「情報社会を支える新しい高性能情報処理技術」
平成14年度採択研究代表者

木下　佳樹

（(独)産業技術総合研究所　システム検証研究センター長）

「検証における記述量爆発問題の構造変換による解決」

1.研究実施の概要

研究のねらい・着眼点　ソフトウェアの数理的検証法研究における最大の課題の一つは，検証の記述が膨大になって人間や自動検証器の能力を超えた長さになってしまう記述量爆発の問題である．この解決のため，ソフトウェアの数学的構造を明確にし，その構造に変換を施すことによって，検証における記述量を劇的に減少させる技法を研究する．

コンセプト　本計画では，ソフトウェアが持つ数学的構造を圏論における函手意味論の手法により取り扱い，自由代数の生成を指導原理として，ソフトウェアの構造を互いに関連づけるために用いる．

本計画におけるもうひとつの重要なコンセプトは，抽象化の考えである．記述の量を減らすために，検証の対象となるシステムMより記述量の少ないシステムNを設定し，望ましい性質PをMが満たすことを検証する代わりに，より記述量の少ないNがPを満たすことを検証すれば十分であるようにするのが抽象化である．本計画では，記述量爆発の問題を，抽象化の考えに基づいて解決することを目指す．

第三のコンセプトはリアクティブ・システムおよび実時間システムである．システム開発の現場で検証が必要とされている多くの事例は，電子機器に組み込まれた制御ソフトウェアであり，リアクティブ・システム，あるいは実時間システムとみなすのが適当である．本計画では，抽象化の対象を主としてリアクティブ・システムおよび実時間システムに想定し，検証が必要とされている場に，研究成果によって貢献することを目指す．

将来展望　強力なシステム検証技術は，システムの製造技術として，潜在的な需要は大きい．**本計画**における基礎研究と，産総研で別途遂行中の企業との連携による実用化研究の成果を産総研システム検証研究センターにおいて相互作用させ，科学的技術の産業への貢献を図る．

2.研究実施内容

（ア）サブテーマ「既存抽象化算法の調査」では，抽象化支援系技術についての動向を

調査した．新しく実用的な抽象化ツールを設計試作するにあたって，既存の抽象化法，とくに自動化の手法を詳細に調査することとした．抽象解釈，データマッピング，述語抽象など，支援系作成の分野において広く知られている抽象化のテクニックを調べたのち，既存もしくは開発中の抽象化を利用している検証ツール，SLAM, BLAST, Bandera, JPF, ESC/Java, FeaVer, SPIN, STeP, PAXの九つの検証系における抽象化技術を調べた．これまで抽象化についてまとまった文献がなかったので，この調査結果をまとめ調査報告とした．報告書は、早くも我国の研究者の間で重宝されている．（イ）サブテーマ「ポインタ処理システムの抽象化算法についての研究」では，高橋-萩谷による並列ゴミ集めの抽象化算法を一般のポインタ処理システムに適用できるよう、一般化を試み，支援系の設計を開始した．（ア）の調査によって，既存の抽象化は数値データを扱うものがほとんどであり，ポインタ構造の抽象化は課題であることがわかったので，この課題に注力する方針を決定した．ポインタ変数を論理式に取り入れるため，それを原子命題として扱う方法の検討を始めた．この方法では既存の高橋-萩谷の抽象化法では公理が非常に多くなってしまうことがわかった．そこで，一般化の研究に着手した．この結果を用いて2004年度以後の支援系試作につなげる．（ウ）サブテーマ「抽象解釈と緩変換拡張理論との比較」では，抽象解釈に必要な圏論的構成を明確にした．抽象解釈は，抽象化の指導原理として最も広く受け入れられており，より一般的なコンテクストの下で抽象解釈を理解することにより，抽象解釈に基づく抽象化支援系作成が容易になる．抽象解釈におけるガロア接続の構成が，「冪集合が自由完備上半束であること」にもとづく自由生成とKan extensionに基づいていることを明確にした．また，よく知られている「与えられた遷移系を模倣する遷移系はACTL式を保存する」という事実も，同じ枠組みで理解されることを明らかにした．（エ）サブテーマ「刺激応答型システムの抽象化過程の数理モデル構築」においては，オートマトンの代数的定式化や抽象化を定式化するために有望だと思われるファイブレーション意味論についての文献調査を行った．前者のためにS. Eilenbergの古典“Automata, Languages and Machines”の第一巻前半を精読し，その方法を用いてAllegoryにおけるオートマトンの定式化を与えた。この結果は，緩変換にもとづく抽象化の理論でオートマトンを取り扱うために使える．ファイブレーションについては，B. Jacobs著“Categorical Logic and Type Theory”のはじめ１／４程度を精読し、簡単な例に関して形式的理論の間の射を調べたが，十分複雑な論理体系に関しては，さらに調査が必要である．

3.研究実施体制

数理モデル研究グループ

① 研究分担グループ長：木下佳樹（独立行政法人産業技術総合研究所
システム検証研究ラボ　研究ラボ長）

② 研究項目：リアクティブシステムおよび実時間システムの検証における抽象化の数理モデルの構築と形式化

（ウ）サブテーマ「抽象解釈と緩変換拡張理論との比較」と（エ）サブテーマ「刺激応答型システムの抽象化過程の数理モデル構築」を担当

支援ソフトウェア研究開発グループ

① 研究分担グループ長：高橋孝一（独立行政法人産業技術総合研究所
システム検証研究ラボ　副研究ラボ長）

② 研究項目：抽象化支援ソフトウェアの方式と試作

（ア）サブテーマ「既存抽象化算法の調査」と（イ）サブテーマ「ポインタ処理システムの抽象化算法についての研究」を担当

4.主な研究成果の発表（論文発表および特許出願）

（１）論文（原著論文）発表

○ 田辺良則、高井利憲、高橋孝一（産業技術総合研究所システム検証研究ラボ）
「抽象化を用いた検証ツールの調査」
産業技術総合研究所算譜科学グループ研究速報
平成１５年１２月８日

○ 高橋孝一、武山誠、高井利憲、西澤弘毅、田辺良則、池上大介、渡邊宏、大崎人士、木下佳樹
「シンポジウム「システム検証の科学技術」予稿集」　平成１６年２月４日-６日

○ 高井利憲（産業技術総合研究所システム検証研究ラボ）
「A Verification Technique Using Term Rewriting Systems and Abstract Interpretation」
産業技術総合研究所算譜科学グループ研究速報
平成１６年３月１日

○ 高井利憲（産業技術総合研究所システム検証研究ラボ）
「ACTAS: Associative and Commutative Tree Automata Simulator」
産業技術総合研究所算譜科学グループ研究速報
平成１６年３月１日

（２）特許出願

なし