H20/B12 定理証明系とその応用に関する研究(1節 共同プロジェクト研究の理念と概要,第4章 共同プロジェクト研究)

雑誌名	東北大学電気通信研究所研究活動報告
巻	15
ページ	263-265
発行年	2009-08
URL	http://hdl.handle.net/10097/48441

共同プロジェクト研究

課題番号　Ｈ２０／Ｂ１２

採択回数	①　２　３

定理証明系とその応用に関する研究

［１］組織

代表者：南出　靖彦
（筑波大学システム情報工学研究科）
対応者：外山　芳人
（東北大学電気通信研究所）
分担者：
浅井　健一
（お茶の水女子大学
人間文化創成科学研究科）
Reynald Affeldt
（独立行政法人産業技術総合研究所
情報セキュリティ研究センター）
磯部　祥尚
（産業技術総合研究所情報技術研究部門）
亀山　幸義,
（筑波大学システム情報工学研究科）
Jacques Garrigue
（名古屋大学多元数理科学研究科）
小林　直樹
（東北大学情報科学研究科）
高橋　和子
（関西学院大学理工学部）
武山　誠
（独立行政法人産業技術総合研究所
システム検証研究センター）
西崎　真也
（東京工業大学情報理工学研究科）
西村　進
（京都大学理学研究科）

研究費：物件費２万円，旅費２５万９千円

［２］研究経過

対話的な定理証明系を、ハードウェアやソフトウェアの検証、数学やプログラミング言語理論の形式化などに応用する研究が活発になってきている。しかし、規模の大きな問題に適用するには、証明の自動化や対象の形式化の手法などの点で課題が多い。本研究では、様々な分野に定理証明系を応用している研究者及びIsabelle、Coq、Agdaなど様々な定理証明系のユーザが集まり、具体的な事例での課題やそれぞれの定理証明系での技術的課題について議論し、その解決を目指した。

平成20年11月25～26日に東北大学電気通信研究所においてメンバー及び国内外の関連する分野の研究による研究集会を開催した。研究集会における発表テーマは次の通りである。

- 亀山幸義, Oleg Kiselyov,, Chung-chieh Shan,「Higher-Order Abstract Syntax を使ったケーススタディ２題 －CPS変換の完全性とマルチステージ言語の Subject Reduction」
- 湯浅能史,「定理証明系を用いた検証の授業について」
- 藤川浩光,「リターンバリアを使う実時間ごみ集めの安全性～抽象化の検証に Isabelle/HOL を使ってみて」
- 青戸等人, Sound Lemma Generation for Proving Inductive Validity of Equations」
- 廣田知子, 浅井健一,「対称λ計算の定式化に向けて」
- 高橋 和子,「Proving Divisibility of an Ideal Electronic Cash Protocol Using Isabelle/HOL」
- 藤原拓也,「Jones による計算可能性理論の形式化の試み」
- 千葉勇輝,「組化技法を用いたパターンによるプログラム変換」
- 武山誠,「Using the Agda Compiler MAlonzo」
- Julien Tesson,「Operational semantics of an imperative BSP mini-language in coq」
- AFFELDT Reynald,「Verification of Security Protocols with a Bounded Number of

Sessions based on Resolution for Rigid Variables」
- David NOWAK,「On Formal Verification of Arithmetic-Based Cryptographic Primitives」
- Jacques Garrigue ,「 Soundness and principality of type inference for structural polymorphism」
- 木下佳樹,「Agda の言語とシステム」
- 磯部祥尚,「The First Step for Implementing a Model Checker in a Theorem Prover -- Toward Automatic Verification in CSP-Prover」
- 南出靖彦,「Nominal Isabelle による CPS 変換の正当性の証明」

［3］成果

（3－1）研究成果

本プロジェクトによる研究集会において、本研究のメンバーが発表した研究成果を以下に記す。

1. プログラミング言語のメタ理論の定式化と検証

束縛変数に関する同値性を直接扱える定理証明系 Nominal Isabelle によって、CPS 変換の形式化とその正当性の検証を行った。CPS 変換を Nominal Isabelle で形式化する場合、変換が導入する新しい束縛変数の扱いが難しく、紙の上の証明をそのまま翻訳することができない。本研究では、必要となる補題を系統的に準備し証明を行うことで、定義や証明の主要な部分を自然な形で記述するができた。(南出靖彦)

プログラム変換の一種である CPS 変換の健全性と完全性を、Twelf システムを用いて形式検証する試みについて述べた。この証明で鍵となる束縛変数の扱いについて論じ、証明で必要とする逆 CPS 変換が compositional となるための工夫について述べた。(亀山幸義)

対象λ計算の導入を行うとともに、その基本的な性質である progress と preservation について、手による証明の概要を示した。また、それを定理証明系 Coq を使って行うにはどうしたらよいかについて検討した。(廣田知子, 浅井健一)

構造的多相性は、多相オブジェクトとバリアントを同時に定式化できる型推論の枠組みであり、Objective Caml の型システムの基礎となっている。証明支援系 Coq を用いて、その型安全性及び型推論アルゴリズムの健全性と完全性の証明に成功した。この証明の過程で見つかった、紙の上での証明ではこれまで考慮されてなかったいくつかの本質的な性質について議論した。(Jacques Garrigue)

