研 究 終 了 報 告 書

「効率的な学習可能性の証明困難さに関する研究」

研究期間: 2019 年 10 月～2021 年 3 月
研 究 者: 七島 幹人

1. 研究のねらい

学習アルゴリズムの設計において，効率的な学習時間は重要な指標の一つである．例えば，どれほど素晴らしい結果が期待される学習アルゴリズムでも，学習に数億年の時間を要するのであれば全く意味が無い．一方で，時間を多くかけるほど，同じデータからでもより多くの知識を得られるということは自然な期待である．また直感的には、同じ学習時間であっても，学習対象が複雑になればなるほど，学習結果は悪くなることが予想される．すなわち，学習効率と学習クラス，及び，精度の間にはトレードオフが存在する．そして，その理論的保障を与えることは，高性能かつ信頼できる機械学習技術に繋がる重要な研究項目である．

「計算論的学習理論」はこのように，どのような学習設定・対象において効率的学習が可能かという問いを研究対象とする研究分野である．当分野における究極的な目標の一つは効率的学習可能なクラスと学習困難なクラスの境界の特定，すなわち，効率的学習可能な最大のクラスと効率的学習困難な最小のクラスの特定である．しかし，現在知られている効率的学習可能クラスの上下界の間には，大きなギャップが存在しており，この目標の達成のためには，多くの未解決問題が残されている．

本研究ではこのような現状を俯瞰し，我々が効率的学習可能性の証明において暗示的に直面している障壁を特定することで，メタ的視点から今後の分野のブレイクスルーに繋げることを目標とする．特に，ここで我々研究者が解こうとしている問題は，ある意味で，学習対象クラスを入力として受け取り，その効率的学習可能性を判定する，計算問題として定式化される．このような学習におけるメタ問題の計算複雑さ理論からの解析から始め，効率的学習可能性証明の困難さ・障壁に関する理論的基盤の確立と，効率的学習可能性という概念のより広い，理論計算機科学的観点からみた性質の特定を行う．また，得られた結果に基づく既存学習モデルの妥当な要件緩和の提案，及び，学習の複雑さ・証明困難さを基にした暗号プリミティヴへの応用を狙う．

2. 研究成果

（1）概要

本研究では，はじめに，研究目標にある学習可能性判定問題の定式化を行い．その計算複雑さの解析を行った．結果としてそのような学習可能性判定問題の計算複雑さが LIH 予想と呼ばれる，多項式サイズ回路の PAC 学習の多項式時間困難性で特徴付くことが判明した．そこで，この結果を本研究の出発点とし，LIH 予想が理論計算機科学においてもつ意味，特に，暗号理論や計算複雑さ理論の従来の概念との関係の調査することで，学習可能性判定問題の困難さのより強い根拠に基づく議論，及び，暗号理論への応用を図った．特に，現状として，LIH 予想と一方向性関数と呼ばれる暗号の核となるプリミティヴ，及び，P≠NP 予想などの計算複雑さ理論の概念との間にはギャップが存在する．そこで，そのようなギャップの詳細な解析・及びそのギャップを緩和する為に有効な手段の特定というメタ的観点からの研究を重点的に行い，以下のような成果を得た．

LIH 予想と暗号理論との関係については，従来の暗号プリミティブの安全性要件を緩和した概念である追加入力付き暗号プリミティヴの理論をより深化させ，LIH 予想に対する初の暗号学的特徴付けや，LIH 予想の自然な変種である平均時 LIH 予想と先行研究で提案されていた追加入力付き一方向性関数との等価性などを証明した．これは，学習複雑さと暗号理論間に暗示的に存在したギャップについて一つのクリアな視点を与える成果である．

LIH 予想と計算複雑さ理論との関係については，特に NP の平均時困難さとの関係性について調査し，ある意味での，最悪時学習から平均時計算への帰着の構成を行った．これは，LIH 予想と暗号理論との従来のギャップを緩和するという観点からも重要な成果である．

加えて，LIH 予想と計算複雑さ理論，及び，暗号理論とのギャップを更に緩和するために有効な手段の特定という目的から，現在の理論計算機科学における標準的な枠組み（相対化する手法・非適応ブラックボックス帰着）による障壁の理論的な解析を行った．現在，ここで得られた知見をもとに，これらの障壁を破るような手法について検討中である．

