August 31 - September 6 Seminar Review

Jiaxin Hu

September 2, 2020

1 8.31 IFDS

Title: The Teaching Dimension of Reinforcement Learning
Presenter: Xuezhou Zhang

People usually teach in two ways: demonstration and reinforcement. Today's talk studies the sample complexity for teaching by reinforcement named "teaching dimension". The presenter discusses the complexity by cases: 1. the teacher generates the arbitrary state-reward vector and overrides the action; 2. the teacher generates the arbitrary state-reward vector but the agent has "free will" to choose the action; 3. the teacher generates arbitrary rewards and the environment-supported states; 4. the teacher generates only arbitrary rewards, and the states are sampled from the environment. Under different controlling levels, the sample complexity increases as the teacher is less deterministic. The presenter not only finds the theoretical complexities but also provides optimal teaching algorithms (e.g. navigation algorithm) that match the optimal teaching dimensions.

Questions: 1. Can this study help us to choose the teaching strategy in practice?
Possible Answer: In practice, we may first evaluate the sizes of action sets, state space, and other related parameters. Then, we determine the strategy after balancing the theoretical complexity and the our goal.

2 9.2 SILO

The Mysteries of Adversarial Robustness for Non-parametric Methods
Presenter: Kamalika Chaudhuri

Adversarial examples are small perturbations to the input that may cause the classifier to misclassify. Today's talk focuses on the adversarial robust non-parametric methods which address the adversarial issue. The robustness of the classification is developed through letting a neighborhood of data points be classified into the same group. Therefore, the goal of robust classification is not to maximize the prediction accuracy, but to maximize the *astuteness* which combines the robustness and accuracy. The optimal classifier is called the r-optimal classifier. The presenter applies the idea of robustness to the non-parametric methods like KNN. For separated data, robust classifiers converge to r-optimal under certain conditions. For non-separated data, an adversarial pruning algorithm is provided. Last, the presenter concludes that the robustness of non-parametric methods depends on the algorithm. However, the current algorithms for parametric methods like Neural Network may not be generalized enough to find a robust classifier.