The Hong Kong University of Science and Technology

Department of Mathematics

PhD THESIS EXAMINATION

Generalization and Robustness in Deep Neural Networks

By

Mr. Yifei HUANG

ABSTRACT

In this thesis, we focus on the theory part of deep neural networks including generalization and robustness which are essential problems in deep learning.

Generalization of deep neural networks is still a mystery although deep learning has been successfully applied into many areas. What we pursue is to give an appropriate explanation for the success behind deep neural networks. In traditional machine learning community, margin dynamics have been used to explain the generalization of bagging and boosting. Motivated by this, we introduce the margin dynamics into deep neural networks to analyze the generalization abilities. A novel perspective is provided to explain the relationship between margin dynamics and generalization error based on phase transitions in dynamics of normalized margin distributions. On the other hand, the robustness of deep neural networks is another problem in deep learning. For most of the existing adversarial defense methods, they need adversarial training to improve robustness of neural networks, hence have to make a trade-off between natural accuracy and adversarial robustness. Inspired by Neural Ordinary Differential Equations (ODEs) and dynamical system theory, we design a stabilized neural ODE network named SONet whose ODE blocks are skew-symmetric and proved to be stable in the sense of Lyapunov.

Date: 05 August 2021, Thursday,

Time: 4:30 p.m.

Venue: Online via Zoom
https://hkust.zoom.us/j/8095658169 (Passcode: 834645)

***Thesis Examination Committee*:**

Chairman	**:**	**Prof. Pan HUI, CSE/HKUST**
Thesis Supervisor	**:**	**Prof. Yuan YAO, MATH/HKUST**
Member	**:**	**Prof. Can YANG, MATH/HKUST**
Member	**:**	**Prof. Yang WANG, MATH/HKUST**
Member	**:**	**Prof. Yangqiu SONG, CSE/HKUST**
External Examiner	**:**	**Prof. Yuling JIAO, Department of Information and Computational Sciences/Wuhan 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).