（2）詳細

A. 「効率的学習可能性判定の LIH 予想による特徴付け」

本項目では，研究目標の一つである学習可能性判定問題の定式化を行い，その計算複雑さの解析を行った．結果として，学習可能性判定問題が多項式時間で解けない(クラス P に含まれない)ことと，多項式サイズの回路が効率的学習不可能であること（LIH 予想）の等価性を得た．LIH 仮定は，計算複雑さの理論における P≠NP 予想のように，計算論的学習理論においては最も基本的な困難性仮定の一つである．本結果はそのような分野の自然な困難性仮定のもとで，我々が効率的に学習可能性判定を行えないようなクラスの存在を示唆する結果となる．この結果は成果リスト(1) 1.中にて発表済である．

またこの結果は，ACT-X の研究において以下の点で重要な指標を与えるものである．すなわち，学習可能性判定問題の困難さの性質を解析するための１つのアプローチとして，LIH 予想の解析を行えばよい．特に現状として，LIH 予想の理論計算機科学全体における位置づけ，特に計算複雑さの理論と暗号理論との関係については分かっていない点が多い．例えば，安

全な暗号システムが存在すれば LIH 予想が導かれ(暗号理論→学習複雑さ), LIH 予想からは P≠NP が導かれる(学習複雑さ→計算複雑さ). 一方でその逆方向は証明されておらず, (学習複雑さ→暗号理論)を示すことは本研究で扱う困難性の暗号への応用, 及び(計算複雑さ→学習複雑さ)を示すことは, より強い根拠の下での本研究の困難性の議論に繋がる. そこで, 今後の研究方針を LIH 仮定の理論計算機科学全体における位置付けと定め, 達成目標として (B) LIH を基にした一方向性関数や疑似乱数生成器の構成(これは暗号方式の核となる暗号プリミティヴである), (C) LIH と計算複雑さ理論, 特に NP 問題の複雑さとの関係の調査, 及び, (D) 目標(B)(C)に関する現在の証明手法による障壁の特定に絞り, 研究を進めた.

B. 「LIH 予想及びその変種と弱い暗号プリミティヴの等価性」
本項目では LIH 予想と一方向性関数をはじめとする基本的暗号プリミティヴの関係・及びギャップの解析を行った. 一つ目の結果として, 既存の疑似乱数生成器の安全性要件を弱めた暗号プリミティブである Auxiliary-Input Local Hitting Set Generator (AILHSG)を導入し, AILHSG の存在と LIH 予想の等価性を証明した. 学習可能性と暗号理論の関係は計算論的学習理論が導入された論文(Valiant, CACM,1984)から言及され研究されてきたが, この結果はその最も基本的な学習モデルである PAC 学習の困難性に対する約 35 年来初の暗号学的な特徴付けと捉えることができる. この結果は成果リスト(1) 1.中にて発表済である.
また, 後続の研究として, 従来の学習モデルを自然に平均時の学習要件に緩和することで, 平均時 LIH 予想を導入し, より標準的暗号プリミティヴに近い, 追加入力付き一方向性関数(AIOWF)の存在との等価性を証明した. この結果は成果リスト(1) 2.中にて発表済であり, 前述の成果と合わせることで学習複雑さと暗号理論の間に暗示的に存在したギャップについて新しく一つのクリアな視点を与えるものである.
また, 既存学習モデルの妥当な要件緩和の提案という研究目標に従い, 成果リスト(1) 2.中の平均時要件をもつ学習モデルにおいて, 従来の学習モデルでは効率的学習アルゴリズムの設計が長年未解決であるような設定に対し(junta 学習), 効率的な学習アルゴリズムを構成することで, 提案学習モデルの効率的アルゴリズム設計における有効性について肯定的な結果を得た.

