2022 年度 個人研究実績・成果報告書

2023 年　4　月　14　日

所属	政策情報学部	職名	教授	氏 名	大矢野潤
研究課題	安全なシステム構築のための検証技法の開発とその具現化				
研究キーワード	ソフトウェア工学、並列モデル、モデル検査、暗号プロトコル、スマートコントラクト	当年度計画に対する達成度	3.概ね順調に研究が進展し、一定の成果を達成したが、一部に遅れ等が発生した		
関連するSDGs項目	9. 産業と技術革新の基盤をつくろう	16. 平和と公正をすべての人に	該当なし	該当なし	

１．研究成果の概要

社会基盤の一部を形成するソフトウェアは高度に安全であることが必要であり、その性質を補償するためには（半）自動証明技術、すなわち、決定可能で同時に現実的な時間内で計算可能な証明アルゴリズムの開発が必要になります。私は、これまで、抽象状態機械の到達性解析による並列プロセスの安全性検証について取り組んできました。安全性は、「悪い状態に到達しない」という到達性解析により検証可能です。近年、インターネット上で利用可能な仮想通貨が開発され、急激にその利用が広まって来ました。大手の仮想通貨取引所の利用高は月間数兆円を超える規模にまで成長しているものもあり、当然そのシステム不具合は社会基盤の信頼性を揺るがすものになるため、スムーズな運用と高度な安全性が同時に求められます。

2018～19 年度は、本学経済研究所より「安全で公平な金融システムの実現に資する FinTech フレームワークの提案」に関する研究助成を認めていただき、既存のスマートコントラクトアルゴリズムをプロトコル記述言語 Promela で記述したものをモデル検査器 SPIN によって検証した結果、「安全ではあるが不公平」な状態を検出することに成功しました。この結果は 2020 年度に論文としてまとめられ、国府台経済研究「安全で公平な金融システムの実現に資する FinTech フレームワークの提案特集号 第 31 巻 第 2 号 2021 年 3 月」において掲載していただくことができました。上記の結果は、特定のプロトコルに関して得られたものであり、さらなる一般化が必要であることはいうまでもありません。しかし、いわゆる暗号プロトコルを直接取り扱うアプローチは、解くべき問題の規模が極端に大きくなりすぎることを痛感し、2021 年度後半からは一般的なモデル検査で観測される「状態数爆発」に対応すべく、これとは逆のアプローチ、すなわち、解くべき問題を手頃な問題に固定し、その解を求める手続きとして抽象解釈実行を試みました。

2022 年度は、ゲームのボードをいわゆる並列プロセスの集合体としてとらえ、パズルが解けた状態を不動点とみなします。その際、パズルを直接解くときにおこる状態を抽象領域に埋め込むことで状態数爆発をうまく回避できることがわかりました。この試みはとても良く機能し Kaggle 上で公表されている 100 万個の sudoku 問題のすべて(https://www.kaggle.com/datasets/bryanpark/sudoku)を現実的な時間(1 問 0.1 秒程度)で解くプログラムとそのインタフェイスを開発しました。さらに、sudoku の解が複数存在する場合において、いわゆる方程式論で登場する代数構造があるのではないかということに気がつきました。現在はこの着想を掘り下げ、抽象解釈とガロア対応、不動点理論を組み合わせてさらなるアルゴリズムの深化を目指せるところまで来ましたので、2023 年度はこの問題について決着し成果を発表したいと考えています。

これに加えて 2022 年度特別講義 A(データビジュアライゼーション)の理論的準備、および開発環境整備を行い、秋学期に授業を実施しました。具体的には鎌ケ谷市の Web サイトで PDF 形式により提供されている環境白書を Web 化し、スマートフォン、PC などデバイスに依存しない形で提供し、さらに統計学、機械学習を地域の水質データに適用し見える化を行う具体的な手続きを実践しました。外部への発信としては、授業の初回と最終回では鎌ケ谷市環境課の職員を招待し、授業の成果を学生と共にプレゼンテーションしました。特に 2023 年 3 月 11 日(土)の「鎌ケ谷プロモーション DAY!!」では、この授業で学んだ成果を学生が市民に対して発表し、官学連携としての市民データサイエンスの有効性を示せたのではないかと考えています。

データマイニングを授業に取り入れるためには通常の授業に比べ、比較にならないほどの準備が必要であり、2022 年度の後半はほとんどこのために費やしたと言っても過言ではありません。「当年度計画に対する達成度」で「遅れが生じた」としている原因はここにあります。しかし、本講義で再確認した機械学習の知見は、授業の範疇を越え、次年度以降私個人の研究の幅を広げる活動であったと考えています。

２．著書・論文・学会発表等（査読の有無及び海外研究機関等の研究者との国際共著論文がある場合は必ず記載）

【論文（査読あり）】

特になし

【著書・論文（査読なし）】

特になし

【学会発表等】

特になし

３．主な経費

閲覧用 PC、書籍の購入

４．その他の特筆すべき事項（表彰、研究資金の受入状況等）

特になし

（本文は 2 ページ以内にまとめること）