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)	論文要旨
Type(English)	Summary

（博士課程）
Doctoral Program

論 文 要 旨

THESIS SUMMARY

系・コース： Department of, Graduate major in	数理・計算科学　系 数理・計算科学　コース	申請学位（専攻分野）： Academic Degree Requested	博士 Doctor of　（　理学　）
学生氏名： Student's Name	七島　幹人	指導教員（主）： Academic Supervisor(main)	伊東　利哉
		指導教員（副）： Academic Supervisor(sub)	

要旨（英文 800 語程度）
Thesis Summary (approx.800 English Words)

Heuristica and Pessiland, introduced by Impagliazzo (CCC'95), are possibilities of our world that are consistent with but far from our current knowledge. Heuristica is a world in which NP-problems are hard in the worst case but easy in the average case. Pessiland is a world in which NP-problems are hard in the average case, and there is no secure cryptography, particularly no central cryptographic primitive called one-way functions. Excluding the possibilities of Heuristica and Pessiland, i.e., basing a one-way function on the worst-case hardness of NP, is one of the most important challenges for unifying the central notions in computational complexity theory and cryptography. One natural approach for excluding Heuristic and Pessiland is to investigate algorithmic aspects of these possible worlds; e.g., to exclude Pessiland, we need to magnify the algorithmic aspects of Pessiland to efficient heuristic schemes that solve every NP-problem on average.

In this thesis, we study algorithmic aspects of Heuristica and Pessiland from the perspective of learning. This is motivated by the known facts that both the worst-case hardness of NP and the existence of one-way functions are characterized by the hardness of variants of Probability Approximately Correct (PAC) learning, as proved by Pitt and Valiant (J. ACM, 1990) and Blum, Furst, Kearns, and Lipton (Crypto'93), respectively. Our results are mainly classified into the following three topics.

I. Learning in Heuristica. We investigate connections between learning and average-case complexity. The original PAC learning model, introduced by Valiant (J. Commun. ACM, 1984), has a worst-case nature due to the requirement that a learner must learn all functions in the target class under all unknown example distributions, and the feasibility thus seems not to follow from the average-case easiness. We falsify this intuition by showing that the feasibility of worst-case PAC learning (even a more challenging task called agnostic learning) is indeed derived from the errorless average-case easiness of NP when the unknown example distributions are efficiently sampled by circuits. Namely, we obtain a reduction from worst-case learning to average-case NP under the additional computational assumption on example distributions.

II. Learning in Pessiland. We establish a robust and unified theory of average-case learning, which shows the equivalence between the non-existence of one-way functions and the feasibility of various average-case learning tasks, including average-case agnostic learning, average-case distributional learning, weak average-case learning with membership queries under the uniform example distribution, and learning adaptively changing distributions without knowledge of the distributions. It is worthy of note that the last learning task was previously thought to be information-theoretically impossible (Naor and Rothblum, ICML'06). We thus obtain a one-way function whose security is based on the intractability of a seemingly impossible average-case learning. In addition, we also present other duality results between learning and cryptography: (i) characterization of the existence of one-way functions by the average-case hardness of an NP-complete learning problem called MINLT in a well-studied average-case setting and (ii) new learning-theoretic characterizations of important cryptographic primitives, such as auxiliary-input one-way functions and polynomial-stretch pseudorandom generators computable in constant parallel time.

III. New and Improved Oracle Separations. We study the limitations of the standard proof framework called relativizing proofs. Here, relativizing proofs are proofs that hold even with additional access to an arbitrary oracle, and almost all results in theoretical computer science shown by reductions, including the main results in this thesis, can be shown by relativizing proofs. We show that, for further improvements of our results, we require profoundly new non-relativizing proofs. First, we show a strong oracle separation between worst-case and average-case complexity. Our result drastically improves the previous separation

result by Impagliazzo (CCC'11) and is tight because it matches the known upper bound shown by Hirahara (STOC'21). The oracle separation shows strong evidence that the additional computational assumption on example distributions is inevitable for any relativizing reduction from worst-case learning to average-case NP. Second, we show a new oracle separation between errorless and error-prone average-case complexity, which was asked in the seminal paper by Impagliazzo (CCC'95). We thus resolve the problem that had been open for more than two decades. The second separation result shows strong evidence that (i) the errorless condition is inevitable for any relativizing reduction from worst-case learning to average-case NP, and (ii) average-case requirements cannot be improved to worst-case even partially in our unified theory of average-case learning unless we develop a non-relativized technique.

Besides the topics above, we obtain a new characterization of the hardness of PAC learning by an auxiliary-input cryptographic primitive, more precisely, an auxiliary-input hitting set generator with a local condition. We further show that, for basing one-way functions on NP-hardness, it suffices to base such auxiliary-input cryptographic primitives on NP-hardness by a restricted form of nonadaptive black-box security reductions. Optimistically, this suggests a new approach towards excluding Heuristica and Pessiland, which reduces constructing a one-way function to constructing an auxiliary-input cryptographic primitive whose security condition is much more relaxed and even weaker than the hardness of PAC learning.