מכון ויצמן למדע

THE WEIZMANN INSTITUTE OF SCIENCE

FACULTY OF MATHEMATICS AND COMPUTER SCIENCE

Vision and Robotics Seminar

on Thursday, May 06, 2021
at 12:15

https://weizmann.zoom.us/j/97720109091?pwd=LzdheCt3VWpXRFFOSGJaa3lkc0JyZz09 A Joint Computer Vision & Machine Learning seminar

Nathan Srebro
Toyota Technological Institute at Chicago

What, How and When can we Learn Adversarially Robustly?

Abstract:

In this talk we will discuss the problem of learning an adversarially robust predictor from clean training data. That is, learning a predictor that performs well not only on future test instances, but also when these instances are corrupted adversarially. There has been much empirical interest in this question, and in this talk we will take a theoretical perspective and see how it leads to practically relevant insights, including: the need to depart from an empirical (robust) risk minimization approach, and thinking of what kind of accesses and reductions can allow learning. Joint work with Omar Montasser and Steve Hanneke.