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　システム検証研究ラボ長）

「検証における記述量爆発問題の構造変換による解決」

1.研究実施概要

研究のねらい・着眼点　ソフトウェアの数理的検証法が，ソフトウェア開発の現場で用いられることは，まだ稀である．その最も大きな原因は，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ことにある，と研究代表者は考えた．この記述量爆発の問題を解決するため，ソフトウェアが持つ数学的構造を明確にして質的な変換を施すことにより，検証における記述量を劇的に（ある場合には無限から有限に）減少させる技法を研究する．一ステップごとのミクロな正確さを求める従来のソフトウェア検証論の成果の上に立って，システムのマクロな整合性と正確さを求めるのが本計画の立場である．

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，より記述量の少ないシステムの数理モデルNを設定して，もとの数理モデルMと関係づける．検証したい項目（システムの性質）をPとするとき，「NにおいてPが成り立つ」⇒「MにおいてPが成り立つ」がなりたつときに，MとNの間に抽象化関係がある，という．（１）Nおよび（２）MとNの間の抽象化関係の二つが見つかれば，MにおいてPが成り立つことを検証する代わりに，より記述量の少ないNにおいてPが成り立つことを検証すれば十分である．本計画では，記述量爆発の問題を，このような抽象化のアプローチで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．プログラムはアルゴリズムの記述だとみなしてモデル化する入力出力関係システムは，無限ループに陥っては困るシステムである．これに対し，電子機器に組み込まれた制御ソフトウェアなどは，刺激に対して応答する無限に動き続けるリアクティブ・システム，さらには，タイムアウトの可能性までもつ実時間システムとみなすのが適当である．本計画では，検証の対象をリアクティブ・システムおよび実時間システムに設定し，誤動作の影響がより大

きな組込み制御システムへの適用の可能性を拓く.

将来展望　強力なシステム検証技術は，広く産業界から求められている需要の大きい技術であり，信頼に足る技術を提供できれば，それ自体で産業化していく可能性をもつものと考える．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相互作用させて，科学的技術に基づく産業振興を目指す.

2.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、システム検証研究ラボ長）

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、システム検証研究ラボ副ラボ長）

② 研究項目：抽象化支援ソフトウェアの方式開発と試作