論文 / 著書情報
Article / Book Information

題目(和文)	
Title(English)	Learning Theory in Heuristica and Pessiland
著者(和文)	七島幹人
Author(English)	Mikito Nanashima
出典(和文)	学位:博士(理学), 学位授与機関:東京工業大学, 報告番号:甲第12330号, 授与年月日:2023年3月26日, 学位の種別:課程博士, 審査員:伊東 利哉,渡辺 治,田中 圭介,鹿島 亮,安永 憲司
Citation(English)	Degree:Doctor (Science), Conferring organization: Tokyo Institute of Technology, Report number:甲第12330号, Conferred date:2023/3/26, Degree Type:Course doctor, Examiner:,,,,
学位種別(和文)	博士論文
Category(English)	Doctoral Thesis
種別(和文)	審査の要旨
Type(English)	Exam Summary

（博士課程）∩

論文審査の要旨及び審査員

報告番号	甲第　　号		学位申請者氏名		七島 幹人	
論文審査 審査員		氏　名	職　名		氏　名	職　名
	主査	伊東 利哉	教授	審査員	安永 憲司	准教授
	審査員	渡辺 治	教授			
		田中 圭介	教授			
		鹿島 亮	准教授			

論文審査の要旨（2000字程度）

本論文は「Learning Theory in Heuristica and Pessiland (NPの平均時容易性に基づく学習理論)」と題し，英文で全10章から構成されている．

これまでに，個別の問題の困難さに基づいて安全な暗号方式を構成する方法は知られていたが，一般のNP問題の困難さに基づいた安全な暗号方式を構成することは，理論計算機科学の分野における長年の未解決問題の一つである．そこで，最悪時間計算量においてNP問題が困難であるが平均時間計算量において容易である状況を想定した世界(Heuristica)と平均時間計算量においてNP問題が困難であるが一方向性関数が存在しない状況を想定した世界(Pessiland)が導入され，それらの2つの世界が起こり得ないことを示すことが，この未解決問題を解明する自然なアプローチとして位置付けられている．本論文では，計算量的学習理論の観点からHeuristicaとPessilandのアルゴリズム的な側面を解析し，上記の未解決問題の解決に向けた多くの理論的知見を得ることに成功している．

第1章「Introduction」では，論文全体の概要について述べるとともに，本論文で示す各成果についてその背景と動機を明らかにしている．

第2章「Preliminaries」では，本論文で用いる表記と重要な概念である計算量理論・平均時解析・学習理論・暗号理論などの導入を行っている．さらに，本論文におけるHeuristicaとPessilandに関する学習理論的な観点の主要結果に関連して，最悪時間計算量においてNP問題が容易であることを想定した世界(Algorithmica)に関する学習理論的な観点の結果を概観している．

第3章「Learning in Heuristica」では，ある計算量理論的仮定の下で，Heuristicaに対して多項式サイズ回路の最悪時間計算量におけるPAC学習可能性が導出されることを示している．これは最悪時間計算量におけるPAC学習不可能性から平均時間計算量におけるNP問題の困難性への最初の帰着である．

第4章「Learning in Pessiland I: A Unified Theory on Average-Case Learning」では，Pessilandにおいて，一方向性関数が存在しないと言う事実が様々な平均時間計算量におけるPAC学習可能性と等価であることを示している．これらの内の一つは，情報理論的に平均時間計算量におけるPAC学習不可能と予想されていた問題が含まれており，長年の未解決問題を否定的に解明している．

第5章「Learning in Pessiland II: More Dichotomies between Learning and Cryptography」では，Pessilandにおいて，一方向性関数が存在しないと言う事実が平均時間計算量におけるPAC学習可能性を導出すること，さらに，一方向性関数の条件を弱めた補助入力一方向性関数の存在と平均時間計算量におけるPAC学習不可能性が等価であることを示している．

第6章「Learning versus Pseudorandom Generators in Constant Parallel Time」では，より限定された計算モデル(深さが定数に制限された多項式サイズ回路)において定義される擬似乱数生成器の存在が様々な平均時間計算量におけるPAC学習不可能性と等価であることを導出している．

第7章「PACland: A World Where PAC Learning is Easy」」では，多項式サイズ回路がPAC学習可能であることを想定した世界(PACland)において，擬似乱数生成器の変種であるHitting Set生成器を対象とし，局所性を有する補助入力Hitting Set生成器の存在がPAC学習不可能と等価であることを示している．

第8章「On Basing Auxiliary-Input Cryptography on NP-Hardness」では，非適応的ブラックボックス安全性還元によりNP問題の困難性から補助入力Hitting Set生成器あるいは補助入力一方向性関数が構成可能であれば，適用的ブラックボックス安全性還元によりNP問題の困難性から一方向性関数が構成可能であることを導出している．この結果は，本論文の主目的である「HeuristicaとPessilandの除外」という未解決問題に対して新たなアプローチの道筋を提示している．

第9章「New and Improved Oracle Separations」では，相対化証明により，本論文で用いた技法の限界を提示している．具体的には，最悪時間計算量におけるNP問題の困難性と平均時間計算量におけるNP問題の容易性を結論付けるオラクルと誤りを許容しない平均時間計算量におけるNP問題の困難性と誤りを許容する平均時間計算量におけるNP問題の容易性を結論付けるオラクルを構成している．

第10章「Conclusions and Future Directions」では，本論文を総括するとともに，今後の課題について述べている．

以上のように，本論文では一般のNP問題の困難さに基づいた安全な暗号方式の構成可能性と言う理論計算機科学分野における長年の中心的未解決問題の一つに対し，計算量的学習理論の観点から解析を行い，学習アルゴリズムの出力仮説サイズの改善，平均時間計算量学習可能性の学習分布の一般化，補助入力Hitting Set生成器の非適応的ブラックボックス安全性還元に基づく構成などの多くの重要な理論的知見を与えている．これら本論文で得られた知見は，学習理論の側面から中心的未解決問題に対する具体的かつ多様なアプローチを可能にするものであり，計算量的学習理論という一つの学術分野に新たな価値を創造したという観点からも理学上貢献するところ大である．よって，本論文は博士（理学）の学位論文として十分価値があるものと認める．