2021 年度 個人研究実績・成果報告書

2022 年 4 月 9 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	モデル検査、スマートコントラクト	当年度計画に対する達成度	2.順調に研究が進展しており、期待どおりの成果が達成できた		
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。2021 年度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、下記の２つのアプローチを開始しました。

1. 機械学習、深層学習のモデル検査への応用
2. 状態空間を対称性で割って得られる商空間へ抽象化

近年、モデル検査に人工知能の分野で得られた技術を応用する試みが開始されています。深層学習で使われるテンソルを一つの状態(ベクトル)とみなし、状態遷移行列によるテンソル計算を GPU などの高速なプロセッサで実行することで、いわゆる「力ずく(brute force)」の状態検査に利用することが可能ではないかと考えるようになりました。これはいわゆる具体的に有効な探査アルゴリズムがない場合の最後の手段の一つとしようというものです。2021 年度は一般的な機械学習と深層学習の調査に着手しました。本研究とは直接関係はないものの、鎌ケ谷市の歴史的古写真を深層学習の一種である GAN(敵対的生成ネットワーク)を用いて自動彩色しました。具体的には、DeOldify というオープンソースソフトウェアのソースコードを解析し若干の変更を加えたものをもちいてモノクロの古写真 36 枚を彩色しました。彩色を施した写真は鎌ケ谷市歴史資料館に寄贈し、歴史資料館館長、学芸員の方々からご好評いただくことができました。また、同調査で得られた知

見は 2022 年度政策情報学部特別講義「データビジュアライゼーション」において、学生のデータサイエンス能力向上を目指した授業において学生に還元することになっています。

次の、状態空間の商空間を計算するモデルケースとして、ペンシルパズルの一種である「数独(Sudoku)」に取り組みました。Mathematics of Sudoku (Wikipedia)によれば、数独の妥当な盤面は約 6.6709×10^{21} 通り存在するが、群論の対称性 (Symmetric) で割って得られる「本質的に異なった」状態(盤面)空間は 5,472,730,538 に限定できることが分かっています。モデル検査の分野においても、対称性を応用した状態数削減は古くから試みられているテクニックの一つです。2021 年度は数独をプロセス代数として定義し、解発見の手続きを状態遷移列としてとらえることができました。これにより対称性の正当性や数独の解を発見するためのテクニックをプロセス代数の言葉で説明することが可能となると考えています。論文等で発表可能な成果に近づいていると実感しており、2022 年度は、まず、その成果をまとめてみたいと考えています。

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

開発用 PC 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）