「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

（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

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

今年度は新たに定理証明研究グループを設けて数理モデル研究グループから独立させ、検証の形式化に関する研究を本格化した。数理モデル研究グループにおけるリアクティブシステムの抽象化・詳細化の数理モデルに関する研究では、リアクティブシステムの数理構造を不動点演算子を持つ高階様相論理として定式化することに取り組んだ。支援ソフトウェア研究開発グループにおいては、ポインタ型を扱うシステムの抽象化支援システムの研究開発を継続した。定理証明研究グループは、スウェーデンChalmers工科大学と共同して、Martin- Löf型理論に基づく定理証明支援系Agdaの開発・保守を開始した。これは、第二年次の研究において、さまざまな検証方式を統合する環境の必要を認識し、Martin-Löf型理論の支援系Agdaおよび函数型言語Haskellを用いて、当プロジェクトで研究開発するいろいろな検証方式の統合環境を形成していく必要があると認識したからである。

各グループで適宜ミーティング、セミナーを開催するほかに、月一回、チーム全体によるセミナーを催し、チーム全体の相互理解促進を図った。

数理モデル研究グループはリアクティブシステムの論理体系として様相μ計算の自然な拡張である高階様相μ計算を採り、これがリアクティブシステム検証に有効なものであることを確認した。具体的には、不定個プロセスの排他制御問題など、二つの問題の記述で、量化記号（quantifier）を本質的に含む検証項目が現れた。

支援ソフトウェア研究開発グループは、我々が開拓した、ポインタシステムの性質を時相論理で記述して検証するアプローチのために必要な時相論理式の充足可能性判定について、効率的に満足できるものを考案し、これに基づいた試作を行った。また、ポインタシステムの本質を抽出した算譜言語を設定、その性質を時相論理式で記述し、これに関して述語抽象化を行う支援ソフトウェアの設計を行った。

定理証明研究グループでは、対話型定理証明支援系Agdaのマニュアル開発、Agda上での様相μ計算の実装、SMVプラグインの開発Chalmersとの共同研究体制を整えた。Agda上で様相μ計算の検証を可能にするμNKおよびAgdaからモデル検査器SMVを起動するplug-in Agda-SMVを開発し、CTLあるいはLTL（いずれも様相μ計算の部分系）の検証で、対話型検証と自動検証を局面に応じて使い分けることを可能にした。

今後は、数理モデル研究グループはリアクティブシステムの論理体系を発展させる。支援ソフトウェア研究開発グループはポインタシステムの本質を抽出した算譜言語の述語抽象化を行う支援ソフトウェアについて設計がほぼできているので、実装は来年度中にできると考える。また、来年度は新しい別の抽象化法を考察していく。定理証明研究グループでは、開発したAgdaプラグインを整備し、支援ソフトウェア研究開発グループが開発したツールのAgdaへの接続を行う。

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（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）

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

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　システム検証研究セタンー　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

定理証明研究グループ

① 研究分担グループ長：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タンー　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.主な研究成果の発表

(1) 論文発表

○ 古澤 仁. A free construction of Kleene algebras with tests. Proceedings of Seventh International Conference on Mathematics of Program Construction, 12-14 July, 2004, Stirling, Scotland, UK, in a volume of Springer-Verlag Lecture Notes in Computer Science. Vol. 3125, pp.129-141. 2004.7.

○ 萩谷昌己，高橋 孝一，山本光晴，佐藤貴洋. Analysis of Synchronous and Asynchronous Cellular Automata using Abstraction by Temporal Logic. Proceeding of International Symposium on Functional and Logic Programming(FLOPS2004), LNCS2998, 2004.4.

○ 高井 利憲. A Verification Technique Using Term Rewriting Systems and Abstract Interpretation. LNCS, Rewriting Techniques and Applications, Vol. 3091, pp.119-133. 2004.6.

○ 高木 理,武山 誠，渡邊 宏. PVSの紹介. コンピュータソフトウェア.

○ 田辺 良則，高井 利憲，高橋 孝一. 抽象化を用いた検証ツール. コンピュータソフトウェア. Vol. 22, No. 1, pp. 2-44, 2005.1.

○ 高木 理，武山 誠，渡邊 宏. Verification of correctness of TSR via PVS. コンピュータソフトウェア.

○ Peter Dybjer, Qiao Haiyan, 武山 誠. Verifying Haskell Programs by Combining Testing, Model Checking and Interactive Theorem Proving. INFORMATION AND SOFTWARE TECHNOLOGY. Vol.46, No.15, pp.101-1025. 2004.12

○ Peter Dybjer, Qiao Haiyan, 武山 誠. Rondom Generators for Dependent Types. Proceedings of the First International Colloquium on Theoretical Aspects of Computing, Guiyang, China, LNCS 3407. pp.342-456. 2004.9
○ 大崎 人士, 高井 利憲. ACTAS: A System Design for Associative and Commutative Tree Automata Theory. ENTCS