C. 「LIH 予想と平均時計算困難さの関係」
本項目では LIH 予想, 特にその中で議論される PAC 学習モデルの学習要件の性質の調査を行った. PAC 学習モデルの学習要件は学習のためのデータ(すなわち, 入力)はある分布の元で生成されるという点での平均時的な要件と, 任意のデータ生成分布の元で学習クラス内の任意の関数を学習するという最悪時要件を持ち合わせており, この点がある意味で, P≠NP 予想(完全に最悪時ケースで議論される)や暗号プリミティヴの存在(完全に平均時ケースで議論される)とのギャップを生じていると考えられる. そこで, 本項目では平均時計算困難さと学習困難性の関係性の調査, 特に, NP 問題における平均時容易さの仮定のみから, 多項式サイズ回路を効率的に学習するアルゴリズムが設計できるか, という点について調査した(これはある意味で, とても性質のいい SAT ヒューリスティクスがあったとき, それをとても性質のよい学習アルゴリズムに変換できるか, という問いに対応している).

結果として，NP 問題における平均時容易さの仮定に基づいて，任意の多項式サイズ回路を任意の未知の P/poly-samplable という自然な仮定をもつデータ分布上で Agnostic 学習する非常に強力な学習アルゴリズムが構成できるという定理を得た．これはある意味で，最悪時要件を持つ学習問題を平均時 NP の問題に帰着する「最悪時学習-平均時計算帰着」の構成と捉えられる成果であり，成果リスト(1) 3.中にて発表済である．

D.　「学習階層の縮退における証明手法の特定」

上記で得られた関係性や等価性を更に発展させるにあたり，理論計算機科学の標準的証明手法の障壁についての解析を行った．これにより，本質的に有効となり得る証明手法をメタ的視点から特定することで，将来的の更なるギャップの緩和に繋げることを狙う．

1 つ目の結果は P≠NP 予想を基にした AIHSG（これは LIH と等価な AILHSG を更に弱めた，非常に弱い安全性要件をもつ暗号的プリミティヴである)の構成についてである．もしこのようなプリミティヴが非適応ブラックボックス帰着という標準的枠組みのなかでの安全性証明に基づいて構成できた場合，その結果を用いて P≠NP 予想を基に一方向性関数を構成できるという結果を得た．これは，理論計算機科学における長年の未解決問題（一方向性関数の NP 困難性に基づく構成）における新たなアプローチを与える一方で，非適応ブラックボックス帰着における AIHSG の NP 困難性に基づく構成がそのような未解決問題の解決よりも難しいという困難性の根拠ともとれる結果である．この結果は 2021 年の ITCS という理論計算機科学における主要国際会議にて発表済である．

2 つめの結果として，相対化する手法における障壁の特定を行った．ここで，相対化する手法とは理論計算機科学における帰着をベースにした証明における標準的な枠組みの一つである．このような標準的な枠組みについての障壁として，例えば，項目 C の成果からデータ分布の P/poly-samplable という仮定を無くそうとした場合，仮に NP よりも強い PH という計算複雑さクラスの平均時容易性を仮定したとしても，殆ど非自明な（例えば劣指数時間）学習さえできないことが分かった．この結果により，現在の標準的証明手法の障壁が明示的に与えられる一方で，そのような障壁に真に有効な手段の開発はできていないというのが現状である．逆に言えば，今後の分野のブレイクスルーによってそのような障壁が破られない限りは，項目 C で新たにおいたデータ生成分布の計算量的仮定は，学習に必要な計算要件を最悪時のものから平均時のものに緩和できるほど有効となり得るという可能性が示唆される．これは，学習問題における計算複雑さ理論的な観点からの更なる解析を動機づけるものである．なお，この結果は成果リスト(1) 3.中にて発表済である．

3. 今後の展開

本研究成果の中で特に今後の発展に繋がると期待されるものは，暗号理論・計算複雑さ理論と効率的学習困難性とのギャップがどこから生じるのかという点についての様々な新しい知見である．今後はこの知見を生かしながら更なるギャップの緩和に努め，（a)「効率的な暗号方式 vs 理論保証をもつ学習アルゴリズム」という，理論計算機科学における win-win な状況の達成，及び，学習における最悪時-平均時帰着（これは新しい評価軸での学習のブースティング技法の開発とも捉えられる）の開発を目指す．特に，本研究で得られた一つの重要な知見として，例えば 2-(2)-C 及び D で述べたように現在我々が直面する標準的証明手法の障壁は上手く（しかしながら現実的な設定の範疇で）学習要件を緩和することで，突破できる可能性があると言う点が挙げられる．今後はこのような要件緩和による障壁の回避を新たに視野に入れながら，ギャップの更なる解析を続け，将来的には，標準的証明手法の障壁を突破できるようなブレイクスルーに繋げることを目指す．

