THE UNIVERSITY OF HONG KONG

Institute of Mathematical Research
Department of Mathematics

Optimization and Machine Learning Seminar

Optimal Classification-based Anomaly Detection with Neural Networks: Theory and Practice in Cybersecurity

Miss. Tian-Yi Zhou
Georgia Institute of Technology, USA

Abstract

Anomaly detection is an important problem in many application areas, such as network security. Many deep learning methods for unsupervised anomaly detection produce good empirical performance but lack theoretical guarantees. By casting anomaly detection into a binary classification problem, we establish non-asymptotic upper bounds and a convergence rate on the excess risk on rectified linear unit (ReLU) neural networks trained on synthetic anomalies. Our convergence rate on the excess risk matches the minimax optimal rate in the literature. Furthermore, we provide lower and upper bounds on the number of synthetic anomalies that can attain this optimality. For practical implementation, we relax some conditions to improve the search for the empirical risk minimizer, which leads to competitive performance to other classification-based methods for anomaly detection. Overall, our work provides the first theoretical guarantees of unsupervised neural network-based anomaly detectors and empirical insights on how to design them well.

Date:	December 23, 2024 (Monday)
Time:	4:00 pm – 5:00 pm
Venue:	Room 210, Run Run Shaw Building HKU

All are welcome