Department of Data Science

香港城市大學
City University of Hong Kong

Statistical Analysis of Adversarial Training

Date: 18 December 2024 (Wednesday)

Time: 9:30am - 10:30am

Seminar Link: https://cityu.zoom.us/j/85095945168

ABSTRACT

Motivated by data perturbation, adversarial training has recently been proposed as a new way of parameter estimation in supervised learning. This talk will discuss the statistical properties of the adversarial training estimator from both asymptotic and non- asymptotic perspectives. Firstly, the asymptotic distribution of the adversarial training estimator will be introduced, based on which a new technique has been proposed to improve the performance of existing adversarial training. Secondly, the non-asymptotic convergence rate of the adversarial training estimator is minimax optimal in high dimensional linear regression. My research aims to provide an understanding of emerging methods in machine learning and artificial intelligence, particularly from their statistical performance perspective. I will discuss some potential future topics.

DS SEMINAR

Ms. Yiling XIE

GUEST SPEAKER'S PROFILE

Ms Yiling XIE is a final-year Ph.D. candidate in the School of Industrial and Systems Engineering at the Georgia Institute of Technology. Her research focuses on developing robust and efficient statistical methodologies to advance machine learning and artificial intelligence. Yiling's research has earned numerous awards, such as being the Runner-up in the 2023 INFORMS Data Mining Best Student Paper Competition, the Winner of the Best Student Poster Competition at the 2024 Georgia Statistics Day, and a Finalist in the 2024 IISE Data Analytics & Information Systems Best Student Paper Competition. Her personal website: https://sites.google.com/view/yilingxie/home

Enquiries: ds.go@cityu.edu.hk

All are welcome