4. 自己評価

本研究では学習可能性判定の困難性の解析を出発点として，LIH 予想と暗号理論・計算複雑さ理論とのギャップの緩和に重点的に着手した．2-(2)-C の成果はその一つの部分的な解決と捉えることができる．また研究の中で，今後の更なるギャップの緩和に繋がる重要な知見も得ており，これらの点は本研究の成功した部分であると考える．その一方で，例えば，LIH 予想を基にした追加入力付き一方向性関数の構成など，現状では有効な解決手段が得られていない未解決課題も多く残っている．そのような課題についても，本研究により以前と比べて見通しは良くなっているため，ここでの知見をもとに戦略を練り直して再挑戦していきたいと考える．また本研究で得られた成果は CORE ランク A*国際会議 3 本(COLTx2, FOCSx1)を含む分野主要会議に採択されており，これは当該領域の個人研究の客観的評価としてもまずまずの成果であると考える．

本研究では元々，海外研究者との交流等を視野に入れつつ，予算の多くを旅費に充てていた．しかしながら，二年次から COVID-19 の流行の影響を受けることとなり，特に国際会議等での海外研究者との交流等を密に行えなかったという点は残念な点として挙げられる．しかしながら，その中でも zoom を活用した国内研究者との定期的な議論を行い，それは本研究を進める大きな助けとなった．加えて，一部の他の ACT-X 研究者とは現在，定期的なセミナーを行っており，ここで形成された若手交流の場は本領域終了後も続いていくものであると期待できる．この点で，当初の想定とは異なるが，本研究は研究者ネットワークの形成の良いきっかけとなったように考える．

5. 主な研究成果リスト

（1）代表的な論文（原著論文）発表

研究期間累積件数：5件

1. Mikito Nanashima, Extending Learnability to Auxiliary-Input Cryptographic Primitives and Meta-PAC Learning, In Proceedings of Thirty Third Conference on Learning Theory (COLT2020), 2020, PMLR 125, 2998-3029.
本論文では LIH 予想と効率的学習可能性判定，及び，従来の疑似乱数生成器の安全性要件を弱めた Auxiliary-Input Local Hitting Set Generator の存在の等価性を証明した．また，P≠NP と一方向性関数の存在間のギャップを学習理論の観点から自然に細分する，学習階層の概念を提唱した．
2. Mikito Nanashima, A Theory of Heuristic Learnability, In Proceedings of Thirty Fourth Conference on Learning Theory (COLT2021), 2021, PMLR 134, 3483-3525.
本論文では，従来の PAC 学習の任意のクラス内の関数を学習するという要件を，（ある分布の元で）平均時の意味で学習するという要件に緩和したモデルを Heuristic PAC 学習モデルとして明示的に定式化し，(a) junta 関数の提案モデルにおける効率的学習可能性の証明，及び，(b)多項式サイズ回路の学習可能性と追加入力付き一方向性関数の存在の等価性を証明した．
3. Shuichi Hirahara and Mikito Nanashima, On Worst-Case Learning in Relativized Heuristica, In Proceedings of Sixty Second IEEE Symposium on Foundations of Computer Science (FOCS2021), 2022 (in press)
本論文では，NP の平均時容易性の元で，多項式サイズ回路が任意の未知の P/poly-samplable（効率的サンプル可能な）データ分布の元で効率的に agnostic 学習可能であることを証明した，ここで，agnostic 学習とは PAC 学習よりもより強力な学習要件の学習である．また，現在の標準的証明手法の枠組み（相対化する証明）の中では，本論文で新たに導入したデータ分布の P/poly-samplable という仮定が，NP の平均時容易性の元での学習アルゴリズム設計において本質的に有効であることを理論的に示した．加えて同様の枠組みの中での PH 内における最悪時-平均時帰着のタイトな限界も明らかにしている．

（2）特許出願

（3）その他の成果（主要な学会発表、受賞、著作物、プレスリリース等）