Statistical Learning under Adversarial Distribution Shift

Chen Dan

November 2021

School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213

Thesis Committee:
Pradeep Ravikumar, Chair
Zico Kolter
Zachary Lipton
Avrim Blum (Toyota Technological Institute in Chicago)
Yuting Wei (University of Pennsylvania)

*Submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy.*

Keywords: Statistical Learning

Abstract

One of the most fundamental assumptions in statistical machine learning is that training and testing data should be sampled independently from the same distribution. However, modern real world applications require that the learning algorithm should perform robustly even when this assumption is no longer valid. Specifically, the training and testing distributions may shift slightly (yet adversarially) within a small neighborhood of each other. This formulation encompasses many new challenges in machine learning, including adversarial examples, outlier contaminated data, group fairness and label imbalance.

In this thesis, we seek to understand the statistical optimality and provide better algorithms under aforementioned adversarial distrbution shift. Our contributions include (1) the first near optimal minimax lower bound for the sample complexity of adversarially robust classification in a Gaussian setting. (2) introducing the framework of distributional and outlier robust optimization, which allowed us to apply distributionally robust optimization to large scale experiments with deep neural networks and outperformed existing methods in sub-population shift tasks.

Finally, we provide preliminary results on two on-going projects about label imbalance and sub-population shift under over-parameterized and high-dimensional data.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Chapter 2

Proposed Works

Bibliography