The Hong Kong University of Science and Technology

Department of Mathematics

PhD THESIS EXAMINATION

Robustness and Generalization in Neural Networks

By

Mr. Weizhi ZHU

ABSTRACT

Robustness and generalization of deep neural networks are two ad-hoc topics. Specifically, robust estimation under Huber's contamination model has become an important topic in statistics and theoretical computer science. Rate-optimal procedures such as Tukey's median and other estimators based on statistical depth functions are impractical because of their computational intractability. Margin enlargement over training data has been an important strategy since perceptrons in machine learning for the purpose of boosting the robustness of classifiers toward a generalization ability.

In this paper, we first study rate-optimal and computational feasible estimators under Huber's contamination model, by building connections between f-GANs, proper scoring rules and depth estimator. For example, we show that depth functions that lead to rate-optimal robust estimators can all be viewed as variational lower bounds of the total variation distance in the framework of f-Learning. Then we would revisit Breiman's dilemma in deep neural networks with recently proposed spectrally normalized margins. A novel perspective is provided to explain Breiman's dilemma based on phase transitions in the dynamic of the normalized margin distribution, which reflects the trade-off between the expressive power of models and the complexity of data.

Date: 07 December 2020, Monday

Time: 9:00 a.m.

Venue: Online via Zoom

https://hkust.zoom.com.cn/j/9298185364

(Passcode: weizhi.zhu)

***Thesis Examination Committee*:**

Chairman	**:**	**Prof. Vincent Kin Nang LAU, ECE/HKUST**
Thesis Supervisor	**:**	**Prof. Yuan YAO, MATH/HKUST**
Member	**:**	**Prof. Jianfeng CAI, MATH/HKUST**
Member	**:**	**Prof. Can YANG, MATH/HKUST**
Member	**:**	**Prof. Haifeng YOU, ACCT/HKUST**
External Examiner	**:**	**Prof. Kewei CHEN, School of Mathematics and Statistics / Arizona State University**

(Open to all faculty and students)

The student's thesis is now being displayed on the reception counter in the General Administration Office (Room 3461).