様式 C-19

科学研究費補助金研究成果報告書

平成 24 年　3 月　31 日現在

機関番号：１１３０１
研究種目：基盤研究（A）
研究期間：2008～2010
課題番号：20240001
研究課題名（和文）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

研究課題名（英文）Advancement and Application of Type Theory for Improving Software Safety

研究代表者
小林　直樹（KOBAYASHI　NAOKI）
東北大学・大学院情報科学研究科・教授
研究者番号：00262155

研究成果の概要（和文）：
本研究では，ソフトウェアの信頼性向上のため，これまで研究代表者らが提案してきた型に基づくプログラム検証手法を実用レベルに引き上げるとともに，検証手法の開拓を目標としていた．前者の主な成果として，C プログラムやセキュリティプロトコルの自動検証ツールの構築が挙げられる．また，後者の主な成果として，高階モデル検査のプログラム検証への応用を示すとともに，世界初の高階モデル検査器の構築に成功した．

研究成果の概要（英文）：
This research project aimed to improve the reliability of computer software, by refining type-based program verification methods we have studied before, and also by inventing new program verification techniques. As the former study, we have constructed verification tools for C programs and cryptographic protocols. As the latter study, we have shown novel applications of higher-order model checking to program verification, and constructed the first higher-order model checker in the world.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2008 年度	10,700,000	3,210,000	13,910,000
2009 年度	8,400,000	2,520,000	10,920,000
2010 年度	10,400,000	3,120,000	13,520,000
年度			
年度			
総　計	29,500,000	8,850,000	38,350,000

研究分野：情報科学
科研費の分科・細目：情報学・情報学基礎
キーワード：ソフトウェア検証、型システム、高階モデル検査、資源使用法検証、
プログラム解析

１．研究開始当初の背景

交通システムや金融システム・原子力発電など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今日の高度情報化社会においては，ソフトウェアの信頼性向上が極めて重要かつ緊急の課題である．本研究ではこれまでに通常のプログラミング言語の型システムの概念を発展させ，プログラムの様々な性質を自動検証するための理論を構築してきた．しかし対象としてきた言語は λ 計算や π 計算など現実のプログラミング言語を極力単純化したものであり，構築した理論を実際のプログラムの検証に適用するには，まだ距離があった．また，型システムに基づいたプログラム検証は自動化が容易な一方で精度の問題があり，より優れたプログラム自動検証手法の必要となっていた．

２．研究の目的

上記の背景をふまえ，研究目的は以下の２つに大別される．

(1) 型システムに基づくソフトウェア検証の理論をさらに発展させ，研究代表者らがこれまでに取り組んできた並行プログラムの通信や同期の整合性，計算資源へのアクセス順序，セキュリティプロトコルなどの検証のための型理論を実用レベルにまで引き上げる．
(2) モデル検査や定理証明など他の検証手法と型に基づく手法とを融合し，新しい，より優れたプログラム検証手法を考案する．

３．研究の方法

上記の研究目的(1)，(2)をふまえ，以下の方針で研究を進めた．

(1) ポインタや例外，割り込みなどこれまで型に基づく我々の検証手法で扱っていなかった機能を扱えるように検証手法を拡張する．それに基づいて実際に検証器を作成し，精度や効率に問題があれば改善を行う．

(2) 型に基づくプログラム検証手法以外の代表的な自動検証手法としてモデル検査があるので，それらの関係や利害得失を明らかにし，融合を試みる．

４．研究成果

上記研究目的および方法の(1)，(2)に対応し，研究成果は以下の２つに大別される．

(1) 型に基づくプログラム検証手法の改良：既存の型に基づく検証手法を改良し，ポインタや割り込みなど現実のプログラミング言語において重要な機能を扱えるようにするとともに，理論に基づいて実際に検証器を構築し，評価を行った．以上の成果をまとめた論文は ACM Transactions on Programming Languages などトップレベルの学術雑誌および査読つき国際会議などに数多く採択され，高く評価されている．より詳しい成果は以下のとおり．

① Ｃプログラム自動検証ツールFreeSafeTy：
C 言語のメモリ管理命令(malloc および free)が正しく用いられていること，例えば獲得されたメモリ領域が解放されない，同じメモリ領域が２重に解放される，といった誤りがないことを型を用いて自動検証するための手法を定式化した．さらに，それに基づく検証ツール FreeSafeTy を構築し，1000 行規模のＣプログラムのメモリ安全性の自動検証に成功した．

②セキュリティプロトコル自動検証ツールSpiCA：
ネットショッピングや電子投票など，暗号を用いて電子的に機密情報を交換したり認証を行ったりするためのセキュリティプロトコルを自動検証するための手法を考案し，それに基づいた自動検証ツール SpiCA を構築し

た．より具体的にはGordon と Jeffrey によるセキュリティプロトコルを型検査の問題に帰着する手法を拡張し，型の自動推論を可能にすることによって実現した．

③割り込みを用いる並行プログラムのデッドロックフリーダムの自動検証手法の確立：
これまでに行ってきた，型に基づく並行プログラムのデッドロックの解析手法を拡張し，割り込みを用いるプログラムも扱えるようにした．

