The Hong Kong University of Science and Technology

Department of Mathematics

PhD THESIS EXAMINATION

Studies on Privacy-Preserving Techniques and Sparsity in Neural Networks

By

Mr. Donghao LI

ABSTRACT

The rapid development of deep learning has ushered in a transformative era. This thesis will explore three important aspects in deep learning that require further research: data privacy, inference efficiency, and generalization ability. Firstly, the dependence of deep learning models on large amounts of data has raised concerns about data privacy. We will analyze potential vulnerabilities and discuss existing technologies, such as data publication algorithms with differential privacy and federated learning, to mitigate privacy risks. Secondly, the computational demands of deep learning models pose challenges for deployment on resource-constrained devices. We will investigate model compression methods based on sparsification. Lastly, we will explore the enhancement of neural network generalization through data augmentation. By addressing these key challenges, this paper aims to contribute to the responsible development and deployment of deep learning technologies, ensuring their effectiveness and ethical impact are carefully considered.

Date : 25 June 2024, Tuesday

Time : 10:00 am

Venue : Room 5501 (Lifts 25/26)

***Thesis Examination Committee*:**

Chairman	**:**	**Prof. Jun ZHANG, ECE/HKUST**
Thesis Supervisor	**:**	**Prof. Yuan YAO, MATH/HKUST**
Member	**:**	**Prof. Xinzhou GUO, MATH/HKUST**
Member	**:**	**Prof. Jianfeng CAI, MATH/HKUST**
Member	**:**	**Prof. Ruohan ZHAN, IEDA/HKUST**
External Examiner	**:**	**Prof. Xin XIE, College of Intelligence and Computing/ Tianjin 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).