

## 2023 年度 個人研究実績・成果報告書

2024 年 4 月 11 日

所属	政策情報学部	職名	教授	氏名	大矢野潤
研究課題	数学パズルのプロセス代数記述と時相論理による解法の形式化				
研究キーワード	数学パズル, プロセス代数, 時相論理, ガロア対応, ソフトウェア工学	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。

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」な状態に到達することを示すことができました。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であるパズルに固定し、その解を求める手続きとして抽象解釈実行を試みることにしました。

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すという着想を得ました。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。この試みはとてよく機能し 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ースを開発しました。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する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るさらなるアルゴリズムを深化させることを開始しました。

2023 年度は引き続きこの問題についてとりくみました。これまでの solver プログラムは手続き型言語 python を使用して記述してきましたが、手続き型言語では記述内容の数学的構造とプログラムの構造との関係が分かりづらいため、2023 年度は Haskell という関数型言語に持ち替えました。アルゴリズムを関数として捉え直す作業は、ほぼ最初からアルゴリズムを作り直すことになりました。本研究で開発したガロア対応を用い

た不動点計算アルゴリズムは人間がペンシルパズルを解く方法に非常に親和性が高く、直感的に理解しやすいものになりました。通常、人間にとって直感的なプログラムの動作は時間がかかるのが相場ですが、本アルゴリズムは **Haskell** による代数的問題解法の教科書的な論文で紹介されているプログラムよりはるかに高速に動作します。具体的には人為的に作成した 10 万通り以上の別解を持つパズルに「教科書的な」アルゴリズムを使用した場合と比較して、4 倍程度高速に動作することを観測しました。技術的に最適化されたアルゴリズムよりも本研究で開発した「直感的な」プログラムが高速に動作することは直感に反するものでしたが、本研究のアルゴリズムがパズルを数学的に綺麗に解いているということを実感しました。

現在は、このアルゴリズムを、単に問題の解集合をもとめるだけでなく、その解が導き出される理由、すなわち問題が持つ数学構造を形式的に解明することができるように深化させています。2024 年度は本アルゴリズムとその理論を完成させ、論文執筆し、学会で発表する予定です。

## 2. 著書・論文・学会発表等

### 【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

サーバマシン周辺機器、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）

本研究に直接関係するものではありませんが、鎌ヶ谷市歴史資料館と共同で取り組んでいる AI を利用した歴史的な古写真の自動彩色プロジェクトの作品が「鎌ヶ谷の小学校 150 年史（展示）」[https://www.city.kamagaya.chiba.jp/sisetsu/kyoudo\\_2/kyoudo-info/syougakkou\\_150th.html](https://www.city.kamagaya.chiba.jp/sisetsu/kyoudo_2/kyoudo-info/syougakkou_150th.html) で展示されました。また、歴史的な古写真を自動彩色したものを一部立体映像化する試みを歴史資料館と共同で開始することになりました。

(本文は 2 ページ以内 にまとめること)