研究課題別事後評価結果

1. 研究課題名: 検証における記述量爆発問題の構造変換による解決

2. 研究代表者名及び主たる研究参加者名(研究機関名・職名は研究参加期間終了時点)

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 研究センター長)

主たる共同研究者

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 グループ長)

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
グループ長 平成15年9月～平成19年11月)

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
グループ長 平成18年4月～平成19年3月)

3. 研究内容及び成果

システム検証での大きな課題の一つにスケーラビリティを得ること、つまりシステムやその性質の記述の量が爆発的に増えても、とり扱うことができる原理を与えることがある。スケーラビリティを得るための有力な手法が抽象化である。一般に、具体的なシステムの性質のうち、注目したい性質を保つが、他の性質は保つとは限らないようなシステムを、元のシステムを抽象化したものという。逆に、抽象的なシステムからはじめて、その性質をすべて保つような具体化を行ったシステムを得ることを、詳細化といっている。抽象化と詳細化は、たがいに逆の関係にある。

1990 年代に、研究代表者らは、詳細化(refinement)の一般的な意味論(数理的モデル)を、圏論における函手意味論の手法を用いて与えた。ここでは、函手的意味論の常套手段に従って、情報処理システムのモデルを函手によって与え、詳細化は二つのモデルの間に与えられるものとして、函手の間の緩変換(lax transformation)として定式化される。詳細化の函手的意味論は、システムを記述する言語(プログラミング言語)によってパラメータ化された形であたえられており、その意味で極めて一般的なものである。研究代表者らは、プログラミング言語として while 命令を採用した場合を調べ、一般的な意味論を入力出力型システムに適用して具体化した。
ところで詳細化と抽象化は上述のように表裏一体の関係にある。意味論は、システムを求める算法までは規定せず、算法が展開される数学的世界を記述するものだから、詳細化の意味論と抽象化の意味論は一致する。つまり詳細化の函手的意味論はそのまま、抽象化の函手的意味論でもある。

本計画では、抽象化の函手的意味論の適用範囲を、入力出力型システムから刺激応答型システムに拡大するための意味論研究を行った。命題様相μ計算の部分体系ではあるが CTL を含む体系 Rμの構築とそこで抽象化の意味論構築と自由生成の存在証明がその内容である。いっぽう、既に具体的な理論が立てられている入力出力型システムについては、研究代表者らの意味論が示す方向で、抽象化支援システムを試作することとした。抽象化支援ツール周辺の文献調査を経て、ポインタ処理を行う while 命令に関する抽象化を支援するシステム MLAT を試作し、これを用いて Deutsch-Schorr-Waite マーキング算法の正当性を検証してそのフィージビリティを示した。一方で、定理証明支援系を作業台(workbench)として用いながら抽象化の正当性を検証する統合検証環境 Agda-IVE を研究開発した。われわれは MLAT を Agda-IVE に組込み、研究計画の最終段階において、Agda-IVE のフィージビリティを確かめるために、実問題の検証を試みた。MPI の実装のひとつである YAMPII の開発者の協力を得て、そのなかから、ポインタ操作に問題が起こり得る部分を抽出し、その部分の正当性を Agda-IVE を用いて行なうという作業を行なった。その結果、Agda-IVE における、Agda と MLAT の相互作用が、システムの検証対象を確定する試行錯誤の段階において極めて有用であることがわかった。

なお、形式技法の基礎研究から技術移転にわたる幅広い活動をおこなうシステム検証研究センターが、本研究を契機に設立され、この分野の研究組織としては国内最大規模の組織として、本研究プロジェクト終了後も活動が続く情勢にあることを付け加えておきたい。3 名の博士号取得者も輩出している。これは本研究の直接の研究成果ではないが、重要なアウトカムあるいは波及効果である。本研究開始時にくらべ、現在ではソフトウェア不具合の社会的影響が格段に強く認識されており、この分野への社会的要請は強い。経済産業省による組み込みシステム検証試験施設の設立も、本研究が開始した研究センターの存在があってこそ可能になったとさえいえる。

