計 0 件）

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

６．研究組織
(1)研究代表者
小林 直樹（KOBAYASHI, Naoki ）
東京大学・大学院情報理工学系研究科・教授
研究者番号：00262155

(2)研究分担者
篠原 歩 （SHINOHARA, Ayumi ）
東北大学・大学院情報科学研究科・教授
研究者番号： 00226151

五十嵐 淳（IGARASHI, Atsushi ）
京都大学・大学院情報学研究科・教授
研究者番号： 40323456

海野 広志（UNNO, Hiroshi ）
筑波大学・大学院システム情報工学研究科・助教
研究者番号： 80569575

(3)連携研究者
寺内 多智弘 (TERAUCHI, Tachio)
北陸先端科学技術大学院大学・情報科学研究科・教授
研究者番号：70447150

住井 英二郎 (SUMII, Eijiro)
東北大学・大学院情報科学研究科・教授
研究者番号：00333550

松田 一孝 (MATSUDA, Kazutaka)
東北大学・大学院情報科学研究科・准教授
研究者番号：10583627