ソフトウェアのミスでロケットが爆発！？　　---ソフトウェア・システムの検証---

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 Ariane5 号は，ソフトウェアのミスにより制御不能に陥り，打ち上げ後約 40 秒で爆発してしまった．32 ビット浮動点小数から 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ェアの欠陥により 50 万台以上の携帯電話が回収されました．

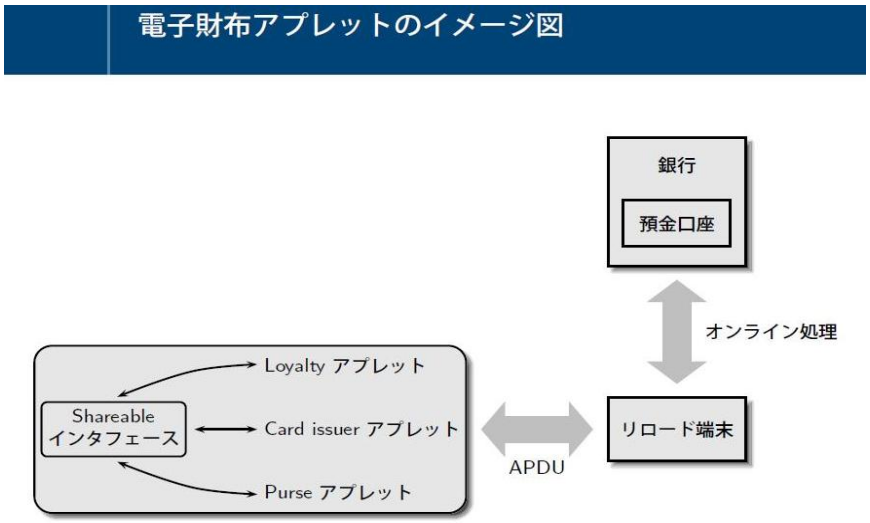
私たちの研究室の大きな目的は，このような不具合が起こらないシステムやソフトウェアの開発を支援する技術を確立することです．現在研究室には，藤田准教授，大学院生 2 名，および 4 年生 4 名が在籍しています（写真）．

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，その仕組みは大変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．ソフトウェアの場合も同様で，“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

的に確固としたものです.

定理証明器を活用した例として,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.

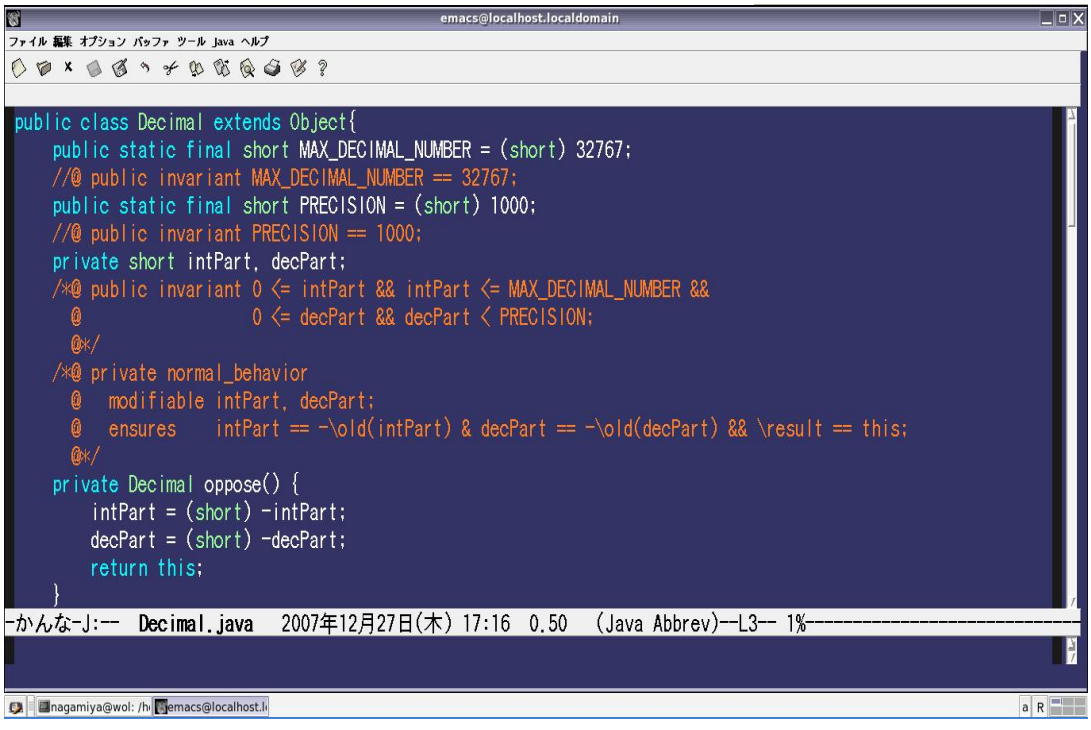


図２：Javaプログラムと JML 仕様

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.