【研究分担】

1. 数理モデルグループ

リアクティブシステム及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を担当

2. 支援ソフトウェア開発グループ

抽象化支援ソフトウェア MLAT の方式開発と試作を担当

3. 定理証明グループ

統合検証環境 Agda-IVE の方式開発と試作を担当

4. 並行プログラム検証研究グループ

YAMPII の検証実験を担当

4. 事後評価結果

4－1. 外部発表(論文、口頭発表等)、特許、研究を通じての新たな知見の取得等の研究成果の状況

1) 外部発表、特許出願等

原著論文 22 件、国際会議 10 件である。主要な成果に関する国際会議論文発表数としては必ずしも多くないが、比較的妥当である。また、成果の内容は一部を除き殆ど論文の形で発表されている。

特許は無い。この分野はソフトウエアの基礎分野であり、作成したソフトウエアは知的所有権を取るというよりも、公開し、広く使ってもらうことが重要である。今回の場合も作成したソフトウエアはそのように公開されており、問題はない。

2) 研究成果の状況

プログラムの検証問題における基礎理論として体系 Rμを構築し抽象化の数理モデルを確立した。また、モデル検査に用いられている論理を拡張しつつ完全性を持たせ、これによって強力な記述力を持つ論理を作り上げた。更に、ポインタ処理プログラムの検証を可能とするとともに、証明支援系を作業台として複数の自動検証ツールを用いる統合検証環境を初めて実現し、これを使った検証法を確立した。

これらは、いずれも形式手法･検証分野における重要なテーマであり、これらのテーマを目標として掲げ国際レベルの成果を上げた点は評価できる。

3) 当初の研究計画に対する、成果の妥当性

当初の計画では意味論研究のみが中心であったが、アドバイザリボードメンバの意見により支援ツール作成も視野に入れた結果、使える統合検証環境の成果を生み、今後の技術移転を容易ならしめて、検証技術全体の発展に繋がる成果となった。研究成果は、理論、方法論、システム開発のいずれにおいてもわが国においてトップレベルのものが幾つか出ている。しかし、具体的な検証事例を積み上げ、検証環境を使いこなして多くの使用経験を積み重ね実用的な抽象化手法のノウハウを蓄積することによって、与えられたプログラムの検証を可能ならしめるための一般的な方法論を明らかにすることは今後に残された問題である。

4－2. 成果の戦略目標･科学技術への貢献

1) 得られた研究成果の科学的･技術的インパクト

証明支援系を他の自動検証系の作業台としてもちいるという統合検証環境のアイデアはこの研究から出た実用的な考えである。従来の証明支援系は、厳格ではあるが、大規模なソフトウエアには適用困難で、それがこのようなシステムの実用を阻んでいた大きな原因である。検証システムを実際に開発し、それを用いて実証的にシステム検証の研究成果を出しているグループは世界的に見ても数少なく、この研究により、実用性に向けた道筋を与えたことは大きな成果であり、インパクトは大きい。検証事例、検証システムや方法論の開発をとおして実証的にそのインパクトを示していくことが今後重要である。

理論的な成果については、その評価にいま少し時間が必要であり、方法論や検証システムの開発をとおしてその有効性を実証していくことになろう。

2) 国内外の類似研究成果と比較した、研究成果のレベルと重要度

形式的手法の研究は欧米で地道ではあるが息長く続けられてきた。フランスではそのための資金が国から出ているし、米国ではスタンフォードの研究などが著名である。わが国の研究はその点、立ち遅れていた状況にあり、国内で比較できる研究は殆ど存在しない。この研究は優れた成果を生んだとは言え、この分野で未だ世界をリードする状況に至っているとは言い難い。しかしながら、世界のトップレベルの成果を生み、トップレベルに追いつく段階になったと言えよう。また、本研究は国内の研究活動をリードしており、学会で活発に活動し、この分野を活性化している点は高く評価される。

