様式 C-7-2

自己評価報告書

平成２３年　４月　12 日現在

機関番号：１１３０１
研究種目：基盤研究（A）
研究期間：2008～2011
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．研究計画の概要

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ことを目標とする．また，そのような実用化に向けた研究を通じて，（１）ポインタや例外，割り込みなどの現実のプログラムに存在する複雑な言語機構を扱うための拡張，（２）検証精度と速度の向上，（３）モデル検査や定理証明など他の検証手法との融合，などの技術的課題 に取り組む．

２．研究の進捗状況

当初の予定だったプログラム検証のための型理論を実用レベルまで引き上げることに関しては、C 言語のメモリ仕様法検証法のための型システムの考案とそれに基づく C プログラム自動検証ツール FreeSafeTy の作成、セキュリティプロトコルの検証のための型理論の考案、およびそれに基づくプロトコル自動検証ツール SpiCA の作成など、一定の成果を挙げている。これら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ている。さらに、当初予定していなかった成果として、高階モデル検査に基づくプログラム検証手法の確立という革新的な成果が得られた。高階モデル検査は、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モデル検査の拡張であり、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した。さらに、高階モデル検査が高階関数型プログラムの自動検証に応用できることを示し、高階モデル検査に基づくプログラム自動検証器を実際に構築してその有効性を示した。以上の成果はこ

の分野のトップの国際会議 POPL、LICS、PLDI 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。現在これらの成果に基づいて、関数型プログラムの自動検証手法の改良を進めている。

３．現在までの達成度

当初の計画以上に進展している。

理由：上記進捗状況で述べたとおり、当初の計画が順調に進展しているとともに高階モデル検査に基づく新しい検証手法の確立という当初予定していなかった革新的な成果が得られている。

４．今後の研究の推進方策

研究進捗状況に述べた通り、高階モデル検査に基づく新しいプログラム検証手法が得られて大きな可能性が拓けたため、今後はその新手法について重点的に研究を行う。

５． 代表的な研究成果
（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.