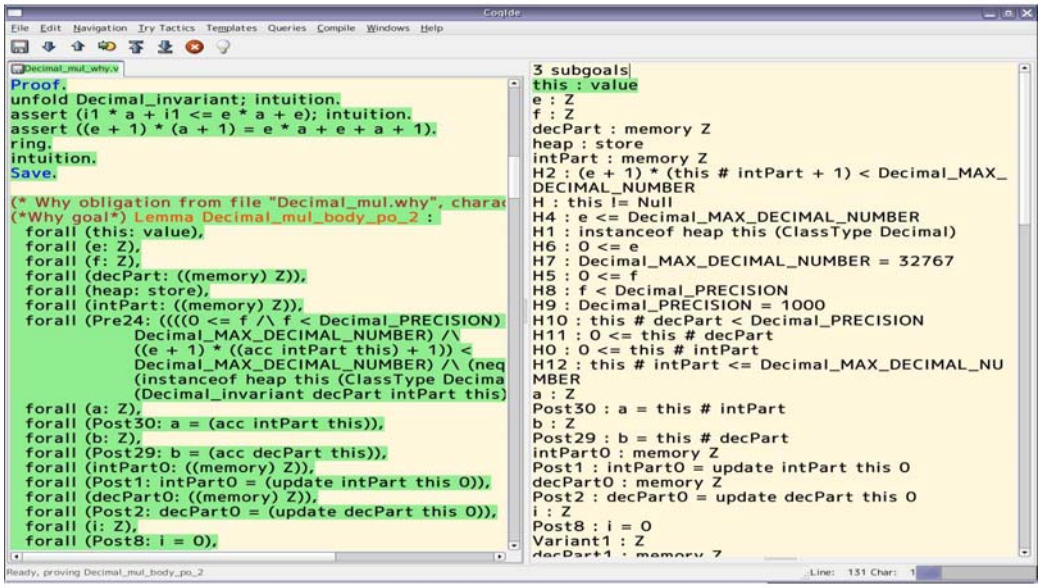
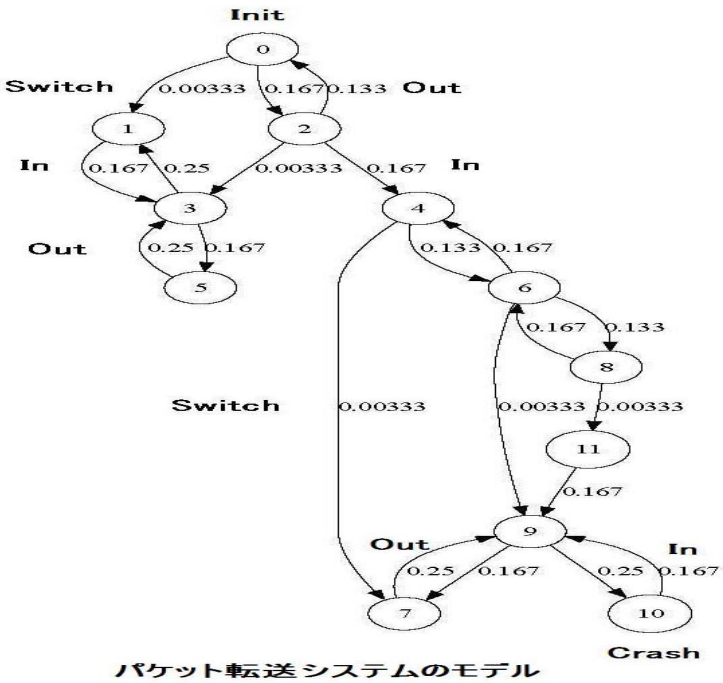


図３：プログラムが仕様を満足していることの証明

次に，モデル検査の技法を使った例として，ネットワーク上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.



パケット転送システムのモデル

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.

