「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　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

本研究は

抽象化シナリオ　与えられた具象システムの検証が記述量爆発によって困難であるため、より検証しやすい抽象システム、およびそれと具象システムとの間の関係を設定し、その関係が、抽象化関係:「抽象システムでの検証が具象システムでの検証を導く」を満たすことを前提として、抽象システムの検証に具象システムの検証を帰着させる

に関する研究をおこなうものである。

本年度も、三つの研究グループを立てて研究活動を進めた。数理モデル研究グループでは、刺激応答系の抽象化シナリオを緩変換の枠組みによって実現するため、様相μ計算の部分系$R\mu$を構築して、そこでの抽象化シナリオの数理モデルを研究した。支援ソフトウェア研究開発グループでは、ポインタ処理を行うプログラム言語における抽象化シナリオの事例を実現する支援ツールの研究開発を行った。また、定理証明研究グループでは、定理証明支援系 Agda の開発を続行、これを自動検証用の外部ツールに拡張するための plug-in 機構を設計し、一階述語論理自動証明器 Gandalf およびモデル検査器 SMV を Agda から呼び出して用いる抽象化シナリオの枠組を提示した。

残りの一年半をかけて、これまでの数理モデル、自動抽象化ツール、統合検証環境に関する成果を適用して並列プログラムの検証ツールを試作し、抽象化シナリオの実例を一つ具体的に示すことを目指す方針である。

２．研究実施内容

＜数理モデル研究グループ＞

この研究の目的は、抽象化技法の数理的意味を定式化することである。

抽象化の定式化のために、本研究では、代数構造の概念を用いたアプローチをとっている。一方、刺激応答系の性質を記述するためには命題様相 μ 計算が広く用いられている。しかし、集合の上の代数構造で、様相 μ 計算に対応するものはないことが知られている。そこで、集合の上の代数構造ではなく、圏の上の代数構造を用いる必要がおこった。そのためには、従来より Lawvere 理論とよばれる手法があるが、より一般的に取り扱うため、我々は Lawvere A-理論とよぶ手法を開発した。これがこの研究の一つ目の成果である。

さらに、様相 μ 計算の部分系R μ を構築し、R μ およびR μ における抽象化過程の数理モデルを、Lawvere A-理論を用いて与えた。R μ は様相 μ 計算の部分系ではあるが、刺激応答系の性質記述に広く用いられるCTLを部分系として含むので、十分実用に耐えるものである。これがこの研究の二つ目の成果である。

以上の仕事により、解釈の定義、健全性定理と完全性定理、抽象化の定義、論理式保存の定理などの間の関係を代数的な概念で結びつける知見が得られた。

＜支援ソフトウェア研究開発グループ＞

我々は「ポインタで指す」ことを様相とする様相論理（2CTL）を用いてヒープの状態を表現する。ヒープを操作するプログラムは、状態をヒープとする遷移系である。したがって、我々の体系には、様相が二つある。「ポインタで指す」ことの様相と「プログラムの 1 ステップの実行」の様相である。この前提のもとで、述語抽象化のテクニックを適用して、プログラムの自動抽象化を行うのが我々のアプローチである。

まずヒープのポインタ操作を記述するプログラミング言語 PML(Pointer Manipulation Language) を構築した。次に、PML で書かれたプログラムと、抽象化のヒントとなるいくつかの 2CTL 式、検証したい性質、の三つを入力すると、述語抽象で抽象化された抽象遷移系を出力するツールを試作し、ポインタ反転アルゴリズムなど、簡単な例の実験を行った。抽象化のアルゴリズムが EXPTIME 完全なので、「よくある場合について、実用に耐える応答性能を得る」のが今後の課題である。

出力をそのまま NuSMV に与えると、プログラムが検証したい性質を満たすかどうかを検証することができる。ただし、本当にプログラムがその性質を満たしていない場合と、抽象化が大雑把すぎたために検証に失敗する場合があり、その反例をを解析することによって、よりよい抽象化が得られる可能性がある。この反例解析の自動化も、今後の課題である。

