「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　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

に関する研究を行うものである。理論研究を行う一方で、このような検証手法を支援するツールを研究試作する。

研究プロジェクトの成果を提示するために、検証ツールを試作して抽象化シナリオの実例を一つ具体的に示すこととし、本 18 年度にはこの目的で並行プログラム検証研究グループを新設した。並行プログラムの実例として MPI 規格の実装 YAMPII をとりあげ、開発グループの協力をえて、このソースコード検証を目指した。一年間の試行錯誤の結果、当初目標としていた並行性に関する性質ではなく、ポインタ操作に関する性質を検証する例を提出することとした。当プロジェクトの成果の一つである MLAT はポインタ操作の検証のためのものなので、並行性を検証するよりも、我々の成果をよく活かせる事例となった。また、ソースコード検証にあたっては、当プロジェクトの成果である抽象化の技法を縦横に使うこととなる。

以下に、各研究グループの研究活動の概略を記す。

数理モデル研究グループでは、多値モデル検査のための抽象化に関する理論を、亀山幸義(筑波大)との共同研究により構築したほか、一階様相 μ 計算の一般モデルに関する完全性を鹿島亮(東工大)と共に証明した。

支援ソフトウェア研究開発グループでは MLAT によってより大きなプログラムを扱えるよう、応答速度を改善すべく、発見的な手法で効率化を進める一方、定理証明研究グループおよび並行プ

ログラム検証研究グループと共同で Agda を用いて部分問題に分割し、部分問題を MLAT で自動検証する手法を研究し Pfvalid/Agda と呼ぶツールを開発した。

定理証明研究グループは、Chalmers 工科大と共同で次期証明支援系 Agda2 の α 版を稼動させたほか、Agda の普及のためにホームページを大幅に拡充した。

並行プログラム検証研究グループでは、YAMPII の一部をとりだして BLAST や Spin などの既成ツールによる検証を行い、自動ツールの可能性を探った。この結果、Pfvalid/Agda を YAMPII に利用する事例を作ることとした。

2. 研究実施内容

〈数理モデル研究グループ〉

リアクティブシステムの抽象化の数理モデルは、平成 17 年度までに行った Rμ の圏論的意味論によって一応の決着を見たが、本 18 年度は、この研究の手法を用いて多値モデル検査における抽象化の研究を亀山幸義（筑波大）と共同で行った。また、16 年度から行なっている一階様相 μ 計算の研究に関して、通常のモデルに関しては帰納的公理化不能であることを昨 17 年度に示したが、鹿島亮（東工大）との共同研究の結果、モデルの定義を変えて、一般モデル（generalised model）に関する完全性を示すことができた。

＜支援ソフトウェア研究開発グループ＞

抽象化支援ツール MLAT の改良。

より大きなシステムを取り扱えるよう、高速化を試みている。これまでの版は、初期状態から到達不能な状態に関しても遷移関係を計算するので無駄が多かった。そこで、計算途中に到達可能性を判定しながら、到達不能状態に関する計算を省略する方式を考案した。また、事後条件の計算もとりいれて状態数を減らす方式を考案し、現在実装中である。なお、DSW (Deutch-Schorr-Wait マーキング算法)の検証への適用の可否を MLAT 高速化の尺度としている。

高速化と並行して、記述力の強化のため、MLAT の状態記述のための論理を 2CTLN から alternation-free μ 計算へと拡張している。例えば alternation-free μ 計算の論理式 $\mu X[p \vee \langle l \rangle(\neg s \wedge X) \vee \langle r \rangle(s \wedge X)]$ は 2CTLN では記述できないが、DSW の検証に必要である。

統合検証環境 Agda との連携。

これは定理証明研究開発グループとの共同で行っている。Agda の汎用 plug-in 機構に MLAT を接続し、MLAT の一部である Pfvalid（Hoare triple の恒真性判定器）を Agda から呼べるようにし、さらに Agda 上に Hoare 論理を定義して、ポインタ操作プログラムの検証実験を行った。この一連の組み合わせによってできる Hoare triple の検証ツールを Pfvalid/Agda と呼んでいる。現状では基本命令やその列に関する Hoare 式が自動証明可能である。まず単純なプログラムの検証の例を作成

