群大工学部 研究室から 72

名前と逆のハードな作業

ソフトウエア・システム検証

大学院工学研究科
情報工学専攻

定理証明器利用とモデル検査で 複雑な仕組みの確認・修正を

数理的技法を駆使して情報社会を保障する

ソフトウエアのミスでロケットが爆発―これは、1996年6月4日に実際に起こった出来事です。ヨーロッパの無人ロケット「Ariane 5号」は、ソフトウエアのミスによる制御不能に陥り、打ち上げ後約40秒で爆発してしまいました。32ビット浮動小数から16ビットへの変換に失敗して、さらにエラー処理がきちんと行われなかったことが原因と報告されています。また、2001年にも携帯電話のソフトウエアの欠陥により50万台以上の携帯電話が回収されました。

私たちの研究室の大きな目的は、このような不具合が起こらないシステムやソフトウエアの開発を支援する技術を確立することです。研究室には藤田准教授、大学院生2人、4年生4人が在籍しています＝写真。

私たちの身の回りのものは便利になり多くの機能を持っています。そして、その仕組みはたいへん複雑になってきています。ものが要求どおりに作られきちんと動作することを確認する作業は、想像以上に手間がかかるものとなってきています。ソフトウエアの場合も同様で、「ソフト」という言葉から受けるイメージとは相反して、その確認や修正は極めてハードな作業です。

現在のところ最も厳密である検証方法は、定理証明器を利用する技法と、「モデル検査」と呼ばれる技法です。どちらの技法も論理学に基づいており、それらの理論の基礎は数学的に揺ぎないものです。

定理証明器を応用した例として、電子財布の中で使われているJavaカードプログラム(図1)の検証事例が挙げられます。Purseアプレットの中でお金の計算をするJavaプログラムとその仕様をまとめたものが図2にあります。

ここで、計算機に実装されている定理証明器を活用して、プログラムが仕様を満たしていることを一つずつ証明していく(図3)ことによって、このプログラムの要求どおりの動作を保障することが可能になります。

次に、モデル検査の技法を使った例として、ネットワークのパケット転送システムの検証が挙げられます。図4はパケット転送システムをモデル化したもので、状態遷移系またはオートマトンと呼ばれています。

このモデルにおいて、計算機の力を借りることにより、システムのとりうる全状態を網羅的に検査することができます。例えば、転送システムの動作を操作(図5)することができます。また、システムがダウン(Crash)する確率などを評価して(図6)、その設計に反映させることができます。モデル検査技法により、IEEEの標準プロトコルの振りあいまいさが発見されて、改善された実例も報告されています。

このような数理的技法を駆使し、情報社会で不可欠であるシステムやソフトウエアの信頼性、安全性を保障することを目指して、研究室のメンバーが力を合わせて研究を行っています。

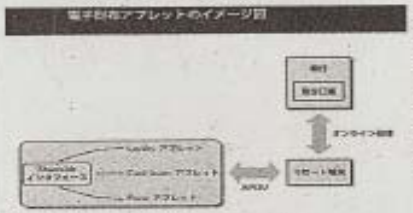
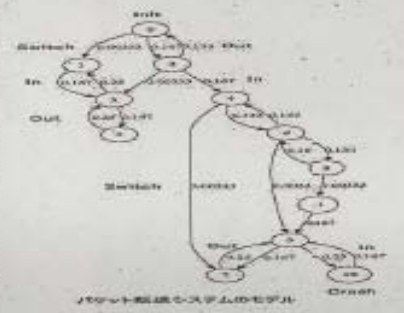


図1

図2

図5

図6



パケット転送システムのモデル

図4

図3

〈私が執筆しました〉

藤田憲悦 准教授

【プロフィル】秋田県出身。東北大学大学院工学研究科博士課程修了、工学博士。九州工業大学を経て2004年から現職。論理学、ラムダ計算などの研究に従事。