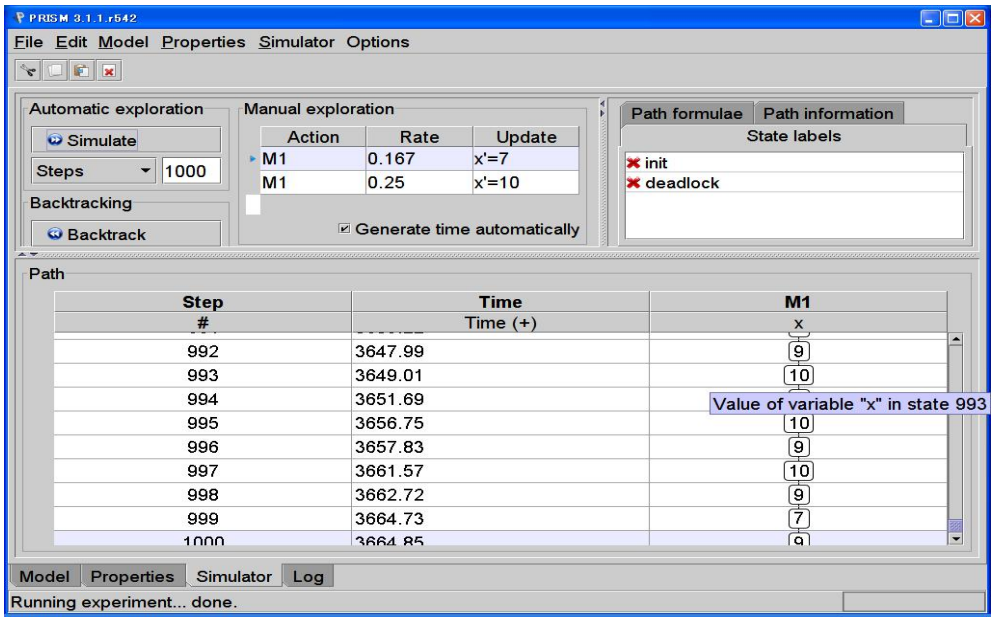


図５：パケット転送システムの動作の模倣

例えば，転送システムの動作を模倣（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誤りや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．

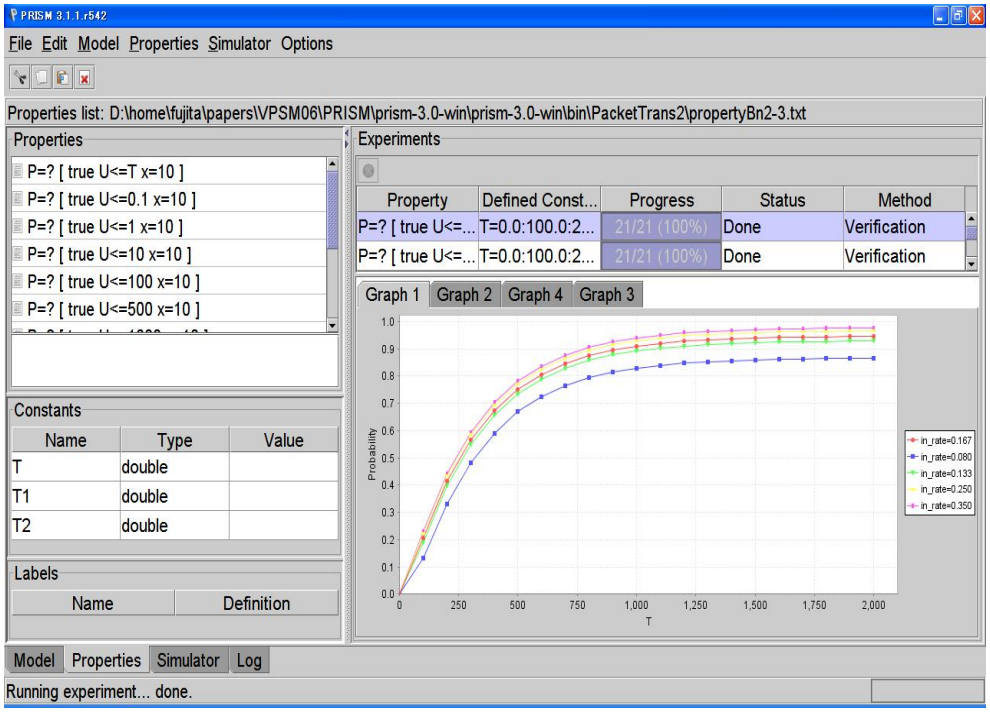


図６：パケット転送システムがダウンする確率の計算

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ェアの信頼性，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．

情報工学科　数理情報工学講座

藤田憲悦：略歴

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 年より現職．論理学，ラムダ計算などの研究に従事．