一方、この研究は、現在情報システムで大きな問題となっているデペンダビリティを向上させる切り札となる研究と考えられ、それをいち早く開始させたことは時宜を得た研究であったと言える。

3) 研究成果のさらなる展開

本研究で作成した統合検証環境を用いて、様々な実用ソフトウエアの信頼性を向上させる実用化研究への展開が期待できる。例えば、ソフトウエアのキー要素となるコンポーネントプログラムの検証がそうで、言語処理系、OS の部分モジュール、組み込み系ソフトウエア、プロセッサ仕様記述などが考えられる。更に、この環境と最近発展しつつあるフリーのモデル検査システムや SAT 解決システム(SAT Solver)などとの連携を図り、より強力な検証システムを実現することも期待される。

また、このプログラムで確立した論理 FOMμに基づいた検証支援ツールの開発や、統合検証環境自体の改良と洗練は、重要な研究テーマであり、それによってこの分野が更に大きく発展する可能性がある。

検証システムを基礎から研究開発しつつ、基礎基盤的な検証研究を進めているのが、本研究の最大の強みであり、その研究スタイルのゆえに、上記本研究で得られた成果をさらに発展させ得る可能性は高い。

当該分野の研究は極めて重要であり、世界的に見て研究投資が進むものと想定される。それに向けて、この分野の人材育成を迅速に立ち上げる必要があり、優れた人材の育成とその周りに多数の人材を配して実用的な検証システムを開発する地道な努力が必要である。

4－3. その他の特記事項（受賞歴など）

1) 本プロジェクトの社会的影響

このプロジェクトに大きく影響され、この研究グループをベースに産総研にシステム検証研究センターが設立された。これは、わが国における形式技法の初の研究拠点であり、この分野発展の重要な組織となり、自動車産業、法定計算など産学官にまたがる広い活動をおこなうものに発展している。また、最近はソフトウエアの脆弱性を原因とするシステム事故が頻発し、また、安全性への要求が国際的にも高まったこともあって、現在は形式技法の存在と重要性が広く知られるところとなり、IPA ソフトウエアエンジニアリングセンター、北陸先端科学技術大学院大学安心電子社会研究センターなどが開始されている。

また、このプロジェクトに影響されて、モデル検査技法の技術者向け研修コースが開発され、その一部がノウハ

ウ化された。その他、技術移転活動に際し、特許やノウハウが生まれており、その一部は有料で産業に利用されている。

こうした活動の結果として、産業界への検証技術の啓蒙に大いに寄与し、また学会においてもこの分野を活性化することに少なからず貢献した。本研究プロジェクトは、こうした付随的な成果に関しても評価するのが適当であると考える。

しかしながら、この分野の研究として函手意味論には圏論の深い理解が必須であり、その人材はまだ不足している。引き続き人材への投資が重要である。

2)総合的評価

研究成果が、すべて世界の最先端であるとは言えないが、研究内容としては統合検証環境など世界レベルのものが幾つか有る。研究活動とその成果のレベルは、間違いなく国内においては最先端にあり、検証分野において国内の研究活動を牽引する役割を果たした。しかしながら、検証システムの有用性を訴えるために、より多くの適用事例を増やしたり企業連携を強化するなどの工夫をより積極的におこなうこともあり得たと思われる。

このプロジェクトは、今後ますます重要性が高まる、バグの無い確実なソフトウエア開発の基礎技術研究である。その活動に当たっては、わが国にその人材が殆ど居なかったことから、人材育成から始めている。この 5 年間の活動成果として、理論、論理体系、検証ツール、統合検証環境など、一連の必要な要素を作り上げた。また、この活動を通して、わが国の各所にこの分野の研究センターが作られ、わが国のこの分野の発展を築いた。そういう意味で大きな成果を挙げたと考えられる。