For favour of Posting

THE HONG KONG UNIVERSITY OF SCIENCE & TECHNOLOGY

Department of Mathematics

PHD STUDENT SEMINAR

Overparametrized Model and Adversarial Robustness

By

Mr. Zhichao HUANG

Abstract

Deep neural networks can predict well even when fitting noisy data. The phenomenon is called benign overfitting. In this seminar, we analyze the overparametrized model under the adversarial perturbation, showing the fitting noise leads to sensitive models to the adversarial perturbation. In contrast to the natural risk where noise cancels out for each dimension, the small perturbation of each feature accumulates to significant change of the output in the adversarial attack. And we also study the adversarial training in these overparametrized models, showing that while it can increase the robustness of the model, it leads to distinct parameter to the oracle and decreases in performance for natural data.

Date : 6 May 2022 (Friday)
Time : 10:00am
Zoom Meeting : https://hkust.zoom.us/j/92129409608 (Passcode: 568117)

All are Welcome!