THE UNIVERSITY OF CHICAGO | DEPARTMENT OF STATISTICS

MASTER'S THESIS PRESENTATION

YI GU

Department of Statistics
The University of Chicago

Designing Robust Neural Network Architectures: Hardness and Trade-offs

MONDAY, May 1, 2023, at 2:30 PM
Jones 226, 5747 S. Ellis Avenue

ABSTRACT

Convolutional neural networks (CNN) has been one of the most successful applications of deep learning.. However, CNN could be easily fooled by images with human-invisible perturbations. Various defensive mechanism has been developed, the very first defense was to training the network with adversarial examples. Recently, there are new lines of work trying to restrict the neural networks as Lipschitz functions. In this paper, we attempt to build robust networks from a different perspective: (1) we explored the possibility of building adversarial robust CNNs with features generated by fixed convolution weights plus specially designed activations. (2) We compared it with existing robust architectures and studied the tradeoffs in adversarial attacks and defenses.