

プログラム検証技術の基礎付けと応用



研究代表者	東北大学・電気通信研究所・教授	
	海野 広志（うんの ひろし）	研究者番号：80569575
研究課題情報	課題番号：25H00446	研究期間：2025年度～2029年度
	キーワード：プログラム検証、論理学、計算論、最適化理論、学習理論	

なぜこの研究を行おうと思ったのか（研究の背景・目的）

●研究の全体像

コンピュータを動かすソフトウェアが意図通りに動作することを数学的に保証する技術が、**プログラム検証**である。最先端のプログラム検証技術は、効率のための様々な工夫の累積により複雑化している。その複雑さのため全貌を見通すことが難しく、その結果として、数学的に誤っていたり、拡張が困難だったりといった問題を抱えている。このような状況を打破するために、本研究では**論理学・計算論・最適化理論・学習理論**などに基づいて数学的に簡潔な理論基盤を確立し、**正しさと拡張性と効率**を兼ね備えた検証技術を実現する。さらに、基礎付けられた検証技術を応用からの要請に応える形で拡張する。特に近年重要性を増している**並行・並列・分散システム**や、セキュリティ・プライバシーに不可欠な**暗号・確率システム**、CやRustといった言語で記述された**システムプログラム**のための自動検証ツールを理論基盤に基づき実現する。

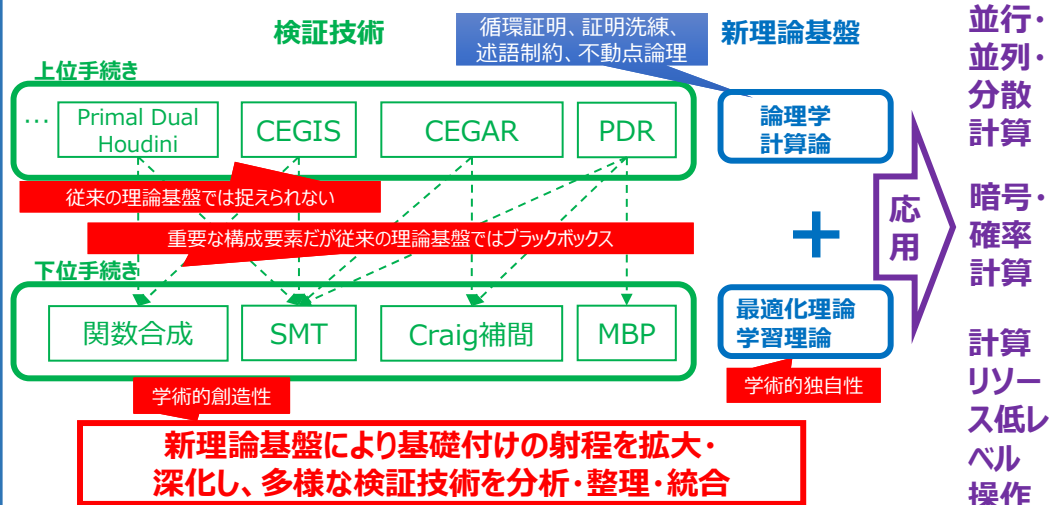


図1 本提案の新理論基盤

●研究の背景

プログラム検証技術は、飛行機の制御プログラム、CPUなどのハードウェアの設計書、パソコンの基本ソフトの一部であるデバイスドライバと呼ばれるプログラム、クラウド計算環境におけるネットワークの設計書など、多様なソフトウェアの検証に用いられ、意識はされにくいものの社会基盤の安定に寄与している。プログラム検証は一般にはコンピュータで完全に行うことはできないことが証明されており、すべては解けないものの現実社会で必要となる範囲なら上手く扱えるような工夫（ヒューリスティクス）が重要となる。長年のプログラム検証の研究は、こうした工夫を様々に集めて、現実の問題を高速に解けることを目指して発展してきた。

こうした工夫の集積である最先端の検証ツールは著しく複雑で、その動作を正確に理解することは研究者にとっても容易ではない。例えば、検証ツールにほどこしたほんの小さな工夫が、検証ツールの重要な性質である停止性を損なっていたのだが、そのことに十年近く誰も気づいていなかった、などということが起きている。検証ツールの複雑さは、正しさや停止性などの検証ツールに必要な性質を保証することを困難にするだけでなく、拡張の困難さや検証に必要な時間の予測不能性など、様々な問題を生んでしまっている。

