研究課題別中間評価結果

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: 木下 佳樹
((独) 産業技術総合研究所情報処理研究部門システム検証研究センター センター長)

3. 研究概要
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のために困難であるため、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、その関係が抽象化条件:「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。

4. 中間評価結果
4－1. 研究の進捗状況と今後の見込み
抽象化の理論は予定通り実現され、途中から追加した抽象化サポートツールの試作も動きつつある。対話型証明支援系 Agda による統合検証環境も研究開始１年後に追加されたものであるが、Agda の研究グループの立ち上げから始めて、自動検証系 plug-in の設計・実現の他、Agda のドキュメンテーションや普及活動も精力的に進めており、順調に作成が進んでいる。これらの追加により研究が明確なものになっている。今後、利用例の蓄積によるシステムの評価と、その結果を手法に反映させることが重要であるが、ほぼ当初の計画通り進んでいると言えよう。

4－2. 研究成果の現状と今後の見込み
抽象化の理論は、Rμ論理の構築とその研究という形で実現され、抽象化サポートツールの試作に関しても、動くものができており、対話型証明支援系Agdaによる統合検証環境も開発が進みつつあって、成果が出ている。論文のみならず、ソフトウエア道具の具体的なものが実現され、他所で使うことが可能になりつつある。しかし、この研究の中心である抽象化支援ツールに関して、明確な成果が出るには、今後、多くの事例適用による実証結果に待たねばならないものと思われる。

4－3. 今後の研究に向けて

抽象化の事例研究を多く積み重ねることが重要である。しかし、それには更に研究員の増強が必要であるが、現在の日本にはこれにすぐ対応可能な人材が少なく、再教育から始める必要があるのが現状であろう。これは日本のソフトウエア基礎分野の人材が払底しており、世界的にも量的に遅れを取っていることに起因するものである。しかし、そういう困難な状況ではあるが、是非とも、この積み重ねの努力を願いたい。わが国においては、このグループに匹敵する規模を備えたシステム検証に関する研究プロジェクトは殆ど存在しないのであるから。

4－4. 戦略目標に向けての展望

本プロジェクトが目標とするシステム検証技術は、世界規模の高速ネットワークシステムが重要な社会基盤として機能し始めた今日の社会において、社会の基本的な安全性と信頼性を確保するための重要な中核技術の一つである。本プロジェクトの成果は、信頼性が高度に求められる組み込み型システム用ソフトウエアなど比較的小規模な問題には直ちに利用が考えられる他、現実の大規模な問題に対しては新たな攻略の糸口を与える可能性もある。更に、本プロジェクトで培われた技術や人材が将来の研究開発の基盤となる可能性は高い。

4－5. 総合的評価

本プロジェクトは、システム検証技術という重要な基盤技術について、明確な目的意識を持ってプロジェクトを運営し活発な研究活動を展開しており、優れた成果を挙げつつある。今後、事例適用の経験を多く積み重ねることで、より実質的で具体的な成果を挙げことができることを期待する。