④ポインタを用いるプログラムの資源使用法解析：
プログラムがファイルやメモリなどの計算資源に仕様通りにアクセスしているか（例えば開いたファイルはいずれ閉じられるか）を解析するための型システムを拡張し，ポインタが扱えるようにした．それまでの我々の手法では，純粋な関数型プログラムしか扱えなかった．

(2) 高階モデル検査に基づく新しいプログラム検証手法の確立

モデル検査は，ハードウェアやソフトウェアの検証手法として近年注目を集めている．高階モデル検査は，通常の（有限状態）モデル検査の本質的な拡張であり，その決定可能性は2006年に証明されていたが，効率のよいアルゴリズムおよび現実的応用は知られていなかった，これに対し，本研究では型理論に基づく効率のよい高階モデル検査アルゴリズムを考案し，世界初の高階モデル検査器の実現に成功するとともに，関数型プログラムの自動検証への応用を示した．以上の成果はこの分野のトップの国際会議POPL 2009/2010，LICS 2009に論文が採択され，APLAS 2009やLICS 2011の招待講演を依頼されるなど，国内外で高い評価を受けている．
より詳しい成果は以下のとおり。
①高階モデル検査と型理論との対応：
高階モデル検査問題が共通型システムにおける型判定問題に帰着できることを示した．これは，既存の高階モデル検査の決定可能性の証明に比べて簡明な別証を与えるとともに②の高階モデル検査アルゴリズムの基礎を与える重要な結果である．
②高階モデル検査アルゴリズム：
高階モデル検査問題はn重指数時間完全という
絶望的な計算量クラスに属し，高階モデル検査器を実際に構築する試みはなされていなかった．それに対し，我々は①の型判定問題への帰着を利用し，典型的な多くの入力に対して現実的な時間で動作するアルゴリズムを考案し，世界初の高階モデル検査器の実現に成功した．
③プログラム検証への応用:
到達可能性検証や資源使用法検証など，関数型プログラムの多くのプログラム検証問題が高階モデル検査に帰着できることを示し，②の結果に基づいて実際に関数型プログラムの自動検証ツールの試作を行った．

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38件）

1. Naoki Kobayashi, Davide Sangiorgi, A hybrid type system for lock-freedom of mobile processes, ACM Transactions on Programming Languages and Systems (TOPLAS), Article Number 16, 49pages, 2010年, 査読有.
2. Takeshi Tsukada and Atsushi Igarashi, A logical foundation for environment classifiers, Logical Methods in Computer Science, 6 (4:8) 巻, pp.1-43, 2010年, 査読有.

3. Naoki Kobayashi, Naoshi Tabuchi and Hiroshi Unno, Higher-Order Multi-parameter Tree Transducers and Recursion Schemes for Program Verification, Proceedings of the 37th ACM SIGPLAN-SIGACT Symposium on principles of Programming Languages (POPL 2010), pp. 495-508, 2010年, 査読有.
4. Naoki Kobayashi, Types and Higher-Order Recursion Schemes for Verification of Higher-Order Programs, Proceedings of the 36th ACM SIGPLAN-SIGACT Symposium on principles of Programming Languages (POPL 2009) pp. 416-428, 2009年, 査読有.
5. Hans Hüttel, Naoki Kobayashi and Takashi Suto, Undecidable Equivalences for Basic Parallel Processes, Information and Computation, 207(7)巻, pp. 812-819, 2009年, 査読有.

〔学会発表〕(計24件)

1. Naoki Kobayashi, Higher-order model checking for program verification, Workshop on automata and logic for data manipulating programs, 2010年12月7日, フランス パリ, 招待講演.
2. Naoki Kobayashi, Types and Recursion Schemes for Higher-Order Program Verification, Workshop on Higher-Order Recursion Schemes and Pushdown Automata, 2010年3月11日, フランス パリ, 招待講演.
3. Naoki Kobayashi, Types and Recursion Schemes for Higher-Order Program Verification, the 7th Asian Symposium on Programming Languages and Systems (APLAS 2009), 2009年12月16日, 韓国 ソウル, 招待講演.
4. Naoki Kobayashi, Higher-Order Program Verification and Language-Based Security, the 13th Annual Asian Computing Science Conference (ASIAN 2009), 2009年12月16日, 韓国 ソウル, 招待講演.
5. Naoki Kobayashi, Substructural Type Systems for Program Analysis, The 9th International Symposium on Functional and Logic Programming (FLOPS 2008), 2008年4月16日, 三重県伊勢市, 招待講演.

〔その他〕

ホームページ等
http://www.kb.ecei.tohoku.ac.jp/

６．研究組織

(1)研究代表者
小林　直樹 (KOBAYASHI NAOKI)
東北大学・大学院情報科学研究科・教授
研究者番号：00262155

(2)研究分担者
五十嵐　淳 (IGARASHI ATSUSHI)
京都大学・大学院情報学研究科・准教授
研究者番号：40323456

住井　英二郎 (SUMII EIJIRO)
東北大学・大学院情報科学研究科・准教授
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・助教
研究者番号：10583627

寺内　多智弘 (TERAUCHI TACHIO)
東北大学・大学院情報科学研究科・助教
研究者番号：70447150