香港中文大學統計學系
Department of Statistics
THE CHINESE UNIVERSITY OF HONG KONG

SEMINAR

DEPARTMENT OF STATISTICS
THE CHINESE UNIVERSITY OF HONG KONG

Domain Generalization with Adversarially Robust Learning: Identification, Estimation, and Uncertainty Quantification

INVITED SPEAKER

Zijian Guo
Associate Professor
Department of Statistics
Rutgers University

TIME

January 17, 2024 (Wed) · 2:00 pm - 3:00 pm

VENUE

LPN LT · Y.C. Liang Hall - LPN LT · CUHK

ABSTRACT

Empirical risk minimization may lead to poor prediction performance when the target distribution differs from the source populations. This talk discusses leveraging data from multiple sources and constructing more generalizable and transportable prediction models. We introduce an adversarially robust prediction model to optimize a worst-case reward concerning a class of target distributions and show that our introduced model is a weighted average of the source populations' conditional outcome models. We leverage this identification result to robustify arbitrary machine learning algorithms, including, for example, high-dimensional regression, random forests, and neural networks.

In our adversarial learning framework, we propose a novel sampling method to quantify the uncertainty of the adversarial robust prediction model. Moreover, we introduce guided adversarially robust transfer learning (GART) that uses a small amount of target domain data to guide adversarial learning. We show that GART achieves a faster convergence rate than the model fitted with the target data. Our comprehensive simulation studies suggest that GART can substantially outperform existing transfer learning methods, attaining higher robustness and accuracy.