また、試作したツールを統合検証環境 Agda と接続する計画も進めており、これまでにインターフェースを決めた。

＜定理証明研究グループ＞

Chalmers 工科大学(スウェーデン)で開発された対話型証明支援系 Agda を用いて統合検証環境の開発を進めている。

外部ツールを接続する際のプラグイン機構を一般化し、一階述語論理の自動証明器 Gandalf 用“FOL プラグイン”および CTL 論理のモデル検査器 NuSMV 用“SMV プラグイン”を実装し、Agda の中から Gandalf や NuSMV を使える環境を提供した。

Agda 上での様相 μ 計算の定式化を拡充し CTL 論理での証明、プラグイン使用を可能にした。

これらを組み合わせて、抽象化シナリオの雛形となる形式化実験を行った。1プログラムの無限状態具体解釈と有限状態抽象解釈を定理証明で結び、後者を SMV で検証した。

依存レコード型とサブタイピングをもつ型理論の拡張に対して、超変数を許す型検査器のプロトタイプ Mendori を実装した。これで得られた知見を活かして Chalmers と共同で、次世代言語 Agda2 のコア言語を設計し、項操作と単一化の実装を行った。

Agda 言語を入出力等の機能と実用的な速度をもつ依存型付作譜言語として実用化するため、Haskell による翻訳実行系 Agate を試作した。Agate によるオーバヘッドは数十%程度であり、依存型を用いた作譜実験を可能とする環境を提供することができた。今後、作譜実験を開始するほか、依存型の機能を用いたコード最適化算法の研究を行う。

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（産業技術総合研究所、研究センター長）

②研究項目：刺激応答系の抽象化シナリオを緩変換の枠組みによって実現する数理モデルと論理の構築

「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（産業技術総合研究所、副センター長）

②研究項目：ポインタ処理を行なうプログラム言語における抽象化の支援ツールの研究開発

「定理証明研究」グループ

①研究分担グループ長：武山　誠（産業技術総合研究所、研究員）

②研究項目：抽象化シナリオ適用のための統合検証環境の構築

４．主な研究成果の発表

（１）　論文（原著論文）発表

○　木下 佳樹、高村 博紀:型理論での形式的証明記述の技法について
日本ソフトウェア科学会第22回大会講演論文集(ISSN　1348-0901)2005(CD ROM)

○　Koki Nishizawa, ″Algebraic Structures for Cocomplete Fibrations and Fibred CCCs″, Programming Science Technical Report, AIST, September 2005

○　Koki Nishizawa and Makoto Takeyama, ″Algebraic Structure for a Fixed Point Logic and Abstract Interpretation″, Programming Science Technical Report, AIST, June 2005

○　Koki Nishizawa and John Power, ″Lawvere Theories Enriched over a General Base″, Programming Science Technical Report, AIST, February 2005

○　Yoshinori Tanabe, Koichi Takahashi, Mitsuharu Yamamoto, Akihiko Tozawa and Masami Hagiya. A Decision Procedure for the Alternation-Free Two-Way Modal μ-Calculus. LNAI, Automated Reasoning with Analytic Tableaux and Related Methods(TABLEAUX 2005), Vol. 3702, pp.277-29, 2005.

○　Yoshinori Tanabe, K, Toshinori Takai,Toshifusa Sekizawa and Koichi Takahashi,. Preconditions of properties described in CTL for statements manipulating pointers, Supplemental Volume of the 2005 International Conference on Dependable Systems and Networks, pp.228-234, 2005.

○　田辺良則, 高橋孝一, 山本光晴, 佐藤貴洋, 萩谷昌己: BDD を用いた 2 方向 CTL 論理式充足可能性決定手続きの実装．コンピュータソフトウェア, Vol.22No.3 (2005), pp.154-166

○　Peter Dybjer, Qiao Haiyan, 武山 誠. ”Rondom Generators for Dependent Types”, Theoretical Aspects of Computing - ICTAC 2004: Revised Selected Papers, Lecture Notes in Computer Science, vol. 3407, pp 341―355, 2005