し、大きなプログラムの検証方法についても検討を行った。

＜定理証明研究開発グループ＞

Chalmers 大との研究協力において、5月に CVS で、9月に Chalmers で、それぞれ一週間の Agda Implementors Meeting 研究集会を開催し、主に次期証明支援系 Agda2 開発について集中合宿的に作業とセミナーを行った。CVS 側は Agda2 のユーザーインターフェース、コンパイラ、Agda1 コードとの変換器などを分担し、Agda2 のα版が稼動を開始した。

また、Chalmers 大から Bengt Nordström 教授を一ヶ月間招聘し、Agda2 コア言語の型検査算法の研究を行った。

Agda の普及のため、公式ホームページ http://unit.aist.go.jp/cvs/Agda/ を新設し、配布体制を大幅に強化した結果、Agda に関する興味を広く喚起し、興味を持つ人に簡単に試してもらえる環境が整った。

Agate への Haskell 関数の埋め込みを一般的に行う機能拡張を施し、また翻訳で生じる無駄なコードを取り除く最適化機能をもつ版を公開した。ライブラリ強化に向けた依存型プログラミングの実験も進め、構文解析組合せ子ライブラリや MLAT に用いられる最弱前提条件計算算法の正しさ証明付き実装を開発した。

＜並行プログラム検証研究グループ＞

研究計画では「YAMPII のメモリ管理機構について、自動検証が可能なシステムを開発する」とし、C プログラムの自動検証器 BLAST を改良することで対応することを試みた。その結果、メモリ管理機構の自動検証は BLAST では困難であることが分かったため、手作業でソースコードの抽象化を行い、SPIN モデル検査器により検証を行ってみた。これらの一連の予備調査により既存のツールでも、検証項目を単純な要件に限定すれば検証が可能なことが分かった。

より完全な検証を行うため、メモリ操作を記述するための言語 PML によりメモリ管理機構を記述し、Pfvalid/Agda による半自動的な検証を試みている。

3. 研究実施体制

(1)「数理モデル研究」グループ

①研究者名

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　センター長)

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

(2)「支援ソフトウェア研究開発」グループ

①研究者名

高橋　孝一((独)産業技術総合研究所　システム検証研究センター　副センター長)

②研究項目

・抽象化支援ソフトウェアの方式と試作

(3)「定理証明研究」グループ

①研究者名

武山　誠((独)産業技術総合研究所　システム検証研究センター　研究員)

②研究項目

・構成的型理論に基づいたリアクティブシステムの検証と抽象化

(4)「並行プログラム検証研究」グループ

①研究者名

山形　頼之((独)産業技術総合研究所　システム検証研究センター　研究員)

②研究項目

・スレッドとポインタを扱うプログラムの自動検証システムの研究開発

4. 研究成果の発表等

(1)論文発表(原著論文)

○奥田 俊弦, 高井 利憲, 田辺 良則, 高橋 孝一

時相論理の充足可能性判定器のための論理式生成法

電子情報通信学会論文誌 D-I, J89-D 巻　4 号 642 頁～650 頁, 2006 年 4 月

○高井 利憲, 古澤 仁

Monodic tree Kleene algebra

Proceedings of 4th International Workshop on Kleene Algebra, Lecture Note in Computer Science, 4136 巻 402 頁～416 頁, 2006 年 8 月

○Hiroki Takamura

The variety of modal FLew-algebras is generated by its finite simple members, Advances in Modal Logic vol.6, pp 469-479, College Publications

○高井 利憲, 古澤仁

クリーニ代数によるプログラム解析入門(チュートリアル),

第三回システム検証の科学技術シンポジウム予稿集, 29 頁～ 36 頁, 2006 年 10 月

○Yoshiki Kinoshita, Koki Nishizawa, Keishi Okamoto

Formalising Coffman Conditions in First Order Modal μ - Calculus,

Programming Science Technical Report, AIST, Oct 2006

○Hiroki Takamura
Semisimplicity, EDPC and discriminator varieties of modal FLew-algebras (Preliminary Version) Programming Science Technical Report, AIST, Feb 2007
○奥田俊弦，高井利憲，田辺良則，高橋孝一
時相論理の充足可能性判定器のための論理式生成法，電子情報通信学会論文誌D-I 2006年4月
○高橋孝一，田辺良則，奥田俊弦
一次元セルオートマトンの有限近似解析，コンピュータソフトウェア，2006年9月
○尾崎 弘幸,武山 誠,木下 佳樹
Agate: an Agda-to-Haskell compiler,「算譜科学研究速報」(Programming Science Technical Report), 2006 年 10 月