●これまでの研究

プログラム検証ツールの複雑化に対処するために、研究代表者と研究分担者らはプログラム検証技術を簡潔な数学的基盤の上に再構築する研究を行ってきた。こうした研究は論理学や計算論などに基づいている。例えば、様々な検証問題を不動点論理式の真偽判定問題として統一的記述することで、特定の問題のために開発された検証技術を別の問題に適用可能にすることで、多様な問題に対して効率的な検証ツールを作成してきた。また、手続き型プログラム検証問題と循環証明体系における証明探索問題の関係を指摘し、既存手法を証明理論を通じて整理した。さきほど触れたプログラム検証技術の非停止バグは、こうした整理を通じて研究代表者らが指摘したものである。

●研究の目的

本研究の目的は、多様なプログラム検証技術をヒューリスティクスも含めより深く分析・整理・統合可能な数学的簡潔さを備えた理論的基盤を与えることである。そのために、数理最適化や学習理論などを駆使して、従来の論理学・計算論では捉えられなかったヒューリスティクスも含めた基礎付けを行う。また高い拡張性を活かして、応用上の重要性の高い並行・並列・分散計算、暗号・確率計算、および低レベルプログラムなどの検証にプログラム検証の最先端技術を適用する。

この研究によって何をどこまで明らかにしようとしているのか

●基礎付けの射程の拡大・深化

本研究の目的は、プログラム検証技術の簡潔な数学的基盤を与え、正しさと拡張性と効率を兼ね備えた検証技術を実現することである。これまでよりも基礎付けの射程を拡大・深化し、高い拡張性を活かして、応用上の重要性の高い並行・並列・分散・確率・暗号・低レベルなどに対応した検証システムを構築する。そのために、プログラム検証の分野ではこれまで利用されてこなかった**最適化理論**（特にLagrange双対性）を駆使することで、最先端検証技術の上位・下位手続き両方を分析・整理・統合し、検証技術・ツールの正しさ・拡張性の向上に貢献する。さらに、**計算論的・統計的学習理論**により検証技術における反復手続きの収束性および収束速度を解析し、検証技術・ツールの効率の向上に貢献する。

●現実のソフトウェアの検証への応用

本提案の有効性を示すために、Webとクラウド技術を支える要素技術である問合せ処理とトランザクション処理の検証を行う。これらは下記の困難により既存技術・ツールでは十分に扱うことができなかった。

- スループットやレイテンシ、耐故障性の向上のために通信を行いながら並列・並行・分散的に動作
 - 悪意を持った攻撃者からセキュリティ・プライバシーを守るために暗号・確率を用いる
 - 高性能を実現するため計算リソースの低レベル操作を許容するシステムプログラミング言語CやRustで記述
- 本提案では新理論基盤により検証ツールを並列・並行・分散計算、暗号・確率計算、計算リソースの低レベル操作に拡張することによって困難を克服する。

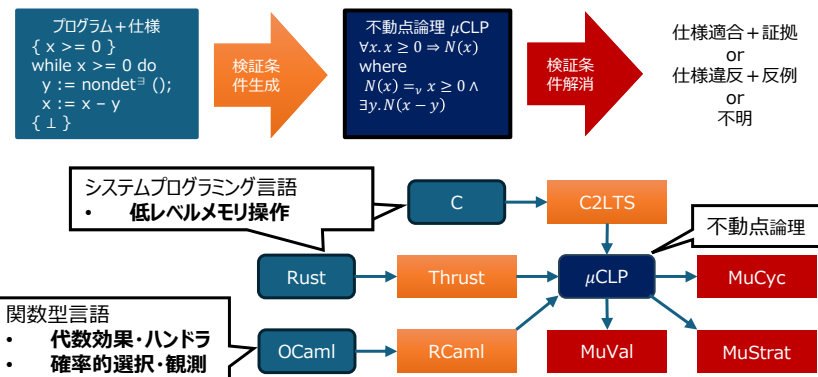


図2 本提案のプログラム検証ツール群 CoAR

本課題では
**CoARの
ツール群を
新理論基盤
により並列・
並行・分散
計算、暗号・
確率計算、
計算リソース
の低レベル操
作に拡張**