2. クリティカルシステムの検証

理想的電子現金に要求される仕様の中で「分割利用可能性」の検証を試みた.「分割利用可能性」は「ある金額から任意の金額を使用した場合，残りの金額も正当な電子現金である」と解釈される．対象とする方式では，電子現金は二分木により実現されており，分割利用するための操作がその上で定義されている．このデータ構造および関数を帰納的な形で形式化し, 定理証明器 Isabeele/HOL を用いて検証を行った．本手法では，分割利用したあとの二分木を完全二分木のリストとし，リストごとに支払い関数を定義して証明している．(高橋和子)

実用性が高く誤検知の起きない，一階述語論理を用いたプロトコル自動検証アルゴリズムを，プロトコルのセッションの数が限られた仮定の上で，標準な技術を利用して構成した．本アルゴリズムは，既存のアルゴリズムでは実現できなかった，完全性と停止性の両方を満たしている．このアルゴリズムにより，誤検知の原因となっていたルール適用の順序とルールの再生成を抑制することができ，その結果，これまで検証が出来なかった暗号プロトコルの検証が可能になった.(AFFELDT Reynald)

システム検証ツールはモデル検査系と定理証明系に大別できる。モデル検査器と比較した定理証明器の長所は帰納法等により無限状態を検証できることにある。一方、その短所は検証の完全自動化が難しいことである。本研究の目的は、定理証明器上にモデル検査器のアルゴリズムを実装し、両方の長所をもつ検証ツールを開発することである。本発表では、並行システムの双模倣関係を自動検証可能なツールを定理証明器 Isabelle 上に試験的に実装したことを報告する。(磯部祥尚)

（3－2）波及効果と発展性など

2005 年から定理証明と定理証明系に関する研究集会を、年に１回開催してきたが、本プロジェクトにより、これまで以上に研究者間の交流を進めることができた。本プロジェクト研究が契機となり、定理証明系を用いたプログラミング言語のメタ理論の検証などの分野でメンバー間の共同研究などが進むことが期待できる。

［4］成果資料

1. A. Tozawa, M. Tatsubori, T. Onodera, Y. Minamide, Copy-on-Write in the PHP Language, In Proc. POPL: The Symposium on Principles of Programming Languages, pp. 200-212, 2009.

2. T. Nishiyama and Y. Minamide, A Translation from the HTML DTD into a Regular Hedge Grammar, In Proc. of the 13th International Conference on Implementation and Applications of Automata, LNCS 5148, pp. 122-131, 2008

3. 安田峰悠, 松本宗太郎, 南出靖彦, ブラウザにおける JavaScript 実行のモデル化, 日本ソフトウェア科学会 第 25 回大会, 2008 年 9 月 10 日～12 日.

4. Jefferson O. Andrade, Yukiyoshi Kameyama, A Direct Algorithm for Multi-Valued Bounded Model Checking, Proc. International Symposium on Automated Technology for Verification and Analysis (ATVA 2008), Lecture Notes in Computer Science 5311, pp. 80-94, Oct. 2008.

5. Yukiyoshi Kameyama, Oleg Kiselyov, Chung-chieh Shan, Shifting the Stage -- Staging with Delimited Control, Proc. ACM SIGPLAN Symposium on Partial Evaluation and Program Manipulation (PEPM'09), Savannah, USA, pp. 111-120, Jan. 2009.

6. Naoki Kobayashi and Hitoshi Ohsaki, Tree Automata for Non-Linear Arithmetic, Proceedings of RTA 2008, Springer LNCS 5117, pp.291-305, 2008.

7. Naoki Kobayashi, Types and Higher-Order Recursion Schemes for Verification of Higher-Order Programs,Proceedings of POPL 2009, pp.416-428, 2009.

8. Sin-ya Katsumata and Susumu Nishimura, Algebraic Fusion of Functions with an Accumulating Parameter and Its Improvement, Journal of Functional Programming, 18(5-6), pp. 781-819, 2008.

9. Susumu Nishimura, Safe Modification of Pointer Programs in Refinement Calculus, International Conference on Mathematics of Program Construction (MPC '08), LNCS 5133, pp. 284-304, 2008.

10. 八尾俊佑, 粟野宏昭, 平岡康, 高橋和子、モデル検査器 SPIN による船舶用システムのモデル化と検証, 第 6 回ディペンダブルシステムワークショップ(特別講演), pp.61--68, July, 2008.

11. Takahashi,K, T.Sumitomo and I.Takeuti. On Embedding a Qualitative Representation in a Two-Dimensional Plane, Spatial Cognition and Computation, Vol.8, No.1-2, pp.4-26, April, 2008.

12. 木谷有沙、浅井健一「限定継続を含む仮想機械導出のためのプログラム変換」第 11 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, 14 pages (2009).

13. Reynald Affeldt and Hubert Comon-Lundh., Verification of Security Protocols with a Bounded Number of Sessions based on Resolution for Rigid Variables. In Special Issue on Computer Security, volume 5458 of Lecture Notes in Computer Science, Springer, 2009. To appear.

14. Yoshinao Isobe and Markus Roggenbach: CSP-Prover -- a Proof Tool for the Verification of Scalable Concurrent Systems, Journal of Computer Software, Japan Society for Software Science and Technology(JSSST), Vol.25, No.4, pp.85--92, 2008.